ON RINGS OF INTEGERS GENERATED BY THEIR UNITS

CHRISTOPHER FREI

Abstract. We give an affirmative answer to the following question by Jarden and Narkiewicz: Is it true that every number field has a finite extension L such that the ring of integers of L is generated by its units (as a ring)?

As a part of the proof, we generalise a theorem by Hinz on power-free values of polynomials over number fields.

1. Introduction

The earliest result regarding the additive structure of units in rings of algebraic integers dates back to 1964, when Jacobson [12] proved that every element of the rings of integers of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ can be written as a sum of distinct units. Later, Śliwa [17] continued Jacobson's work, proving that there are no other quadratic number fields with that property, nor any pure cubic ones. Belcher [2], [3] continued along these lines and investigated cubic and quartic number fields.

In a particularly interesting lemma [2, Lemma 1], Belcher characterised all quadratic number fields whose ring of integers is generated by its units: These are exactly the fields $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, for which either

(1) $d \in \{-1, -3\}$, or
(2) $d > 0$, $d \not\equiv 1 \mod 4$, and $d + 1$ or $d - 1$ is a perfect square, or
(3) $d > 0$, $d \equiv 1 \mod 4$, and $d + 4$ or $d - 4$ is a perfect square.

This result was independently proved again by Ashrafi and Vámos [1], who also showed the following: Let $\mathcal{O}$ be the ring of integers of a quadratic or complex cubic number field, or of a cyclotomic number field of the form $\mathbb{Q}(\zeta_{2^n})$. Then there is no positive integer N such that every element of $\mathcal{O}$ is a sum of N units.

Jarden and Narkiewicz [13] proved a more general result which implies that the ring of integers of every number field has this property: If R is a finitely generated integral domain of zero characteristic then there is no integer N such that every element of R is a sum of at most N units. This also follows from a result obtained independently by Hajdu [10]. The author [7] proved an analogous version of this and of Belcher's result for rings of S-integers in function fields.

In [13], Jarden and Narkiewicz raised three open problems:

A. Give a criterion for an algebraic extension K of the rationals to have the property that the ring of integers of K is generated by its units.
B. Is it true that each number field has a finite extension L such that the ring of integers of L is generated by its units?
C. Let K be an algebraic number field. Obtain an asymptotical formula for the number $N_k(x)$ of positive rational integers $n \leq x$ which are sums of at most k units of the ring of integers of K.

The result by Belcher stated above solves Problem A for quadratic number fields. Similar criteria have been found for certain types of cubic and quartic number fields

2010 *Mathematics Subject Classification.* Primary 11R04; Secondary 11R27.

Key words and phrases. sums of units, rings of integers, generated by units, additive unit representations.

The author is supported by the Austrian Science Foundation (FWF) project S9611-N23.

[5], [18], [21]. All these results have in common that the unit group of the ring in question is of rank 1.

Quantitative questions similar to Problem C were investigated in [5], [6], [9]. The property asked for in Problem B is known to hold for number fields with an Abelian Galois group, due to the Kronecker-Weber theorem. However, this is all that was known until recently, when the author [8] affirmatively answered the question in the function field case. In this paper, we use similar ideas to solve Problem B in its original number field version:

Theorem 1. *For every number field K there exists a number field L containing K such that the ring of integers of L is generated by its units (as a ring).*

It is crucial to our proof to establish the existence of integers of K with certain properties (see Proposition 4). We achieve this by asymptotically counting such elements. To this end, we need a generalised version of a theorem by Hinz [11, Satz 1.1], which is provided first. Let us start with some notation.

2. Notation and auxiliary results

All rings considered are commutative and with unity, and the ideal $\{0\}$ is never seen as a prime ideal. Two ideals $\mathfrak{a}$, $\mathfrak{b}$ of a ring R are *relatively prime* if $\mathfrak{a}+\mathfrak{b}=R$. Two elements α, $\beta \in R$ are *relatively prime* if the principal ideals (α), (β) are.

The letter K denotes a number field of degree $n>1$, with discriminant d_K and ring of integers $\mathcal{O}_K$. Let there be r distinct real embeddings $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$ and $2s$ distinct non-real embeddings $\sigma_{r+1}, \ldots, \sigma_n : K \to \mathbb{C}$, such that $\overline{\sigma_{r+j}} = \sigma_{r+s+j}$, for all $1 \leq j \leq s$. Then $\sigma : K \to \mathbb{R}^n$ is the standard embedding given by

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \Re\sigma_{r+1}(\alpha), \Im\sigma_{r+1}(\alpha), \ldots, \Re\sigma_{r+s}(\alpha), \Im\sigma_{r+s}(\alpha)).$$

An element $\alpha \in \mathcal{O}_K$ is called *totally positive*, if $\sigma_i(\alpha)>0$ for all $1 \leq i \leq r$.

A non-zero ideal of $\mathcal{O}_K$ is called *m-free*, if it is not divisible by the m-th power of any prime ideal of $\mathcal{O}_K$, and an element $\alpha \in \mathcal{O}_K \setminus \{0\}$ is called *m-free*, if the principal ideal (α) is m-free. We denote the *absolute norm* of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ by $\mathfrak{N}\mathfrak{a}$, that is $\mathfrak{N}\mathfrak{a} = [\mathcal{O}_K : \mathfrak{a}]$. For non-zero ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_K$, the ideal $(\mathfrak{a}, \mathfrak{b})$ is their greatest common divisor. If $\beta \in \mathcal{O}_K \setminus \{0\}$ then we also write $(\mathfrak{a}, \beta)$ instead of $(\mathfrak{a}, (\beta))$. By $\operatorname{supp} \mathfrak{a}$, we denote the set of all prime divisors of the ideal $\mathfrak{a}$ of $\mathcal{O}_K$. The symbol μ stands for the Möbius function for ideals of $\mathcal{O}_K$.

For $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, with $x_i \geq 1$ for all $1 \leq i \leq n$, and $x_{r+s+i} = x_{r+i}$, for all $1 \leq i \leq s$, we define

$$\mathcal{R}(\underline{x}) := \{\alpha \in \mathcal{O}_K \mid \alpha \text{ totally positive, } |\sigma_i(\alpha)| \leq x_i \text{ for all } 1 \leq i \leq n\},$$

and

$$x := x_1 \cdots x_n.$$

Let $f \in \mathcal{O}_K[X]$ be an irreducible polynomial of degree $g \geq 1$. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, let

$$L(\mathfrak{a}) := |\{\beta + \mathfrak{a} \in \mathcal{O}_K/\mathfrak{a} \mid f(\beta) \equiv 0 \mod \mathfrak{a}\}|.$$

By the Chinese remainder theorem, we have $L(\mathfrak{a}_1 \cdots \mathfrak{a}_k) = L(\mathfrak{a}_1) \cdots L(\mathfrak{a}_k)$, for ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ of $\mathcal{O}_K$ that are mutually relatively prime.

We say that the ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a *fixed divisor* of f if $\mathfrak{a}$ contains all $f(\alpha)$, for $\alpha \in \mathcal{O}_K$.

Hinz established the following result, asymptotically counting the set of all $\alpha \in \mathcal{R}(\underline{x})$ such that $f(\alpha)$ is m-free:

Theorem 2 (([11, Satz 1.1]))**.** *If $m \geq \max\{2, \sqrt{2g^2+1} - (g+1)/2\}$, such that no m-th power of a prime ideal of $\mathcal{O}_K$ is a fixed divisor of f, then*

$$\sum_{\substack{\alpha \in \mathcal{R}(\underline{x}) \\ f(\alpha)\ m\text{-free}}} 1 = \frac{(2\pi)^s}{\sqrt{|d_K|}} \cdot x \cdot \prod_{\mathfrak{P}} \left(1 - \frac{L(\mathfrak{P}^m)}{\mathfrak{N}\mathfrak{P}^m}\right) + O(x^{1-u}),$$

as x tends to infinity. Here, $u = u(n, g)$ is an effective positive constant depending only on n and g, the infinite product over all prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ is convergent and positive, and the implicit O-constant depends on K, m and f.

A subring $\mathcal{O}$ of $\mathcal{O}_K$ is called an *order* of K if $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, or, equivalently, $\mathbb{Q}\mathcal{O} = K$. Orders of K are one-dimensional Noetherian domains. For any order $\mathcal{O}$ of K, the *conductor* $\mathfrak{f}$ of $\mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ that is contained in $\mathcal{O}$, that is

$$\mathfrak{f} = \{\alpha \in \mathcal{O}_K \mid \alpha\mathcal{O}_K \subseteq \mathcal{O}\}.$$

In particular, $\mathfrak{f} \supsetneqq \{0\}$, since $\mathcal{O}_K$ is finitely generated as an $\mathcal{O}$-module. For more information about orders, see for example [16, Section I.12].

