ACTA ARITHMETICA
LX.3 (1992)

Effective finiteness theorems for decomposable forms of given discriminant

by

J. H. Evertse* (Leiden) and K. Győry** (Debrecen)

Introduction. Let K be an algebraic number field, S a finite set of prime ideals in K and O_S the ring of S-integers in K. Two binary forms $F(X,Y), G(X,Y) \in O_S[X,Y]$ are called *equivalent* if there is a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2, O_S)$ such that $G(X,Y) = F(\alpha X + \beta Y, \gamma X + \delta Y)$. In 1972, Birch and Merriman [1] proved that for given integer $r \geq 3$, there are only finitely many equivalence classes of binary forms $F \in O_S[X,Y]$ of degree r whose discriminant $D(F)$ belongs to the group of S-units O_S^*. The proof in [1] is ineffective in the sense that it does not provide an algorithm to find a full set of representatives for these equivalence classes. In a series of papers, Győry [8], [9], [12] obtained effective finiteness results for monic polynomials with coefficients in O_S and with given non-zero discriminant; for binary forms F with $F(1,0) = 1$ these results imply an effective version of Birch and Merriman's theorem. In our recent paper [6] we made the result of Birch and Merriman effective in full generality, without any restriction on F.

The purpose of the present paper is to extend our results from [6] on binary forms to decomposable forms in $n \geq 2$ variables. The general result over algebraic number fields is stated in Section 2; here we restrict ourselves to the case of the field of rationals $\mathbb{Q}$. Let $\{p_1, \ldots, p_s\}$ $(s \geq 0)$ be a finite set of primes and consider the ring $R = \mathbb{Z}[(p_1 \ldots p_s)^{-1}]$. A polynomial $F(\mathbf{X}) \in R[X_1, \ldots, X_n]$ is called a *decomposable form* if it can be factored as $F(\mathbf{X}) = \lambda l_1(\mathbf{X})^{k_1} \ldots l_t(\mathbf{X})^{k_t}$ where $\lambda \in \mathbb{Q}^*$, $l_1, \ldots, l_t$ are pairwise non-proportional homogeneous linear polynomials with coefficients in some algebraic number field L and $k_1, \ldots, k_t$ are positive integers with $k_1 + \ldots + k_t = \deg(F)$.

* The research of the first author has been made possible by a fellowship of the Royal Netherlands Academy of Arts and Sciences.

** The research of the second author has been supported in part by Grant 273 from the Hungarian National Foundation for Scientific Research.

Let $\mathcal{I}(F)$ be the collection of L-linearly independent subsets $\{l_{i_1},\dots,l_{i_n}\}$ (n = number of variables of F) of $\{l_1,\dots,l_t\}$. We denote the coefficient determinant of $\{l_{i_1},\dots,l_{i_n}\} \in \mathcal{I}(F)$ by $\det(l_{i_1},\dots,l_{i_n})$. Further, by $\widehat{R}$ we denote the integral closure of R in L. Denote by (a) the $\widehat{R}$-ideal generated by a, and by (l_i) the $\widehat{R}$-ideal generated by the coefficients of l_i for $i = 1,\dots,t$. Assume that $\mathcal{I}(F) \neq \emptyset$. Then there is a positive rational integer $D = D_R(F)$, composed of prime numbers outside $\{p_1,\dots,p_s\}$, such that

$$(D) = \prod_{\mathcal{I}(F)} \left\{ \frac{\det(l_{i_1},\dots,l_{i_n})}{(l_{i_1})\dots(l_{i_n})} \right\}^2,$$

where the product is taken over all sets $\{l_{i_1},\dots,l_{i_n}\}$ in $\mathcal{I}(F)$; further, the integer D does not depend on the choice of $l_1,\dots,l_t$ (cf. Section 3) and $D_R(\mu F) = D_R(F)$ for all $\mu \in \mathbb{Q}^*$. The integer $D_R(F)$ is called the *R-discriminant* of F. If $\mathcal{I}(F) = \emptyset$ then we put $D_R(F) = 0$. For instance, if F is a binary form with relatively prime coefficients in $\mathbb{Z}$, then $D_{\mathbb{Z}}(F)$ is just the absolute value of the discriminant $D(F)$ of F. Two decomposable forms $F(\mathbf{X}), G(\mathbf{X}) \in R[X_1,\dots,X_n]$ are called *R-equivalent* if there is a matrix $U \in \mathrm{GL}(n,R)$ with $G(\mathbf{X}) = F(U\mathbf{X})$. Two R-equivalent decomposable forms have the same R-discriminant (cf. Section 1). The *height* of a rational number a/b with $a,b \in \mathbb{Z}$, $\gcd(a,b) = 1$ is defined by $h(a/b) = \max(|a|,|b|)$; the *height $h(F)$ of a polynomial F* with coefficients in $\mathbb{Q}$ is defined as the maximum of the heights of the coefficients of F. We have

THEOREM 1. *Let $F(\mathbf{X}) \in R[X_1,\dots,X_n]$ be a decomposable form of degree r with relatively prime coefficients and with $D_R(F) = D \neq 0$. Then F is R-equivalent to a decomposable form G with $h(G) \leq C$, where C is an effectively computable number depending only on n, r, D, s and $p_1,\dots,p_s$.*

We remark that Theorem 1 implies, in an effective way, that there are only finitely many R-equivalence classes of decomposable forms in $R[X_1,\dots,X_n]$ with relatively prime coefficients, with given degree and given non-zero R-discriminant.

For $n = 2$ and $R = \mathbb{Z}$ (when $s = 0$), Theorem 1 gives (in a less explicit form) Theorem 1 of [6] on binary forms with given discriminant.

We shall get Theorem 1 as a special case of a more general result on decomposable forms on O_S-modules, where O_S is the ring of S-integers of an algebraic number field (cf. Section 2, Corollary 4). The proof of this general result uses an effective result of Győry ([10], Lemma 6) on the S-unit equation in two variables; so the proof of our result ultimately goes back to Baker's theory on linear forms in logarithms and its p-adic analogue.

As an application of our general results on decomposable forms, we deduce (cf. Section 2, Corollary 6) an effective finiteness result for finitely

generated O_S-modules with given discriminant. Our results on decomposable forms can also be applied to the study of decomposable form equations of the form

$$(*) \qquad F(\mathbf{x}) = a \quad \text{in } \mathbf{x} = (x_1, \dots, x_n) \in R^n ,$$

where $F(\mathbf{X})$ is as in Theorem 1 and $a \in R \setminus \{0\}$. For instance, if one can prove that the set of solutions of $(*)$ has a special structure provided that $D_R(F)$ is sufficiently large, then it follows that there are only finitely many R-equivalence classes of decomposable forms F for which the set of solutions of $(*)$ does not have that special structure. A result of this type will be published in a forthcoming paper of the first author [3], which extends to the case $n \geq 2$ Theorem 2(i) of [5] obtained for $n = 2$. Another possible application concerns effective results on equation $(*)$. For a certain class of decomposable forms which is invariant under linear transformations of F and which includes binary forms, discriminant forms, index forms and certain special norm forms (cf. [11], [4]) it is possible to give an effectively computable number C'_F depending only on n, r, s, $p_1, \dots, p_s$, $h(F)$ and a, such that $\max_i h(x_i) \leq C'_F$ for every solution $\mathbf{x} = (x_1, \dots, x_n)$ of $(*)$. It might be possible to improve this bound in certain cases, by first looking for a matrix $U \in \mathrm{GL}(n, R)$ such that $G(\mathbf{X}) = F(U\mathbf{X})$ has height $\leq C$, then computing the upper bound C'_G for the heights of the solutions of $(*)$ with F replaced by G and finally deriving an upper bound for the heights of the solutions $\mathbf{x}$ of $(*)$ by estimating from above the heights of the entries of U^{-1}. Probably we shall publish a paper about these effective results.

In Section 1, we introduce some general notions about decomposable forms which will be needed in the later sections. In Section 2, we state our effective results about decomposable forms on O_S-modules. The remaining sections will be devoted to the proofs of these results.

1. General facts on decomposable forms. Let K be a field and V a finite-dimensional K-vector space. A *decomposable form* on V is a function $F : V \to K$ with the following property: there are an extension L/K, a positive integer r and K-linear functions $l_i : V \to L$ $(i = 1, \dots, r)$ such that

$$(1.1) \qquad F(\mathbf{x}) = l_1(\mathbf{x}) \dots l_r(\mathbf{x}) \quad \text{for all } \mathbf{x} \in V .$$

We call $(l_1, \dots, l_r)$ a *factorization* of F in L. If K is infinite then r is uniquely determined by F; in this case r is called the *degree* of F. The smallest extension L of K in which F has a factorization is called the *splitting field* of F over K; it is a finite, normal extension of K. The *rank* of F is defined as the dimension of the L-vector space of K-linear functions generated by $\{l_1, \dots, l_r\}$. It is easy to see that rank F is independent of $l_1, \dots, l_r$ and L and is at most $\dim_K V$. We say that F is of *maximal rank*

if rank $F = \dim_K V$.

Let K^n be the space consisting of all n-dimensional column vectors with entries in K. The vectors $\mathbf{e}_1 = (1, 0, \ldots, 0)^T, \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)^T$ form the standard basis of K^n. We shall identify a decomposable form F on K^n with the homogeneous polynomial $F(\mathbf{X}) = F(X_1\mathbf{e}_1 + \ldots + X_n\mathbf{e}_n) \in K[X_1, \ldots, X_n]$. This homogeneous polynomial is also called a decomposable form.

Let R be an integral domain (always with 1) with quotient field K. An *R-lattice* is a finitely generated R-submodule of a K-vector space. An R-lattice $\mathfrak{M}$ contained in the K-vector space V is called an R-lattice in V. We define rank $\mathfrak{M}$ as the dimension $\dim_K K\mathfrak{M}$ over K of the K-vector space $K\mathfrak{M} = \{\lambda\mathbf{x} : \lambda \in K,\ \mathbf{x} \in \mathfrak{M}\}$. An *$R$-lattice decomposable form pair* is a pair $(\mathfrak{M}, F)$ consisting of an R-lattice $\mathfrak{M}$ and a decomposable form F on $K\mathfrak{M}$ of maximal rank. Two R-lattice decomposable form pairs $(\mathfrak{M}_1, F_1)$ and $(\mathfrak{M}_2, F_2)$ are called *equivalent* if there is an R-module isomorphism $\varphi : \mathfrak{M}_1 \to \mathfrak{M}_2$ such that

$$F_2(\varphi(\mathbf{x})) = F_1(\mathbf{x}) \quad \text{for all } \mathbf{x} \in \mathfrak{M}_1 \tag{1.2}$$

and *weakly equivalent* if there are an R-module isomorphism $\varphi : \mathfrak{M}_1 \to \mathfrak{M}_2$ and ([1]) $\lambda \in K^*$ such that

$$\lambda F_2(\varphi(\mathbf{x})) = F_1(\mathbf{x}) \quad \text{for all } \mathbf{x} \in \mathfrak{M}_1\,. \tag{1.3}$$

Example 1. Let $n \geq 1$ and R^n the lattice of n-dimensional column vectors with entries in R. The group of R-module automorphisms of R^n is given by $\{\mathbf{x} \mapsto U\mathbf{x} : U \in \mathrm{GL}(n, R)\}$, where $\mathrm{GL}(n, R)$ is the multiplicative group of $n \times n$ matrices with entries in R and with determinant contained in the unit group R^* of R. Hence two R-lattice decomposable form pairs (R^n, F_1) and (R^n, F_2) are equivalent if and only if there is a $U \in \mathrm{GL}(n, R)$ with $F_2(U\mathbf{x}) = F_1(\mathbf{x})$ for $\mathbf{x} \in R^n$, and weakly equivalent if and only if there are $\lambda \in K^*$ and $U \in \mathrm{GL}(n, R)$ with $\lambda F_2(U\mathbf{x}) = F_1(\mathbf{x})$ for $\mathbf{x} \in R^n$.

Example 2. Let M/K be a finite, separable extension with norm $N_{M/K} : M \to K$. Then $N_{M/K}$ is the product of the distinct K-isomorphisms $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \ldots, [M : K])$ of M which are K-linear functions. Hence $N_{M/K}$ is a decomposable form of maximal rank on M which is called a *norm form*. Let $\mathfrak{M}$ be an R-lattice in M and denote the restriction of $N_{M/K}$ to $K\mathfrak{M}$ also by $N_{M/K}$. Then $(\mathfrak{M}, N_{M/K})$ is an R-lattice decomposable form pair. It is not difficult to prove that if $\mathfrak{M}_1$, $\mathfrak{M}_2$ are two R-lattices in M, then $(\mathfrak{M}_1, N_{M/K})$ and $(\mathfrak{M}_2, N_{M/K})$ are weakly equivalent if and only

([1]) For any integral domain R, R^* will denote the unit group of R; thus if R is a field then $R^* = R \setminus \{0\}$.

if there are $\mu \in M^*$ and a K-isomorphism σ of M such that

$$\mathfrak{M}_2 = \mu\sigma(\mathfrak{M}_1)\,.$$

Let now R be a Dedekind domain with quotient field K of characteristic 0 (for instance the ring of S-integers of an algebraic number field). By an R-ideal we mean a non-zero R-lattice in K; R-ideals contained in R are said to be *integral*. The R-ideal or, more generally, R-lattice generated by $\alpha_1, \dots, \alpha_m$ is denoted by $(\alpha_1, \dots, \alpha_m)$.

By a result of Kaplansky [14] (see also [18], Ch. I, §2), every R-lattice of rank n is isomorphic to $R^{n-1} \oplus \mathfrak{a}$ for some R-ideal $\mathfrak{a}$. Moreover, $R^{n-1} \oplus \mathfrak{a}$ and $R^{n-1} \oplus \mathfrak{b}$ are isomorphic if and only if $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ denote, as usual, the standard basis of K^n. Since every R-ideal can be generated by at most two elements, every R-lattice $\mathfrak{M}$ of rank n is isomorphic to either

$$\begin{aligned} &(\mathbf{e}_1, \dots, \mathbf{e}_n) = R^n \quad \text{(if } \mathfrak{M} \text{ is free)} \quad \text{or} \\ &(\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n) \quad \text{(if } \mathfrak{M} \text{ is not free)}\,, \end{aligned} \tag{1.4}$$

where $\alpha, \beta \in R$ and the ideal $\mathfrak{a} = (\alpha, \beta)$ is not principal. Let $\mathfrak{M}$ be an R-sublattice of R^n of rank n. Then for every R-module automorphism φ of $\mathfrak{M}$ there is a unique $n \times n$ matrix with entries in K such that $\varphi(\mathbf{x}) = U\mathbf{x}$ for all $\mathbf{x} \in \mathfrak{M}$. Let $G(\mathfrak{M})$ be the group of matrices corresponding to the automorphisms of $\mathfrak{M}$. Then, trivially, two R-lattice decomposable form pairs $(\mathfrak{M}, F_1)$ and $(\mathfrak{M}, F_2)$ are equivalent (or weakly equivalent) if and only if there is (are) $U \in G(\mathfrak{M})$ (and $\lambda \in K^*$) such that

$$F_2(\mathbf{x}) = F_1(U\mathbf{x}) \quad (\lambda F_2(\mathbf{x}) = F_1(U\mathbf{x}),\ \text{resp.}) \quad \text{for all } \mathbf{x} \in \mathfrak{M}\,.$$

It is obvious that $G(R^n) = \mathrm{GL}(n, R)$. Further, the following can be easily verified: if $\mathfrak{M} = (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$ where $\alpha, \beta \in R$ and $\mathfrak{a} = (\alpha, \beta)$ is non-principal, then

$$G(\mathfrak{M}) = \left\{ U = \begin{pmatrix} u_{11} & \dots & u_{1n} \\ \dots\dots\dots\dots & & \\ u_{n1} & \dots & u_{nn} \end{pmatrix} : \begin{array}{l} u_{ij} \in R \text{ for } 1 \le i,\ j \le n-1;\ u_{nn} \in R\,; \\ u_{in} \in \mathfrak{a}^{-1} \text{ for } 1 \le i \le n-1;\ u_{nj} \in \mathfrak{a} \text{ for } 1 \le j \le n-1\,; \\ \det U \in R^*\,. \end{array} \right\} \tag{1.5}$$

Let $(\mathfrak{M}, F)$ be an R-lattice decomposable form pair such that rank $\mathfrak{M} = n$, $\deg(F) = r$ and F has splitting field L, and put $V = K\mathfrak{M}$. We can factor F as

$$F(\mathbf{x}) = \lambda \prod_{i=1}^{t} l_i(\mathbf{x})^{k_i} \quad \text{for all } \mathbf{x} \in V\,, \tag{1.6}$$

where $\lambda \in K^*$, $l_1, \ldots, l_t : V \to L$ are pairwise L-linearly independent linear functions and $k_1, \ldots, k_t$ are positive integers with $k_1 + \ldots + k_t = r$. Let $\widehat{R}$ be the integral closure of R in L. For any R-ideal $\mathfrak{b}$ in K we shall write $\mathfrak{b}$ instead of $\mathfrak{b}\widehat{R}$. Let $l_i(\mathfrak{M})$ be the set consisting of the elements $l_i(\mathbf{x})$, $\mathbf{x} \in \mathfrak{M}$, $i = 1, \ldots, t$. One can show (cf. Section 3) that there is an R-ideal $\mathfrak{c}(\mathfrak{M}, F)$, called the *content* of $(\mathfrak{M}, F)$, such that

$$\mathfrak{c}(\mathfrak{M}, F) = (\lambda) \prod_{i=1}^{t} (l_i(\mathfrak{M}))^{k_i}\,, \tag{1.7}$$

where (λ), $(l_i(\mathfrak{M}))$ denote the $\widehat{R}$-ideals in L generated by λ and $l_i(\mathfrak{M})$, respectively. It is easy to check that the definition of the content is independent of the choice of λ, $l_1, \ldots, l_t$. It is also easy to verify that if $(\mathfrak{M}, F)$ and $(\mathfrak{M}', F')$ are *equivalent* R-lattice decomposable form pairs, then

$$\mathfrak{c}(\mathfrak{M}, F) = \mathfrak{c}(\mathfrak{M}', F')\,. \tag{1.8}$$

We now introduce the *discriminant* of $(\mathfrak{M}, F)$. Let $\mathcal{I}(F)$ be the collection of L-linearly independent subsets $\{l_{i_1}, \ldots, l_{i_n}\}$ (with $n = \operatorname{rank} \mathfrak{M} = \dim_K V$) of $\{l_1, \ldots, l_t\}$. For $\mathcal{L} = \{l_{i_1}, \ldots, l_{i_n}\} \in \mathcal{I}(F)$, let $\mathfrak{d}(\mathfrak{M}, \mathcal{L})$ be the $\widehat{R}$-ideal in L generated by all numbers

$$\det \begin{pmatrix} l_{i_1}(\mathbf{x}_1) & \cdots & l_{i_n}(\mathbf{x}_1) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ l_{i_1}(\mathbf{x}_n) & \cdots & l_{i_n}(\mathbf{x}_n) \end{pmatrix}$$

with $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathfrak{M}$. (We remark that $\mathfrak{d}(\mathfrak{M}, \mathcal{L})$ is indeed finitely generated, since there is an $\alpha \in L^*$ with $\alpha\mathfrak{d}(\mathfrak{M}, \mathcal{L}) \subseteq \widehat{R}$). The ideal

$$\mathfrak{D}(\mathfrak{M}, F) = \prod_{\mathcal{L} \in \mathcal{I}(F)} \left(\frac{\mathfrak{d}(\mathfrak{M}, \mathcal{L})}{(l_{i_1}(\mathfrak{M})) \ldots (l_{i_n}(\mathfrak{M}))} \right)^2 \tag{1.9}$$

where the product is taken over all sets $\mathcal{L} = \{l_{i_1}, \ldots, l_{i_n}\}$ in $\mathcal{I}(F)$, is called the *discriminant* of $(\mathfrak{M}, F)$. In the trivial case $n = 1$ we have $\mathfrak{D}(\mathfrak{M}, F) = (1)$. In Section 3 we shall show that $\mathfrak{D}(\mathfrak{M}, F)$ is an *integral* R-ideal. (We remark that without squaring, the ideal on the right-hand side of (1.9) would be contained in $\widehat{R}$ but not necessarily in R.) Further, since by assumption F is of maximal rank, $\mathfrak{D}(\mathfrak{M}, F)$ is non-zero.

