Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)
Vol. XII (2013), 467-497

Multiply monogenic orders

ATTILA BÉRCZES, JAN-HENDRIK EVERTSE AND KÁLMÁN GYŐRY

Abstract. Let $A = \mathbb{Z}[x_1, \ldots, x_r] \supset \mathbb{Z}$ be a domain which is finitely generated over $\mathbb{Z}$ and integrally closed in its quotient field L. Further, let K be a finite extension field of L. An A-order in K is a domain $\mathcal{O} \supset A$ with quotient field K which is integral over A. A-orders in K of the type $A[\alpha]$ are called monogenic. It was proved by Győry [10] that for any given A-order $\mathcal{O}$ in K there are at most finitely many A-equivalence classes of $\alpha \in \mathcal{O}$ with $A[\alpha] = \mathcal{O}$, where two elements α, β of $\mathcal{O}$ are called A-equivalent if $\beta = u\alpha + a$ for some $u \in A^*$, $a \in A$. If the number of A-equivalence classes of α with $A[\alpha] = \mathcal{O}$ is at least k, we call $\mathcal{O}$ k times monogenic.

In this paper we study orders which are more than one time monogenic. Our first main result is that if K is any finite extension of L of degree ≥ 3, then there are only finitely many three times monogenic A-orders in K. Next, we define two special types of two times monogenic A-orders, and show that there are extensions K which have infinitely many orders of these types. Then under certain conditions imposed on the Galois group of the normal closure of K over L, we prove that K has only finitely many two times monogenic A-orders which are not of these types. Some immediate applications to canonical number systems are also mentioned.

Mathematics Subject Classification (2010): 11R99 (primary); 11D99, 11J99 (secondary).

1. Introduction

In this introduction we present our results in the special case $A = \mathbb{Z}$. Our general results over arbitrary finitely generated domains A are stated in the next section.

Let K be an algebraic number field of degree $d \geq 2$ with ring of integers $\mathcal{O}_K$. The number field K is called *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. This is equivalent to the fact that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ forms a $\mathbb{Z}$-module basis for $\mathcal{O}_K$. The

The research was supported in part by grants T67580 and T75566 (A.B., K.G.) of the Hungarian National Foundation for Scientific Research, and the János Bolyai Research Scholarship (A.B.). The work is supported by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund. (A.B.)

Received July 18, 2011; accepted August 22, 2011.

existence of such a basis, called *power integral basis*, considerably facilitates the calculations in $\mathcal{O}_K$ and the study of arithmetical properties of $\mathcal{O}_K$.

The quadratic and cyclotomic number fields are monogenic, but this is not the case in general. Dedekind [4] gave the first example for a non-monogenic number field.

More generally, an order $\mathcal{O}$ in K, that is a subring of $\mathcal{O}_K$ with quotient field equal to K, is said to be monogenic if $\mathcal{O} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}$. Then for $\beta = \pm\alpha + a$ with $a \in \mathbb{Z}$ we also have $\mathcal{O} = \mathbb{Z}[\beta]$. Such elements α, β of $\mathcal{O}$ are called $\mathbb{Z}$*-equivalent*.

In this paper, we deal with the "Diophantine equation"

$$\mathbb{Z}[\alpha] = \mathcal{O} \text{ in } \alpha \in \mathcal{O} \tag{1.1}$$

where $\mathcal{O}$ is a given order in K. As has been explained above, the solutions of (1.1) can be divided into $\mathbb{Z}$-equivalence classes. It was proved by Győry [7–9] that there are only finitely many $\mathbb{Z}$-equivalence classes of $\alpha \in \mathcal{O}$ with (1.1), and that a full system of representatives for these classes can be determined effectively. Evertse and Győry [5] gave a uniform and explicit upper bound, depending only on $d = [K : \mathbb{Q}]$, for the number of $\mathbb{Z}$-equivalence classes of such α. For various generalizations and effective versions, we refer to Győry [13].

In what follows, the following definition will be useful.

Definition. An order $\mathcal{O}$ is called *k times monogenic,* if there are at least k distinct $\mathbb{Z}$-equivalence classes of α with (1.1), in other words, if there are at least k pairwise $\mathbb{Z}$-inequivalent elements $\alpha_1, \dots, \alpha_k \in \mathcal{O}$ such that

$$\mathcal{O} = \mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k].$$

Similarly, the order $\mathcal{O}$ is called *precisely/at most k times monogenic,* if there are precisely/at most k $\mathbb{Z}$-equivalence classes of α with (1.1).

It is not difficult to show that any order $\mathcal{O}$ in a quadratic number field is precisely one time monogenic, *i.e.*, there exist $\alpha \in \mathcal{O}$ with (1.1), and these α are all $\mathbb{Z}$-equivalent to one another.

Our first result is as follows.

Theorem 1.1. *Let K be a number field of degree ≥ 3. Then there are at most finitely many three times monogenic orders in K.*

This result is a refinement of work of Bérczes [1].

The bound 3 is best possible, *i.e.*, there are number fields K having infinitely many two times monogenic orders. We believe that if K is an arbitrary number field of degree ≥ 3, then with at most finitely many exceptions, all two times monogenic orders in K are of a special structure. Below, we state a theorem which confirms this if we impose some restrictions on K.

Let K be a number field of degree at least 3. An order $\mathcal{O}$ in K is called of **type I** if there are $\alpha, \beta \in \mathcal{O}$ and $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$ such that

$$K = \mathbb{Q}(\alpha), \quad \mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \quad \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}, \quad a_3 \neq 0. \tag{1.2}$$

Notice that β is not $\mathbb{Z}$-equivalent to α, since $a_3 \neq 0$ and K has degree at least 3. So orders of type I are two times monogenic.

Orders $\mathcal{O}$ of type II exist only for number fields of degree 4. An order $\mathcal{O}$ in a quartic number field K is called of **type II** if there are $\alpha, \beta \in \mathcal{O}$ and $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Z}$ with $a_0 b_0 \neq 0$ such that

$$\begin{aligned} &K = \mathbb{Q}(\alpha), \quad \mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \\ &\beta = a_0\alpha^2 + a_1\alpha + a_2, \quad \alpha = b_0\beta^2 + b_1\beta + b_2. \end{aligned} \tag{1.3}$$

Orders of type II are certainly two times monogenic. At the end of this section, we give examples of number fields having infinitely many orders of type I, respectively II.

Let E be a field of characteristic 0, and $F = E(\theta)/E$ a finite field extension of degree d. Denote by $\theta^{(1)}, \ldots, \theta^{(d)}$ the conjugates of θ over E, and by G the normal closure $E(\theta^{(1)}, \ldots, \theta^{(d)})$ of F over E. We call F *m times transitive* over E ($m \leq d$) if for any two ordered m-tuples of distinct indices $(i_1, \ldots, i_m)$, $(j_1, \ldots, j_m)$ from $\{1, \ldots, d\}$, there is $\sigma \in \mathrm{Gal}(G/E)$ such that

$$\sigma(\theta^{(i_1)}) = \theta^{(j_1)}, \ldots, \sigma(\theta^{(i_m)}) = \theta^{(j_m)}.$$

If $E = \mathbb{Q}$, we simply say that F is m times transitive.

We denote by S_n the permutation group on n elements.

Our result on two times monogenic orders is as follows.

Theorem 1.2. **(i)** *Let K be a cubic number field. Then every two times monogenic order in K is of type I.*

(ii) *Let K be a quartic number field of which the normal closure has Galois group S_4. Then there are at most finitely many two times monogenic orders in K which are not of type I or of type II.*

(iii) *Let K be a four times transitive number field of degree at least 5. Then there at most finitely many two times monogenic orders in K which are not of type I.*

In Section 2 we present some immediate applications of our results to canonical number systems. In Section 3 we formulate generalizations of Theorems 1.1 and 1.2 for the case that the ground ring is an arbitrary integrally closed domain which is finitely generated over $\mathbb{Z}$. Sections 4–6 contain auxiliary results, and Sections 7–9 contain our proofs.

Our proofs of Theorems 1.1 and 1.2 use finiteness results on unit equations in more than two unknowns, together with some combinatorial arguments. At present, it is not known how to make the results on unit equations effective, therefore we are not able to determine effectively the three times monogenic orders in Theorem 1.1, or the two times monogenic orders not of type I or II in Theorem 1.2. Although it is possible to estimate from above the number of solutions of unit equations, it is because of the combinatorial arguments in our proofs that we are not able to estimate from above the numbers of exceptional orders in Theorems 1.1 and 1.2.

We finish this introduction with constructing number fields having infinitely many orders of type I, respectively type II.

Let K be a number field of degree ≥ 3 which is not a totally complex quadratic extension of a totally real field. By Dirichlet's Unit Theorem, for any proper subfield L of K, the rank of $\mathcal{O}_L^*$ (the group of units of the ring of integers of L) is smaller than that of $\mathcal{O}_K^*$. We show that K has infinitely many orders of type I. Take $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$ with $a_3 \neq 0$. Suppose that there is $u_0 \in \mathcal{O}_K^*$ such that $u_0 \equiv a_4 \pmod{a_3}$. This is the case for instance if $a_3 = 1$. By the Euler-Fermat Theorem for number fields, there is a positive integer t such that $u^t \equiv 1 \pmod{a_3}$ for every $u \in \mathcal{O}_K^*$. Hence the group of units $u \in \mathcal{O}_K^*$ with $u \equiv 1 \pmod{a_3}$ has finite index in $\mathcal{O}_K^*$. Consequently, there are infinitely many units $u \in \mathcal{O}_K^*$ with $u \equiv a_4 \pmod{a_3}$. By our assumption on K, among these, there are infinitely many u with $\mathbb{Q}(u) = K$. For each such u, put

$$\alpha := \frac{u - a_4}{a_3}, \quad \beta := \frac{a_1\alpha + a_2}{a_3\alpha + a_4}.$$

Then clearly, $K = \mathbb{Q}(\alpha)$. From the minimal polynomial of u we derive a relation $u^{-1} = f(u)$ with $f \in \mathbb{Z}[X]$. Hence $\beta = (a_1\alpha + a_2) f(a_3\alpha + a_4) \in \mathbb{Z}[\alpha]$. Since $\beta = (a_4\beta - a_2)/(-a_3\beta + a_1)$ and $-a_3\beta + a_1 = \pm u^{-1}$, we obtain in a similar fashion $\alpha \in \mathbb{Z}[\beta]$. Therefore, $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. By varying $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ and u we obtain infinitely many orders of type I in K.

For instance, for $u \in \mathcal{O}_K^*$ we have $\mathbb{Z}[u] = \mathbb{Z}[u^{-1}]$ and the discriminant of this order is the discriminant of (the minimal polynomial of) u. By Győry [8, Corollaire 2.2], there are at most finitely many units $u \in \mathcal{O}_K^*$ of given discriminant. Hence there are infinitely many distinct orders among $\mathbb{Z}[u]$ ($u \in \mathcal{O}_K^*$).

We now construct quartic fields with infinitely many orders of type II. The construction is based on the theory of cubic resolvents, see van der Waerden [20, Section 64].

Let r, s be integers such that the polynomial $f(X) = (X^2 - r)^2 - X - s$ is irreducible and has Galois group S_4. There are infinitely many such pairs (r, s) (see, *e.g.*, Kappe and Warren [14]). Denote by $\alpha^{(1)} = \alpha, \alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}$ the roots of f and let $K := \mathbb{Q}(\alpha)$. Define

$$\begin{aligned}
\eta_1 &:= -(\alpha^{(1)} + \alpha^{(2)})(\alpha^{(3)} + \alpha^{(4)}) = (\alpha^{(1)} + \alpha^{(2)})^2, \\
\eta_2 &:= -(\alpha^{(1)} + \alpha^{(3)})(\alpha^{(2)} + \alpha^{(4)}) = (\alpha^{(1)} + \alpha^{(3)})^2, \\
\eta_3 &:= -(\alpha^{(1)} + \alpha^{(4)})(\alpha^{(2)} + \alpha^{(3)}) = (\alpha^{(1)} + \alpha^{(4)})^2.
\end{aligned}$$

Then

$$(X - \eta_1)(X - \eta_2)(X - \eta_3) = X^3 - 4rX^2 + 4sX - 1. \tag{1.4}$$

Take

$$\sqrt{\eta_1} = \alpha^{(1)} + \alpha^{(2)}, \ \sqrt{\eta_2} = \alpha^{(1)} + \alpha^{(3)}, \ \sqrt{\eta_3} = \alpha^{(1)} + \alpha^{(4)}.$$

Then

$$\sqrt{\eta_1} \cdot \sqrt{\eta_2} \cdot \sqrt{\eta_3} = 1. \tag{1.5}$$

By the Gauss-Fermat Theorem over number fields, there exists a positive integer t such that

$$\eta_1^t \equiv 1 \pmod 4. \tag{1.6}$$

Consider for $m = 0, 1, 2, \ldots$ the numbers

$$\alpha_m := \tfrac{1}{2}\left(\sqrt{\eta_1}^{1+2mt} + \sqrt{\eta_2}^{1+2mt} + \sqrt{\eta_3}^{1+2mt}\right),$$
$$\beta_m := \tfrac{1}{2}\left(\sqrt{\eta_1}^{-1-2mt} + \sqrt{\eta_2}^{-1-2mt} + \sqrt{\eta_3}^{-1-2mt}\right).$$

The numbers α_m are invariant under any automorphism that permutes $\alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}$, *i.e.*, under any automorphism that leaves K invariant, hence they belong to K. Further, they have four distinct conjugates, so $\mathbb{Q}(\alpha_m) = K$. Next, by (1.5),

$$\beta_m = \alpha_m^2 - r_m, \quad \alpha_m = \beta_m^2 - s_m,$$

where

$$r_m = \tfrac{1}{4}\left(\eta_1^{1+2mt} + \eta_2^{1+2mt} + \eta_3^{1+2mt}\right),$$
$$s_m = \tfrac{1}{4}\left(\eta_1^{-1-2mt} + \eta_2^{-1-2mt} + \eta_3^{-1-2mt}\right).$$

By (1.4),(1.6), r_m, s_m are rational integers, hence α_m, β_m are algebraic integers for every m. We thus obtain for every non-negative integer m an order $\mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$ of type II in K.

