The number of families of solutions of decomposable form equations

by

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

1. Introduction. In [16], Schmidt introduced the notion of family of solutions of norm form equations and showed that there are only finitely many such families. In [18], Voutier gave an explicit upper bound for the number of families. Independently, in [5], Győry extended the notion of family of solutions of norm form equations to decomposable form equations and gave an explicit upper bound for the number of families. In this paper, we obtain a significant improvement of the upper bounds of Voutier and Győry, by applying the results from Evertse [4].

Let \( \beta \) be a non-zero rational integer. Further, let \( M \) denote an algebraic number field of degree \( r \) and \( l(X) = \alpha_1 X_1 + \ldots + \alpha_m X_m \) a linear form with coefficients in \( M \). There is a non-zero \( c \in \mathbb{Q} \) such that the norm form

\[
F(X) = cN_{M/\mathbb{Q}}(l(X)) = c \prod_{i=1}^{r} (\alpha_{1}^{(i)} X_1 + \ldots + \alpha_{m}^{(i)} X_m)
\]

has its coefficients in \( \mathbb{Z} \). Here, we denote by \( \alpha^{(1)}, \ldots, \alpha^{(r)} \) the conjugates of \( \alpha \in M \). We deal among other things with norm form equations of the shape

\[
F(x) = \pm \beta \quad \text{in } x \in \mathbb{Z}^m.
\]

It is more convenient for us to consider the equivalent equation which is also called a norm form equation,

\[
cN_{M/\mathbb{Q}}(x) = \pm \beta \quad \text{in } x \in M,
\]

where \( M \) is the \( \mathbb{Z} \)-module \( \{ x = l(x) : x \in \mathbb{Z}^m \} \) which is contained in \( M \).

In 1971, Schmidt [15] proved his fundamental result that (1.2) has only finitely many solutions if \( M \) satisfies some natural non-degeneracy condition. Later, Schmidt [16] dealt also with the case where \( M \) is degenerate and

Research of the second author was supported in part by Grants 16975 and 16791 from the Hungarian National Foundation for Scientific Research and by the Foundation for Hungarian Higher Education and Research.
showed that in that case, the set of solutions of (1.2) can be divided in a natural way into families, and is the union of finitely many such families.

Below, we give a precise definition of a family of solutions of (1.2); here we mention that it is a coset $xU_{M,J}$ contained in $M$, where $x$ is a solution of (1.2) and $U_{M,J}$ is a particular subgroup of finite index in the unit group of the ring of integers of some subfield $J$ of $M$. Schmidt’s results have been generalised to equations of the type

$$cN_{M/K}(x) \in \beta\mathcal{O}^*_S$$

in $x \in M$, where $K$ is an algebraic number field, $\mathcal{O}_S$ is the ring of $S$-integers in $K$ for some finite set of places $S$, $\mathcal{O}^*_S$ is the unit group of $\mathcal{O}_S$, $c, \beta$ are elements of $K^* = K \setminus \{0\}$, $M$ is a finite extension of $K$, and $M$ is a finitely generated $\mathcal{O}_S$-module contained in $M$. In fact, Schlickewei [13] proved the analogue of Schmidt’s result on families of solutions in the case where $\mathcal{O}_S$ is contained in $\mathbb{Q}$, and Laurent [9] generalised this to arbitrary algebraic number fields $K$. The main tools in the proofs of these results were Schmidt’s subspace theorem and Schlickewei’s generalisation to the $p$-adic case and to number fields.

In [5], Györy generalised the concept of family of solutions to decomposable form equations over $\mathcal{O}_S$, i.e. to equations of the form

$$F(x) \in \beta\mathcal{O}^*_S$$

in $x = (x_1, \ldots, x_m) \in \mathcal{O}^*_S$, where $K, S$ are as above, $\beta$ is a non-zero element of $\mathcal{O}_S$ and $F(X) = F(X_1, \ldots, X_m)$ is a decomposable form with coefficients in $\mathcal{O}_S$, that is, $F$ can be expressed as a product of linear forms in $m$ variables with coefficients in some extension of $K$. We can reformulate (1.4) in a shape similar to (1.3) as follows. According to [1], pp. 77–81, there are finite extension fields $M_1, \ldots, M_t$ of $K$, linear forms $l_j(X) = \alpha_{1j}X_1 + \ldots + \alpha_{mj}X_m$ with coefficients in $M_j$ for $j = 1, \ldots, t$ and $c \in K^*$ such that

$$F(X) = c \prod_{j=1}^t N_{M_j/K}(l_j(X)).$$

Now let

$$A = M_1 \oplus \ldots \oplus M_t$$

be the direct $K$-algebra sum of $M_1, \ldots, M_t$, that is, the cartesian product $M_1 \times \ldots \times M_t$ endowed with coordinatewise addition and multiplication. If we express an element of $A$ as $(\alpha_1, \ldots, \alpha_t)$, then we implicitly assume that $\alpha_j \in M_j$ for $j = 1, \ldots, t$. We define the norm $N_{A/K}(a)$ of $a = (\alpha_1, \ldots, \alpha_t) \in A$ to be the determinant of the $K$-linear map $x \mapsto ax$ from $A$ to itself. This norm is known to be multiplicative. Further, we have

$$N_{A/K}(a) = N_{M_1/K}(\alpha_1) \cdots N_{M_t/K}(\alpha_t)$$
where $N_{M_i/K}$ is the usual field norm. Note that the $\mathcal{O}_S$-module 
\[
\mathcal{M} = \{x = (l_1(x), \ldots, l_t(x)) : x \in \mathcal{O}_S^\times \}
\]
is contained in $A$. Now (1.5) and (1.6) imply that (1.4) is equivalent to 
(1.7) 
\[cN_{A/K}(x) \in \beta \mathcal{O}_S^\times \text{ in } x \in \mathcal{M};\]
(1.7) will also be referred to as a decomposable form equation. In [5], Győry showed that the set of solutions of (1.7) is the union of finitely many families. Further, in [5] he extended some of his results to decomposable form equations over arbitrary finitely generated integral domains over $\mathbb{Z}$.

In [17], Schmidt made a further significant advancement by deriving, as a consequence of his quantitative subspace theorem, an explicit upper bound for the number of solutions of norm form equation (1.2) over $\mathbb{Z}$ for every non-degenerate module $\mathcal{M}$. Schlickewei proved a $p$-adic generalisation of Schmidt's quantitative subspace theorem and used it to derive an explicit upper bound for the number of solutions of $S$-unit equations [14]. Among others, this was used by Győry [5] to obtain an explicit upper bound for the number of families of solutions of decomposable form equation (1.7). Independently, Voutier [18] obtained upper bounds similar to Győry's for the number of families of solutions of norm form equation (1.3), in the special case where $K = \mathbb{Q}$, $\beta = 1$. Recently, Evertse [4] improved the results of Schmidt and Schlickewei just mentioned. In this paper, we apply the results from [4] to obtain an upper bound for the number of families of solutions of (1.7) which is much sharper than Győry's and Voutier's (cf. Theorem 1 in Section 1.2).

In Section 1.1 we introduce the necessary terminology. In Section 1.2 we state our main results (Theorems 1 and 2) and some corollaries. In particular, in Corollary 2 we give an upper bound for the number of $\mathcal{O}_S^\times$-cosets of solutions of (1.7) in the case where that number is finite; here, an $\mathcal{O}_S^\times$-coset is a set $x\mathcal{O}_S^\times = \{\varepsilon x : \varepsilon \in \mathcal{O}_S^\times\}$ where $x$ is a fixed solution of (1.7). Further, in Section 2 we derive from Theorem 1 an asymptotic formula (cf. Corollary 4) for the number of $\mathcal{O}_S^\times$-cosets of solutions of (1.7), whenever this number is infinite. The other sections are devoted to the proofs of Theorems 1 and 2.

1.1. Terminology. Here and in the sequel we use the following notation: the unit group of a ring $R$ with 1 is denoted by $R^\times$ and for $x \in R$ and a subset $H$ of $R$ we define $xH := \{xh : h \in H\}$. Let $K$ be an algebraic number field. Denote by $\mathcal{O}_K$ the ring of integers and by $M_K$ the collection of places (equivalence classes of absolute values) on $K$. Recall that $M_K$ consists of finitely many infinite (i.e. archimedean) places (the number of these being $r_1 + r_2$ where $r_1, r_2$ denote the number of isomorphic embeddings of $K$ into $\mathbb{R}$ and the number of complex conjugate pairs of isomorphic embeddings of $K$ into $\mathbb{C}$, respectively) and of infinitely many finite (non-archimedean) places
which may be identified with the prime ideals of \( \mathcal{O}_K \). For every \( v \in M_K \) we choose an absolute value \( | \cdot |_v \) from \( v \). Now let \( S \) be a finite subset of \( M_K \) containing all infinite places. The ring of \( S \)-integers and its unit group, the group of \( S \)-units, are defined by

\[
\mathcal{O}_S = \{ x \in K : |x|_v \leq 1 \text{ for } v \notin S \}, \quad \mathcal{O}_S^* = \{ x \in K : |x|_v = 1 \text{ for } v \notin S \},
\]

respectively, where \( v \notin S \) means \( v \in M_K \setminus S \). For a finite extension \( J \) of \( K \), we denote by \( \mathcal{O}_{J,S} \) the integral closure of \( \mathcal{O}_S \) in \( J \).

We first introduce families of solutions for norm form equations

\[
(1.3) \quad cN_{M/K}(x) \in \beta \mathcal{O}_S^* \quad \text{in } x \in \mathcal{M},
\]

where, as before, \( M \) is a finite extension of \( K \), \( \mathcal{M} \) is a finitely generated \( \mathcal{O}_S \)-module contained in \( M \) and \( c, \beta \) are elements of \( K^* \). Let \( V := KM \) be the \( K \)-vector space generated by \( \mathcal{M} \). For a subfield \( J \) of \( M \) containing \( K \), define the sets

\[
(1.8) \quad V^J = \{ x \in V : xJ \subseteq V \}, \quad \mathcal{M}^J = V^J \cap \mathcal{M}.
\]

As is easily seen, we have \( \lambda x \in V^J \) for \( x \in V^J \), \( \lambda \in J \). Further, define the subgroup of the unit group of \( \mathcal{O}_{J,S} \),

\[
(1.9) \quad \mathcal{U}_{J,M} := \{ \varepsilon \in \mathcal{O}_{J,S}^* : \varepsilon \mathcal{M}^J = \mathcal{M}^J \}.
\]

For instance from Lemma 9 of [5] it follows that \( \mathcal{U}_{J,M} \) has finite index in \( \mathcal{O}_{J,S}^* \). Note that \( N_{M/K}(\varepsilon) \in \mathcal{O}_S^* \) for \( \varepsilon \in \mathcal{U}_{J,M} \). Hence if \( x \in \mathcal{M}^J \) is a solution of (1.3) then so is every element of the coset \( x\mathcal{U}_{J,M} \). Such a coset is called a family of solutions (or rather an \((J,M)\)-family of solutions) of (1.3). Laurent [9] proved the generalisation of Schmidt’s result that the set of solutions of (1.3) is the union of at most finitely many families.

Now let \( A = M_1 \oplus \ldots \oplus M_t \) be the direct \( K \)-algebra sum of finite extension fields \( M_1, \ldots, M_t \) of \( K \). Note that \( A \) has unit element \( 1_A = (1, \ldots, 1) \) (\( t \) times) where \( 1 \) is the unit element of \( K \) and that the unit group of \( A \) is \( A^* = \{ (\xi_1, \ldots, \xi_t) \in A : \xi_1 \ldots \xi_t \neq 0 \} \). For each \( K \)-subalgebra \( B \) of \( A \), denote by \( \mathcal{O}_{B,S} \) the integral closure of \( \mathcal{O}_S \) in \( B \). Thus,

\[
\mathcal{O}_{A,S} = \mathcal{O}_{M_1,S} \oplus \ldots \oplus \mathcal{O}_{M_t,S}
\]

is the direct sum of the integral closures of \( \mathcal{O}_S \) in \( M_1, \ldots, M_t \), respectively, and

\[
\mathcal{O}_{B,S} = \mathcal{O}_{A,S} \cap B
\]

for each \( K \)-subalgebra \( B \) of \( A \). From these facts and (1.6) it follows easily that for \( b \in \mathcal{O}_{A,S} \) we have \( N_{A/K}(b) \in \mathcal{O}_S \) and that for \( b \) in the unit group \( \mathcal{O}_{A,S}^* \) we have \( N_{A/K}(b) \in \mathcal{O}_S^* \).