If the linear functions $l_1, \ldots, l_t$ are multiplied by constants $\alpha_1, \ldots, \alpha_t$, respectively, then for $\mathcal{L} = \{l_{i_1}, \ldots, l_{i_n}\} \in \mathcal{I}(F)$, both the ideals $\mathfrak{d}(\mathfrak{M}, \mathcal{L})$ and $(l_{i_1}(\mathfrak{M})) \ldots (l_{i_n}(\mathfrak{M}))$ are multiplied by $\alpha_{i_1}, \ldots, \alpha_{i_n}$. Hence the right-hand side of (1.9) does not change. This implies that the definition of $\mathfrak{D}(\mathfrak{M}, F)$ is independent of the choice of λ, $l_1, \ldots, l_t$. Moreover,

$$\mathfrak{D}(\mathfrak{M}, \mu F) = \mathfrak{D}(\mathfrak{M}, F) \quad \text{for all } \mu \in K^*\,. \tag{1.10}$$

Let now $(\mathfrak{M}', F')$ be an R-lattice decomposable form pair which is equivalent to $(\mathfrak{M}, F)$. Then

$$F'(\mathbf{x}') = \lambda \prod_{i=1}^{t} l_i'(\mathbf{x}')^{k_i} \quad \text{for all } \mathbf{x}' \in \mathfrak{M}',$$

where $l_i' = l_i \circ \varphi^{-1}$ for $i = 1, \dots, t$ and some R-module isomorphism $\varphi : \mathfrak{M} \to \mathfrak{M}'$. It is trivial that $l_i'(\mathfrak{M}') = l_i(\mathfrak{M})$ for $i = 1, \dots, t$ and that $\mathfrak{d}(\mathfrak{M}', \mathcal{L}') = \mathfrak{d}(\mathfrak{M}, \mathcal{L})$ for all $\mathcal{L} \in \mathcal{I}(F)$, where $\mathcal{L}' := \{l_i' : l_i \in \mathcal{L}\}$. Hence $\mathfrak{D}(\mathfrak{M}', F') = \mathfrak{D}(\mathfrak{M}, F)$. Together with (1.10) this implies that if $(\mathfrak{M}, F)$, $(\mathfrak{M}', F')$ are two weakly equivalent R-lattice decomposable form pairs, then

$$\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{D}(\mathfrak{M}', F'). \tag{1.11}$$

EXAMPLE 3. Let $F(X, Y) \in R[X, Y]$ be a binary form without multiple factors and with splitting field L. Then F can be factored in $L[X, Y]$ as

$$F(X, Y) = \prod_{i=1}^{r} (\alpha_i X - \beta_i Y)$$

with $\alpha_i, \beta_i \in L$ and $\alpha_i \beta_j - \alpha_j \beta_i \neq 0$ for $1 \leq i < j \leq r$. A straightforward computation shows that the discriminant of the R-lattice binary form pair (R^2, F) is equal to

$$\mathfrak{D}(R^2, F) = \mathfrak{c}(R^2, F)^{-(2r-2)} \Big(\prod_{1 \leq i < j \leq r} (\alpha_i \beta_j - \alpha_j \beta_i)^2 \Big).$$

It is not difficult to prove that if R is the ring of S-integers of an algebraic number field, then $\mathfrak{D}(R^2, F)$ is just the S-discriminant of F defined in [6].

EXAMPLE 4. Let $F(\mathbf{X}) \in K[X_1, \dots, X_n]$ be a decomposable form (i.e. a decomposable form on K^n). Then $F(\mathbf{X}) = \lambda l_1(\mathbf{X})^{k_1} \dots l_t(\mathbf{X})^{k_t}$ where $\lambda \in K^*$ and $l_1, \dots, l_t$ are pairwise non-proportional linear forms with coefficients in the splitting field L of F. It is easy to verify that if F is of maximal rank then

$$\mathfrak{D}(R^n, F) = \prod_{\mathcal{I}(F)} \left(\frac{\det(l_{i_1}, \dots, l_{i_n})}{(l_{i_1}) \dots (l_{i_n})} \right)^2,$$

where $\mathcal{I}(F)$ is the collection of L-linearly independent subsets $\{l_{i_1}, \dots, l_{i_n}\}$ of $\{l_1, \dots, l_t\}$ and where (l_i) denotes the $\widehat{R}$-ideal generated by the coefficients of l_i. Hence for the ring $R = \mathbb{Z}[(p_1 \dots p_s)^{-1}]$ considered in the Introduction, $\mathfrak{D}(R^n, F)$ is equal to (D_R).

We now give another characterization for the discriminant. Let $(\mathfrak{M}, F)$ be an R-lattice decomposable form pair as above. Every R-ideal $\mathfrak{a}$ can be uniquely expressed as

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})},$$

where the product is taken over all prime ideals $\mathfrak{p}$ of R and where the exponents $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ are integers of which at most finitely many are non-zero. For $\alpha \in K$ we put $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}((\alpha))$ if $\alpha \neq 0$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \infty$ if $\alpha = 0$. Fix a prime ideal $\mathfrak{p}$ of R, and let $R_{\mathfrak{p}} = \{\alpha \in K : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0\}$ be the local ring corresponding to $\mathfrak{p}$. Choose $\lambda \in K^*$ such that the decomposable form $F_{\mathfrak{M},\mathfrak{p}} := \lambda F$ has $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{c}(\mathfrak{M}, F_{\mathfrak{M},\mathfrak{p}})) = 0$. Note that $F_{\mathfrak{M},\mathfrak{p}}$ maps $\mathfrak{M}$ to $R_{\mathfrak{p}}$. Denote the maximal ideal of $R_{\mathfrak{p}}$ also by $\mathfrak{p}$, and let $\overline{K}_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}$ be the residue class field. The reduction of $\mathfrak{M}$ mod $\mathfrak{p}$ is defined as the factor module

$$\overline{\mathfrak{M}}_{\mathfrak{p}} = \mathfrak{M}/\mathfrak{p}\mathfrak{M}$$

(where $\mathfrak{p}\mathfrak{M} = \{\lambda\mathbf{x} : \lambda \in \mathfrak{p}, \mathbf{x} \in \mathfrak{M}\}$) and the reduction of $F_{\mathfrak{M},\mathfrak{p}}$ mod $\mathfrak{p}$

$$\overline{F}_{\mathfrak{M},\mathfrak{p}} : \overline{\mathfrak{M}}_{\mathfrak{p}} \to \overline{K}_{\mathfrak{p}} : \mathbf{x} \bmod \mathfrak{p} \mapsto F_{\mathfrak{M},\mathfrak{p}}(\mathbf{x}) \bmod \mathfrak{p}\,.$$

Note that $\overline{\mathfrak{M}}_{\mathfrak{p}}$ is a finite-dimensional $\overline{K}_{\mathfrak{p}}$-vector space and that $\overline{F}_{\mathfrak{M},\mathfrak{p}}$ is a decomposable form on this space. The form $\overline{F}_{\mathfrak{M},\mathfrak{p}}$ is determined by $\mathfrak{M}$, F and $\mathfrak{p}$ up to a constant factor in $\overline{K}_{\mathfrak{p}}^*$.

Let K_0 be a field, V_0 a finite-dimensional K_0-vector space and $F_0 : V_0 \to K_0$ a decomposable form. Further, let $(m_1, \ldots, m_r)$ be a factorization of F_0 in some extension L_0 of K_0. We denote by $N(F_0)$ the number of subsets $\{i_1, \ldots, i_u\}$ with $2 \leq u \leq r$ of $\{1, \ldots, r\}$ such that $\{m_{i_1}, \ldots, m_{i_u}\}$ is L_0-linearly independent. It is easy to verify that $N(F_0)$ is independent of the choice of the factorization $\{m_1, \ldots, m_r\}$ and that $N(\lambda F_0) = N(F_0)$ for $\lambda \in K_0^*$. In Section 3 we shall show that for every prime ideal $\mathfrak{p}$ of the Dedekind domain R considered above we have

$$\begin{gathered} N(\overline{F}_{\mathfrak{M},\mathfrak{p}}) \leq N(F)\,, \\ N(\overline{F}_{\mathfrak{M},\mathfrak{p}}) < N(F) \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}(\mathfrak{M}, F)) > 0\,. \end{gathered} \tag{1.12}$$

Let M/K be a finite extension, and $\mathfrak{M}$ an R-lattice in M. We define the discriminant of $\mathfrak{M}$ by

$$\mathfrak{D}(\mathfrak{M}) = \mathfrak{D}(\mathfrak{M}, N_{M/K})\,.$$

By (1.11) and Example 2, if $\mathfrak{M}$, $\mathfrak{M}'$ are R-lattices in M such that $\mathfrak{M}' = \mu\sigma(\mathfrak{M})$ for some $\mu \in M^*$ and some K-isomorphism σ of M, then

$$\mathfrak{D}(\mathfrak{M}') = \mathfrak{D}(\mathfrak{M})\,.$$

Example 5. Let $\mathfrak{M}$ be a *full* R-lattice in M, that is, an R-lattice in M with largest possible rank $[M:K]$. Put $n = [M:K]$ and for $\omega_1, \ldots, \omega_n \in M$, denote by $D_{M/K}(\omega_1, \ldots, \omega_n)$ the discriminant of $\{\omega_1, \ldots, \omega_n\}$ (cf. [15], p. 64). Further, denote by $D_{M/K}(\mathfrak{M})$ the R-ideal generated by all numbers $D_{M/K}(\omega_1, \ldots, \omega_n)$ with $\omega_1, \ldots, \omega_n \in \mathfrak{M}$. Let $\widehat{R}$ be the integral closure of R in M and denote by $N_{M/K}(\mathfrak{M})$ the norm of the $\widehat{R}$-ideal in M generated by

$\mathfrak{M}$. It is not difficult to show that

$$\mathfrak{D}(\mathfrak{M}) = D_{M/K}(\mathfrak{M})/\{N_{M/K}(\mathfrak{M})\}^2 . \tag{1.13}$$

If in particular $\mathfrak{M}$ is integral over R (i.e. $\mathfrak{M} \subseteq \widehat{R}$), then $\mathfrak{D}(\mathfrak{M})$ divides $D_{M/K}(\mathfrak{M})$.

2. Results. Before stating our results we have to introduce heights and some notions related to S-integers.

The *height* $h(\alpha)$ of an algebraic number α is defined as follows: let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial with relatively prime coefficients and with $f(\alpha) = 0$, and suppose that $f(X)$ factors as $a(X-\alpha_1)\dots(X-\alpha_d)$ over the algebraic closure of $\mathbb{Q}$ with $\alpha_1 = \alpha$. Then

$$h(\alpha) = \Big\{|a| \prod_{i=1}^{d} \max(1, |\alpha_i|)\Big\}^{1/d} . \tag{2.1}$$

The *height* $h(F)$ of a polynomial F with algebraic coefficients is defined as the maximum of the heights of these coefficients.

Let K be an algebraic number field of degree d. Denote by O_K the ring of integers of K, and by M_K the set of prime ideals of O_K. Take a finite set of prime ideals S. The *ring of S-integers* is defined by

$$O_S = \{\alpha \in K : \operatorname{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \in M_K \setminus S\} .$$

The *unit group* of O_S is the group of S-units

$$O_S^* = \{\alpha \in K : \operatorname{ord}_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p} \in M_K \setminus S\} .$$

The ring O_S is a Dedekind domain with prime ideals $\mathfrak{p}O_S$, $\mathfrak{p} \in M_K \setminus S$. For convenience we shall identify the prime ideals of O_S with those of O_K in $M_K \setminus S$. We shall denote by $(\alpha_1, \dots, \alpha_n)$ the O_S-ideal or O_S-lattice generated by $\alpha_1, \dots, \alpha_n$, unless otherwise stated.

For every O_S-ideal $\mathfrak{a}$ there is a unique O_K-ideal $\mathfrak{a}^*$, composed of O_K-prime ideals outside S, such that $\mathfrak{a} = \mathfrak{a}^* O_S$; we put

$$|\mathfrak{a}|_S = \{N_{K/\mathbb{Q}}(\mathfrak{a}^*)\}^{1/d} .$$

Every O_S-ideal $\mathfrak{a}$ can be written uniquely as $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$, where $\mathfrak{b}$, $\mathfrak{c}$ are integral O_S-ideals with $\mathfrak{b} + \mathfrak{c} = (1)$. We put

$$m_S(\mathfrak{a}) = |\mathfrak{b}|_S \cdot |\mathfrak{c}|_S .$$

It is easy to show that for every $C \geq 1$ there are only finitely many O_S-ideals $\mathfrak{a}$ with $m_S(\mathfrak{a}) \leq C$.

Let $\mathbf{e}_1 = (1, 0, \dots, 0)^T, \dots, \mathbf{e}_n = (0, \dots, 0, 1)^T$. From the remarks made in Section 1 it follows that every O_S-lattice of rank n is isomorphic to either $O_S^n = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ or $(\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$ where $\mathfrak{a} = (\alpha, \beta)$ is an integral, non-principal O_S-ideal. Here $\mathfrak{a}$ can be replaced by any ideal belonging to

the same O_S-ideal class as $\mathfrak{a}$. By Lemma 5 in Section 4 of this paper, every non-principal O_S-ideal class contains an integral O_S-ideal (α, β) such that

$$h(\alpha) \le C_1, \quad h(\beta) \le C_1\,, \tag{2.2}$$

where C_1 is an effectively computable number depending only on $d = [K : \mathbb{Q}]$ and the discriminant D_K of K. We conclude that every O_S-lattice of rank n is isomorphic to either

$$\begin{cases} (\mathbf{e}_1, \dots, \mathbf{e}_n) = O_S^n \quad \text{or} \\ (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n) \text{ with } \alpha, \beta \in O_S,\ h(\alpha) \le C_1\,, \\ \qquad\qquad\qquad\qquad\qquad h(\beta) \le C_1,\ (\alpha, \beta) \text{ non-principal.} \end{cases} \tag{2.3}$$

The lattices in (2.3) are called *reduced*. If $(\mathfrak{M}, F)$ is an O_S-lattice decomposable form pair in which $\mathfrak{M}$ is reduced and rank $\mathfrak{M} = n$, then F is a decomposable form on K^n. The *height* of F is defined as the height of the corresponding polynomial $F(\mathbf{X}) = F(X_1\mathbf{e}_1 + \ldots + X_n\mathbf{e}_n) \in K[X_1, \dots, X_n]$.

We are now in a position to state our results. By D_M we denote the discriminant of a number field M. As before, we put $d = [K : \mathbb{Q}]$. Further, let s denote the cardinality of S, and P the largest of the prime numbers lying below the prime ideals in S with $P = 1$ if $S = \emptyset$. Finally, let L be a finite, normal extension of K, let r and n be positive integers, and let $\mathfrak{d}$ be a non-zero integral O_S-ideal.

THEOREM 2. *Let $(\mathfrak{M}, F)$ be an O_S-lattice decomposable form pair such that* rank $\mathfrak{M} = n$, $\deg(F) = r$, *F has splitting field L and $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$. Then $(\mathfrak{M}, F)$ is weakly equivalent to a pair $(\mathfrak{M}', F')$, where $\mathfrak{M}'$ is a reduced O_S-lattice of rank n, and F' is a decomposable form on K^n with*

$$h(F') \le C_2 |\mathfrak{d}|_S^{C_3}\,,$$

where C_2, C_3 are effectively computable numbers depending only on d, $|D_L|$, s, P, n and r.

In [6], we proved Theorem 2 in the case that $\mathfrak{M} = O_S^2$ and F is a binary form, and gave explicit expressions for C_2 and C_3.

The main tool in the proof of Theorem 2 is an effective result of Győry ([10], Lemma 6) on the S-unit equation $\alpha x + \beta y = 1$ in $x, y \in O_S^*$. This result of Győry was proved by means of Baker's theory on linear forms in logarithms of algebraic numbers and its p-adic analogue.

We now state some consequences of Theorem 2 which will be proved in Section 7. The upper bound for $h(F')$ in Theorem 2 depends on $|D_L|$. In Section 7 we shall prove that $|D_L| \le C_4$, where C_4 is an effectively computable number depending only on d, $|D_K|$, s, P, n, r and $|\mathfrak{d}|_S$. Thus we obtain the following.

COROLLARY 1. *Let* $(\mathfrak{M}, F)$ *be as in Theorem* 2. *Then* $(\mathfrak{M}, F)$ *is weakly equivalent to a pair* $(\mathfrak{M}', F')$, *where* $\mathfrak{M}'$ *is a reduced* O_S*-lattice of rank* n, *and* F' *is a decomposable form on* K^n *with*

$$h(F') \leq C_5\,,$$

where C_5 *is an effectively computable number depending only on* d, $|D_K|$, s, P, n, r *and* $|\mathfrak{d}|_S$.

We note that for $n = 2$ and $\mathfrak{M} = \mathfrak{M}' = O_S^2$, our Corollary 1 (see also Example 3 in Section 1) implies, in a less explicit form, Theorem 2 of [6].

Assume that K is effectively given, i.e. that an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ is given such that $K \cong \mathbb{Q}[X]/(f(X))$. Let α be a zero of f. Then every element of K can be expressed uniquely as $(\sum_{i=0}^{d-1} a_i\alpha^i)/a_d$ ($d = \deg(f)$), where $a_0, \ldots, a_{d-1}, a_d$ are rational integers with $\gcd(a_0, \ldots, a_{d-1}, a_d) = 1$ and $a_d > 0$; the tuple $(a_0, \ldots, a_d)$ is called a *representation* of the element in question. We say that an element of K is given (or computable) if the finite tuple of integers by which it is represented is given (or can be computed). Then sums, differences, products and quotients of given elements in K can be computed. We assume that S is effectively given in the sense that for every prime ideal in S, a set of generators is given. Then for every given $\alpha \in K$ it can be effectively decided whether $\alpha \in O_S$ (or $\alpha \in O_S^*$).

COROLLARY 2. *For any positive integers* n *and* r *and every integral* O_S*-ideal* $\mathfrak{d}$, *there are only finitely many weak equivalence classes of* O_S*-lattice decomposable form pairs* $(\mathfrak{M}, F)$ *such that* $\operatorname{rank} \mathfrak{M} = n$, $\deg(F) = r$ *and* $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$. *Further, if a set of generators for* $\mathfrak{d}$ *is given, then a full set of representatives of these weak equivalence classes can be effectively determined.*

Corollary 2 does not follow at once from Corollary 1, since if $(\mathfrak{M}_1, F_1)$ and $(\mathfrak{M}_2, F_2)$ are two O_S-lattice decomposable form pairs such that $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are reduced and F_1 and F_2 have small heights, then it might still happen that $(\mathfrak{M}_1, F_1)$ and $(\mathfrak{M}_2, F_2)$ are weakly equivalent. We shall prove that there is an algorithm to decide whether two such pairs $(\mathfrak{M}_1, F_1)$, $(\mathfrak{M}_2, F_2)$ are weakly equivalent or not.

By combining Corollary 1 with (1.12) we get

COROLLARY 3. *Let* $(\mathfrak{M}, F)$ *be an* O_S*-lattice decomposable form pair such that* $\operatorname{rank} \mathfrak{M} = n$, $\deg(F) = r$ *and* $N(\overline{F}_{\mathfrak{M},\mathfrak{p}}) = N(F)$ *for every prime ideal* $\mathfrak{p}$ *of* O_S. *Then* $(\mathfrak{M}, F)$ *is weakly equivalent to a pair* $(\mathfrak{M}', F')$ *such that* $\mathfrak{M}'$ *is reduced and* $h(F') \leq C_6$, *where* C_6 *is an effectively computable number depending only on* d, $|D_K|$, s, P, n, *and* r.

We now state some results on (not weak) equivalence classes of O_S-lattice decomposable form pairs. Let $\mathfrak{c}$ be a non-zero O_S-ideal.

COROLLARY 4. *Let $(\mathfrak{M}, F)$ be an O_S-lattice decomposable form pair such that* rank $\mathfrak{M} = n$, $\deg(F) = r$, *F has splitting field L, $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$ and $\mathfrak{c}(\mathfrak{M}, F) = \mathfrak{c}$. Then $(\mathfrak{M}, F)$ is equivalent to a pair $(\mathfrak{M}', F')$, where $\mathfrak{M}'$ is a reduced O_S-lattice of rank n, and F' is a decomposable form on K^n with*

$$h(F') \le C_7 m_S(\mathfrak{c}) |\mathfrak{d}|_S^{C_8} \quad \text{and} \quad h(F') \le C_9 m_S(\mathfrak{c}),$$

where C_7, C_8, C_9 are effectively computable numbers such that C_7, C_8 depend only on d, $|D_L|$, s, P, n and r, and C_9 only on d, $|D_K|$, s, P, n, r and $|\mathfrak{d}|_S$.

Corollary 4 implies that there are only finitely many equivalence classes of O_S-lattice decomposable form pairs $(\mathfrak{M}, F)$ with rank $\mathfrak{M} = n$, $\deg(F) = r$, $\mathfrak{c}(\mathfrak{M}, F) = \mathfrak{c}$ and $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$. Further, by arguments similar to the proof of Corollary 2 one can prove the existence of an effective algorithm that selects one pair $(\mathfrak{M}, F)$ from each of these equivalence classes. We remark that in view of Example 4 of Section 1, Theorem 1 stated in the Introduction is exactly Corollary 4 with the second inequality for $K = \mathbb{Q}$, $O_S = R = \mathbb{Z}[(p_1 \dots p_s)^{-1}]$, $\mathfrak{M} = \mathfrak{M}' = R^n$, $\mathfrak{c} = (1)$ and $\mathfrak{d} = (D_R(F)) = (D)$.

From Corollary 4 we shall derive the following.

COROLLARY 5. *Let $(\mathfrak{M}, F)$ be as in Corollary 4. Then $\mathfrak{M} = (\omega_1, \dots, \omega_m)$ where either $\mathfrak{M}$ is free and $m = n$, or $\mathfrak{M}$ is not free, $m = n + 1$ and $\omega_{n+1} = \gamma\omega_n$ for some $\gamma \in K^*$ with $h(\gamma) \le C_{10}$, $F(\omega_1)F(\omega_2)\dots F(\omega_m) \ne 0$ and*

$$h(F(\omega_i)) \le C_{11} m_S(\mathfrak{c}) |\mathfrak{d}|_S^{C_{12}} \quad \text{and} \quad h(F(\omega_i)) \le C_{13} m_S(\mathfrak{c}) \tag{2.4}$$

for $i = 1, \dots, m$, where C_{10}, C_{11}, C_{12}, C_{13} are effectively computable numbers such that C_{10} depends only on d and $|D_K|$, C_{11} and C_{12} only on d, $|D_L|$, s, P, n and r, and C_{13} only on d, $|D_K|$, s, P, n, r and $|\mathfrak{d}|_S$.

A trivial consequence of Corollary 5 is that the bounds occurring on the right-hand side of the estimates in (2.4) are upper bounds for

$$\min\{h(F(\mathbf{x})) : \mathbf{x} \in \mathfrak{M},\ F(\mathbf{x}) \ne 0\}.$$

Hence, for $n = 2$ and $\mathfrak{M} = O_S^2$, Corollary 5 implies (in a less explicit form) Corollary 5 of [6].

