ACTA ARITHMETICA
Online First version

Orders with few rational monogenizations

by

Jan-Hendrik Evertse (Leiden)

To the memory of Professor Andrzej Schinzel (1937–2021)

1. Introduction

Summary. Recall that a monogenic order is an order of the shape $\mathbb{Z}[\alpha]$, where α is an algebraic integer. This is generalized to orders $\mathbb{Z}_\alpha$ for not necessarily integral algebraic numbers α as follows. For an algebraic number α of degree n, let $\mathcal{M}_\alpha$ be the $\mathbb{Z}$-module generated by $1, \alpha, \dots, \alpha^{n-1}$; then $\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}$ is the ring of scalars of $\mathcal{M}_\alpha$. We call an order of the shape $\mathbb{Z}_\alpha$ *rationally monogenic*. If α is an algebraic integer, then $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha]$ is monogenic. Rationally monogenic orders are invariant rings of primitive polynomials or binary forms (see, e.g., [5], [15], [16], [17], [6], [19], [10, Chap. 16]). If α, β are two $\mathrm{GL}_2(\mathbb{Z})$-equivalent algebraic numbers, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Given an order $\mathcal{O}$ of a number field, we call a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of α with $\mathbb{Z}_\alpha = \mathcal{O}$ a *rational monogenization* of $\mathcal{O}$.

We prove the following. If K is a quartic number field, then K has only finitely many orders with more than two rational monogenizations. This is best possible. Further, if K is a number field of degree ≥ 5, the Galois group of whose normal closure is 5-transitive, then K has only finitely many orders with more than one rational monogenization. The proof uses finiteness results for unit equations, which in turn were derived from Schmidt's Subspace Theorem. Except for the hypothesis on the normal closure of K, our result implies a conjecture posed in [4].

2020 *Mathematics Subject Classification*: Primary 11R99; Secondary 11D61, 11J87.
Key words and phrases: orders, rationally monogenic orders, rational monogenization, invariant orders of binary forms, $\mathrm{GL}_2(\mathbb{Z})$-equivalence, unit equations.
Received 20 January 2023.
Published online 12 September 2023.

DOI: 10.4064/aa230120-16-7

We generalize the above results to rationally monogenic orders over rings of S-integers of number fields. Our results extend work of Bérczes, Győry and the author [2] on monogenic orders.

Background and results. Let K be a number field. Denote its ring of integers by $\mathcal{O}_K$. An order $\mathcal{O}$ of K (i.e., a subring of K that as a $\mathbb{Z}$-module is free of rank $[K:\mathbb{Q}]$) is called *monogenic* if there is $\alpha \in \mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$. The set of α with $\mathbb{Z}[\alpha] = \mathcal{O}$ can be divided into so-called $\mathbb{Z}$-equivalence classes, where α_1, α_2 are called $\mathbb{Z}$-*equivalent* if $\alpha_1 - \alpha_2 \in \mathbb{Z}$ or $\alpha_1 + \alpha_2 \in \mathbb{Z}$. A $\mathbb{Z}$-equivalence class of α with $\mathbb{Z}[\alpha] = \mathcal{O}$ is called a *monogenization* of $\mathcal{O}$. Every order of a quadratic number field has precisely one monogenization. Orders of number fields of degree ≥ 3 may be non-monogenic or have more than one monogenization. From work of Győry [12, 13] it can be deduced, and in fact in an effective form, that if K is any number field of degree ≥ 3 then every order $\mathcal{O}$ of K has at most finitely many monogenizations. If one keeps the number field K fixed and restricts to monogenic orders of K, then most of these have only a few monogenizations. Bérczes, Győry and the author [2, Theorem 1.1] obtained the following result.

THEOREM A. *Let K be a number field of degree ≥ 3. Then K has only finitely many orders with more than two monogenizations.*

This result is optimal. For instance, if ε is a unit of $\mathcal{O}_K$ with $\mathbb{Q}(\varepsilon) = K$, then $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$, while ε and ε^{-1} are not $\mathbb{Z}$-equivalent. More generally, let $\alpha \in \mathcal{O}_K$ be such that $\mathbb{Q}(\alpha) = K$, suppose there are integers c, d such that $c\alpha + d$ is a unit of $\mathcal{O}_K$, let a, b be integers such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, and put $\beta := \frac{a\alpha+b}{c\alpha+d}$. Then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, while α and β are not $\mathbb{Z}$-equivalent.

This suggests that it is natural to consider the $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of elements α with $\mathbb{Z}[\alpha] = \mathcal{O}$. Here, $\alpha, \beta \in K$ are called $\mathrm{GL}_2(\mathbb{Z})$-*equivalent* if there is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $\beta = \frac{a\alpha+b}{c\alpha+d}$.

We say that a group G acts t-*transitively* on a finite set $\mathcal{S}$ if for any pairwise distinct $i_1, \ldots, i_t \in \mathcal{S}$ and pairwise distinct $j_1, \ldots, j_t \in \mathcal{S}$, there is $\sigma \in G$ such that $\sigma(i_1) = j_1, \ldots, \sigma(i_t) = j_t$. If $K = \mathbb{Q}(\alpha)$ and L is the normal closure of K, we say that $\mathrm{Gal}(L/\mathbb{Q})$ is t-*transitive* if it acts t-transitively on the set $\{\alpha^{(1)}, \ldots, \alpha^{(n)}\}$ of conjugates of α.

Then from [2, Theorems 1.1 and 1.2(ii)], the following can be deduced:

THEOREM B. *Let K be a number field of degree ≥ 5 such that the Galois group of its normal closure is 4-transitive. Then for all orders $\mathcal{O}$ of K with at most finitely many exceptions, the set of α with $\mathbb{Z}[\alpha] = \mathcal{O}$ is contained in at most one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.*

It is not known whether the condition on the normal closure of K is necessary. It can be proved in an elementary way that if K is a cubic number field and $\mathcal{O}$ an order of K, then the set of $\alpha \in \mathcal{O}$ with $\mathbb{Z}[\alpha] = \mathcal{O}$ is contained in

at most one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class. For quartic number fields K, the above theorem is false. In fact, [2, end of Section 1] gives the following construction:

THEOREM C. *Let r, s be integers such that $f(X) = (X^2 - r)^2 - X - s$ is irreducible, and let $K = \mathbb{Q}(\alpha)$, where α is a root of f. Then K has infinitely many orders $\mathcal{O}_m$ $(m = 1, 2, \ldots)$ with the following property: $\mathcal{O}_m = \mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$, where $\beta_m = \alpha_m^2 - r_m$, $\alpha_m = \beta_m^2 - s_m$ for some integers r_m, s_m.*

It is clear that α_m, β_m in the above theorem are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

Our aim is to generalize Theorem B to orders attached to non-integral algebraic numbers. Let α be an algebraic number of degree n and $f_\alpha \in \mathbb{Z}[X]$ its primitive minimal polynomial, i.e., with coefficients having gcd 1. Then the order $\mathbb{Z}_\alpha$ attached to α is the invariant ring or order of f_α (see Nakagawa [15], Simon [16] or [5], [17], [6], [19], [10, Chap. 16]). Nakagawa and Simon defined this order by giving a $\mathbb{Z}$-module basis for it, together with a multiplication table. A direct definition of $\mathbb{Z}_\alpha$ is as follows. Define the $\mathbb{Z}$-module

$$\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\}. \tag{1.1}$$

Then $\mathbb{Z}_\alpha$ is the ring of scalars of $\mathcal{M}_\alpha$, i.e.,

$$\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}. \tag{1.2}$$

If α is an algebraic integer, then $\alpha^i \in \mathcal{M}_\alpha$ for $i \geq n$, and thus, $\mathbb{Z}_\alpha = \mathcal{M}_\alpha = \mathbb{Z}[\alpha]$. Further, if α, β are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, i.e., $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then one easily verifies that $\mathcal{M}_\beta = (c\alpha + d)^{1-n}\mathcal{M}_\alpha$, which implies $\mathbb{Z}_\beta = \mathbb{Z}_\alpha$.

To simplify the formulation of our results, we introduce the following terminology. We call an order $\mathcal{O}$ of a number field K *rationally monogenic* if $\mathcal{O} = \mathbb{Z}_\alpha$ for some α with $K = \mathbb{Q}(\alpha)$. A $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of α with $\mathbb{Z}_\alpha = \mathcal{O}$ is called a *rational monogenization* of $\mathcal{O}$.

We give some other descriptions for $\mathbb{Z}_\alpha$. Let again α be an algebraic number of degree n, and denote by f_α its primitive minimal polynomial, i.e., $f_\alpha = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ with $a_0 > 0$ and $\gcd(a_0, \ldots, a_n) = 1$. Then $\mathbb{Z}_\alpha$ is the $\mathbb{Z}$-module with basis

$$1, \omega_1, \ldots, \omega_{n-1}, \quad \omega_i = a_0\alpha^i + a_1\alpha^{i-1} + \cdots a_{i-1}\alpha \quad (i = 1, \ldots, n-1) \tag{1.3}$$

(see [10, p. 365, Thm. 16.2.9, formula (16.2.7)] or Lemma 2.1 in the present paper). This is precisely the invariant order of f_α as defined by Nakagawa [15] and Simon [16]. Del Corso, Dvornicich and Simon [6, Prop. 2] (see also Lemma 2.1 in the present paper) proved the much simpler expression

$$\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}].$$

From the basis (1.3) one deduces that the discriminant of the order $\mathbb{Z}_\alpha$ is

equal to the discriminant of f_α, i.e.,

$$\begin{aligned} D(\mathbb{Z}_\alpha) &= D_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \omega_1, \dots, \omega_{n-1}) \\ &= a_0^{2n-2} D_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}) \\ &= a_0^{2n-2} \prod_{1 \le i < j \le n} (\alpha^{(i)} - \alpha^{(j)})^2 = D(f_\alpha), \end{aligned} \tag{1.4}$$

where $\alpha^{(1)}, \dots, \alpha^{(n)}$ are the conjugates of α.

The orders $\mathbb{Z}_\alpha$ are part of a much more general theory on invariant rings of binary forms (see [15], [17], [6], [19], [10, Chap. 16]). We briefly comment on this at the end of this section.

It follows from the work of Birch and Merriman [5] on binary forms that an order of a number field has at most finitely many rational monogenizations. Győry and the author [8, Cor. 2] proved that every algebraic number α of degree n is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to an algebraic number α^* with height $H(\alpha^*) \le C(n, D)$, where $H(\alpha^*)$ is the maximum of the absolute values of the coefficients of f_{α^*}, D is the discriminant of f_α, and $C(n, D)$ is effectively computable. Together with (1.4) this implies that it can be decided effectively whether a given order of a number field has rational monogenizations and that these can be determined effectively.

It can be shown that a rationally monogenic order $\mathcal{O}$ of a number field of degree ≥ 3 is *primitive*, i.e., there are no order $\mathcal{O}'$ and integer $a > 1$ such that $\mathcal{O} = \mathbb{Z} + a\mathcal{O}'$. It follows from classical work of Delone and Faddeev [7] that every primitive order of a cubic number field has precisely one rational monogenization. Further, work of Bérczes, Győry and the author [1] implies that an order of a number field of degree $n \ge 4$ cannot have more than $n \cdot 2^{24n^3}$ rational monogenizations. Győry and the author [10, Chap. 17] improved this to 2^{5n^2}. From recent work of Bhargava [3] it follows that for quartic orders this bound can be improved to 40.

We are now ready to state the main result of this paper, which gives a generalization of Theorem B to not necessarily integral algebraic numbers α.

Theorem 1.1.

(i) *Let K be a quartic number field. Then K has only finitely many orders with more than two rational monogenizations.*
(ii) *Let K be a number field of degree ≥ 5 and suppose that the Galois group of its normal closure is 5-transitive. Then K has only finitely many orders with more than one rational monogenization.*

Theorem C implies that there are quartic number fields, having infinitely many orders with two rational monogenizations. We do not know whether the condition on the normal closure of K is necessary if $[K : \mathbb{Q}] \ge 5$. Probably, trying to remove or relax this condition would considerably complicate the proof.

The proof of Theorem 1.1 uses, among other things, finiteness results for unit equations in more than two unknowns. The present proofs of these depend on ineffective methods from Diophantine approximation, e.g., Schmidt's Subspace Theorem or the Faltings–Rémond method. As a consequence, our proof of Theorem 1.1 is ineffective in that it does not allow one to determine the exceptional orders. Further, although for unit equations we have good upper bounds for the number of solutions, it is because of the 'other things' that we cannot give an upper bound for the number of exceptional orders.