Let \( c, \beta \in K^* \), let \( \mathcal{M} \) be a finitely generated \( \mathcal{O}_S \)-module contained in \( A \), and consider the equation

\[
(1.7) \quad cN_{A/K}(x) \in \beta \mathcal{O}_S^* \quad \text{in } x \in \mathcal{M}.
\]
Families of solutions of (1.7) are defined in precisely the same way as for (1.3), but now the role of the subfields \( J \) of \( M \) in (1.3) is played by the \( K \)-subalgebras \( B \) of \( A \) that contain the unit element \( 1_A \) of \( A \). Thus, let \( V := KM \) be the \( K \)-vector space, contained in \( A \), generated by \( M \) and for each \( K \)-subalgebra \( B \) of \( A \) with \( 1_A \in B \) define the sets
\[
(1.10) \quad V^B := \{ x \in V : xB \subseteq V \}, \quad \mathcal{M}^B := V^B \cap \mathcal{M}
\]
and the subgroup of the unit group of \( \mathcal{O}_{B,S} \),
\[
(1.11) \quad \mathcal{U}_{\mathcal{M},B} := \{ \varepsilon \in \mathcal{O}_{B,S}^\ast : \varepsilon \mathcal{M}^B = \mathcal{M}^B \}
\]
which is known to have finite index \([\mathcal{O}_{B,S}^\ast : \mathcal{U}_{\mathcal{M},B}]\) in \( \mathcal{O}_{B,S}^\ast \) (cf. [5], Lemma 9). Clearly, \( V^B \) is closed under multiplication by elements of \( B \) (and in fact the largest subspace of \( V \) with this property). An \((\mathcal{M}, B)\)-family of solutions of (1.7) is a coset \( x\mathcal{U}_{\mathcal{M},B} \), where \( B \) is a \( K \)-subalgebra of \( A \) containing \( 1_A \) and \( x \in \mathcal{M}^B \) is a solution of (1.7); since \( N_{A/K}(\varepsilon) \in \mathcal{O}_S^\ast \) for \( \varepsilon \in \mathcal{U}_{\mathcal{M},B} \), every element of \( x\mathcal{U}_{\mathcal{M},B} \) is a solution of (1.7). If \( A = M \) is a finite extension field of \( K \) this notion of family of solutions coincides with that for norm form equation (1.3), since then the \( K \)-subalgebras of \( A \) containing \( 1_A \) are precisely the subfields of \( M \) containing \( K \). In [5], Győry proved among other things that the set of solutions of (1.7) is the union of finitely many families.

1.2. Results. Below, we first recall Győry’s result on the number of families of solutions of (1.7) and then state our improvement. As before, let \( K \) be an algebraic number field, \( S \) a finite set of places on \( K \) containing all infinite places, \( A = M_1 \oplus \ldots \oplus M_t \) where \( M_1, \ldots, M_t \) are finite extensions of \( K \), and \( \mathcal{M} \) a finitely generated (not necessarily free) \( \mathcal{O}_S \)-submodule of \( A \). Let \( a_i = (\alpha_{i1}, \ldots, \alpha_{it}) \) \((i = 1, \ldots, m)\) be a set of generators of \( \mathcal{M} \). Thus,

\[
\mathcal{M} = \{ x = (l_1(x), \ldots, l_t(x)) : x \in \mathcal{O}_S^m \}
\]

where \( l_j(x) = \alpha_{1j}x_1 + \ldots + \alpha_{mj}x_m \) for \( j = 1, \ldots, t \), and by (1.6) we have \( N_{A/K}(x) = \prod_{j=1}^t N_{M_j/K}(l_j(x)) \). We call \( d \) a denominator of \( \mathcal{M} \) if \( d \in K^\ast \) and if the polynomial \( d \prod_{j=1}^t N_{M_j/K}(l_j(x)) \) has its coefficients in \( \mathcal{O}_S \). This notion of denominator is easily shown to be independent of the choice of the generators \( a_1, \ldots, a_m \).

We consider equation (1.7), and impose the following conditions on \( S, A, \mathcal{M}, \beta \) and \( c \):

\[
(1.12) \quad \begin{cases} S \text{ has cardinality } s, \\ A \text{ has dimension } \sum_{i=1}^t [M_i : K] = r \geq 2 \text{ as a } K \text{-vector space,} \\ \text{the } K \text{-vector space } V := KM \text{ has dimension } n \geq 2, \\ \beta \in \mathcal{O}_S \setminus \{0\}, \quad c \text{ is a denominator of } \mathcal{M}. \end{cases}
\]

For every finite place \( v \) on \( K \), let \( \operatorname{ord}_v(\cdot) \) denote the discrete valuation corresponding to \( v \) with value group \( \mathbb{Z} \); recall that \( | \cdot |_v = C_v^{-\operatorname{ord}_v(\cdot)} \) for some
$C_v > 1$. For $\beta \in K^*$, let $\omega_S(\beta)$ denote the number of $v \not\in S$ with $\text{ord}_v(\beta) \neq 0$ and put

$$\psi_1(\beta) := \left( \begin{array}{c} r \\ n-1 \end{array} \right) \omega_S(\beta) \prod_{\nu \in S} \binom{\text{ord}_\nu(\beta) + n}{n}.$$  

Further, let $D$ be the degree over $\mathbb{Q}$ of the normal closure of the composite $M_1 \ldots M_t$ over $\mathbb{Q}$; thus, $[K : \mathbb{Q}] \leq D \leq (r[K : \mathbb{Q}])!$. Győry [5] proved that the set of solutions of (1.7) is contained in some finite union of cosets of unit groups

$$(1.13)\quad x_1\mathcal{O}_{B_1,S}^* \cup \ldots \cup x_w\mathcal{O}_{B_w,S}^* \quad \text{with} \quad w \leq (48D)^{237n^D} \psi_1(\beta),$$

where for $i = 1, \ldots, w$, $B_i$ is a $K$-subalgebra of $A$ with $1_A \in B_i$, $x_i \in A^*$ with $x_iB_i \subset V$, and where the set of solutions of (1.7) contained in $x_i\mathcal{O}_{B_i,S}^*$ is the union of at most $[\mathcal{O}_{B_i,S}^* : \mathcal{U}_{A.B_i}]$ $(\mathcal{M}, B_i)$-families of solutions. This implies an upper bound for the number of families of solutions of (1.7) which depends on $n, r, \beta, s$ and the indices $[\mathcal{O}_{B_i,S}^* : \mathcal{U}_{A.B_i}]$ (cf. [5], Theorem 3), so ultimately on the module $\mathcal{M}$. We mention that Voutier [18], Chap. V independently obtained a result similar to (1.13) but only for norm form equation (1.3) and with $K = \mathbb{Q}$, $\beta = 1$.

Győry’s result can be improved as follows. A $K$-subalgebra $B$ of $A$ is said to be $S$-minimal if $1_A \in B$, and if for each proper $K$-subalgebra $B'$ of $B$ with $1_A \in B'$, the quotient group $\mathcal{O}_{B,S}^*/\mathcal{O}_{B',S}^*$ is infinite. A family of solutions of (1.7) is said to be reducible if it is the union of finitely many strictly smaller families of solutions, and irreducible otherwise. Put

$$(1.14)\quad \psi_2(\beta) := \left( \begin{array}{c} r \\ n-1 \end{array} \right) \omega_S(\beta) \prod_{\nu \in S} \binom{\text{ord}_\nu(\beta) + n - 1}{n - 1},$$

$$e(n) := \frac{1}{3} n(n+1)(2n+1) - 2.$$  

THEOREM 1. Assume (1.12). The set of solutions of

$$(1.7)\quad cN_{A/K}(x) \in \beta\mathcal{O}_S^* \quad \text{in} \quad x \in \mathcal{M}$$

can be expressed as a finite union of irreducible families of solutions. More precisely, the set of solutions of (1.7) is contained in some finite union of cosets

$$(1.15)\quad x_1\mathcal{O}_{B_1,S}^* \cup \ldots \cup x_w\mathcal{O}_{B_w,S}^* \quad \text{with} \quad w \leq (2^{33}r^2)^{e(n)\psi_2(\beta)}$$

such that for $i = 1, \ldots, w$, $B_i$ is an $S$-minimal $K$-subalgebra of $A$, $x_i \in A^*$ with $x_iB_i \subset V$, and the set of solutions of (1.7) contained in $x_i\mathcal{O}_{B_i,S}^*$ is the union of at most $[\mathcal{O}_{B_i,S}^* : \mathcal{U}_{A.B_i}]$ $(\mathcal{M}, B_i)$-families of solutions which are all irreducible.
Remark 1. The right-hand side of Győry’s bound (1.13) depends doubly exponentially on $n$ and in the worst case when $D = (r[K : \mathbb{Q}])!$ triply exponentially on $r$, whereas our bound (1.15) depends only polynomially on $r$ and exponentially on $n^3$. (1.13) can be better than (1.15) in terms of $r$ only if $D$ is very small compared with $r$, e.g. if $A = \mathbb{Q}^r$ for some large $r$. It is likely that, in (1.15), $2^{33}$ can be improved upon, and that $e(n)$ can be replaced by a linear expression of $n$.

For some very special type of norm form equation, Voutier succeeded in deriving an upper bound for the number of families of solutions independent of the module $\mathcal{M}$ (see the remark after Corollary 1). It is an open problem whether an explicit bound independent of $\mathcal{M}$ exists in full generality, for equations (1.3) or (1.7) (1).

Remark 2. We can express the set of solutions of (1.7) as a minimal finite union of irreducible families, that is, as a union $\mathcal{F}_1 \cup \ldots \cup \mathcal{F}_g$ where $\mathcal{F}_1, \ldots, \mathcal{F}_g$ are irreducible families of solutions, none of which is contained in the union of the others. We claim that any other irreducible family of solutions of (1.7) is contained in one of $\mathcal{F}_1, \ldots, \mathcal{F}_g$. In other words, $\mathcal{F}_1, \ldots, \mathcal{F}_g$ are the maximal irreducible families of solutions of (1.7). Hence Theorem 1 above gives automatically an upper bound for the number of maximal irreducible families. To prove our claim, let $\mathcal{G}$ be an arbitrary irreducible family of solutions of (1.7). Then $\mathcal{G}$ is the union of the sets $\mathcal{G} \cap \mathcal{F}_i$ for $i = 1, \ldots, g$ and by Lemma 3 in Section 2, each of these sets is a union of finitely many families. Then one of these families, contained in $\mathcal{F}_1$, say, is equal to $\mathcal{G}$. Hence $\mathcal{G} \subseteq \mathcal{F}_1$.

Remark 3. There is only one way to express the set of solutions of (1.7) as a minimal union of irreducible families, since the families appearing in such a union are the maximal irreducible families of solutions of (1.7).

We also investigate the problem to give an upper bound for the number of $K$-subalgebras $B$ of $A$ for which (1.7) has $(\mathcal{M}, B)$-families of solutions. Let again $V = K\mathcal{M}$. Suppose again that $\dim_K A = r$ and $\dim_K V = n$. If $x$ is a solution in $\mathcal{M}^B$, then $x \in V^B \cap A^*$, where $A^*$ is the unit group of $A$. Hence (1.7) can have $(\mathcal{M}, B)$-families of solutions only for those $K$-subalgebras $B$ of $A$ for which

$$1_A \in B, \quad V^B \cap A^* \neq \emptyset.$$ (1.16)

In [5], Győry proved that the number of algebras $B$ with (1.16) is at most $n^r$. We can improve this as follows:

(1) Added in proof: W. M. Schmidt and P. Voutier have recently proved that, in general, an upper bound for the number of families of solutions of (1.3) or (1.7) must depend on the module $\mathcal{M}$ (see also footnote (2)).
Theorem 2. The number of $K$-subalgebras $B$ of $A$ with (1.16) is at most $(n \max(r - n, 2))^n$.

We do not know whether the dependence on $r$ is necessary.

We derive some corollaries from Theorem 1. First we specialise Theorem 1 to norm form equation (1.3). Let $K, S$ be as above so that in particular $S$ has cardinality $s$. Further, let $M$ be a finite extension of $K$ of degree $r \geq 2$, $\mathcal{M}$ a finitely generated $\mathcal{O}_S$-submodule of $M$ such that the $K$-vector space $K\mathcal{M}$ has dimension $n \geq 2$, and $c, \beta$ constants such that $\beta \in \mathcal{O}_S \setminus \{0\}$ and $c$ is a denominator of $\mathcal{M}$. Then, by applying Theorem 1 with $A = \mathcal{M}$, we get at once the following result which improves upon the corresponding results in [5] and [18]:

Corollary 1. The set of solutions of
\[ cN_{M/K}(x) \in \beta\mathcal{O}^*_S \quad \text{in } x \in \mathcal{M} \]
can be expressed as a finite union of irreducible families of solutions. More precisely, the set of solutions of (1.3) is contained in some finite union of cosets
\[ x_1\mathcal{O}^*_{J_1,S} \cup \ldots \cup x_w\mathcal{O}^*_{J_w,S} \quad \text{with } w \leq (2^{33}r^2)^{e(n)s}\psi_2(\beta) \]
such that for $i = 1, \ldots, w$, $J_i$ is a subfield of $M$ containing $K$, $x_i \in M^*$ is such that $x_i J_i \subset V$, and the set of solutions of (1.3) in $x_i\mathcal{O}^*_{J_i,S}$ is the union of at most $[\mathcal{O}^*_{J_i,S} : \mathcal{U}_{\mathcal{M},J_i}] (\mathcal{M}, J_i)$-families of solutions which are all irreducible.

As mentioned before, for a very special type of norm form equation Voutier ([18], Theorem V.3) obtained an upper bound for the number of families independent of $M$: namely, he proved that if $M$ is a $\mathbb{Z}$-module of rank 3 contained in the ring of integers of an algebraic number field $M$ of degree $r > \text{rank } \mathcal{M} = 3$, then the set of solutions of the equation
\[ N_{M/Q}(x) = 1 \quad \text{in } x \in \mathcal{M} \]
is the union of at most $r^{28n}r^2$ families $(^2)$.

We return to equation (1.7). In what follows, we consider $K$ as a $K$-subalgebra of $A$ by identifying $\alpha \in K$ with $\alpha \cdot 1_A$. The set of solutions of (1.7) can be divided into $\mathcal{O}^*_S$-cosets $x\mathcal{O}^*_S$. Györy [5], Corollary 2, gave an explicit upper bound for the number of $\mathcal{O}^*_S$-cosets of solutions of (1.7) in the case where this number is finite. We can improve this as follows:

Corollary 2. Assume (1.12). Suppose that (1.7) has only finitely many $\mathcal{O}^*_S$-cosets of solutions. Then this number is at most $(2^{33}r^2)^{e(n)s}\psi_2(\beta)$.