Assume now that $f \in \mathcal{O}[X]$. Then we define, for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$,

$$L_{\mathcal{O}}(\mathfrak{a}) := |\{\alpha + (\mathcal{O} \cap \mathfrak{a}) \in \mathcal{O}/(\mathcal{O} \cap \mathfrak{a}) \mid f(\alpha) \equiv 0 \mod (\mathcal{O} \cap \mathfrak{a})\}|\,.$$

The natural monomorphism $\mathcal{O}/(\mathcal{O} \cap \mathfrak{a}) \to \mathcal{O}_K/\mathfrak{a}$ yields $L_{\mathcal{O}}(\mathfrak{a}) \leq L(\mathfrak{a})$, and if $\mathfrak{a}_1$, …, $\mathfrak{a}_k$ are ideals of $\mathcal{O}_K$ such that all $\mathfrak{a}_i \cap \mathcal{O}$ are mutually relatively prime then $L_{\mathcal{O}}(\mathfrak{a}_1 \cdots \mathfrak{a}_k) = L_{\mathcal{O}}(\mathfrak{a}_1) \cdots L_{\mathcal{O}}(\mathfrak{a}_k)$.

In our generalised version of Theorem 2, we do not count all $\alpha \in \mathcal{R}(\underline{x})$ such that $f(\alpha)$ is m-free, but all $\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}$, such that $f(\alpha)$ is m-free and $\mathfrak{f}(\alpha) \notin \mathfrak{P}$, for finitely many given prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$.

Theorem 3. *Let $\mathcal{O}$ be an order of K of conductor $\mathfrak{f}$, and $f \in \mathcal{O}[X]$ an irreducible (over $\mathcal{O}_K$) polynomial of degree $g \geq 1$. Let $\mathcal{P}$ be a finite set of prime ideals of $\mathcal{O}_K$ that contains the set $\mathcal{P}_{\mathfrak{f}} := \operatorname{supp} \mathfrak{f}$. Let*

$$m \geq \max\left\{2, \sqrt{2g^2+1} - (g+1)/2\right\} \tag{1}$$

be an integer such that no m-th power of a prime ideal of $\mathcal{O}_K$ is a fixed divisor of f, and denote by $N(\underline{x})$ the number of all $\alpha \in \mathcal{O} \cap \mathcal{R}(\underline{x})$, such that

1. *for all $\mathfrak{P} \in \mathcal{P}$, $f(\alpha) \notin \mathfrak{P}$*
2. *$f(\alpha)$ is m-free.*

Then

$$N(\underline{x}) = Dx + O(x^{1-u}),$$

as x tends to infinity. Here, $u = u(n, g)$ is an explicitly computable positive constant that depends only on n and g. The implicit O-constant depends on K, $\mathcal{P}$, f and m. Moreover,

$$D = \frac{(2\pi)^s}{\sqrt{|d_K|}[\mathcal{O}_K : \mathcal{O}]} \sum_{\mathfrak{a}|\mathfrak{f}} \frac{\mu(\mathfrak{a}) L_{\mathcal{O}}(\mathfrak{a})}{[\mathcal{O} : \mathfrak{a} \cap \mathcal{O}]} \prod_{\mathfrak{P} \in \mathcal{P} \setminus \mathcal{P}_{\mathfrak{f}}} \left(1 - \frac{L(\mathfrak{P})}{\mathfrak{N}\mathfrak{P}}\right) \prod_{\mathfrak{P} \notin \mathcal{P}} \left(1 - \frac{L(\mathfrak{P}^m)}{\mathfrak{N}\mathfrak{P}^m}\right).$$

The sum runs over all ideals of $\mathcal{O}_K$ dividing $\mathfrak{f}$, and the infinite product over all prime ideals $\mathfrak{P} \notin \mathcal{P}$ of $\mathcal{O}_K$ is convergent and positive.

For our application, the proof of Theorem 1, we only need the special case where $m = g = 2$, and we do not need any information about the remainder term. However, the additional effort is small enough to justify a full generalisation of Theorem 2, instead of just proving the special case. The following proposition contains all that we need of Theorem 3 to prove Theorem 1.

Proposition 4. *Assume that for every prime ideal of $\mathcal{O}_K$ dividing 2 or 3, the relative degree is greater than 1, and that $\mathcal{O} \neq \mathcal{O}_K$ is an order of K. Let $\mathcal{P}$ be a finite set of prime ideals of $\mathcal{O}_K$, and let $\eta \in \mathcal{O} \smallsetminus K^2$. Then there is an element $\omega \in \mathcal{O}_K$ with the following properties:*

(1) $\omega \notin \mathcal{O}$,
(2) for all $\mathfrak{P} \in \mathcal{P}$, $\omega^2 - 4\eta \notin \mathfrak{P}$, and
(3) $\omega^2 - 4\eta$ is squarefree.

The basic idea to prove Theorem 1 is as follows: Let $\mathcal{O}$ be the ring generated by the units of $\mathcal{O}_K$. With Proposition 4, we find certain elements $\omega_1, \ldots, \omega_r$ of $\mathcal{O}_K$, such that $\mathcal{O}[\omega_1, \ldots, \omega_r] = \mathcal{O}_K$. Due to the special properties from Proposition 4, we can construct an extension field L of K, such that $\omega_1, \ldots, \omega_r$ are sums of units of $\mathcal{O}_L$, and $\mathcal{O}_L$ is generated by units as a ring extension of $\mathcal{O}_K$. This is enough to prove that $\mathcal{O}_L$ is generated by its units as a ring.

3. Proof of Theorem 3

We follow the same strategy as Hinz [11] in his proof of Theorem 2, with modifications where necessary. For any vector $v \in \mathbb{R}^n$, we denote its Euclidean length by $|v|$. We use a theorem by Widmer to count lattice points:

Theorem 5 (([19, Theorem 5.4]))**.** *Let Λ be a lattice in $\mathbb{R}^n$ with successive minima (with respect to the unit ball) $\lambda_1, \ldots, \lambda_n$. Let B be a bounded set in $\mathbb{R}^n$ with boundary ∂B. Assume that there are M maps $\Phi : [0,1]^{n-1} \to \mathbb{R}^n$ satisfying a Lipschitz condition*

$$|\Phi(v) - \Phi(w)| \leq L\,|v - w|\,,$$

such that ∂B is covered by the union of the images of the maps Φ. Then B is measurable, and moreover

$$\left| |B \cap \Lambda| - \frac{\operatorname{Vol} B}{\det \Lambda} \right| \leq c_0(n) M \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i}.$$

For $i = 0$, the expression in the maximum is to be understood as 1. Furthermore, one can choose $c_0(n) = n^{3n^2/2}$.

We need some basic facts about contracted ideals in orders. The statements of the following lemma can hardly be new, but since the author did not find a reference we shall prove them for the sake of completeness.

Lemma 6. *Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order of K with conductor $\mathfrak{f}$. Then, for any ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_K$, the following holds:*
(1) if $\mathfrak{a} + \mathfrak{f} = \mathcal{O}_K$ and $\mathfrak{b} \mid \mathfrak{f}$ then $(\mathfrak{a} \cap \mathcal{O}) + (\mathfrak{b} \cap \mathcal{O}) = \mathcal{O}$.
(2) if $\mathfrak{a} + \mathfrak{f} = \mathcal{O}_K$, $\mathfrak{b} + \mathfrak{f} = \mathcal{O}_K$, and $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$ then $(\mathfrak{a} \cap \mathcal{O}) + (\mathfrak{b} \cap \mathcal{O}) = \mathcal{O}$.
(3) if $\mathfrak{a} + \mathfrak{f} = \mathcal{O}_K$ then $[\mathcal{O} : \mathfrak{a} \cap \mathcal{O}] = \mathfrak{N}\mathfrak{a}$.

Proof. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ with $\mathfrak{a} + \mathfrak{f} = \mathcal{O}_K$, we have

$$(\mathfrak{a} \cap \mathcal{O}) + \mathfrak{f} = (\mathfrak{a} + \mathfrak{f}) \cap \mathcal{O} = \mathcal{O}_K \cap \mathcal{O} = \mathcal{O}.$$

The first equality holds because for every $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{f} \subseteq \mathcal{O}$ with $\alpha + \beta \in \mathcal{O}$ it follows that $\alpha \in \mathcal{O}$.

Moreover, if $\mathfrak{c}$ is an ideal of $\mathcal{O}$ with $\mathfrak{c} + \mathfrak{f} = \mathcal{O}$ then

$$\mathfrak{c}\mathcal{O}_K + \mathfrak{f} \supseteq (\mathfrak{c} + \mathfrak{f})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K.$$

Therefore,

$$\varphi : \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O} \text{ and } \psi : \mathfrak{c} \mapsto \mathfrak{c}\mathcal{O}_K$$

are maps between the sets of ideals

$$\{\mathfrak{a} \subseteq \mathcal{O}_K \mid \mathfrak{a} + \mathfrak{f} = \mathcal{O}_K\} \text{ and } \{\mathfrak{c} \subseteq \mathcal{O} \mid \mathfrak{c} + \mathfrak{f} = \mathcal{O}\}.$$

Let us prove that φ and ψ are inverse to each other. Clearly, $(\varphi \circ \psi)(\mathfrak{c}) \supseteq \mathfrak{c}$ and $(\psi \circ \varphi)(\mathfrak{a}) \subseteq \mathfrak{a}$. Also,

$$(\varphi \circ \psi)(\mathfrak{c}) = (\mathfrak{c}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} = (\mathfrak{c}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{c} + \mathfrak{f}) \subseteq \mathfrak{c} + \mathfrak{f}(\mathfrak{c}\mathcal{O}_K \cap \mathcal{O}) \subseteq \mathfrak{c} + \mathfrak{c}\mathfrak{f}\mathcal{O}_K \subseteq \mathfrak{c},$$

and

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}((\mathfrak{a} \cap \mathcal{O}) + \mathfrak{f}) \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + \mathfrak{f}\mathfrak{a} \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + (\mathfrak{a} \cap \mathcal{O}) = (\psi \circ \varphi)(\mathfrak{a}).$$

Clearly, φ and ψ are multiplicative, so the monoid of ideals of $\mathcal{O}$ relatively prime to $\mathfrak{f}$ is isomorphic with the monoid of ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{f}$. (In the special case where $\mathcal{O}$ is an order in an imaginary quadratic field this is proved in [4, Proposition 7.20].)