We state a consequence, which partly confirms Conjecture 4.2 in [4]. We adopt the terminology of [4]. Given a number field K, denote by $\mathcal{PI}(K)$ the set of primitive, irreducible polynomials $f \in \mathbb{Z}[X]$, such that there is α with $f(\alpha)=0$ and $\mathbb{Q}(\alpha)=K$. We call two polynomials $f, g \in \mathcal{PI}(K)$ $\mathrm{GL}_2(\mathbb{Z})$-*equivalent* if there is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $g(X) = \pm(cX+d)^{\deg f} f\left(\frac{aX+b}{cX+d}\right)$. Further, f and g are called *Hermite equivalent* if there are α, β such that $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)=K$, $f(\alpha)=0$, $g(\beta)=0$ and $\mathcal{M}_\beta = \lambda \mathcal{M}_\alpha$ for some $\lambda \in K^*$ (see (1.1) above). It was shown in [4] that $\mathrm{GL}_2(\mathbb{Z})$-equivalent polynomials are Hermite equivalent. As we will show, Theorem 1.1 implies the following, which except for the assumption on the normal closure of K is [4, Conjecture 4.2].

THEOREM 1.2.

(i) *Let K be a quartic number field. Then there are only finitely many Hermite equivalence classes in $\mathcal{PI}(K)$ that fall apart into more than two $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes.*

(ii) *Let K be a number field of degree ≥ 5 such that the Galois group of its normal closure is 5-transitive. Then there are only finitely many Hermite equivalence classes in $\mathcal{PI}(K)$ that fall apart into more than one $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.*

Another consequence of our investigations, which probably could be proved by other means as well, is the following.

THEOREM 1.3. *Let K be a number field of degree ≥ 3. Then K has infinitely many orders that are rationally monogenic but not monogenic.*

Finally, we would like to comment on the connection between the orders $\mathbb{Z}_\alpha$ defined above, and invariant orders of binary forms. Birch and Merriman [5] introduced for a binary form

$$F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X,Y]$$

that is irreducible over $\mathbb{Q}$ the $\mathbb{Z}$-module $\mathbb{Z}_F$ with $\mathbb{Z}$-basis $1, \omega_1, \ldots, \omega_{n-1}$ given by (1.3), where $F(\alpha,1)=0$. Nakagawa [15] proved that $\mathbb{Z}_F$ is an order of the number field $\mathbb{Q}(\alpha)$, in fact,

$$\omega_i\omega_j = -\sum_{\max(i+j-n,1)\leq k\leq i} a_{i+j-k}\omega_k + \sum_{j<k\leq \min(i+j,n)} a_{i+j-k}\omega_k \tag{1.5}$$

for $i, j = 1, \ldots, n-1$, where $\omega_n := -a_n$. Thus, $\mathbb{Z}_F$ is called the *invariant ring* or *order* of F. This order was further studied by Simon [16, 17] and Del Corso, Dvornicich and Simon [6].

Notice that in the definition of $\mathbb{Z}_F$ we have not required that the coefficients of F have greatest common divisor 1. Our order $\mathbb{Z}_\alpha$ is just $\mathbb{Z}_F$ where $F(X,Y) = Y^{\deg \alpha} f_\alpha(X/Y)$ is an irreducible binary form whose coefficients have greatest common divisor 1.

More generally, given any commutative ring R and binary form $F = \sum_{i=0}^n a_i X^{n-i} Y^i \in R[X,Y]$, one can formally define the invariant ring R_F of F by taking the free R-module with basis $1, \omega_1, \ldots, \omega_{n-1}$ with prescribed multiplication table (1.5). Here, it is no longer required that F is irreducible, nor even that $a_0 \neq 0$, and even $a_0 = \cdots = a_n = 0$ is allowed. Wood [19] studied invariant rings of binary forms in a much broader context.

The remainder of our paper is organized as follows. In Section 2 we have collected some basic properties of rationally monogenic orders. Although these are all known, we have provided proofs for convenience of the reader. Sections 3 and 4 contain preparations, where in Section 3 we apply finiteness results for unit equations. In Section 5 we finish the proofs of Theorems 1.1–1.3. Finally, in Section 6 we generalize the orders $\mathbb{Z}_\alpha$ to domains $\mathcal{O}_{S,\alpha}$, where $\mathcal{O}_S$ is the ring of S-integers of a number field $\Bbbk$ and α is algebraic over $\Bbbk$, and state and prove a generalization of Theorem 1.1 but with a notion of equivalence that is slightly weaker than $\mathrm{GL}_2(\mathcal{O}_S)$-equivalence.

2. Lemmas over principal ideal domains. In this section, we have collected some generalities on rationally monogenic orders. We state and prove everything over an arbitrary principal ideal domain A of characteristic 0. Most of the results in this section have been proved elsewhere in a more general context (see for instance [10, Chaps. 16 and 17], [1], [6]). For convenience of the reader we have repeated the short proofs, specialized to the situation of this paper. In the proofs of Theorems 1.1–1.3 we apply the results of the present section with $A = \mathbb{Z}$. In Section 6 we use a local-to-global argument, and apply the results of the present section to localizations of $\mathcal{O}_S$.

In what follows, if F is any field, $\xi \in \mathbb{P}^1(F) := F \cup \{\infty\}$ and $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(F)$, we write $C\xi := \frac{a\xi+b}{c\xi+d}$, with the conventions that this is ∞ if $\xi = \infty$ and $c = 0$; a/c if $\xi = \infty$ and $c \neq 0$; and ∞ if $c \neq 0$ and $\xi = -d/c$.

Let A be a principal ideal domain of characteristic 0, and $\Bbbk$ its field of fractions. Fix a finite extension K of $\Bbbk$ of degree $n \geq 3$. Let L be its normal closure over $\Bbbk$ and $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the $\Bbbk$-isomorphic embeddings of K in L. Further, denote by A_K, A_L the integral closures of A in K and L, respectively. Recall that both A_K, A_L are Dedekind domains; in the case that $A = \mathbb{Z}$, A_K and A_L are just the rings of integers of K and L.

Given any domain $B \supseteq A$, we call $\alpha, \beta \in K$ $\mathrm{GL}_2(B)$-*equivalent* if there is $C \in \mathrm{GL}_2(B)$ such that $\beta = C\alpha$.

Let $\alpha \in K$ with $K = \Bbbk(\alpha)$. Define the free A-module

$$\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in A\} \tag{2.1}$$

and its ring of scalars

$$A_\alpha := \{\xi \in K : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}. \tag{2.2}$$

As one easily verifies, if α, β are two $\mathrm{GL}_2(A)$-equivalent elements of A, then $\mathcal{M}_\alpha = \lambda\mathcal{M}_\beta$ for some $\lambda \in K^*$, and thus $A_\alpha = A_\beta$.

We give some other descriptions of A_α. Let $f_\alpha = a_0X^n + \cdots + a_n \in A[X]$ be a primitive minimal polynomial of α, i.e., with $\gcd(a_0, \ldots, a_n) = 1$. Such a polynomial exists since A is a principal ideal domain.

Lemma 2.1. *We have*

$$A_\alpha = \{x_0 + x_1\omega_1 + \cdots + x_{n-1}\omega_{n-1} : x_0, \ldots, x_{n-1} \in A\} \tag{2.3}$$

where

$$\omega_i := a_0\alpha^i + a_1\alpha^{i-1} + \cdots + a_{i-1}\alpha \quad (i = 1, \ldots, n-1),$$

and

$$A_\alpha = A[\alpha] \cap A[\alpha^{-1}]. \tag{2.4}$$

Identity (2.3) follows from [10, p. 365, Thm. 16.2.9, formula (16.2.7)]), while (2.4) is a consequence of [6, Prop. 2]. For the convenience of the reader, we repeat the proofs.

Proof of Lemma 2.1. Let $\mathcal{N}_\alpha$ denote the A-module on the right-hand side of (2.3). We prove the inclusions $\mathcal{N}_\alpha \subseteq A_\alpha \subseteq A[\alpha] \cap A[\alpha^{-1}] \subseteq \mathcal{N}_\alpha$.

First observe that if $1 \le i \le n-1$, $0 \le j \le n-1$, then

$$\omega_i\alpha^j = \sum_{k=0}^{i-1} a_k\alpha^{i+j-k} \in \mathcal{M}_\alpha \qquad \text{if } i + j \le n-1,$$

$$\omega_i\alpha^j = (\omega_i - f_\alpha(\alpha))\alpha^j = -\sum_{k=i}^{n} a_k\alpha^{i+j-k} \in \mathcal{M}_\alpha \qquad \text{if } i + j \ge n,$$

implying $\mathcal{N}_\alpha \subseteq A_\alpha$.

Second, $A_\alpha \subseteq \mathcal{M}_\alpha \cap \alpha^{1-n}\mathcal{M}_\alpha \subseteq A[\alpha] \cap A[\alpha^{-1}]$.

Third, let $\xi = P(\alpha) = Q(\alpha^{-1}) \in A[\alpha] \cap A[\alpha^{-1}]$, where $P, Q \in A[X]$. We prove by induction on $\deg P$ that $\xi \in \mathcal{N}_\alpha$. For $\deg P = 0$ this is clear. Let $\deg P = r \ge 1$. Consider the polynomial

$$H(X) := X^{\deg Q}P(X) - X^{\deg Q}Q(X^{-1}) \in A[X].$$

The polynomial H is non-zero, since otherwise $P(X) = Q(X^{-1})$, which is impossible. Let b be the leading coefficient of P. Then b is also the leading

coefficient of H. Since $H(\alpha)=0$, f_α must divide H in $\Bbbk[X]$. But by assumption, the coefficients of f_α have gcd 1, so by Gauss' Lemma f_α divides H in $A[X]$, in particular, the leading coefficient a_0 of f_α divides b. Now if $r \geq n$, we have $P(\alpha)=P^*(\alpha)$ where $P^*(X)=P(X)-(b/a_0)X^{r-n}f_\alpha(X)$ is a polynomial in $A[X]$ of degree $<r$ and we can apply the induction hypothesis. If $r<n$, then $P(\alpha)=(b/a_0)\omega_r+P^*(\alpha)$, where $P^*\in A[X]$ has degree $<r$. We already know that $\omega_r \in A[\alpha]\cap A[\alpha^{-1}]$, so $P^*(\alpha)\in A[\alpha]\cap A[\alpha^{-1}]$. We can again apply the induction hypothesis. ∎

Let $\mathcal{M}$ be an A-submodule of A_K with basis $\gamma_1,\dots,\gamma_n$, say, where $n=[K:\Bbbk]$. The *discriminant ideal* $\mathfrak{d}_{\mathcal{M}/A}$ of $\mathcal{M}$ over A is defined as the ideal of A generated by $D_{K/\Bbbk}(\gamma_1,\dots,\gamma_n):=(\det(\gamma_i^{(j)})_{i,j=1,\dots,n})^2$. This does not depend on the choice of basis.

LEMMA 2.2. *Let $\alpha\in K$ with $\Bbbk(\alpha)=K$ and let $f_\alpha=a_0X^n+\cdots+a_n\in A[X]$ be a primitive minimal polynomial of α. Then $\mathfrak{d}_{A_\alpha/A}=D(f_\alpha)A$, where $D(f_\alpha)=a_0^{2n-2}\prod_{1\leq i<j\leq n}(\alpha^{(i)}-\alpha^{(j)})^2$.*

Proof. Same reasoning as in (1.4). ∎

For $\alpha_1,\dots,\alpha_r\in L$, denote by $[\alpha_1,\dots,\alpha_r]$ the fractional ideal of A_L, i.e., A_L-module, generated by $\alpha_1,\dots,\alpha_r$. Further, for a finitely generated A-submodule $\mathcal{M}$ of K and for distinct $i,j\in\{1,\dots,n\}$, let $\mathfrak{d}_{ij}(\mathcal{M})$ be the fractional ideal of A_L generated by $\xi^{(i)}-\xi^{(j)}$ for all $\xi\in\mathcal{M}$. Thus, if $\mathcal{M}$ is generated as an A-module by $\xi_1,\dots,\xi_r$, we have

$$\mathfrak{d}_{ij}(\mathcal{M})=[\xi_1^{(i)}-\xi_1^{(j)},\dots,\xi_r^{(i)}-\xi_r^{(j)}]. \tag{2.5}$$

LEMMA 2.3. *Let α be such that $K=\Bbbk(\alpha)$ and $i,j\in\{1,\dots,n\}$ with $i\neq j$. Then*

$$[\alpha^{(i)}-\alpha^{(j)}]=[1,\alpha^{(i)}]\cdot[1,\alpha^{(j)}]\cdot\mathfrak{d}_{ij}(A_\alpha).$$