$(^2)$ Added in proof: W. M. Schmidt and P. Voutier have recently constructed a class of ternary cubic norm form equations $N_{M/Q}(x) = 1$ in which there are equations with arbitrarily many families of solutions.
For $\beta = 1$, this gives the Corollary to Theorem 1 of [4].

**Proof.** Let $B$ be one of the $S$-minimal $K$-subalgebras of $A$ occurring in (1.15). We may assume that (1.7) has an $(\mathcal{M}, B)$-family of solutions, $x\mathcal{U}_{\mathcal{M}, B}$, say. By identifying $\varepsilon \in \mathcal{O}_S^*$ with $\varepsilon \cdot 1_A$, we may view $\mathcal{O}_S^*$ as a subgroup of $\mathcal{U}_{\mathcal{M}, B}$. Let $w \leq \infty$ be the index of $\mathcal{O}_S^*$ in $\mathcal{U}_{\mathcal{M}, B}$. Then $x\mathcal{U}_{\mathcal{M}, B}$ is the union of precisely $w$ $\mathcal{O}_S^*$-cosets. So our assumption implies that $w$ is finite. Therefore, $[\mathcal{O}_{B, S}^*: \mathcal{O}_S]$ is finite. Now since $B$ is $S$-minimal, it follows that $B = K$. So each algebra $B_i$ occurring in (1.15) is equal to $K$, i.e. $\mathcal{O}_{B_i, S}^* = \mathcal{O}_S^*$, and Corollary 2 follows.

In general, it is as yet not effectively decidable whether (1.7) has only finitely many $\mathcal{O}_S^*$-cosets of solutions. Schmidt [17], Theorem 3, derived an explicit upper bound for the number of solutions of norm form equations over $\mathbb{Z}$ satisfying an effectively decidable non-degeneracy condition. It is possible to give a similar effective non-degeneracy condition for (1.7) as well, which implies that for every $\beta \in \mathcal{O}_S \setminus \{0\}$, the number of $\mathcal{O}_S^*$-cosets of solutions is finite. Moreover, under that condition we can derive an upper bound for the number of $\mathcal{O}_S^*$-cosets of solutions with a better dependence on $\beta$ in that unlike the bound in Corollary 2, it does not depend on the quantities $\text{ord}_v(\beta)$ ($v \in M_K \setminus S$) appearing in $\psi_2(\beta)$.

The vector space $V = K\mathcal{M}$ is said to be non-degenerate if $V^B \cap A^* = \emptyset$ for every $K$-subalgebra $B$ of $A$ with $1_A \in B$, $B \neq K$, where $A^*$ is the unit group of $A$. (1.16) implies that in that case, each algebra $B_i$ occurring in (1.15) is equal to $K$. Hence the set of solutions of (1.7) is the union of finitely many $\mathcal{O}_S^*$-cosets.

**Corollary 3.** Assume (1.12) and in addition that $V = K\mathcal{M}$ is non-degenerate. Then the set of solutions of (1.7) is the union of at most $(2^{33}r^2)^{n}(n + \omega_S(\beta))$ $\mathcal{O}_S^*$-cosets.

**Proof.** We apply Theorem 1 with $S' := S \cup \{v \notin S : \text{ord}_v(\beta) > 0\}$ replacing $S$. Thus, $\beta \in \mathcal{O}_S^*$. We have to replace $s$ by the cardinality of $S'$ which is $s' := s + \omega_S(\beta)$. Moreover, in the definition of $\psi_2(\beta)$, $S$ has to be replaced by $S'$, which means that $\psi_2(\beta)$ has to be replaced by $1$. Let $\mathcal{M}'$ be the $\mathcal{O}_{S'}$-module generated by $\mathcal{M}$. Thus, every solution of (1.7) satisfies

$$(1.7') \quad cN_{A/K}(x) \in \mathcal{O}_S^*, \quad x \in \mathcal{M'}.$$  

Clearly, $c$ is a denominator of $\mathcal{M}'$. Moreover, since $V$ is non-degenerate, the set of solutions of (1.7') is the union of finitely many $\mathcal{O}_S^*$-cosets. So by Corollary 2, the set of solutions of (1.7'), and hence also the set of solutions of (1.7), is contained in the union of at most $(2^{33}r^2)^{n}n' \mathcal{O}_S^*$-cosets. Now if any two solutions $x_1, x_2$ of (1.7) belong to the same $\mathcal{O}_S^*$-coset then they belong to the same $\mathcal{O}_S^*$-coset: for if $x_2 = \varepsilon x_1$ with $\varepsilon \in \mathcal{O}_S^*$, then $\varepsilon' = cN_{A/K}(x_2)/cN_{A/K}(x_1) \in \mathcal{O}_S^*$, hence $\varepsilon \in \mathcal{O}_S^*$. This proves Corollary 3.
2. An asymptotic formula. In this section, we state and prove an asymptotic density result for the collection of \( O_{K^*} \)-cosets of solutions of equation (1.7), in the case where the number of these is infinite. This asymptotic density result is a consequence of (the qualitative part of) Theorem 1.

We recall the definition of absolute (multiplicative) Weil height. Let \( \overline{Q} \) denote the algebraic closure of \( Q \). Let \( x = (x_1, \ldots, x_n) \in \overline{Q}^n \setminus \{0\} \). Take any algebraic number field \( L \) containing \( x_1, \ldots, x_n \), and let \( \sigma_1, \ldots, \sigma_d \) be the isomorphic embeddings of \( L \) into \( \overline{Q} \), where \( d = [L : Q] \). Further, let \( (x_1, \ldots, x_n) \) denote the fractional ideal with respect to the ring of integers of \( L \), generated by \( x_1, \ldots, x_n \), and denote by \( N_{L/Q}((x_1, \ldots, x_n)) \) its norm. Then the absolute Weil height of \( x \) is defined by

\[
H(x) = H(x_1, \ldots, x_n) := \left\{ \prod_{i=1}^d \max(\{ |\sigma_i(x_1)|, \ldots, |\sigma_i(x_n)| \}) \right\}^{1/d}.
\]

It is clear that \( H(x) \) does not depend on the choice of \( L \). Further,\nn\[
(2.1) \quad H(\lambda x) = H(x) \quad \text{for } x \in \overline{Q}^n \setminus \{0\}, \ \lambda \in \overline{Q}^*.
\]

Now let \( K \) be an algebraic number field and \( A = M_1 \oplus \ldots \oplus M_t \), where \( M_1, \ldots, M_t \) are finite extension fields of \( K \). We define the height \( \overline{H}(x) \) of \( x = (\xi_1, \ldots, \xi_t) \in A \) to be the absolute Weil height of the vector with coordinates consisting of \( \xi_1, \ldots, \xi_t \) and their conjugates over \( K \), that is, if \( \tau_{i,1}, \ldots, \tau_{i,r_i} \) with \( r_i = [M_i : K] \) are the \( K \)-isomorphic embeddings of \( M_i \) into \( \overline{Q} \) then we put\n
\[
\overline{H}(x) := H(\tau_{1,1}(\xi_1), \ldots, \tau_{1,r_1}(\xi_1), \ldots, \tau_{t,1}(\xi_t), \ldots, \tau_{t,r_t}(\xi_t)).
\]

Note that by (2.1) we have\n
\[
(2.2) \quad \overline{H}(x) = \overline{H}(\lambda x) \quad \text{for } x \in A \setminus \{0\}, \ \lambda \in K^*,
\]

i.e. \( \overline{H} \) may be viewed as a height on the collection \( (A \setminus \{0\})/K^* \) of \( K^* \)-cosets \( xK^* \) (\( x \in A \setminus \{0\} \)). This height satisfies\n
\[
(2.3) \quad \# \{ x \in (A \setminus \{0\})/K^* : \overline{H}(x) \leq X \} < \infty \quad \text{for } X > 0.
\]

Namely, by Northcott’s theorem [10], [11] we know that for every \( d > 0 \), \( X > 0 \), there are, up to multiplication by elements from \( \overline{Q}^* \), only finitely many \( x = (\xi_1, \ldots, \xi_n) \in \overline{Q}^n \setminus \{0\} \) with \( H(x) \leq X \) and \( \left[ Q(\xi_1) : Q \right] \leq d \) for \( i = 1, \ldots, n \). This implies that the set of non-zero elements \( x \) of \( A \) with \( \overline{H}(x) \leq X \) can be divided into finitely many classes, where \( x = (\xi_1, \ldots, \xi_n), \ y = (\eta_1, \ldots, \eta_n) \in A \) are said to belong to the same class if \( (\tau_{1,1}(\xi_1), \ldots, \tau_{t,r_t}(\xi_t)) = \alpha (\tau_{1,1}(\eta_1), \ldots, \tau_{t,r_t}(\eta_t)) \) for some \( \alpha \in \overline{Q}^* \). But clearly, if for instance \( \xi_1 \neq 0 \), then \( \alpha = \tau_{1,1}(\eta_1/\xi_1) = \ldots = \tau_{t,r_t}(\eta_t/\xi_1) \), which implies that \( \alpha \in K \). So if \( x, y \in A \setminus \{0\} \) belong to the same class then they belong to the same \( K^* \)-coset.
Decomposable form equations

For a finitely generated abelian group \( \Lambda \), denote by \( \Lambda_{\text{tors}} \) the torsion subgroup of \( \Lambda \) and by rank \( \Lambda \) the rank of the free abelian group \( \Lambda/\Lambda_{\text{tors}} \). Let as usual \( S \) be a finite set of places on \( K \) which contains all infinite places. For a \( K \)-subalgebra \( B \) of \( A \) containing the unit element \( 1_A \) of \( A \) we put
\[
\varrho_{B,S} := \text{rank} \frac{O_{B,S}^*}{O_S^*},
\]
where we view \( O_{B,S}^* \) as a subgroup of \( O_{B,S}^* \) by identifying \( \varepsilon \in O_S^* \) with \( \varepsilon \cdot 1_A \). By a straightforward generalisation of Dirichlet’s unit theorem, \( O_{B,S}^* \) is finitely generated, hence \( \varrho_{B,S} \) is finite.

Let again \( \beta, c \in K^* \), and let \( M \) be a finitely generated \( O_S \)-submodule of \( A \) such that condition (1.12) holds. For every \( X > 0 \) we consider the set of solutions of
\[
(2.4) \quad cN_{A/K}(x) \in \beta O_S^* \quad \text{in} \quad x \in M \quad \text{with} \quad \overline{H}(x) \leq X.
\]
From (2.2) and \( O_S^* \subset K^* \) it follows that the set of solutions of (2.4) can be divided into \( O_S^* \)-cosets \( xO_S^* \). Denote by \( N(X) \) the maximal number of distinct \( O_S^* \)-cosets contained in the set of solutions of (2.4). From (2.3) it follows that \( N(X) \) is finite: namely, if \( x, y \) are solutions of (2.4) with \( y = \varepsilon x \) for some \( \varepsilon \in K^* \), then \( \varepsilon^r = N_{A/K}(y)/N_{A/K}(x) \in O_S^* \), so \( x, y \) belong to the same \( O_S^* \)-coset.

For norm form equations over \( \mathbb{Q} \), asymptotic formulas for \( N(X) \) were derived by Győry and Pethő [6] (in the archimedean case) and Pethő [12] (for an arbitrary finite set of places \( S \)); Győry and Pethő [7] and Everest [2] obtained more precise results in certain special cases. From (the qualitative part of) Theorem 1 we derive the following generalisation of Pethő’s result [12]:

**Corollary 4.** We have
\[
N(X) = \gamma(\log X)^\varrho + O((\log X)^{\varrho - 1}) \quad \text{as} \quad X \to \infty,
\]
where \( \gamma \) is a positive number independent of \( X \) and where \( \varrho \) is the maximum of the numbers \( \varrho_{B,S} \), taken over all \( K \)-subalgebras \( B \) of \( A \) with \( 1_A \in B \) for which the equation \( cN_{A/K}(x) \in \beta O_S^* \) in \( x \in M \) has \( (M,B) \)-families of solutions.

We mention that for \( O_S = \mathbb{Z} \), Everest and Győry [3] recently obtained some refinements for equations of the form (1.4).

**Remark 4.** \( \gamma, \varrho \) and the constant in the error term are all ineffective. By (1.16), we can estimate \( \varrho \) from above by the effectively computable number \( \varrho_0 \), which is the maximum of the numbers \( \varrho_{B,S} \), taken over all \( K \)-subalgebras \( B \) of \( A \) with \( 1_A \in B \), \( V^B \cap A^* \neq \emptyset \). Further, using the explicit bound in Theorem 1, one can effectively compute an upper bound for \( \gamma \); we shall not work this out.
To derive Corollary 4 we need some lemmas. The first lemma is undoubt-
edly well-known but we could not find a proof of it in the literature.

**Lemma 1.** Let $\Lambda$ be a finitely generated additive abelian group of rank $\varrho$, and let $f$ be a function from $\Lambda$ to $\mathbb{R}$ with the following properties:

\begin{align*}
(2.5) & \quad f(x) \geq 0 \quad \text{for } x \in \Lambda; \\
(2.6) & \quad f(x + y) \leq f(x) + f(y) \quad \text{for } x, y \in \Lambda; \\
(2.7) & \quad f(\lambda x) = \lambda f(x) \quad \text{for } x \in \Lambda, \lambda \in \mathbb{Z}_{\geq 0}; \\
(2.8) & \quad \text{for every } Y > 0, \text{ the set } \{x \in \Lambda : f(x) \leq Y\} \text{ is finite.}
\end{align*}

Then

\begin{align*}
(2.9) & \quad \# \{x \in \Lambda : f(x) \leq Y\} = \gamma Y^\varrho + O(Y^{\varrho-1}) \quad \text{as } Y \to \infty
\end{align*}

where $\gamma = \gamma(\Lambda, f)$ is a positive constant.