We claim that among the orders $\mathbb{Z}[\alpha_m]$ there are infinitely many distinct ones. Denote by D_m the discriminant of $\mathbb{Z}[\alpha_m]$. Then D_m is equal to the discriminant of α_m, and a straightforward computation shows that this is equal to the discriminant of η_1^{1+2mt}. By [8, Corollaire 2.2], we have $|D_m| \to \infty$ as $m \to \infty$. This implies our claim.

2. Application to canonical number systems

Let K be an algebraic number field of degree ≥ 2, and $\mathcal{O}$ an order in K. A nonzero element α in $\mathcal{O}$ is called a *basis of a canonical number system* (or CNS basis) for $\mathcal{O}$ if every nonzero element of $\mathcal{O}$ can be represented in the form

$$a_0 + a_1\alpha + \cdots + a_m\alpha^m$$

with $m \geq 0$, $a_i \in \{0, 1, \ldots, |N_{K/\mathbb{Q}}(\alpha)| - 1\}$ for $i = 0, \ldots, m$, and $a_m \neq 0$. Canonical number systems can be viewed as natural generalizations of radix representations of rational integers to algebraic integers.

When there exists a canonical number system in $\mathcal{O}$, then $\mathcal{O}$ is called a CNS *order*. Orders of this kind have been intensively investigated; we refer to the survey paper [2] and the references given there.

It was proved by Kovács [15] and Kovács and Pethő [16] that $\mathcal{O}$ is a CNS order if and only if $\mathcal{O}$ is monogenic. More precisely, if α is a CNS basis in $\mathcal{O}$, then it is easily seen that $\mathcal{O} = \mathbb{Z}[\alpha]$. Conversely, $\mathcal{O} = \mathbb{Z}[\alpha]$ does not imply in general that α is a CNS basis. However, in this case there are infinitely many α' which are $\mathbb{Z}$-equivalent to α such that α' is a CNS basis for $\mathcal{O}$. A characterization of CNS bases in $\mathcal{O}$ is given in [16].

The close connection between elements α of $\mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$ and CNS bases in $\mathcal{O}$ enables one to apply results concerning monogenic orders to CNS orders and CNS bases. The results presented in Section 1 have immediate applications of this type. For example, it follows that up to $\mathbb{Z}$-equivalence there are only finitely many canonical number systems in $\mathcal{O}$.

We say that $\mathcal{O}$ is a *k-times* CNS order if there are at least k pairwise $\mathbb{Z}$-inequivalent CNS bases in $\mathcal{O}$. Theorem 1.1 gives the following.

Corollary 2.1. *Let K be an algebraic number field of degree ≥ 3. Then there are at most finitely many three times CNS orders in K.*

3. Results over finitely generated domains

Let A be a domain with quotient field L of characteristic 0. Suppose that A is integrally closed, and that A is finitely generated over $\mathbb{Z}$ as a $\mathbb{Z}$-algebra. Let K be a finite extension of L of degree at least 3, A_K the integral closure of A in K, and $\mathcal{O}$ an A-order in K, that is a subring of A_K which contains A and which has quotient field K. Consider the equation

$$A[\alpha] = \mathcal{O} \quad \text{in } \alpha \in \mathcal{O}. \tag{3.1}$$

The solutions of this equation can be divided into A-equivalence classes, where two elements α, β of $\mathcal{O}$ are called *A-equivalent* if $\beta = u\alpha + a$ for some $a \in A$ and $u \in A^*$. Here A^* denotes the multiplicative group of invertible elements of A. As is known (see Roquette [19]), A^* is finitely generated.

It was proved by Győry [10] that the set of α with (3.1) is a union of finitely many A-equivalence classes. An explicit upper bound for the number of these A-equivalence classes has been derived by Evertse and Győry [5]. An effective version has been established by Győry for certain special types of domains [11].

We now formulate our generalizations of the results from the previous sections to A-orders. We call an A-order $\mathcal{O}$ *k times monogenic,* if equation (3.1) has at least k A-equivalence classes of solutions.

Theorem 3.1. *Let A be a domain with quotient field L of characteristic 0 which is integrally closed and finitely generated over $\mathbb{Z}$, and let K be a finite extension of L of degree ≥ 3. Then there are at most finitely many three times monogenic A-orders in K.*

We now turn to two times monogenic A-orders. Let again K be a finite extension of L of degree at least 3. We call $\mathcal{O}$ an A-order in K of **type I** if there are $\alpha, \beta \in \mathcal{O}$ and $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, L)$ such that

$$K = L(\alpha),\ \mathcal{O} = A[\alpha] = A[\beta],\ \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4},\ a_3 \neq 0. \tag{3.2}$$

It should be noted that in the previous section (with $L = \mathbb{Q}$, $A = \mathbb{Z}$) we had in our definition (1.2) of orders of type I the stronger requirement $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$ instead of $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Q})$. In fact, if A is a principal ideal domain, we can choose a_1, a_2, a_3, a_4 in (3.2) such that $a_1, a_2, a_3, a_4 \in A$ and the ideal generated by $a_1, \ldots, a_4$ equals A. In that case, according to Lemma 6.4 proved in Section 6 below, (3.2) implies that $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, A)$.

A-orders of type II exist only in extensions of L of degree 4. Thus, let K be an extension of L of degree 4. We call $\mathcal{O}$ an A-order in K of **type II** if there are $\alpha, \beta \in \mathcal{O}$ and $a_0, a_1, a_2, b_0, b_1, b_2 \in A$ with $a_0 b_0 \neq 0$, such that

$$\begin{aligned} &K = L(\alpha),\ \ \mathcal{O} = A[\alpha] = A[\beta], \\ &\beta = a_0\alpha^2 + a_1\alpha + a_2,\ \ \alpha = b_0\beta^2 + b_1\alpha + b_2. \end{aligned} \tag{3.3}$$

Theorem 3.2. *Let A be a domain with quotient field L of characteristic 0 which is integrally closed and finitely generated over $\mathbb{Z}$, and let K be a finite extension of L. Denote by G the normal closure of K over L.*

- **(i)** *Suppose $[K : L] = 3$. Then every two times monogenic A-order in K is of type I.*
- **(ii)** *Suppose $[K : L] = 4$ and $\mathrm{Gal}(G/L) \cong S_4$. Then there are only finitely many two times monogenic A-orders in K which are not of type I or type II.*
- **(iii)** *Suppose $[K : L] \geq 5$ and that K is four times transitive over L. Then there are only finitely many two times monogenic A-orders in K which are not of type I.*

4. Equations with unknowns from a finitely generated multiplicative group

The main tools in the proofs of Theorems 3.1 and 3.2 are finiteness results on polynomial equations of which the unknowns are taken from finitely generated multiplicative groups. In this section, we have collected what is needed. Below, G is a field of characteristic 0.

Lemma 4.1. *Let $a_1, a_2 \in G^*$ and let Γ be a finitely generated subgroup of G^*. Then the equation*

$$a_1 x_1 + a_2 x_2 = 1 \quad \text{in } x_1, x_2 \in \Gamma \tag{4.1}$$

has only finitely many solutions.

Proof. See Lang [17]. □

A pair $(a_1, a_2) \in (G^*)^2 = G^* \times G^*$ is called *normalized* if $(1, 1)$ is a solution to (4.1), *i.e.*, $a_1 + a_2 = 1$. If (4.1) has a solution, (y_1, y_2), say, then by replacing (a_1, a_2) by $(a_1 y_1, a_2 y_2)$ we obtain an equation like (4.1) with a normalized pair of coefficients, whose number of solutions is the same as that of the original equation.

Lemma 4.2. *Let Γ be a finitely generated subgroup of G^*. There is a finite set of normalized pairs in $(G^*)^2$, such that for every normalized pair $(a_1, a_2) \in (G^*)^2$ outside this set, equation* (4.1) *has at most two solutions, the pair* $(1, 1)$ *included.*

Proof. This result is due to Evertse, Győry, Stewart and Tijdeman [6]; see also [12]. We note that the proof depends ultimately on the Subspace Theorem, hence it is ineffective. □

We consider more generally polynomial equations

$$f(x_1, \ldots, x_n) = 0 \text{ in } x_1, \ldots, x_n \in \Gamma \tag{4.2}$$

where f is a non-zero polynomial from $G[X_1, \ldots, X_n]$ and Γ is a finitely generated subgroup of G^*. Denote by T an auxiliary variable. A solution $(x_1, \ldots, x_n)$ of (4.2) is called *degenerate*, if there are integers $c_1, \ldots, c_n$, not all zero, such that

$$f(x_1 T^{c_1}, \ldots, x_n T^{c_n}) \equiv 0 \text{ identically in } T, \tag{4.3}$$

and *non-degenerate* otherwise.

Lemma 4.3. *Let f be a non-zero polynomial from $G[X_1, \ldots, X_n]$ and Γ a finitely generated subgroup of G^*. Then equation* (4.2) *has only finitely many non-degenerate solutions.*

Proof. Given a multiplicative Abelian group H, we denote by H^n its n-fold direct product with componentwise multiplication.

Let V be the hypersurface given by $f = 0$. Notice that the degenerate solutions $\mathbf{x}$ are precisely those, for which there exists an algebraic subgroup H of $(G^*)^n$ of dimension ≥ 1 such that $\mathbf{x}H \subseteq V$. By a theorem of Laurent [18], the intersection $V \cap \Gamma^n$ is contained in a finite union of cosets $\mathbf{x}_1 H_1 \cup \cdots \cup \mathbf{x}_r H_r$ where $H_1, \ldots, H_r$ are algebraic subgroups of $(G^*)^n$, $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are elements of Γ^n, and $\mathbf{x}_i H_i \subseteq V$ for $i = 1, \ldots, r$. The non-degenerate solutions in our lemma are precisely the zero-dimensional cosets among $\mathbf{x}_1 H_1, \ldots, \mathbf{x}_r H_r$, while the degenerate solutions are in the union of the positive dimensional cosets. □

5. Finitely generated domains

We recall some facts about domains finitely generated over $\mathbb{Z}$.

Let A be an integrally closed domain with quotient field L of characteristic 0 which is finitely generated over $\mathbb{Z}$. Then A is a Noetherian domain. Moreover, A is a *Krull domain;* see *e.g.* Bourbaki [3], Chapter VII, Section 1. This means the following. Denote by $\mathcal{P}(A)$ the collection of minimal non-zero prime ideals of A, these are the non-zero prime ideals that do not contain a strictly smaller non-zero prime ideal. Then there exist normalized discrete valuations $\mathrm{ord}_{\mathfrak{p}}$ ($\mathfrak{p} \in \mathcal{P}(A)$) on L, such that the following conditions are satisfied:

$$\text{for every } x \in K^* \text{ there are only finitely many } \mathfrak{p} \in \mathcal{P}(A) \text{ with } \mathrm{ord}_{\mathfrak{p}}(x) \neq 0, \tag{5.1}$$

$$A = \left\{x \in K \ : \ \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for } \mathfrak{p} \in \mathcal{P}(A)\right\}, \tag{5.2}$$

$$\mathfrak{p} = \left\{x \in A \ : \ \mathrm{ord}_{\mathfrak{p}}(x) > 0\right\} \text{ for } \mathfrak{p} \in \mathcal{P}(A). \tag{5.3}$$

These valuations $\mathrm{ord}_{\mathfrak{p}}$ are uniquely determined. As is easily seen, for $x, y \in L^*$ we have

$$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(y) \text{ for all } \mathfrak{p} \in \mathcal{P}(A) \Longleftrightarrow xy^{-1} \in A^*. \tag{5.4}$$

Let G be a finite extension of L. Denote by A_G the integral closure of A in G, and by A_G^* the unit group, *i.e.*, group of invertible elements of A_G. We will apply the results from Section 4 with $\Gamma = A_G^*$. To this end, we need the following lemma.

Lemma 5.1. *The group A_G^* is finitely generated.*

Proof. The domain A_G is contained in a free A-module of rank $[G : L]$. Since A is Noetherian, the domain A_G is finitely generated as an A-module, and so it is finitely generated as an algebra over $\mathbb{Z}$. Then by a theorem of Roquette [19], the group A_G^* is finitely generated. □

6. Other auxiliary results

We have collected some elementary lemmas needed in the proofs of Theorems 3.1 and 3.2. Let A be an integrally closed domain with quotient field L of characteristic 0 which is finitely generated over $\mathbb{Z}$, and K a finite extension of L with $[K : L] =: d \geq 3$. Denote by G the normal closure of K over L. Let $\sigma_1 = \mathrm{id}, \ldots, \sigma_d$ be the distinct L-isomorphisms of K in G, and for $\alpha \in K$ write $\alpha^{(i)} := \sigma_i(\alpha)$ for $i = 1, \ldots, d$. Denote by A_K and A_G the integral closures of A in K and G, respectively, and by A_G^* the multiplicative group of invertible elements of A_G.

The *discriminant* of $\alpha \in K$ is given by

$$D_{K/L}(\alpha) := \prod_{1 \leq i < j \leq d} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2.$$

This is an element of L. We have $L(\alpha) = K$ if and only if all conjugates of α are distinct, hence if and only if $D_{K/L}(\alpha) \neq 0$. Further, if α is integral over A then $D_{K/L}(\alpha) \in A$ since A is integrally closed.

Lemma 6.1. *Let $\alpha, \beta \in A_K$ and suppose that $L(\alpha) = L(\beta) = K$, $A[\alpha] = A[\beta]$. Then*

(i) $\dfrac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \in A_G^*$ *for* $i, j \in \{1, \ldots, d\}$, $i \neq j$,

(ii) $\dfrac{D_{K/L}(\beta)}{D_{K/L}(\alpha)} \in A^*$.

Proof. (i) Let $i, j \in \{1, \ldots, d\}$, $i \neq j$. We have $\beta = f(\alpha)$ for some $f \in A[X]$. Hence

$$\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} = \frac{f(\alpha^{(i)}) - f(\alpha^{(j)})}{\alpha^{(i)} - \alpha^{(j)}} \in A_G.$$

Likewise $(\alpha^{(i)} - \alpha^{(j)})/(\beta^{(i)} - \beta^{(j)}) \in A_G$. This proves (i).
(ii) We have on the one hand, $D_{K/L}(\beta)/D_{K/L}(\alpha) \in L^*$, on the other hand

$$\frac{D_{K/L}(\beta)}{D_{K/L}(\alpha)} = \prod_{1 \leq i < j \leq d} \left(\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \right)^2 \in A_G^*.$$

Since A is integrally closed, this proves (ii). □

We call two elements α, β of K L-equivalent if $\beta = u\alpha + a$ for some $u \in L^*, a \in L$.