If $\mathfrak{a}$, $\mathfrak{b}$ are as in *(1)* then $\mathfrak{f} \subseteq \mathfrak{b} \cap \mathcal{O}$, and thus $\mathcal{O} = (\mathfrak{a} \cap \mathcal{O}) + \mathfrak{f} \subseteq (\mathfrak{a} \cap \mathcal{O}) + (\mathfrak{b} \cap \mathcal{O})$.

Suppose now that $\mathfrak{a}$, $\mathfrak{b}$ are as in *(2)*, and $\varphi(\mathfrak{a}) + \varphi(\mathfrak{b}) =: \mathfrak{c} \subseteq \mathcal{O}$. Then $\mathfrak{c} + \mathfrak{f} \supseteq \varphi(\mathfrak{a}) + \mathfrak{f} = \mathcal{O}$, whence $\mathfrak{c} = \varphi(\mathfrak{d})$, for some ideal $\mathfrak{d}$ of $\mathcal{O}_K$ relatively prime to $\mathfrak{f}$. Now $\mathfrak{a} \subseteq \mathfrak{d}$ and $\mathfrak{b} \subseteq \mathfrak{d}$, so $\mathfrak{d} = \mathcal{O}_K$, and thus $\mathfrak{c} = \mathcal{O}$.

To prove *(3)*, we show that the natural monomorphism $\Phi : \mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}$ is surjective. This holds true, since

$$\mathcal{O}_K = \mathfrak{a} + \mathfrak{f} \subseteq \mathfrak{a} + \mathcal{O}.$$

$\square$

For now, let us prove Theorem 3 with the additional assumption that $f(\alpha) \neq 0$ for all totally positive $\alpha \in \mathcal{O}_K$. This holds of course if $\deg f \geq 2$, since f is irreducible over $\mathcal{O}_K$. At the end of the proof, we specify the changes necessary to drop this assumption. Let

$$\Pi := \prod_{\mathfrak{P} \in \mathcal{P}} \mathfrak{P}.$$

It is well known that

$$\sum_{\mathfrak{a} | \mathfrak{b}} \mu(\mathfrak{a}) = \begin{cases} 1, & \text{if } \mathfrak{b} = \mathcal{O}_K \\ 0, & \text{otherwise,} \end{cases}$$

for any nonzero ideal $\mathfrak{b}$ of $\mathcal{O}_K$. Assume that $f(\alpha) \neq 0$. Then

$$\sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) = \begin{cases} 1, & \text{if for all } \mathfrak{P} \in \mathcal{P},\ f(\alpha) \notin \mathfrak{P} \\ 0, & \text{otherwise.} \end{cases}$$

Write $(f(\alpha)) = \mathfrak{c}_1\mathfrak{c}_2^m$, where $\mathfrak{c}_1$ is m-free. Then $\mathfrak{b}^m \mid f(\alpha)$ if and only if $\mathfrak{b} \mid \mathfrak{c}_2$, whence

$$\sum_{\mathfrak{b}^m | f(\alpha)} \mu(\mathfrak{b}) = \begin{cases} 1, & \text{if } f(\alpha) \text{ is } m\text{-free} \\ 0, & \text{otherwise.} \end{cases}$$

Therefore,

$$N(\underline{x}) = \sum_{\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}} \sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) \sum_{\mathfrak{b}^m | f(\alpha)} \mu(\mathfrak{b}). \tag{2}$$

Put

$$N_1(\underline{x}, y) := \sum_{\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}} \sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) \sum_{\substack{(\mathfrak{b}, \Pi) = 1 \\ \mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} \leq y}} \mu(\mathfrak{b}), \tag{3}$$

and

$$N_2(\underline{x}, y) := \sum_{\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}} \sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) \sum_{\substack{\mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} > y}} \mu(\mathfrak{b}). \tag{4}$$

It will turn out that, with a suitable choice of y, the main component of $N(\underline{x})$ is $N_1(\underline{x}, y)$. In fact, since

$$\sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) \sum_{\substack{(\mathfrak{b},\Pi)\neq 1 \\ \mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} \leq y}} \mu(\mathfrak{b}) = 0,$$

for all $\alpha \in \mathcal{O}_K$ with $f(\alpha) \neq 0$, we have

$$N(\underline{x}) = N_1(\underline{x}, y) + N_2(\underline{x}, y). \tag{5}$$

3.1. **Estimation of** $N_2(\underline{x}, y)$**.** We can reduce the estimation of $N_2(\underline{x}, y)$ to a similar computation to that which has already been performed by Hinz [11]. Indeed, for any nonzero ideal $\mathfrak{q}$ of $\mathcal{O}_K$, we have

$$\begin{aligned} |N_2(\underline{x}, y)| &\leq \sum_{\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}} \Big| \sum_{\mathfrak{a} | (\Pi, f(\alpha))} \mu(\mathfrak{a}) \Big| \cdot \Big| \sum_{\substack{\mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} > y}} \mu(\mathfrak{b}) \Big| \\ &\leq \Big(\sum_{\mathfrak{a} | \Pi} \mu(\mathfrak{a})^2 \Big) \sum_{\alpha \in \mathcal{R}(\underline{x})} \Big| \sum_{\mathfrak{c} | \mathfrak{q}} \sum_{\substack{\mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} > y \\ (\mathfrak{b}, \mathfrak{q}) = \mathfrak{c}}} \mu(\mathfrak{b}) \Big| \\ &\leq \mathfrak{N}\Pi \mathfrak{N}\mathfrak{q} \sum_{\alpha \in \mathcal{R}(\underline{x})} \sum_{\substack{\mathfrak{b}^m | f(\alpha) \\ \mathfrak{N}\mathfrak{b} > y / \mathfrak{N}\mathfrak{q} \\ (\mathfrak{b}, \mathfrak{q}) = 1}} \mu(\mathfrak{b})^2. \end{aligned}$$

The last expression differs only by a multiplicative constant from the right-hand side of [11, (2.6)], so we can use Hinz's estimates [11, pp. 139-145] without any change. With a suitable choice of $\mathfrak{q}$ ([11, (2.8)]), we get (see Lemma 2.2 and the proof of Theorem 2.1 from [11])

$$N_2(\underline{x}, y) = O(x^{g/(2l+1)} y^{(l-m)/(2l+1)} (x y^{(l-m)/g} + 1)), \tag{6}$$

for any integer $1 \leq l \leq m - 1$, as x, $y \to \infty$. The implicit O-constant depends on K, f, m, and $\mathcal{P}$.

3.2. **Computation of** $N_1(\underline{x}, y)$**.** Now let us compute $N_1(\underline{x}, y)$. We have

$$N_1(\underline{x}, y) = \sum_{\mathfrak{a} | \Pi} \mu(\mathfrak{a}) \sum_{\substack{(\mathfrak{b}, \Pi) = 1 \\ \mathfrak{N}\mathfrak{b} \leq y}} \mu(\mathfrak{b}) \left| M_{\mathfrak{a},\mathfrak{b}}(\underline{x}) \right|, \tag{7}$$

where $M_{\mathfrak{a},\mathfrak{b}}(\underline{x})$ is the set of all $\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}$ such that $f(\alpha) \in \mathfrak{a}$ and $f(\alpha) \in \mathfrak{b}^m$. Since all occurring ideals $\mathfrak{a}$, $\mathfrak{b}$ are relatively prime, we have

$$\begin{aligned} M_{\mathfrak{a},\mathfrak{b}}(\underline{x}) &= \{\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O} \mid f(\alpha) \equiv 0 \mod \mathfrak{a}\mathfrak{b}^m\} \\ &= \bigcup_{\substack{\beta + \mathfrak{a}\mathfrak{b}^m \in \mathcal{O}_K / \mathfrak{a}\mathfrak{b}^m \\ f(\beta) \equiv 0 \mod \mathfrak{a}\mathfrak{b}^m}} ((\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}), \end{aligned}$$

where the union over all roots of f modulo $\mathfrak{a}\mathfrak{b}^m$ is disjoint. We asymptotically count each of the sets $(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}$ by counting lattice points. Consider the natural monomorphism $\varphi : \mathcal{O}/(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}) \to \mathcal{O}_K/\mathfrak{a}\mathfrak{b}^m$, mapping $\alpha + (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O})$ to $\alpha + \mathfrak{a}\mathfrak{b}^m$.

Lemma 7. *The set* $(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O}$ *is not empty if and only if* $\beta + \mathfrak{a}\mathfrak{b}^m$ *is in the image of* φ.