Proof (cf. [10, Lemma 17.6.4]). Let $\omega_1,\dots,\omega_{n-1}$ be as in (2.3). Then

$$\alpha f_\alpha(X)=(X-\alpha)(\omega_1X^{n-1}+\omega_2X^{n-2}+\cdots+\omega_n),$$

where $\omega_n:=-a_n$. This implies

$$\begin{aligned}&(\alpha^{(i)}-\alpha^{(j)})Xf_\alpha(X)\\&=(X-\alpha^{(j)})\alpha^{(i)}f_\alpha(X)-(X-\alpha^{(i)})\alpha^{(j)}f_\alpha(X)\\&=(X-\alpha^{(i)})(X-\alpha^{(j)})\cdot((\omega_1^{(i)}-\omega_1^{(j)})X^{n-1}+\cdots+(\omega_{n-1}^{(i)}-\omega_{n-1}^{(j)})).\end{aligned}$$

We apply Gauss' lemma for Dedekind domains, which in our case asserts that if $g_1,g_2\in L[X]$ then $[g_1g_2]=[g_1]\cdot[g_2]$, where $[g]$ is the fractional ideal of A_L generated by the coefficients of $g\in L[X]$. Using the fact that the

coefficients of f_α have gcd 1, together with (2.3) and (2.5), we obtain

$$\begin{aligned}[\alpha^{(i)} - \alpha^{(j)}] &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot [\omega_1^{(i)} - \omega_1^{(j)}, \dots, \omega_{n-1}^{(i)} - \omega_{n-1}^{(j)}] \\ &= [1, \alpha^{(i)}] \cdot [1, \alpha^{(j)}] \cdot \mathfrak{d}_{ij}(A_\alpha). \ \blacksquare\end{aligned}$$

If $[K : \Bbbk] = n \geq 4$ then for α with $K = \Bbbk(\alpha)$ and pairwise distinct $i, j, k, l \in \{1, \dots, n\}$, we define the *cross ratio*

$$\mathrm{cr}_{ijkl}(\alpha) := \frac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})}. \tag{2.6}$$

LEMMA 2.4. *Suppose* $[K : \Bbbk] = n \geq 4$. *Let* α, β *be such that* $\Bbbk(\alpha) = \Bbbk(\beta) = K$ *and* $A_\alpha = A_\beta$. *Then for all pairwise distinct* $i, j, k, l \in \{1, \dots, n\}$ *we have*

$$\frac{\mathrm{cr}_{ijkl}(\alpha)}{\mathrm{cr}_{ijkl}(\beta)} \in A_L^*.$$

Proof. Lemma 2.3 implies $[\mathrm{cr}_{ijkl}(\alpha)] = [\mathrm{cr}_{ijkl}(\beta)]$ for all i, j, k, l. ∎

LEMMA 2.5. *Let* K *be a finite extension of* $\Bbbk$, *and let* α, β *be such that* $\Bbbk(\alpha) = \Bbbk(\beta) = K$.

(i) *Suppose that* $[K : \Bbbk] = 3$. *Then* α, β *are* $\mathrm{GL}_2(\Bbbk)$*-equivalent.*
(ii) *Suppose* $[K : \Bbbk] = n \geq 4$. *Then* α, β *are* $\mathrm{GL}_2(\Bbbk)$*-equivalent if and only if* $\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta)$ *for all pairwise distinct* $i, j, k, l \in \{1, \dots, n\}$.

Proof (cf. [10, Lemma 17.7.2]). (ii) From elementary projective geometry, we know that $\mathrm{cr}_{ijkl}(\alpha) = \mathrm{cr}_{ijkl}(\beta)$ for all pairwise distinct $i, j, k, l \in \{1, \dots, n\}$ if and only if there is $C \in \mathrm{GL}_2(L)$ such that $\beta^{(i)} = C\alpha^{(i)}$ for $i = 1, \dots, n$. Suppose the latter to be the case. Then since $n \geq 4$, the matrix C is determined uniquely up to a scalar. Clearly, we have $\beta^{(i)} = \sigma(C)\alpha^{(i)}$ for $i = 1, \dots, n$ and every $\sigma \in \mathrm{Gal}(L/\Bbbk)$. If we assume that one of the entries of C is 1, then $\sigma(C) = C$ for every $\sigma \in \mathrm{Gal}(L/\Bbbk)$, i.e., $C \in \mathrm{GL}_2(\Bbbk)$.

(i) By elementary projective geometry, there is a unique (up to a scalar factor) $C \in \mathrm{GL}_2(L)$ such that $\beta^{(i)} = C\alpha^{(i)}$ for $i = 1, 2, 3$. If we take C such that one of its entries is 1 then similarly to above it follows that $C \in \mathrm{GL}_2(\Bbbk)$. ∎

LEMMA 2.6. *Assume that* $[K : \Bbbk] \geq 3$. *Let* α, β *be such that* $\Bbbk(\alpha) = \Bbbk(\beta) = K$ *and* $A_\alpha = A_\beta$. *Suppose that* α, β *are* $\mathrm{GL}_2(\Bbbk)$*-equivalent. Then* α, β *are* $\mathrm{GL}_2(A)$*-equivalent.*

Proof (cf. [10, Proposition 17.6.5]). Since A is a principal ideal domain, we may assume that $\beta = C\alpha$, where the entries of C belong to A and have gcd 1. Further, C can be put in Smith Normal Form, i.e., there are matrices $U, V \in \mathrm{GL}_2(A)$ such that $UCV = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in A \setminus \{0\}$. Let $\beta_1 := U\beta$, $\alpha_1 := V^{-1}\alpha$. Then since $\alpha, \beta \notin \Bbbk$ we have $\alpha_1, \beta_1 \neq \infty$, and moreover $A_{\alpha_1} = A_{\beta_1}$ and $\beta_1 = a\alpha_1$. We have to show that $a \in A^*$.

Let $f_{\alpha_1}(X) = a_0X^n + \cdots + a_n \in A[X]$ be a primitive minimal polynomial of α_1, i.e., with $\gcd(a_0, \ldots, a_n) = 1$. Then β_1 has primitive minimal polynomial

$$f_{\beta_1}(X) = \lambda f_{\alpha_1}(X/a) = \lambda(a^{-n}a_0X^n + a^{1-n}a_1X^{n-1} + \cdots + a_n),$$

where $\lambda \in \Bbbk$ is such that the coefficients of f_{β_1} are in A and have gcd 1. By (2.3), A_{α_1} is a free A-module with basis $1, \omega_1, \ldots, \omega_{n-1}$ with $\omega_i = \sum_{k=0}^{i-1} a_k\alpha_1^{i-k}$ for $i = 1, \ldots, n-1$. By replacing α_1 with $\beta_1 = a\alpha_1$, and a_i by $\lambda a^{i-n}a_i$, we see that A_{β_1} has basis $1, \lambda a^{1-n}\omega_1, \lambda a^{2-n}\omega_2, \ldots, \lambda a^{-1}\omega_{n-1}$. Since $A_{\alpha_1} = A_{\beta_1}$, this must imply

$$\lambda a^{i-n} \in A^* \quad \text{for } i = 1, \ldots, n-1,$$

hence $a \in A^*$ and $\lambda \in A^*$. ∎

3. Application of unit equations. Let K be a number field of degree $n \geq 4$ and L its normal closure. In the case $n = 4$ we do not impose any constraints on L, while for $n \geq 5$ we assume that $\mathrm{Gal}(L/\mathbb{Q})$ is 5-transitive.

We call $\alpha_1 \in K$ *k-special* if $K = \mathbb{Q}(\alpha_1)$ and there are $\alpha_2, \ldots, \alpha_k$ such that $\mathbb{Z}_{\alpha_1} = \cdots = \mathbb{Z}_{\alpha_k}$ and $\alpha_1, \ldots, \alpha_k$ are pairwise $\mathrm{GL}_2(\mathbb{Z})$-inequivalent. We call α_1 *special* if it is 2-special.

Theorem 1.1 follows, once we have shown that in the case $n = 4$, the 3-special numbers of K lie in only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, and in the case $n \geq 5$ that the special numbers of K lie in only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. Indeed, the orders of K with k rational monogenizations are all of the shape $\mathbb{Z}_\alpha$ where α is k-special, and if such α lie in only finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes, there are only finitely many orders $\mathbb{Z}_\alpha$.

In the present section we prove the following proposition. Here, we apply some results from the theory of unit equations.

Proposition 3.1.

(i) *Let K be a quartic number field. Then the set of 3-special numbers of K is contained in finitely many $\mathrm{GL}_2(\mathbb{Q})$-equivalence classes.*

(ii) *Let K be a number field of degree $n \geq 5$ such that the Galois group of its normal closure L is 5-transitive. Then the set of special numbers of K is contained in finitely many $\mathrm{GL}_2(\mathbb{Q})$-equivalence classes.*

We will show later (see Proposition 5.1 below) that the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of a special number is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes.

We start with some initial observations. Let $\alpha, \beta \in K$ with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$, $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and α, β $\mathrm{GL}_2(\mathbb{Z})$-inequivalent. Then

$$\mathrm{cr}_{ijkl}(\alpha) \neq \mathrm{cr}_{ijkl}(\beta) \quad \text{for all pairwise distinct } i, j, k, l \in \{1, \ldots, n\}. \tag{3.1}$$

Indeed, suppose that for some tuple (i,j,k,l), say $(1,2,3,4)$, we have equality. In the case $n=4$ this implies equality for each permutation (i,j,k,l) of $(1,2,3,4)$ since $\mathrm{cr}_{ijkl}(\cdot)$ is a fractional linear transformation of $\mathrm{cr}_{1234}(\cdot)$. In the case $n \geq 5$, we obtain equality for all i,j,k,l since by our assumption on the normal closure L, there is $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ that maps $\mathrm{cr}_{1234}(\cdot)$ to $\mathrm{cr}_{ijkl}(\cdot)$. Lemma 2.5 now implies that α, β are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, and subsequently Lemma 2.6 implies that α, β are $\mathrm{GL}_2(\mathbb{Z})$-equivalent, contrary to our assumption.

Another important observation is the identity for cross ratios

$$\mathrm{cr}_{ijkl}(\alpha) + \mathrm{cr}_{ilkj}(\alpha) = 1 \tag{3.2}$$

for all $\alpha \in K$ and all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$. Now let α, β be such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Put

$$\varepsilon_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)};$$

then from (3.2) and Lemma 2.4 we deduce

$$\mathrm{cr}_{ijkl}(\alpha) \cdot \varepsilon_{ijkl} + \mathrm{cr}_{ilkj}(\alpha) \cdot \varepsilon_{ilkj} = 1, \quad \varepsilon_{ijkl} \in \mathcal{O}_L^*,\ \varepsilon_{ilkj} \in \mathcal{O}_L^*, \tag{3.3}$$

where $\mathcal{O}_L$ is the ring of integers of L. This allows us to apply the theory of unit equations.

We first prove part (i), and then part (ii).

Proof of Proposition 3.1(i). Let K be a quartic number field, and let $\alpha \in K$ be 3-special. Choose $\beta, \gamma \in K$ such that α, β, γ are pairwise $\mathrm{GL}_2(\mathbb{Z})$-inequivalent, and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta = \mathbb{Z}_\gamma$. Put

$$\varepsilon_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)}, \qquad \eta_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\gamma)}{\mathrm{cr}_{ijkl}(\alpha)}$$

for each permutation (i,j,k,l) of $(1,2,3,4)$.

By (3.1)–(3.3), the pairs $(1,1)$, $(\varepsilon_{1234}, \varepsilon_{1432})$, $(\eta_{1234}, \eta_{1432})$ are three distinct solutions to the equation

$$\mathrm{cr}_{1234}(\alpha)x + \mathrm{cr}_{1432}(\alpha)y = 1 \quad \text{in } x, y \in \mathcal{O}_L^*. \tag{3.4}$$

We now apply the following result on unit equations [1].

LEMMA 3.2. *Let F be a field of characteristic 0 and Γ a subgroup of F^* of finite rank. Then there are only finitely many pairs $(a,b) \in F^* \times F^*$ with $a+b=1$ such that the equation*

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

has more than two solutions, the pair $(1,1)$ included.

---

[1] Equations with unknowns from a multiplicative group Γ of finite rank are often called *unit equations* since in most applications, Γ is the unit group of a domain.

Proof. This is essentially a result of Győry, Stewart, Tijdeman, and the author [11, Thm. 1]; see also [9, Thm. 6.1.6]. Their proof uses a finiteness result for linear unit equations in several unknowns, which in turn follows from Schmidt's Subspace Theorem. ∎

We continue with the proof of Proposition 3.1(i). Since (3.4) has three distinct solutions in $\mathcal{O}_L^*$ including $(1,1)$, and $\mathcal{O}_L^*$ is finitely generated, Lemma 3.2 implies that if α runs through the 3-special numbers of K, then $\mathrm{cr}_{1234}(\alpha)$ runs through a finite set. If (i,j,k,l) is a permutation of $(1,2,3,4)$, then $\mathrm{cr}_{ijkl}(\cdot)$ is a fractional linear transformation of $\mathrm{cr}_{1234}(\cdot)$, hence $\mathrm{cr}_{ijkl}(\alpha)$ runs through a finite set as well. Now Lemma 2.5(ii) implies that the 3-special numbers $\alpha \in K$ lie in only finitely many $\mathrm{GL}_2(\mathbb{Q})$-equivalence classes. ∎

Proof of Proposition 3.1(ii). Let K be a number field of degree $n \geq 5$ such that the Galois group of its normal closure L is 5-transitive. Take a special $\alpha \in K$. Choose β such that $\mathbb{Z}_\beta = \mathbb{Z}_\alpha$. Recall that by Lemma 2.4,

$$\varepsilon_{ijkl} := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} \in \mathcal{O}_L^*$$

for all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$. Viewing (3.2) and (3.3) as linear equations in $\mathrm{cr}_{ijkl}(\alpha)$ and $\mathrm{cr}_{lijk}(\alpha)$, from Cramer's rule we derive

$$\mathrm{cr}_{ijkl}(\alpha) = \frac{\varepsilon_{ilkj} - 1}{\varepsilon_{ilkj} - \varepsilon_{ijkl}}. \tag{3.5}$$

Our strategy is as follows. Using algebraic relations between the ε_{ijkl} and finiteness results for unit equations, we show that if α runs through the special numbers of K, then one of the ε_{ijkl}, say ε_{1234}, runs through a finite set. Our assumption that $\mathrm{Gal}(L/\mathbb{Q})$ is 5-transitive implies that the numbers ε_{ijkl} are all conjugate to one another, thus it follows that ε_{ijkl} runs through a finite set for all i,j,k,l. But then (3.5) implies that $\mathrm{cr}_{ijkl}(\alpha)$ runs through a finite set for all i,j,k,l. Finally, Lemma 2.5(ii) implies that the special numbers $\alpha \in K$ lie in only finitely many $\mathrm{GL}_2(\mathbb{Q})$-equivalence classes.

We first collect some algebraic relations between the ε_{ijkl}. It is straightforward to verify

$$\begin{cases} \varepsilon_{ijkl} = \varepsilon_{jilk} = \varepsilon_{klij} = \varepsilon_{lkji}, \\ \varepsilon_{ijkl}^{-1} = \varepsilon_{ikjl}, \\ \dfrac{\varepsilon_{ijkl}}{\varepsilon_{ijlk}} = \varepsilon_{ilkj} \end{cases} \tag{3.6}$$

for all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$ and moreover,

$$\frac{\varepsilon_{ijkl}}{\varepsilon_{ijkm}} = \varepsilon_{jmlk} \tag{3.7}$$

for all pairwise distinct $i,j,k,l,m \in \{1,\dots,n\}$.

We derive a few more relations. From (3.5) and (3.6) it follows that $\mathrm{cr}_{ijkl}(\beta) = \varepsilon_{ijkl}\mathrm{cr}_{ijkl}(\alpha) = \frac{\varepsilon_{ilkj}-1}{\varepsilon_{iljk}-1}$. Picking a fifth index m, we get

$$1 = \frac{\mathrm{cr}_{jmlk}(\beta)\mathrm{cr}_{ijkm}(\beta)}{\mathrm{cr}_{ijkl}(\beta)} = \frac{\varepsilon_{jklm}-1}{\varepsilon_{jkml}-1} \cdot \frac{\varepsilon_{imkj}-1}{\varepsilon_{imjk}-1} \cdot \frac{\varepsilon_{iljk}-1}{\varepsilon_{ilkj}-1}.$$

We apply this with $(i,j,k,l,m) = (5,1,2,3,4)$. Thus, we obtain

$$(\varepsilon_{1234}-1)(\varepsilon_{1245}-1)(\varepsilon_{1253}-1) = (\varepsilon_{1243}-1)(\varepsilon_{1254}-1)(\varepsilon_{1235}-1), \tag{3.8}$$

where, as mentioned before, all entries belong to $\mathcal{O}_L^*$. We apply the following result.

LEMMA 3.3. *Let F be a field of characteristic 0 and Γ a subgroup of F^* of finite rank. Consider the equation*

$$(x_1-1)(x_2-1)(x_3-1) = (y_1-1)(y_2-1)(y_3-1) \quad \text{in } x_1,x_2,x_3,y_1,y_2,y_3 \in \Gamma. \tag{3.9}$$

There is a finite subset $\mathcal{S}$ of Γ such that every solution of (3.9) *satisfies one of the following:*

(a) *at least one of $x_1,\dots,y_3$ belongs to $\mathcal{S}$;*
(b) *there are $s_1,s_2,s_3 \in \{\pm 1\}$ such that (x_1,x_3,x_3) is a permutation of $(y_1^{s_1},y_2^{s_2},y_3^{s_3})$;*
(c) *at least one of the numbers in $\{x_ix_j, x_i/x_j, y_iy_j, y_i/y_j : 1 \le i < j \le 3\}$ is either -1 or a primitive cube root of unity.*

Proof. This is a result of Bérczes, Győry, and the author [2, Prop. 8.1]. They deduced the above lemma from a finiteness result for linear unit equations in several unknowns, and so again Schmidt's Subspace Theorem is in the background. ∎

We apply Lemma 3.3 with $\Gamma = \mathcal{O}_L^*$ to (3.8). We show that each of the three cases (a)–(c) gives rise to only finitely many possible values for ε_{1234}. Recall that we assume that $\mathrm{Gal}(L/\mathbb{Q})$ is 5-transitive. Hence for any two quintuples of distinct indices (i,j,k,l,m) and (i',j',k',l',m'), there is $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ mapping $\alpha^{(i)},\beta^{(i)},\dots,\alpha^{(m)},\beta^{(m)}$ to $\alpha^{(i')},\beta^{(i')},\dots,\alpha^{(m')},\beta^{(m')}$, respectively. Consequently, any two ε_{ijkl}, $\varepsilon_{i'j'k'l'}$ are conjugate to each other. Similarly, from an identity between ε-s with indices from a quintuple (i,j,k,l,m) we can derive a similar identity with indices from (i',j',k',l',m') by applying a suitable element of $\mathrm{Gal}(L/\mathbb{Q})$.

The above observations imply that if we have shown that one of the ε_{ijkl} runs through a finite set, then so does ε_{1234}. This settles case (a). As for (b) and (c), using again the above observations, we are left with the following subcases. Let $\mathcal{T}$ denote the group of 6th roots of unity in L.

CASE b1. $\varepsilon_{1234} = \varepsilon_{1243}$. Then by (3.6), $\varepsilon_{1432} = \frac{\varepsilon_{1234}}{\varepsilon_{1243}} = 1$, which by conjugacy implies $\varepsilon_{1234} = 1$.

CASE b2. $\varepsilon_{1234} = \varepsilon_{1243}^{-1}$. By (3.6), $\varepsilon_{1243}^{-1} = \varepsilon_{1234}^{-1}\varepsilon_{1432}$, so $\varepsilon_{1234}^2 = \varepsilon_{1432}$. By conjugacy, we may interchange the indices 2 and 3, while keeping 1 and 4 fixed, so we also have $\varepsilon_{1324} = \varepsilon_{1342}^{-1}$. Applying again (3.6), this gives $\varepsilon_{1234} = \varepsilon_{1432}^{-1}$. Hence $\varepsilon_{1234}^3 = 1$.

CASE b3. $\varepsilon_{1234} = \varepsilon_{1254}$. By (3.6) and (3.7), $1 = \frac{\varepsilon_{1234}}{\varepsilon_{1254}} = \frac{\varepsilon_{2143}}{\varepsilon_{2145}} = \varepsilon_{1534}$. By conjugacy, $\varepsilon_{1234} = 1$.

CASE b4. $\varepsilon_{1234} = \varepsilon_{1254}^{-1}$. By conjugacy, we may interchange 2 and 3, keeping $1, 4, 5$ fixed, so we have $\varepsilon_{1324} = \varepsilon_{1354}^{-1}$, which together with (3.6) implies $\varepsilon_{1234} = \varepsilon_{1354}$. From (3.6) and (3.7) we deduce $\frac{\varepsilon_{1254}}{\varepsilon_{1354}} = \varepsilon_{1234}$. Multiplying these relations together, we obtain $\varepsilon_{1234}^3 = 1$.

CASE c1. $\varepsilon_{1234} \cdot \varepsilon_{1245} \in \mathcal{T}$. By interchanging 3 and 5, and keeping $1, 2, 4$ fixed, we see that $\varepsilon_{1254} \cdot \varepsilon_{1243} \in \mathcal{T}$. Using (3.6) and (3.7), we get

$$\frac{\varepsilon_{1234} \cdot \varepsilon_{1245}}{\varepsilon_{1254} \cdot \varepsilon_{1243}} = \frac{\varepsilon_{1534}}{\varepsilon_{2534}} = \varepsilon_{1532} \in \mathcal{T}$$

and by conjugacy, $\varepsilon_{1234} \in \mathcal{T}$.

CASE c2. $\frac{\varepsilon_{1234}}{\varepsilon_{1245}} \in \mathcal{T}$. Interchanging 2 and 3, and keeping $1, 4, 5$ fixed, we obtain $\frac{\varepsilon_{1324}}{\varepsilon_{1345}} \in \mathcal{T}$, and then, using $\varepsilon_{1324} = \varepsilon_{1234}^{-1}$, we get $\varepsilon_{1245} \cdot \varepsilon_{1345} \in \mathcal{T}$. By taking conjugates, we obtain $\varepsilon_{1234} \cdot \varepsilon_{1235} \in \mathcal{T}$, and also $\varepsilon_{1234} \cdot \varepsilon_{5234} \in \mathcal{T}$. Applying (3.7), the latter yields $\varepsilon_{1234} \cdot \frac{\varepsilon_{1234}}{\varepsilon_{1235}} \in \mathcal{T}$. Hence $\varepsilon_{1234}^3 \in \mathcal{T}$.

As mentioned above, this completes the proof of Proposition 3.1. ∎

4. Investigation of $\mathrm{GL}_2(\Bbbk)$-classes. Let K be a number field of degree ≥ 4. In the next section we show (Proposition 5.1) that the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of each special number in K is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. Together with Proposition 3.1 this will imply Theorem 1.1. In the present section, we develop some machinery needed for the proof of Proposition 5.1. We have worked out this machinery for arbitrary principal ideal domains of characteristic 0 so that we can use it also in Section 6 where we will prove a generalization of Theorem 1.1 over rings of S-integers of number fields.

Let A be a principal ideal domain of characteristic 0, $\Bbbk$ its field of fractions, K an extension of $\Bbbk$ of degree $n \geq 4$, and L the normal closure of K over $\Bbbk$. We consider so-called *special pairs* in K, i.e., pairs (α, β) such that $\Bbbk(\alpha) = \Bbbk(\beta) = K$, $A_\alpha = A_\beta$ and α, β are $\mathrm{GL}_2(A)$-inequivalent. Two special pairs (α, β) and (α^*, β^*) are called $\mathrm{GL}_2(\Bbbk)$-*equivalent* if α^* is $\mathrm{GL}_2(\Bbbk)$-equivalent to α and β^* is $\mathrm{GL}_2(\Bbbk)$-equivalent to β.

Let (α,β), (α^*,β^*) be two $\mathrm{GL}_2(\Bbbk)$-equivalent special pairs. Then since we are working over a principal ideal domain A,

$$\alpha^* = C\alpha, \quad \beta^* = C'\beta, \tag{4.1}$$

where $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $C' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ with

$$\begin{aligned} a,b,c,d \in A, \quad & \gcd(a,b,c,d) = 1, \qquad \Delta := ad-bc \neq 0, \\ a',b',c',d' \in A, \quad & \gcd(a',b',c',d') = 1, \quad \Delta' := a'd'-b'c' \neq 0. \end{aligned}$$

Recall that by Lemma 2.4 we have $\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} \in A_L^*$ for all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$.

Proposition 4.1. *Let $\mathfrak{d}$ be the discriminant ideal of A_α, and let $\mathfrak{a}(\alpha,\beta)$ denote the ideal of A_L generated by all numbers $\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} - 1$ for all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$. Then*

$$\Delta A_L \supseteq \mathfrak{d}^5 \cdot \mathfrak{a}(\alpha,\beta)^2. \tag{4.2}$$

Recall that by Lemmas 2.5 and 2.6, the ideal $\mathfrak{a}(\alpha,\beta)$ is not zero. We mention that our proof also implies that $\Delta/\Delta' \in A^*$, but this will not be needed.

We start with some preparations and then prove two lemmas, which together imply Proposition 4.1.

Let C, C' be the matrices from (4.1). Since A is a principal ideal domain, there are matrices $U,V,U',V' \in \mathrm{GL}_2(A)$ such that

$$UCV = \begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}, \quad U'C'V' = \begin{pmatrix} \Delta' & 0 \\ 0 & 1 \end{pmatrix}.$$

Put $\alpha_1 := V^{-1}\alpha$, $\alpha_1^* := U\alpha^*$, $\beta_1 := V'^{-1}\beta$, $\beta_1^* := U'\beta$. Then $\alpha_1^* = \Delta\alpha_1$, $\beta_1^* = \Delta'\beta_1$, $A_{\alpha_1} = A_{\beta_1}$, $A_{\alpha_1^*} = A_{\beta_1^*}$, (α_1,β_1), (α_1^*,β_1^*) are $\mathrm{GL}_2(\Bbbk)$-equivalent special pairs, and $\mathfrak{a}(\alpha_1,\beta_1) = \mathfrak{a}(\alpha,\beta)$. So in the proof of Proposition 4.1 we may replace α, α^*, β, β^* by α_1, α_1^*, β_1, β_1^*, in other words, without loss of generality we may assume

$$\alpha^* = \Delta\alpha, \quad \beta^* = \Delta'\beta. \tag{4.3}$$

So assume (4.3). Let

$$f_\alpha = a_0X^n + \cdots + a_n, \quad f_\beta = b_0X^n + \cdots + b_n$$

be primitive minimal polynomials of α,β. By Lemma 2.1, the ring $A_\alpha = A_\beta$ has A-module bases

$$\{1,\omega_1,\dots,\omega_{n-1}\}, \quad \{1,\rho_1,\dots,\rho_{n-1}\}$$

respectively, where

$$\omega_i = \sum_{j=0}^{i-1} a_j \alpha^{i-j}, \quad \rho_i = \sum_{j=0}^{i-1} b_j \beta^{i-j} \qquad (i = 1, \ldots, n-1). \tag{4.4}$$

Hence there are a matrix $M = (m_{ij})_{i,j=1,\ldots,n-1} \in \mathrm{GL}_{n-1}(A)$ and $m_{i,0} \in A$ $(i = 1, \ldots, n-1)$ such that

$$\rho_i = m_{i,0} + \sum_{j=1}^{n-1} m_{ij}\omega_j \quad \text{for } i = 1, \ldots, n-1. \tag{4.5}$$

Let us write $[\ldots]$ for the fractional ideal of A generated by the elements between the brackets.

Lemma 4.2. *The following holds:*

$$[\Delta] = [\Delta'], \tag{4.6}$$

$$m_{ij} \equiv 0 \pmod{\Delta^{j-i}} \quad \textit{for } i = 1, \ldots, n-1,\ j > i, \tag{4.7}$$

$$\gcd(m_{ii}, \Delta) = 1 \quad \textit{for } i = 1, \ldots, n-1, \tag{4.8}$$

$$[a_0, \Delta] = [b_0, \Delta]. \tag{4.9}$$

Proof. By (4.3), there are non-zero $\lambda, \mu \in \Bbbk$ such that α^*, β^* have primitive minimal polynomials

$$\begin{aligned} f_{\alpha^*} &= \lambda(a_0\Delta^{-n}X^n + a_1\Delta^{1-n}X^{n-1} + \cdots + a_n), \\ f_{\beta^*} &= \mu(b_0\Delta'^{-n}X^n + b_1\Delta'^{1-n}X^{n-1} + \cdots + b_n). \end{aligned} \tag{4.10}$$

From (4.3), (4.10) it follows that $A_{\alpha^*} = A_{\beta^*}$ has A-module bases

$$\{1, \lambda\Delta^{1-n}\omega_1, \ldots, \lambda\Delta^{-1}\omega_{n-1}\}, \quad \{1, \mu\Delta'^{1-n}\rho_1, \ldots, \mu\Delta'^{-1}\rho_{n-1}\}. \tag{4.11}$$

Hence there are $M^* = (m^*_{ij})_{i,j=1,\ldots,n-1} \in \mathrm{GL}_{n-1}(A)$ and $m^*_{i,0} \in A$ $(i = 1, \ldots, n-1)$ such that

$$\mu\Delta'^{i-n}\rho_i = m^*_{i,0} + \sum_{j=1}^{n-1} m^*_{ij}\lambda\Delta^{j-n}\omega_j \quad \text{for } i = 1, \ldots, n-1.$$

A comparison with (4.5) gives

$$\mu\Delta'^{i-n}\rho_i = t_{i,0} + \sum_{j=1}^{n-1} t_{ij}\omega_j \qquad (i = 1, \ldots, n),$$

where

$$t_{ij} = \mu\Delta'^{i-n}m_{ij} = \lambda\Delta^{j-n}m^*_{ij} \qquad (i, j = 1, \ldots, n-1). \tag{4.12}$$

Since $M = (m_{ij}) \in \mathrm{GL}_{n-1}(A)$, the entries of each row of M have gcd 1. It follows that the fractional ideal generated by the entries of the ith row of $T = (t_{ij})_{i,j=1,\ldots,n-1}$ is $[\mu\Delta'^{i-n}]$. Hence the fractional ideal generated by all entries of T is $[\mu\Delta'^{1-n}]$. Similarly, since also $M^* \in \mathrm{GL}_{n-1}(A)$, the fractional

ideal generated by the entries of the jth column of T is $[\lambda\Delta^{j-n}]$. Hence the fractional ideal generated by all entries of T is $[\lambda\Delta^{1-n}]$. So $[\lambda\Delta^{1-n}] = [\mu\Delta'^{1-n}]$. On the other hand, using $\det M \in A^*$ and $\det M^* \in A^*$, we find that $[\det T] = [\lambda^{n-1}\Delta^{-n(n-1)/2}] = [\mu^{n-1}\Delta'^{-n(n-1)/2}]$. By combining these two identities and the fact that $n \geq 4$, we obtain

$$[\lambda] = [\mu], \qquad [\Delta] = [\Delta'].$$

This proves (4.6). Further, by (4.12),

$$[m_{ij}] = [\Delta^{j-i} m_{ij}^*],$$

and since $m_{ij}^* \in A$ this implies (4.7). Combining (4.7) with $\det M \in A^*$ we obtain (4.8).

It remains to prove (4.9). Note that by (4.4) we have

$$\omega_1^2 = a_1\omega_1 - a_0\omega_2, \qquad \rho_1^2 = b_1\rho_1 - b_0\rho_2.$$

Substituting (4.5) and using the congruences (4.7), we obtain the following congruences modulo ΔA_α:

$$\begin{aligned} b_1(m_{1,0} + m_{1,1}\omega_1) - b_0(m_{2,0} + m_{2,1}\omega_1 + m_{2,2}\omega_2) \\ &\equiv (m_{1,0} + m_{1,1}\omega_1)^2 \equiv m_{1,0}^2 + 2m_{1,0}m_{1,1}\omega_1 + m_{1,1}^2\omega_1^2 \\ &\equiv m_{1,0}^2 + 2m_{1,0}m_{1,1}\omega_1 + m_{1,1}^2(a_1\omega_1 - a_0\omega_2) \\ &\equiv m_{1,0}^2 + (2m_{1,0}m_{1,1} + m_{1,1}^2 a_1)\omega_1 - m_{1,1}^2 a_0\omega_2 \pmod{\Delta A_\alpha}. \end{aligned}$$

Comparing the coefficients of ω_2, we see that $b_0 m_{2,2} \equiv a_0 m_{1,1}^2 \pmod{\Delta}$. Combined with (4.8), this gives (4.9). ∎

For the remainder of the proof of (4.2) it will be convenient to work locally. Let $\mathcal{V}_L$ be the set of discrete valuations on L corresponding to the non-zero prime ideals of A_L, i.e., $v \in \mathcal{V}_L$ corresponds to the prime ideal $\mathfrak{p}$ if $v(x)$ is the exponent of $\mathfrak{p}$ in the unique prime ideal decomposition of $[x]$. Further, put $\delta_v := v(\mathfrak{d}) = \min\{v(x) : x \in \mathfrak{d}\}$.

LEMMA 4.3. *Let $v \in \mathcal{V}_L$. Then for all pairwise distinct $i, j, k, l \in \{1, \dots, n\}$ we have*

$$v(\Delta) \leq 5\delta_v + 2 \cdot v\left(\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} - 1\right). \tag{4.13}$$

Proof. We assume without loss of generality that

$$v(\Delta) > 5\delta_v. \tag{4.14}$$

We frequently use the following facts. Let as before $x \mapsto x^{(i)}$ $(i = 1, \dots, n)$ be the $\Bbbk$-isomorphic embeddings of K in L so that

$$f_\alpha = a_0(X - \alpha^{(1)}) \cdots (X - \alpha^{(n)}), \qquad f_\beta = b_0(X - \beta^{(1)}) \cdots (X - \beta^{(n)}).$$

Since f_α, f_β are primitive, by Gauss' Lemma we have

$$v(a_0)+\sum_{i=1}^{n}\min(0,v(\alpha^{(i)}))=0,\quad v(b_0)+\sum_{i=1}^{n}\min(0,v(\beta^{(i)}))=0. \tag{4.15}$$

By Lemma 2.2 we have $\mathfrak{d}=[D(f_\alpha)]=[D(f_\beta)]$. Using

$$D(f_\alpha)=a_0^{2n-2}\prod_{1\le i<j\le n}(\alpha^{(i)}-\alpha^{(j)})^2$$

and likewise for f_β, and inserting (4.15), we obtain

$$\begin{aligned}\tfrac{1}{2}\delta_v &= \sum_{1\le i<j\le n}\big(v(\alpha^{(i)}-\alpha^{(j)})-\min(0,v(\alpha^{(i)}))-\min(0,v(\alpha^{(j)}))\big)\\ &= \sum_{1\le i<j\le n}\big(v(\beta^{(i)}-\beta^{(j)})-\min(0,v(\beta^{(i)}))-\min(0,v(\beta^{(j)}))\big).\end{aligned} \tag{4.16}$$

For $a,b,c\in L$ we write $a\equiv b \pmod c$ if $v(a-b)\ge v(c)$. By (4.5) and (4.7),

$$b_0\beta^{(i)}\equiv m_{1,0}+m_{1,1}a_0\alpha^{(i)} \pmod{\Delta} \quad \text{for } i=1,\dots,n;$$

here we use the fact that ω_j, ρ_j $(j=1,\dots,n-1)$ and their conjugates all lie in A_L. This implies

$$b_0(\beta^{(i)}-\beta^{(j)})\equiv m_{1,1}a_0(\alpha^{(i)}-\alpha^{(j)}) \pmod{\Delta} \quad \text{for } i,j=1,\dots,n. \tag{4.17}$$

In the remainder of the proof we distinguish the cases $v(a_0)\le\frac{1}{2}v(\Delta)$ and $v(a_0)>\frac{1}{2}v(\Delta)$. First assume that

$$v(a_0)\le\tfrac{1}{2}v(\Delta).$$

Let i,j be any two distinct indices from $\{1,\dots,n\}$. Then by (4.8) and (4.16),

$$\begin{aligned}&v(m_{1,1}a_0(\alpha^{(i)}-\alpha^{(j)}))\\ &\qquad\le v(a_0)+v(\alpha^{(i)}-\alpha^{(j)})-\min(0,v(\alpha^{(i)}))-\min(0,v(\alpha^{(j)}))\\ &\qquad\le \tfrac{1}{2}v(\Delta)+\tfrac{1}{2}\delta_v,\end{aligned}$$

and together with (4.17) this gives

$$v\left(\frac{b_0(\beta^{(i)}-\beta^{(j)})}{m_{1,1}a_0(\alpha^{(i)}-\alpha^{(j)})}-1\right)\ge\tfrac{1}{2}v(\Delta)-\tfrac{1}{2}\delta_v,$$

which is >0 by (4.14). Using the trivial observation for discrete valuations

$$v(x_i-1)\ge c>0 \text{ for } i=1,2,3,4 \implies v\left(\frac{x_1x_2}{x_3x_4}-1\right)\ge c \tag{4.18}$$

we deduce

$$v\left(\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)}-1\right)\ge\tfrac{1}{2}v(\Delta)-\tfrac{1}{2}\delta_v$$

for all pairwise distinct $i,j,k,l\in\{1,\dots,n\}$, which implies (4.13).

Next, assume that

$$v(a_0) > \tfrac{1}{2}v(\Delta). \tag{4.19}$$

Then (4.9) implies that also

$$v(b_0) > \tfrac{1}{2}v(\Delta). \tag{4.20}$$

We first observe that

$$v(a_1) \le \delta_v, \quad v(b_1) \le \delta_v. \tag{4.21}$$

Indeed, recall that the discriminant $D(F)$ of a binary form

$$F = \sum_{i=0}^{n} x_i X^{n-i} Y^i$$

is a polynomial in $\mathbb{Z}[x_0, \dots, x_n]$. Consequently, if F as above and $G = \sum_{i=0}^{n} y_i X^{n-i} Y^i$ are binary forms in $A[X, Y]$, we have

$$v(D(F) - D(G)) \ge \min_{0 \le i \le n} v(x_i - y_i).$$

Applying this with $F(X,Y)=Y^n f_\alpha(X/Y)$ and $G(X,Y)=F(X,Y)-a_0X^n-a_1X^{n-1}Y$, and noting that $D(G) = 0$ since G is divisible by Y^2, we see that

$$\delta_v = v(D(F)) = v(D(F) - D(G)) \ge \min(v(a_0), v(a_1)).$$

By (4.19) and (4.14) we have $v(a_0) > \frac{1}{2}v(\Delta) > \delta_v$. Hence $v(a_1) \le \delta_v$. The proof of $v(b_1) \le \delta_v$ is the same, using (4.20) instead of (4.19).

Assume without loss of generality that

$$v(\alpha^{(1)}) = \min(v(\alpha^{(1)}), \dots, v(\alpha^{(n)})).$$

Then

$$v(\alpha^{(i)}) \ge -\tfrac{1}{2}\delta_v \quad \text{for } i = 2, \dots, n. \tag{4.22}$$

Indeed, suppose that $v(\alpha^{(i)}) < -\frac{1}{2}\delta_v$ for some $i \ge 2$. Then by (4.16),

$$\tfrac{1}{2}\delta_v \ge v({\alpha^{(1)}}^{-1} - {\alpha^{(i)}}^{-1}) > \tfrac{1}{2}\delta_v,$$

which is impossible. Thus,

$$\begin{aligned} &v(a_0\alpha^{(i)}) > \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \quad \text{for } i \ge 2, \\ &v(a_0\alpha^{(1)}) = v(a_1 + a_0(\alpha^{(2)} + \cdots + \alpha^{(n)})) \le \delta_v, \end{aligned} \tag{4.23}$$

where in the derivation of the first inequality we use (4.19) and in that of the last inequality we use (4.21) and (4.14).

Let k be an index such that

$$v(\beta^{(k)}) = \min(v(\beta^{(1)}), \dots, v(\beta^{(n)})).$$

Then completely similarly to (4.22) and (4.23) we derive

$$\begin{aligned} &v(\beta^{(i)}) \geq -\tfrac{1}{2}\delta_v \quad \text{for } i \neq k,\\ &v(b_0\beta^{(k)}) \leq \delta_v, \quad v(b_0\beta^{(i)}) > \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \quad \text{for } i \neq k, \end{aligned} \tag{4.24}$$

where we have used (4.20) instead of (4.19). We show that the index k must be equal to 1. Recall that by (4.17),

$$b_0(\beta^{(i)} - \beta^{(1)}) \equiv m_{1,1}a_0(\alpha^{(i)} - \alpha^{(1)}) \pmod{\Delta} \quad \text{for } i \geq 2.$$

Assuming $k \neq 1$, for $i \neq 1, k$ this congruence contradicts the two inequalities

$$\begin{aligned} &v(b_0(\beta^{(i)} - \beta^{(1)})) > \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \quad \text{implied by (4.24)},\\ &v(m_{1,1}a_0(\alpha^{(i)} - \alpha^{(1)})) \leq \delta_v < \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \end{aligned}$$

implied by (4.8), (4.23), (4.14). So indeed $k = 1$, and thus (4.24) becomes

$$\begin{aligned} &v(\beta^{(i)}) \geq -\tfrac{1}{2}\delta_v \quad \text{for } i \geq 2,\\ &v(b_0\beta^{(1)}) \leq \delta_v, \quad v(b_0\beta^{(i)}) > \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \quad \text{for } i \geq 2. \end{aligned} \tag{4.25}$$

Let $i \in \{2, \ldots, n\}$. By (4.5) and (4.7) we have

$$b_0(\beta^{(i)})^2 + b_1\beta^{(i)} \equiv m_{2,0} + m_{2,1}a_0\alpha^{(i)} + m_{2,2}(a_0(\alpha^{(i)})^2 + a_1\alpha^{(i)}) \pmod{\Delta},$$

while

$$\begin{aligned} v(a_0(\alpha^{(i)})^2) &> \tfrac{1}{2}v(\Delta) - \delta_v \qquad \text{by (4.19), (4.22)},\\ v(b_0(\beta^{(i)})^2) &> \tfrac{1}{2}v(\Delta) - \delta_v \qquad \text{by (4.20), (4.25)},\\ v(a_0\alpha^{(i)}) &> \tfrac{1}{2}v(\Delta) - \tfrac{1}{2}\delta_v \qquad \text{by (4.19), (4.22)}. \end{aligned}$$

These relations together imply

$$v(b_1\beta^{(i)} - m_{2,0} - m_{2,2}a_1\alpha^{(i)}) > \tfrac{1}{2}v(\Delta) - \delta_v \quad \text{for } i \geq 2.$$

Now let i, j be any two distinct indices with $2 \leq i, j \leq n$. Then by the inequality just derived,

$$v\big(b_1(\beta^{(i)} - \beta^{(j)}) - m_{2,2}a_1(\alpha^{(i)} - \alpha^{(j)})\big) > \tfrac{1}{2}v(\Delta) - \delta_v. \tag{4.26}$$

Further, by (4.8), (4.21), and (4.16),

$$\begin{aligned} &v(m_{2,2}a_1(\alpha^{(i)} - \alpha^{(j)}))\\ &\leq v(a_1) + v(\alpha^{(i)} - \alpha^{(j)}) - \min(0, v(\alpha^{(i)})) - \min(0, v(\alpha^{(j)})) \leq \tfrac{3}{2}\delta_v, \end{aligned} \tag{4.27}$$

which together with (4.26) implies

$$v\left(\frac{b_1(\beta^{(i)} - \beta^{(j)})}{m_{2,2}a_1(\alpha^{(i)} - \alpha^{(j)})} - 1\right) > \tfrac{1}{2}v(\Delta) - \tfrac{5}{2}\delta_v. \tag{4.28}$$

Inequality (4.28) holds for any pair of indices $i, j \geq 2$. We still have to look at the case where one of the indices is 1. Let $j \geq 2$. Then by (4.23)

and (4.14),

$$v(a_0(\alpha^{(1)} - \alpha^{(j)})) \le \delta_v,$$

which together with (4.17) implies

$$v\left(\frac{b_0(\beta^{(1)} - \beta^{(j)})}{m_{1,1}a_0(\alpha^{(1)} - \alpha^{(j)})} - 1\right) > v(\Delta) - \delta_v. \tag{4.29}$$

Finally, from (4.28), (4.29), (4.14) and observation (4.18) we deduce

$$v\left(\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} - 1\right) > \tfrac{1}{2}v(\Delta) - \tfrac{5}{2}\delta_v$$

for all pairwise distinct $i, j, k, l \in \{1, \dots, n\}$. This implies (4.13) and thus completes the proof of Lemma 4.3. ∎

Proof of Proposition 4.1. By applying Lemma 4.3 for all $v \in \mathcal{V}_L$, the inclusion (4.2) clearly follows. ∎

5. Proofs of Theorems 1.1–1.3. Let K be a number field. Recall that $\alpha_1 \in K$ is *k-special* if $K = \mathbb{Q}(\alpha_1)$ and there are $\alpha_2, \dots, \alpha_k$ such that $\alpha_1, \dots, \alpha_k$ are pairwise $\mathrm{GL}_2(\mathbb{Z})$-inequivalent and $\mathbb{Z}_{\alpha_1} = \cdots = \mathbb{Z}_{\alpha_k}$. A 2-special number is called *special*. We first prove the following.

Proposition 5.1. *Let K be a number field of degree $n \ge 3$. Then the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of every special $\alpha \in K$ is the union of at most finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes.*

Proof. First let $n = 3$. By Lemmas 2.5(i) and 2.6, any two numbers α, β with $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. Hence there are no special numbers in K.

Next let $n \ge 4$. Denote by L the normal closure of K. Let $\mathcal{C}$ be the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of a special $\alpha \in K$. We first split $\mathcal{C}$ into finitely many subclasses. Since cross ratios of $\mathrm{GL}_2(\mathbb{Q})$-equivalent numbers are the same, we may define $\mathrm{cr}_{ijkl}(\mathcal{C}) := \mathrm{cr}_{ijkl}(\alpha)$ for any $\alpha \in \mathcal{C}$ and any distinct $i, j, k, l \in \{1, \dots, n\}$. For every $\alpha \in \mathcal{C}$ there is $\beta \in K$ such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and β is not $\mathrm{GL}_2(\mathbb{Z})$-equivalent to α. From Lemma 2.4 and (3.3) it follows that $\varepsilon_{ijkl} := \mathrm{cr}_{ijkl}(\beta)/\mathrm{cr}_{ijkl}(\alpha) \in \mathcal{O}_L^*$ for all distinct $i, j, k, l \in \{1, \dots, n\}$ and

$$\mathrm{cr}_{ijkl}(\mathcal{C})\varepsilon_{ijkl} + \mathrm{cr}_{ilkj}(\mathcal{C})\varepsilon_{ilkj} = 1 \tag{5.1}$$

for all distinct $i, j, k, l \in \{1, \dots, n\}$.

We apply the following result, due to Lang [14].

Lemma 5.2. *Let F be a field of characteristic 0, let $a, b \in F^*$, and let Γ be a subgroup of F^* of finite rank. Then the equation*

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

has only finitely many solutions.

By applying this to (5.1) with $\Gamma = \mathcal{O}_L^*$, we infer that there is a finite set depending only on $\mathcal{C}$ such that for all i,j,k,l, ε_{ijkl} belongs to this set, and so, for all i,j,k,l, $\mathrm{cr}_{ijkl}(\beta)$ belongs to a finite set depending only on $\mathcal{C}$. Now Lemma 2.5(ii) implies that the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of β belongs to a finite collection depending only on $\mathcal{C}$. Further, by Lemma 2.6, the classes in this collection are disjoint from $\mathcal{C}$. This implies that $\mathcal{C}$ can be partitioned into a finite collection of subclasses

$$\mathcal{C}(\mathcal{D}) := \{\alpha \in \mathcal{C} : \text{there is } \beta \in \mathcal{D} \text{ with } \mathbb{Z}_\alpha = \mathbb{Z}_\beta\},$$

where $\mathcal{D}$ is the $\mathrm{GL}_2(\mathbb{Q})$-equivalence class of some special number, distinct from $\mathcal{C}$.

Take a $\mathrm{GL}_2(\mathbb{Q})$-equivalence class $\mathcal{D} \neq \mathcal{C}$ for which $\mathcal{C}(\mathcal{D}) \neq \emptyset$. We have to show that $\mathcal{C}(\mathcal{D})$ is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. We use the fact that for every positive integer Δ there is a finite set $\mathcal{F}(\Delta)$ of integer 2×2-matrices such that if C is any 2×2-matrix with $|\det C| = \Delta$, then there is $U \in \mathrm{GL}_2(\mathbb{Z})$ with $UC \in \mathcal{F}(\Delta)$.

Fix $\alpha \in \mathcal{C}(\mathcal{D})$ and then $\beta \in \mathcal{D}$ with $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Then choose $\alpha^* \in \mathcal{C}(\mathcal{D})$; we let α^* vary. Further choose $\beta^* \in \mathcal{D}$ with $\mathbb{Z}_{\alpha^*} = \mathbb{Z}_{\beta^*}$. Thus, (α,β) and (α^*,β^*) are two $\mathrm{GL}_2(\mathbb{Q})$-equivalent special pairs as in Proposition 4.1, with $A = \mathbb{Z}$. Let C be the matrix from (4.1), so with $\alpha^* = C\alpha$, and put $\Delta := |\det C|$. Then there is $U \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$UC =: C_1 \in \mathcal{F}(\Delta).$$

Let $\alpha^{**} := U\alpha^* = C_1\alpha$. By Proposition 4.1, Δ belongs to a finite set depending on α,β, hence so does C_1, and thus α^{**}. This implies that the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of α^* belongs to a finite collection depending on α,β. This shows that indeed $\mathcal{C}(\mathcal{D})$ is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. ∎

Proof of Theorem 1.1. Propositions 3.1 and 5.1 imply that if K is quartic then the 3-special numbers $\alpha \in K$ lie in finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. Further, if K has degree ≥ 5 and the Galois group of its normal closure is 5-transitive, then the special numbers in K lie in finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. As we observed in Section 3, this implies Theorem 1.1. ∎

Proof of Theorem 1.2. Let K be either a quartic field, or a number field of degree ≥ 5 such that the Galois group of the normal closure of K is 5-transitive. Consider a Hermite equivalence class $\mathcal{H}$ of polynomials in $\mathcal{PI}(K)$ that falls apart into at least three $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes if $[K:\mathbb{Q}] = 4$, and into at least two $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes if $[K:\mathbb{Q}] \geq 5$. Recall that $f,g \in \mathcal{PI}(K)$ are Hermite equivalent if f has a root α and g a root β such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathcal{M}_\beta = \lambda\mathcal{M}_\alpha$ for some non-zero λ. This implies $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Now if $f,g \in \mathcal{H}$ are $\mathrm{GL}_2(\mathbb{Z})$-inequivalent, then so are α,β. So the

order $\mathcal{O} = \mathbb{Z}_\alpha$ has at least three rational monogenizations if $[K : \mathbb{Q}] = 4$, and at least two rational monogenizations if $[K : \mathbb{Q}] \geq 5$. Since $\mathcal{O}$ is an order of a conjugate of K and K has only finitely many conjugates, Theorem 1.1 implies that there are only finitely many possibilities for $\mathcal{O}$. Given $\mathcal{O}$, the set of α with $\mathbb{Z}_\alpha = \mathcal{O}$ is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. Hence the set of $f \in \mathcal{PI}(K)$ having a root α with $\mathbb{Z}_\alpha = \mathcal{O}$ is the union of finitely many $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes. The class $\mathcal{H}$ is the union of some of these classes. So we have only finitely many possibilities for $\mathcal{H}$. ∎

Proof of Theorem 1.3. Take an algebraic number α of degree $n \geq 3$. Let $f_\alpha(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ be the primitive minimal polynomial of α and $F_\alpha(X, Y) := X^n f_\alpha(X/Y)$ its homogenization. By Thue's Theorem [18], there is a number C such that if x, y are integers with $F_\alpha(x, y) = \pm 1$, then $|x|, |y| \leq C$. Let p, q be distinct prime numbers such that $p, q > C^* := \max(C, |a_0|, |a_n|)$. The number $(q/p)\alpha$ has primitive minimal polynomial $f_{q\alpha/p}(X) = q^n f_\alpha(pX/q)$ (one verifies easily that the coefficients of this polynomial have gcd 1, since $p, q > |a_0|, |a_n|$). The polynomial $f_{q\alpha/p}$, hence by (1.4) the order $\mathbb{Z}_{q\alpha/p}$, has discriminant $(pq)^{n(n-1)}D(f_\alpha)$. So the orders $\mathbb{Z}_{q\alpha/p}$, with p, q running through the primes exceeding C^*, are all different.

We claim that among these orders, at most finitely many are monogenic. Indeed, suppose that $\mathbb{Z}_{q\alpha/p}$ is monogenic. Then $\mathbb{Z}_{q\alpha/p} = \mathbb{Z}_\beta = \mathbb{Z}[\beta]$ for some algebraic integer β. Assume that β is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q\alpha/p$. That is, $\beta = \frac{a(q\alpha/p)+b}{c(q\alpha/p)+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Then the necessarily monic primitive minimal polynomial of β is

$$f_\beta(X) = \pm q^n(-cX + a)^n f_\alpha\left(\frac{p(dX - b)}{q(-cX + a)}\right).$$

Its homogenization is

$$F_\beta(X, Y) = Y^n f_\beta(X/Y) = \pm F_\alpha(p(dX - bY), q(-cX + aY)).$$

Since β is integral, the leading coefficient of f_β is 1, which implies $1 = F_\beta(1, 0) = \pm F_\alpha(pd, -qc)$. But this is impossible, since at least one of $|pd|, |qc|$ exceeds the bound C defined above. We conclude that β cannot be $\mathrm{GL}_2(\mathbb{Z})$-equivalent to $q\alpha/p$. So any order $\mathbb{Z}_{q\alpha/p}$ that is monogenic must have two rational monogenizations. By Proposition 5.1 there are at most finitely many pairs of distinct primes $p, q > C^*$ for which this is possible. This leaves us with infinitely many rationally monogenic orders $\mathbb{Z}_{q\alpha/p}$ that are not monogenic. ∎

6. A generalization over the S-integers. In this section, we will state and prove a generalization of Theorem 1.1 to the ring $\mathcal{O}_S$ of S-integers of a number field. The ring of S-integers is a Dedekind domain, but in general not

a principal ideal domain, therefore, the arguments from the previous sections cannot be carried over. Thus, in our generalization of Theorem 1.1 we will not work with $\mathrm{GL}_2(\mathcal{O}_S)$-equivalence of algebraic numbers, but rather with numbers that are $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$-equivalent for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_S$, where $\mathcal{O}_\mathfrak{p}$ is the localization of $\mathcal{O}_S$ at $\mathfrak{p}$.

Before stating and proving our result, we have collected some generalizations of the material from Section 2 to Dedekind domains of characteristic 0. Most of these are equivalent, but for our purposes more convenient formulations of material from [10, Chap. 17].

Let A be a Dedekind domain of characteristic 0 and $\Bbbk$ its quotient field. Denote by $\mathcal{P}(A)$ the collection of non-zero prime ideals of A and by $\mathrm{Cl}(A)$ the class group of A (fractional ideals modulo principal fractional ideals). Further, let $\mathrm{Cl}(A)[m]$ be the subgroup of elements of $\mathrm{Cl}(A)$ whose mth power is the principal ideal class. The localization of A at a prime ideal $\mathfrak{p} \in \mathcal{P}(A)$ is given by

$$A_\mathfrak{p} := \{x/y : x \in A,\ y \in A \setminus \mathfrak{p}\}.$$

We define the group of matrices

$$G(A) := \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} \Bbbk^* \mathrm{GL}_2(A_\mathfrak{p}),$$

that is, the group of matrices C such that for every $\mathfrak{p} \in \mathcal{P}(A)$ there is $\lambda_\mathfrak{p} \in \Bbbk^*$ with $\lambda_\mathfrak{p}^{-1} C \in \mathrm{GL}_2(A_\mathfrak{p})$.

Let $\alpha, \beta \in \overline{\Bbbk}$ be of degree ≥ 3 over $\Bbbk$. We say that α, β are $G(A)$-*equivalent* if there is $C \in G(A)$ with $\beta = C\alpha$. Then

(6.1) α, β are $G(A)$-equivalent
$$\iff \alpha, \beta \text{ are } \mathrm{GL}_2(A_\mathfrak{p})\text{-equivalent for every } \mathfrak{p} \in \mathcal{P}(A).$$

Indeed, $\Rightarrow$ is clear. As for $\Leftarrow$, suppose that α, β are $\mathrm{GL}_2(A_\mathfrak{p})$-equivalent for every $\mathfrak{p} \in \mathcal{P}(A)$. Then there is $C \in \mathrm{GL}_2(\Bbbk)$ such that $\beta = C\alpha$. But C is determined uniquely up to a scalar in $\Bbbk^*$, hence $C \in \Bbbk^* \mathrm{GL}_2(A_\mathfrak{p})$ for every $\mathfrak{p} \in \mathcal{P}(A)$, i.e., $C \in G(A)$.

We compare $G(A)$-equivalence with $\mathrm{GL}_2(A)$-equivalence.

LEMMA 6.1. $G(A)/\Bbbk^* \mathrm{GL}_2(A) \cong \mathrm{Cl}(A)[2]$.

Proof. Let $[a_1, \ldots, a_r]$ denote the fractional ideal of A generated by $a_1, \ldots, a_r$ and for a matrix C with entries in $\Bbbk$, let $[C]$ denote the fractional ideal generated by the entries of C. We claim that

$$G(A) = \{C \in \mathrm{GL}_2(\Bbbk) : [\det C] = [C]^2\}. \tag{6.2}$$

Indeed, let $C \in G(A)$. Then for all $\mathfrak{p} \in \mathcal{P}(A)$ there is $\lambda_\mathfrak{p} \in \Bbbk^*$ such that $\lambda_\mathfrak{p}^{-1} C \in \mathrm{GL}_2(A_\mathfrak{p})$, hence $[C]^2 \cdot A_\mathfrak{p} = \lambda_\mathfrak{p}^2 A_\mathfrak{p} = [\det C] \cdot A_\mathfrak{p}$ for all $\mathfrak{p}$, implying $[C]^2 = [\det C]$. Conversely, assume $[\det C] = [C]^2$. Then for all $\mathfrak{p} \in \mathcal{P}(A)$

there is $\lambda_\mathfrak{p} \in \Bbbk^*$ with $[C]A_\mathfrak{p} = \lambda_\mathfrak{p} A_\mathfrak{p}$ since $A_\mathfrak{p}$ is a principal ideal domain. So $\det(\lambda_\mathfrak{p}^{-1}C) = \lambda_\mathfrak{p}^{-2} \det C \in A_\mathfrak{p}^*$, i.e., $\lambda_\mathfrak{p}^{-1}C \in \mathrm{GL}_2(A_\mathfrak{p})$ for all $\mathfrak{p} \in \mathcal{P}(A)$, implying $C \in G(A)$.

Now define the map

$$G(A) \to \mathrm{Cl}(A)[2], \qquad C \mapsto \text{ideal class of } [C].$$

By (6.2) this is a well-defined group homomorphism. Its kernel is the group of matrices $C \in G(A)$ such that $[C]$ is principal, this is precisely $\Bbbk^*\mathrm{GL}_2(A)$. To show that the homomorphism is surjective, pick any ideal class of A whose square is principal, and take an ideal from this class. By a well-known property of Dedekind domains, this ideal is generated by two elements, say it is $[a, b]$. Then, using another property of Dedekind domains, $[a^2, b^2] = [a, b]^2 = [\lambda]$ for some $\lambda \in A$, hence there are $u, v \in A$ such that $ua^2 - vb^2 = \lambda$. Take $C = \left(\begin{smallmatrix} a & b \\ vb & ua \end{smallmatrix}\right)$. Then $[C]^2 = [a, b]^2 = [\lambda] = [\det C]$, so $C \in G(A)$, and C maps to the ideal class of $[a, b]$. ∎

Lemma 6.1 implies that a $G(A)$-equivalence class is the union of precisely $\#(\mathrm{Cl}(A)[2])$ $\mathrm{GL}_2(A)$-equivalence classes. This quantity is finite for instance if A is the ring of S-integers of a number field.

Let K be a finite extension of $\Bbbk$ of degree $n \geq 3$. Given α with $\Bbbk(\alpha) = K$, we define the A-module

$$\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in A\}$$

and its ring of scalars

$$A_\alpha := \{\xi \in K : \xi\mathcal{M}_\alpha = \mathcal{M}_\alpha\}.$$

For $\mathfrak{p} \in \mathcal{P}(A)$, let $\mathcal{M}_{\mathfrak{p},\alpha}$ be the $A_\mathfrak{p}$-module generated by $1, \alpha, \ldots, \alpha^{n-1}$, and set $A_{\mathfrak{p},\alpha} := \{\xi \in K : \xi\mathcal{M}_{\mathfrak{p},\alpha} \subseteq \mathcal{M}_{\mathfrak{p},\alpha}\}$. Then

$$A_{\mathfrak{p},\alpha} = A_\mathfrak{p} A_\alpha \quad \text{for all } \mathfrak{p} \in \mathcal{P}(A), \tag{6.3}$$

$$A_\alpha = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} A_{\mathfrak{p},\alpha}. \tag{6.4}$$

Lemma 6.2. *Let $\alpha, \beta \in K$ be such that $\Bbbk(\alpha) = \Bbbk(\beta) = K$ and α, β are $G(A)$-equivalent. Then $A_\alpha = A_\beta$.*

Proof. From (6.1) it follows that α, β are $\mathrm{GL}_2(A_\mathfrak{p})$-equivalent for all $\mathfrak{p}$, so $A_{\mathfrak{p},\alpha} = A_{\mathfrak{p},\beta}$ for all $\mathfrak{p}$. Now apply (6.4). ∎

Lemma 6.3. *Let $\alpha, \beta \in K$ satisfy $\Bbbk(\alpha) = \Bbbk(\beta) = K$ and $A_\alpha = A_\beta$. Suppose that α, β are $\mathrm{GL}_2(\Bbbk)$-equivalent. Then they are $G(A)$-equivalent.*

Proof. From (6.3) it follows that $A_{\mathfrak{p},\alpha} = A_{\mathfrak{p},\beta}$ and then from Lemma 2.6 that α, β are $\mathrm{GL}_2(A_\mathfrak{p})$-equivalent for all $\mathfrak{p} \in \mathcal{P}(A)$; here we have used the fact that the $A_\mathfrak{p}$ are principal ideal domains. Now (6.1) implies that they are $G(A)$-equivalent. ∎

Suppose that $[K:\Bbbk]=n\geq 4$. Let L be the normal closure of $K/\Bbbk$ and $x\mapsto x^{(i)}$ $(i=1,\ldots,n)$ the $\Bbbk$-isomorphic embeddings $K\hookrightarrow L$. Denote by A_L the integral closure of A in L. Define the cross ratios $\mathrm{cr}_{ijkl}(\alpha)$ $(K=\Bbbk(\alpha))$ by (2.6).

LEMMA 6.4. *Let α, β be such that $\Bbbk(\alpha)=\Bbbk(\beta)=K$ and $A_\alpha=A_\beta$. Then for all pairwise distinct $i,j,k,l\in\{1,\ldots,n\}$ we have*

$$\frac{\mathrm{cr}_{ijkl}(\alpha)}{\mathrm{cr}_{ijkl}(\beta)}\in A_L^*.$$

Proof. For $\mathfrak{p}\in\mathcal{P}(A)$, let $A_{\mathfrak{p},L}$ be the integral closure of $A_\mathfrak{p}$ in L. Then $\bigcap_{\mathfrak{p}\in\mathcal{P}(A)}A_{\mathfrak{p},L}=A_L$. By (6.3) we have $A_{\mathfrak{p},\alpha}=A_{\mathfrak{p},\beta}$, and so by Lemma 2.4, $\frac{\mathrm{cr}_{ijkl}(\alpha)}{\mathrm{cr}_{ijkl}(\beta)}\in A_{\mathfrak{p},L}^*$ for all $\mathfrak{p}\in\mathcal{P}(A)$. Since $\bigcap_{\mathfrak{p}\in\mathcal{P}(A)}A_{\mathfrak{p},L}^*=A_L^*$, this implies our lemma. ∎

We now specialize to rings of S-integers of number fields. Let $\Bbbk$ be a number field and $\mathcal{O}_\Bbbk$ its ring of integers. Let S be a finite set of non-zero prime ideals of $\mathcal{O}_\Bbbk$, and

$$\mathcal{O}_S:=\{x/y : x,y\in\mathcal{O}_\Bbbk,\ y \text{ composed of prime ideals from } S\}$$

the ring of S-integers. As before, we denote by $\mathcal{P}(\mathcal{O}_S)$ the set of non-zero prime ideals of $\mathcal{O}_S$. Further, for $\mathfrak{p}\in\mathcal{P}(\mathcal{O}_S)$, we denote by $\mathcal{O}_\mathfrak{p}$ the localization of $\mathcal{O}_S$ at $\mathfrak{p}$, so that

$$G(\mathcal{O}_S)=\bigcap_{\mathfrak{p}\in\mathcal{P}(\mathcal{O}_S)}\Bbbk^*\mathrm{GL}_2(\mathcal{O}_\mathfrak{p}).$$

Let K be a finite extension of $\Bbbk$ of degree $n\geq 4$, and L the normal closure of $K/\Bbbk$.

Denote by $\mathcal{O}_{S,K}$ the integral closure of $\mathcal{O}_S$ in K. By an *$\mathcal{O}_S$-order* of K we mean a ring $\mathcal{O}$ such that $\mathcal{O}_S\subseteq\mathcal{O}\subseteq\mathcal{O}_{S,K}$ and $\Bbbk\mathcal{O}=K$.

Recall that $\alpha,\beta\in K$ are called *$G(\mathcal{O}_S)$-equivalent* if $\beta=C\alpha$ for some $C\in G(\mathcal{O}_S)$. A *rational monogenization* of an $\mathcal{O}_S$-order $\mathcal{O}$ is a $G(\mathcal{O}_S)$-equivalence class of α such that $\mathcal{O}_{S,\alpha}=\mathcal{O}$.

Taking α with $K=\Bbbk(\alpha)$, we say that the Galois group $\mathrm{Gal}(L/\Bbbk)$ is t-transitive if the action of $\mathrm{Gal}(L/\Bbbk)$ on the set of conjugates of α in L is t-transitive. We are now ready to state our generalization.

THEOREM 6.5. *Let $\Bbbk$ be an algebraic number field and S a finite set of prime ideals from $\mathcal{O}_\Bbbk$. Further, let K be a finite extension of $\Bbbk$, and L the normal closure of $K/\Bbbk$.*

(i) *Assume that $[K:\Bbbk]=4$. Then K has only finitely many $\mathcal{O}_S$-orders with more than two rational monogenizations.*

(ii) *Assume that* $[K:\Bbbk] \geq 5$ *and that* $\mathrm{Gal}(L/\Bbbk)$ *is* 5*-transitive. Then* K *has only finitely many* $\mathcal{O}_S$*-orders with more than one rational monogenization.*

The proof is very similar to that of Theorem 1.1. We will mainly focus on the differences.

We keep the notation and assumptions from Theorem 6.5. We call $\alpha_1 \in K$ *k-special* if $\Bbbk(\alpha_1) = K$ and if there are $\alpha_2, \dots, \alpha_k \in K$ such that $\alpha_1, \dots, \alpha_k$ are pairwise $G(\mathcal{O}_S)$-inequivalent and $\mathcal{O}_{S,\alpha_1} = \cdots = \mathcal{O}_{S,\alpha_k}$. We call α_1 *special* if it is 2-special.

Proof of Theorem 6.5. It suffices to show that if $[K:\Bbbk] = 4$ then the 3-special numbers in K lie in at most finitely many $G(\mathcal{O}_S)$-equivalence classes, while if $[K:\Bbbk] \geq 5$ and $\mathrm{Gal}(L/\Bbbk)$ is 5-transitive then the special numbers in K lie in at most finitely many $G(\mathcal{O}_S)$-equivalence classes.

Step 1. *The* 3*-special numbers in* K *if* $[K:\Bbbk] = 4$*, respectively the special numbers in* K *if* $[K:\Bbbk] \geq 5$ *lie in at most finitely many* $\mathrm{GL}_2(\Bbbk)$*-equivalence classes.*

The proof is exactly the same as that of Proposition 3.1, replacing everywhere $\mathbb{Z}$, $\mathbb{Q}$, $\mathcal{O}_L^*$ by $\mathcal{O}_S$, $\Bbbk$, $\mathcal{O}_{S,L}^*$, where $\mathcal{O}_{S,L}$ is the integral closure of $\mathcal{O}_S$ in L. Lemmas 3.2 and 3.3 can be applied with $\Gamma = \mathcal{O}_{S,L}^*$, since the latter group is finitely generated by the Dirichlet–Chevalley–Weil theorem.

Step 2. *Let* K *be any extension of* $\Bbbk$ *with* $[K:\Bbbk] \geq 4$*. Then the* $\mathrm{GL}_2(\Bbbk)$*-equivalence class of each special number in* K *is the union of finitely many* $G(\mathcal{O}_S)$*-equivalence classes.*

Let $\mathcal{C}$ be the $\mathrm{GL}_2(\Bbbk)$-equivalence class of a special number in K. Completely similarly to the proof of Proposition 5.1, applying Lemma 6.4, Lemma 5.2 with $\Gamma = \mathcal{O}_{S,L}^*$, and Lemma 6.3, one shows that $\mathcal{C}$ is the union of finitely many subclasses

$$\mathcal{C}(\mathcal{D}) := \{\alpha \in \mathcal{C} : \text{there is } \beta \in \mathcal{D} \text{ with } \mathcal{O}_{S,\alpha} = \mathcal{O}_{S,\beta}\},$$

where $\mathcal{D} \neq \mathcal{C}$ is the $\mathrm{GL}_2(\Bbbk)$-equivalence class of a special number.

Let $\mathcal{D} \neq \mathcal{C}$ be a $\mathrm{GL}_2(\Bbbk)$-equivalence class such that $\mathcal{C}(\mathcal{D}) \neq \emptyset$. We show by means of a local-to-global argument that $\mathcal{C}(\mathcal{D})$ is the union of finitely many $G(\mathcal{O}_S)$-equivalence classes.

Fix $\alpha \in \mathcal{C}(\mathcal{D})$, and then $\beta \in \mathcal{D}$ with $\mathcal{O}_{S,\alpha} = \mathcal{O}_{S,\beta}$. Let T be the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_S$ such that $\mathfrak{p}$ divides the discriminant ideal $\mathfrak{d}$ of $\mathcal{O}_{S,\alpha}$, or such that some prime ideal $\mathfrak{P}$ of $\mathcal{O}_{S,L}$ above $\mathfrak{p}$ divides the ideal $\mathfrak{a}(\alpha,\beta)$ of $\mathcal{O}_{S,L}$ generated by the numbers $\frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)} - 1$ for all pairwise distinct $i,j,k,l \in \{1,\dots,n\}$. Clearly, T is finite. Next, choose $\alpha^* \in \mathcal{C}(\mathcal{D})$ that we let vary, and then $\beta^* \in \mathcal{D}$ with $\mathcal{O}_{S,\alpha^*} = \mathcal{O}_{S,\beta^*}$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_S$. We apply the theory of Section 4 with $A = \mathcal{O}_\mathfrak{p}$. By (6.3) we have $\mathcal{O}_{\mathfrak{p},\alpha} = \mathcal{O}_{\mathfrak{p},\beta}$, $\mathcal{O}_{\mathfrak{p},\alpha^*} = \mathcal{O}_{\mathfrak{p},\beta^*}$. Hence (α, β) and (α^*, β^*) are two $\mathrm{GL}_2(\Bbbk)$-equivalent special pairs as in Proposition 4.1. Let C be the matrix from (4.1), i.e., with $\alpha^* = C\alpha$, and put $\Delta := \det C$. We use the fact that there is a finite set $\mathcal{F}([\Delta])$ of 2×2-matrices with entries in $\mathcal{O}_\mathfrak{p}$, depending only on $\mathfrak{p}$ and on the ideal $[\Delta] := \Delta\mathcal{O}_\mathfrak{p}$, such that there is $U \in \mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$ with

$$UC =: C_1 \in \mathcal{F}([\Delta]).$$

Let $\alpha^{**} := U\alpha^* = C_1\alpha$. Proposition 4.1 implies that $[\Delta]$ belongs to a finite set depending on α, β and $\mathfrak{p}$, hence so does C_1, and thus α^{**}. This implies that the $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$-equivalence class of α^* belongs to a finite collection depending on $\alpha, \beta, \mathfrak{p}$.

But for $\mathfrak{p} \notin T$, i.e., for all but finitely many $\mathfrak{p}$, Proposition 4.1 implies that $[\Delta] = [1]$, hence α^* is $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$-equivalent to α. Now from (6.1) it follows that there is a finite collection of $G(\mathcal{O}_S)$-equivalence classes depending only on α, β to which α^* must belong. This shows that indeed $\mathcal{C}(\mathcal{D})$ is the union of finitely many $G(\mathcal{O}_S)$-equivalence classes, and completes Step 2 of our proof of Theorem 6.5. ∎

References

[1] A. Bérczes, J.-H. Evertse and K. Győry, *On the number of equivalence classes of binary forms of given degree and given discriminant*, Acta Arith. 113 (2004), 363–399.

[2] A. Bérczes, J.-H. Evertse and K. Győry, *Multiply monogenic orders*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) 12 (2013), 467–497.

[3] M. Bhargava, *On the number of monogenizations of a quartic order* (with an appendix by S. Akhtari), Publ. Math. Debrecen 100 (2022), 513–531.

[4] M. Bhargava, J.-H. Evertse, K. Győry, L. Remete and A. A. Swaminathan, *Hermite equivalence of polynomials*, Acta Arith. (online, 2023).

[5] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. 24 (1972), 385–394.

[6] I. Del Corso, R. Dvornicich and D. Simon, *Decomposition of primes in non-maximal orders*, Acta Arith. 120 (2005), 231–244.

[7] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Tr. Mat. Inst. Steklova 11 (1940), 340 pp. (in Russian); English transl.: Transl. Math. Monogr. 10, Amer. Math. Soc., Providence, RI, 1964.

[8] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compos. Math. 79 (1991), 169–204.

[9] J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge Stud. Adv. Math. 146, Cambridge Univ. Press, 2015.

[10] J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, New Math. Monogr. 32, Cambridge Univ. Press, 2017.

[11] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. 92 (1988), 461–477.

[12] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. 23 (1973), 419–426.
[13] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné, III*, Publ. Math. Debrecen 23 (1976), 141–165.
[14] S. Lang, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. 6 (1960), 27–43.
[15] J. Nakagawa, *Binary forms and orders of algebraic number fields*, Invent. Math. 97 (1989), 219–235.
[16] D. Simon, *The index of nonmonic polynomials*, Indag. Math. (N.S.) 12 (2001), 505–517.
[17] D. Simon, *La classe invariante d'une forme binaire*, C. R. Math. Acad. Sci. Paris 336 (2003), 7–10.
[18] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305.
[19] M. M. Wood, *Rings and ideals parameterized by binary n-ic forms*, J. London Math. Soc. 83 (2011), 208–231.

Jan-Hendrik Evertse
Mathematisch Instituut
Universiteit Leiden
Leiden, the Netherlands
E-mail: evertse@math.leidenuniv.nl
https://pub.math.leidenuniv.nl/∼evertsejh