Lemma 6.2. *Let $\alpha, \beta \in A_K$ and suppose that $L(\alpha) = L(\beta) = K$, $A[\alpha] = A[\beta]$, and α, β are L-equivalent. Then α, β are A-equivalent.*

Proof. By assumption, $\beta = u\alpha + a$ with $u \in L^*, a \in L$. By the previous lemma, $u^{d(d-1)} = D_{K/L}(\beta)/D_{K/L}(\alpha) \in A^*$, and then $u \in A^*$ since A is integrally closed. Consequently, $a = \beta - u\alpha$ is integral over A. Hence $a \in A$. This shows that α, β are A-equivalent. □

For $\alpha \in K$ with $K = L(\alpha)$ we define the ordered $(d-2)$-tuple

$$\tau(\alpha) := \Big(\frac{\alpha^{(3)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}}, \ldots, \frac{\alpha^{(d)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}} \Big). \tag{6.1}$$

Lemma 6.3. **(i)** *Let α, β with $L(\alpha) = L(\beta) = K$. Then α, β are L-equivalent if and only if $\tau(\alpha) = \tau(\beta)$.*

(ii) *Let $\alpha, \beta \in A_K$ and suppose that $L(\alpha) = L(\beta) = K$, $A[\alpha] = A[\beta]$. Then α, β are A-equivalent if and only if $\tau(\alpha) = \tau(\beta)$.*

Proof. (i) If α, β are L-equivalent, then clearly $\tau(\alpha) = \tau(\beta)$. Assume conversely that $\tau(\alpha) = \tau(\beta)$. Then there are unique $u \in G^*, a \in G$ such that

$$(\beta^{(1)}, \dots, \beta^{(d)}) = u(\alpha^{(1)}, \dots, \alpha^{(d)}) + a(1, \dots, 1). \tag{6.2}$$

In fact, the unicity of u, a follows since thanks to our assumption $K = L(\alpha)$, the numbers $\alpha^{(1)}, \dots, \alpha^{(d)}$ are distinct. As for the existence, observe that (6.2) is satisfied with $u = (\beta^{(2)} - \beta^{(1)})/(\alpha^{(2)} - \alpha^{(1)}), a = \beta^{(1)} - u\alpha^{(1)}$.

Take σ from the Galois group Gal (G/L). Then $\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_d$ is a permutation of the L-isomorphisms $\sigma_1, \dots, \sigma_d : K \hookrightarrow G$. It follows that σ permutes $(\alpha^{(1)}, \dots, \alpha^{(d)})$ and $(\beta^{(1)}, \dots, \beta^{(d)})$ in the same way. So by applying σ to (6.2) we obtain

$$(\beta^{(1)}, \dots, \beta^{(d)}) = \sigma(u)(\alpha^{(1)}, \dots, \alpha^{(d)}) + \sigma(a)(1, \dots, 1).$$

By the unicity of u, a in (6.2) this implies $\sigma(u) = u$, $\sigma(a) = a$. This holds for every $\sigma \in$ Gal (G/L). So in fact $u \in L^*, a \in L$, that is, α, β are L-equivalent.

(ii) Use Lemma 6.2. □

We denote by $(a_1, \dots, a_r)$ the ideal of A generated by $a_1, \dots, a_r$.

Lemma 6.4. *Let $\alpha, \beta \in A_K$ with $L(\alpha) = L(\beta) = K$, $A[\alpha] = A[\beta]$. Suppose there is a matrix $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in$ GL(2, L) with*

$$\beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}, \quad a_3 \neq 0, \tag{6.3}$$

$$a_1, a_2, a_3, a_4 \in A, \quad (a_1, a_2, a_3, a_4) = (1). \tag{6.4}$$

Then $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in$ GL(2, A).

Remark. Let $\mathcal{O}$ be an A-order of type I, as defined in Section 3. Then there exist α, β with $\mathcal{O} = A[\alpha] = A[\beta]$, and a matrix $U := \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in$ GL(2, L) with (6.3). If A is a principal ideal domain then by taking a suitable scalar multiple of U we can arrange that (6.4) also holds, and thus, that $U \in$ GL(2, A).

Proof. Since $\alpha \in A_K$ and $L(\alpha) = K$, it has a monic minimal polynomial $f \in A[X]$ over L of degree d. Moreover, since $A[\beta] = A[\alpha]$, we have

$$\beta = r_0 + r_1\alpha + \cdots + r_{d-1}\alpha^{d-1} \text{ with } r_0, \dots, r_{d-1} \in A. \tag{6.5}$$

Hence

$$(a_3X + a_4)(r_{d-1}X^{d-1} + \cdots + r_0) - a_1X - a_2 = a_3r_{d-1}f(X). \tag{6.6}$$

Equating the coefficients, we see that

$$a_4r_0 - a_2 \in a_3r_{d-1}A, \quad a_4r_1 + a_3r_0 - a_1 \in a_3r_{d-1}A, \tag{6.7}$$

$$a_4r_j + a_3r_{j-1} \in a_3r_{d-1}A \ (j = 2, \dots, d-1). \tag{6.8}$$

We first prove that

$$a_3^{1-j} r_j \in A \text{ for } j = 1, \dots, d-1. \tag{6.9}$$

In fact, we prove by induction on i ($1 \le i \le d-1$), the assertion that $a_3^{1-j} r_j \in A$ for $j = 1, \dots, i$, and $a_3^{1-i} r_j \in A$ for $j = i+1, \dots, d-1$. For $i = 1$ this is clear. Let $2 \le i \le d-1$ and suppose that the assertion is true for $i-1$ instead of i. Then $s_j := a_3^{2-i} r_j \in A$ for $j = i, \dots, d-1$. Further, by (6.8), we have $a_4 s_j + a_3 s_{j-1} = z_j a_3 s_{d-1}$ with $z_j \in A$ for $j = i, \dots, d-1$. Next, by (6.7) we have $a_1, a_2 \in (a_3, a_4)$, and then $(a_3, a_4) = (1)$ by (6.4). That is, there are $x, y \in A$ with $x a_3 + y a_4 = 1$. Consequently, for $j = i, \dots, d-1$, we have

$$s_j = (x a_3 + y a_4) s_j = a_3 (x s_j + y(z_j s_{d-1} - s_{j-1})) \in a_3 A,$$

i.e., $a_3^{1-i} r_j = a_3^{-1} s_j \in A$. This completes our induction step, and completes the proof of (6.9).

Now define the binary form $F(X, Y) := Y^d f(X/Y)$. Then (6.6) implies

$$a_3 r_{d-1} F(X, Y) = (a_3 X + a_4 Y)(\cdots) - Y^{d-1}(a_1 X + a_2 Y).$$

Substituting $X = a_4,\ Y = -a_3$, and using (6.9), it follows that

$$F(a_4, -a_3) = s^{-1}(a_1 a_4 - a_2 a_3) \text{ with } s \in A. \tag{6.10}$$

Denote by $\alpha^{(1)}, \dots, \alpha^{(d)}$ the conjugates of α, and by $\beta^{(1)}, \dots, \beta^{(d)}$ the corresponding conjugates of β. Then for the discriminant of β we have, by (6.3), (6.10),

$$\begin{aligned} D_{K/L}(\beta) &= \prod_{1 \le i < j \le d} (\beta^{(i)} - \beta^{(j)})^2 \\ &= (a_1 a_4 - a_2 a_3)^{d(d-1)} \left(\prod_{i=1}^{d} (a_4 + a_3 \alpha^{(i)}) \right)^{-2d+2} \prod_{1 \le i < j \le d} (\alpha^{(i)} - \alpha^{(j)})^2 \\ &= (a_1 a_4 - a_2 a_3)^{d(d-1)} F(a_4, -a_3)^{-2d+2} D_{K/L}(\alpha) \\ &= s^{2d-2} (a_1 a_4 - a_2 a_3)^{(d-1)(d-2)} D_{K/L}(\alpha). \end{aligned}$$

On the other hand, by Lemma 6.1, (ii) we have $D_{K/L}(\beta)/D_{K/L}(\alpha) \in A^*$. Using also that A is integrally closed, it follows that $a_1 a_4 - a_2 a_3 \in A^*$. This completes our proof. □

7. Proof of Theorem 3.1

The proof splits into two parts. Consider $\beta \in A_K$ with $K = L(\beta)$. The first part, which is Lemma 7.1 below, implies that the set of β such that $A[\beta]$ is three times monogenic, is contained in a union of at most finitely many L-equivalence

classes. The second part, which is Lemma 7.2 below, implies that if $\mathcal{C}$ is a given L-equivalence class, then the set of $\beta \in \mathcal{C}$ such that $A[\beta]$ is two times monogenic, is in a union of at most finitely many A-equivalence classes. (Lemma 7.2 is used in the proof of Theorem 3.2 as well, therefore it deals with two times monogenic orders.) Any three times monogenic A-order in K can be expressed as $A[\beta]$. A combination of Lemmas 7.1 and 7.2 clearly yields that the set of such β lies in finitely many A-equivalence classes. Since A-equivalent β give rise to equal A-orders $A[\beta]$, there are only finitely many three times monogenic orders in K.

Lemma 7.1. *The set of β such that*

$$\beta \in A_K,\ L(\beta) = K,\quad A[\beta] \text{ is three times monogenic} \tag{7.1}$$

is contained in a union of at most finitely many L-equivalence classes.

Proof. Assume the contrary. Then there is an infinite sequence of triples $\{(\beta_{1p}, \beta_{2p}, \beta_{3p}) :\ p = 1, 2, \ldots\}$ such that

$$\beta_{hp} \in A_K,\ L(\beta_{hp}) = K \text{ for } h = 1, 2, 3,\ p = 1, 2, \ldots; \tag{7.2}$$

$$\beta_{1p}\ (p = 1, 2, \ldots) \text{ lie in different } L\text{-equivalence classes} \tag{7.3}$$

and for $p = 1, 2, \ldots,$

$$\begin{cases} A[\beta_{1p}] = A[\beta_{2p}] = A[\beta_{3p}], \\ \beta_{1p}, \beta_{2p}, \beta_{3p} \text{ lie in different } A\text{-equivalence classes} \end{cases} \tag{7.4}$$

(so the β_{1p} play the role of β in the statement of our lemma). For any three distinct indices i, j, k from $\{1, \ldots, d\}$, and for $h = 1, 2, 3$, $p = 1, 2, \ldots$, put

$$\beta_{hp}^{(ijk)} := \frac{\beta_{hp}^{(i)} - \beta_{hp}^{(j)}}{\beta_{hp}^{(i)} - \beta_{hp}^{(k)}}.$$

By (7.2), these numbers are well-defined and non-zero.

We start with some observations. Let i, j, k be any three distinct indices from $\{1, \ldots, d\}$. By Lemma 6.1 and the obvious identities $\beta_{hp}^{(ijk)} + \beta_{hp}^{(kji)} = 1$ $(h = 1, 2, 3)$, the pairs $(\beta_{hp}^{(ijk)}/\beta_{1p}^{(ijk)}, \beta_{hp}^{(kji)}/\beta_{1p}^{(kji)})$ $(h = 1, 2, 3)$ are solutions to

$$\beta_{1p}^{(ijk)} x + \beta_{1p}^{(kji)} y = 1 \text{ in } x, y \in A_G^*. \tag{7.5}$$

Notice that (7.5) has solution $(1, 1)$. So according to Lemmas 4.2, 5.1, there is a finite set $\mathcal{A}_{ijk}$ such that if $\beta_{1p}^{(ijk)} \notin \mathcal{A}_{ijk}$, then (7.5) has at most two solutions, including $(1, 1)$. In particular, there are at most two distinct pairs among $(\beta_{hp}^{(ijk)}/\beta_{1p}^{(ijk)}, \beta_{hp}^{(kji)}/\beta_{1p}^{(kji)})$ $(h = 1, 2, 3)$. Consequently,

$$\beta_{1p}^{(ijk)} \notin \mathcal{A}_{ijk} \Longrightarrow \text{two among } \beta_{1p}^{(ijk)}, \beta_{2p}^{(ijk)}, \beta_{3p}^{(ijk)} \text{ are equal.} \tag{7.6}$$

We start with the case $d = 3$. Then $\tau(\beta_{hp}) = (\beta_{hp}^{(132)})$ for $h = 1, 2, 3$. By (7.3) and Lemma 6.3,(i) the numbers $\beta_{1p}^{(132)}$ $(p = 1, 2, \ldots)$ are pairwise distinct. By (7.6) and Lemma 6.3,(ii), for all but finitely many p, two among the numbers $\beta_{hp}^{(132)}$ $(h = 1, 2, 3)$ are equal and hence two among β_{hp} $(h = 1, 2, 3)$ are A-equivalent which contradicts (7.4).

Now assume $d \geq 4$. We have to distinguish between subsets $\{i, j, k\}$ of $\{1, \ldots, d\}$ and indices h for which there are infinitely many distinct numbers among $\beta_{hp}^{(ijk)}$ $(p = 1, 2, \ldots)$, and $\{i, j, k\}$ and h for which among these numbers there are only finitely many distinct ones. This does not depend on the choice of ordering of i, j, k, since any permutation of (i, j, k) transforms $\beta_{hp}^{(ijk)}$ into one of $(\beta_{hp}^{(ijk)})^{-1}$, $1 - \beta_{hp}^{(ijk)}$, $(1 - \beta_{hp}^{(ijk)})^{-1}$, $1 - (\beta_{hp}^{(ijk)})^{-1}$, $(1 - (\beta_{hp}^{(ijk)})^{-1})^{-1}$.