In that case, let $\varepsilon \in [0, 1/n]$, *and* $c \geq 1/m$ *such that* $\mathfrak{N}\mathfrak{b} \leq x^c$. *Then*

$$\left| |(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}| - c_1(K) \frac{x}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \right| \leq c_2(K) \frac{x^{1-\varepsilon}}{\mathfrak{N}\mathfrak{b}^{(1-\varepsilon)/c}}.$$

Here, $c_1(K) = (2\pi)^s/\sqrt{|d_K|}$, and $c_2(K)$ is an explicitly computable constant which depends only on K.

Proof. If $\alpha \in (\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O}$ then $\beta + \mathfrak{a}\mathfrak{b}^m = \alpha + \mathfrak{a}\mathfrak{b}^m = \varphi(\alpha + (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}))$. If, on the other hand, $\beta + \mathfrak{a}\mathfrak{b}^m = \varphi(\alpha + (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}))$, for some $\alpha \in \mathcal{O}$, then $\alpha + \mathfrak{a}\mathfrak{b}^m = \beta + \mathfrak{a}\mathfrak{b}^m$, and thus $\alpha \in (\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O}$.

Assume now that $(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O}$ is not empty. Then, for any $\alpha \in (\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O}$, we have

$$|(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}| = |(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}) \cap (\mathcal{R}(\underline{x}) - \alpha)|\,.$$

Let $\sigma : K \to \mathbb{R}^n$ be the standard embedding defined in Section 2, and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be the linear automorphism given by

$$T(e_i) = x^{1/n}/x_i \cdot e_i, \text{ for } 1 \leq i \leq r, \text{ and}$$

$$T(e_{r+i}) = x^{1/n}/x_{r+\lceil i/2 \rceil} \cdot e_{r+i}, \text{ for } 1 \leq i \leq 2s,$$

where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$. Then

$$\det T = x/(x_1 \cdots x_r x_{r+1}^2 \cdots x_{r+s}^2) = x/(x_1 \cdots x_n) = 1. \tag{8}$$

Therefore, $T(\sigma(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}))$ is a lattice in $\mathbb{R}^n$ with determinant

$$\det T(\sigma(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O})) = 2^{-s}\sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]. \tag{9}$$

Moreover, $T(\sigma(\mathcal{R}(\underline{x}) - \alpha)) = T(\sigma(\mathcal{O}_K)) \cap B$, where B is a product of r line segments of length $x^{1/n}$ and s disks of radius $x^{1/n}$. Clearly,

$$\mathrm{Vol}(B) = \pi^s x. \tag{10}$$

We construct maps $\Phi : [0,1]^{n-1} \to \mathbb{R}^n$ as in Theorem 5. Write $B = l_1 \times \cdots \times l_r \times d_{r+1} \times \cdots \times d_{r+s}$, with line segments l_i of length $x^{1/n}$ and disks d_i of radius $x^{1/n}$. Put

$$B_i := l_1 \times \cdots \times l_{i-1} \times (\partial l_i) \times l_{i+1} \times \cdots \times l_r \times d_{r+1} \times \cdots \times d_{r+s},$$

for $1 \leq i \leq r$, and

$$B_i := l_1 \times \cdots \times l_r \times d_{r+1} \times \cdots \times d_{i-1} \times (\partial d_i) \times d_{i+1} \times \cdots \times d_{r+s},$$

for $r + 1 \leq i \leq r + s$. Then

$$\partial B = \bigcup_{i=1}^{r+s} B_i.$$

For $1 \leq i \leq r$, ∂l_i consists of two points, and the remaining factor of B_i is contained in an $(n-1)$-dimensional cube of edge-length $2x^{1/n}$. For $r + 1 \leq i \leq r + s$, ∂d_i is a circle of radius $x^{1/n}$, and the remaining factor of B_i is contained in an $(n-2)$-dimensional cube of edge-length $2x^{1/n}$. Therefore, we find $2r + s$ maps $\Phi : [0,1]^{n-1} \to \mathbb{R}^n$ with

$$|\Phi(v) - \Phi(w)| \leq 2\pi x^{1/n} |v - w|\,, \tag{11}$$

such that ∂B is covered by the union of the images of the maps Φ.

Since

$$\begin{aligned}|(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}| &= |T(\sigma(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O})) \cap T(\sigma(\mathcal{R}(\underline{x}) - \alpha))| \\ &= |T(\sigma(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O})) \cap B|\,,\end{aligned}$$

Theorem 5 and (9), (10), (11) yield

$$\left| |(\beta + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{R}(\underline{x}) \cap \mathcal{O}| - \frac{(2\pi)^s}{\sqrt{|d_K|}} \frac{x}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \right| \leq c_3(K) \frac{x^{i/n}}{\lambda_1 \cdots \lambda_i}. \tag{12}$$

Here, $c_3(K) = (2r+s)(2\pi)^{n-1} n^{3n^2/2}$, $i \in \{0, \ldots, n-1\}$, and $\lambda_1, \ldots, \lambda_i$ are the first i successive minima of the lattice $T(\sigma(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}))$ with respect to the unit ball.

Let us further estimate the right-hand side of (12). First, we need a lower bound for λ_i in terms of $\mathfrak{N}\mathfrak{b}$. For each i, there is some $\alpha \in (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}) \smallsetminus \{0\}$ with $\lambda_i = |T(\sigma(\alpha))|$. Since $\alpha \in \mathfrak{b}^m$, the inequality of weighted arithmetic and geometric means and (8) yield (cf. [15, Lemma 5], [19, Lemma 9.7])

$$\mathfrak{N}\mathfrak{b}^m \leq |N(\alpha)| = \prod_{j=1}^{n} |\sigma_j(\alpha)| = \prod_{j=1}^{r+s} \left| \frac{x^{1/n}}{x_j} \sigma_j(\alpha) \right|^{d_j}$$
$$\leq \left(\frac{1}{n} \sum_{j=1}^{r+s} d_j \left| \frac{x^{1/n}}{x_j} \sigma_j(\alpha) \right|^2 \right)^{n/2} \leq \left(\frac{2}{n} \right)^{n/2} \lambda_i^n.$$

Here, $d_j = 1$ for $1 \leq j \leq r$, and $d_j = 2$ for $r+1 \leq j \leq r+s$. Recall that $n \geq 2$. With the assumptions on ε and c in mind, we get

$$\frac{x^{i/n}}{\lambda_1 \cdots \lambda_i} \leq \left(\frac{2}{n} \right)^{i/2} \frac{x^{i/n}}{\mathfrak{N}\mathfrak{b}^{mi/n}} \leq \frac{x^{1-\varepsilon}}{\mathfrak{N}\mathfrak{b}^{mi/n + (1-\varepsilon-i/n)/c}} \leq \frac{x^{1-\varepsilon}}{\mathfrak{N}\mathfrak{b}^{(1-\varepsilon)/c}}.$$

□

Since $f \in \mathcal{O}[X]$, we can conclude from $\beta + \mathfrak{a}\mathfrak{b}^m = \varphi(\alpha + (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}))$ that $f(\beta) \in \mathfrak{a}\mathfrak{b}^m$ if and only if $f(\alpha) \in \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}$. Therefore,

$$M_{\mathfrak{a},\mathfrak{b}}(\underline{x}) = \bigcup_{\substack{\alpha + (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}) \in \mathcal{O}/(\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}) \\ f(\alpha) \equiv 0 \mod (\mathfrak{a}\mathfrak{b}^m \cap \mathcal{O})}} \left((\alpha + \mathfrak{a}\mathfrak{b}^m) \cap \mathcal{O} \cap \mathcal{R}(\underline{x}) \right),$$

and thus

$$\left| |M_{\mathfrak{a},\mathfrak{b}}(\underline{x})| - c_1(K) L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m) \frac{x}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \right| \leq c_2(K) L(\mathfrak{a}) L(\mathfrak{b}^m) \frac{x^{1-\varepsilon}}{\mathfrak{N}\mathfrak{b}^{(1-\varepsilon)/c}},$$

whenever $\mathfrak{N}\mathfrak{b} \leq x^c$, for some $c \geq 1/m$, and $\varepsilon \in [0, 1/n]$. Notice that $L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m) \leq L(\mathfrak{a}\mathfrak{b}^m) = L(\mathfrak{a}) L(\mathfrak{b}^m)$, since $\mathfrak{a}$, $\mathfrak{b}$ are relatively prime. Therefore,

$$\Big| \sum_{\substack{(\mathfrak{b},\Pi)=1 \\ \mathfrak{N}\mathfrak{b} \leq x^c}} \mu(\mathfrak{b}) \, |M_{\mathfrak{a},\mathfrak{b}}(\underline{x})| - c_1(K) x \sum_{(\mathfrak{b},\Pi)=1} \mu(\mathfrak{b}) \frac{L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \Big|$$
$$\leq \Big| \sum_{\substack{(\mathfrak{b},\Pi)=1 \\ \mathfrak{N}\mathfrak{b} \leq x^c}} \mu(\mathfrak{b}) \left(|M_{\mathfrak{a},\mathfrak{b}}(\underline{x})| - c_1(K) x \frac{L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \right) \Big|$$
$$+ \Big| c_1(K) x \sum_{\substack{(\mathfrak{b},\Pi)=1 \\ \mathfrak{N}\mathfrak{b} > x^c}} \mu(\mathfrak{b}) \frac{L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \Big|$$
$$\leq c_2(K) x^{1-\varepsilon} L(\mathfrak{a}) \sum_{(\mathfrak{b},\Pi)=1} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{\mathfrak{N}\mathfrak{b}^{(1-\varepsilon)/c}}$$
$$+ c_1(K) L(\mathfrak{a}) x \sum_{\substack{(\mathfrak{b},\Pi)=1 \\ \mathfrak{N}\mathfrak{b} > x^c}} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]}.$$