Let M/K be a finite extension of degree r. Two O_S-lattices $\mathfrak{M}_1$, $\mathfrak{M}_2$ in M are said to be *similar* if $\mathfrak{M}_2 = \mu\mathfrak{M}_1$ for some $\mu \in M^*$.

COROLLARY 6. *Let $\mathfrak{M}$ be an O_S-lattice of rank n in M with $\mathfrak{D}(\mathfrak{M}) = \mathfrak{d}$. Then $\mathfrak{M}$ is similar to an O_S-lattice $(\omega_1, \dots, \omega_m)$ with $\omega_1, \dots, \omega_m \in M^*$, where either $\mathfrak{M}$ is free and $m = n$, or $\mathfrak{M}$ is not free, $m = n + 1$ and $\omega_{n+1} = \gamma\omega_n$ for some $\gamma \in K^*$ with $h(\gamma) \le C_{14}$ and*

$$h(\omega_i) \le C_{15} |\mathfrak{d}|_S^{C_{16}} \quad \text{and} \quad h(\omega_i) \le C_{17} \quad \text{for } i = 1, \dots, m, \tag{2.5}$$

where C_{14}, C_{15}, C_{16}, C_{17} are effectively computable numbers such that C_{14} depends only on d and $|D_K|$, C_{15}, C_{16} only on d, $|D_M|$, s, P, n and $r = [M:K]$, and C_{17} only on d, $|D_K|$, s, P, n, r and $|\mathfrak{d}|_S$.

We say that an O_S-lattice $\mathfrak{M}$ is of *degree* r over K if it is contained in some finite extension of K, and the smallest extension of K containing $\mu\mathfrak{M}$ for some non-zero algebraic number μ has degree r over K. Corollary 6 implies that there are only finitely many similarity classes of O_S-lattices $\mathfrak{M}$ of degree r and rank n with $\mathfrak{D}(\mathfrak{M}) = \mathfrak{d}$. Further, in view of (1.5) it is easy to prove the existence of an algorithm to choose such $\mathfrak{M}$ from each of these similarity classes.

We note that from Corollary 6 and relation (1.13) one can also deduce effective finiteness results for full, integral O_S-lattices $\mathfrak{M}$ of given (finite) rank and given (non-zero) ordinary discriminant $D(\mathfrak{M})$. We shall not work these out here. For $K = \mathbb{Q}$ and $S = \emptyset$, these imply a result of Nagell ([17], Theorem 6) which says that there are only finitely many full and integral $\mathbb{Z}$-modules with a given (finite) rank and a given (non-zero) ordinary discriminant, and all these $\mathbb{Z}$-modules can be effectively determined.

3. Properties of decomposable forms and discriminants. In this section, we prove the facts about decomposable forms and discriminants mentioned in Section 1; namely, that $\mathfrak{c}(\mathfrak{M}, F)$ is an R-ideal, that $\mathfrak{D}(\mathfrak{M}, F)$ is an integral R-ideal, and that $\mathfrak{D}(\mathfrak{M}, F)$ satisfies (1.12), and some other facts needed in this paper.

Let R be a Dedekind domain with quotient field K of characteristic 0, and $(\mathfrak{M}, F)$ an R-lattice decomposable form pair such that rank $\mathfrak{M} = n$, $\deg(F) = r$ and F has splitting field L. Let $\mathrm{Gal}(L/K)$ denote the Galois group of L/K. Since F maps $K\mathfrak{M}$ to K, it can be factored as

$$F(\mathbf{x}) = \lambda \prod_{i=1}^{t} l_i(\mathbf{x})^{k_i} \quad \text{for } \mathbf{x} \in K\mathfrak{M}\,, \tag{3.1}$$

where $\lambda \in K^*$, $l_1, \dots, l_t : V \to L$ are pairwise non-proportional linear functions and $k_1, \dots, k_t$ are positive integers such that

$$\sigma \circ l_i = l_{\sigma(i)}, \quad k_{\sigma(i)} = k_i \quad \text{for } i = 1, \dots, t,\ \sigma \in \mathrm{Gal}(L/K)\,, \tag{3.2}$$

where $(\sigma(1), \dots, \sigma(t))$ is a permutation of $(1, \dots, t)$ for $\sigma \in \mathrm{Gal}(L/K)$. Define the fields M_i $(i = 1, \dots, t)$ by

$$\mathrm{Gal}(L/M_i) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(i) = i\}\,. \tag{3.3}$$

Then $l_i(\mathfrak{M}) \subset M_i$ for $i = 1, \dots, t$. Partition $\{1, \dots, t\}$ into $\mathrm{Gal}(L/K)$-orbits $\mathcal{C}_1, \dots, \mathcal{C}_u$ such that i and j belong to the same orbit if and only if $\sigma(i) = j$ for some $\sigma \in \mathrm{Gal}(L/K)$. For convenience, we assume that $i \in \mathcal{C}_i$ for $i = 1, \dots, u$. We shall frequently use the following fact:

(3.4) let $S_1, \dots, S_t$ be non-empty sets such that $S_i \subseteq M_i$ and $\sigma(S_i) = S_{\sigma(i)}$ for $i = 1, \dots, t$, $\sigma \in \mathrm{Gal}(L/K)$; then it is possible to choose π_i from S_i such that $\sigma(\pi_i) = \pi_{\sigma(i)}$ for $i = 1, \dots, t$, $\sigma \in \mathrm{Gal}(L/K)$.

Namely, for $i = 1, \dots, u$ one can choose π_i arbitrarily from S_i and then the remaining π_i can be selected such that the relationships $\sigma(\pi_i) = \pi_{\sigma(i)}$ for $i = 1, \dots, u$, $\sigma \in \mathrm{Gal}(L/K)$ are all satisfied. This is possible since $S_i \subseteq M_i$ for $i = 1, \dots, t$.

Let $\mathfrak{p}$ be a prime ideal of R. As before, we put

$$R_{\mathfrak{p}} = \{\alpha \in K : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0\}, \qquad \mathfrak{M}_{\mathfrak{p}} = R_{\mathfrak{p}}\mathfrak{M},$$

and denote the maximal ideal of $R_{\mathfrak{p}}$ also by $\mathfrak{p}$. Let $\widehat{R}$, $\widehat{R}_{\mathfrak{p}}$ denote the integral closures of R, $R_{\mathfrak{p}}$, respectively, in L, and let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the prime ideals of $\widehat{R}$ lying above $\mathfrak{p}$. In what follows, we denote the $\widehat{R}_{\mathfrak{p}}$-ideal generated by $\alpha_1, \dots, \alpha_r$ by $(\alpha_1, \dots, \alpha_r)_{\mathfrak{p}}$. Further, the $\widehat{R}_{\mathfrak{p}}$-ideal generated by the numbers $l_i(\mathbf{x})$, $\mathbf{x} \in \mathfrak{M}$, is denoted by $(l_i(\mathfrak{M}))_{\mathfrak{p}}$. Note that $l_i(\mathbf{x}) \in M_i$ for $\mathbf{x} \in \mathfrak{M}$. Both $\widehat{R}_{\mathfrak{p}}$ and $\widehat{R}_{i,\mathfrak{p}} := \widehat{R}_{\mathfrak{p}} \cap M_i$ are principal ideal domains (cf. [2], Ch. III, §4). Hence $(l_i(\mathfrak{M}))_{\mathfrak{p}}$ is generated by an element in M_i. In other words, there are $\pi_i \in M_i$ such that

$$(l_i(\mathfrak{M}))_{\mathfrak{p}} = (\pi_i)_{\mathfrak{p}} \quad \text{for } i = 1, \dots, t. \tag{3.5}$$

By applying (3.4) to the sets $\{\xi_i \in M_i : (l_i(\mathfrak{M}))_{\mathfrak{p}} = (\xi_i)_{\mathfrak{p}}\}$ we infer that $\pi_1, \dots, \pi_t$ can be chosen such that

$$\sigma(\pi_i) = \pi_{\sigma(i)} \quad \text{for } i = 1, \dots, t,\ \sigma \in \mathrm{Gal}(L/K). \tag{3.6}$$

Put $\pi = \pi_1^{k_1} \dots \pi_t^{k_t}$. Then $\sigma(\pi) = \pi$ for each $\sigma \in \mathrm{Gal}(L/K)$, hence $\pi \in K$. Further,

$$\mathrm{ord}_{\mathfrak{P}_j}(\mathfrak{c}(\mathfrak{M}, F)) = \mathrm{ord}_{\mathfrak{P}_j}(\pi) \quad \text{for } j = 1, \dots, g.$$

Hence $\mathfrak{c}(\mathfrak{M}, F)$ is an R-ideal.

Define the linear functions $m_i = \pi_i^{-1} l_i : \mathfrak{M} \to L$ $(i = 1, \dots, t)$. Then, by (3.2), (3.5) and (3.6),

$$\sigma \circ m_i = m_{\sigma(i)}, \qquad (m_i(\mathfrak{M}))_{\mathfrak{p}} = (1)_{\mathfrak{p}} \quad \text{for } i = 1, \dots, t,\ \sigma \in \mathrm{Gal}(L/K). \tag{3.7}$$

Since $R_{\mathfrak{p}}$ is a principal ideal domain, $\mathfrak{M}_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module of rank n (cf. [18], Ch. I, §2). Hence $\mathfrak{M}_{\mathfrak{p}}$ has an $R_{\mathfrak{p}}$-basis $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ with $\mathbf{x}_i \in \mathfrak{M}$ for $i = 1, \dots, n$. Let $\mathcal{I}'(F)$ be the collection of L-linearly independent subsets $\{m_{i_1}, \dots, m_{i_n}\}$ ($n = \mathrm{rank}\ \mathfrak{M}$) of $\{m_1, \dots, m_t\}$. Define the number

$$\delta_{\mathfrak{p}} = \prod_{\mathcal{I}'(F)} \{\det(m_{i_k}(\mathbf{x}_j))_{1 \leq k,\, j \leq n}\}^2, \tag{3.8}$$

where the product is taken over all sets $\{m_{i_1},\dots,m_{i_n}\}$ in $\mathcal{I}'(F)$. From (1.10), (3.7) and the fact that $\{\mathbf{x}_1,\dots,\mathbf{x}_n\}$ is an $R_\mathfrak{p}$-basis of $\mathfrak{M}_\mathfrak{p}$, it follows that

$$\operatorname{ord}_{\mathfrak{P}_i}(\delta_\mathfrak{p}) = \operatorname{ord}_{\mathfrak{P}_i}(\mathfrak{D}(\mathfrak{M},F)) \quad \text{for } i=1,\dots,g\,. \tag{3.9}$$

We notice that $\delta_\mathfrak{p}\in\widehat{R}_\mathfrak{p}$, since $(m_i(\mathfrak{M}))_\mathfrak{p}=(1)_\mathfrak{p}$ for $i=1,\dots,t$. Further, $\{\sigma\circ m_{i_1},\dots,\sigma\circ m_{i_n}\}$ is L-linearly independent if and only if $\{m_{i_1},\dots,m_{i_n}\}$ is. Hence each $\sigma\in\operatorname{Gal}(L/K)$ permutes the sets of $\mathcal{I}'(F)$. Moreover, each factor on the right-hand side of (3.8) depends only on the set $\{m_{i_1},\dots,m_{i_n}\}$ and not on its ordering because of the exponent 2. It follows that each $\sigma\in\operatorname{Gal}(L/K)$ permutes the factors on the right-hand side of (3.8), which implies that $\sigma(\delta_\mathfrak{p})=\delta_\mathfrak{p}$. Therefore, $\delta_\mathfrak{p}\in\widehat{R}_\mathfrak{p}\cap K=R_\mathfrak{p}$. We conclude that $\mathfrak{D}(\mathfrak{M},F)$ is an integral R-ideal.

We now prove formula (1.12). We recall that $\overline{\mathfrak{M}}_\mathfrak{p}=\mathfrak{M}/\mathfrak{p}\mathfrak{M}$. We take

$$F_{\mathfrak{M},\mathfrak{p}}(\mathbf{x}) = \prod_{i=1}^{t} m_i(\mathbf{x})^{k_i} \quad \text{for } \mathbf{x}\in K\mathfrak{M}\,,$$

which can be done since $(m_i(\mathfrak{M}))_\mathfrak{p}=(1)_\mathfrak{p}$ for $i=1,\dots,t$. By $\overline{F}_{\mathfrak{M},\mathfrak{p}}$ we denote the decomposable form on $\overline{\mathfrak{M}}_\mathfrak{p}\colon \mathbf{x} \bmod \mathfrak{p}\mapsto F_{\mathfrak{M},\mathfrak{p}}(\mathbf{x}) \bmod \mathfrak{p}$.

LEMMA 1. *We have* $N(\overline{F}_{\mathfrak{M},\mathfrak{p}})\le N(F)$. *Further*, $N(\overline{F}_{\mathfrak{M},\mathfrak{p}})<N(F)$ *if and only if* $\operatorname{ord}_\mathfrak{p}(\mathfrak{D}(\mathfrak{M},F))>0$.

Proof. Let $\mathfrak{P}$ be one of the prime ideals of $\widehat{R}$ lying above $\mathfrak{p}$. Put $\overline{K}_\mathfrak{p}=R/\mathfrak{p}\cong R_\mathfrak{p}/\mathfrak{p}$ and $\overline{L}_\mathfrak{P}=\widehat{R}/\mathfrak{P}\cong\widehat{R}_\mathfrak{p}/\mathfrak{P}$. Since, by (3.7), $m_i(\mathfrak{M})\subseteq\widehat{R}_\mathfrak{p}$ for $i=1,\dots,t$, we can define the reductions of m_i mod $\mathfrak{P}$ by

$$\overline{m}_i(\mathbf{x} \bmod \mathfrak{p}\mathfrak{M}) = m_i(\mathbf{x}) \bmod \mathfrak{P}\,.$$

Then

$$\overline{F}_{\mathfrak{M},\mathfrak{p}}(\mathbf{x}) = \prod_{i=1}^{t} \overline{m}_i(\mathbf{x})^{k_i} \quad \text{for } \mathbf{x}\in\overline{\mathfrak{M}}_\mathfrak{p}\,.$$

Obviously, if $\{\overline{m}_{i_1},\dots,\overline{m}_{i_u}\}$ is some $\overline{L}_\mathfrak{P}$-linearly independent subset of $\{\overline{m}_1,\dots,\overline{m}_t\}$ then $\{m_{i_1},\dots,m_{i_u}\}$ is L-linearly independent. Hence $N(\overline{F}_{\mathfrak{M},\mathfrak{p}})\le N(F)$. Further, $N(\overline{F}_{\mathfrak{M},\mathfrak{p}})<N(F)$ if and only if there is an L-linearly independent subset $\{m_{i_1},\dots,m_{i_u}\}$ of $\{m_1,\dots,m_t\}$ with $u\ge 2$ such that $\{\overline{m}_{i_1},\dots,\overline{m}_{i_u}\}$ is $\overline{L}_\mathfrak{P}$-linearly dependent. But each linearly independent subset of $\{m_1,\dots,m_t\}$ can be extended to a linearly independent subset of cardinality n. Hence $N(\overline{F}_{\mathfrak{M},\mathfrak{p}})<N(F)$ if and only if there is a set $\{m_{i_1},\dots,m_{i_n}\}$ in $\mathcal{I}'(F)$ with $u\ge 2$ such that $\{\overline{m}_{i_1},\dots,\overline{m}_{i_n}\}$ is $\overline{L}_\mathfrak{P}$-linearly dependent. But $\{\overline{m}_{i_1},\dots,\overline{m}_{i_n}\}$ is $\overline{L}_\mathfrak{P}$-linearly dependent if and only if

$$\operatorname{ord}_\mathfrak{P}(\det(m_{i_k}(\mathbf{x}_j))_{i\le k,\,j\le n})>0\,,$$

where $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ is the $R_\mathfrak{p}$-basis of $\mathfrak{M}_\mathfrak{p}$ used in the definition of $\delta_\mathfrak{p}$. This shows that $N(\overline{F}_{\mathfrak{M},\mathfrak{p}}) < N(F)$ if and only if $\mathrm{ord}_\mathfrak{P}(\delta_\mathfrak{p}) > 0$. Together with (3.9) this implies Lemma 1. ∎

As before, $\mathcal{C}_1, \dots, \mathcal{C}_u$ denote the $\mathrm{Gal}(L/K)$-orbits of $\{1, \dots, r\}$ where the action of $\mathrm{Gal}(L/K)$ on $\{1, \dots, u\}$ is defined by (3.2). Further, $i \in \mathcal{C}_i$ for $i = 1, \dots, t$. Let $\widehat{R}_i$ be the integral closure of R in the field M_i defined by (3.3) and let $\mathfrak{d}_i$ be the discriminant of the ring extension $\widehat{R}_i/R$ (see e.g. [13]).

LEMMA 2. *We have* $\mathfrak{D}(\mathfrak{M}, F)^n \subseteq (\mathfrak{d}_1 \dots \mathfrak{d}_u)^2$.

Proof. It suffices to prove that for every prime ideal $\mathfrak{p}$ of R,

$$n \, \mathrm{ord}_\mathfrak{p}(\delta_\mathfrak{p}) \geq 2 \sum_{i=1}^{u} \mathrm{ord}_\mathfrak{p}(\mathfrak{d}_i)\,, \tag{3.10}$$

where $\delta_\mathfrak{p}$ is defined by (3.8) for some $R_\mathfrak{p}$-basis $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ of $\mathfrak{M}_\mathfrak{p}$ with $\mathbf{x}_i \in \mathfrak{M}$ for $i = 1, \dots, n$. Fix a prime ideal $\mathfrak{p}$, and consider one of the factors

$$\Delta = \det((m_{i_k}(\mathbf{x}_j))_{1 \leq k,\, j \leq n})$$

in (3.8) where $\{m_{i_1}, \dots, m_{i_n}\} \in \mathcal{I}'(F)$. Let $\mathbf{m}_i$ be the vector with coordinates $(m_i(\mathbf{x}_1), \dots, m_i(\mathbf{x}_n))$. In what follows, if $\mathbf{a}$ is any vector with coordinates in L, then $(\mathbf{a})_\mathfrak{p}$ denotes the $\widehat{R}_\mathfrak{p}$-ideal generated by the coordinates of $\mathbf{a}$. Thus, using (3.7), we get

$$\begin{aligned}(\Delta)_\mathfrak{p} &= (\det(\mathbf{m}_{i_1}, \dots, \mathbf{m}_{i_n}))_\mathfrak{p} = (\det(\mathbf{m}_{i_1}, \mathbf{m}_{i_2} - \mathbf{m}_{i_1}, \dots, \mathbf{m}_{i_n} - \mathbf{m}_{i_1}))_\mathfrak{p} \\ &\subseteq (\mathbf{m}_{i_2} - \mathbf{m}_{i_1})_\mathfrak{p} \dots (\mathbf{m}_{i_n} - \mathbf{m}_{i_1})_\mathfrak{p}\,.\end{aligned}$$

We can do the same for $\mathbf{m}_{i_2}, \dots, \mathbf{m}_{i_n}$ in the rôle of $\mathbf{m}_{i_1}$. Thus

$$(\Delta)_\mathfrak{p}^n \subseteq \prod_{\substack{1 \leq k,\, l \leq n \\ k \neq l}} (\mathbf{m}_{i_k} - \mathbf{m}_{i_l})_\mathfrak{p}\,.$$

It is easy to see that every pair $\{\mathbf{m}_i, \mathbf{m}_j\}$ with distinct $i, j \in \{1, \dots, t\}$ is contained in one of the sets of $\mathcal{I}'(F)$. Since, by (3.7), each vector $\mathbf{m}_i$ has its coordinates in $\widehat{R}_\mathfrak{p}$, it follows that

$$(\delta)_\mathfrak{p}^n \subseteq \Big\{ \prod_{\substack{1 \leq i,\, j \leq n \\ i \neq j}} (\mathbf{m}_i - \mathbf{m}_j)_\mathfrak{p} \Big\}^2.$$

This implies that

$$(\delta_\mathfrak{p})_\mathfrak{p}^n \subseteq \prod_{k=1}^{u} \Big\{ \prod_{\substack{i,j \in \mathcal{C}_k \\ i \neq j}} (\mathbf{m}_i - \mathbf{m}_j)_\mathfrak{p} \Big\}^2,$$

where the second product takes the value 1 if $\mathcal{C}_k$ has only one element. Now (3.10) follows once we have proved that

$$\prod_{\substack{i,j\in\mathcal{C}_k\\ i\neq j}} (\mathbf{m}_i - \mathbf{m}_j)_{\mathfrak{p}} \subseteq \mathfrak{d}_{k,\mathfrak{p}} \quad \text{for } k = 1,\dots,u\,, \tag{3.11}$$

where $\mathfrak{d}_{k,\mathfrak{p}} := \mathfrak{d}_k R_{\mathfrak{p}}$. Put $r := [M_k : K]$, let $\alpha \mapsto \alpha^{(i)}$ $(i = 1,\dots,r)$ denote the distinct K-isomorphisms of M_k and for $\mathbf{a} \in M_k^n$ define $\mathbf{a}^{(i)}$ by applying $\alpha \mapsto \alpha^{(i)}$ to the coordinates of $\mathbf{a}$. Then there is a vector $\mathbf{m} \in R_{k,\mathfrak{p}}^n$ such that the left-hand side of (3.11) is equal to

$$\prod_{1\le i<j\le r} (\mathbf{m}^{(i)} - \mathbf{m}^{(j)})_{\mathfrak{p}}^2 =: \mathfrak{a}\,.$$

Put $K(\mathbf{X}) := K(X_1,\dots,X_n)$, $M_k(\mathbf{X}) := M_k(X_1,\dots,X_n)$, $L(\mathbf{X}) := L(X_1,\dots,X_n)$ where $X_1,\dots,X_n$ are independent variables. Consider in $L(\mathbf{X})$ the polynomials

$$A^{(i)}(\mathbf{X}) = \sum_{l=1}^{n} m_l^{(i)} X_l \quad \text{for } i = 1,\dots,r\,,$$

where $(m_1,\dots,m_n)^T = \mathbf{m}$. Consider also the polynomial

$$D(\mathbf{X}) = \prod_{1\le i<j\le r} \{A^{(i)}(\mathbf{X}) - A^{(j)}(\mathbf{X})\}^2\,.$$

By Gauss' lemma, the $R_{\mathfrak{p}}$-ideal generated by the coefficients of D is equal to $\mathfrak{a}$. Since $R_{\mathfrak{p}}$ is a principal ideal domain, $\widehat{R}_{k,\mathfrak{p}}$ has an $R_{\mathfrak{p}}$-basis, say $\{\omega_1,\dots,\omega_r\}$ (cf. e.g. [20], Ch. V, §4). Then this basis is also an $R_{\mathfrak{p}}[\mathbf{X}]$-basis of $\widehat{R}_{k,\mathfrak{p}}[\mathbf{X}]$, where $R_{\mathfrak{p}}[\mathbf{X}] := R_{\mathfrak{p}}[X_1,\dots,X_n]$ and $\widehat{R}_{k,\mathfrak{p}}[\mathbf{X}] := \widehat{R}_{k,\mathfrak{p}}[X_1,\dots,X_n]$. Then $A \in \widehat{R}_{k,\mathfrak{p}}[\mathbf{X}]$. Further, $D(\mathbf{X})$ is precisely the discriminant of $\{1, A,\dots,A^{r-1}\}$ with respect to $M_k(\mathbf{X})/K(\mathbf{X})$:

$$D(\mathbf{X}) = D_{M_k(\mathbf{X})/K(\mathbf{X})}(1, A,\dots,A^{r-1})\,.$$

From elementary properties of discriminants it follows that there is a polynomial $G(\mathbf{X}) \in R_{\mathfrak{p}}[\mathbf{X}]$ such that

$$D(\mathbf{X}) = G(\mathbf{X}) D_{M_k(\mathbf{X})/K(\mathbf{X})}(\omega_1,\dots,\omega_r) = G(\mathbf{X}) D_{M_k/K}(\omega_1,\dots,\omega_r)\,.$$

This implies that each coefficient of $D(\mathbf{X})$ is divisible in $R_{\mathfrak{p}}$ by $D_{M_k/K}(\omega_1,\dots,\omega_r)$ and hence by the relative discriminant $\mathfrak{d}_{k,\mathfrak{p}}$. Therefore, $\mathfrak{a}$ is divisible by $\mathfrak{d}_{k,\mathfrak{p}}$. This proves (3.11). ∎

4. Preliminaries. In this section we provide some basic tools needed in the proofs of our results. As before, K is an algebraic number field of degree d, S a finite set of prime ideals of O_K, and O_S the ring of S-integers. The O_S-ideal or O_S-lattice generated by $\alpha_1,\dots,\alpha_n$ is denoted by $(\alpha_1,\dots,\alpha_n)$.