By assumption (7.3) and Lemma 6.3,(i), the tuples $\tau(\beta_{1p}) = (\beta_{1p}^{(132)}, \ldots, \beta_{1p}^{(1d2)})$ $(p = 1, 2, \ldots)$ are all distinct. Hence one of the sets $\{1, 2, 3\}, \ldots, \{1, 2, d\}$, say $\{i, j, k\}$, is such that there are infinitely many distinct numbers among $\beta_{1p}^{(ijk)}$ $(p = 1, 2, \ldots)$. Choose an infinite subsequence of indices p such that the numbers $\beta_{1p}^{(ijk)}$ are pairwise distinct. Suppose there is another subset $\{i', j', k'\} \neq \{i, j, k\}$ such that if p runs through the infinite subsequence just chosen, then $\beta_{1p}^{(i'j'k')}$ runs through an infinite set. Then for some infinite subsequence of these p, the numbers $\beta_{1p}^{(i'j'k')}$ are pairwise distinct. Continuing in this way, we infer that there is a non-empty collection $\mathcal{S}$ of 3-element subsets $\{i, j, k\}$ of $\{1, \ldots, d\}$, and an infinite sequence $\mathcal{P}$ of indices p, such that for each $\{i, j, k\} \in \mathcal{S}$ the numbers $\beta_{1p}^{(ijk)}$ $(p \in \mathcal{P})$ are pairwise distinct, while for each $\{i, j, k\} \notin \mathcal{S}$, there are only finitely many distinct elements among $\beta_{1p}^{(ijk)}$ $(p \in \mathcal{P})$.

Notice that if $\{i, j, k\} \notin \mathcal{S}$, then among the equations (7.5) with $p \in \mathcal{P}$, there are only finitely many distinct ones, and by Lemmas 4.1, 5.1, each of these equations has only finitely many solutions. Therefore, there are only finitely many distinct numbers among $\beta_{hp}^{(ijk)}/\beta_{1p}^{(ijk)}$ hence only finitely many among $\beta_{hp}^{(ijk)}$ $(h = 2, 3,$ $p \in \mathcal{P})$. Conversely, if $\{i, j, k\} \in \mathcal{S}$, $h \in \{2, 3\}$, there are infinitely many distinct numbers among $\beta_{hp}^{(ijk)}$ $(p \in \mathcal{P})$. For if not, then by the same argument, interchanging the roles of β_{hp}, β_{1p}, it would follow that there are only finitely many distinct numbers among $\beta_{1p}^{(ijk)}$ $(p \in \mathcal{P})$, contradicting $\{i, j, k\} \in \mathcal{S}$.

We conclude that there is an infinite subsequence of p, which after renaming we may assume to be $1, 2, \ldots$, such that for $h = 1, 2, 3$,

$$\beta_{hp}^{(ijk)} \ (p = 1, 2, \ldots) \text{ are pairwise distinct if } \{i, j, k\} \in \mathcal{S}, \tag{7.7}$$

$$\begin{aligned} &\text{there are only finitely many distinct numbers among} \\ &\beta_{hp}^{(ijk)} \ (p = 1, 2, \ldots) \text{ if } \{i, j, k\} \notin \mathcal{S}. \end{aligned} \tag{7.8}$$

Notice that this characterization of $\mathcal{S}$ is symmetric in β_{hp} ($h = 1, 2, 3$); this will be used frequently.

We frequently use the following property of $\mathcal{S}$: if i, j, k, l are any four distinct indices from $\{1, \dots, d\}$, then

$$\{i, j, k\} \in \mathcal{S} \Longrightarrow \{i, j, l\} \in \mathcal{S} \text{ or } \{i, k, l\} \in \mathcal{S}. \tag{7.9}$$

Indeed, if $\{i, j, l\}, \{i, k, l\} \notin \mathcal{S}$ then also $\{i, j, k\} \notin \mathcal{S}$ since $\beta_{hp}^{(ijk)} = \beta_{hp}^{(ijl)}/\beta_{hp}^{(ikl)}$.

Pick a set from $\mathcal{S}$, which without loss of generality we may assume to be $\{1, 2, 3\}$. By (7.9), for $k = 4, \dots, d$ at least one of the sets $\{1, 2, k\}$, $\{1, 3, k\}$ belongs to $\mathcal{S}$. Define the set of pairs

$$\mathcal{C} := \Big\{(j, k) : \ j \in \{2, 3\}, \ k \in \{3, \dots, d\}, \ j \neq k, \ \{1, j, k\} \in \mathcal{S}\Big\}. \tag{7.10}$$

Thus, for each $k \in \{3, \dots, d\}$ there is j with $(j, k) \in \mathcal{C}$. Further, for every $p = 1, 2, \dots$ there is a pair $(j, k) \in \mathcal{C}$ such that

$$\beta_{1p}^{(1jk)} \neq \beta_{2p}^{(1jk)}.$$

Indeed, if this were not the case, then since $\beta_{hp}^{(12k)} = \beta_{hp}^{(13k)}\beta_{hp}^{(123)}$, it would follow that for some p,

$$\beta_{1p}^{(12k)} = \beta_{2p}^{(12k)} \text{ for } k = 3, \dots, d,$$

and then $\tau(\beta_{1p}) = \tau(\beta_{2p})$. Together with Lemma 6.3,(ii) this would imply that β_{1p}, β_{2p} are A-equivalent, contrary to (7.4). Clearly, there is a pair $(j, k) \in \mathcal{C}$ such that $\beta_{1p}^{(1jk)} \neq \beta_{2p}^{(1jk)}$ for infinitely many p. After interchanging the indices 2 and 3 if $j = 3$ and then permuting the indices $3, \dots, d$, which does not affect the above argument, we may assume that $j = 2, k = 3$. That is, we may assume that $\{1, 2, 3\} \in \mathcal{S}$ and

$$\beta_{1p}^{(123)} \neq \beta_{2p}^{(123)} \text{ for infinitely many } p.$$

We now bring (7.6) into play. It implies that for infinitely many p we have $\beta_{3p}^{(123)} \in \{\beta_{1p}^{(123)}, \beta_{2p}^{(123)}\}$. After interchanging β_{1p}, β_{2p} (which does not affect the definition of $\mathcal{S}$ or the above arguments) we may assume that $\{1, 2, 3\} \in \mathcal{S}$ and

$$\beta_{1p}^{(123)} = \beta_{3p}^{(123)} \neq \beta_{2p}^{(123)} \tag{7.11}$$

for infinitely many p.

We repeat the above argument. After renaming again, we may assume that the above infinite sequence of indices p for which (7.11) is true is $p = 1, 2, \dots$, and thus, (7.7) and (7.8) are true again. Define again the set $\mathcal{C}$ by (7.10). Similarly as above, we conclude that there is a pair $(j, k) \in \mathcal{C}$ such that among $p = 1, 2, \dots$ there is an infinite subset with $\beta_{1p}^{(1jk)} \neq \beta_{3p}^{(1jk)}$. Then necessarily, $k \neq 3$. After interchanging 2 and 3 if $j = 3$ (which does not affect (7.11)) and rearranging the other

indices $4, \dots, d$, we may assume that $j = 2, k = 4$. Thus, $\{1, 2, 3\}, \{1, 2, 4\} \in \mathcal{S}$ and there are infinitely many p for which we have (7.11) and

$$\beta_{1p}^{(124)} \neq \beta_{3p}^{(124)}.$$

By (7.6), for all but finitely many of these p we have $\beta_{2p}^{(124)} \in \{\beta_{1p}^{(124)}, \beta_{3p}^{(124)}\}$. After interchanging β_{1p}, β_{3p} if necessary, which does not affect (7.11), we may conclude that $\{1, 2, 3\}, \{1, 2, 4\} \in \mathcal{S}$ and there are infinitely many p with (7.11) and

$$\beta_{1p}^{(124)} = \beta_{2p}^{(124)} \neq \beta_{3p}^{(124)}. \tag{7.12}$$

Next, by (7.9), at least one of $\{1, 3, 4\}, \{2, 3, 4\}$ belongs to $\mathcal{S}$. Relations (7.11), (7.12) remain unaffected if we interchange $\beta_{hp}^{(1)}$ and $\beta_{hp}^{(2)}$, so without loss of generality, we may assume that $\{1, 3, 4\} \in \mathcal{S}$. By (7.6), for all but finitely many of the p with (7.11) and (7.12), at least two among the numbers $\beta_{hp}^{(134)}$ $(h = 1, 2, 3)$ must be equal. Using (7.11), (7.12) and $\beta_{hp}^{(134)} = \beta_{hp}^{(124)}/\beta_{hp}^{(123)}$, it follows that $\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\} \in \mathcal{S}$ and for infinitely many p we have (7.11), (7.12) and

$$\beta_{2p}^{(134)} = \beta_{3p}^{(134)} \neq \beta_{1p}^{(134)}. \tag{7.13}$$

We now show that this is impossible. For convenience we introduce the notation

$$\tilde{\beta}_{hp}^{(i)} := \frac{\beta_{hp}^{(i)} - \beta_{hp}^{(4)}}{\beta_{hp}^{(3)} - \beta_{hp}^{(4)}} = \beta_{hp}^{(4i3)}$$

for $h = 1, 2, 3$, $i = 1, 2, 3, 4$, $p = 1, 2, \dots$. Notice that $\tilde{\beta}_{hp}^{(3)} = 1$, $\tilde{\beta}_{hp}^{(4)} = 0$, and $\beta_{hp}^{(ijk)} = \frac{\tilde{\beta}_{hp}^{(i)} - \tilde{\beta}_{hp}^{(j)}}{\tilde{\beta}_{hp}^{(i)} - \tilde{\beta}_{hp}^{(k)}}$ for any distinct $i, j, k \in \{1, 2, 3, 4\}$. Thus, (7.11)–(7.13) translate into

$$\frac{\tilde{\beta}_{1p}^{(1)} - \tilde{\beta}_{1p}^{(2)}}{\tilde{\beta}_{1p}^{(1)} - 1} = \frac{\tilde{\beta}_{3p}^{(1)} - \tilde{\beta}_{3p}^{(2)}}{\tilde{\beta}_{3p}^{(1)} - 1} \neq \frac{\tilde{\beta}_{2p}^{(1)} - \tilde{\beta}_{2p}^{(2)}}{\tilde{\beta}_{2p}^{(1)} - 1}, \tag{7.14}$$

$$\frac{\tilde{\beta}_{1p}^{(1)} - \tilde{\beta}_{1p}^{(2)}}{\tilde{\beta}_{1p}^{(1)}} = \frac{\tilde{\beta}_{2p}^{(1)} - \tilde{\beta}_{2p}^{(2)}}{\tilde{\beta}_{2p}^{(1)}} \neq \frac{\tilde{\beta}_{3p}^{(1)} - \tilde{\beta}_{3p}^{(2)}}{\tilde{\beta}_{3p}^{(1)}}, \tag{7.15}$$

$$\frac{\tilde{\beta}_{2p}^{(1)} - 1}{\tilde{\beta}_{2p}^{(1)}} = \frac{\tilde{\beta}_{3p}^{(1)} - 1}{\tilde{\beta}_{3p}^{(1)}} \neq \frac{\tilde{\beta}_{1p}^{(1)} - 1}{\tilde{\beta}_{1p}^{(1)}}. \tag{7.16}$$

We distinguish between the cases $\{2, 3, 4\} \in \mathcal{S}$ and $\{2, 3, 4\} \notin \mathcal{S}$.

First suppose that $\{2, 3, 4\} \in \mathcal{S}$. Then by (7.6), there are infinitely many p such that (7.14)–(7.16) hold and at least two among $\tilde{\beta}_{hp}^{(2)} = \beta_{hp}^{(423)}$ $(h = 1, 2, 3)$ are

equal. But this is impossible, since (7.14),(7.15) imply $\tilde{\beta}_{1p}^{(2)} \neq \tilde{\beta}_{2p}^{(2)}$; (7.14),(7.16) imply $\tilde{\beta}_{1p}^{(2)} \neq \tilde{\beta}_{3p}^{(2)}$; and (7.15),(7.16) imply $\tilde{\beta}_{2p}^{(2)} \neq \tilde{\beta}_{3p}^{(2)}$.

Hence $\{2, 3, 4\} \notin \mathcal{S}$. This means that there are only finitely many distinct numbers among $\tilde{\beta}_{hp}^{(2)} = \beta_{hp}^{(423)}$, $(h = 1, 2, 3,\ p = 1, 2, \ldots)$. It follows that there are (necessarily non-zero) constants c_1, c_2, c_3 such that $\tilde{\beta}_{hp}^{(2)} = c_h$ for $h = 1, 2, 3$ and infinitely many p. By (7.16), (7.15), respectively, we have for all these p that $\tilde{\beta}_{2p}^{(1)} = \tilde{\beta}_{3p}^{(1)}$ and $\tilde{\beta}_{2p}^{(1)} = (c_2/c_1)\tilde{\beta}_{1p}^{(1)}$. By substituting this into (7.14), we get

$$\frac{\tilde{\beta}_{1p}^{(1)} - c_1}{\tilde{\beta}_{1p}^{(1)} - 1} = \frac{c_2\tilde{\beta}_{1p}^{(1)} - c_1c_3}{c_2\tilde{\beta}_{1p}^{(1)} - c_1}.$$

By (7.14), (7.16) we have $c_1 \neq c_3$, hence

$$\tilde{\beta}_{1p}^{(1)} = \beta_{1p}^{(413)} = \frac{c_1(c_1 - c_3)}{c_1c_2 + c_1 - c_2 - c_1c_3}$$

is a constant independent of p. But this contradicts $\{1, 3, 4\} \in \mathcal{S}$ and (7.7).

So our assumption that Lemma 7.1 is false leads in all cases to a contradiction. This completes our proof. □

Lemma 7.2. *Let $\mathcal{C}$ be an L-equivalence class in K. Then the set of β such that*

$$\beta \in A_K \cap \mathcal{C},\ L(\beta) = K, \quad A[\beta] \text{ is two times monogenic} \tag{7.17}$$

is contained in a union of at most finitely many A-equivalence classes.

Remark. As mentioned before, Lemma 7.2 is used also in the proof of Theorem 3.2. Our proof of Lemma 7.2 does not enable to estimate the number of A-equivalence classes. It is for this reason that we can not prove quantitative versions of Theorems 3.1 and 3.2.

Proof. We assume that the set of β with (7.17) is not contained in a union of finitely many A-equivalence classes and derive a contradiction.