Let $s > 1$ be a real number. As in [11, top of p. 138], we get

$$\sum_{\mathfrak{N}\mathfrak{b} \leq y} \mu(\mathfrak{b})^2 L(\mathfrak{b}^m) = O(y),$$

whence

$$\sum_{\substack{(\mathfrak{b},\Pi)=1 \\ \mathfrak{N}\mathfrak{b} > x^c}} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{\mathfrak{N}\mathfrak{b}^s} = O(x^{c(1-s)}),$$

by partial summation. Therefore, the sum

$$\sum_{(\mathfrak{b},\Pi)=1} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{\mathfrak{N}\mathfrak{b}^{(1-\varepsilon)/c}}$$

converges whenever $c < 1-\varepsilon$. Since $[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}] \geq \mathfrak{N}\mathfrak{b}^m$, we have

$$\sum_{\substack{(\mathfrak{b},\Pi)=1\\ \mathfrak{N}\mathfrak{b}>x^c}} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} \leq \sum_{\substack{(\mathfrak{b},\Pi)=1\\ \mathfrak{N}\mathfrak{b}>x^c}} \mu(\mathfrak{b})^2 \frac{L(\mathfrak{b}^m)}{\mathfrak{N}\mathfrak{b}^m} = O(x^{c(1-m)}).$$

Putting everything together, we get

$$\sum_{\substack{(\mathfrak{b},\Pi)=1\\ \mathfrak{N}\mathfrak{b}\leq x^c}} \mu(\mathfrak{b})\, |M_{\mathfrak{a},\mathfrak{b}}(\underline{x})| = c_1(K)x \sum_{(\mathfrak{b},\Pi)=1} \mu(\mathfrak{b}) \frac{L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} + O(x^{1-\varepsilon} + x^{1+c(1-m)}), \tag{13}$$

whenever $1/m \leq c < 1-\varepsilon$ and $0 \leq \varepsilon \leq 1/n$, as $x \to \infty$. The implicit O-constant depends on K, $\mathfrak{a}$, $\mathcal{P}$, f, m, c and ε.

3.3. **End of the proof.** By (5), (6), (7) and (13), we get

$$\begin{aligned} N(\underline{x}) &= N_1(\underline{x}, x^c) + N_2(\underline{x}, x^c) \\ &= c_1(K)x \sum_{a|\Pi} \mu(\mathfrak{a}) \sum_{(\mathfrak{b},\Pi)=1} \mu(\mathfrak{b}) \frac{L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}^m \cap \mathcal{O}]} + R \\ &=: Dx + R, \end{aligned}$$

where

$$R = O(x^{1-\varepsilon} + x^{1-c(m-1)} + x^{g/(2l+1)-c(m-l)/(2l+1)}(x^{1-c(m-l)/g} + 1))$$

holds for every $0 \leq \varepsilon \leq 1/n$, $1/m \leq c < 1-\varepsilon$, and $l \in \{1, \dots, m-1\}$, as $x \to \infty$. The implicit O-constant depends on K, $\mathcal{P}$, f, m, c, and ε.

Assume first that $m > g+1$. Then we put

$$l := m - g, \quad c := 1 - 5/(g+10), \quad \varepsilon := \min\{1/n,\ 4/(g+10)\},$$

to get

$$R = O(x^{1-1/n} + x^{1-4/(g+10)} + x^{1-g(g+5)/(g+10)} + x^{(g+5)/(g+10)}) = O(x^{1-u(n,g)}),$$

with $u(n,g)$ as in the theorem.

Now suppose that $2 \leq m \leq g+1$. Then

$$R = O(x^{1-\varepsilon} + x^{1-c(m-1)} + x^{1+g/(2l+1)-c(m-l)(g+2l+1)/(g(2l+1))}).$$

We proceed as in [11, Section 3, Proof of Theorem 1.1]. For every m that satisfies (1), we find some $1 \leq l \leq m-1 \leq g$, such that $m - l > g^2/(2l+g+1)$. Then we can choose some c, depending only on g, l, with

$$\frac{1}{m} \leq \frac{g(2l+2)}{g(2l+2)(m-l+1)} \leq \frac{g(2l+1)+g^2}{(m-l)(2l+g+1)+g(2l+1)} \leq c < 1.$$

A straightforward computation shows that

$$1 + g/(2l+1) - c(m-l)(g+2l+1)(g(2l+1)) \leq c.$$

For any $0 < \varepsilon < 1-c$, $\varepsilon \leq 1/n$, we get

$$R = O(x^{1-\varepsilon} + x^{1-c} + x^c) = O(x^{1-u(n,g)}),$$

for a suitable choice of $u(n,g)$. Notice that there are only finitely many values of m for every g.

The only task left is to prove that D has the form claimed in the theorem. We split up D in the following way: Let Π_1 be the product of all prime ideals in $\mathcal{P} \setminus \mathcal{P}_{\mathfrak{f}}$. Then

$$D = c_1(K) \sum_{\mathfrak{a} | \mathfrak{f}} \mu(\mathfrak{a}) \sum_{\mathfrak{b} | \Pi_1} \mu(\mathfrak{b}) \sum_{(\mathfrak{c}, \Pi)=1} \frac{\mu(\mathfrak{c}) L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}\mathfrak{c}^m)}{[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}\mathfrak{c}^m \cap \mathcal{O}]}$$
$$= \frac{c_1(K)}{[\mathcal{O}_K : \mathcal{O}]} \sum_{\mathfrak{a} | \mathfrak{f}} \frac{\mu(\mathfrak{a}) L_{\mathcal{O}}(\mathfrak{a})}{[\mathcal{O} : \mathfrak{a} \cap \mathcal{O}]} \sum_{\mathfrak{b} | \Pi_1} \frac{\mu(\mathfrak{b}) L_{\mathcal{O}}(\mathfrak{b})}{[\mathcal{O} : \mathfrak{b} \cap \mathcal{O}]} \sum_{(\mathfrak{c}, \Pi)=1} \frac{\mu(\mathfrak{c}) L_{\mathcal{O}}(\mathfrak{c}^m)}{[\mathcal{O} : \mathfrak{c}^m \cap \mathcal{O}]}.$$

This holds because for all combinations of $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ as above, the $\mathcal{O}$-ideals $(\mathfrak{a} \cap \mathcal{O})$, $(\mathfrak{b} \cap \mathcal{O})$ and $(\mathfrak{c}^m \cap \mathcal{O})$ are relatively prime to each other, by Lemma 6. Therefore,

$$[\mathcal{O}_K : \mathfrak{a}\mathfrak{b}\mathfrak{c}^m \cap \mathcal{O}] = [\mathcal{O}_K : \mathcal{O}][\mathcal{O} : \mathfrak{a} \cap \mathcal{O}][\mathcal{O} : \mathfrak{b} \cap \mathcal{O}][\mathcal{O} : \mathfrak{c}^m \cap \mathcal{O}],$$

and

$$L_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}\mathfrak{c}^m) = L_{\mathcal{O}}(\mathfrak{a}) L_{\mathcal{O}}(\mathfrak{b}) L_{\mathcal{O}}(\mathfrak{c}^m).$$

Finally, we notice that, by Lemma 6, $[\mathcal{O} : \mathfrak{r} \cap \mathcal{O}] = \mathfrak{N}\mathfrak{r}$ and thus $L_{\mathcal{O}}(\mathfrak{r}) = L(\mathfrak{r})$, for any ideal $\mathfrak{r}$ of $\mathcal{O}_K$ relatively prime to $\mathfrak{f}$. A simple Euler product expansion yields the desired form of D. All factors of the infinite product

$$\prod_{\mathfrak{P} \notin \mathcal{P}} \left(1 - \frac{L(\mathfrak{P}^m)}{\mathfrak{N}\mathfrak{P}^m}\right)$$

are positive, since no $\mathfrak{P}^m$ is a fixed divisor of f. For all but the finitely many prime ideals of $\mathcal{O}_K$ that divide the discriminant of f, we have $L(\mathfrak{P}^m) = L(\mathfrak{P}) \leq g$. Therefore, the infinite product is convergent and positive.

This concludes the proof of Theorem 3 under the assumption that f has no totally positive root in K. If f has such a root then we let the first sum in (2), (3), (4) run over all $\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}$ such that $f(\alpha) \neq 0$. The estimation of $N_2(\underline{x}, y)$ in Section 3.1 holds still true, since a possible α with $f(\alpha) = 0$ is ignored in Hinz's estimates anyway. In (7), we get an error term $O(y)$. This additional error term becomes irrelevant in Section 3.3.

4. Proof of Proposition 4

We need the following estimate for the index $[\mathcal{O}_K : \mathcal{O}]$.