We recall that if $\mathfrak{a}$ is any O_S-ideal then $|\mathfrak{a}|_S = N_{K/\mathbb{Q}}(\mathfrak{a}^*)^{1/d}$, where $\mathfrak{a}^*$ is the O_K-ideal composed of prime ideals outside S such that $\mathfrak{a} = \mathfrak{a}^* O_S$. We put

$$|\alpha|_S = |(\alpha)|_S \quad \text{for } \alpha \in K\,.$$

We recall that if $\mathfrak{a} = \mathfrak{b}\cdot\mathfrak{c}^{-1}$ where $\mathfrak{b}$, $\mathfrak{c}$ are integral O_S-ideals with $\mathfrak{b}+\mathfrak{c} = (1)$, then $m_S(\mathfrak{a}) := |\mathfrak{b}|_S \cdot |\mathfrak{c}|_S$. We put

$$m_S(\alpha) = m_S((\alpha)) \quad \text{for } \alpha \in K\,.$$

We shall frequently use the fact that for any two O_S-ideals $\mathfrak{a}$, $\mathfrak{b}$, and $k \in \mathbb{Z}$

$$|\mathfrak{ab}|_S = |\mathfrak{a}|_S \cdot |\mathfrak{b}|_S, \quad m_S(\mathfrak{ab}) \le m_S(\mathfrak{a}) m_S(\mathfrak{b}), \quad m_S(\mathfrak{a}^k) = m_S(\mathfrak{a})^{|k|}\,, \tag{4.1}$$

and for any two $\alpha, \beta \in K^*$

$$|\alpha\beta|_S = |\alpha|_S |\beta|_S, \quad m_S(\alpha\beta) \le m_S(\alpha) m_S(\beta), \quad m_S(\alpha^k) = m_S(\alpha)^{|k|}\,. \tag{4.2}$$

Further, if L/K is a finite extension and T is the set of prime ideals of O_L ([2]) lying above those in S then O_T, the ring of T-integers in L, is the integral closure of O_S in L. Then we have, by the definition of $|\cdot|_S$ and $m_S(\cdot)$

$$\begin{cases} |\mathfrak{a}|_T = |\mathfrak{a}|_S, \quad m_T(\mathfrak{a}) = m_S(\mathfrak{a}) & \text{for every } O_S\text{-ideal } \mathfrak{a}\,; \\ |\alpha|_T = |\alpha|_S, \quad m_T(\alpha) = m_S(\alpha) & \text{for all } \alpha \in K^*\,. \end{cases} \tag{4.3}$$

We recall that the height $h(F)$ of a polynomial F with algebraic coefficients is defined as the maximum of the heights of the coefficients of F. Further, the height $h(\mathbf{a})$ of a vector $\mathbf{a}$ with algebraic coordinates is defined as the maximum of the heights of the coordinates of $\mathbf{a}$. We define the height $h(A)$ of a matrix A with algebraic entries in a similar way. We recall some properties of the height from ([6], Lemma 1). Let α, β, $\alpha_1, \dots, \alpha_n$ be algebraic numbers with $\beta \neq 0$, and $f(X_1, \dots, X_n)$, $g(X)$ polynomials with algebraic coefficients. Then the following properties hold:

$$\begin{cases} h(\alpha^k) = h(\alpha)^{|k|} \quad \text{for } k \in \mathbb{Z}\,; \\ h(\alpha\beta) \le h(\alpha)h(\beta)\,;\ h(\alpha/\beta) \le h(\alpha)h(\beta)\,; \\ h(\alpha_1 + \ldots + \alpha_n) \le n h(\alpha_1)\ldots h(\alpha_n)\,; \end{cases} \tag{4.4}$$

$$\begin{cases} \text{if } f(X_1, \dots, X_n) \text{ has exactly } r \text{ non-zero coefficients} \\ \text{and degree } d_j \text{ in } X_j \text{ for } j = 1, \dots, n \text{ then} \\ h(f(\alpha_1, \dots, \alpha_n)) \le r h(f)^r h(\alpha_1)^{d_1} \ldots h(\alpha_n)^{d_n}\,; \end{cases} \tag{4.5}$$

$$|\alpha|_S \le h(\alpha) \quad \text{if } \alpha \in K\,; \tag{4.6}$$

$$\text{if } \theta \text{ is a zero of } g(X), \text{ then } h(\theta) \le \{4h(g)\}^{\deg(g)+1}. \tag{4.7}$$

From (4.4) and (4.5) it follows that if upper bounds for the heights of algebraic numbers $\alpha_1, \dots, \alpha_n$ are known and β is some rational expression in $\alpha_1, \dots, \alpha_n$, then an upper bound for $h(\beta)$ can be computed. This fact will be used frequently without refering to (4.4) and (4.5).

([2]) For any algebraic number field M, we denote by O_M the ring of integers of M.

In what follows, let s denote the cardinality of S, and P the largest of the prime numbers lying below the prime ideals in S, with $P = 1$ if $s = 0$.

LEMMA 3. *Let $\mathfrak{a}$ be an O_S-ideal. Then there is an $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$ and*

(i) $|\alpha|_S \leq c_1 |\mathfrak{a}|_S$,
(ii) $h(\alpha) \leq c_1 |\mathfrak{a}|_S$ *if $\mathfrak{a}$ is integral*

where c_1 is an effectively computable number depending only on d and $|D_K|$.

Proof. First we prove (ii). Let $\mathfrak{a}$ be an integral O_S-ideal and let $\mathfrak{a}^*$ be the O_K-ideal composed of prime ideals outside S such that $\mathfrak{a} = \mathfrak{a}^* O_S$. Let $\alpha \mapsto \alpha^{(i)}$ be the distinct $\mathbb{Q}$-isomorphisms of K in $\overline{\mathbb{Q}}$. By Satz 6 of [16], $\mathfrak{a}^*$ contains an element $\alpha \neq 0$ with $|\alpha^{(i)}| \leq c_1 N_{K/\mathbb{Q}}(\mathfrak{a}^*)^{1/d}$ for $i = 1, \ldots, d$ where c_1 is an effectively computable number depending only on d and $|D_K|$. Now Lemma 3(ii) follows from the fact that $h(\alpha) \leq \max_i |\alpha^{(i)}|$ and $N_{K/\mathbb{Q}}(\mathfrak{a}^*)^{1/d} = |\mathfrak{a}|_S$.

We now prove (i). Take $\delta \in K^*$ such that $\mathfrak{a}' := \delta\mathfrak{a} \subseteq O_S$. By (ii) there is an $\alpha' \in \mathfrak{a}'$ such that $\alpha' \neq 0$ and $h(\alpha') \leq c_1 |\mathfrak{a}'|_S$. Now (4.6) implies that $|\alpha'|_S \leq c_1 |\mathfrak{a}'|_S$. Put $\alpha := \delta^{-1}\alpha'$. Then (4.1), (4.2) imply that $|\alpha|_S \leq c_1 |\mathfrak{a}|_S$. ∎

We write $\alpha \equiv \beta \bmod \mathfrak{a}$ if $\alpha - \beta$ belongs to the O_S-ideal $\mathfrak{a}$ and, for $\gamma \in O_S$, $\alpha \equiv \beta \bmod \gamma$ if $\alpha - \beta \in (\gamma)$.

LEMMA 4. *Let $\mathfrak{a}$ be an integral O_S-ideal and $\beta \in O_S$. Then there is an $\alpha \in O_K$ such that*

$$\alpha \equiv \beta \bmod \mathfrak{a}, \qquad h(\alpha) \leq c_2 |\mathfrak{a}|_S \,,$$

where c_2 is an effectively computable number depending only on d and $|D_K|$.

Proof. See Lemma 6 of [6] with an explicitly given c_2. ∎

We now prove the result stated in Section 2, that every non-principal O_S-ideal class contains an integral ideal with generators of small height.

LEMMA 5. *Let $\mathfrak{a}$ be a non-principal O_S-ideal. Then there are $\gamma \in K^*$ and $\alpha, \beta \in O_S$ such that*

$$\gamma\mathfrak{a} = (\alpha, \beta), \qquad h(\alpha) \leq c_3, \qquad h(\beta) \leq c_3 \,,$$

where c_3 is an effectively computable number depending only on d and $|D_K|$.

Proof. c_4, c_5 will denote effectively computable numbers depending only on d and $|D_K|$. By Lemma 3(i) we can choose $\gamma \in \mathfrak{a}^{-1}$ such that $\gamma \neq 0$ and $|\gamma|_S \leq c_1 |\mathfrak{a}|_S^{-1}$. Put $\mathfrak{b} = \gamma\mathfrak{a}$. Note that $\mathfrak{b}$ is an integral O_S-ideal with $|\mathfrak{b}|_S \leq c_1$. By Lemma 3(ii) we can choose $\alpha \in \mathfrak{b}$ such that $\alpha \neq 0$ and $h(\alpha) \leq c_1 |\mathfrak{b}|_S \leq c_4$. Then $\mathrm{ord}_\mathfrak{p}(\alpha) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in M_K \setminus S$. By the Chinese Remainder Theorem (see e.g. [2], Ch. III, §3, Thm. 4) we can

choose $\beta \in O_S$ such that

$$\begin{aligned} &\mathrm{ord}_{\mathfrak{p}}(\beta) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) \quad \text{for all } \mathfrak{p} \in M_K \setminus S \text{ with } \mathrm{ord}_{\mathfrak{p}}(\alpha) > \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\,, \\ &\mathrm{ord}_{\mathfrak{p}}(\beta) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) \quad \text{for all } \mathfrak{p} \in M_K \setminus S \text{ with } \mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\,. \end{aligned} \tag{4.8}$$

Further, if β satisfies (4.8) then so does every $\beta' \in O_S$ with $\beta' \equiv \beta \bmod \alpha$. Hence by Lemma 4 and (4.6) there is a $\beta \in O_S$ satisfying (4.8) and

$$h(\beta) \leq c_2 |\alpha|_S \leq c_2 h(\alpha) \leq c_5\,.$$

For every $\mathfrak{p} \in M_K \setminus S$ we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = \min(\mathrm{ord}_{\mathfrak{p}}(\alpha), \mathrm{ord}_{\mathfrak{p}}(\beta))$. Hence $\mathfrak{b} = (\alpha, \beta)$. This proves Lemma 5. ∎

We now state some results on S-units.

LEMMA 6. *Let $\alpha \in K^*$ and $n \in \mathbb{N}$. Then there is an $\varepsilon \in O_S^*$ such that*

$$h(\varepsilon^n \alpha) \leq c_6^n m_S(\alpha), \quad \text{and} \quad h(\varepsilon^n \alpha) \leq c_6^n |\alpha|_S \quad \text{if } \alpha \in O_S \setminus \{0\}\,,$$

where c_6 is an effectively computable number depending only on d, $|D_K|$, s and P.

Proof. c_7, c_8 will denote effectively computable numbers depending only on d, $|D_K|$, s and P. Let $\mathfrak{a}$, $\mathfrak{b}$ be the integral O_S-ideals with $(\alpha) = \mathfrak{a}\mathfrak{b}^{-1}$ and $\mathfrak{a} + \mathfrak{b} = (1)$. By Lemma 3(i) we can choose $\gamma \in \mathfrak{b}$ with $\gamma \neq 0$ and $|\gamma|_S \leq c_1 |\mathfrak{b}|_S$. Put $\beta = \alpha \cdot \gamma$. Then $\beta \in \mathfrak{a}$ and $|\beta|_S \leq c_1 |\mathfrak{a}|_S$. Note that $\beta, \gamma \in O_S$. By Lemma 10 of [6] there are $\eta, \zeta \in O_S^*$ such that

$$h(\eta^n \beta) \leq c_7^n |\beta|_S \leq c_8^n |\mathfrak{a}|_S, \quad h(\zeta^n \gamma) \leq c_7^n |\gamma|_S \leq c_8^n |\mathfrak{b}|_S\,.$$

Put $\varepsilon = \eta/\zeta$. Then, by Lemma 3, $h(\varepsilon^n \alpha) \leq c_6^n |\mathfrak{a}|_S |\mathfrak{b}|_S = c_6^n m_S(\alpha)$. Further, if $\alpha \in O_S \setminus \{0\}$ then $m_S(\alpha) = |\alpha|_S$ and the proof is complete. ∎

We apply Lemma 6 in the following situation. Let L/K be a finite, normal extension, and let $A_1, \ldots, A_t$ be finite, non-empty subsets of L^* such that

$$\sigma(A_i) = A_{\sigma(i)} \quad \text{for } i = 1, \ldots, t, \quad \sigma \in \mathrm{Gal}(L/K)\,, \tag{4.9}$$

where $(\sigma(1), \ldots, \sigma(t))$ is a permutation of $(1, \ldots, t)$ for $\sigma \in \mathrm{Gal}(L/K)$. Consider the $\mathrm{Gal}(L/K)$-orbits $\mathcal{C}_1, \ldots, \mathcal{C}_u$ of $\{1, \ldots, t\}$ introduced in Section 3 (where i, j belong to the same orbit if and only if $\sigma(i) = j$ for some $\sigma \in \mathrm{Gal}(L/K)$). Let T be the set of prime ideals in O_L lying above those in S. Assume that

$$\begin{aligned} &m_T(\alpha) \leq C \quad \text{for } \alpha \in A_1 \cup \ldots \cup A_t \quad \text{and} \\ &h(\alpha/\beta) \leq C \quad \text{for } \alpha, \beta \in A_i,\ i = 1, \ldots, t\,. \end{aligned} \tag{4.10}$$

LEMMA 7. *For every $n_1, \ldots, n_u \in \mathbb{Z} \setminus \{0\}$ there are $\varepsilon_1, \ldots, \varepsilon_t \in O_T^*$ such that*

$$\sigma(\varepsilon_i) = \varepsilon_{\sigma(i)} \quad \textit{for } i = 1, \ldots, t \textit{ and for each } \sigma \in \mathrm{Gal}(L/K) \tag{4.11}$$

and

$$h(\varepsilon_i^{n_j}\alpha) \le c_9^{|n_j|}C^2 \quad \textit{for all } \alpha \in A_i \textit{ with } i \in \mathcal{C}_j,\ j = 1,\dots,u\,,$$

where c_9 is an effectively computable number depending only on d, $[L:K]$, $|D_L|$, s and P.

Proof. Let $\mathcal{C}$ be an arbitrary but fixed $\mathrm{Gal}(L/K)$-orbit of $\{1,\dots,t\}$. It suffices to prove that for every $n \in \mathbb{N}$, there are $\varepsilon_i \in O_T^*$ with $i \in \mathcal{C}$ such that

$$\sigma(\varepsilon_i) = \varepsilon_{\sigma(i)} \quad \text{for each } i \in \mathcal{C} \text{ and } \sigma \in \mathrm{Gal}(L/K) \tag{4.12}$$

and

$$h(\varepsilon_i^n\alpha) \le c_9^n C^2 \quad \text{for all } \alpha \in A_i \text{ with } i \in \mathcal{C}\,.$$

Let a_i be the cardinality of A_i for $i \in \mathcal{C}$. Put $\beta_i = \prod_{\alpha\in A_i}\alpha$ for $i \in \mathcal{C}$. Then by (4.9) we have $\sigma(\beta_i) = \beta_{\sigma(i)}$ for each $i \in \mathcal{C}$ and $\sigma \in \mathrm{Gal}(L/K)$. Let M_i $(i \in \mathcal{C})$ be the field defined by

$$\mathrm{Gal}(L/M_i) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(i) = i\}\,.$$

Then $\beta_i \in M_i^*$ for each $i \in \mathcal{C}$. By (4.9), Lemma 6, (3.4) and (4.10), we can choose $\varepsilon_i \in O_T^* \cap M_i^*$ $(i \in \mathcal{C})$ such that (4.12) is satisfied and

$$h(\varepsilon_i^{na_i}\beta_i) \le c_{10}^{na_i} m_T(\beta_i) \le \{c_9^n C\}^{a_i} \tag{4.13}$$

with some effectively computable number c_{10} which depends only on d, $[L:K]$, $|D_L|$, s and P. By the second inequality of (4.10), for every $\alpha \in A_i$ we have

$$h(\alpha^{a_i}/\beta_i) \le \prod_{\beta\in A_i} h(\alpha/\beta) \le C^{a_i}\,.$$

By combining this with (4.13) we get

$$h(\varepsilon_i^n\alpha) \le \{h(\varepsilon_i^{na_i}\beta_i)h(\alpha^{a_i}/\beta_i)\}^{1/a_i} \le c_9^n C^2 \quad \text{for } i \in \mathcal{C}\,. \ \blacksquare$$

The next result is our main tool in the proof of Theorem 2.

Lemma 8. *Let $x_0, x_1, x_2 \in K^*$ such that*

$$x_0 + x_1 + x_2 = 0 \quad \textit{and} \quad m_S(x_i) \le A \quad \textit{for } i = 0,1,2\,.$$

Then

$$h(x_i/x_j) \le c_{11}A^{c_{12}} \quad \textit{for } i,j \in \{0,1,2\}\,, \tag{4.14}$$

where c_{11}, c_{12} are effectively computable numbers depending only on d, $|D_K|$, s and P.

Proof. Let $\mathfrak{a}_i$, $\mathfrak{b}_i$ be the integral O_S-ideals such that $(x_i) = \mathfrak{a}_i\mathfrak{b}_i^{-1}$ and $\mathfrak{a}_i + \mathfrak{b}_i = (1)$ $(i = 0,1,2)$ and put $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_3$. By Lemma 3 (i) we can choose $\beta \in \mathfrak{b}$ such that $\beta \ne 0$ and $|\beta|_S \le c_1|\mathfrak{b}|_S$. Put $y_i = \beta x_i$ for $i = 0,1,2$. Then

$$y_0 + y_1 + y_2 = 0, \quad y_i \in O_S \setminus \{0\},\ |y_i|_S \le B := c_1A^4 \text{ for } i = 0,1,2\,.$$

By Lemma 11 of [6], there are effectively computable numbers c_{13}, c_{14} depending only on d, $|D_K|$, s and P, such that

$$h(y_i/y_j) \le c_{13}B^{c_{14}} \quad \text{for } i,j \in \{0,1,2\}\,.$$

This implies (4.14). We remark that Lemma 11 of [6] was a reformulation of an effective result of Győry on S-unit equations ([10], Lemma 6), and that Győry proved this result by applying Baker's theory on linear forms in logarithms and its p-adic analogue. ∎

5. Effective reduction of matrices. As before, let K be an algebraic number field and S a finite set of prime ideals of O_K. The parameters d, D_K, s and P have the same meaning as in the previous sections. If V is any set then $V^{m,n}$ denotes the collection of $m \times n$ matrices with entries in V. If A, $B \in K^{m,n}$ then we write $A \equiv B \bmod \mathfrak{a}$ if the entries of $A - B$ belong to the O_S-ideal $\mathfrak{a}$, and $A \equiv B \bmod \gamma$ if $\mathfrak{a} = (\gamma)$ for some $\gamma \in K^*$. For every integral O_S-ideal $\mathfrak{a}$, let $G(n,\mathfrak{a})$ be the multiplicative group of matrices U with the following properties:

$$U \in O_S^{n,n}; \quad \det U \in O_S^*\,;$$

$$U \equiv \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix} \bmod \mathfrak{a} \quad \text{for some } \varepsilon_1,\dots,\varepsilon_n \in O_S^*\,.$$

It easily follows from (1.5) that if $\mathfrak{a} = (\alpha,\beta)$ and $\mathfrak{M}$ is the O_S-lattice $(\mathbf{e}_1,\dots,\mathbf{e}_{n-1},\alpha\mathbf{e}_n,\beta\mathbf{e}_n)$ then

$$G(n,\mathfrak{a}) \subseteq G(\mathfrak{M})\,. \tag{5.1}$$

In this section we shall prove the following result.