Pick β with (7.17). Then there exist numbers α such that $A[\alpha] = A[\beta]$ and α is not A-equivalent to β. Consider such α. Then from the identities

$$\frac{\alpha^{(i)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}} + \frac{\alpha^{(2)} - \alpha^{(i)}}{\alpha^{(2)} - \alpha^{(1)}} = 1 \quad (i = 3, \ldots, d)$$

and Lemma 6.1 it follows that the pairs

$$\left(\frac{\alpha^{(i)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}}, \frac{\alpha^{(2)} - \alpha^{(i)}}{\alpha^{(2)} - \alpha^{(1)}}\right) \quad (i = 3, \ldots, d) \tag{7.18}$$

satisfy

$$x + y = 1 \quad \text{in } x, y \in \Gamma,$$

where Γ is the multiplicative group generated by A_G^* and the numbers

$$\frac{\beta^{(i)} - \beta^{(1)}}{\beta^{(2)} - \beta^{(1)}}, \ \frac{\beta^{(2)} - \beta^{(i)}}{\beta^{(2)} - \beta^{(1)}} \ (i = 3, \ldots, d).$$

By Lemma 6.3,(i), the group Γ depends only on the given L-equivalence class $\mathcal{C}$ and is otherwise independent of β. By Lemma 5.1, the group Γ is finitely generated, and then by Lemma 4.1, the pairs (7.18) belong to a finite set depending only on Γ, hence only on $\mathcal{C}$. Therefore, the tuple $\tau(\alpha)$ belongs to a finite set depending only on $\mathcal{C}$. In view of Lemma 6.3,(i), this means that α belongs to a union of finitely many L-equivalence classes which depends on $\mathcal{C}$ but is otherwise independent of β. Now by Dirichlet's box principle, there is an L-equivalence class $\mathcal{C}'$ with the following property: the set of β such that

$$\begin{cases} \beta \in A_K, \ L(\beta) = K, \ \beta \in \mathcal{C}, \\ \text{there is } \alpha \in \mathcal{C}' \text{ such that } A[\alpha] = A[\beta] \\ \text{and } \alpha \text{ is not } A\text{-equivalent to } \beta \end{cases} \tag{7.19}$$

cannot be contained in a union of finitely many A-equivalence classes.

Fix β_0 with (7.19) and then fix α_0 such that $A[\alpha_0] = A[\beta_0]$, $\alpha_0 \in \mathcal{C}'$ and α_0 is not A-equivalent to β_0.

Let β be an arbitrary number with (7.19). Choose α such that $A[\alpha] = A[\beta]$, $\alpha \in \mathcal{C}'$ and α is not A-equivalent to β. Then there are $u, u' \in L^*$, $a, a' \in L$ with

$$\beta = u\beta_0 + a, \ \ \alpha = u'\alpha_0 + a'. \tag{7.20}$$

For these u, u' we have

$$D_{K/L}(\beta) = u^{d(d-1)} D_{K/L}(\beta_0), \quad D_{K/L}(\alpha) = u'^{d(d-1)} D_{K/L}(\alpha_0). \tag{7.21}$$

On the other hand, it follows from $A[\alpha_0] = A[\beta_0]$, $A[\alpha] = A[\beta]$ and Lemma 6.1 (ii) that $D_{K/L}(\beta)/D_{K/L}(\alpha) \in A^*$ and $D_{K/L}(\beta_0)/D_{K/L}(\alpha_0) \in A^*$. Combined with (7.21) and our assumption that A is integrally closed, this gives

$$u'/u \in A^*. \tag{7.22}$$

Since $L(\beta_0) = K$ and $\alpha_0 \in A[\beta_0]$ there is a unique polynomial $F_0 \in L[X]$ of degree $< d$, which in fact belongs to $A[X]$, such that $\alpha_0 = F_0(\beta_0)$. Likewise, there is a unique polynomial $F \in L[X]$ of degree $< d$ which in fact belongs to $A[X]$, such that $\alpha = F(\beta)$. Inserting (7.20), it follows that $F(X) = u'F_0\left((X - a)/u\right) + a'$. Suppose that $F_0 = \sum_{j=0}^{m} a_j X^j$ with $m < d$ and $a_m \neq 0$. Then F has leading coefficient $a_m u' u^{-m}$ which belongs to A. Together with (7.22) this implies

$$u^{1-m} a_m \in A. \tag{7.23}$$

Further, by (7.21)

$$u^{d(d-1)} D_{K/L}(\beta_0) = D_{K/L}(\beta) \in A. \tag{7.24}$$

We distinguish between the cases $m > 1$ and $m = 1$. First let $m > 1$. We have shown that every β with (7.19) can be expressed as $\beta = u\beta_0 + a$ with $u \in L^*$, $a \in L$ and moreover, u satisfies (7.23), (7.24). Hence

$$-\frac{\mathrm{ord}_{\mathfrak{p}}(D_{K/L}(\beta_0))}{d(d-1)} \le \mathrm{ord}_{\mathfrak{p}}(u) \le \frac{\mathrm{ord}_{\mathfrak{p}}(a_m)}{m-1} \text{ for } \mathfrak{p} \in \mathcal{P}(A),$$

where $\mathcal{P}(A)$ is the collection of minimal non-zero prime ideals of A and $\mathrm{ord}_{\mathfrak{p}}$ ($\mathfrak{p} \in \mathcal{P}(A)$) are the associated discrete valuations, as explained in Section 5. Thus, for the tuple $v(u) := (\mathrm{ord}_{\mathfrak{p}}(u) : \mathfrak{p} \in \mathcal{P}(A))$ we have only finitely many possibilities.

We partition the set of β with (7.19) into a finite number of classes according to the tuple $v(u)$. Let $\beta_1 = u_1\beta_0 + a_1$, $\beta_2 = u_2\beta_0 + a_2$ belong to the same class, where $u_1, u_2 \in L^*$ and $a_1, a_2 \in L$. Then $v(u_1) = v(u_2)$ and so, $u_1 u_2^{-1} \in A^*$ by (5.4). Hence $\beta_2 = v\beta_1 + b$ with $v \in A^*$ and $b \in L$. But $b = \beta_2 - v\beta_1$ is integral over A, hence belongs to A since A is integrally closed. So two elements with (7.19) belonging to the same class are A-equivalent. But then, the set of β with (7.19) is contained in a union of finitely many A-equivalence classes, which is against our assumption.

Now assume that $m = 1$. Then

$$\alpha_0 = a_1\beta_0 + a_0 \quad \text{with } a_1 \in A \setminus \{0\},\ a_0 \in A,$$

hence $a_1^{d(d-1)} = D_{K/L}(\alpha_0)/D_{K/L}(\beta_0)$. By Lemma 6.1 (ii) we have $a_1^{d(d-1)} \in A^*$, and then $a_1 \in A^*$ since by assumption A is integrally closed. Hence α_0, β_0 are A-equivalent, which is against our choice of α_0, β_0. We arrive again at a contradiction.

Consequently, our initial assumption that the set of β with (7.17) cannot be contained in finitely many A-equivalence classes leads to a contradiction. This proves Lemma 7.2. □

Now our proof of Theorem 3.1 is complete.

8. Reduction of Theorem 3.2 to a polynomial unit equation

We keep the assumptions and notation from the previous sections. In particular, A is an integrally closed domain with quotient field L of characteristic 0 which is finitely generated over $\mathbb{Z}$ and K is a finite extension of L. Further, we denote by G the normal closure of K over L. As it will turn out, the proof of part (i) of Theorem 3.2 is elementary. Therefore, in this section we assume that $[K : L] =: d \ge 4$. Let $\mathcal{O} = A[\alpha] = A[\beta]$ be a two times monogenic A-order in K, where α, β are not A-equivalent.

By Lemma 6.1,(i) we have

$$\varepsilon_{ij} := \frac{\alpha^{(i)} - \alpha^{(j)}}{\beta^{(i)} - \beta^{(j)}} \in A_G^* \text{ for } i, j = 1, \ldots, d,\ i \ne j, \tag{8.1}$$

where A_G^* is the unit group of the integral closure of A in G. Let i, j, k be any three distinct indices from $\{1, \dots, d\}$. By Lemma 6.1, the identity

$$\frac{\beta^{(j)} - \beta^{(i)}}{\beta^{(j)} - \beta^{(k)}} + \frac{\beta^{(i)} - \beta^{(k)}}{\beta^{(j)} - \beta^{(k)}} = 1$$

and a similar identity for α, the two pairs $(1, 1)$ and $(\varepsilon_{ij}/\varepsilon_{jk}, \varepsilon_{ik}/\varepsilon_{jk})$ satisfy

$$\frac{\beta^{(j)} - \beta^{(i)}}{\beta^{(j)} - \beta^{(k)}} \cdot x + \frac{\beta^{(i)} - \beta^{(k)}}{\beta^{(j)} - \beta^{(k)}} \cdot y = 1 \quad \text{in } x, y \in A_G^*. \tag{8.2}$$

Now a straightforward computation gives

$$\frac{\varepsilon_{ik}}{\varepsilon_{jk}} - 1 = \frac{\beta^{(i)} - \beta^{(j)}}{\beta^{(i)} - \beta^{(k)}} \cdot \left(\frac{\varepsilon_{ij}}{\varepsilon_{jk}} - 1 \right). \tag{8.3}$$

This is valid for any three distinct indices i, j, k. Now take four distinct indices i, j, k, l from $\{1, \dots, d\}$. By applying (8.3) but with the respective triples (i, j, k), (i, k, l), (i, l, j) replacing (i, j, k), and taking the product, the terms with the conjugates of β disappear, and we obtain

$$\left(\frac{\varepsilon_{ik}}{\varepsilon_{jk}} - 1 \right) \left(\frac{\varepsilon_{il}}{\varepsilon_{kl}} - 1 \right) \left(\frac{\varepsilon_{ij}}{\varepsilon_{jl}} - 1 \right) = \left(\frac{\varepsilon_{ij}}{\varepsilon_{jk}} - 1 \right) \left(\frac{\varepsilon_{ik}}{\varepsilon_{kl}} - 1 \right) \left(\frac{\varepsilon_{il}}{\varepsilon_{jl}} - 1 \right). \tag{8.4}$$

In the remainder of this section we focus on the equation

$$(x_1 - 1)(x_2 - 1)(x_3 - 1) = (y_1 - 1)(y_2 - 1)(y_3 - 1) \quad \text{in } x_1, x_2, x_3, y_1, y_2, y_3 \in \Gamma \tag{8.5}$$

where Γ is a finitely generated multiplicative group, contained in a field of characteristic 0. As we just observed, the tuple

$$\left(\frac{\varepsilon_{ik}}{\varepsilon_{jk}}, \frac{\varepsilon_{il}}{\varepsilon_{kl}}, \frac{\varepsilon_{ij}}{\varepsilon_{jl}}, \frac{\varepsilon_{ij}}{\varepsilon_{jk}}, \frac{\varepsilon_{ik}}{\varepsilon_{kl}}, \frac{\varepsilon_{il}}{\varepsilon_{jl}} \right) \tag{8.6}$$

is a solution to (8.5) with $\Gamma = A_G^*$. Recall that by Lemma 5.1, the group A_G^* is finitely generated.

We prove the following Proposition concerning (8.5).

Proposition 8.1. *Let G be a field of characteristic 0 and Γ a finitely generated subgroup of G^*. Then there is a finite subset $\mathcal{S}$ of Γ with $1 \in \mathcal{S}$ such that for every solution $(x_1, \dots, y_3) \in \Gamma^6$ of (8.5), at least one of the following holds:*

- **(i)** *at least one of $x_1, \dots, y_3$ belongs to $\mathcal{S}$;*
- **(ii)** *there are $\eta_1, \eta_2, \eta_3 \in \{\pm 1\}$ such that (y_1, y_2, y_3) is a permutation of $(x_1^{\eta_1}, x_2^{\eta_2}, x_3^{\eta_3})$;*

(iii) *one of the numbers in* $\{x_i x_j,\ x_i/x_j,\ y_i y_j,\ y_i/y_j : 1 \le i < j \le 3\}$ *is equal to either* -1*, or to a primitive cube root of unity.*

We remark here that case (iii) may occur. For instance, let $i^2 = -1$, let ρ denote a primitive cube root of unity, and assume that $i, \rho \in \Gamma$. Then for every $u \in \Gamma$, the tuple $(u^6, iu^3, -iu^3, u^4, \rho u^4, \rho^2 u^4)$ satisfies (8.5). There are various other such infinite families of solutions. Proposition 8.1 contains only the information needed for the proof of Theorem 3.2.

Proposition 8.1 is deduced from the following lemma. Here and below, T is an auxiliary variable, and by $\equiv$ we indicate that an identity holds identically in T.

Lemma 8.2. *Let* G, Γ *be as in Proposition 8.1. Let* m, n *be non-negative integers with* $m + n > 0$*. Then there is a finite subset* $\mathcal{T}$ *of* Γ *with* $1 \in \mathcal{T}$ *such that for every solution* $(x_1, \dots, x_m,\ y_1, \dots, y_n, z) \in \Gamma^{m+n+1}$ *of*

$$(1 - x_1) \cdots (1 - x_m) = z(1 - y_1) \cdots (1 - y_n), \tag{8.7}$$

at least one of the following holds:

(i) *at least one of* $x_1, \dots, y_n$ *belongs to* $\mathcal{T}$*;*

(ii) *there are integers* $c_1, \dots, c_m,\ d_1, \dots, d_n, e$ *with* $c_1 \cdots c_m d_1 \cdots d_n \neq 0$*, such that*

$$(1 - x_1 T^{c_1}) \cdots (1 - x_m T^{c_m}) \equiv z T^e (1 - y_1 T^{d_1}) \cdots (1 - y_n T^{d_n}). \tag{8.8}$$

Proof. We proceed by induction on $m + n$. For $m = 1, n = 0$, say, our assertion is a simple consequence of the fact that the equation $1 - x_1 = z$ has only finitely many solutions in $x_1, z \in \Gamma$. Let $p \ge 2$, and suppose that the lemma is true for all pairs of non-negative integers m, n with $m + n < p$. Take non-negative integers m, n with $m + n = p$. By Lemma 4.3, for all but finitely many solutions $(x_1, \dots, y_n, z) \in \Gamma^{m+n+1}$ of (8.7) with $x_i \neq 1$ for $i = 1, \dots, m$, $y_j \neq 1$ for $j = 1, \dots, n$, there are integers $c_1, \dots, d_n, e$, not all 0, such that (8.8) holds, but some of $c_1, \dots, c_m, d_1, \dots, d_n$ may be zero. Notice that (8.8) cannot hold with $e \neq 0$ and all c_i, d_j equal to 0. Fix a solution $(x_1, \dots, y_n, z)$ satisfying (8.8) where some of the c_i, d_j are 0, and put $I := \{i : c_i \neq 0\}$, $I^c := \{1, \dots, m\} \setminus I$, $J := \{j : d_j \neq 0\}$, $J^c := \{1, \dots, n\} \setminus J$. Then at least one of I, J is non-empty.