Lemma 8. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be distinct prime ideals of $\mathcal{O}$. For each $1 \leq i \leq k$, let*

$$\mathfrak{p}_i \mathcal{O}_K = \mathfrak{P}_{i,1}^{e_{i,1}} \cdots \mathfrak{P}_{i,l_i}^{e_{i,l_i}}$$

be the factorisation of $\mathfrak{p}_i$ in $\mathcal{O}_K$, with distinct prime ideals $\mathfrak{P}_{i,j}$ of $\mathcal{O}_K$, and $e_{i,j}$, $l_i \geq 1$. Then

$$[\mathcal{O}_K : \mathcal{O}] \geq \prod_{i=1}^{k} \frac{1}{[\mathcal{O} : \mathfrak{p}_i]} \prod_{j=1}^{l_i} \mathfrak{N}\mathfrak{P}_{i,j}^{e_{i,j}},$$

with equality if and only if $\mathfrak{f}$ divides $\prod_{i=1}^{k} \prod_{j=1}^{l_i} \mathfrak{P}_{i,j}^{e_{i,j}}$.

Proof. Put

$$\Pi := \prod_{i=1}^{k} \prod_{j=1}^{l_i} \mathfrak{P}_{i,j}^{e_{i,j}}.$$

Then we have

$$[\mathcal{O}_K : \mathcal{O}] = \frac{[\mathcal{O}_K : \Pi][\Pi : \Pi \cap \mathcal{O}]}{[\mathcal{O} : \Pi \cap \mathcal{O}]} \geq \frac{\mathfrak{N}\Pi}{[\mathcal{O} : \bigcap_{i=1}^{k} \mathfrak{p}_i]} = \frac{\prod_{i=1}^{k} \prod_{j=1}^{l_i} \mathfrak{N}\mathfrak{P}_{i,j}^{e_{i,j}}}{\prod_{i=1}^{k} [\mathcal{O} : \mathfrak{p}_i]},$$

since $[\mathcal{O} : \Pi \cap \mathcal{O}] = [\mathcal{O} : \bigcap_{i=1}^{k} \mathfrak{p}_i] = \prod_{i=1}^{k} [\mathcal{O} : \mathfrak{p}_i]$, by the Chinese remainder theorem. Moreover, we have $\Pi = \Pi \cap \mathcal{O}$ if and only if $\mathfrak{f}$ divides Π. $\square$

Without loss of generality, we may assume that $\mathcal{P}$ contains all prime ideals of $\mathcal{O}_K$ dividing the conductor $\mathfrak{f}$ of $\mathcal{O}$. Since $\eta \in \mathcal{O} \smallsetminus K^2$, the polynomial $f := X^2 - 4\eta \in \mathcal{O}[X]$ is irreducible over $\mathcal{O}_K$. Evaluating f at 0 and 1, we see that the only fixed divisor of f is (1).

We put $x_1 = \cdots = x_n$, so

$$\mathcal{R}(\underline{x}) = \{\alpha \in \mathcal{O}_K \mid \alpha \text{ totally positive}, \max_{1\le i\le n} |\sigma_i(\alpha)| \le x^{1/n}\}$$

depends only on x. Let $N(x)$ be the number of all $\alpha \in \mathcal{R}(\underline{x})$, such that

(1) for all $\mathfrak{P} \in \mathcal{P}$, $\alpha^2 - 4\eta \notin \mathfrak{P}$, and
(2) $\alpha^2 - 4\eta$ is squarefree,

and let $N_{\mathcal{O}}(x)$ be the number of all $\alpha \in \mathcal{R}(\underline{x}) \cap \mathcal{O}$ with the same two properties.

Theorem 3, with $m = g = 2$, invoked once with the maximal order $\mathcal{O}_K$ and once with the order $\mathcal{O}$, yields

$$N(x) = Dx + O(x^{1-u}) \text{ and } N_{\mathcal{O}}(x) = D_{\mathcal{O}}x + O(x^{1-u}).$$

To prove the proposition, it is enough to show that

$$\lim_{x\to\infty} \frac{N_{\mathcal{O}}(x)}{x} < \lim_{x\to\infty} \frac{N(x)}{x},$$

that is, $D_{\mathcal{O}} < D$.

By Theorem 3, the infinite product

$$\prod_{\mathfrak{P}\notin\mathcal{P}} \left(1 - \frac{L(\mathfrak{P}^2)}{\mathfrak{N}\mathfrak{P}^2}\right)$$

is convergent and positive. Moreover, we notice that

$$(1 - L(\mathfrak{P})/\mathfrak{N}\mathfrak{P}) > 1/2, \tag{14}$$

for every prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$. This is obvious if $2 \notin \mathfrak{P}$, since then $\mathfrak{N}\mathfrak{P} \ge 5$ by the hypotheses of the proposition, but f is of degree 2, so $L(\mathfrak{P}) \le 2$. If $2 \in \mathfrak{P}$ then we have $f \equiv X^2 \mod \mathfrak{P}$, whence $L(\mathfrak{P}) = 1$. On the other hand, $\mathfrak{N}\mathfrak{P} \ge 4$, so (14) holds again. Therefore, the finite product

$$\prod_{\mathfrak{P}\in\mathcal{P}\setminus\mathcal{P}_{\mathfrak{f}}} \left(1 - \frac{L(\mathfrak{P})}{\mathfrak{N}\mathfrak{P}}\right)$$

is positive as well. The proposition is proved if we can show that

$$\frac{1}{[\mathcal{O}_K : \mathcal{O}]} \sum_{\mathfrak{a}\mid\mathfrak{f}} \frac{\mu(\mathfrak{a})L_{\mathcal{O}}(\mathfrak{a})}{[\mathcal{O} : \mathfrak{a}\cap\mathcal{O}]} < \prod_{\mathfrak{P}\in\mathcal{P}_{\mathfrak{f}}} \left(1 - \frac{L(\mathfrak{P})}{\mathfrak{N}\mathfrak{P}}\right). \tag{15}$$

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the prime ideals of $\mathcal{O}$ that contain the conductor $\mathfrak{f}$, and, for each $1 \le i \le k$, let

$$\mathfrak{p}_i\mathcal{O}_K = \mathfrak{P}_{i,1}^{e_{i,1}} \cdots \mathfrak{P}_{i,l_i}^{e_{i,l_i}},$$

with distinct prime ideals $\mathfrak{P}_{i,j}$ of $\mathcal{O}_K$, and $e_{i,j}$, $l_i \ge 1$. Then the $\mathfrak{P}_{i,j}$ are exactly the prime ideals of $\mathcal{O}_K$ dividing $\mathfrak{f}$, that is, the elements of $\mathcal{P}_{\mathfrak{f}}$.

Notice that, for every ideal $\mathfrak{a} \mid \mathfrak{P}_{i,1} \cdots \mathfrak{P}_{i,l_i}$ of $\mathcal{O}_K$, we have $\mathfrak{a}\cap\mathcal{O} = \mathfrak{p}_i$ if $\mathfrak{a} \ne \mathcal{O}_K$, and $\mathfrak{a} \cap \mathcal{O} = \mathcal{O}$ if $\mathfrak{a} = \mathcal{O}_K$, since $\mathcal{O}$ is one-dimensional. As all $\mathfrak{p}_i$, $\mathfrak{p}_j$, $i \ne j$, are relatively prime, we get

$$\sum_{\mathfrak{a}|\mathfrak{f}} \frac{\mu(\mathfrak{a})L_{\mathcal{O}}(\mathfrak{a})}{[\mathcal{O}:\mathfrak{a}\cap\mathcal{O}]} = \prod_{i=1}^{k} \sum_{\mathfrak{a}|\mathfrak{P}_{i,1}\cdots\mathfrak{P}_{i,l_i}} \frac{\mu(\mathfrak{a})L_{\mathcal{O}}(\mathfrak{a})}{[\mathcal{O}:\mathfrak{a}\cap\mathcal{O}]}$$

$$= \prod_{i=1}^{k}\left(1+\frac{L_{\mathcal{O}}(\mathfrak{P}_{i,1})}{[\mathcal{O}:\mathfrak{p}_i]}\sum_{\substack{J\subseteq\{1,\ldots,l_i\}\\ J\neq\emptyset}}(-1)^{|J|}\right) = \prod_{i=1}^{k}\left(1-\frac{L_{\mathcal{O}}(\mathfrak{P}_{i,1})}{[\mathcal{O}:\mathfrak{p}_i]}\right).$$

Thus, (15) is equivalent to

$$\prod_{i=1}^{k}\left(1-\frac{L_{\mathcal{O}}(\mathfrak{P}_{i,1})}{[\mathcal{O}:\mathfrak{p}_i]}\right) < [\mathcal{O}_K:\mathcal{O}]\prod_{i=1}^{k}\prod_{j=1}^{l_i}\left(1-\frac{L(\mathfrak{P}_{i,j})}{\mathfrak{N}\mathfrak{P}_{i,j}}\right).$$