LEMMA 9. *Let $n \ge 2$ be an integer. For every non-singular matrix A in $O_S^{n,n}$, there is a matrix U in $G(n,\mathfrak{a})$ such that*

$$h(AU) \le c_{15}\{|\det A|_S \cdot |\mathfrak{a}|_S\}^{c'_{15}}$$

where c_{15}, c'_{15} are effectively computable numbers such that c_{15} depends only on d, $|D_K|$, s, P and n, and c'_{15} only on n.

In the proof of Lemma 9 we need some auxiliary results.

LEMMA 10. *Let $A_1, A_2 \in O_S^{n,n}$ be two non-singular matrices with $(\det A_1)/(\det A_2) \in O_S^*$ and $A_1 \equiv A_2 \bmod (\det A_1)\mathfrak{a}$. Then there is a matrix $U \in G(n,\mathfrak{a})$ with $A_2 = A_1U$.*

Proof. Let $U = A_1^{-1}A_2$. By assumption, there is a matrix $C \in \mathfrak{a}^{n,n}$ such that $A_2 = A_1 + (\det A_1)C$. Hence

$$U = A_1^{-1}(A_1 + (\det A_1)C) = I + \{(\det A_1)A_1^{-1}\}C \equiv I \bmod \mathfrak{a}\,,$$

where I is the $n \times n$ identity matrix. Further, $\det U \in O_S^*$. Hence $U \in G(n, \mathfrak{a})$. ∎

LEMMA 11. *Let $A \in K^{m,n}$ be a matrix of rank m, $\mathbf{b} \in K^m$ and assume that the system of linear equations*

$$A\mathbf{x} = \mathbf{b} \quad \text{in } \mathbf{x} \in O_S^n \tag{5.2}$$

is solvable. Then (5.2) has a solution $\mathbf{x} \in O_S^n$ with

$$h(\mathbf{x}) \leq c_{16}\{h(A)h(\mathbf{b})\}^{c'_{16}},$$

where c_{16}, c'_{16} are effectively computable numbers such that c_{16} depends only on d, $|D_K|$ and n, and c'_{16} only on n.

Proof. For $i = 17, \ldots, 20$, c_i, c'_i will denote effectively computable numbers such that c_i depends only on d, $|D_K|$ and n, and c'_i only on n. We assume that the matrix C formed by the first m columns of A is non-singular, which is no restriction. Then

$$C^{-1}A = (I, A')$$

where I is the $m \times m$ unit matrix and $A' \in K^{m,n-m,}$. For every solution $\mathbf{x} \in O_S^n$ of (5.2), let $\mathbf{y}$, $\mathbf{z}$ be the vectors consisting of the first m coordinates of $\mathbf{x}$ and the last $n - m$ coordinates of $\mathbf{x}$, respectively. Put $\mathbf{b}' = C^{-1}\mathbf{b}$. Then (5.2) is equivalent to

$$\mathbf{y} + A'\mathbf{z} = \mathbf{b}' \quad \text{in } \mathbf{y} \in O_S^m,\ \mathbf{z} \in O_S^{n-m}. \tag{5.3}$$

Let $(\mathbf{y}_0, \mathbf{z}_0)$ be a solution of (5.3). By (2.1), (4.4) and (4.6), there is a non-zero rational integer a such that aA' has integral entries in K and

$$|a|_S \leq c_{17}h(A')^{c'_{17}} \leq c_{18}h(A)^{c'_{18}}.$$

By Lemma 4, there is a vector $\mathbf{z} \in O_S^{n-m}$ with

$$\mathbf{z} \equiv \mathbf{z}_0 \bmod a, \quad h(\mathbf{z}) \leq c_2|a|_S \leq c_{19}h(A)^{c'_{19}}. \tag{5.4}$$

Put $\mathbf{y} = \mathbf{b}' - A'\mathbf{z}$. It is easy to see that $\mathbf{y} \in O_S^m$. Further, $(\mathbf{y}, \mathbf{z})$ is a solution of (5.3), and, by (4.4) and (5.4),

$$h(\mathbf{y}) \leq c_{20}\{h(A')h(\mathbf{z})h(\mathbf{b})\}^{c'_{20}} \leq c_{16}\{h(A)h(\mathbf{b})\}^{c'_{16}}. \ ∎$$

If B is any $n \times n$ matrix then we denote by B_{ij} the matrix obtained by removing the ith row and jth column from B. For $n = 1$, we shall take $\det B_{1,1} = 1$. If $\mathfrak{p}$ is any prime ideal of O_K outside S and $\alpha_1, \ldots, \alpha_n \in K$ then we put $\operatorname{ord}_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_n) = \min(\operatorname{ord}_{\mathfrak{p}}(\alpha_1), \ldots, \operatorname{ord}_{\mathfrak{p}}(\alpha_n))$.

LEMMA 12. *Let $n \geq 1$ be an integer, let $A \in O_S^{n,n}$ be a non-singular matrix, let S' be a finite set of prime ideals of O_K outside S, and let $\mathfrak{b}$ be*

an O_S-ideal with

$$\begin{aligned} &\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0 \quad \textit{for all } \mathfrak{p} \in M_K \setminus (S \cup S')\,, \\ &\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b}) > \operatorname{ord}_{\mathfrak{p}}(\det A) \quad \textit{for all } \mathfrak{p} \in S'\,. \end{aligned} \tag{5.5}$$

Then there exists a matrix $B \in O_S^{n,n}$ with the following properties:

$$B \equiv A \bmod \mathfrak{b}\,; \tag{5.6}$$

$$h(B) \le c_{21}|\mathfrak{b}|_S^{c_{21}}\,, \tag{5.7}$$

where c_{21}, c'_{21} are effectively computable numbers such that c_{21} depends only on d, $|D_K|$ and n, and c'_{21} only on n;

$$\det B \ne 0\,; \tag{5.8}$$

$$\operatorname{ord}_{\mathfrak{p}}(\det B_{1n}, \dots, \det B_{nn}) = 0 \quad \textit{for all } \mathfrak{p} \in M_K \setminus (S \cup S')\,. \tag{5.9}$$

P r o o f. $c_{22}, \dots, c_{27}$ will denote effectively computable numbers of the form $c|\mathfrak{b}|_S^{c'}$, where c depends only on d, $|D_K|$, n, and c' only on n. We proceed by induction on n. For $n = 1$, our assertion means that if $\alpha \in O_S \setminus \{0\}$ and $\mathfrak{b}$ is an integral O_S-ideal with $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0$ for all $\mathfrak{p} \in M_K \setminus \{S \cup S'\}$ and $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b}) > \operatorname{ord}_{\mathfrak{p}}(\alpha)$ for all $\mathfrak{p} \in S'$, then there is a $\beta \in O_S \setminus \{0\}$ with $\beta \equiv \alpha \bmod \mathfrak{b}$ and $h(\beta) \le c_{22}$; by Lemma 4 we know that this is true. Hence let $n \ge 2$ and assume that Lemma 12 holds for $n - 1$.

By Lemma 4, there is a matrix $A' \in O_S^{n,n}$ such that

$$A' \equiv A \bmod \mathfrak{b} \quad \text{and} \quad h(A') \le c_{23}\,. \tag{5.10}$$

Then $\det A' \equiv \det A \bmod \mathfrak{b}$. Since $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b}) > \operatorname{ord}_{\mathfrak{p}}(\det A)$ for all $\mathfrak{p} \in S'$, this implies that $\det A' \ne 0$. Hence at least one of the determinants $\det(A'_{1,n}), \dots$ $\dots, \det(A'_{n,n})$ must be non-zero; we assume that $\det(A_{n,n}) \ne 0$, which is no restriction. Put $A = A'_{n,n}$. Since $h(\overline{A}) \le h(A') \le c_{23}$, by (4.6) we have $|\det \overline{A}|_S \le h(\overline{A}) \le c_{23}$. It is easy to see that there is an integral O_S-ideal $\overline{\mathfrak{b}}$ such that

$$\begin{aligned} &\operatorname{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}}) \ge \operatorname{ord}_{\mathfrak{p}}(\mathfrak{b})\,; \\ &\operatorname{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}}) > \max(\operatorname{ord}_{\mathfrak{p}}(\det \overline{A}), \operatorname{ord}_{\mathfrak{p}}(\det A')) \quad \text{for } \mathfrak{p} \in S'\,, \\ &\operatorname{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}}) \ge 0 \quad \text{for all } \mathfrak{p} \in M_K \setminus (S \cup S')\,, \\ &|\overline{\mathfrak{b}}|_S \le c_{24}\,. \end{aligned} \tag{5.11}$$

By the induction hypothesis, there is a matrix $\overline{B} \in O_S^{n-1,n-1}$ such that

$$\begin{aligned} &\overline{B} \equiv \overline{A} \bmod \overline{\mathfrak{b}}, \quad h(\overline{B}) \le c_{25}, \quad \det \overline{B} \ne 0\,, \\ &\operatorname{ord}_{\mathfrak{p}}(\det \overline{B}_{1,n-1}, \dots, \det \overline{B}_{n-1,n-1}) = 0 \\ &\qquad\qquad \text{for all } \mathfrak{p} \in M_K \setminus (S \cup S')\,. \end{aligned} \tag{5.12}$$

Here we put $\overline{B}_{1,n-1} := 1$ if $n = 2$. By the Chinese Remainder Theorem, we

can choose $\xi \in O_S$ such that

$$(5.13)\quad \begin{cases} \operatorname{ord}_{\mathfrak{p}}(\xi) \geq \operatorname{ord}_{\mathfrak{p}}(\overline{\mathfrak{b}}) & \text{for all } \mathfrak{p} \in S'; \\ \operatorname{ord}_{\mathfrak{p}}(\xi) = 0 & \text{for all } \mathfrak{p} \in M_K \setminus (S \cup S') \\ & \quad \text{with } \operatorname{ord}_{\mathfrak{p}}(\gamma_1, \dots, \gamma_n) > 0; \\ \operatorname{ord}_{\mathfrak{p}}(\xi) > 0 & \text{for all } \mathfrak{p} \in M_K \setminus (S \cup S') \text{ with } \operatorname{ord}_{\mathfrak{p}}(\gamma_n) > 0 \\ & \quad \text{and } \operatorname{ord}_{\mathfrak{p}}(\gamma_1, \dots, \gamma_{n-1}) = 0; \\ \operatorname{ord}_{\mathfrak{p}}(\xi) \geq 0 & \text{for the other prime ideals } \mathfrak{p} \text{ in } M_K \setminus (S \cup S'). \end{cases}$$

Then, by (5.5) and (5.11), $\xi \in \mathfrak{b}$. It is easy to check that if ξ_0 satisfies (5.13), then so does every $\xi \in O_S$ with $\xi \equiv \xi_0 \bmod (\det \overline{B})\overline{\mathfrak{b}}$. By (5.10), (5.12), (4.6) and Lemma 4, we can choose ξ such that

$$(5.14)\qquad h(\xi) \leq c_{26}\,.$$

Let C be the $n \times n$ matrix obtained from A' by replacing $\overline{A}$ by $\overline{B}$ and leaving the nth row and nth column of A' unchanged. Let $C = (c_{ij})_{1 \leq i,j \leq n}$. We construct B from C by replacing $c_{n,n-1}$ by $c_{n,n-1} + \xi$ with the above ξ and leaving the other entries of C unchanged. Write

$$\overline{\beta}_i = \det \overline{B}_{i,n-1}, \qquad \gamma_i = \det C_{in}, \qquad beta_i = \det B_{in}\,.$$

Then

$$(5.15)\quad \beta_1 = \gamma_1 + \xi\overline{\beta}_1, \quad \dots, \quad \beta_{n-1} = \gamma_{n-1} + \xi\overline{\beta}_{n-1}, \quad \beta_n = \gamma_n = \det \overline{B}\,.$$

By construction, we have $B \equiv A \bmod \mathfrak{b}$, hence

$$\operatorname{ord}_{\mathfrak{p}}(\det B) = \operatorname{ord}_{\mathfrak{p}}(\det A) \quad \text{for all } \mathfrak{p} \in S'\,,$$

which implies that $\det B \neq 0$. Further, $h(B) \leq c_{27}$ by (5.10), (5.12) and (5.14).

It remains to prove (5.9), i.e.

$$(5.16)\qquad \operatorname{ord}_{\mathfrak{p}}(\beta_1, \dots, \beta_n) = 0 \quad \text{for all } \mathfrak{p} \in M_K \setminus (S \cup S')\,.$$

This is obvious if $\operatorname{ord}_{\mathfrak{p}}(\beta_n) = \operatorname{ord}_{\mathfrak{p}}(\det \overline{B}) = 0$. Let $\mathfrak{p} \in M_K \setminus (S \cup S')$ be such that $\operatorname{ord}_{\mathfrak{p}}(\det \overline{B}) > 0$. If $\operatorname{ord}_{\mathfrak{p}}(\gamma_i) = 0$ for some $i \in \{1, \dots, n-1\}$ then by (5.15) and (5.13) we have $\operatorname{ord}_{\mathfrak{p}}(\beta_i) = 0$. By (5.12) we know that there is an $i \in \{1, \dots, n-1\}$ with $\operatorname{ord}_{\mathfrak{p}}(\overline{\beta}_i) = 0$. Hence if $\operatorname{ord}_{\mathfrak{p}}(\gamma_j) > 0$ for $j = 1, \dots, n-1$, then by (5.15) and (5.13), $\operatorname{ord}_{\mathfrak{p}}(\beta_i) = 0$. This proves (5.16) and completes the proof of Lemma 12. ∎

Proof of Lemma 9. By Lemma 3(ii), we can choose $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$ and $h(\alpha) \leq c_1 |\mathfrak{a}|_S$. Further, by Lemma 6, we can choose $\varepsilon \in O_S^*$ such that $h(\varepsilon \det A) \leq c_6 |\det A|_S$. Put

$$A_1 = A \begin{pmatrix} \varepsilon & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \quad \text{and} \quad \Delta = \det A_1\,;$$

then

$$h(\Delta) \le c_6 |\det A|_S .$$

Since

$$\begin{pmatrix} \varepsilon & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in G(n, \mathfrak{a}) ,$$

by Lemma 10 it suffices to prove that there is a matrix $C \in O_S^{n,n}$ with

$$C \equiv A_1 \bmod \alpha\Delta, \quad h(C) \le c_{28}(h(\alpha)h(\Delta))^{c'_{28}}, \quad \det C = \Delta , \tag{5.17}$$

where c_{28}, c'_{28} are effectively computable numbers such that c_{28} depends only on d, $|D_K|$, s, P and n, and c'_{28} only on n. In what follows, $c_{29}, \dots, c_{32}$ denote effectively computable numbers of the form $c(h(\alpha)h(\Delta))^{c'}$ where c depends only on d, $|D_K|$, s, P and n, and c' only on n; we shall frequently use the fact that, by (4.6), $|\alpha|_S \le h(\alpha)$ and $|\Delta|_S \le h(\Delta)$.

By Lemma 12, there is a matrix $B \in O_S^{n,n}$ such that

$$\begin{aligned} &B \equiv A_1 \bmod \alpha\Delta^2, \quad h(B) \le c_{29}, \quad \det B \ne 0 , \\ &\operatorname{ord}_{\mathfrak{p}}(\det B_{1n}, \dots, \det B_{nn}) = 0 \\ &\qquad \text{for every } \mathfrak{p} \in M_K \setminus S \text{ with } \operatorname{ord}_{\mathfrak{p}}(\alpha\Delta) = 0 . \end{aligned} \tag{5.18}$$

Let $\kappa_1, \dots, \kappa_n$ be the entries in the last column of B, and put $\Delta_i = \det B_{in}$ for $i = 1, \dots, n$. We shall construct C by replacing κ_i by $\kappa_i + \xi_i\alpha\Delta$ for certain $\xi_i \in O_S$, $i = 1, \dots, n$, and leaving the other entries of B unchanged. Then, by (5.18), $C \equiv A_1 \bmod \alpha\Delta$. We have to choose $\xi_1, \dots, \xi_n$ such that $\det C = \Delta$, that is,

$$\sum_{i=1}^{n} (-1)^{i-1} \Delta_i (\kappa_i + \xi_i \alpha\Delta) = \Delta . \tag{5.19}$$

Since $B \equiv A_1 \bmod \alpha\Delta^2$ and $\det A_1 = \Delta$, there is a $\gamma \in O_S$ such that

$$\det B = \Delta - \gamma\alpha\Delta^2 . \tag{5.20}$$

Hence

$$\sum_{i=1}^{n} (-1)^{i-1} \Delta_i \kappa_i = \Delta - \gamma\alpha\Delta^2 = \Delta(1 - \gamma\alpha\Delta) . \tag{5.21}$$

By inserting this into (5.19) we get

$$\sum_{i=1}^{n} (-1)^{i-1} \Delta_i \xi_i = \gamma\Delta . \tag{5.22}$$

If $\mathfrak{p}$ is a prime ideal of O_K outside S with $\mathrm{ord}_{\mathfrak{p}}(\alpha\Delta) > 0$, then $\mathrm{ord}_{\mathfrak{p}}(1 - \gamma\alpha\Delta) = 0$, hence, by (5.21),

$$\mathrm{ord}_{\mathfrak{p}}(\Delta_1, \ldots, \Delta_n) \leq \mathrm{ord}_{\mathfrak{p}}(\Delta)\,.$$

Together with (5.18) this implies that $\Delta \in (\Delta_1, \ldots, \Delta_n)$. Hence (5.22) is solvable in $\xi_1, \ldots, \xi_n \in O_S$. By (5.18) and (5.20) we have

$$\max(h(\Delta_1), \ldots, h(\Delta_n), h(\gamma\Delta)) \leq c_{30}\,.$$

Now Lemma 11 implies that there are $\xi_1, \ldots, \xi_n$ satisfying (5.22) with $h(\xi_i) \leq c_{31}$ for $i = 1, \ldots, n$. We conclude that $h(C) \leq c_{32}$. ∎

6. Proof of Theorem 2. Let K be an algebraic number field and S a finite set of prime ideals of O_K. Further, let $(\mathfrak{M}, F)$ be an O_S-lattice decomposable form pair such that $\mathrm{rank}\,\mathfrak{M} = n$, $\deg(F) = r$, F has splitting field L and $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$. In what follows, $c_{33}, \ldots, c_{63}$ will denote effectively computable numbers of the form $c|\mathfrak{d}|_S^{c'}$, where c, c' depend only on $d = [K : \mathbb{Q}], |D_L|, n, r$, the cardinality s of S and the maximum P of the prime numbers lying below the prime ideals in S.

Since every O_S-lattice is isomorphic to a reduced one, we may assume that $\mathfrak{M}$ is reduced. Then, as was seen in Section 2, F can be considered as a polynomial in $K[X_1, \ldots, X_n]$. We shall prove that there are $\mu \in K^*$ and a matrix $U \in G(\mathfrak{M})$ such that the polynomial $F'(\mathbf{X}) = \mu F(U\mathbf{X})$ has height

$$h(F') \leq c_{33}\,. \tag{6.1}$$

This obviously implies Theorem 2. Since this is trivial for $n = 1$, we shall assume $n \geq 2$.