For $i \in I$, put $a_i := |c_i|$ and $u_i := x_i^{\pm 1}$ with $u_i^{a_i} = x_i^{-c_i}$. Likewise, for $j \in J$, put $b_j := |d_j|$, and $v_j := y_j^{\pm 1}$ such that $v_j^{b_j} = y_j^{-d_j}$. Then (8.7) implies that

$$\prod_{i \in I} (T^{a_i} - u_i) \cdot \prod_{i \in I^c} (1 - x_i) \equiv z' T^f \prod_{j \in J} (T^{b_j} - v_j) \cdot \prod_{j \in I^c} (1 - y_j)$$

with $z' \in \Gamma$, $f \in \mathbb{Z}$. Since both sides of this identity must be polynomials with equal leading coefficients, we have $f = 0$, and

$$\prod_{i \in I^c} (1 - x_i) = z' \prod_{j \in I^c} (1 - y_j). \tag{8.9}$$

By combining this with (8.8) we obtain

$$\prod_{i\in I}(1 - T^{c_i}x_i) \equiv z''T^e \prod_{j\in J}(1 - T^{d_j}y_j), \tag{8.10}$$

where $z'z'' = z$. Recall that all but finitely many solutions of (8.7) satisfy both (8.9), (8.10).

We apply the induction hypothesis to (8.9). Notice that $|I^c| + |J^c| < m + n$ since at least one of the sets I, J is non-empty. It follows that there exists a finite set $\mathcal{T}'$ with $1 \in \mathcal{T}'$ such that for every tuple $(x_i : i \in I^c;\ y_j : j \in J^c; z')$ with entries from Γ, satisfying (8.9), either one of the x_i $(i \in I^c)$ or y_j $(j \in J^c)$ belongs to $\mathcal{T}'$, or there are integers c_i $(i \in I^c)$, d_j : $(j \in J^c)$, e' with $\prod_{i\in I^c} c_i \prod_{j\in J^c} d_j \neq 0$ such that

$$\prod_{i\in I^c}(1 - x_iT^{c_i}) \equiv z'T^{e'} \prod_{j\in I^c}(1 - y_jT^{d_j}).$$

By multiplying this with (8.10), we obtain an identity of the type (8.8) where none of the c_i, d_j are 0. All solutions $(x_1, \dots, x_m;\ y_1, \dots, y_n;\ z) \in \Gamma^{m+n+1}$ of (8.7) satisfy this identity, except those for which some x_i or y_j belongs to $\mathcal{T}'$ or the finitely many solutions with all x_i, y_j different from 1 for which (8.9), (8.10) do not both hold. This completes our induction step, and our proof. □

Proof of Proposition 8.1. We take for $\mathcal{S}$ the set $\mathcal{T}$ from Lemma 8.2, taken with $m = n = 3$ and $z = 1$. Pick a solution $(x_1, \dots, y_3) \in \Gamma^6$ of (8.5) with none of the x_i, y_j in $\mathcal{S}$. Then there are integers $c_1, \dots, d_3$ and e with $c_1c_2c_3d_1d_2d_3 \neq 0$ such that

$$(1-x_1T^{c_1})(1-x_2T^{c_2})(1-x_3T^{c_3}) \equiv T^e(1-y_1T^{d_1})(1-y_2T^{d_2})(1-y_3T^{d_3}). \tag{8.11}$$

For $i = 1, 2, 3$, define $a_i := |c_i|$, $b_i := |d_i|$, $u_i := x_i^{\pm 1}$, $v_i := y_i^{\pm 1}$, where $u_i^{a_i} = x_i^{-c_i}$, $v_i^{b_i} = y_i^{-d_i}$. Then (8.11) can be rewritten as an identity in polynomials

$$(T^{a_1} - u_1)(T^{a_2} - u_2)(T^{a_3} - u_3) \equiv (T^{b_1} - v_1)(T^{b_2} - v_2)(T^{b_3} - v_3) \tag{8.12}$$

with positive integers $a_1, \dots, b_3$; here we have divided out possible powers of T on both sides.

In what follows we assume that

$$u_i + u_j \neq 0,\ \ v_i + v_j \neq 0 \text{ for } 1 \leq i < j \leq 3 \tag{8.13}$$

and prove that at least one of the following two alternatives must hold:

$$(v_1, v_2, v_3) \text{ is a permutation of } (u_1, u_2, u_3); \tag{8.14}$$

$$\{u_i/u_j,\ v_i/v_j\ (i \leq i < j \leq 3)\} \text{ contains a primitive cube root of unity.} \tag{8.15}$$

This clearly implies Proposition 8.1. Since (8.13)–(8.15) are invariant under permutations of u_1, u_2, u_3, under permutations of v_1, v_2, v_3 and under interchanging the tuples (u_1, u_2, u_3), (v_1, v_2, v_3), it suffices to consider the cases (i)–(x) below.

Case (i). $a_1 > a_2 > a_3$, $b_1 > b_2 > b_3$.
Then (8.12) becomes

$$\begin{aligned} & T^{a_1+a_2+a_3} - u_3T^{a_1+a_2} - u_2T^{a_1+a_3} - u_1T^{a_2+a_3} \\ & \qquad + u_2u_3T^{a_1} + u_1u_3T^{a_2} + u_1u_2T^{a_3} - u_1u_2u_3 \\ \equiv\ & T^{b_1+b_2+b_3} - v_3T^{b_1+b_2} - v_2T^{b_1+b_3} - v_1T^{b_2+b_3} \\ & \qquad + v_2v_3T^{b_1} + v_1v_3T^{b_2} + v_1v_2T^{b_3} - v_1v_2v_3. \end{aligned}$$

We have either $a_2 + a_3 \neq a_1$ and $b_2 + b_3 \neq b_1$ or $a_2 + a_3 = a_1$ and $b_2 + b_3 = b_1$. But in each of these cases, the second largest exponent on T on the left is $a_1 + a_2$ and that on the right $b_1 + b_2$; hence $u_3 = v_3$. Likewise, the third largest exponent on T on the left is $a_1 + a_3$ and that on the right $b_1 + b_3$; so $u_2 = v_2$. Finally, $u_1u_2u_3 = v_1v_2v_3$; hence $u_1 = v_1$. This implies (8.14).

Case (ii). $a_1 > a_2 > a_3$, $b_1 = b_2 > b_3$.
Then (8.12) becomes

$$\begin{aligned} & T^{a_1+a_2+a_3} - u_3T^{a_1+a_2} - u_2T^{a_1+a_3} - u_1T^{a_2+a_3} + u_2u_3T^{a_1} \\ & \qquad + u_1u_3T^{a_2} + u_1u_2T^{a_3} - u_1u_2u_3 \\ \equiv\ & T^{2b_1+b_3} - v_3T^{2b_1} - (v_1 + v_2)T^{b_1+b_3} \\ & \qquad + (v_1 + v_2)v_3T^{b_1} + v_1v_2T^{b_3} - v_1v_2v_3. \end{aligned}$$

By (8.13), the right-hand side consists of 6 terms with different exponents on T and non-zero coefficients. So on the left-hand side, two terms have to cancel each other and this is possible only if $a_2 + a_3 = a_1$ and $u_1 = u_2u_3$. Comparing the remaining term with the largest exponent on T on the left with the term with the largest exponent on T on the right, and also the terms on both sides with the second largest, third largest exponent on T, etc., we see that $a_1 + a_2 + a_3 = 2b_1 + b_3$, $a_1 + a_2 = 2b_1$, $a_1 + a_3 = b_1 + b_3$. This implies $a_3 = b_3$, $a_1 = b_1$, $a_2 = b_1$, contradicting $a_1 > a_2$. So Case (ii) is impossible.

Case (iii). $a_1 > a_2 > a_3$, $b_1 > b_2 = b_3$.
Then (8.12) becomes

$$\begin{aligned} & T^{a_1+a_2+a_3} - u_3T^{a_1+a_2} - u_2T^{a_1+a_3} - u_1T^{a_2+a_3} + u_2u_3T^{a_1} \\ & \qquad + u_1u_3T^{a_2} + u_1u_2T^{a_3} - u_1u_2u_3 \\ \equiv\ & T^{b_1+2b_3} - (v_2 + v_3)T^{b_1+b_3} - v_1T^{2b_3} \\ & \qquad + v_2v_3T^{b_1} + v_1(v_2 + v_3)T^{b_3} - v_1v_2v_3. \end{aligned}$$

Again, on the left-hand side we must have cancellation of two terms, implying $a_2 + a_3 = a_1$ and $u_1 = u_2u_3$. On the right-hand side, all six terms must have different exponents on T, so $2b_3 \neq b_1$. If $2b_3 > b_1$, then comparing on both sides the three terms with the largest powers of T, we get $a_1 + a_2 + a_3 = b_1 + 2b_3$, $a_1 + a_2 = b_1 + b_3$, $a_1 + a_3 = 2b_3$, implying $a_1 = a_3 = b_3$ which is impossible.

So $b_1 > 2b_3$. Then comparing the exponents on T of the corresponding terms on the left- and right-hand side does not lead to a contradiction. Comparing the coefficients of the terms with the second largest exponent on T, *i.e.*, with $T^{a_1+a_2}$, $T^{b_1+b_3}$, with the third largest exponent, etc., we get $u_3 = v_2 + v_3$, $u_2 = -v_2v_3$, $u_1u_3 = -v_1$, $u_1u_2 = v_1(v_2 + v_3)$, $u_1u_2u_3 = v_1v_2v_3$. Consequently, $v_1v_2v_3 = u_1u_2u_3 = v_1(v_2 + v_3)^2$, hence $v_2v_3 = (v_2 + v_3)^2$, $v_2^2 + v_2v_3 + v_3^2 = 0$, v_2/v_3 is a primitive cube root of unity. This implies (8.15).

Case (iv). $a_1 > a_2 > a_3$, $b_1 = b_2 = b_3$.
In this case, the expansion of the left-hand side of (8.12) gives at least 6 non-zero terms with distinct powers of T, while the right-hand side cannot have more than 4 terms. So this case is impossible.

Case (v). $a_1 = a_2 > a_3$, $b_1 = b_2 > b_3$.
Then (8.12) becomes

$$\begin{aligned} &T^{2a_1+a_3} - u_3T^{2a_1} - (u_1 + u_2)T^{a_1+a_3} \\ &\qquad +(u_1 + u_2)v_3T^{a_1} + u_1u_2T^{a_3} - a_1a_2a_3 \\ &\equiv T^{2b_1+b_3} - v_3T^{2b_1} - (v_1 + v_2)T^{b_1+b_3} \\ &\qquad +(v_1 + v_2)v_3T^{b_1} + v_1v_2T^{b_3} - v_1v_2v_3. \end{aligned}$$

By (8.13) we have on both sides 6 non-zero terms with distinct powers of T. Comparing the terms on both sides with the second highest power of T, *i.e.*, T^{2a_1} and T^{2b_1}, we get $u_3 = v_3$. Comparing the terms with the third highest power of T, *i.e.*, $T^{a_1+a_3}$ and $T^{b_1+b_3}$, we obtain $u_1 + u_2 = v_1 + v_2$, and finally, from the terms with the smallest positive power of T, *i.e.*, T^{a_3}, T^{b_3}, we obtain $u_1u_2 = v_1v_2$. Hence $\{u_1, u_2\} = \{v_1, v_2\}$. This implies (8.14).

Case (vi). $a_1 = a_2 > a_3$, $b_1 > b_2 = b_3$.
Then (8.12) becomes

$$\begin{aligned} &T^{2a_1+a_3} - u_3T^{2a_1} - (u_1 + u_2)T^{a_1+a_3} \\ &\qquad +(u_1 + u_2)u_3T^{a_1} + u_1u_2T^{a_3} - u_1u_2u_3 \\ &\equiv T^{b_1+2b_3} - (v_2 + v_3)T^{b_1+b_3} - v_1T^{2b_3} \\ &\qquad +v_2v_3T^{b_1} + v_1(v_2 + v_3)T^{b_3} - v_1v_2v_3. \end{aligned}$$

On the left-hand side there are 6 non-zero terms with distinct powers of T. So on the right-hand side we must also have 6 non-zero terms with distinct powers of T. We have either $2b_3 > b_1$ or $2b_3 < b_1$. If $2b_3 > b_1$ then, on comparing the terms with the three largest exponents on T on both sides we get $2a_1 + a_3 = b_1 + 2b_3$, $2a_1 = b_1 + b_3$, $a_1 + a_3 = 2b_3$, hence $a_1 = a_3 = b_3$, which is impossible. So $b_1 > 2b_3$. Then comparing the coefficients of the terms with the largest exponent on T on both sides, the terms with the second largest exponent, etc. we get $u_3 = v_2 + v_3$, $u_1 + u_2 = v_3$, $(u_1 + u_2)u_3 = v_2v_3$, $u_1u_2 = v_1(v_2 + v_3)$, $u_1u_2u_3 = v_1v_2v_3$. This leads to $v_1v_2v_3 = v_1(v_2 + v_3)^2$, and then similarly as in Case (iii) it follows that v_2/v_3 is a primitive cube root of unity. Hence (8.15) holds.

Case (vii). $a_1 = a_2 > a_3, \quad b_1 = b_2 = b_3$.
This case is impossible since on the left-hand side of (8.12) we have 6 non-zero terms with distinct powers of T and on the right-hand side not more than 4 terms.

Case (viii). $a_1 > a_2 = a_3, \quad b_1 > b_2 = b_3$.
Then (8.12) becomes

$$\begin{aligned} & T^{a_1+2a_3} - (u_2+u_3)T^{a_1+a_3} - u_1T^{2a_3} \\ & \qquad +u_2u_3T^{a_1} + u_1(u_2+u_3)T^{a_3} - u_1u_2u_3 \\ \equiv\ & T^{b_1+2b_3} - (v_2+v_3)T^{b_1+b_3} - v_1T^{2b_3} \\ & \qquad +v_2v_3T^{b_1} + v_1(v_2+v_3)T^{b_3} - v_1v_2v_3. \end{aligned}$$

There are various possibilities depending on whether $2a_3 = a_1$, $2a_3 \neq a_1$, $u_1 = u_2u_3$, $u_1 \neq u_2u_3$ and similarly for the b_i's and v_i's. But in each of these cases, $a_1 + a_3$ is the second largest exponent on T occurring on the left and $b_1 + b_3$ the second largest exponent on the right and so $u_2 + u_3 = v_2 + v_3$. Further, a_3 is the smallest positive exponent on the left and b_3 the smallest positive exponent on the right and so $u_1(u_2 + u_3) = v_1(v_2 + v_3)$; and finally $u_1u_2u_3 = v_1v_2v_3$. It follows that $u_1 = v_1$, $u_2u_3 = v_2v_3$, and then $\{u_2, u_3\} = \{v_2, v_3\}$. This implies (8.14).

Case (ix). $a_1 > a_2 = a_3, \quad b_1 = b_2 = b_3$.
Then (8.12) becomes

$$\begin{aligned} & T^{a_1+2a_3} - (u_2+u_3)T^{a_1+a_3} - u_1T^{2a_3} + u_2u_3T^{a_1} \\ & \qquad +u_1(u_2+u_3)T^{a_3} - u_1u_2u_3 \\ \equiv\ & T^{3b_1} - (v_1+v_2+v_3)T^{2b_1} + (v_2v_3+v_1v_3+v_1v_2)T^{b_1} - v_1v_2v_3. \end{aligned}$$

Then necessarily, $a_1 = 2a_3$ and $u_1 = u_2u_3$. Further, all terms on the right-hand side are non-zero. Comparing the terms with the largest and second largest exponent on T, we see that $a_1 + 2a_3 = 3b_1$, $a_1 + a_3 = 2b_1$, hence $a_1 = a_3 = b_1$ which is impossible.

Case (x). $a_1 = a_2 = a_3, \quad b_1 = b_2 = b_3$.
Then (8.12) implies at once (8.14). This completes the proof of Proposition 8.1. □

9. Proof of Theorem 3.2

Let as before A be an integrally closed domain with quotient field L of characteristic 0 which is finitely generated over $\mathbb{Z}$, and K an extension of L of finite degree $d \geq 3$. Further, denote by G the normal closure of K over L. In what follows, we consider pairs (α, β) such that

$$\begin{cases} L(\alpha) = L(\beta) = K, \ \alpha, \beta \text{ are integral over } A, \\ A[\alpha] = A[\beta], \ \alpha, \beta \text{ are not } A\text{-equivalent.} \end{cases} \tag{9.1}$$

The next lemma implies part (i) of Theorems 3.2 and 1.2.

Lemma 9.1. *Suppose that* $[K : L] = 3$. *Let* (α, β) *be a pair with* (9.1). *Then there is a matrix* $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ *such that*

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{GL}(2, L), \quad \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}, \quad a_3 \neq 0. \tag{9.2}$$

Further, if A *is a principal ideal domain then* $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ *can be chosen from* $\mathrm{GL}(2, A)$.

Proof. Let σ_i $(i = 1, 2, 3)$ be the L-isomorphisms of K into G, and write $\alpha^{(i)} := \sigma_i(\alpha)$, $\beta^{(i)} := \sigma_i(\beta)$ for $i = 1, 2, 3$. By straightforward linear algebra, there are $a_1, a_2, a_3, a_4 \in G$ such that

$$\beta^{(i)} = \frac{a_1\alpha^{(i)} + a_2}{a_3\alpha^{(i)} + a_4} \text{ for } i = 1, 2, 3.$$

If we choose the first non-zero element among $a_1, \ldots, a_4$ equal to 1, then $a_1, \ldots, a_4$ are uniquely determined. By applying $\sigma \in \mathrm{Gal}(G/L)$ and observing that σ permutes the $\alpha^{(i)}$ in the same way as the $\beta^{(i)}$, we infer that $\sigma(a_i) = a_i$ for $i = 1, \ldots, 4$. Hence $a_i \in L$ for $i = 1, \ldots, 4$. The matrix $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ must have non-zero determinant since otherwise $\beta^{(1)} = \beta^{(2)} = \beta^{(3)}$, contrary to our assumption $L(\beta) = K$. Next, we must have $a_3 \neq 0$. For otherwise, α, β are L-equivalent, hence A-equivalent by Lemma 6.2, contrary to our assumptions. This proves (9.2).

In case that A is a principal ideal domain, by taking a scalar multiple of $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$, we can see to it that $a_1, \ldots, a_4 \in A$ and $(a_1, \ldots, a_4) = (1)$. Then $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, A)$ by Lemma 6.4. This completes the proof of Lemma 9.1. □

In what follows, we assume that

$$\begin{cases} [K : L] = d \geq 4, \ \mathrm{Gal}(G/L) \cong S_4 \text{ if } d = 4, \\ K \text{ is four times transitive over } L \text{ if } d \geq 5. \end{cases} \tag{9.3}$$

For every pair (α, β) with (9.1) we define, in the usual manner,

$$\varepsilon_{ij} := \frac{\alpha^{(i)} - \alpha^{(j)}}{\beta^{(i)} - \beta^{(j)}} \quad (1 \leq i, j \leq d, \ i \neq j).$$

We start with a simple, but for our proof important observation.

Lemma 9.2. *Let* α, β *satisfy* (9.1)*, and let* (p_1, p_2, p_3, p_4), (q_1, q_2, q_3, q_4) *be two ordered tuples of distinct indices from* $\{1, \ldots, d\}$. *Then there is* $\sigma \in \mathrm{Gal}(G/L)$ *such that*

$$\sigma(\varepsilon_{p_i, p_j}) = \varepsilon_{q_i, q_j} \text{ for each distinct } i, j \in \{1, 2, 3, 4\}.$$

Proof. By (9.3), there is $\sigma \in \mathrm{Gal}(K/L)$ such that $\sigma(\alpha^{(p_i)}) = \alpha^{(q_i)}$ for $i = 1, 2, 3, 4$. The same holds with β instead of α. This implies the lemma at once. □

Our next observation is that for any pair (α, β) with (9.1),

$$\frac{\varepsilon_{ij}}{\varepsilon_{ik}} \neq 1 \text{ for } i, j, k \in \{1, \dots, d\}, \text{ with } i, j, k \text{ distinct.} \tag{9.4}$$

Indeed, suppose there are distinct indices i, j, k with $\varepsilon_{ij} = \varepsilon_{ik}$. Then by Lemma 9.2 we have $\varepsilon_{1j} = \varepsilon_{12}$ for $j = 3, \dots, d$. This implies that $\tau(\alpha) = \tau(\beta)$, where $\tau(\cdot)$ is given by (6.1). Now Lemma 6.3 (ii) implies that α, β are A-equivalent, contrary to (9.1).

Lemma 9.3. *There is a finite set $\mathcal{E}$ such that for every pair (α, β) with* (9.1)*, at least one of the following alternatives holds:*

- **(i)** *$\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{E}$ for each ordered triple (i, j, k) of distinct indices from $\{1, \dots, d\}$;*
- **(ii)** *$\varepsilon_{ij}\varepsilon_{kl} = \varepsilon_{ik}\varepsilon_{jl}$ for each ordered quadruple (i, j, k, l) of distinct indices from $\{1, \dots, d\}$;*
- **(iii)** *$d = 4$, and $\varepsilon_{ij} = -\varepsilon_{kl}$ for each permutation (i, j, k, l) of $(1, 2, 3, 4)$.*

Proof. Pick a pair (α, β) with (9.1). We apply Proposition 8.1 to (8.5), with $\Gamma = A_G^*$ and with for $(x_1, x_2, x_3, y_1, y_2, y_3)$ the tuple (8.6) with $(i, j, k, l) = (1, 2, 3, 4)$, *i.e.*,

$$\left(\frac{\varepsilon_{13}}{\varepsilon_{23}}, \frac{\varepsilon_{14}}{\varepsilon_{34}}, \frac{\varepsilon_{12}}{\varepsilon_{24}}, \frac{\varepsilon_{12}}{\varepsilon_{23}}, \frac{\varepsilon_{13}}{\varepsilon_{34}}, \frac{\varepsilon_{14}}{\varepsilon_{24}}\right). \tag{9.5}$$

Let $\mathcal{S}$ be the finite set from Proposition 8.3. Let $\mathcal{E}$ consist of all conjugates over L of the elements from $\mathcal{S}$, as well as all roots of unity of order up to 18.

First suppose that alternative (i) of Proposition 8.1 holds. Then there are distinct $p, q, r \in \{1, \dots, 4\}$, such that $\varepsilon_{pq}/\varepsilon_{pr} \in \mathcal{S}$. By Lemma 9.2 we then have $\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{E}$ for each triple (i, j, k) of distinct indices from $\{1, \dots, d\}$. This is alternative (i) of our lemma.

Next, suppose that alternative (ii) of Proposition 8.1 holds. Then

$$\frac{\varepsilon_{13}}{\varepsilon_{23}} \in \left\{\frac{\varepsilon_{12}}{\varepsilon_{23}}, \frac{\varepsilon_{13}}{\varepsilon_{34}}, \frac{\varepsilon_{14}}{\varepsilon_{24}}, \frac{\varepsilon_{23}}{\varepsilon_{12}}, \frac{\varepsilon_{34}}{\varepsilon_{13}}, \frac{\varepsilon_{24}}{\varepsilon_{14}}\right\}.$$

By (9.4), $\varepsilon_{13}/\varepsilon_{23}$ cannot be equal to $\varepsilon_{12}/\varepsilon_{23}$ or $\varepsilon_{13}/\varepsilon_{34}$. If $\varepsilon_{13}/\varepsilon_{23} = \varepsilon_{14}/\varepsilon_{24}$, then $\varepsilon_{13}\varepsilon_{24} = \varepsilon_{14}\varepsilon_{23}$. Then by Lemma 9.2 $\varepsilon_{ij}\varepsilon_{kl} = \varepsilon_{ik}\varepsilon_{jl}$ for any four distinct indices $i, j, k, l \in \{1, \dots, d\}$. This is alternative (ii) of our lemma.

Assume that $\varepsilon_{13}/\varepsilon_{23} = \varepsilon_{23}/\varepsilon_{12}$; then $\varepsilon_{23}^2 = \varepsilon_{12}\varepsilon_{13}$. By Lemma 9.2, we have also $\varepsilon_{13}^2 = \varepsilon_{12}\varepsilon_{23}$. Hence $(\varepsilon_{23}/\varepsilon_{13})^3 = 1$. Again by Lemma 9.2, and the fact that $\mathcal{E}$ contains all cube roots of unity, this implies alternative (i) of our lemma.

Next, assume that $\varepsilon_{13}/\varepsilon_{23} = \varepsilon_{34}/\varepsilon_{13}$. Then $\varepsilon_{13}^2 = \varepsilon_{23}\varepsilon_{34}$. Then by Lemma 9.2, $\varepsilon_{23}^2 = \varepsilon_{13}\varepsilon_{34}$. This implies again $(\varepsilon_{13}/\varepsilon_{23})^3 = 1$ and then alternative (i) of our lemma.

Finally, assume that $\varepsilon_{13}/\varepsilon_{23} = \varepsilon_{24}/\varepsilon_{14}$. Then $\varepsilon_{13}\varepsilon_{14} = \varepsilon_{23}\varepsilon_{24}$. By Lemma 9.2, the same holds after interchanging the indices 2 and 3, and also after interchanging 2 and 4; that is, we have also $\varepsilon_{12}\varepsilon_{14} = \varepsilon_{23}\varepsilon_{34}$ and $\varepsilon_{13}\varepsilon_{12} = \varepsilon_{34}\varepsilon_{24}$. Multiplying

together the last two identities and dividing by the first, we obtain $\varepsilon_{12}^2 = \varepsilon_{34}^2$, or $\varepsilon_{12} = \pm\varepsilon_{34}$. First suppose that $\varepsilon_{12} = \varepsilon_{34}$. Then by Lemma 9.2, we have also $\varepsilon_{13} = \varepsilon_{24}$, $\varepsilon_{14} = \varepsilon_{23}$. Substituting this into (8.4) with $(i, j, k, l) = (1, 2, 3, 4)$, we obtain

$$\left(\frac{\varepsilon_{13}}{\varepsilon_{14}} - 1\right)\left(\frac{\varepsilon_{14}}{\varepsilon_{12}} - 1\right)\left(\frac{\varepsilon_{12}}{\varepsilon_{13}} - 1\right) = \left(\frac{\varepsilon_{12}}{\varepsilon_{14}} - 1\right)\left(\frac{\varepsilon_{13}}{\varepsilon_{12}} - 1\right)\left(\frac{\varepsilon_{14}}{\varepsilon_{13}} - 1\right).$$

But this is impossible, since by (9.4), both sides are non-zero, and since the left-hand side is the opposite of the right-hand side. Hence $\varepsilon_{12} = -\varepsilon_{34}$ and then by Lemma 9.2, also $\varepsilon_{13} = -\varepsilon_{24}$, $\varepsilon_{14} = -\varepsilon_{23}$. If $d \geq 5$, then again by Lemma 9.2, $\varepsilon_{12} = -\varepsilon_{35}$, implying $\varepsilon_{34} = \varepsilon_{35}$, which is impossible by (9.4). Hence $d = 4$. We conclude that alternative (iii) of our lemma holds.