Clearly, $\Pi := \prod_{i=1}^{k}\prod_{j=1}^{l_i}\mathfrak{P}_{i,j}^{e_{i,j}}$ divides the conductor $\mathfrak{f}$. Let us first assume that Π is a proper divisor of $\mathfrak{f}$. Then Lemma 8 (with strict inequality, since $\mathfrak{f}$ does not divide Π), (14), and the fact that $\mathfrak{N}\mathfrak{P}\geq 4$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ imply

$$[\mathcal{O}_K:\mathcal{O}]\prod_{i=1}^{k}\prod_{j=1}^{l_i}\left(1-\frac{L(\mathfrak{P}_{i,j})}{\mathfrak{N}\mathfrak{P}_{i,j}}\right) > \prod_{i=1}^{k}\frac{\mathfrak{N}\mathfrak{P}_{i,1}^{e_{i,1}}}{[\mathcal{O}:\mathfrak{p}_i]}\left(1-\frac{L(\mathfrak{P}_{i,1})}{\mathfrak{N}\mathfrak{P}_{i,1}}\right)\prod_{j=2}^{l_i}\frac{\mathfrak{N}\mathfrak{P}_{i,j}^{e_{i,j}}}{2}$$

$$\geq \prod_{i=1}^{k}\frac{\mathfrak{N}\mathfrak{P}_{i,1}}{[\mathcal{O}:\mathfrak{p}_i]}\left(1-\frac{L(\mathfrak{P}_{i,1})}{\mathfrak{N}\mathfrak{P}_{i,1}}\right)2^{l_i-1} \geq \prod_{i=1}^{k}\left(1-\frac{L_{\mathcal{O}}(\mathfrak{P}_{i,1})}{[\mathcal{O}:\mathfrak{p}_i]}\right).$$

For the last inequality, notice that either $\mathcal{O}_K/\mathfrak{P}_{i,1}\simeq\mathcal{O}/\mathfrak{p}_i$, and thus $L(\mathfrak{P}_{i,1}) = L_{\mathcal{O}}(\mathfrak{P}_{i,1})$, or

$$\frac{\mathfrak{N}\mathfrak{P}_{i,1}}{[\mathcal{O}:\mathfrak{p}_i]}\left(1-\frac{L(\mathfrak{P}_{i,1})}{\mathfrak{N}\mathfrak{P}_{i,1}}\right) > 2\cdot\frac{1}{2} = 1 \geq 1-\frac{L_{\mathcal{O}}(\mathfrak{P}_{i,1})}{[\mathcal{O}:\mathfrak{p}_i]}.$$

We are left with the case where $\Pi=\mathfrak{f}$. Then, for all $1\leq i\leq k$, we have

$$l_i > 1 \text{ or } e_{i,1} > 1 \text{ or } [\mathcal{O}_K/\mathfrak{P}_{i,1}:\mathcal{O}/\mathfrak{p}_i] > 1. \tag{16}$$

Indeed, suppose otherwise, that is $\mathfrak{p}_i\mathcal{O}_K=\mathfrak{P}_{i,1}$ and $\mathcal{O}_K/\mathfrak{P}_{i,1}\simeq\mathcal{O}/\mathfrak{p}_i$, for some i. We put $\tilde{\mathcal{O}} := (\mathcal{O}_K)_{\mathfrak{P}_{i,1}}$, the integral closure of the localisation $\mathcal{O}_{\mathfrak{p}_i}$, $\mathfrak{m} := \mathfrak{p}_i\mathcal{O}_{\mathfrak{p}_i}$, the maximal ideal of $\mathcal{O}_{\mathfrak{p}_i}$, and $\mathfrak{M} := \mathfrak{P}_{i,1}\tilde{\mathcal{O}}$, the maximal ideal of $\tilde{\mathcal{O}}$. Then

$$[\tilde{\mathcal{O}}:\mathcal{O}_{\mathfrak{p}_i}] = \frac{[\tilde{\mathcal{O}}:\mathfrak{M}][\mathfrak{M}:\mathfrak{m}]}{[\mathcal{O}_{\mathfrak{p}_i}:\mathfrak{m}]} = \frac{[\mathcal{O}_K:\mathfrak{P}_{i,1}][\mathfrak{M}:\mathfrak{m}]}{[\mathcal{O}:\mathfrak{p}_i]} = 1.$$

The second equality holds because $\mathcal{O}_K/\mathfrak{P}_{i,1}\simeq\tilde{\mathcal{O}}/\mathfrak{M}$, and $\mathcal{O}/\mathfrak{p}_i\simeq\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{m}$. The third equality holds because $\mathfrak{M}=\mathfrak{P}_{i,1}\tilde{\mathcal{O}}=\mathfrak{f}\tilde{\mathcal{O}}$, whence $\mathfrak{M}$ is clearly contained in the conductor of $\mathcal{O}_{p_i}$ in $\tilde{\mathcal{O}}$. (Here we used the hypothesis $\Pi=\mathfrak{f}$.) Therefore $\mathfrak{M}=\mathfrak{M}\cap\mathcal{O}_{\mathfrak{p}_i}=\mathfrak{m}$.

Therefore, $\mathcal{O}_{p_i}$ is a discrete valuation ring. According to [16, Theorem I.12.10], this is the case if and only if $\mathfrak{p}_i$ does not contain $\mathfrak{f}$. Since $\mathfrak{p}_i$ contains $\mathfrak{f}$, we have proved (16). (In [16, Section I.13], it is stated that (16) holds even without the requirement that $\Pi=\mathfrak{f}$, but no proof is given.)

With Lemma 8, (14), and the fact that $\mathfrak{N}\mathfrak{P} \geq 4$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$, we get

$$[\mathcal{O}_K : \mathcal{O}] \prod_{i=1}^{k} \prod_{j=1}^{l_i} \left(1 - \frac{L(\mathfrak{P}_{i,j})}{\mathfrak{N}\mathfrak{P}_{i,j}}\right) > \prod_{i=1}^{k} \frac{1}{[\mathcal{O} : \mathfrak{p}_i]} \prod_{j=1}^{l_i} \frac{\mathfrak{N}\mathfrak{P}_{i,j}^{e_{i,j}}}{2}$$
$$\geq \prod_{i=1}^{k} \frac{\mathfrak{N}\mathfrak{P}_{i,1}}{[\mathcal{O} : \mathfrak{p}_i]} \frac{\mathfrak{N}\mathfrak{P}_{i,1}^{e_{i,1}-1}}{2} 2^{l_i - 1} \geq \prod_{i=1}^{k} 2^{([\mathcal{O}_K/\mathfrak{P}_{i,1} : \mathcal{O}/\mathfrak{p}_i]-1)+(e_{i,1}-1)+(l_i-1)-1}.$$

To conclude our proof, we notice that the last expression is at least 1, by (16).

5. Proof of Theorem 1

We need to construct extensions of K where we have good control over the ring of integers. This is achieved by the following two lemmata.

Lemma 9 (([14, Lemma 1]))**.** *Let r be a positive integer, and $\beta \in \mathcal{O}_K$, such that $g = X^r - \beta \in \mathcal{O}_K[X]$ is irreducible. Let η be a root of g, $L = K(\eta)$, and $\mathfrak{D}_{L|K}$ the relative discriminant of $L|K$. For every prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ not dividing $\gcd(r, v_{\mathfrak{P}}(\beta))$, we have*

$$v_{\mathfrak{P}}(\mathfrak{D}_{L|K}) = r \cdot v_{\mathfrak{P}}(r) + r - \gcd(r, v_{\mathfrak{P}}(\beta)).$$

Lemma 10. *Let ω, $\eta \in \mathcal{O}_K$, such that $\omega^2 - 4\eta$ is squarefree and relatively prime to 2. Assume that the polynomial $h := X^2 - \omega X + \eta \in \mathcal{O}_K[X]$ is irreducible, and let α be a root of h. Then the ring of integers of $K(\alpha)$ is $\mathcal{O}_K[\alpha]$, and the relative discriminant $\mathfrak{D}_{K(\alpha)|K}$ of $K(\alpha)$ over K is the principal ideal $(\omega^2 - 4\eta)$.*

Proof. The discriminant of α over K is

$$d(\alpha) = \det \begin{pmatrix} 1 & (\omega + \sqrt{\omega^2 - 4\eta})/2 \\ 1 & (\omega - \sqrt{\omega^2 - 4\eta})/2 \end{pmatrix}^2 = \omega^2 - 4\eta.$$

Let, say, $(\omega^2 - 4\eta) = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, with an integer $s \geq 0$ and distinct prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_K$ not containing 2. Then the relative discriminant $\mathfrak{D}_{K(\alpha)|K}$ divides $\mathfrak{P}_1 \cdots \mathfrak{P}_s$.

Since $K(\alpha) = K(\sqrt{\omega^2 - 4\eta})$, Lemma 9 implies that $v_{\mathfrak{P}_i}(\mathfrak{D}_{K(\alpha)|K}) = 1$, for all $1 \leq i \leq s$, whence the relative discriminant $\mathfrak{D}_{K(\alpha)|K}$ is the principal ideal $(\omega^2 - 4\eta) = (d(\alpha))$. This is enough to prove that the ring of integers of $K(\alpha)$ is $\mathcal{O}_K[\alpha]$ (see, for example, [20, Chapter V, Theorem 30]). □

We may assume that K satisfies the hypotheses of Proposition 4, since it is enough to prove the theorem for the number field $K(\sqrt{5}) \supseteq \mathbb{Q}(\sqrt{5})$.

We may also assume that the field K is generated by a unit of $\mathcal{O}_K$. If not, say $K = \mathbb{Q}(\beta)$, where $\beta \in \mathcal{O}_K$. Let α be a root of the polynomial $X^2 - \beta X + 1 \in \mathcal{O}_K[X]$. Then $\mathbb{Q}(\alpha) \supseteq K$, whence it is enough to prove the theorem for $\mathbb{Q}(\alpha)$, and α is a unit of the ring of integers of $\mathbb{Q}(\alpha)$.