It follows from our assumption that either

$$\mathfrak{M} = O_S^n \quad \text{or} \quad \mathfrak{M} = (\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)\,, \tag{6.2}$$

where $\mathfrak{a} = (\alpha, \beta)$ is an integral O_S-ideal and

$$h(\alpha) \leq c_{34}, \quad h(\beta) \leq c_{34}\,. \tag{6.3}$$

Let T be the set of prime ideals of O_L lying above those in S. For $Q(\mathbf{X}) \in L[X_1, \ldots, X_n]$, let (Q) be the O_T-ideal generated by the coefficients of Q, and put $|Q|_T = N_{L/\mathbb{Q}}(\mathfrak{b})^{1/[L:\mathbb{Q}]}$, where $\mathfrak{b}$ is the O_L-ideal composed of prime ideals outside T, such that $\mathfrak{b}O_T = (Q)$. Further, for $\sigma \in \mathrm{Gal}(L/K)$ we denote by $\sigma(Q)$ the polynomial obtained by applying σ to the coefficients of Q. We claim that the decomposable form F (considered as a polynomial in $K[X_1, \ldots, X_n]$) can be factored as

$$F(\mathbf{X}) = \lambda \prod_{i=1}^{t} l_i(\mathbf{X})^{k_i} \tag{6.4}$$

where $\lambda \in K^*$, $l_1, \dots, l_t$ are pairwise non-proportional linear forms in $L[X_1, \dots, X_n]$ and $k_1, \dots, k_t$ are positive integers such that

$$\text{(6.5.a)} \qquad \sigma(l_i) = l_{\sigma(i)}, \quad k_i = k_{\sigma(i)} \quad \text{for } i = 1, \dots, t \text{ and for all } \sigma \in \mathrm{Gal}(L/K),$$

and

$$\text{(6.5.b)} \qquad l_i(\mathbf{X}) \in O_T[X_1, \dots, X_n] \quad \text{and} \quad |l_i|_T \le c_{35} \quad \text{for } i = 1, \dots, t,$$

where $(\sigma(1), \dots, \sigma(t))$ is a permutation of $(1, \dots, t)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Namely, it is obvious that there exist $\lambda' \in K^*$ and linear forms $l'_1, \dots, l'_t$ which satisfy (6.4) and (6.5.a). Then $l'_i(\mathbf{X}) \in M_i[X_1, \dots, X_n]$, where the field M_i is defined by

$$\mathrm{Gal}(L/M_i) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(i) = i\}.$$

Let (l'_i) be the O_T-ideal generated by the coefficients of l'_i. By Lemma 3(i) and (3.4) there exist $\alpha_i \in (l'_i)^{-1} \cap M_i$ with $\alpha_i \neq 0$, $|\alpha_i|_T \le c_{36}|l'_i|_T^{-1}$ and $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ for $i = 1, \dots, t$ and $\sigma \in \mathrm{Gal}(L/K)$. Put

$$\lambda = \lambda' \prod_{i=1}^{t} \alpha_i^{-k_i} \quad \text{and} \quad l_i = \alpha_i l'_i \quad \text{for } i = 1, \dots, t.$$

Then obviously $\lambda \in K^*$ and $l_1, \dots, l_t$ satisfy (6.5.a) and (6.5.b).

Let λ, $l_1, \dots, l_t$ satisfy (6.4), (6.5.a), (6.5.b) and let $\mathcal{I}(F)$ be the collection of linearly independent subsets $\{l_{i_1}, \dots, l_{i_n}\}$ ($n = \mathrm{rank}\ \mathfrak{M}$) of $\{l_1, \dots, l_t\}$. We denote by $\det(l_{i_1}, \dots, l_{i_n})$ the coefficient determinant of $l_{i_1}, \dots, l_{i_n}$.

Lemma 13. *For each $\{l_{i_1}, \dots, l_{i_n}\} \in \mathcal{I}(F)$, we have*

$$|\det(l_{i_1}, \dots, l_{i_n})|_T \le c_{37}.$$

Proof. By assumption, $\mathfrak{M}$ is one of the O_S-lattices given in (6.2); we put $\alpha = 1$, $\beta = 0$, $\mathfrak{a} = (1)$ if $\mathfrak{M} = O_S^n$. For $\mathcal{L} = \{l_{i_1}, \dots, l_{i_n}\} \in \mathcal{I}(F)$, let $\mathfrak{d}(\mathfrak{M}, \mathcal{L})$ be the O_T-ideal generated by the numbers $\det(l_{i_k}(\mathbf{x}_j))_{1 \le k,j \le n}$ for $\mathbf{x}_1, \dots, \mathbf{x}_n \in \mathfrak{M}$. Since $\mathfrak{M} \subseteq O_S^n$, the ideal $\mathfrak{d}(\mathfrak{M}, \mathcal{L})$ must be divisible by $\det(l_{i_1}, \dots, l_{i_n})$. Let $(l_i(\mathfrak{M}))$ be the O_T-ideal generated by the numbers $l_i(\mathbf{x})$ with $\mathbf{x} \in \mathfrak{M}$. Then $(l_i(\mathfrak{M}))$ is generated by $l_i(\mathbf{e}_1), \dots, l_i(\mathbf{e}_{n-1}), \alpha l_i(\mathbf{e}_n)$ and $\beta l_i(\mathbf{e}_n)$, hence it divides $\alpha(l_i)$. Together with (4.6), (6.3) and (6.5.b) this implies that

$$|(l_i(\mathfrak{M}))|_T \le |\alpha|_T \cdot |l_i|_T \le c_{38} \quad \text{for } i = 1, \dots, t.$$

By the definition of $\mathfrak{D}(\mathfrak{M}, F)$ we have

$$\Big(\prod_{\mathcal{I}(F)} \det(l_{i_1}, \dots, l_{i_n}) \Big)^2 \supseteq \prod_{\mathcal{I}(F)} \mathfrak{d}(\mathfrak{M}, \mathcal{L})^2 = \mathfrak{d} \cdot \prod_{\mathcal{I}(F)} (l_{i_1}(\mathfrak{M}) \dots l_{i_n}(\mathfrak{M}))^2,$$

hence

$$\Big(\prod_{\mathcal{I}(F)} |\det(l_{i_1},\dots,l_{i_n})|_T\Big)^2 \le c_{39}\,, \tag{6.6}$$

where the products are taken over all sets $\mathcal{L}=\{l_{i_1},\dots,l_{i_n}\}$ in $\mathcal{I}(F)$. Since $l_i(\mathbf{X})\in O_T[X_1,\dots,X_n]$, each factor $|\det(l_{i_1},\dots,l_{i_n})|_T$ is ≥ 1. Now Lemma 13 follows at once from (6.6). ∎

We define a hypergraph $\mathcal{G}$ as follows: take as vertices $1,\dots,t$ and as edges those subsets I of $\{1,\dots,t\}$ for which $\{l_i : i\in I\}$ is linearly dependent over L, while $\{l_i : i\in I'\}$ is linearly independent over L for every proper, non-empty subset I' of I. Thus, for each edge I of $\mathcal{G}$ we have a linear relation

$$\sum_{i\in I} c_i^{(I)} l_i = 0 \quad \text{identically in } \mathbf{X}\,, \tag{6.7}$$

where $c_i^{(I)}\in L^*$ for $i\in I$. Put $c_{ij}^{(I)}=c_i^{(I)}/c_j^{(I)}$ for any distinct $i,j\in I$. Then

$$l_j = -\sum_{i\in I\setminus\{j\}} c_{ij}^{(I)} l_i \quad \text{for } j\in I\,. \tag{6.8}$$

Since $\{l_i : i\in I\setminus\{j\}\}$ is linearly independent for $j\in I$, this implies that the numbers $c_{ij}^{(I)}$ are uniquely determined by $l_1,\dots,l_t$. We claim that

$$m_T(c_{ij}^{(I)}) \le c_{40} \quad \begin{array}{l}\text{for each edge } I \text{ of } \mathcal{G}\\ \text{and for any distinct } i,j\in I\,,\end{array} \tag{6.9}$$

where $m_T(\alpha)$ is defined similarly to $m_S(\alpha)$ in Section 4. Indeed, assume for convenience that $I=\{1,\dots,k\}\cup\{j\}$ with some $j>n$ and that $\{l_1,\dots,l_n\}$ is linearly independent. Then

$$c_{ij}^{(I)} = -\frac{\det(l_1,\dots,l_{i-1},l_j,l_{i+1},\dots,l_n)}{\det(l_1,\dots,l_n)} \tag{6.10}$$

and (6.9) follows from Lemma 13. We remark that if the linear forms l_i are replaced by $l_i'=\varepsilon_i l_i$ for $i=1,\dots,t$, then by (6.8), the numbers $c_{ij}^{(I)}$ will change into $c_{ij}'^{(I)}=\varepsilon_j\varepsilon_i^{-1}c_{ij}^{(I)}$. The most important part in the proof of Theorem 2 is to show that $\varepsilon_1,\dots,\varepsilon_t$ can be chosen so that the linear forms l_i' still satisfy (6.5.a) and (6.5.b) and that the numbers $c_{ij}'^{(I)}$ have small heights. For this, we shall have to use frequently (6.9) and Lemma 8.

In $\mathcal{G}$, a *path* of length v from i to j with $i,j\in\{1,\dots,t\}$ is a tuple

$$C=(i_1,I_1,i_2,I_2,\dots,i_v,I_v,i_{v+1})\,,$$

where $i_1,\dots,i_{v+1}\in\{1,\dots,t\}$, $i_1,\dots,i_v$ are pairwise distinct, $i_1=i$, $i_{v+1}=j$, $i_u\ne i_{u+1}$ and $i_u,i_{u+1}\in I_u$ for some edge I_u of $\mathcal{G}$ for $u=1,\dots,v$. The length of C is denoted by $l(C)$. A shortest path from i to j is a path from

i to j of minimal length. Put

$$g(C) = c_{i_1 i_2}^{(I_1)} c_{i_2 i_3}^{(I_2)} \dots c_{i_v i_{v+1}}^{(I_v)} .$$

We write $C^{-1} = (i_{v+1}, I_v, i_v, \dots, i_2, I_1, i_1)$. If $C_1 = (i_1, I_1, \dots, I_v, i_{v+1})$ and $C_2 = (i_{v+1}, I_{v+1}, \dots, I_m, i_{m+1})$ then we write $C_1 C_2 = (i_1, I_1, \dots, i_{v+1}, I_{v+1}, i_{v+1}, \dots, I_m, i_{m+1})$. Thus

$$g(C^{-1}) = g(C)^{-1} \quad \text{and} \quad g(C_1 C_2) = g(C_1) g(C_2) . \tag{6.11}$$

LEMMA 14. *Let C_1, C_2 be two paths in $\mathcal{G}$ from i to j with $i, j \in \{1, \dots, t\}$. Then*

$$h(g(C_1)/g(C_2)) \le c_{41}^{l(C_1)+l(C_2)} .$$

Proof. A path $(i_1, I_1, \dots, I_v, i_1)$ is called a *cycle*. It is easily seen that, by (6.11), it suffices to show Lemma 14 for paths C_1, C_2 which have no common vertices apart from i and j. If C_1, C_2 are two such paths from i to j, then $C_1 C_2^{-1}$ is a cycle. So in view of (6.11) it is enough to prove that for every cycle C in $\mathcal{G}$,

$$h(g(C)) \le c_{41}^{l(C)} . \tag{6.12}$$

Fix a subset J of $\{1, \dots, t\}$ of cardinality n such that $\{l_j : j \in J\}$ is linearly independent. For each edge I of $\mathcal{G}$, $\{l_i : i \in I\}$ is linearly dependent, hence ([3]) $|I \setminus J| \ge 1$. We say that a cycle $C = (i_1, I_1, \dots, I_v, i_1)$ is *J-admissible* if $|I_1 \setminus J| = \dots = |I_v \setminus J| = 1$. We first prove (6.12) for J-admissible cycles.

A J-admissible cycle $C = (i_1, I_1, \dots, i_v, I_v, i_1)$ is called *minimal* if either $v = 2$ or $v \ge 3$ and there are no $p, q \in \{1, \dots, v\}$ with $p < q$ and $\{p, q\} \ne \{1, 2\}, \{2, 3\}, \dots, \{v-1, v\}, \{1, v\}$ and an edge I of $\mathcal{G}$ such that $|I \setminus J| = 1$ and $i_p, i_q \in I$. For such a minimal J-admissible cycle with $v \ge 3$ we must have $i_1, \dots, i_v \in J$. Indeed, suppose that $i_u \notin J$ for some u with $1 \le u \le v$. Then there is a unique subset H of J such that

$$l_{i_u} = \sum_{h \in H} d_h l_h$$

for some $d_h \in L^*$. Now $I_{u-1} = I_u = \{i_u\} \cup H$ (with the convention that $I_0 := I_v$) and so i_{u-1} and i_{u+1} (with $i_{v+1} := i_1$) belong to $\{i_u\} \cap H$, which is impossible by the minimality of C.

We shall prove that for every J-admissible cycle C of length ≥ 3 there are minimal J-admissible cycles $C_1, \dots, C_w$ such that $w \le l(C) - 2$ and

$$g(C) = g(C_1) \dots g(C_w) . \tag{6.13}$$

([3]) By $|A|$ we denote the cardinality of a set A.

We proceed by induction on $l(C)$. Every J-admissible cycle of length 3 must be minimal, which proves (6.13) for such cycles C. Assume that (6.13) holds for all J-admissible cycles of length $< v$ where $v \geq 4$, and let $C = (i_1, I_1, \dots, I_v, i_1)$ be a J-admissible cycle. If C is minimal then (6.13) obviously holds with $C_1 = C$. Hence we assume that C is not minimal. Then there are $p, q \in \{1, \dots, v\}$ with $p < q$ and $\{p, q\} \neq \{1, 2\}, \dots$ $\dots, \{v-1, v\}, \{1, v\}$ and an edge I of $\mathcal{G}$ with $|I \setminus J| = 1$ containing i_p and i_q. Put $C' = (i_1, I_1, \dots, i_p, I, i_q, \dots, i_1)$, $C'' = (i_p, I_{p+1}, \dots, i_q, I, i_p)$. Then C', C'' are J-admissible cycles with $3 \leq l(C') < l(C)$, $3 \leq l(C'') < l(C)$ and $l(C') + l(C'') = l(C) + 2$. Further, $g(C) = g(C')g(C'')$. Now (6.13) follows for C, by applying the induction hypothesis to C' and C''.

In view of (6.13), (6.12) follows for J-admissible cycles, once we have proved that for every *minimal* J-admissible cycle C,

$$h(g(C)) \leq c_{42}\,. \tag{6.14}$$

The only minimal J-admissible cycles of length 2 are of the form (i_1, I, i_2, I, i_1) and for such cycles C one has $g(C) = 1$. So we only consider minimal J-admissible cycles of length ≥ 3. As we showed above, all vertices of such a minimal cycle C belong to J. For convenience we assume that $J = \{1, \dots, n\}$ and that $C = (1, I_1, 2, I_2, \dots, v, I_v, 1)$ is a minimal J-admissible cycle with $v \geq 3$. Let p_u be the element of I_u not belonging to J, and let $I'_u = I_u \cap \{v+1, \dots, n\}$ for $u = 1, \dots, v$. Then, by (6.8),

$$l_{p_u} = d_{uu} l_u + d_{u,u+1} l_{u+1} + \sum_{j \in I'_u} d_{uj} l_j \quad \text{for } u = 1, \dots, v-1\,,$$

and

$$l_{p_v} = d_{v1} l_1 + d_{vv} l_v + \sum_{j \in I'_v} d_{vj} l_j\,,$$

where $d_{uj} = -c_{j,p_u}^{(I_u)}$ for $u = 1, \dots, v$. This implies that

$$\frac{\det(l_{p_1}, \dots, l_{p_v}, l_{v+1}, \dots, l_n)}{\det(l_1, \dots, l_n)} \tag{6.15}$$

$$= \begin{vmatrix} d_{11} & d_{12} & & & 0 \\ & d_{22} & d_{23} & & \\ \vdots & & \ddots & \ddots & \\ & 0 & & d_{v-1,v-1} & d_{v-1,v} \\ d_{1v} & & & & d_{vv} \end{vmatrix}$$

$$= d_{11} d_{22} \dots d_{vv} \pm d_{12} \dots d_{v-1,v} d_{1v}\,.$$

Put $\xi = d_{11} \dots d_{vv}$, $\eta = d_{12} \dots d_{v-1,v} d_{1v}$, and denote the left-hand side of (6.15) by ζ. Then, by (6.15), $\xi \pm \eta = \zeta$. Since $d_{uj}/d_{uk} = c_{jk}^{(I_u)}$ for $j, k \in I_u$,

we have

$$\xi/\eta = \pm g(C)\,. \tag{6.16}$$

Further, by (6.9) and (4.2), $m_T(\xi) \le c_{43}$, $m_T(\eta) \le c_{43}$ and by Lemma 13 we also have $m_T(\zeta) \le c_{43}$. If $\zeta = 0$, then $\xi/\eta = \pm 1$. If $\zeta \ne 0$ then by Lemma 8, $h(\xi/\eta) \le c_{44}$. Now (6.16) implies that $h(g(C)) \le c_{42}$. This proves (6.14).

For every path $C = (i_1, I_1, \dots, i_v, I_v, i_{v+1})$ in $\mathcal{G}$ we put

$$m(C) = \max\{|I_u \setminus J| : 1 \le u \le v\}\,.$$

Obviously, $m(C) \ge 1$. We shall prove that for every cycle C in $\mathcal{G}$ with $m(C) = m \ge 1$, there is a J-admissible cycle C' in $\mathcal{G}$ with $l(C') \le 2^{m-1} l(C)$ and

$$h(g(C)/g(C')) \le c_{45}^{l(C)}\,. \tag{6.17}$$

Since $m \le n$, this implies Lemma 14.

We shall prove (6.17) by induction on $m(C)$. For $m(C) = 1$ we are done. Let $m \ge 2$ and assume that (6.17) holds for all cycles C in $\mathcal{G}$ with $m(C) < m$. Let $C = (i_1, I_1, \dots, i_v, I_v, i_1)$ be a cycle with $m(C) = m$ and put $i_{v+1} := i_1$. In view of (6.11), it suffices to prove that for each $u \in \{1, \dots, v\}$ with $|I_u \setminus J| = m$, there is a path C_u from i_u to i_{u+1} such that

$$h\left(\frac{g(i_u, I_u, i_{u+1})}{g(C_u)}\right) \le c_{46}, \quad l(C_u) \le 2, \quad m(C_u) \le m - 1\,. \tag{6.18}$$

For convenience, we write $i_u = i$, $i_{u+1} = j$, $I_u = I$. First assume that there are an edge I' of $\mathcal{G}$ and a subset J' of $\{1, \dots, t\}$ of cardinality n such that $\{l_j : j \in J'\}$ is linearly independent, and

$$i, j \in I', \quad |I \setminus J'| = 1, \quad |I' \setminus J'| = 1, \quad |I' \setminus J| \le m - 1\,.$$

Then the cycle $C_0 = (i, I, j, I', i)$ is J'-admissible and, by (6.11) and (6.12),

$$h(g(i, I, j)/g(i, I', j)) = h(g(C_0)) \le c_{47}\,,$$

which proves (6.18). Now assume that there are no sets I', J' with the properties specified above. Choose p from I with $p \notin J$. Let H be a subset of J of cardinality $n - |I| + 1$ such that if $G := (I \setminus \{p\}) \cup H$, then $\{l_k : k \in G\}$ is linearly independent and has cardinality n. Then by (6.8)

$$l_p = \sum_{k \in G} d_k l_k \quad \text{with } d_k = \begin{cases} -c_{kp}^{(I)} & \text{for } k \in I \setminus \{p\}, \\ d_k = 0 & \text{for } k \notin I \setminus \{p\}. \end{cases} \tag{6.19}$$

Since $|G \cap J| = |(I \setminus \{p\}) \setminus J| = m - 1 \ge 1$, there is a $q \in J$ with $q \notin G$. We can express l_q uniquely as

$$l_q = \sum_{k \in G} e_k l_k \quad \text{with } e_k \in L\,. \tag{6.20}$$

There is a $z \in I \setminus \{p\}$ with $e_z \neq 0$ since $\{l_k : k \in J\}$ is linearly independent. Since $z \in I \setminus \{p\}$ we also have $d_z \neq 0$. From (6.19) it follows that

$$l_z = d_z^{-1} l_p - \sum_{k \in G \setminus \{z\}} (d_k/d_z) l_k \,.$$

By substituting this into (6.20) we get

$$\begin{aligned} l_q &= \sum_{k \in G'} f_k l_k \quad \text{with } G' = G \cup \{p\} \setminus \{z\}\,, \\ f_p &= e_z/d_z, \quad f_k = e_k - f_p d_k \quad \text{for } k \neq p\,. \end{aligned} \tag{6.21}$$

Note that $|G'| = n$ and that $\{l_k : k \in G'\}$ is linearly independent. The sets $I' = \{q\} \cup \{k \in G : e_k \neq 0\}$ and $I'' = \{q\} \cup \{k \in G' : f_k \neq 0\}$ are edges of $\mathcal{G}$. Further,

$$\begin{aligned} |I \setminus G| = 1, \quad |I' \setminus G| = 1, \quad |I' \setminus J| \leq m-1\,, \\ |I \setminus G'| = 1, \quad |I'' \setminus G'| = 1, \quad |I'' \setminus J| \leq m-1\,. \end{aligned}$$

By our assumption, neither I' nor I'' contains both i and j. Assume for instance that $j \notin I'$. Then either $j \neq p$, in which case we have $e_j = 0$, so $j \neq z$, whence $f_j = -f_p d_j \neq 0$, that is $j \in I''$; or $j = p$, in which case $f_j = f_p \neq 0$ and also $j \in I''$. Therefore, $i \notin I''$ and $0 = f_i = e_i - f_p d_i$. But then $e_i \neq 0$ and $i \in I'$. Let $C_u = (i, I', q, I'', j)$. Then in view of $e_i = f_p d_i$, $f_j = -f_p d_j$ (with $d_p := -1$) we have

$$g(C_u) = c_{iq}^{(I')} c_{qj}^{(I'')} = e_i f_j^{-1} = -\frac{f_p d_i}{f_p d_j} = -\frac{d_i}{d_j} = -g(i, I, j)\,.$$

This implies (6.18). The proof of Lemma 14 is now complete. ∎

LEMMA 15. *There are $\varepsilon_1, \dots, \varepsilon_t \in O_T^*$ such that*

$$\sigma(\varepsilon_i) = \varepsilon_{\sigma(i)} \quad \textit{for } i = 1, \dots, t \textit{ and for each } \sigma \in \mathrm{Gal}(L/K)\,, \tag{6.22}$$

$$h\left(\frac{\varepsilon_j}{\varepsilon_i} c_{ij}^{(I)}\right) \leq c_{48} \tag{6.23}$$

for every edge I of $\mathcal{G}$ and for all distinct $i, j \in I$.

P r o o f. We apply Lemma 7. For distinct $i, j \in \{1, \dots, t\}$, let $P(i,j)$ be the collection of *shortest* paths in $\mathcal{G}$ from i to j and set $P(i,j) = \emptyset$ if no path between i and j exists. For a non-isolated vertex i of $\mathcal{G}$, let A_i be the set consisting of all numbers of the form

$$\prod_{j : P(i,j) \neq \emptyset} g(C_{ij})\,,$$

where C_{ij} is any path in $P(i,j)$, and for an isolated vertex i in $\mathcal{G}$ let $A_i = \{1\}$. By (6.5.a), each $\sigma \in \mathrm{Gal}(L/K)$ maps linearly (in)dependent subsets

of $\{l_1, \dots, l_t\}$ onto linearly (in)dependent subsets, hence it maps edges of $\mathcal{G}$ onto edges of $\mathcal{G}$, and

$$\sigma(c_{ij}^{(I)}) = c_{\sigma(i),\sigma(j)}^{\sigma(I)}$$

for each edge I of $\mathcal{G}$ and each distinct $i, j \in I$. This implies that

$$\sigma(A_i) = A_{\sigma(i)} \quad \text{for } i = 1, \dots, t \text{ and for each } \sigma \in \mathrm{Gal}(L/K)\,. \tag{6.24}$$

Further, if i is not isolated then each element α of A_i is the product of numbers of the form $c_{pq}^{(I)}$, and each shortest path between two vertices has length at most r. Hence we have, by (6.9) and (4.2),

$$m_T(\alpha) \le c_{49} \quad \text{for each } \alpha \in A_i \text{ and } i = 1, \dots, t\,. \tag{6.25}$$

Further, by Lemma 14 we have

$$h(\alpha/\beta) \le c_{50} \quad \text{for each } \alpha, \beta \in A_i \text{ and } i = 1, \dots, t\,. \tag{6.26}$$

Each $\sigma \in \mathrm{Gal}(L/K)$ maps connected components of $\mathcal{G}$ onto connected components. Let $\mathcal{C}$ be a $\mathrm{Gal}(L/K)$-orbit of $\{1, \dots, t\}$ as defined in Section 3. The connected components of $\mathcal{G}$ containing an element of $\mathcal{C}$ as vertex have the same cardinality which will be denoted by $n_{\mathcal{C}}$. By Lemma 7, (6.24), (6.25) and (6.26), there are $\varepsilon_1, \dots, \varepsilon_t \in O_T^*$ satisfying (6.22) and

$$h(\varepsilon_i^{-n_{\mathcal{C}}}\alpha) \le c_{51} \quad \text{for each } \alpha \in A_i, i \in \mathcal{C}\,. \tag{6.27}$$

We now prove that these $\varepsilon_1, \dots, \varepsilon_t$ satisfy (6.23). Let I be an edge of $\mathcal{G}$ and $i, j \in I$. Suppose that $i \in \mathcal{C}$, $j \in \mathcal{C}'$ for $\mathrm{Gal}(L/K)$-orbits $\mathcal{C}$, $\mathcal{C}'$. Then $n_{\mathcal{C}}$ and $n_{\mathcal{C}'}$ have the same value, say n'. It is clear that $n' \le t \le r$. Take

$$\alpha_i = \prod_{k:P(i,k)\neq\emptyset} g(C_{ik}) \quad \text{and} \quad \alpha_j = \prod_{k:P(j,k)\neq\emptyset} g(C'_{jk})\,,$$

where C_{ik} is any shortest path from i to k and C'_{jk} any shortest path from j to k. By Lemma 14 and (6.11) we have $k \neq i, j$,

$$h(c_{ij}^{(I)}/g(C_{ij})) \le c_{52}\,,$$

$$h(c_{ij}^{(I)} \cdot g(C'_{ji})) \le c_{52}, \qquad h(c_{ij}^{(I)} \cdot g(C'_{jk}C_{ik}^{-1})) \le c_{52}\,,$$

hence

$$h((c_{ij}^{(I)})^q \cdot \alpha_j/\alpha_i) \le c_{53}, \qquad \text{where } q = n' - 1\,.$$

Together with (6.27) this yields

$$h\left(\frac{\varepsilon_j}{\varepsilon_i}c_{ij}^{(I)}\right) \le \left[h\left(\frac{\varepsilon_i^{-q}\alpha_i}{\varepsilon_j^{-q}\alpha_j}\right) \cdot h\left((c_{ij}^{(I)})^q\frac{\alpha_j}{\alpha_i}\right)\right]^{1/q} \le c_{48}\,.$$

This proves Lemma 15. ∎

In what follows, we put $l'_i = \varepsilon_i l_i$ for $i = 1, \dots, t$, and $c_{ij}^{\prime(I)} = (\varepsilon_j/\varepsilon_i)c_{ij}^{(I)}$. Note that $l'_1, \dots, l'_t$ satisfy (6.5.a) and (6.5.b).

LEMMA 16. *There are a linearly independent set of linear forms* $\{m_1, \ldots, m_n\}$ *with* $m_i \in O_S[X_1, \ldots, X_n]$ *and numbers* $d_{ij} \in L$ *such that*

$$l_i' = \sum_{j=1}^{n} d_{ij} m_j \quad \text{for } i = 1, \ldots, t\,,$$
$$h(d_{ij}) \le c_{54} \quad \text{for } i = 1, \ldots, t \text{ and } j = 1, \ldots, n\,.$$

Proof. Partition $\{1, \ldots, t\}$ into $\mathrm{Gal}(L/K)$-orbits as in Section 3. Assume for the moment that $\{1, \ldots, u\}$ is such an orbit. Define M_1 by $\mathrm{Gal}(L/M_1) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(1) = 1\}$. By [16], Satz 6, M_1 has a $\mathbb{Q}$-basis $\{\omega_1, \ldots, \omega_m\}$ with

$$|\sigma(\omega_i)| \le c_{55}, \quad \omega_i \in O_{M_1} \quad \text{for } i = 1, \ldots, m \text{ and for each } \sigma \in \mathrm{Gal}(L/K)\,. \tag{6.28}$$

We may assume that $\{\omega_1, \ldots, \omega_u\}$ is a K-basis of M_1. Then there are linear forms $n_1, \ldots, n_u \in K[X_1, \ldots, X_n]$ such that

$$l_1' = \sum_{j=1}^{u} \omega_j n_j\,. \tag{6.29}$$

Pick $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i(1) = i$ for $i = 1, \ldots, u$ and put

$$d := (\det(\sigma_i(\omega_j))_{1 \le i,j \le u})^2\,.$$

Then $d \in K^*$ and the linear forms $m_j = d n_j$ $(j = 1, \ldots, u)$ have their coefficients in O_S. Put $\omega_{ij} = d^{-1}\sigma_i(\omega_j)$ for $i, j \in \{1, \ldots, u\}$. Then, by (6.28)

$$l_i' = \sum_{j=1}^{u} \omega_{ij} m_j \quad \text{for } i = 1, \ldots, u\,,$$
$$h(\omega_{ij}) \le c_{56} \quad \text{for } 1 \le i, j \le u\,.$$

By applying this argument to the other $\mathrm{Gal}(L/K)$-orbits we find linear forms $m_1, \ldots, m_t \in O_S[X_1, \ldots, X_n]$ and an invertible matrix $\Omega = (\omega_{ij})$ with entries in L such that

$$l_i' = \sum_{j=1}^{t} \omega_{ij} m_j \quad \text{for } i = 1, \ldots, t \quad \text{and} \quad h(\Omega) \le c_{57}\,. \tag{6.30}$$

We assume that $\{l_1', \ldots, l_n'\}$ and $\{m_1, \ldots, m_n\}$ are linearly independent, which is no restriction. Every linear form l_i' $(i = n+1, \ldots, t)$ can be expressed uniquely as

$$l_i' = \sum_{j=1}^{n} e_{ij} l_j'\,, \tag{6.31}$$

where $E := (e_{ij}) \in L^{t-n,n}$. The sets $I_i = \{i\} \cup \{j : e_{ij} \neq 0\}$ are edges of $\mathcal{G}$, hence, in (6.31), either $e_{ij} = 0$ or $e_{ij} = -c_{ji}^{(I_i)}$ by (6.8). Now Lemma 15 implies that

$$h(E) \leq c_{58}\,.$$

Since $\{m_1, \dots, m_n\}$ is linearly independent there is a matrix $D = (d_{ij}) \in L^{t,n}$ such that

$$l'_i = \sum_{j=1}^{n} d_{ij} m_j \quad \text{for } i = 1, \dots, t\,.$$

We can express the entries of D as rational functions in the entries of Ω and E: first, by expressing $m_1, \dots, m_t$ as linear combinations of $l'_1, \dots, l'_t$, which is possible since Ω is invertible; secondly, by expressing $m_1, \dots, m_n$ as linear combinations of $l'_1, \dots, l'_n$, which can be done by (6.31); thirdly, by expressing $l'_1, \dots, l'_n$ as linear combinations of $m_1, \dots, m_n$; and finally, by expressing $l'_1, \dots, l'_t$ as linear combinations of $m_1, \dots, m_n$, using (6.31). Hence it follows that $h(D) \leq c_{54}$.

Proof of Theorem 2. Let d_{ij} be numbers and $m_1, \dots, m_n$ linear forms with the properties specified in the statement of Lemma 16. Let $B \in O_S^{n,n}$ be the matrix whose ith row consists of the coefficients of m_i and put

$$G(\mathbf{X}) = \prod_{i=1}^{t} \Big(\sum_{j=1}^{n} d_{ij} X_j \Big)\,, \tag{6.32}$$

where $\mathbf{X} = (X_1, \dots, X_n)^T$. From Lemma 16 and the construction of $l'_1, \dots$ $\dots, l'_t$, it follows that there is a $\mu \in K^*$ with

$$\mu F(\mathbf{X}) = G(B\mathbf{X})\,. \tag{6.33}$$

Assume that $\{l'_1, \dots, l'_n\}$ is linearly independent and let $A \in L^{n,n}$ be the matrix whose ith row consists of the coefficients of l'_i. By Lemma 13 we have $|\det A|_T = |\det(l_1, \dots, l_n)|_T \leq c_{37}$. Further, by Lemma 16, there is an invertible matrix $D \in L^{n,n}$ with $A = DB$ and $h(D) \leq c_{59}$. Then, by (4.6), $|\det D^{-1}|_T \leq h(\det D^{-1}) = h(\det D) \leq c_{60}$. Hence

$$|\det B|_S \leq c_{61}\,.$$

By our assumption, the O_S-lattice $\mathfrak{M}$ is equal to either O_S^n or $(\mathbf{e}_1, \dots$ $\dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$ with $h(\alpha) \leq c_{34}$ and $h(\beta) \leq c_{34}$. Put $\mathfrak{a} = (1)$ if $\mathfrak{M} = O_S^n$ and $\mathfrak{a} = (\alpha, \beta)$ otherwise. In the second case we have, by (4.6),

$$|\mathfrak{a}|_S \leq \max(|\alpha|_S, |\beta|_S) \leq \max(h(\alpha), h(\beta)) \leq c_{62}\,;$$

in the first case, this evidently holds. By Lemma 9, there is a matrix $U \in$

$G(n, \mathfrak{a})$ such that the matrix $B' = BU$ satisfies

$$h(B') \le c_{63}\,. \tag{6.34}$$

Note that by (5.1), the matrix U belongs to $G(\mathfrak{M})$. Put

$$F'(\mathbf{X}) = G(B'\mathbf{X})\,;$$

then, by (6.33), $\mu F(U\mathbf{X}) = F'(\mathbf{X})$. Finally, by (6.32), Lemma 16 and (6.34), we have $h(F') \le c_{33}$. This proves (6.1) and hence Theorem 2. ∎

7. Proof of Corollaries. As above, K is an algebraic number field of degree d and S is a finite set of prime ideals of O_K of cardinality s such that the largest of the prime numbers lying below prime ideals of S is equal to P. Let $(\mathfrak{M}, F)$ be an O_S-lattice decomposable form pair such that $\operatorname{rank}\mathfrak{M} = n$, $\deg(F) = r$, F has splitting field L and $D(\mathfrak{M}, F) = \mathfrak{d}$.

Proof of Corollary 1. By Theorem 2, $(\mathfrak{M}, F)$ is weakly equivalent to a pair $(\mathfrak{M}', F')$, where $\mathfrak{M}'$ is a reduced O_S-lattice, and $h(F') \le c_{64}$ with an effectively computable number c_{64} depending only on d, $|D_L|$, s, P, n, r and $|\mathfrak{d}|_S$. Hence it suffices to prove the following lemma.

Lemma 17. *We have $|D_L| \le c_{65}$, where c_{65} is an effectively computable number depending only on d, $|D_K|$, s, P, n, r and $|\mathfrak{d}|_S$.*

Proof. c_{66} and c_{67} will denote effectively computable numbers depending only on the parameters listed in Lemma 17. F can be factored as in (3.1), into linear functions $l_1, \dots, l_t$ satisfying (3.2). Define the fields M_i $(i = 1, \dots, t)$ as in (3.3). Let $\mathcal{C}_1, \dots, \mathcal{C}_u$ be the $\mathrm{Gal}(L/K)$-orbits of $\{1, \dots, t\}$ relative to the $\mathrm{Gal}(L/K)$-action defined in (3.2) and assume that $i \in \mathcal{C}_i$ for $i = 1, \dots, u$. Let $O_{S,i}$ be the integral closure of O_S in M_i, and $\mathfrak{d}_i$ the discriminant of the ring extension $O_{S,i}/O_S$. Then, by Lemma 2,

$$|\mathfrak{d}_1 \dots \mathfrak{d}_u|_S \le |\mathfrak{d}|_S^{n/2} \le c_{66}\,. \tag{7.1}$$

By Lemma 14 of [6], we have

$$|D_{M_i}| \le c_{67}|\mathfrak{d}|_S \quad \text{for } i = 1, \dots, u\,. \tag{7.2}$$

Let $m_i = [M_i : K]$ for $i = 1, \dots, u$. Since L is the composite of $M_1, \dots, M_t$ we have, by a result of Stark ([19], Lemma 7),

$$D_L \Big| \prod_{i=1}^{t} D_{M_i}^{[L:M_i]} = \prod_{i=1}^{u} D_{M_i}^{m_i[L:M_i]} = \Big(\prod_{i=1}^{u} D_{M_i}\Big)^{[L:K]}\,.$$

Together with (7.1), (7.2) and the inequality $[L : K] \le r!$, this proves Lemma 17. ∎

Proof of Corollary 2. We shall frequently use the following facts: (i) for every $C \ge 1$ it is possible to determine effectively a finite set con-

taining all $\alpha \in K$ with $h(\alpha) \le C$ (see e.g. [7]), and (ii) for every O_S-ideal $\mathfrak{a}$ given by a set of generators and every $\alpha \in K$, it is possible to decide whether $\alpha \in \mathfrak{a}$ or not. We remark that by Lemma 11, it can be decided effectively whether a system of linear equations $A\mathbf{x} = \mathbf{b}$ is solvable in $\mathbf{x} \in O_S^n$, and fact (ii) is a special case of this.

By Corollary 1, for given n, r and $\mathfrak{d}$, each weak equivalence class contains an O_S-lattice decomposable form pair $(\mathfrak{M}, F)$ such that $\mathfrak{M}$ is reduced, $\operatorname{rank} \mathfrak{M} = n$, $\deg(F) = r$, $\mathfrak{D}(\mathfrak{M}, F) = \mathfrak{d}$ and $h(F) \le c_{68}$, where c_{68} is an effectively computable number depending only on d, s, P, n, r, $|D_K|$ and $|\mathfrak{d}|_S$. It is possible to determine effectively a finite set containing all pairs $(\mathfrak{M}, F)$ with these properties; what remains is to find an effective method to decide whether any two pairs $(\mathfrak{M}_1, F_1)$, $(\mathfrak{M}_2, F_2)$ in that finite set are weakly equivalent or not.

First we give a procedure to determine effectively whether any two reduced lattices are isomorphic. This is trivial if $\mathfrak{M}_1$ or $\mathfrak{M}_2$ is O_S^n. Hence we may assume that $\mathfrak{M}_1 = (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$, $\mathfrak{M}_2 = (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \gamma\mathbf{e}_n, \delta\mathbf{e}_n)$, where α, β, γ, δ are given elements of O_S with $h(\alpha), h(\beta), h(\gamma), h(\delta) \le c_{69}$ for some effectively computable number c_{69} depending only on d and $|D_K|$. If there is an $a \in K^*$ with $a(\alpha, \beta) = (\gamma, \delta)$ then, by (4.6), $m_S(a) \le c_{70}$ where c_{70} is also an effectively computable number depending only on d and $|D_K|$. By Lemma 6, there is an $\varepsilon \in O_S^*$ with $h(\varepsilon a) \le c_{71}$, where c_{71} is an effectively computable number depending only on d, $|D_K|$, S and P. This implies that there is a $b \in K^*$ with $(b\alpha, b\beta) = (\gamma, \delta)$ and $h(b) \le c_{71}$. Hence in order to decide whether (α, β), (γ, δ) belong to the same ideal class it suffices to check, for each b in some effectively computable finite set, whether the O_S-ideals $(b\alpha, b\beta)$ and (γ, δ) are equal.

So we can restrict ourselves to pairs $(\mathfrak{M}, F)$ where $\mathfrak{M}$ is a fixed, given reduced O_S-lattice, and hence a reduced O_S-sublattice of O_S^n of rank n. Two O_S-lattice decomposable form pairs $(\mathfrak{M}, F_1)$ and $(\mathfrak{M}, F_2)$ are weakly equivalent if and only if there are $\lambda \in K^*$ and a matrix $U \in G(\mathfrak{M})$ such that $F_2(\mathbf{X}) = \lambda F_1(U\mathbf{X})$ (cf. Section 1). For a given matrix $U \in K^{n,n}$ it can be decided whether $U \in G(\mathfrak{M})$ and $F_2(\mathbf{X}) = \lambda F_1(U\mathbf{X})$ for some $\lambda \in K^*$. Therefore, it suffices to prove the following lemma.

LEMMA 18. *Let $\mathfrak{M}$ be a reduced O_S-lattice, and let $F_1(\mathbf{X})$, $F_2(\mathbf{X})$ be two decomposable forms on $K\mathfrak{M}$ of degree r and maximal rank n such that*

$$F_2(\mathbf{X}) = \lambda F_1(U\mathbf{X}) \tag{7.3}$$

for some $\lambda \in K^*$ and $U \in G(\mathfrak{M})$. Then there are $\lambda' \in K^*$ and $U' \in G(\mathfrak{M})$ such that

$$F_2(\mathbf{X}) = \lambda' F_1(U'\mathbf{X}) \quad \text{and} \quad h(U') \le c_{72}\,,$$

where c_{72} is an effectively computable number depending only on d, $|D_K|$, s, P, n, r, $h(F_1)$ and $h(F_2)$.

P r o o f. $c_{73}, \dots, c_{81}$ will denote effectively computable numbers depending only on the parameters specified in Lemma 18. By (7.3), we can express F_1, F_2 as

$$F_1(\mathbf{X}) = \mu \prod_{i=1}^{t} l_i(\mathbf{X})^{k_i}, \quad F_2(\mathbf{X}) = \nu \prod_{i=1}^{t} m_i(\mathbf{X})^{k_i}\,, \tag{7.4}$$

where $\mu, \nu \in K^*$, $k_1, \dots, k_t$ are positive integers, $l_1, \dots, l_t$ are pairwise non-proportional linear forms and $m_1, \dots, m_t$ are pairwise non-proportional linear forms with coefficients in the common splitting field L of F_1 and F_2. Let O_T be the integral closure of O_S in L. We claim that $l_1, \dots, l_t$, $m_1, \dots, m_t$ can be chosen such that

$$\begin{gathered} l_i(\mathbf{X}) \in O_T[X_1, \dots, X_n], \quad m_i(\mathbf{X}) \in O_T[X_1, \dots, X_n]\,, \\ h(l_i) \le c_{73}, \quad h(m_i) \le c_{73} \quad \text{for } i = 1, \dots, t\,; \end{gathered} \tag{7.5.a}$$

$$\lambda_i m_i(\mathbf{X}) = l_i(U\mathbf{X}) \quad (i = 1, \dots, t) \quad \text{for some } \lambda_1, \dots, \lambda_t \in L^*\,; \tag{7.5.b}$$

$$\sigma(l_i) = l_{\sigma(i)}, \quad \sigma(m_i) = m_{\sigma(i)}, \quad k_{\sigma(i)} = k_i \quad \text{for } i = 1, \dots, t,\ \sigma \in \mathrm{Gal}(L/K)\,, \tag{7.5.c}$$

where $(\sigma(1), \dots, \sigma(t))$ is a permutation of $(1, \dots, t)$ for each $\sigma \in \mathrm{Gal}(L/K)$. Namely, choose linear forms $l_1', \dots, l_t'$, $m_1', \dots, m_t'$ satisfying (7.4), (7.5.b), (7.5.c) such that at least one of the coefficients of each of these forms is equal to 1. Construct polynomials $f_1(X)$, $f_2(X)$ from $F_1(\mathbf{X})$ and $F_2(\mathbf{X})$, respectively, by setting $X_1 = X$, $X_2 = X^{r+1}, \dots, X_n = X^{(r+1)^{n-1}}$, where $r = \deg(F_1) = \deg(F_2)$. Then $h(f_1) = h(F_1)$ and $h(f_2) = h(F_2)$. Now the coefficients of $l_1', \dots, l_t'$, $m_1', \dots, m_t'$ are rational functions of the zeros of f_1 and f_2. Hence by (4.7) and (4.5),

$$h(l_i') \le c_{74}, \quad h(m_i') \le c_{74} \quad \text{for } i = 1, \dots, t\,.$$

Choose $a \in O_S \setminus \{0\}$ such that $h(a) \le c_{75}$ and

$$al_i',\ am_i' \in O_T[X_1, \dots, X_n] \quad \text{for } i = 1, \dots, t\,.$$

Then the linear forms $l_i := al_i'$, $m_i := am_i'$ $(i = 1, \dots, t)$ satisfy (7.5.a,b,c).

By (7.5.b,c), (1.5) and (4.6), we have

$$m_T(\lambda_i) \le c_{76}, \quad \sigma(\lambda_i) = \lambda_{\sigma(i)} \quad \text{for } i = 1, \dots, t,\ \sigma \in \mathrm{Gal}(L/K)\,. \tag{7.6}$$

Let $\mathcal{G}$ be the hypergraph with vertices $1, \dots, t$ whose edges are those subsets I of $\{1, \dots, t\}$ for which $\{l_i : i \in I\}$ is linearly dependent and each proper, non-empty subset of $\{l_i : i \in I\}$ is linearly independent. The hypergraph corresponding to $m_1, \dots, m_t$ is exactly the same, by (7.5.b). Let $\mathcal{G}_1, \dots, \mathcal{G}_v$ denote the connected components of $\mathcal{G}$ (two vertices belong to the same

connected component if and only if there is a path connecting them). By (6.8), there are uniquely determined numbers $c_{ij}^{(I)}$, $d_{ij}^{(I)} \in L^*$ such that

$$l_j = -\sum_{i \in I \setminus \{j\}} c_{ij}^{(I)} l_i \quad \text{and} \quad m_j = -\sum_{i \in I \setminus \{j\}} d_{ij}^{(I)} m_i \tag{7.7}$$

for each edge I of $\mathcal{G}$ and each $j \in I$. By (6.10) and (7.5.a) we have

$$h(c_{ij}^{(I)}),\, h(d_{ij}^{(I)}) \le c_{77}\,. \tag{7.8}$$

From (7.5.b) and (7.7) it follows that

$$m_j = -\sum_{i \in I \setminus \{j\}} c_{ij}^{(I)} (\lambda_i/\lambda_j) m_i\,.$$

Hence

$$\lambda_i/\lambda_j = d_{ij}^{(I)}/c_{ij}^{(I)}\,.$$

Together with (7.8) this implies the following: if i, j belong to the same connected component then

$$h(\lambda_i/\lambda_j) \le c_{78}\,. \tag{7.9}$$

We assume that $\{l_1, \dots, l_n\}$ and hence $\{m_1, \dots, m_n\}$ is linearly independent, which is no restriction. Put $\Delta = \det(l_1, \dots, l_n)$. By assumption, $\mathfrak{M} = (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$, and by (2.3) and (4.6), the ideal $\mathfrak{a} = (\alpha, \beta)$ has $|\mathfrak{a}|_S \le c_{79}$. Let h be the cardinality of the unit group of the residue class ring $O_T/\Delta\mathfrak{a}$. Then, by (7.5.a), (4.6) and $|\mathfrak{a}|_S \le c_{79}$, we have

$$h \le c_{80}\,. \tag{7.10}$$

Let $A_j = \{\lambda_i : i \in \mathcal{G}_j\}$ for $j = 1, \dots, v$. Each σ maps linearly (in)dependent linear forms onto linearly (in)dependent linear forms, hence there is a permutation σ^* of $1, \dots, v$ such that $\sigma(\mathcal{G}_j) = \mathcal{G}_{\sigma^*(j)}$ for $j = 1, \dots, v$. Therefore, by (7.6) and (7.5.c), $\sigma(A_j) = A_{\sigma^*(j)}$ for $j = 1, \dots, v$ and $\sigma \in \mathrm{Gal}(L/K)$. Further, (7.9) holds. Hence we can apply Lemma 7 with v instead of t and we infer that there are $\eta_1, \dots, \eta_v \in O_T^*$ such that

$$\sigma(\eta_j) = \eta_{\sigma^*(j)} \quad \text{for } j = 1, \dots, v \text{ and } \sigma \in \mathrm{Gal}(L/K)$$

and

$$h(\eta_j^h \lambda_i) \le c_{81} \quad \text{for } \lambda_i \in A_j\,.$$

We note that in order to use Lemma 7 we must have an estimate $|D_L| \le c_{82}$ where D_L is the discriminant of the splitting field L of F_1 and F_2 over K. However, this can be done by using Example 4 from Section 1, (7.5.a) and Lemma 17.

For each $i \in \{1, \dots, t\}$, put $\varepsilon_i = \eta_j$ if $i \in \mathcal{G}_j$ for $j = 1, \dots, v$. Then

$$\text{(7.11)} \qquad \begin{cases} \varepsilon_i = \varepsilon_k & \text{if } i, k \in \mathcal{G}_j \text{ for some } j \in \{1, \dots, v\}; \\ \sigma(\varepsilon_i) = \varepsilon_{\sigma(i)} & \text{for } i = 1, \dots, t \text{ and for all } \sigma \in \mathrm{Gal}\,(L/K); \\ h(\varepsilon_i^h \lambda_i) \le c_{81} & \text{for } i = 1, \dots, t. \end{cases}$$

We claim that there is a matrix $U'' \in G(n, \mathfrak{a})$ such that

$$\text{(7.12)} \qquad \varepsilon_i^h l_i(\mathbf{X}) = l_i(U''\mathbf{X}) \quad \text{for } i = 1, \dots, t\,.$$

Let $B \in O_T^{n,n}$ be the matrix whose ith row consists of the coefficients of l_i, and $B' \in O_T^{n,n}$ the matrix whose ith row consists of the coefficients of $\varepsilon_i^h l_i$ for $i = 1, \dots, n$. By our choice of h we have $\varepsilon_i^h \equiv 1 \bmod \Delta\mathfrak{a}$, hence $B' \equiv B \bmod \Delta\mathfrak{a}$ (in O_T). Further, $(\det B')/(\det B) = (\varepsilon_1 \dots \varepsilon_n)^h \in O_T^*$. Hence by Lemma 10 with K replaced by L, there is a matrix $U'' \in O_T^{n,n}$ such that $\det U'' \in O_T^*$,

$$\text{(7.13)} \qquad U'' \equiv \begin{pmatrix} \zeta_1 & & 0 \\ & \ddots & \\ 0 & & \zeta_n \end{pmatrix} \bmod \mathfrak{a} \quad \text{with some } \zeta_1, \dots, \zeta_n \in O_T^*$$

and

$$B' = BU''\,.$$

This matrix U'' satisfies (7.12) for $i = 1, \dots, n$. For every $i \in \{n+1, \dots, t\}$ there is a unique subset I_i of $\{1, \dots, n\}$ such that $l_i = \sum_{j \in I_i} c_j l_j$ for certain $c_j \in L^*$. Now $I_i \cup \{i\}$ is an edge of $\mathcal{G}$, hence by (7.11), $\varepsilon_j = \varepsilon_i$ for $j \in I_i$. Therefore,

$$\varepsilon_i^h l_i = \sum_{j \in I_i} c_j (\varepsilon_j^h l_j) \quad \text{for } j = n+1, \dots, t\,.$$

We conclude that (7.12) holds also for $i = n+1, \dots, t$. By (7.11) and (7.5.c) we have

$$\sigma(\varepsilon_i^h l_i) = \varepsilon_{\sigma(i)}^h l_{\sigma(i)} \quad \text{for } i = 1, \dots, t \text{ and for each } \sigma \in \mathrm{Gal}(L/K)\,.$$

Thus the matrix U'' satisfying (7.12) must have its entries in K. Together with (7.13) this implies that $U'' \in G(n, \mathfrak{a})$, whence, by $G(n, \mathfrak{a}) \subseteq G(\mathfrak{M})$, $U'' \in G(\mathfrak{M})$ holds.

Put $\lambda_i' = \varepsilon_i^h \lambda_i$ for $i = 1, \dots, t$. Then, by (7.5.b) and (7.12), there is a matrix $U' \in G(\mathfrak{M})$ such that

$$\lambda_i' m_i(\mathbf{X}) = l_i(U'\mathbf{X}) \quad \text{for } i = 1, \dots, t\,.$$

By (7.11) we have $h(\lambda_i') \le c_{81}$, and by (7.5.a), $h(l_i) \le c_{73}$, and $h(m_i) \le c_{73}$ for $i = 1, \dots, t$. This implies that $h(U') \le c_{72}$. Further, by (7.5.c), (7.6) and (7.11), we get $\prod_{i=1}^t (\lambda_i')^{k_i} \in K^*$. Hence there is a $\lambda' \in K^*$ such that $F_2(\mathbf{X}) = \lambda' F_1(U'\mathbf{X})$, which proves Lemma 18. ∎

Proof of Corollary 3. Immediate consequence of (1.12) and Corollary 1 with $D(\mathfrak{M}, F) = (1)$. ∎

In the proofs of Corollaries 4 and 5, $c_{82}, \ldots, c_{93}$ will denote effectively computable numbers of the form $c'|\mathfrak{d}|_S^{c''}$, where c', c'' depend only on d, $|D_L|$, s, P, n and r.

Proof of Corollary 4. By Theorem 2, $(\mathfrak{M}, F)$ is weakly equivalent to a pair $(\mathfrak{M}', F'')$, where $\mathfrak{M}'$ is a reduced O_S-lattice and $h(F'') \le c_{82}$. Choose $\lambda \in K^*$ and an isomorphism $\varphi : \mathfrak{M} \to \mathfrak{M}'$ such that $\lambda F''(\mathbf{x}) = F(\varphi(\mathbf{x}))$ for $\mathbf{x} \in \mathfrak{M}$. Then $(\lambda) = \mathfrak{c}(\mathfrak{M}, F)\mathfrak{c}(\mathfrak{M}', F'')^{-1}$. By using some arguments from the proof of Lemma 18 one can show that $F''(\mathbf{X})$ has a factorization $F''(\mathbf{X}) = \lambda \prod_{i=1}^{t} l_i(\mathbf{X})^{k_i}$ where the l_i are pairwise non-proportional linear forms with $l_i(\mathbf{X}) \in O_T[X_1, \ldots, X_n]$, $h(l_i) \le c_{83}$ for $i = 1, \ldots, t$ and $h(\lambda) \le c_{84}$. Hence $m_S(\mathfrak{c}(\mathfrak{M}', F'')) \le c_{85}$ and so

$$m_S(\lambda) \le m_S(\mathfrak{c}(\mathfrak{M}, F)) m_S(\mathfrak{c}(\mathfrak{M}', F'')) \le c_{86} m_S(\mathfrak{c}(\mathfrak{M}, F)) .$$

By Lemma 6, we can choose $\varepsilon \in O_S^*$ such that

$$h(\varepsilon^r \lambda) \le c_{87} m_S(\mathfrak{c}(\mathfrak{M}, F)) . \tag{7.14}$$

We note that in Lemma 6, $|D_K|$ was involved, but $|D_K| \le |D_L|$. Put $F' = \varepsilon^r \lambda F''$. Since the mapping $\mathbf{x} \mapsto \varepsilon\varphi(\mathbf{x})$ is an isomorphism $\mathfrak{M} \to \mathfrak{M}'$, the pairs $(\mathfrak{M}, F)$ and $(\mathfrak{M}', F')$ are equivalent. Further, by (7.14) and $\mathfrak{c}(\mathfrak{M}, F) = \mathfrak{c}$,

$$h(F') \le c_{88} m_S(\mathfrak{c}) .$$

This proves the first inequality of Corollary 4. The second one follows by applying Lemma 17. ∎

Proof of Corollary 5. By Corollary 4, there are a reduced O_S-lattice $\mathfrak{M}'$ of rank n and a decomposable form F' on K^n such that $(\mathfrak{M}, F)$ and $(\mathfrak{M}', F')$ are equivalent and $h(F') \le c_{89} m_S(\mathfrak{c})$. This implies

$$h(F'(\mathbf{e}_j)) \le c_{89} m_S(\mathfrak{c}) \quad \text{for } j = 1, \ldots, n . \tag{7.15}$$

Further, by (2.3) we have either (i) $\mathfrak{M}' = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ where $\mathfrak{M}'$ is free, or (ii) $\mathfrak{M}' = (\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$ with $\alpha, \beta \in O_S \setminus \{0\}$ satisfying (2.3). By a well-known argument (see e.g. the proof of Lemma 1 in [2], Ch. II, §1) it follows that there are $u_{21}, \ldots, u_{n1}$ with $F'(\mathbf{e}_1 + u_{21}\mathbf{e}_2 + \ldots + u_{n1}\mathbf{e}_n) \ne 0$ such that $u_{j1} \in \{0, 1, \ldots, r\}$ in case (i) and $u_{j1} \in \{0, \alpha, 2\alpha, \ldots, r\alpha\}$ in case (ii) for $j = 2, \ldots, n$. Put $\mathbf{e}_1' := \mathbf{e}_1 + \sum_{i=2}^{n} u_{i1}\mathbf{e}_i$. We can inductively construct $\mathbf{e}_2', \ldots, \mathbf{e}_n'$ such that $F'(\mathbf{e}_j') \ne 0$ and that

$$\mathbf{e}_j' = u_{1j}\mathbf{e}_1' + \ldots + u_{j-1,j}\mathbf{e}_{j-1}' + \mathbf{e}_j + u_{j+1,j}\mathbf{e}_{j+1} + \ldots + u_{n,j}\mathbf{e}_n$$

with $u_{ij} \in \{0, 1, \ldots, r\}$ in case (i) and $u_{ij} \in \{0, \alpha, 2\alpha, \ldots, r\alpha\}$ in case (ii) for $i = 2, \ldots, n$, $j = 2, \ldots, n$. It is easy to check that $\mathfrak{M}' = (\mathbf{e}_1', \ldots, \mathbf{e}_n')$ in case (i) and $\mathfrak{M}' = (\mathbf{e}_1', \ldots, \mathbf{e}_{n-1}', \alpha\mathbf{e}_n', \beta\mathbf{e}_n')$ in case (ii). Let $V = (v_{ij})$ be the

$n \times n$ matrix defined by $\mathbf{e}'_i = V\mathbf{e}_i$ for $i = 1, \dots, n$ and put $F''(\mathbf{X}) = F'(V\mathbf{X})$. Then $(\mathfrak{M}', F'')$ is equivalent to $(\mathfrak{M}', F')$ and hence to $(\mathfrak{M}, F)$. Further, it is easy to see that $h(V) \le c_{90}$. Hence we get $h(F'') \le c_{91} m_S(\mathfrak{c})$, which implies that

$$h(F''(\mathbf{e}_j)) \le c_{91} m_S(\mathfrak{c}) \quad \text{for } j = 1, \dots, n\,. \tag{7.16}$$

Further, $F''(\mathbf{e}_1) \dots F''(\mathbf{e}_n) = F'(\mathbf{e}'_1) \dots F'(\mathbf{e}'_n) \neq 0$.

There is an O_S-module isomorphism $\varphi : \mathfrak{M}' \to \mathfrak{M}$ such that $F''(\mathbf{x}) = F(\varphi(\mathbf{x}))$ for each $\mathbf{x} \in \mathfrak{M}'$. In case (i) we put $\omega_j = \varphi(\mathbf{e}_j)$ for $j = 1, \dots, n$, while in case (ii) we put $\omega_j = \varphi(\mathbf{e}_j)$ for $j = 1, \dots, n-1$, $\omega_n = \varphi(\alpha\mathbf{e}_n)$, $\omega_{n+1} = \varphi(\beta\mathbf{e}_n) = \gamma\omega_n$ where $\gamma = \beta/\alpha$ and, by (2.3), $h(\gamma) \le c_{92}$ with some effectively computable c_{92} which depends only on d and $|D_K|$. Therefore $\mathfrak{M} = (\omega_1, \dots, \omega_n)$ where either $\mathfrak{M}$ is free and $m = n$, or $\mathfrak{M}$ is not free, $m = n+1$ and $\omega_{n+1} = \gamma\omega_n$ with the above γ, $F(\omega_1) \dots F(\omega_m) \neq 0$, and, by (7.16) and (2.3), we get in both cases

$$h(F(\omega_j)) \le c_{93} \quad \text{for } j = 1, \dots, m\,.$$

This proves the first inequality of (2.4). The second one follows by applying Lemma 17. ∎

Proof of Corollary 6. If there are $\mu \in M^*$ and a subfield M' of M such that $\mu\mathfrak{M} \subseteq M'$, then

$$N_{M/K}(\alpha) = N_{M/K}(\mu)^{-1} N_{M'/K}(\mu\alpha)^{[M:M']} \quad \text{for all } \alpha \in \mathfrak{M}\,.$$

Hence $\mathfrak{D}(\mathfrak{M}, N_{M/K}) = \mathfrak{D}(\mu\mathfrak{M}, N_{M'/K})$. Therefore we may, and shall, assume that there is no $\mu \in M^*$ such that $\mu\mathfrak{M}$ is contained in a proper subfield of M. Note that in this case, the normal closure L of M/K is the splitting field of the restriction of $N_{M/K}$ to $K\mathfrak{M}$.

Next c_{94}, c_{95}, c_{96} will denote effectively computable numbers of the form $c'|\mathfrak{d}|_S^{c''}$ where $\mathfrak{d} = \mathfrak{D}(\mathfrak{M})$ and c', c'' depend only on $d, r = [M : K]$, $|D_L|$, s, P and $n = \operatorname{rank} \mathfrak{M}$. By Theorem 2, there are a reduced O_S-lattice $\mathfrak{M}''$ of rank n, a decomposable form F' on K^n, an isomorphism $\varphi : \mathfrak{M}'' \to \mathfrak{M}$ and $\lambda \in K^*$ such that

$$F'(\mathbf{X}) = \lambda N_{M/K}(\varphi(\mathbf{x})) \quad \text{for all } \mathbf{x} \in \mathfrak{M}'' \text{ and } h(F) \le c_{94}\,. \tag{7.17}$$

φ can be extended uniquely to a K-linear mapping $K^n \to M$. Denote the conjugates of $\alpha \in M$ over K by $\alpha = \alpha^{(1)}, \dots, \alpha^{(r)}$ and define the linear functions $l_j : K^n \to L$ $(j = 1, \dots, r)$ by

$$l_j(\mathbf{x}) = \{\varphi(\mathbf{e}_1)^{-1}\varphi(\mathbf{x})\}^{(j)} \quad \text{for all } \mathbf{x} \in K^n\,.$$

Then, by (7.17),

$$l_1(\mathbf{x}) \dots l_r(\mathbf{x}) = N_{M/K}(\varphi(\mathbf{e}_1))^{-1} N_{M/K}(\varphi(\mathbf{x})) = F'(\mathbf{e}_1)^{-1} F'(\mathbf{x}) =: G(\mathbf{x})\,.$$

Now (7.17) implies that

$$h(G) \le c_{95} \quad \text{with } c_{95} = c_{94}^2 .$$

By a similar argument to the proof of Lemma 18, and using the fact that each l_i is a linear form one of whose coefficients is equal to 1, it follows that

$$h(l_j) \le c_{96} \quad \text{for } j = 1, \dots, r . \tag{7.18}$$

Let $\mathfrak{M}' = \varphi(\mathbf{e}_1)^{-1}\mathfrak{M}$. If $\mathfrak{M}'' = O_S^n$ then take $\omega_i = l_1(\mathbf{e}_i)$ for $i = 1, \dots, n$, and if $\mathfrak{M}'' = (\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \alpha\mathbf{e}_n, \beta\mathbf{e}_n)$ with $\alpha, \beta \in O_S$ satisfying (2.3), then take $\omega_i = l_1(\mathbf{e}_i)$ for $i = 1, \dots, n-1$, $\omega_n = \alpha l_1(\mathbf{e}_n)$ and $\omega_{n+1} = \beta l_1(\mathbf{e}_n) = \gamma\omega_n$ with $\gamma = \beta/\alpha$. Put $m = n$ in the first case and $m = n+1$ in the second case. Then $\mathfrak{M}'$ is similar to $\mathfrak{M}$ and we have $\mathfrak{M}' = (\omega_1, \dots, \omega_n)$. Further, as we have seen in the proof of Lemma 17, $|D_L|$ can be estimated from above in terms of $|D_M|$ and $[M : K]$ only. Hence, by (7.18) and by (2.3) in the second case, we get the first inequality of (2.5). The second one follows by using Lemma 17. ∎

Acknowledgements. We thank the referee for his helpful remarks.

References

[1] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. 25 (1972), 385–394.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, 2nd ed., Academic Press, New York and London 1967.

[3] J. H. Evertse, *Decomposable form equations with a small linear scattering*, to appear.

[4] J. H. Evertse and K. Győry, *Decomposable form equations*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, 1988, 175–202.

[5] —, —, *Thue–Mahler equations with a small number of solutions*, J. Reine Angew. Math. 399 (1989), 60–80.

[6] —, —, *Effective finiteness results for binary forms with given discriminant*, Compositio Math. 79 (1991), 169–204.

[7] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, 1988, 110–174.

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

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

[10] —, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), 583–600.

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

[12] 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.
[13] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York and London 1973.
[14] I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. 72 (1952), 327–340.
[15] S. Lang, *Algebraic Number Theory*, Springer, 1970.
[16] K. Mahler, *Über die Annäherung algebraischer Zahlen durch periodische Algorithmen*, Acta Math. 68 (1937), 109–144.
[17] T. Nagell, *Contributions à la théorie des modules et des anneaux algébriques*, Ark. Mat. 6 (1965), 161–178.
[18] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa 1974.
[19] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
[20] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, D. Van Nostrand Co., Toronto–New York–London 1958.

DEPARTMENT OF MATHEMATICS
AND COMPUTER SCIENCE
UNIVERSITY OF LEIDEN
P.O. BOX 9512
2300 RA LEIDEN, THE NETHERLANDS

MATHEMATICAL INSTITUTE
LAJOS KOSSUTH UNIVERSITY
H-4010 DEBRECEN, HUNGARY

Received on 21.8.1990
and in revised form on 13.3.1991 (2070)