Finally, suppose that (iii) of Proposition 8.1 holds. Then if $(x_1, \ldots, y_3)$ is the tuple (9.5) we have that at least one of the numbers $x_i x_j$, x_i/x_j, $y_i y_j$, y_i/y_j $(1 \leq i < j \leq 3)$ is -1 or a primitive cube root of unity. All these possibilities can be combined by saying that there is a permutation (i, j, k, l) of $(1, 2, 3, 4)$ such that $\varepsilon_{ik}\varepsilon_{il}/\varepsilon_{jk}\varepsilon_{kl}$ or $\varepsilon_{ik}\varepsilon_{kl}/\varepsilon_{il}\varepsilon_{jk}$ is -1 or a primitive cube root of unity. By Lemma 9.2, we may replace the indices i, j, k, l by $1, \ldots, 4$, respectively. Then $(\varepsilon_{13}\varepsilon_{14}/\varepsilon_{23}\varepsilon_{34})^6 = 1$ or $(\varepsilon_{13}\varepsilon_{34}/\varepsilon_{14}\varepsilon_{23})^6 = 1$.

First suppose that $(\varepsilon_{13}\varepsilon_{14}/\varepsilon_{23}\varepsilon_{34})^6 = 1$. Applying again Lemma 9.2, the same holds if we interchange the indices 2 and 4, *i.e.*, $(\varepsilon_{13}\varepsilon_{12}/\varepsilon_{34}\varepsilon_{23})^6 = 1$. As a consequence, $(\varepsilon_{12}/\varepsilon_{14})^6 = 1$. But then another application of Lemma 9.2 implies that $\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{E}$ for any three distinct indices i, j, k, *i.e.*, alternative (i) of our lemma.

Finally, suppose that $(\varepsilon_{13}\varepsilon_{34}/\varepsilon_{14}\varepsilon_{23})^6 = 1$. By Lemma 9.2, interchanging the indices 1 and 3, we get also $(\varepsilon_{13}\varepsilon_{14}/\varepsilon_{34}\varepsilon_{12})^6 = 1$. Multiplying the two identities gives $(\varepsilon_{13}^2/\varepsilon_{12}\varepsilon_{23})^6 = 1$. Again by Lemma 9.2, interchanging the indices 2 and 3, we get $(\varepsilon_{12}^2/\varepsilon_{13}\varepsilon_{23})^6 = 1$. Then on dividing the last two identities, we get $(\varepsilon_{13}/\varepsilon_{12})^{18} = 1$. A final application of Lemma 9.2 leads to $\varepsilon_{ij}/\varepsilon_{ik} \in \mathcal{E}$ for any three distinct indices i, j, k, which is alternative (i) of our lemma. This completes our proof. □

Proof of Theorem 3.2, (ii), (iii). Consider the two times monogenic A-orders $\mathcal{O} = A[\alpha] = A[\beta]$ in K, where α, β satisfy (9.1).

First consider those A-orders $\mathcal{O}$ such that the pair (α, β) satisfies alternative (i) of Lemma 9.3. Then by (8.3), (9.4), there is a finite set $\mathcal{F}$ independent of α, β such that $\frac{\beta^{(i)}-\beta^{(j)}}{\beta^{(i)}-\beta^{(k)}} \in \mathcal{F}$ for any three distinct $i, j, k \in \{1, \ldots, d\}$. Hence for the tuple $\tau(\beta)$ defined by (6.1) there are only finitely many possibilities. Then Lemma 6.3 implies that for the A-orders $\mathcal{O}$ under consideration, the corresponding β lie in only finitely many L-equivalence classes. Subsequently, by Lemma 7.2 these β lie in only finitely many A-equivalence classes, and thus there are only finitely many possibilities for the A-order $\mathcal{O}$.

Next, we consider those A-orders $\mathcal{O} = A[\alpha] = A[\beta]$ such that (α, β) satisfies alternative (ii) of Lemma 9.3. Take such a pair (α, β). By assumption, $\varepsilon_{ij}\varepsilon_{kl} =$

$\varepsilon_{ik}\varepsilon_{jl}$, hence, in view of (8.1),

$$\frac{(\beta^{(i)}-\beta^{(j)})(\beta^{(k)}-\beta^{(l)})}{(\beta^{(i)}-\beta^{(k)})(\beta^{(j)}-\beta^{(l)})} = \frac{(\alpha^{(i)}-\alpha^{(j)})(\alpha^{(k)}-\alpha^{(l)})}{(\alpha^{(i)}-\alpha^{(k)})(\alpha^{(j)}-\alpha^{(l)})}$$

for every quadruple (i, j, k, l) of distinct indices from $\{1, \dots, d\}$. In other words, the cross ratio of any four numbers among the $\alpha^{(i)}$'s is equal to the cross ratio of the corresponding numbers among the $\beta^{(i)}$'s. Then by elementary projective geometry, there is a matrix $C = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, G)$ such that

$$\beta^{(i)} = \frac{a_1\alpha^{(i)} + a_2}{a_3\alpha^{(i)} + a_4} \quad \text{for } i = 1, \dots, d.$$

If we assume that the first non-zero entry among $a_1, \dots, a_4$ is 1, the matrix C is uniquely determined. Any $\sigma \in \mathrm{Gal}(G/L)$ permutes the sequences $\alpha^{(1)}, \dots, \alpha^{(d)}$ and $\beta^{(1)}, \dots, \beta^{(d)}$ in the same manner, hence the above relation holds with $\sigma(C)$ instead of C; so $\sigma(C) = C$. It follows that $C \in \mathrm{GL}(2, L)$. We observe that $a_3 \neq 0$. For otherwise, α, β are L-equivalent and then A-equivalent by Lemma 6.2, contrary to (9.1). This shows that $\mathcal{O} = A[\alpha] = A[\beta]$ is of type I. Notice that if A is a principal ideal domain, then by taking a suitable scalar multiple of C we can arrange that $a_1, \dots, a_4 \in A$ and $(a_1, \dots, a_4) = (1)$, and thus, $C \in \mathrm{GL}(2, A)$ by Lemma 6.4.

Finally, we consider those A-orders $\mathcal{O} = A[\alpha] = A[\beta]$ such that (α, β) satisfies alternative (iii) of Lemma 9.3; then $d = 4$. Take such a pair (α, β). By assumption, $\varepsilon_{ij} = -\varepsilon_{kl}$ for every permutation (i, j, k, l) of $(1, 2, 3, 4)$. Define

$$u_0 := \varepsilon_{12}\varepsilon_{13}\varepsilon_{14},$$
$$\alpha_0 := \tfrac{1}{2}u_0(\varepsilon_{12}^{-1} + \varepsilon_{13}^{-1} + \varepsilon_{14}^{-1}), \quad \beta_0 := \tfrac{1}{2}(\varepsilon_{12} + \varepsilon_{13} + \varepsilon_{14}).$$

By (9.3), the group $\mathrm{Gal}(G/L)$ acts on $\{\alpha^{(1)}, \dots, \alpha^{(4)}\}$ as the full permutation group. Say that $\sigma(\alpha^{(i)}) = \alpha^{(\sigma(i))}$ for $\sigma \in \mathrm{Gal}(G/L)$, $i = 1, 2, 3, 4$. Then $\sigma(\beta^{(i)}) = \beta^{(\sigma(i))}$ for $i = 1, 2, 3, 4$ and thus, $\sigma(\varepsilon_{ij}) = \varepsilon_{\sigma(i),\sigma(j)}$ for $1 \leq i, j \leq 4$, $i \neq j$. Further, $\mathrm{Gal}(G/K)$ consists of those L-automorphisms that permute $\alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}$ and leave $\alpha = \alpha^{(1)}$ unchanged. Hence u_0, α_0, β_0 are invariant under $\mathrm{Gal}(G/K)$ and so belong to K. But u_0 is in fact invariant under $\mathrm{Gal}(G/L)$, hence belongs to L. Notice that

$$\beta_0^2 = \alpha_0 + r_0, \quad \alpha_0^2 = u_0\beta_0 + s_0 \quad \text{with } r_0, s_0 \in L. \tag{9.6}$$

Indeed, (9.6) holds with

$$r_0 := \tfrac{1}{4}(\varepsilon_{12}^2 + \varepsilon_{13}^2 + \varepsilon_{14}^2), \quad s_0 := \tfrac{1}{4}u_0^2(\varepsilon_{12}^{-2} + \varepsilon_{13}^{-2} + \varepsilon_{14}^{-2}),$$

and these r_0, s_0 are invariant under $\mathrm{Gal}(G/L)$.

A straightforward computation gives

$$\alpha_0^{(2)} = \tfrac{1}{2}u_0(\varepsilon_{21}^{-1} + \varepsilon_{23}^{-1} + \varepsilon_{24}^{-1}) = \tfrac{1}{2}u_0(\varepsilon_{12}^{-1} - \varepsilon_{13}^{-1} - \varepsilon_{14}^{-1})$$

and similarly, $\beta_0^{(2)} = \frac{1}{2}(\varepsilon_{12} - \varepsilon_{13} - \varepsilon_{14})$. Hence

$$\frac{\alpha_0^{(1)} - \alpha_0^{(2)}}{\beta_0^{(1)} - \beta_0^{(2)}} = \frac{-u_0(\varepsilon_{13}^{-1} + \varepsilon_{14}^{-1})}{-(\varepsilon_{13} + \varepsilon_{14})} = u_0\varepsilon_{13}^{-1}\varepsilon_{14}^{-1} = \varepsilon_{12}.$$

By taking conjugates over L we get

$$\frac{\alpha_0^{(i)} - \alpha_0^{(j)}}{\beta_0^{(i)} - \beta_0^{(j)}} = \varepsilon_{ij} \text{ for } 1 \le i, j \le 4,\ i \ne j. \tag{9.7}$$

As a consequence, the four conjugates of α_0 over L are distinct, and also the four conjugates of β_0 over L are all distinct. Hence $L(\alpha_0) = L(\beta_0) = K$. Notice that in the deduction of (8.3), no properties of α, β were used other than that $L(\alpha) = L(\beta) = K$. That is, the same reasoning applies if we replace α, β by α_0, β_0. But then, applying (8.3) both with (α, β) and with (α_0, β_0), using (9.7), (9.4), we obtain

$$\frac{\beta^{(i)} - \beta^{(j)}}{\beta^{(i)} - \beta^{(k)}} = \frac{\beta_0^{(i)} - \beta_0^{(j)}}{\beta_0^{(i)} - \beta_0^{(k)}} \ (1 \le i, j, k \le d,\ i, j, k \text{ distinct}).$$

By multiplying this identity with $\varepsilon_{ij}/\varepsilon_{ik}$ we obtain

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} = \frac{\alpha_0^{(i)} - \alpha_0^{(j)}}{\alpha_0^{(i)} - \alpha_0^{(k)}} \ (1 \le i, j, k \le d,\ i, j, k \text{ distinct}).$$

This shows that $\tau(\beta) = \tau(\beta_0)$, $\tau(\alpha) = \tau(\alpha_0)$, where $\tau(\cdot)$ is defined by (6.1). By Lemma 6.3, (i), there are $\lambda, \lambda' \in L^*$, $\mu, \mu' \in L$, such that

$$\alpha = \lambda\alpha_0 + \mu, \quad \beta = \lambda'\beta_0 + \mu'.$$

By combining this with (9.6), we obtain

$$\beta = a_0\alpha^2 + a_1\alpha + a_2, \quad \alpha = b_0\beta^2 + b_1\beta + b_2$$

with $a_0, a_1, a_2, b_0, b_1, b_2 \in L$ and $a_0b_0 \ne 0$. But in fact, we have $a_0, \dots, b_2 \in A$ since by assumption, $A[\alpha] = A[\beta]$. This shows that $\mathcal{O} = A[\alpha] = A[\beta]$ is an A-order of type II. This completes the proof of Theorem 3.2. □

References

[1] A. BÉRCZES, *On the number of solutions of index form equations*, Publ. Math. Debrecen **56** (2000), 251–262.

[2] H. BRUNOTTE, A. HUSZTI and A. PETHŐ, *Bases of canonical number systems in quartic algebraic number fields*, J. Théor. Nombres Bordeaux **18** (2006), 537–557.

[3] N. BOURBAKI, "Commutative Algebra", Chapters 1–7, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989.

[4] R. DEDEKIND, *Über die Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh. König. Ges. Wissen. Göttingen **23** (1878), 1–23.

[5] J.-H. EVERTSE and K. GYŐRY, *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358** (1985), 6–19.
[6] J.-H. EVERTSE, K. GYŐRY, C. L. STEWART and R. TIJDEMAN, *On S-unit equations in two unknowns*, Invent. Math. **92** (1988), 461–477.
[7] K. GYŐRY, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426.
[8] K. GYŐRY, *Sur les polynômes à coefficients entiers et de dicriminant donné III*, Publ. Math. Debrecen **23** (1976), 141–165.
[9] K. GYŐRY, *Corps de nombres algébriques d'anneau d'entiers monogène*, In: "Séminaire Delange-Pisot-Poitou", 20e année: 1978/1979. Théorie des nombres, Fasc. 2 (French), Secrétariat Math., Paris, 1980, pp. Exp. No. 26, 7.
[10] K. GYŐRY, *On certain graphs associated with an integral domain and their applications to Diophantine problems*, Publ. Math. Debrecen **29** (1982), 79–94.
[11] 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.
[12] K. GYŐRY, *Upper bounds for the number of solutions of unit equations in two unknowns*, Lithuanian Math. J. **32** (1992), 40–44.
[13] K. GYŐRY, *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69** (2006), 473–499.
[14] L.-C. KAPPE and B. WARREN, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), 133–137.
[15] B. KOVÁCS, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), 405–407.
[16] B. KOVÁCS and A. PETHŐ, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. **55** (1991), 287–299.
[17] S. LANG, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. **6** (1960), 27–43.
[18] M. LAURENT, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), 299–327.
[19] P. ROQUETTE, *Einheiten und Divisorklassen in endlich erzeugbaren Körpern*, Jber. Deutsch. Math. Verein **60** (1957), 1–21.
[20] B.L. VAN DER WAERDEN, "Algebra I" (8. Auflage), Springer Verlag, 1971.

Institute of Mathematics
University of Debrecen
Number Theory Research Group
Hungarian Academy of Sciences and
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
berczesa@math.klte.hu
gyory@math.klte.hu

Universiteit Leiden
Mathematisch Instituut
Postbus 9512
2300 RA Leiden, The Netherlands
evertse@math.leidenuniv.nl