**Proof.** We first assume that $\Lambda = \mathbb{Z}^\varrho$. For $x = (\xi_1, \ldots, \xi_\varrho) \in \mathbb{R}^\varrho$ we define the maximum norm $\|x\| := \max(|\xi_1|, \ldots, |\xi_\varrho|)$. Letting $e_i = (0, \ldots, 1, \ldots, 0)$ $(i = 1, \ldots, \varrho)$ denote the vector in $\mathbb{Z}^\varrho$ with a single 1 on the $i$th place, we infer from (2.5)–(2.7) that for $x = (\xi_1, \ldots, \xi_\varrho), y = (\eta_1, \ldots, \eta_\varrho) \in \mathbb{Z}^\varrho$ we have

$$|f(x) - f(y)| \leq \max(f(x - y), f(y - x)) \leq \sum_{i=1}^{\varrho} |\xi_i - \eta_i| \max(f(e_i), f(-e_i)),$$

whence

$$|f(x) - f(y)| \leq C\|x - y\|,$$

where $C := \sum_{i=1}^{\varrho} \max(f(e_i), f(-e_i))$.

We extend $f$ to a function on $\mathbb{Q}^\varrho$ by putting $f(x) := \lambda^{-1} f(\lambda x)$ for $x \in \mathbb{Q}^\varrho$ where $\lambda$ is the smallest positive integer such that $\lambda x \in \mathbb{Z}^\varrho$. This extended $f$ satisfies again (2.5)–(2.7) and (2.10), but now for all $x, y \in \mathbb{Q}^\varrho$ and $\lambda \in \mathbb{Q}_{\geq 0}$. Using (2.10) and taking limits we can extend $f$ to a continuous function $f : \mathbb{R}^\varrho \to \mathbb{R}$ which satisfies (2.5)–(2.7) and (2.10) for all $x, y \in \mathbb{R}^\varrho$ and $\lambda \in \mathbb{R}_{\geq 0}$.

For $Y > 0$ we define the set $C_Y := \{x \in \mathbb{R}^\varrho : f(x) \leq Y\}$. Since $f$ is continuous, this set is Lebesgue measurable. By (2.7) we have $C_Y = \{Y x : x \in C_1\}$. Hence $C_Y$ has Lebesgue measure $\gamma Y^\varrho$, where $\gamma$ is the Lebesgue measure of $C_1$. We can cover $\mathbb{R}^\varrho$ by the unit cubes $U_z := \{x \in \mathbb{R}^\varrho : \|x - z\| \leq 1/2 \} \ (z \in \mathbb{Z}^\varrho)$. These cubes have Lebesgue measure 1, and any two different cubes have at most part of their boundary in common. (2.7) and (2.10) imply that

$$C_{Y - C/2} \subseteq \bigcup_{z \in \mathbb{Z}^\varrho \atop f(z) \leq Y} U_z \subseteq C_{Y + C/2} \quad \text{for } Y \geq C/2.$$
Now let \( n(Y) \) be the number of \( z \in \mathbb{Z}^g \) with \( f(z) \leq Y \). By comparing Lebesgue measures, we get
\[
(2.11) \quad \gamma(Y - C/2)^g \leq n(Y) \leq \gamma(Y + C/2)^g \quad \text{for } Y \geq C/2.
\]
From (2.8) it follows that \( n(Y) \) is finite; hence \( \gamma \) is finite. Moreover, for \( Y \) sufficiently large, \( n(Y) > 0 \), hence \( \gamma > 0 \). Now (2.9) follows at once from (2.11). This settles the case \( A = \mathbb{Z}^g \).

Now let \( A \) be an arbitrary additive abelian group. There are \( u_1, \ldots, u_g \in A \), such that every \( x \in A \) can be expressed uniquely as
\[
x = t + \zeta_1 u_1 + \ldots + \zeta_g u_g \quad \text{with } t \in A_{\text{tors}}, \quad z = (\zeta_1, \ldots, \zeta_g) \in \mathbb{Z}^g.
\]
Put \( f'(z) := f(\zeta_1 u_1 + \ldots + \zeta_g u_g). \) (2.6) implies that \( f'(z) - f(-t) \leq f(x) \leq f'(z) + f(t) \). Further, (2.7) with \( \lambda = 0 \) implies that \( f(0) = 0 \). More generally, (2.7) implies that \( f(t) = 0 \) for \( t \in A_{\text{tors}} \) since for such \( t \) there is a positive integer \( \lambda \) with \( \lambda t = 0 \). Hence \( f(x) = f'(z) \) for \( x \in A \). Clearly, \( f' \) and \( \mathbb{Z}^g \) satisfy (2.5)–(2.8). So by what we proved above we have
\[
\# \{ z \in \mathbb{Z}^g : f'(z) \leq Y \} = \gamma Y^g + O(Y^{g-1}) \quad \text{as } Y \to \infty
\]
with some positive \( \gamma' \). From this, one deduces easily that (2.9) holds with \( \gamma = \gamma' \cdot \# A_{\text{tors}} \). This completes the proof of Lemma 1. \( \blacksquare \)

For a subset \( F \) of \( A \) with the property that for each \( x \in F \) the coset \( xO_S \) is contained in \( F \), we denote by \( N_F(X) \) the maximal number of distinct \( O_S \)-cosets \( xO_S \) with \( x \in F \) and \( H(x) \leq X \).

**Lemma 2.** Let \( F = x\mathcal{M}_B \) be a family of solutions of (1.7), where \( B \) is a \( K \)-subalgebra of \( A \) containing \( 1_A \) and \( x \in \mathcal{M}_B \). Then for some positive real \( \gamma \) depending only on \( \mathcal{M} \) and \( B \) we have
\[
(2.12) \quad N_F(X) = \gamma (\log X)^{g_B,s} + O((\log X)^{g_B,s-1}) \quad \text{as } X \to \infty.
\]

**Proof.** We use the following properties of the absolute Weil height which are straightforward consequences of its definition:
\[
(2.13) \quad \begin{cases} H(x) \geq 1 & \text{for } x \notin \mathbb{Q}^n \setminus \{0\}, \\ H(x_1y_1, \ldots, x ny_n) \leq H(x_1, \ldots, x_n) H(y_1, \ldots, y_n) & \text{for } x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{Q}, \\ H(x_1^\lambda, \ldots, x_n^\lambda) = H(x_1, \ldots, x_n)^\lambda & \text{for } x_1, \ldots, x_n \in \mathbb{Q}, \lambda \in \mathbb{Z}_{\geq 0}. 
\end{cases}
\]
Let \( \mathcal{U} := \mathcal{M}_B \) and \( g_0 := g_B,s \). Since \( \mathcal{U} \) has finite index in \( \mathcal{O}_B,S \), the factor group \( \mathcal{U}/\mathcal{O}_S \) has rank \( g_0 \). We apply Lemma 1 to \( A = \mathcal{U}/\mathcal{O}_S \) and \( f = \log H \). By (2.2), \( f \) is well-defined on \( A \). Further, (2.13) implies (2.5)–(2.7), and (2.8) follows from (2.3) and the fact that \( \mathcal{U}/\mathcal{O}_S = \mathcal{U}/(K^* \cap \mathcal{U}) \) may be viewed as a subgroup of \( A^*/K^* \). It follows that
\[
(2.14) \quad N_{\mathcal{U}}(X) = \gamma (\log X)^{g_0} + O((\log X)^{g_0-1}) \quad \text{as } X \to \infty
\]
for some positive constant $\gamma$. By (2.13) we have $c_1 \overline{H}(xu) \leq \overline{H}(u) \leq c_2 \overline{H}(xu)$ for $u \in \mathcal{U}$, where $c_1 = \overline{H}(x)^{-1}$ and $c_2 = \overline{H}(x^{-1})$, and this implies that $N_{\mathcal{U}}(c_2^{-1}X) \leq N_{x\mathcal{U}}(X) \leq N_{\mathcal{U}}(c_1^{-1}X)$. Now Lemma 2 follows from (2.14) and the fact that both $(\log(c_1^{-1}X))^{\varepsilon_0}$ and $(\log(c_2^{-1}X))^{\varepsilon_0}$ differ from $(\log X)^{\varepsilon_0}$ by at most $O((\log X)^{\varepsilon_0 - 1})$. ■

**Lemma 3.** For any two $K$-subalgebras $B_1$, $B_2$ of $A$ containing $1_A$, the intersection of an $(M, B_1)$-family and an $(M, B_2)$-family is the union of at most finitely many $(M, B_1 \cap B_2)$-families.

**Proof.** Let $\mathcal{G}_i = x_i \mathcal{U}_{M,B_i}$ with $x_i \in M^{B_i}$ for $i = 1, 2$ be the two families of solutions and put $B := B_1 \cap B_2$. Let $x_0 \in \mathcal{G}_1 \cap \mathcal{G}_2$. Then $x_0 \in M^{B_1} \cap M^{B_2}$. From definition (1.10) it follows easily that $M_i \subseteq M^B$ for $i = 1, 2$, whence $x_0 \in M^B$. Further, we have $\mathcal{G}_i = x_0 \mathcal{U}_{M,B_i}$ for $i = 1, 2$, hence $\mathcal{G}_1 \cap \mathcal{G}_2 = x_0(\mathcal{U}_{M,B_1} \cap \mathcal{U}_{M,B_2})$. We claim that $\mathcal{U}_{M,B}$ is a subgroup of finite index in $\mathcal{U}_{M,B_1} \cap \mathcal{U}_{M,B_2}$; then it follows at once that $\mathcal{G}_1 \cap \mathcal{G}_2$ is the union of finitely many families $y \mathcal{U}_{M,B}$ with $y \in M^B$. To prove the claim, let $\varepsilon \in \mathcal{U}_{M,B}$ and take $i \in \{1, 2\}$. Then $\varepsilon \in B \subseteq B_i$, whence by (1.10), $\varepsilon M_i \subseteq V^{B_i}$, where $V = KM$. Further, by (1.11) we have $\varepsilon M_i \subseteq \varepsilon M^B = M^B \subseteq M$. Therefore, by (1.10), $\varepsilon M_i \subseteq M_i$. Similarly, we find $\varepsilon M_i \subseteq M_i$. Hence $\varepsilon M_i = M_i$, i.e., $\varepsilon \in \mathcal{U}_{M,B_i}$ for $i = 1, 2$. So $\mathcal{U}_{M,B} \subseteq \mathcal{U}_{M,B_1} \cap \mathcal{U}_{M,B_2}$. Now our claim follows from the fact that both groups have finite index in $\mathcal{O}_{B,S} = \mathcal{O}_{B_1,S} \cap \mathcal{O}_{B_2,S}$. ■

**Proof of Corollary 4.** By Theorem 1, the set of solutions of (1.7) can be expressed as

$$\mathcal{F}_1 \cup \ldots \cup \mathcal{F}_p$$

where for each $i$, $\mathcal{F}_i$ is an $(M, B_i)$-family of solutions of (1.7) for some $K$-subalgebra $B_i$ of $A$ containing $1_A$. For a tuple $I = \{i_1 < \ldots < i_p\}$ of integers from $\{1, \ldots, p\}$, let $B_I := B_{i_1} \cap \ldots \cap B_{i_p}$, $\mathcal{F}_I := \mathcal{F}_{i_1} \cap \ldots \cap \mathcal{F}_{i_p}$, and let $N_I(X)$ be the number of cosets $x \mathcal{O}_S$ with $x \in \mathcal{F}_I$ and $\overline{H}(x) \leq X$. Put $\gamma_1 := \max\{q_{B_i,S} : i = 1, \ldots, p\}$. Thus, $q_{B_i,S} \leq \gamma_1$ for each tuple $I$ as above. Lemma 3 implies that for each $I$, $\mathcal{F}_I$ is the union of finitely many $(M, B_i)$-families. So by Lemma 2 we have

$$N_I(X) = \gamma_1 (\log X)^{\varepsilon_1} + O((\log X)^{\varepsilon_1 - 1}) \quad \text{as } X \to \infty$$

where $\gamma_1 = 0$ if $q_{B_i,S} < \varepsilon_1$. Note that $\gamma_1 > 0$ for at least one $i \in \{1, \ldots, p\}$. Now by (2.15) and the rule of inclusion and exclusion we have

$$N(X) = \sum_{i=1}^p N_i(X) - \sum_{I \neq I_1} N_I(X) + \sum_{I \neq I_2} N_I(X) - \ldots,$$

hence

$$N(X) = \gamma (\log X)^{\varepsilon_1} + O((\log X)^{\varepsilon_1 - 1}) \quad \text{as } X \to \infty$$
where
\[ \gamma = \sum_{i=1}^{p} \gamma_i - \sum_{i \neq 1} \gamma_i + \sum_{i=1} \gamma_i - \ldots \]

Since \( N(X) \geq N_i(X) \) for \( i = 1, \ldots, p \) we have \( \gamma \geq \gamma_i \) for \( i = 1, \ldots, p \), hence \( \gamma > 0 \). Lemma 2 implies that (1.7) does not have any family of solutions \( x \mu_{\mathcal{M},B} \) with \( \varrho_{B,S} > \varrho_1 \); therefore, \( \varrho_1 = \varrho \). This completes the proof of Corollary 4.

3. Reduction to \( \mathcal{O}_{A,S}^* \)-cosets. Let \( K \) be an algebraic number field, and let \( S, M_1, \ldots, M_t, A = M_1 \oplus \ldots \oplus M_t, \mathcal{M} \) be as in Section 1.2. Further, let \( s = \#S, r = \dim_K A \geq 2, n = \dim_K K, \mathcal{M} \geq 2, c, \beta \) be as in (1.12). For \( x \in A \), we define the coset \( x \mathcal{O}_{A,S}^* = \{ \varepsilon x : \varepsilon \in \mathcal{O}_{A,S}^* \} \). In this section we prove Lemma 4 below which is in fact an improvement of Lemma 5 of [5].

**Lemma 4.** The set of solutions of
\[
(1.7) \quad cN_{A/K}(x) \in \beta \mathcal{O}_S^* \quad \text{in} \quad x \in \mathcal{M}
\]
is contained in some union \( x_1 \mathcal{O}_{A,S}^* \cup \ldots \cup x_t \mathcal{O}_{A,S}^* \) where \( t_1 \leq \psi_2(\beta) \) and where for \( j = 1, \ldots, t_1, x_j \in \mathcal{M} \) is a solution of (1.7).

We prove this by slightly refining some arguments of Schmidt [17]. In the proof of Lemma 4 we need some further lemmas. We first recall some lemmas from [17]. Let \( E \) be a field endowed with a non-archimedean additive valuation \( V \) (i.e. \( V(xy) = V(x) + V(y), V(x+y) \geq \min(V(x),V(y)) \) for \( x, y \in E, V(0) = \infty \), and there is an \( x \in E \) with \( V(x) \neq 0, V(x) \neq \infty \)). For \( z = (z_1, \ldots, z_n) \in E^n, \) put \( V(z) = \min(V(z_1), \ldots, V(z_n)) \). Further, let \( L_1, \ldots, L_r \) be \( r \geq n \) linear forms in \( n \) variables with coefficients in \( E \).

**Lemma 5.** Let \( z \in E^n \) with \( z \neq 0 \). There is a subset \( S \) of \( \{1, \ldots, r\} \) of cardinality \( n-1 \) such that every \( z' \in E^n \) with
\[ V(z') \geq V(z), \quad V(L_i(z')) \geq V(L_i(z)) \quad \text{for} \quad i \in S \]

satisfies
\[ V(L_i(z')) \geq V(L_i(z)) \quad \text{for} \quad i = 1, \ldots, r. \]

**Proof.** This is precisely Lemma 13 of [17], except that that lemma has the additional condition \( V(z) = 0 \). Suppose that \( V(z) \neq 0 \). Let \( \lambda \in E \) be such that \( V(\lambda) = V(z) \) and put \( z_1 := \lambda^{-1}z \). Then \( V(z_1) = 0 \). Now Lemma 5 follows at once from Lemma 13 of [17] applied to \( z_1 \), on observing that \( V(L_i(z_1)) = V(L_i(z)) - V(\lambda) \) for \( i = 1, \ldots, r \).

We call the subset \( S \) related to \( z \) as in Lemma 5 an anchor for \( z \).
Lemma 6. Let \(d_1, \ldots, d_r\) be positive rational numbers, \(\gamma\) a real and \(S\) a subset of \(\{1, \ldots, r\}\) of cardinality \(n - 1\). Put

\[
T(S) := \left\{ z \in E^n : \sum_{i=1}^{r} d_i V(L_i(z)) = \gamma, \ S \text{ is an anchor for } z \right\}.
\]

Then for any \(z_1, z_2 \in T(S)\) with \(V(L_i(z_1)) = V(L_i(z_2))\) for \(i \in S\) we have \(V(L_i(z_1)) = V(L_i(z_2))\) for \(i = 1, \ldots, r\).

Proof. Let \(z_1, z_2 \in T(S)\) with \(V(L_i(z_1)) = V(L_i(z_2))\) for \(i \in S\). We may assume without loss of generality that \(V(z_2) \geq V(z_1)\). Then by Lemma 5 we have \(V(L_i(z_2)) \geq V(L_i(z_1))\) for \(i = 1, \ldots, r\). Together with \(\sum_{i=1}^{r} d_i V(L_i(z_j)) = \gamma\) for \(j = 1, 2\) this implies that \(V(L_i(z_2)) = V(L_i(z_1))\) for \(i = 1, \ldots, r\). \(\blacksquare\)

As before, if we express an element of \(A\) as a \(t\)-tuple \((\xi_1, \ldots, \xi_t)\), say, then it is implicitly assumed that \(\xi_i \in M_i\) for \(i = 1, \ldots, t\). Fix \(v \in M_K \setminus S\). For \(i = 1, \ldots, t\), let \(w_{i1}, \ldots, w_{i g_i}\) denote the places on \(M_i\) which lie above \(v\), and denote by \(e_{ij}, f_{ij}\) the ramification index and residue class degree, respectively, of \(w_{ij}\) over \(v\). Let \(\overline{K}\) denote the algebraic closure of \(K\). Choose a continuation of \(\text{ord}_v\) to \(\overline{K}\) and denote this also by \(\text{ord}_v\); then \(\text{ord}_v\) assumes its values in \(\mathbb{Q}\). For \(i = 1, \ldots, t\) let \(E_i\) denote the collection of \(K\)-isomorphic embeddings of \(M_i\) into \(\overline{K}\); then \(E_i\) can be expressed as a disjoint union,

\[
E_i = E_{i1} \cup \ldots \cup E_{i g_i}, \quad \text{with } \#E_{ij} = e_{ij} f_{ij} \text{ for } j = 1, \ldots, g_i
\]

such that for \(j = 1, \ldots, g_i\),

\[
(3.1) \quad \text{ord}_{w_{ij}}(\alpha) = e_{ij} \text{ord}_{v}(\sigma(\alpha)) \quad \text{for } \alpha \in M_i, \ \sigma \in E_{ij}.
\]

Lemma 7. There are integers \(c_{ij}\) \((i = 1, \ldots, t, \ j = 1, \ldots, g_i)\) and \(u_v\) with \(u_v \leq \text{ord}_v(\beta)\) such that for every solution \(x = (\xi_1, \ldots, \xi_t) \in M\) of (1.7) we have

\[
(3.2) \quad \text{ord}_{w_{ij}}(\xi_i) - c_{ij} \geq 0 \quad \text{for } i = 1, \ldots, t, \ j = 1, \ldots, g_i,
\]

\[
(3.3) \quad \sum_{i=1}^{t} \sum_{j=1}^{g_i} f_{ij} \{\text{ord}_{w_{ij}}(\xi_i) - c_{ij}\} = u_v.
\]

Proof. Let \(\{a_k = (\alpha_{k1}, \ldots, \alpha_{kt}) : k = 1, \ldots, m\}\) be a set of generators of \(M\) as an \(\mathcal{O}_S\)-module. Define the integers

\[
(3.4) \quad c_{ij} = \min \{\text{ord}_{w_{ij}}(\alpha_{ki}) : k = 1, \ldots, m\} \quad \text{for } i = 1, \ldots, t, \ j = 1, \ldots, g_i.
\]

Let \(x = (\xi_1, \ldots, \xi_t) \in M\) be a solution of (1.7). Then \(x = \sum_{k=1}^{m} \beta_k a_k\) for certain \(\beta_1, \ldots, \beta_m \in \mathcal{O}_S\). Since the place \(w_{ij}\) lies above \(v \in M_K \setminus S\), we have \(\text{ord}_{w_{ij}}(\beta_k) \geq 0\) for \(i = 1, \ldots, t, \ j = 1, \ldots, g_i\). Together with \(\xi_i = \sum_{k=1}^{m} \beta_k \alpha_{ki}\) for \(i = 1, \ldots, t\) and (3.4), this implies \(\text{ord}_{w_{ij}}(\xi_{ij}) \geq c_{ij}\) for \(i = 1, \ldots, t, \ j = 1, \ldots, g_i\). This proves (3.2).
We now prove (3.3) for some $u_v$. By assumption, $c$ is a denominator for $\mathcal{M}$, i.e.
\[
c \prod_{i=1}^{t} N_{M_i/K}(\alpha_{i1}X_1 + \ldots + \alpha_{im}X_m) \in \mathcal{O}_S[X_1, \ldots, X_m].
\]
Since $x = (\xi_1, \ldots, \xi_t)$ is a solution of (1.7) we have $c \prod_{i=1}^{t} N_{M_i/K}(\xi_i) \in \beta\mathcal{O}_S^n$, so
\[
F(X) = \beta \prod_{i=1}^{t} N_{M_i/K}\left(\sum_{k=1}^{m} \frac{\alpha_{ki}X_k}{\xi_i}\right) \in \mathcal{O}_S[X_1, \ldots, X_m].
\]
For a polynomial $P(X) \in \overline{K}[X_1, \ldots, X_m]$ denote by $\text{ord}_v(P)$ the minimum of the numbers $\text{ord}_v(\alpha)$ for all coefficients $\alpha$ of $P$. By Gauss' lemma (cf. [8], p. 55, Prop. 2.1) we have $\text{ord}_v(PQ) = \text{ord}_v(P) + \text{ord}_v(Q)$ for $P, Q \in \overline{K}[X_1, \ldots, X_m]$. By applying this to (3.5) we obtain
\[
0 \leq \text{ord}_v(F) = \text{ord}_v(\beta) + \sum_{i=1}^{t} \sum_{\sigma \in \mathcal{E}_i} \min_{1 \leq k \leq m} \text{ord}_v(\sigma(\alpha_{ki}/\xi_i))
\]
\[
= \text{ord}_v(\beta) + \sum_{i=1}^{t} \sum_{j=1}^{g_i} \sum_{\sigma \in \mathcal{E}_{ij}} \min_{1 \leq k \leq m} \text{ord}_v(\sigma(\alpha_{ki}/\xi_i))
\]
\[
= \text{ord}_v(\beta) + \sum_{i=1}^{t} \sum_{j=1}^{g_i} f_{ij} \min_{1 \leq k \leq m} \text{ord}_{w_{ij}}(\alpha_{ki}/\xi_i) \quad \text{by (3.1)}
\]
\[
= \text{ord}_v(\beta) + \sum_{i=1}^{t} \sum_{j=1}^{g_i} f_{ij} \{c_{ij} - \text{ord}_{w_{ij}}(\xi_i)\} \quad \text{by (3.4)}.
\]
This implies (3.3) with $u_v = \text{ord}_v(\beta) - \text{ord}_v(F)$.  

**Lemma 8.** If $x = (\xi_1, \ldots, \xi_t)$ runs through the set of solutions of (1.7), then the tuple $\psi_v(x) := (\text{ord}_{w_{ij}}(\xi_i) : i = 1, \ldots, t, j = 1, \ldots, g_i)$ runs through a set of cardinality at most $(\frac{r}{n-1})^{(\text{ord}_v(\beta)+n-1)}$.

**Proof.** Let
\[
\mathcal{O}_\psi := \{y \in K : \text{ord}_\psi(y) \geq 0\}, \quad \mathcal{M}_\psi := \mathcal{M}\mathcal{O}_\psi
\]
be the local ring at $v$, and the localisation of $\mathcal{M}$ at $v$, respectively. We note that $\mathcal{O}_\psi \subset \mathcal{O}_\psi$ and $\mathcal{M} \subset \mathcal{M}_\psi$. Since $\mathcal{O}_\psi$ is a principal ideal domain, the $\mathcal{O}_\psi$-module $\mathcal{M}_\psi$ is free of rank $n = \dim_K \mathcal{M}$. Let $\{a_k = (\alpha_{k1}, \ldots, \alpha_{kn}) : k = 1, \ldots, n\}$ be an $\mathcal{O}_\psi$-basis of $\mathcal{M}_\psi$. Further, let $x = (\xi_1, \ldots, \xi_t) \in \mathcal{M}$ be a solution of (1.7). Then $x = z_1a_1 + \ldots + z_na_n$ for some vector $z = (z_1, \ldots, z_n) \in \mathcal{O}_\psi^n$ which is uniquely determined by $x$. For each $i \in \{1, \ldots, t\}$ and each $\sigma \in \mathcal{E}_i$ (the collection of $K$-isomorphic embeddings of $M_i$ into $\overline{K}$)
define the linear form $L_{i\sigma}(z) := \sigma(\alpha_{i1})z_1 + \ldots + \sigma(\alpha_{in})z_n$. Thus
\begin{equation}
\sigma(\xi_i) = L_{i\sigma}(z) \quad \text{for } i = 1, \ldots, t, \sigma \in \mathcal{E}_i.
\end{equation}

Recall that $\sum_{i=1}^t |M_i : K| = r$. Let $L_1, \ldots, L_r$ be the linear forms $L_{i\sigma}$ ($i = 1, \ldots, t$, $\sigma \in \mathcal{E}_i$) in some order. For $i = 1, \ldots, t$, $j = 1, \ldots, g_i$, let
\[ F_{ij} = \{ k \in \{1, \ldots, r\} : L_k = L_{i\sigma} \text{ for some } \sigma \in \mathcal{E}_{ij} \}, \]
where the set $\mathcal{E}_{ij}$ is defined by (3.1). Then by (3.1) and (3.6),
\begin{equation}
\text{ord}_{w_{ij}}(\xi_i) = e_{ij} \text{ord}_{w}(\sigma(\xi_i)) = e_{ij} \text{ord}_{w}(L_k(z))
\end{equation}
for $i = 1, \ldots, t$, $j = 1, \ldots, g_i$, $k \in F_{ij}$.

We apply Lemma 6 with $E = K$ and $V = \text{ord}_v$. Let $\mathcal{S}_x \subset \{1, \ldots, r\}$ be an anchor for $z$ in the sense of Lemma 5. Then $\mathcal{S}_x$ has cardinality $n - 1$, and the tuple $(\text{ord}_v(L_k(z)) : k = 1, \ldots, r)$ is uniquely determined by $\mathcal{S}_x$ and the $(n - 1)$-tuple $(\text{ord}_v(L_k(z)) : k \in \mathcal{S}_x)$. Let
\[ \mathcal{S}_x' = \{ (i, j) : 1 \leq i \leq t, 1 \leq j \leq g_i, F_{ij} \cap \mathcal{S}_x \neq \emptyset \}. \]

Now (3.7) implies that once $\mathcal{S}_x$ is given, the tuple $(\text{ord}_{w_{ij}}(\xi_i) : (i, j) \in \mathcal{S}_x')$ determines uniquely $\text{ord}_v(L_k(z)) : k \in \mathcal{S}_x$, the latter determines uniquely $(\text{ord}_v(L_k(z)) : k = 1, \ldots, r)$ and this last tuple determines uniquely $(\text{ord}_{w_{ij}}(\xi_i) : i = 1, \ldots, t, j = 1, \ldots, g_i) = \psi_v(x)$, again by (3.7). We conclude that $\psi_v(x)$ is determined uniquely by $\mathcal{S}_x$ and the tuple $(\text{ord}_{w_{ij}}(\xi_i) : (i, j) \in \mathcal{S}_x')$.

By Lemma 7 there are integers $c_{ij}$ ($i = 1, \ldots, t$, $j = 1, \ldots, g_i$) such that $\text{ord}_{w_{ij}}(\xi_i) - c_{ij} \geq 0$ for $(i, j) \in \mathcal{S}_x'$ and
\begin{equation}
\sum_{(i, j) \in \mathcal{S}_x'} \{ \text{ord}_{w_{ij}}(\xi_i) - c_{ij} \} \leq \sum_{i=1}^t \sum_{j=1}^{g_i} f_{ij} \{ \text{ord}_{w_{ij}}(\xi_i) - c_{ij} \} \leq \text{ord}_v(\beta).
\end{equation}

The set $\mathcal{S}_x'$ has cardinality $\leq n - 1$, since $\mathcal{S}_x$ has cardinality $n - 1$ and the sets $F_{ij}$ are pairwise disjoint. Given the set $\mathcal{S}_x$, (3.8) implies that for the tuple $(\text{ord}_{w_{ij}}(\xi_i) : (i, j) \in \mathcal{S}_x')$ we have at most $\left( \frac{\text{ord}_v(\beta)}{\mathcal{S}_x'} \right) \leq \left( \frac{\text{ord}_v(\beta) + n - 1}{\mathcal{S}_x'} \right)$ possibilities. Moreover, as $\mathcal{S}_x$ is a subset of $\{1, \ldots, r\}$ of cardinality $n - 1$, we have at most $\binom{n - 1}{n - t}$ possibilities for $\mathcal{S}_x$. This proves Lemma 8. \hfill \blacksquare

**Proof of Lemma 4.** For $x = (\xi_1, \ldots, \xi_t) \in A$ define the tuple of integers $\psi(x) := (\text{ord}_{w_i}(\xi_i) : i = 1, \ldots, t, w_i \nmid S)$ where $w_i \nmid S$ indicates that $w_i$ runs through all places on $M_i$ not lying above a place in $S$. Then $\psi$ is an additive homomorphism on $A^*$ with kernel $O_{A,S}^*$, since $x = (\xi_1, \ldots, \xi_t) \in O_{A,S}^* \Leftrightarrow \xi_i \in O_{M_i,S}$ for $i = 1, \ldots, t \Leftrightarrow \text{ord}_{w_i}(\xi_i) = 0$ for $i = 1, \ldots, t$, $w_i \nmid S$. In particular, for $x_1, x_2 \in A^*$ we have $\psi(x_1) = \psi(x_2) \Leftrightarrow x_1 O_{A,S}^* = x_2 O_{A,S}^*$.

Now $\psi(x)$ can be obtained by combining all tuples $\psi_v(x)$ ($v \in M_K \setminus S$) from Lemma 8. Hence if $x$ runs through all solutions of (1.7), then $\psi(x)$
runs through a set of cardinality at most
\[
\prod_{v \in M_K \setminus S} \begin{pmatrix} r & n-1 \\ n-1 & \end{pmatrix} = \psi_2(\beta).
\]
This completes the proof of Lemma 4. ■

4. Proof of Theorem 1. Let \( K, S, s = \# S, M_1, \ldots, M_t, A = M_1 \oplus \ldots \oplus M_t, r = \dim_K A \geq 2, M, n = \dim_K KM, c, \beta \) be as in (1.12). Further, put \( V := KM \). By Lemma 4, the set of solutions of (1.7) is contained in some finite union of \( O_{A,S}^* - \) cosets. For the moment, we consider only the solutions of (1.7) in a fixed \( O_{A,S}^* \)-coset \( x_0 O_{A,S}^* \). More generally, we deal with elements of the set

\[
(4.1) \quad V \cap x_0 O_{A,S}^*
\]
where \( x_0 \) is a fixed element of \( A^* \). As before, we view \( K \) as a \( K \)-subalgebra of \( A \) by identifying \( \alpha \in K \) with \( \alpha A = (\alpha, \ldots, \alpha) \) (\( r \) times).

**Lemma 9.** Let \( B = \{ \alpha \in A : aV \subseteq V \} \) be the algebra of scalars of \( V \). Suppose that \( n \geq 2 \) and that the quotient group \( O_{B,S}^*/O_S^* \) is finite. Then there are proper \( K \)-linear subspaces \( Y_1, \ldots, Y_{t_2} \) of \( V \) such that

\[
V \cap x_0 O_{A,S}^* \subseteq Y_1 \cup \ldots \cup Y_{t_2} \quad \text{with} \quad t_2 \leq (2^{66} r^4)^{n^2 s}.
\]

**Proof.** We assume that \( x_0 = 1 \); this is no loss of generality since if \( x_0 \neq 1 \), we may prove Lemma 9 with \( x_0^{-1} V \cap O_{A,S}^* \) replacing \( V \cap x_0 O_{A,S}^* \). We want to apply Lemma 16 of [4] and for this purpose we must introduce some notation.

For \( i = 1, \ldots, t \), let \( \tau_{i,1}, \ldots, \tau_{i,r_i} \) (\( r_i = [M_i : K] \)) be the \( K \)-isomorphic embeddings of \( M_i \) into \( K \) and define the map \( f : A \to K^r \) by

\[
f(x) := (\tau_{i,1}(\xi_1), \ldots, \tau_{i,r_i}(\xi_1), \ldots, \tau_{i,1}(\xi_t), \ldots, \tau_{i,r_i}(\xi_t))
\]
for \( x = (\xi_1, \ldots, \xi_t) \in A \).

Thus, \( f(x) = (x_1, \ldots, x_r) \in K^r \). Let \( G \) denote the Galois group of \( K/K \). Clearly, for \( \sigma \in G, i = 1, \ldots, t, \sigma \circ \tau_{i,1}, \ldots, \sigma \circ \tau_{i,r_i} \) is a permutation of \( \tau_{i,1}, \ldots, \tau_{i,r_i} \). This implies that there is an action by \( G \) on \( \{1, \ldots, r \} \) attaching to each \( \sigma \in G \) a permutation \( (\sigma(1), \ldots, \sigma(r)) \) of \( (1, \ldots, r) \) such that for \( x \in A \) we have

\[
\sigma(x_i) = x_{\sigma(i)} \quad \text{for} \quad i = 1, \ldots, r, \quad \sigma \in G,
\]
where \( (x_1, \ldots, x_r) = f(x) \). Define the \( K \)-algebra

\[
A = \{ x = (x_1, \ldots, x_r) \in K^r : \sigma(x_i) = x_{\sigma(i)} \ \text{for} \ i = 1, \ldots, r, \ \sigma \in G \}.
\]
Then \( f \) is an injective \( K \)-homomorphism from \( A \) to \( A \). For instance from Lemma 2 of [4] it follows that \( K \)-linearly independent vectors of \( A \) are also
Let \( B \) be contained in some union \( W \) and let \( \mathcal{O}_S \) denote the integral closure of \( \mathcal{O}_S \) in \( K \). \( \mathcal{O}_S \) is the unit group of \( \mathcal{O}_S \), and \( \mathcal{O}_S^r \) the \( r \)-fold cartesian product of this unit group. It is easy to verify that

\[
(4.2) \quad f(\mathcal{O}_{A,S}^*) = A \cap (\mathcal{O}_S^*)^r.
\]

A symmetric partition of \( \{1, \ldots, r\} \) is a collection of sets \( \mathcal{P} = \{P_1, \ldots, P_q\} \) such that \( P_1 \cup \cdots \cup P_q = \{1, \ldots, r\} \), \( P_i \cap P_j = \emptyset \) for \( 1 \leq i < j \leq q \) and such that for each \( P \in \mathcal{P} \), \( \sigma \in G \), the set \( \sigma(P) = \{\sigma(k) : k \in P\} \) belongs also to \( \mathcal{P} \). To a symmetric partition \( \mathcal{P} \) we attach the \( K \)-subalgebra of \( A \),

\[
A_{\mathcal{P}} = \{x = (x_1, \ldots, x_r) \in A : x_i = x_j \text{ for each pair of indices } i, j \text{ belonging to the same set of } \mathcal{P}\}.
\]

Let \( W := f(V) \) and let \( \mathcal{P} \) be a symmetric partition of \( \{1, \ldots, r\} \) such that

\[
(4.3) \quad xW \subseteq W \quad \text{for } x \in A_{\mathcal{P}}.
\]

Let \( \tilde{B} := f^{-1}(A_{\mathcal{P}}) \). Then \( \tilde{B} \) is a \( K \)-subalgebra of \( B \). Hence \( \mathcal{O}_{B,S}^*/\mathcal{O}_S^* \) (with \( \varepsilon \in \mathcal{O}_S^* \) identified with \( (\varepsilon, \ldots, \varepsilon) \) \( t \) times) is finite. Now (4.2) implies that \( f \) maps \( \mathcal{O}_{B,S}^* \) to \( \mathcal{O}_{P,S}^* := A_{\mathcal{P}} \cap (\mathcal{O}_S^*)^r \). Further, \( f \) maps \( \mathcal{O}_S^* \) to \( f(\mathcal{O}_S^*) := \{(\varepsilon, \ldots, \varepsilon) \text{ \( (r \) times)} : \varepsilon \in \mathcal{O}_S^*\} \). Hence

\[
(4.4) \quad \mathcal{O}_{P,S}/f(\mathcal{O}_S^*) \text{ is finite.}
\]

Now let \( \mathcal{P} \) be the symmetric partition specified in the statement of Lemma 16 of [4]. This \( \mathcal{P} \) satisfies (4.3), hence (4.4) and so the condition of Lemma 16 of [4] is satisfied. Therefore, according to Lemma 16 of [4], the set \( W \cap (\mathcal{O}_S^*)^r \) is contained in some union \( W_1 \cup \cdots \cup W_{t_2} \) of proper linear subspaces of \( W \) with \( t_2 \leq (2^{6r+4})^n s \). By (4.2) we have \( V \cap \mathcal{O}_{A,S}^* = f^{-1}(W \cap (\mathcal{O}_S^*)^r) \). Hence \( V \cap \mathcal{O}_{A,S}^* \subseteq Y_1 \cup \cdots \cup Y_{t_2} \) with \( Y_i = f^{-1}(W_i) \) for \( i = 1, \ldots, t_2 \). This proves Lemma 9.

We want to relax the condition of Lemma 9 that \( \mathcal{O}_{B,S}^*/\mathcal{O}_S^* \) be finite and for this, we need some preparations.

We recall that a \( K \)-subalgebra \( B \) of \( A \) is said to be \( S \)-minimal if \( 1_A \in B \), and if \( B \) has no proper \( K \)-subalgebra \( B' \) with \( 1_A \in B' \) for which \( \mathcal{O}_{B,S}/\mathcal{O}_{B',S}^* \) is finite. Every \( K \)-subalgebra \( B \) of \( A \) with \( 1_A \in B \) has an \( S \)-minimal \( K \)-subalgebra \( B' \) for which \( \mathcal{O}_{B,S}/\mathcal{O}_{B',S}^* \) is finite. Namely, let \( B' \) be the intersection of all \( K \)-subalgebras \( B_1 \) of \( B \) with \( 1_A \in B_1 \) for which \( \mathcal{O}_{B,S}/\mathcal{O}_{B_1,S}^* \) is finite. Then \( \mathcal{O}_{B,S}^* \) is the intersection of all groups \( \mathcal{O}_{B_1,S}^* \). Furthermore, \( B \) has only finitely many \( K \)-subalgebras. Hence \( \mathcal{O}_{B,S}/\mathcal{O}_{B',S}^* \) is finite. If \( B'' \) is a \( K \)-subalgebra of \( B' \) with \( 1_A \in B'' \) such that \( \mathcal{O}_{B'',S}/\mathcal{O}_{B',S}^* \) is finite, then \( \mathcal{O}_{B,S}/\mathcal{O}_{B'',S}^* \) is finite, and therefore \( B'' \supseteq B' \). Hence \( B' \) is \( S \)-minimal.
In what follows, let
\[ B = \{ x \in A : xV \subseteq V \} \]
be the algebra of scalars of \( A \), and let \( B' \) be an \( S \)-minimal \( K \)-subalgebra of \( B \) for which \( O_{B,S}/O_{B',S} \) is finite. Every \( K \)-subalgebra of \( A \) is semisimple, i.e. isomorphic to a direct sum of finite extension fields of \( K \). So in particular we have
\[ B' \cong L'_1 \oplus \ldots \oplus L'_q \]
for certain finite extension fields \( L'_1, \ldots, L'_q \) of \( K \). Then \( B' \) has \( K \)-subalgebras \( L''_1, \ldots, L''_q \) such that
\[
\begin{align*}
B' &= L''_1 + \ldots + L''_q \quad \text{as vector space}, \\
L''_i \cdot L''_j &= (0) \quad \text{for } 1 \leq i < j \leq q, \\
L''_i &\cong L'_i \quad \text{for } i = 1, \ldots, q.
\end{align*}
\]
For \( i = 1, \ldots, q \), denote by \( 1_i \) the unit element of \( L''_i \). Then (4.5) and \( 1_A \in B' \) imply that
\[
1_A = 1_1 + \ldots + 1_q, \quad 1_i \cdot 1_j = 0 \quad \text{for } 1 \leq i < j \leq q.
\]
Let \( 1_i = (\xi_{i1}, \ldots, \xi_{it}) \) with \( \xi_{ij} \in M_j \) for \( j = 1, \ldots, t \). Since \( 1^2_i = 1_i \), we have \( \xi^2_{ij} = \xi_{ij} \), whence \( \xi_{ij} \in \{0,1\} \) for \( j = 1, \ldots, t \). Together with (4.6) this implies that there are subsets \( P_1, \ldots, P_q \) of \( \{1, \ldots, t\} \) such that
\[
\begin{align*}
1_i &= (\xi_{i1}, \ldots, \xi_{it}) \quad \text{with } \xi_{ij} = 1 \quad \text{for } j \in P_i, \quad \xi_{ij} = 0 \quad \text{for } j \notin P_i, \\
P_1 \cup \ldots \cup P_q &= \{1, \ldots, t\}, \quad P_i \cap P_j = \emptyset \quad \text{for } 1 \leq i < j \leq q.
\end{align*}
\]
Define the \( K \)-algebras
\[ A_i = \bigoplus_{j \in P_i} M_j \quad \text{for } i = 1, \ldots, q, \]
the projections
\[ \Pi_i : A \rightarrow A_i : (\xi_1, \ldots, \xi_t) \mapsto (\xi_j : j \in P_i) \quad \text{for } i = 1, \ldots, q, \]
and
\[ \Pi = (\Pi_1, \ldots, \Pi_q) : A \rightarrow A_1 \oplus \ldots \oplus A_q : x \mapsto (\Pi_1(x), \ldots, \Pi_q(x)). \]
\( \Pi \) is merely a permutation of coordinates, so \( \Pi \) is a \( K \)-algebra isomorphism from \( A \) to \( A_1 \oplus \ldots \oplus A_q \). Further define
\[ B_i := \Pi_i(B), \quad L_i := \Pi_i(B'), \quad V_i := \Pi_i(V) \quad \text{for } i = 1, \ldots, q, \]
where \( B_i, L_i \) are \( K \)-subalgebras, and \( V_i \) is a subspace of \( A_i \). Then we have:

**Lemma 10.** (i) \( \Pi(B) = B_1 \oplus \ldots \oplus B_q \), \( \Pi(B') = L_1 \oplus \ldots \oplus L_q \), \( \Pi(V) = V_1 \oplus \ldots \oplus V_q \).

(ii) For \( i = 1, \ldots, q \), \( L_i \) is isomorphic to a finite extension field of \( K \).

(iii) \( B_i = \{ x \in A_i : xV_i \subseteq V_i \} \) for \( i = 1, \ldots, q \).
Therefore, \( B \) is a subalgebra of \( O \), hence \( \Pi(x) \) is a field, hence \( \Pi_i(x) \) is non-trivial as its image contains \((1, \ldots, 1)\) and \( L''_j \) is a field.

(ii) Let \( i \in \{1, \ldots, q\} \). We first show that \( \Pi_i(L''_j) = \Pi_i(B') \). Now \( L''_j \) is a \( K \)-subalgebra of \( B' \), hence \( \Pi_i(L''_j) \subseteq \Pi_i(B') \). Conversely, let \( x \in B' \). Then

\[
x = x_1 + \ldots + x_q \quad \text{with} \quad x_j \in L''_j \quad \text{for} \quad j = 1, \ldots, q.
\]

Now (4.7) and (4.8) imply that for \( j = 1, \ldots, q \), the coordinates of \( y \) with indices in \( P_j \) are equal to the corresponding coordinates of \( y_j \). Hence \( \Pi_j(y) = \Pi_j(y_j) = x_j \) for \( j = 1, \ldots, q \). Therefore, \( \Pi_i(y) = x \). We infer that indeed \( \Pi_i(V) = V_1 \oplus \ldots \oplus V_q \).

(iii) Let \( i \in \{1, \ldots, q\} \). We first show that \( \Pi_i(L''_j ) = \Pi_i(B' ) \). Now \( L''_j \) is a \( K \)-subalgebra of \( B' \), hence \( \Pi_i(L''_j) \subseteq \Pi_i(B') \). Conversely, let \( x \in B' \). Then \( x = x_1 + \ldots + x_q \) with \( x_j \in L''_j \) for \( j = 1, \ldots, q \). Now \( \Pi_i(1) = (1, \ldots, 1) \) and by (4.5) we have \( 1 x_j = 0 \) for \( j \neq i \). Hence

\[
\Pi_i(x) = \Pi_i(1; x) = \Pi_i(1; x_i) = \Pi_i(x_1) \in \Pi_i(L''_j).
\]

This shows that indeed \( \Pi_i(L''_j) = \Pi_i(B' ) \). Now \( \Pi_i \) is non-trivial as its image contains \((1, \ldots, 1)\) and \( L''_j \) is a field.

Fix again \( i \in \{1, \ldots, q\} \). We have \( L_i \subseteq B_i \subseteq A_i \), so that \( A_i \) may be viewed as an \( L_i \)-algebra and \( B_i \) as an \( L_i \)-subalgebra of \( A_i \). Further, the unit element \( 1_{A_i} \) of \( A_i \) is just the unit element of \( L_i \), and so \( 1_{A_i} \in B_i \). Lastly, by Lemma 10(iii), \( V_i \) is an \( L_i \)-vector space. Note that \( O_{A_i,S} = \oplus_{j \in P_i} O_{L_i,S} \), \( O_{B_i,S} = O_{A_i,S} \cap B_i \), \( O_{L_i,S} = O_{A_i,S} \cap L_i \) are the integral closures of \( O_S \) in \( A_i, B_i, L_i \), respectively. Clearly, \( O_{B_i,S}^* / O_{L_i,S}^* \) is a homomorphic image of \( O_{B_i,S}^* / O_{B_i,S} \), so

\[
O_{B_i,S}^* / O_{L_i,S}^* \text{ is finite.}
\]

We are now ready to prove the following generalisation of Lemma 9:

**Lemma 11.** Either \( V = yB' \) for some \( y \in A \), or there are proper \( K \)-linear subspaces \( Y_1, \ldots, Y_{t_3} \) of \( V \) such that

\[
V \cap x_0 O_{A,S}^* \subseteq Y_1 \cup \ldots \cup Y_{t_3} \text{ with } t_3 \leq (2^{66} r^4)^{n^2}.
\]

**Proof.** As mentioned before, for \( i = 1, \ldots, q \), \( V_i \) may be viewed as an \( L_i \)-vector space. First assume that \( \dim_{L_i} V_i = 1 \) for \( i = 1, \ldots, q \). Then for \( i = 1, \ldots, q \) there is an \( y_i \in A_i \), such that \( V_i = y_i L_i \). Together with
Lemma 10(i) this implies that $V = \Pi^{-1}(y_1L_1 \oplus \ldots \oplus y_qL_q) = yB'$ with $y = \Pi^{-1}((y_1, \ldots, y_q))$.

Now assume that $\dim_{L_1} V_1 \geq 2$, say. Put $n_1 := \dim_{L_1} V_1, r_1 := \dim_{L_1} A_1$, let $S_1$ be the set of places lying above those in $S$, and $s_1$ the cardinality of $S_1$. Then since $V_1$ is a $K$-linear subspace of $\Pi(V) \cong V$, and $A_1$ of $\Pi(A) \cong A$, we have

$$n_1[L_1 : K] = \dim_K V_1 \leq n, \quad r_1[L_1 : K] = \dim_K A_1 \leq r,$$

$s_1 \leq s[L_1 : K]$.

Further, putting $x_0 := \Pi_1(x_0)$, we have

$$\Pi_1(V \cap x_0O_{A,S}^*) \subseteq V_1 \cap x_0O_{A,S}^*.$$

In view of Lemma 10(iii) and of (4.9), we may apply Lemma 9 with $L_1, A_1, B_1, V_1, S_1$ replacing $A, V, S$ this implies that $V_1 \cap x_0O_{A,S}^* \subseteq Z_1 \cup \ldots \cup Z_{t_3}$, where $Z_j = 1$ is a proper $K$-linear subspace of $V$. This proves Lemma 11. 

We recall that $e(n)$ is defined by $e(n) = \frac{1}{2}n(n + 1)(2n + 1) - 2$.

**Lemma 12.** There are $y_1, \ldots, y_{t_4} \in A^*$ and $S$-minimal $K$-subalgebras $B_1, \ldots, B_{t_4}$ of $A$ such that

$$y_iB_i \subseteq V \quad \text{for } i = 1, \ldots, t_4,$$

$$V \cap x_0O_{A,S}^* \subseteq y_1O_{B_1,S}^* \cup \ldots \cup y_{t_4}O_{B_{t_4},S}^* \quad \text{with } t_4 \leq (2^{33}r^2)^{e(n)}.$$ 

**Proof.** We first deal with the special case where $V = yB_1$ for some $y \in A$ and some $S$-minimal $K$-subalgebra $B_1$ of $A$. Assume that $V \cap x_0O_{A,S}^* \neq \emptyset$ and let $y_1 \in V \cap x_0O_{A,S}^*$. Then $x_0O_{A,S}^* = y_1O_{A,S}^*$. By assumption we have $x_0 \in A^*$, hence $y_1 \in A^*$. Further, $y_1 = yz$ for some $z \in B_1$, and so $z \in B_1^*$. Therefore, $V = yB_1 = y_1B_1$. It follows that

$$V \cap x_0O_{A,S}^* = y_1B_1 \cap y_1O_{A,S}^* = y_1O_{B_1,S}^*,$$

which implies Lemma 12 for $V = yB_1$.

We prove Lemma 12 in full generality by induction on $n = \dim_K V$. If $n = 1$, then $V = yK$ for some $y \in A$ and we are done since $K$ is an $S$-minimal subalgebra of $A$. Suppose that $n \geq 2$, and that $V$ is not equal to $yB$ for some $y \in A$ and some $S$-minimal $K$-subalgebra $B$ of $A$. Then by Lemma 11 we have $V \cap x_0O_{A,S}^* \subseteq Y_1 \cup \ldots \cup Y_{t_4}$ with $t_4 \leq (2^{33}r^2)^{e(n)}$, where $Y_1, \ldots, Y_{t_4}$ are proper $K$-linear subspaces of $V$. Now by the induction
hypothesis we have for $i = 1, \ldots, t_3$,
\[ Y_i \cap x_0 O_{A,S}^* \subseteq y_i,1 O_{B_{1,1},S}^* \cup \ldots \cup y_{i, t_5} O_{B_{1,t_5},S}^* \] with $t_5 \leq (2^{33} r^2)^{e(n-1)s}$
where $y_{i,j} \in A^*$, and $B_{i,j}$ is an $S$-minimal $K$-subalgebra of $A$ with $y_{i,j}B_{i,j} \subseteq Y_i$ for $j = 1, \ldots, t_5$. It follows that
\[ V \cap x_0 O_{A,S}^* \subseteq \bigcup_{i=1}^{t_5} \bigcup_{j=1}^{t_5} y_{i,j} O_{B_{i,j},S}^* \] with $y_{i,j}B_{i,j} \subseteq V$.

Since $t_3 t_5 \leq (2^{33} r^2)^{(2n^2 + e(n-1))s} = (2^{33} r^2)^{e(n)s}$, this proves Lemma 12. 

Before finishing the proof of Theorem 1, we prove the following lemma:

**Lemma 13.** Let $B$ be an $S$-minimal $K$-subalgebra of $A$, and $x_0 M_{M,B}$ an $(M, B)$-family of solutions of (1.7) with $x_0 \in M^B$. Then $x_0 U_{M,B}$ is irreducible.

**Proof.** Suppose that $x_0 U_{M,B}$ is reducible. Then there are proper subfamilies $x_1 U_{M,B_1}, \ldots, x_w U_{M,B_w}$ of $x_0 U_{M,B}$ such that
\[ (4.10) \quad x_0 U_{M,B} = x_1 U_{M,B_1} \cup \ldots \cup x_w U_{M,B_w}. \]
Further, there is no loss of generality to assume that
\[ (4.11) \quad x_i \in M^{B_i}, \quad B_i \subsetneq B \text{ for } i = 1, \ldots, w. \]
Namely, if for instance $B_1$ is not a $K$-subalgebra of $B$ then by Lemma 3, $x_1 U_{M,B_1} = x_1 U_{M,B} \cap x_1 U_{M,B_1}$ is the union of finitely many $(M, B \cap B_1)$-families and, in (4.10), we may replace $x_1 U_{M,B_1}$ by this union. Further, if $B_1 = B$ then $x_1 U_{M,B_1}$ is not a proper subfamily of $x_0 U_{M,B}$.

Put $\zeta_B := \text{rank} O_{B,S}^*/O_S^*$, $\zeta := \max_{i=1,\ldots,w} \{\text{rank} O_{B_i,S}^*/O_S^*\}$. From (4.11) and the fact that $B$ is $S$-minimal, it follows that $\zeta < \zeta_B$. On the other hand, letting $N_{x}(X)$ be the quantity in the statement of Lemma 2, it follows from Lemma 2 and (4.10) that
\[ N_{x_0 U_{M,B}}(X) = \gamma (\log X)^{\beta \zeta} + O((\log X)^{\beta \zeta - 1}) \text{ as } X \to \infty \text{ with } \gamma > 0, \]
\[ N_{x_0 U_{M,B}}(X) = N_{\bigcup_{i=1}^{w} x_i U_{M,B_i}}(X) = O((\log X)^{\zeta}) \text{ as } X \to \infty. \]
Thus, the assumption that $x_0 U_{M,B}$ is reducible leads to a contradiction. This proves Lemma 13. 

**Proof of Theorem 1.** By Lemma 4, the set of solutions of (1.7) is contained in some union $\bigcup_{j=1}^{t_1} \{V \cap x_j O_{A,S}^*\}$ with $x_j \in A^*$ for $j = 1, \ldots, t_1$ and $t_1 \leq \psi_2(\beta)$. By Lemma 12, for $j = 1, \ldots, t_1$, $V \cap x_j O_{A,S}^*$ is a subset of some finite union $\bigcup_{h=1}^{t_4} y_{jh} O_{B_{jh,S}}^*$ with $t_4 \leq (2^{33} r^2)^{e(n)s}$, where $y_{jh} \in A^*$ and $B_{jh}$ is an $S$-minimal $K$-subalgebra of $A$ with $y_{jh} B_{jh} \subseteq V$, $h = 1, \ldots, t_4$. It follows that the set of solutions of (1.7) is contained in $\bigcup_{h=1}^{w} y_{h} O_{B_{h,S}}^*$ with
w \leq (2^{33} r^2)^{(c(n)} \psi_2(\beta), \text{ where } y_h \in A^* \text{ and } B_h \text{ is an } S\text{-minimal } K\text{-subalgebra of } A \text{ with } y_hB_h \subseteq V, \ h = 1, \ldots, w.

We recall that if $B$ is an $S$-minimal $K$-subalgebra of $A$, then, by Lemma 13, any $(\mathcal{M}, B)$-family of solutions is automatically irreducible. Hence the proof of Theorem 1 is complete once we show that the set of solutions of (1.7) belonging to some coset $yO^*_B, S$ with $y \in A^*, yB \subseteq V$ is the union of at most $I := [O^*_B, S : \mathcal{U}_{\mathcal{M}, B}]$ $(\mathcal{M}, B)$-families of solutions. Clearly, $yO^*_B, S$ is the union of $I$ cosets $z\mathcal{U}_{\mathcal{M}, B}$ with $z \in A^*$. Suppose that $z\mathcal{U}_{\mathcal{M}, B}$ contains a solution, say $z_0$, of (1.7). Then $z\mathcal{U}_{\mathcal{M}, B} = z_0\mathcal{U}_{\mathcal{M}, B}$. We have $z_0 \in \mathcal{M}$ and also $z_0B = zB = yB \subseteq V$, so $z_0 \in V^B \cap \mathcal{M} = \mathcal{M}^B$, which implies that $z \in \mathcal{M}^B$. This proves that $z\mathcal{U}_{\mathcal{M}, B}$ is an $(\mathcal{M}, B)$-family of solutions of (1.7). This completes the proof of Theorem 1. $

5. Proof of Theorem 2. We will prove Theorem 2 more generally, for arbitrary fields $K$ of characteristic 0. Thus, let $K$ be any field of characteristic 0, $A = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_t$ where $\mathcal{M}_1, \ldots, \mathcal{M}_t$ are finite extension fields of $K$ with $\dim_K \mathcal{M}_i = \sum_{i=1}^t [\mathcal{M}_i : K] = r$, and $V$ is an $n$-dimensional $K$-linear subspace of $A$. It is our purpose to prove that there are at most $n \max(r - n, 2)^n$ $K$-subalgebras of $A$ with

\begin{equation}
1_A \in B, \quad V^B \cap A^* \neq \emptyset.
\end{equation}

We make some reductions. Let $\overline{K}$ be the algebraic closure of $K$ and $\overline{A} = \overline{K}^r$ with coordinatewise addition and multiplication. For $x = (x_1, \ldots, x_t) \in A$, put $f(x) := (r_1(x_1), \ldots, r_t(x_t), \ldots, \tau_t, 1(x_1), \ldots, \tau_t, r_t(x_t))$, where for $i = 1, \ldots, t$, $\tau_i, 1, \ldots, \tau_t, r_t = [\mathcal{M}_i : K]$ are the $K$-isomorphic embeddings of $\mathcal{M}_i$ into $\overline{K}$. Then $f$ is an injective $K$-algebra homomorphism from $A$ into $\overline{A}$. It is easy to check that $f$ maps $K$-linearly independent elements of $A$ to $\overline{K}$-linearly independent elements of $\overline{A}$. Hence, if for a $K$-linear subspace $W$ of $A$ we define $\overline{W}$ to be the $\overline{K}$-vector space generated by $f(W)$, we see that $\dim_{\overline{K}} \overline{W} = \dim_K W$ and that $W$ is uniquely determined by $\overline{W}$. Finally, if $B$ is a $K$-subalgebra of $A$ then $\overline{B}$ is a $\overline{K}$-subalgebra of $\overline{A}$: namely, if $x, y \in \overline{B}$, then $x = \sum \xi_i f(x_i), y = \sum \eta_j f(y_j)$ with $\xi_i, \eta_j \in \overline{K}, x_i, y_j \in B$ and therefore, $xy = \sum \xi_i \eta_j f(x_i y_j) \in \overline{B}$. Note that $1 = (1, \ldots, 1) (r \text{ times})$ is the element of $A$ and that $\overline{A} = \{ (\xi_1, \ldots, \xi_r) \in \overline{K}^r : \xi_1 \ldots \xi_r \neq 0 \}$. For $K$-subalgebras $B$ of $A$ with (1.16) we have

\begin{equation}
1 \in \overline{B}, \quad V^B \cap A^* \neq \emptyset.
\end{equation}

Namely, it is clear that $1 \in \overline{B}$. Further, if $x \in V^B \cap A^*$, we have $f(x) \in A^*$ and also $xB \subseteq V$, whence $f(x)B \subseteq V$, i.e. $f(x) \in V^B \cap A^*$. Since $B$ is uniquely determined by $\overline{B}$, it follows that the number of $K$-subalgebras $B$ of $A$ with (1.16) is at most the number of $K$-subalgebras $\overline{B}$ of $\overline{A}$ with (5.1). Hence it suffices to prove the following:
Lemma 14. \( \overline{A} \) has at most \( \{n \max(r-n,2)\}^n \) \( K \)-subalgebras \( \overline{B} \) with (5.1).

Proof. Let \( \overline{B} \) be a \( K \)-subalgebra of \( \overline{A} \) with (5.1). Then, for some \( q \leq r \), \( \overline{B} \) is isomorphic to \( K^j \) with coordinatewise operations. This implies that \( \overline{B} \) has \( K \)-subalgebras \( L_1'', \ldots, L_q'' \) such that \( L_i'' = K \) for \( i = 1, \ldots, q \), \( L_i'' + \ldots + L_q'' = \overline{B} \), and \( L_i'', L_j'' = 0 \) for \( 1 \leq i < j \leq q \). Letting \( 1_i \) be the unit element of \( L_i'' \) for \( i = 1, \ldots, q \), we find, completely similarly to (4.7) and (4.8), that there are non-empty subsets \( P_1, \ldots, P_q \) of \( \{1, \ldots, r\} \) such that

\[
(5.2) \quad 1_i = (\xi_{i1}, \ldots, \xi_{ir}) \quad \text{with} \quad \xi_{ij} = 1 \quad \text{for} \quad j \in P_i, \quad \xi_{ij} = 0 \quad \text{for} \quad j \notin P_i,
\]

\[
(5.3) \quad P_1 \cup \ldots \cup P_q = \{1, \ldots, r\}, \quad P_i \cap P_j = \emptyset \quad \text{for} \quad 1 \leq i < j \leq r.
\]

First suppose that \( r > n \). On noting that \( \dim_K V = n \), after a permutation of coordinates if necessary, we may assume that \( V \) is the set of solutions \( (\xi_1', \ldots, \xi_r') \) of a system of linear equations

\[
(5.4) \quad \xi_k = \sum_{j=1}^{n} c_{kj} \xi_j \quad \text{for} \quad k = n+1, \ldots, r,
\]

with \( c_{kj} \in K \). Let \((\xi_1', \ldots, \xi_r') \in V^{P} \cap \overline{A}^{n} \). Then \( 1_i x \in V \) for \( i = 1, \ldots, q \). (5.2) implies that the coordinates of \( 1_i x \) with indices in \( P_i \) are the same as those of \( x \), while the coordinates of \( 1_i x \) with indices outside \( P_i \) are 0. Together with (5.4) this implies

\[
(5.5) \quad \begin{cases} 
\xi_k = \sum_{j \in Q_i} c_{kj} \xi_j & \text{for} \quad k \in R_i, \quad i = 1, \ldots, q, \\
0 = \sum_{j \in Q_i} c_{kj} \xi_j & \text{for} \quad k \in \overline{R}_i := \{n+1, \ldots, r\} \setminus R_i, \quad i = 1, \ldots, q,
\end{cases}
\]

where \( Q_i := P_i \cap \{1, \ldots, n\}, \quad R_i := P_i \cap \{n+1, \ldots, r\}, \quad i = 1, \ldots, q \). Note that

\[
(5.6) \quad \begin{cases} 
Q_1 \cup \ldots \cup Q_q = \{1, \ldots, n\}, \quad Q_i \cap Q_j = \emptyset & \text{for} \quad 1 \leq i < j \leq q, \\
R_1 \cup \ldots \cup R_q = \{n+1, \ldots, r\}, \quad R_i \cap R_j = \emptyset & \text{for} \quad 1 \leq i < j \leq q, \\
Q_i \cap R_j \neq \emptyset & \text{for} \quad i, j = 1, \ldots, q.
\end{cases}
\]

Further, by (5.2) and the fact that \( \overline{B} = L_1'' + \ldots + L_q'' = 1_1 K + \ldots + 1_q K \), we see that \( \overline{B} \) is determined uniquely by \( P_1, \ldots, P_q \), whence by \( Q_1, \ldots, Q_q, \quad R_1, \ldots, R_q \). Recalling that \( x \in A^* \) we infer that it suffices to prove

\[
(5.7) \quad \text{there are at most} \quad \{n \max(r-n,2)\}^n \text{collections} \quad \{Q_1, \ldots, Q_q, R_1, \ldots, R_q\} \quad \text{with (5.6)} \quad \text{such that} \quad (5.5) \quad \text{has a solution with} \quad \xi_1 \ldots \xi_r \neq 0.
\]

For the moment, we fix \( Q_1, \ldots, Q_q \) and determine an upper bound for the number of collections \( \{R_1, \ldots, R_q\} \) for which (5.5) has a solution with \( \xi_1 \ldots \xi_r \neq 0 \). Let \( n_i := \#Q_i \) for \( i = 1, \ldots, q \). Take \( i \in \{1, \ldots, q\} \). We have \( Q_i \neq \emptyset \) since otherwise \( R_i \neq \emptyset \) and each solution of (5.5) has \( \xi_k = 0 \) for
Decomposable form equations

393

Define the vectors $c_k = (c_{kj} : j \in Q_i)$ ($k = n + 1, \ldots, r$). We have $\text{rank}\{c_k : k \in \tilde{R}_i\} \leq n_i - 1$, since otherwise each solution of (5.5) has $\xi_j = 0$ for $j \in Q_i$. Further, for each $l \in R_i$ the vector $c_l$ is linearly independent of $\{c_k : k \in \tilde{R}_i\}$, since otherwise the equations $\sum_{j \in Q_i} c_{kj} \xi_j = 0$ for $k \in \tilde{R}_i$ imply $\sum_{j \in Q_i} c_{lj} \xi_j = 0$ for some $l \in R_i$, and so each solution of (5.5) has $\xi_l = 0$. It follows that $\{c_k : k \in \tilde{R}_i\}$ consists of all vectors in $\{c_k : k = n + 1, \ldots, r\}$ that are linear combinations of some linearly independent subset of $\{c_k : k \in \tilde{R}_i\}$. But then, this linearly independent subset uniquely determines $R_i$. Recalling that $\text{rank}\{c_k : k \in \tilde{R}_i\} \leq n_i - 1$, we infer that the number of possibilities for $R_i$ is at most the number of linearly independent subsets of $\{c_k : k = n + 1, \ldots, r\}$ of cardinality $\leq n_i - 1$, and the latter is at most

$$\binom{r - n}{0} + \binom{r - n}{1} + \cdots + \binom{r - n}{n_i - 1} \leq \max(r - n, 2)^{n_i}.$$ 

Therefore, for given $Q_1, \ldots, Q_q$, the number of possibilities for $\{R_1, \ldots, R_q\}$ is at most

$$\left(\max(r - n, 2)\right)^{n_1 + \cdots + n_q} = \left(\max(r - n, 2)\right)^n.$$

The number of possibilities for $\{Q_1, \ldots, Q_q\}$ is at most the number of partitions of $\{1, \ldots, n\}$ into disjoint sets, which is $\leq n^n$. This implies (5.7), hence Lemma 14 for $r > n$. If $r = n$, then the sets $R_1, \ldots, R_q$ do not occur and we only have to estimate the number of possibilities for $\{Q_1, \ldots, Q_q\}$. So in that case, Lemma 14 follows also. 

References