Therefore, the ring generated by the units of $\mathcal{O}_K$ is an order. Let us call that order $\mathcal{O}^U$. If $\mathcal{O}^U = \mathcal{O}_K$ then there is nothing to prove, so assume from now on that $\mathcal{O}^U \neq \mathcal{O}_K$.

Choose a unit $\eta \in \mathcal{O}_K^* \setminus K^2$. We use Proposition 4 to obtain elements $\omega_1, \ldots,$ $\omega_r \in \mathcal{O}_K$ with

$$\mathcal{O}_K = \mathcal{O}^U[\omega_1, \ldots, \omega_r], \tag{17}$$

such that

(18) all $\omega_i^2 - 4\eta$ are squarefree and relatively prime to 2 and each other.

Start with

$$\mathcal{P} := \operatorname{supp}(2), \quad \mathcal{O} := \mathcal{O}^U,$$

and choose an element ω_1 as in Proposition 4. Then $\mathcal{O}^U[\omega_1]$ is an order larger than $\mathcal{O}^U$, whence

$$[\mathcal{O}_K : \mathcal{O}^U[\omega_1]] = \frac{[\mathcal{O}_K : \mathcal{O}^U]}{[\mathcal{O}^U[\omega_1] : \mathcal{O}^U]} \leq \frac{[\mathcal{O}_K : \mathcal{O}^U]}{2}.$$

Assume now that $\omega_1, \ldots, \omega_{i-1}$ have been chosen. If $\mathcal{O}^U[\omega_1, \ldots, \omega_{i-1}] = \mathcal{O}_K$ then stop, otherwise put

$$\mathcal{P} := \operatorname{supp}(2) \cup \bigcup_{j=1}^{i-1} \operatorname{supp}(\omega_j^2 - 4\eta), \quad \mathcal{O} := \mathcal{O}^U[\omega_1, \ldots, \omega_{i-1}].$$

Let ω_i be an element as in Proposition 4. Then

$$[\mathcal{O}_K : \mathcal{O}^U[\omega_1, \ldots, \omega_i]] \leq [\mathcal{O}_K : \mathcal{O}^U[\omega_1, \ldots, \omega_{i-1}]]/2 \leq [\mathcal{O}_K : \mathcal{O}^U]/2^i.$$

Therefore, the above process stops after $r \leq \log_2([\mathcal{O}_K : \mathcal{O}^U])$ steps, with elements $\omega_1, \ldots, \omega_r \in \mathcal{O}_K \smallsetminus \mathcal{O}^U$, such that $\mathcal{O}_K = \mathcal{O}^U[\omega_1, \ldots, \omega_r]$. Conditions (18) hold by our construction.

For $1 \leq i \leq r$, let α_i be a root of the polynomial $X^2 - \omega_i X + \eta \in \mathcal{O}_K[X]$. Then α_i is a unit in the ring of integers of $K(\alpha_i)$. Moreover, $\alpha_i \notin K$, since otherwise $\alpha_i \in \mathcal{O}_K^*$, and $\omega_i = \alpha_i + \eta\alpha_i^{-1} \in \mathcal{O}^U$, a contradiction. By Lemma 10, the ring of integers of $K(\alpha_i)$ is $\mathcal{O}_K[\alpha_i]$, and the relative discriminant $\mathfrak{D}_{K(\alpha_i)|K}$ of $K(\alpha_i)$ over K is the principal ideal $(\omega_i^2 - 4\eta)$.

We use the following well-known fact (for a proof, see [16, Theorem I.2.11]):

Lemma 11. *Let $L|K$ and $L'|K$ be two Galois extensions of K such that*

(1) $L \cap L' = K$,
(2) L has a relative integral basis $\{\beta_1, \ldots, \beta_l\}$ over K,
(3) L' has a relative integral basis $\{\beta'_1, \ldots, \beta'_{l'}\}$ over K, and
(4) the relative discriminants $\mathfrak{D}_{L|K}$ and $\mathfrak{D}_{L'|K}$ are relatively prime.

Then the compositum LL' has a relative integral basis over K consisting of all products $\beta_i\beta'_j$, and the relative discriminant of $LL'|K$ is

$$\mathfrak{D}_{LL'|K} = \mathfrak{D}_{L|K}^{[L':K]}\mathfrak{D}_{L'|K}^{[L:K]}.$$

Consider the extension fields $L_i := K(\alpha_1, \ldots, \alpha_i)$ of K. We claim that L_i has an integral basis over K consisting of (not necessarily all) products of the form

$$\prod_{j \in J} \alpha_j, \quad \text{for } J \subseteq \{1, \ldots, i\},$$

and that the relative discriminant $\mathfrak{D}_{L_i|K}$ is relatively prime to all relative discriminants $\mathfrak{D}_{K(\alpha_j)|K}$, for $i < j \leq r$.

With (18), this claim clearly holds for $L_1 = K(\alpha_1)$. If the claim holds for L_{i-1}, and $\alpha_i \in L_{i-1}$, then it holds for $L_i = L_{i-1}$ as well. If $K(\alpha_i) \not\subseteq L_{i-1}$ then the extensions $L_{i-1}|K$ and $K(\alpha_i)|K$ satisfy all requirements of Lemma 11, whence the claim holds as well for $L_i = L_{i-1}K(\alpha_i)$.

Now put $L := L_r$. Then the ring of integers of L is $\mathcal{O}_L = \mathcal{O}_K[\alpha_1, \ldots, \alpha_r]$. With (17) and $\omega_i = \alpha_i + \eta\alpha_i^{-1}$, we get

$$\mathcal{O}_L = \mathcal{O}^U[\omega_1, \ldots, \omega_r, \alpha_1, \ldots, \alpha_r] = \mathcal{O}^U[\alpha_1, \alpha_1^{-1}, \ldots, \alpha_r, \alpha_r^{-1}],$$

and the latter ring is generated by units of $\mathcal{O}_L$.

Acknowledgements. I would like to thank Martin Widmer for many helpful comments and discussions, in particular about Lemma 7 and the linear transformation T that occurs there. The idea of using such transformations stems from an upcoming paper by Widmer.

References

[1] N. Ashrafi and P. Vámos. On the unit sum number of some rings. *Q. J. Math.*, 56(1):1–12, 2005.

[2] P. Belcher. Integers expressible as sums of distinct units. *Bull. Lond. Math. Soc.*, 6:66–68, 1974.

[3] P. Belcher. A test for integers being sums of distinct units applied to cubic fields. *J. Lond. Math. Soc. (2)*, 12(2):141–148, 1975/76.

[4] D. A. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[5] A. Filipin, R. F. Tichy, and V. Ziegler. The additive unit structure of pure quartic complex fields. *Funct. Approx. Comment. Math.*, 39(1):113–131, 2008.

[6] A. Filipin, R. F. Tichy, and V. Ziegler. On the quantitative unit sum number problem—an application of the subspace theorem. *Acta Arith.*, 133(4):297–308, 2008.

[7] C. Frei. Sums of units in function fields. *Monatsh. Math.*, DOI: 10.1007/s00605-010-0219-7.

[8] C. Frei. Sums of units in function fields II - The extension problem. *accepted by Acta Arith.*

[9] C. Fuchs, R. F. Tichy, and V. Ziegler. On quantitative aspects of the unit sum number problem. *Arch. Math.*, 93:259–268, 2009.

[10] L. Hajdu. Arithmetic progressions in linear combinations of S-units. *Period. Math. Hung.*, 54(2):175–181, 2007.

[11] J. G. Hinz. Potenzfreie Werte von Polynomen in algebraischen Zahlkörpern. *J. Reine Angew. Math.*, 332:134–150, 1982.

[12] B. Jacobson. Sums of distinct divisors and sums of distinct units. *Proc. Am. Math. Soc.*, 15:179–183, 1964.

[13] M. Jarden and W. Narkiewicz. On sums of units. *Monatsh. Math.*, 150(4):327–332, 2007.

[14] P. Llorente, E. Nart, and N. Vila. Discriminants of number fields defined by trinomials. *Acta Arith.*, 43(4):367–373, 1984.

[15] D. Masser and J. D. Vaaler. Counting algebraic numbers with large height. II. *Trans. Amer. Math. Soc.*, 359(1):427–445, 2006.

[16] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[17] J. Śliwa. Sums of distinct units. *Bull. Acad. Pol. Sci.*, 22:11–13, 1974.

[18] R. F. Tichy and V. Ziegler. Units generating the ring of integers of complex cubic fields. *Colloq. Math.*, 109(1):71–83, 2007.

[19] M. Widmer. Counting primitive points of bounded height. *Trans. Amer. Math. Soc.*, 362:4793–4829, 2010.

[20] O. Zariski and P. Samuel. *Commutative algebra. Vol. 1.* Graduate Texts in Mathematics, No. 28. Springer-Verlag, New York, 1975.

[21] V. Ziegler. The additive unit structure of complex biquadratic fields. *Glas. Mat.*, 43(63)(2):293–307, 2008.

E-mail address: `frei@math.tugraz.at`

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria