Dipl.-Ing. Christopher FREI

Sums of units in number fields and function fields

DISSERTATION

zur Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften

Doktoratsstudium der Technischen Wissenschaften im Rahmen der Doktoratsschule „Mathematik und Wissenschaftliches Rechnen“

TU Graz
Graz University of Technology

Technische Universität Graz

Betreuer:
Univ.-Prof. Dr.phil. Robert F. TICHY

Institut für Analysis und Computational Number Theory
(Math A)

Graz, im Juli 2011

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Graz, am ....

(Unterschrift)

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitely marked all material which has been quotes either literally or by content from the used sources.

....

date (signature)

Danksagung

Ich danke meinem Betreuer Prof. Robert F. Tichy, der es mir ermöglicht hat, in diesem interessanten und spannenden Teilgebiet der Mathematik zu arbeiten, und der mir immer mit gutem Rat zur Seite gestanden ist, sowie allen Kolleginnen und Kollegen an den mathematischen Instituten der TU Graz, für ein freundliches, entspanntes und anregendes Arbeitsklima.

Besonderer Dank geht an Jochen Resch, der für sämtliche Computerprobleme eine Lösung hat, Martin Widmer und Christian Elsholtz, von deren Erfahrung ich in vielen mathematischen Gesprächen profitieren konnte, Hermine Panzenböck und Irene Wilfinger, die bei organisatorischen Problemen immer unkompliziert geholfen haben, sowie an alle Mitglieder der kunst/gruppe olga, die immer für unterhaltsame Kaffeepausen gesorgt haben.

Vor allem danke ich meiner Familie und meinen Freunden, insbesondere meiner Mutter Margit Frei, die mich immer bei meinen Entscheidungen unterstützt und mir ein sehr schönes Leben hier in Graz ermöglicht haben.

Vorwort

Es ist unmittelbar ersichtlich, dass sich jedes Element n des Rings $\mathbb{Z}$ der ganzen Zahlen als Summe von $|n|$ Einheiten des Rings (das sind die invertierbaren Elemente, im Fall von $\mathbb{Z}$ also die Elemente ± 1) schreiben lässt (die leere Summe wollen wir wie allgemein üblich als 0 annehmen). Dies soll als erstes triviales Beispiel für jene Eigenschaften dienen, die im Rahmen dieser Dissertation untersucht werden.

Für einen Ring R (mit Einselement) lässt sich die natürliche Frage stellen, ob und wie R von seinen Einheiten additiv erzeugt ist. Konkret beinhaltet dies die folgenden Fragen:

Ist jedes Element von R als Summe von Einheiten darstellbar? Falls ja, gibt es für jedes Element Darstellungen mit einer fixen oder beschränkten Anzahl an Summanden? Falls nein, besitzt R zumindest eine „natürliche“ Erweiterung S, sodass jedes Element von S als Summe von Einheiten darstellbar ist? Mühelos lässt sich erkennen, dass genau dann jedes Element von R als Summe von Einheiten darstellbar ist, wenn R als Ring von seinen Einheiten erzeugt ist.

Die im Rahmen dieser Arbeit untersuchten Ringe sind jene, die in der Zahlentheorie an vordergründiger Stelle auftreten, nämlich Ganzheitsringe in algebraischen Zahlkörpern, sowie deren analoge Konstrukte, S-Ganzheitsringe in algebraischen Funktionenkörpern einer Unbestimmten.

Die Arbeit besteht aus vier Artikeln, von denen zwei bereits von Fachzeitschriften zur Publikation angenommen wurden und zwei sich unter Begutachtung befinden.

Der erste Artikel gibt eine Übersicht über zahlreiche Resultate zum Thema der Einheitensummen und kann daher als Einleitung verstanden werden.

Im zweiten Artikel werden zwei grundlegende Resultate über Einheitensummen in Ganzheitsringen algebraischer Zahlkörper auf den Funktionenkörperfall übertragen.

Der dritte Artikel behandelt und löst ein offenes Problem, das von Jarden und Narkiewicz für algebraische Zahlkörper formuliert wurde, im Funktionenkörperfall.

Der vierte Artikel enthält schließlich das Hauptresultat der Dissertation, die vollständige Lösung des Problems von Jarden und Narkiewicz im ursprünglichen Zahlkörperfall.

Es folgen kurze Beschreibungen der vier Artikel, die in ihrer Gesamtheit diese Dissertation ausmachen.

Additive unit representations in global fields - A survey

Dieser Artikel entstand in Zusammenarbeit mit Fabrizio Barroero, zur Zeit Dissertant in Graz, und Prof. Robert F. Tichy, unserem gemeinsamen Betreuer. Es handelt sich um den jüngsten der vier in dieser Dissertation zusammengefassten Artikel, der eine Übersicht über zentrale Fragestellungen und Resultate aus dem Umfeld der Einheitensummen bietet. Besonderes Augenmerk gilt Ganzheitsringen in algebraischen Zahlkörpern und Funktionenkörpern, sowie Matrizenringen.

Aufgrund seines Übersichtscharakters dient der Artikel vor allem als Einleitung der Dissertation, er enthält jedoch auch neue Resultate. Zur Zeit befindet er sich in Begutachtung bei einer Fachzeitschrift.

Sums of units in function fields

Jarden und Narkiewicz zeigten im Jahr 2007, dass es im Ganzheitsring jedes algebraischen Zahlkörpers, für jede natürliche Zahl n, Elemente gibt, die sich nicht als Summen von höchstens n Einheiten schreiben lassen. Im ersten Teil des Artikels wird ein analoges Resultat für S-Ganzheitsringe algebraischer Funktionenkörper einer Unbestimmten über perfekten Grundkörpern bewiesen. Die hierbei zentral verwendeten Hilfsmittel sind Resultate von Mason über S-Einheitengleichungen in Funktionenkörpern.

Das zweite Hauptresultat des Artikels ist eine Klassifikation jener quadratischen Funktionenkörper, deren Ganzheitsringe von ihren Einheiten erzeugt werden. Die analoge Version für Zahlkörper wurde erstmals 1974 von Belcher gezeigt.

Der Artikel wurde von den Monatsheften für Mathematik zur Publikation angenommen und ist bereits als Onlineversion erschienen.

Sums of units in function fields II - The extension problem

Motiviert durch die Situation im Fall quadratischer Zahlkörper, in dem sich relativ einfach eine positive Antwort zeigen lässt, stellten Jarden und Narkiewicz die folgende Frage: Besitzt jeder Zahlkörper eine endliche Erweiterung L, sodass der Ganzheitsring von L von seinen Einheiten erzeugt ist?

Das Hauptresultat dieses Artikels ist die positive Beantwortung der analogen Frage im Fall von S-Ganzheitsringen in algebraischen Funktionenkörpern einer Unbestimmten über perfekten Grundkörpern.

Zur Verwendung kommen klassische Methoden der algebraischen Zahlentheorie, die jedoch in dieser Form erstmals auf Probleme im Bereich der Einheitensummen angewandt werden.

Der Artikel wurde von Acta Arithmetica zur Publikation angenommen.

On rings of integers generated by their units

In diesem Artikel wird der Ansatz aus „Sums of units in function fields II - The extension problem“ modifiziert und erweitert, um schließlich die ursprüngliche Frage von Jarden und Narkiewicz im Zahlkörperfall zu beantworten.

Zur erfolgreichen Übertragung der Methode auf den Zahlkörperfall werden neue, weniger direkte Argumente benötigt. Der Beweis einer Existenzaussage gelingt mit Hilfe eines asymptotischen Abzähltheorems.

Dieses Abzähltheorem ist eine Verallgemeinerung eines Resultats von Hinz, durch das potenzfreie Werte von Polynomen in Ganzheitsringen algebraischer Zahlkörper gezählt werden.

Der Artikel befindet sich zur Zeit unter Begutachtung bei einer Fachzeitschrift.

Preface

Clearly, every element n of the ring $\mathbb{Z}$ of rational integers can be written as a sum of $|n|$ units of the ring (units are invertible elements, in the case of $\mathbb{Z}$ those are the elements ± 1; we assume, as usual, that the empty sum equals 0). This shall serve as a first example of the properties which are investigated in this thesis.

Given a ring R (with unity), it is a natural problem to investigate whether and how R is additively generated by its units. Concretely, this includes the following questions:

Is every element of R representable as a sum of units? If yes, are there, for each element, representations with a fixed or bounded number of summands? If not, does R have at least a "natural" extension S such that every element of S can be represented as a sum of units? Obviously, every element of R is representable as a sum of units if and only if R is generated by its units as a ring.

The rings investigated in this thesis are the ones occurring most notably in number theory, namely, rings of integers in algebraic number fields and their analogues, rings of S-integers in algebraic function fields of one variable.

The thesis consists of four articles, two of which have been accepted for publication by journals, and two are under review.

The first article provides an overview on various results in the area of sums of units and thus can be understood as an introduction.

In the second article, two fundamental results on sums of units in rings of integers of algebraic number fields are transferred to the function field case.

The third article considers and solves the function field version of an open problem which was raised by Jarden and Narkiewicz in the number field case.

Finally, the fourth article contains the main result of this thesis, the complete solution of the problem by Jarden and Narkiewicz in its original number field version.

Let us continue with short descriptions of the four articles constituting the thesis.

Additive unit representations in global fields - A survey

This article is joint work with Fabrizio Barroero, currently a doctoral student in Graz, and our adviser Prof. Robert F. Tichy. It is the latest of the four articles forming this thesis and offers an overview on central topics and results in the area of sums of units. Special attention is paid to rings of integers in algebraic number fields and function fields on the one hand, and matrix rings on the other hand.

Being a survey, this article serves primarily as an introduction to this thesis, but it contains some new results as well. As of now, the article is under review by a journal.

Sums of units in function fields

Jarden and Narkiewicz proved in 2007 that in the ring of integers of every algebraic number field, for every positive integer n, there are elements that can not be written as sums of at most n units. The first part of this article is devoted to the development of an analogous result for rings of S-integers in algebraic function fields of one variable over perfect base fields. The central tools used in this part of the article are results by Mason on S-unit equations over function fields.

The second main result of the article is a classification of those quadratic function fields whose rings of integers are generated by their units. The analogous version for number fields was introduced by Belcher in 1974.

The article has been accepted for publication by Monatshefte für Mathematik and has already appeared online.

Sums of units in function fields II - The extension problem

Motivated by the situation in the case of quadratic number fields, where a positive answer is relatively easy to find, Jarden and Narkiewicz raised the following question: Does every number field have a finite extension L such that the ring of integers of L is generated by its units?

The main result of this article is an affirmative answer to the analogous question for rings of S-integers in algebraic function fields of one variable over perfect base fields.

The proofs use classical methods from algebraic number theory, which are in this form applied for the first time to problems in the area of sums of units.

The article has been accepted for publication by Acta Arithmetica.

On rings of integers generated by their units

In this article, the approach from “Sums of units in function fields II - The extension problem” is modified and extended to answer the original question by Jarden and Narkiewicz in the number field case.

For successfully transferring the method to number fields, new, less direct, arguments are needed. An existence statement is established with the help of an asymptotic counting theorem.

This counting theorem is a generalisation of a result by Hinz, counting power-free values of polynomials in rings of integers of algebraic number fields.

Currently, the article is under review by a journal.

Contents

Additive unit representations in global fields - A survey 17

Sums of units in function fields 35

Sums of units in function fields II - The extension problem 55

On rings of integers generated by their units 67

Curriculum Vitae 91

Additive unit representations in global fields - A survey

Fabrizio Barroero, Christopher Frei and Robert F. Tichy

Dedicated to Kálmán Győry, Attila Pethő, János Pintz and András Sarközy.

Abstract

We give an overview on recent results concerning additive unit representations. Furthermore the solutions of some open questions are included. The central problem is whether and how certain rings are (additively) generated by their units. This has been investigated for several types of rings related to global fields, most importantly rings of algebraic integers. We also state some open problems and conjectures which we consider to be important in this field.

1 The unit sum number

In 1954, Zelinsky [37] proved that every endomorphism of a vector space V over a division ring D is a sum of two automorphisms, except if $D = \mathbb{Z}/2\mathbb{Z}$ and $\dim V = 1$. This was motivated by investigations of Dieudonné on Galois theory of simple and semisimple rings [6] and was probably the first result about the additive unit structure of a ring.

Using the terminology of Vámos [34], we say that an element r of a ring R (with unity 1) is *k-good* if r is a sum of exactly k units of R. If every element of R has this property then we call R *k-good.* By Zelinsky's result, the endomorphism ring of a vector space with more than two elements is 2-good. Clearly, if R is k-good then it is also l-good for every integer $l > k$. Indeed, we can write any element of R as

$$r = (r - (l - k) \cdot 1) + (l - k) \cdot 1,$$

2010 *Mathematics Subject Classification*: 00-02; 11R27; 16U60

Key words and phrases: global fields, sums of units, unit sum number, additive unit representations

and expressing $r - (l - k) \cdot 1$ as a sum of k units gives a representation of r as a sum of l units.

Goldsmith, Pabst and Scott [17] defined the *unit sum number* $u(R)$ of a ring R to be the minimal integer k such that R is k-good, if such an integer exists. If R is not k-good for any k then we put $u(R) := \omega$ if every element of R is a sum of units, and $u(R) := \infty$ if not. We use the convention $k < \omega < \infty$ for all integers k.

Clearly, $u(R) \leq \omega$ if and only if R is generated by its units. Here are some easy examples from [17]:

- $u(\mathbb{Z}) = \omega$,
- $u(K[X]) = \infty$, for any field K,
- $u(K) = 2$, for any field K with more than 2 elements, and
- $u(\mathbb{Z}/2\mathbb{Z}) = \omega$.

Goldsmith, Pabst and Scott [17] were mainly interested in endomorphism rings of modules. For example, they proved independently from Zelinsky that the endomorphism ring of a vector space with more than two elements has unit sum number 2, though they mentioned that this result can hardly be new.

Henriksen [21] proved that the ring $M_n(R)$ of $n \times n$-matrices ($n \geq 2$) over any ring R is 3-good.

Herwig and Ziegler [22] proved that for every integer $n \geq 2$ there exists a factorial domain R such that every element of R is a sum of at most n units, but there is an element of R that is no sum of $n - 1$ units.

The introductory section of [34] contains a historical overview of the subject with some references. We also mention the survey article [31] by Srivastava.

In the following sections, we are going to focus on rings of ($S-$)integers in global fields.

2 Rings of integers

The central result regarding rings of integers in number fields, or more generally, rings of S-integers in global fields ($S \neq \emptyset$ finite), is that they are not k-good for any k, thus their unit sum number is ω or ∞. This was first proved by Ashrafi and Vámos [2] for rings of integers of quadratic and complex cubic number fields, and of cyclotomic number fields generated by a primitive 2^n-th root of unity. They conjectured, however, that it holds true for the rings of integers of all algebraic number fields (finite extensions of $\mathbb{Q}$). The proof of an even stronger version of this was given by Jarden and Narkiewicz [24] for a much more general class of rings:

Theorem 1. *[24, Theorem 1] 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.*

In particular, we have $u(R) \geq \omega$, for any ring R of integers of an algebraic number field.

This theorem is an immediate consequence of the following lemma, which Jarden and Narkiewicz proved by means of Evertse and Győry's [10] bound on the number of solutions of S-unit equations combined with van der Waerden's theorem [36] on arithmetic progressions.

Lemma 2. *[24, Lemma 4] If R is a finitely generated integral domain of zero characteristic and $n \geq 1$ is an integer then there exists a constant $A_n(R)$ such that every arithmetic progression in R having more than $A_n(R)$ elements contains an element which is not a sum of n units.*

Lemma 2 is a special case of a theorem independently found by Hajdu [20]. Hajdu's result provides a bound for the length of arithmetic progressions in linear combinations of elements from a finitely generated multiplicative subgroup of a field of zero characteristic. Here the linear combinations are of fixed length and only a given finite set of coefficient-tuples is allowed. Hajdu used his result to negatively answer the following question by Pohst: Is it true that every prime can be written in the form $2^u \pm 3^v$, with non-negative integers u, v?

Using results by Mason [27, 28] on S-unit equations in function fields, Frei [14] proved the function field analogue of Theorem 1. It holds in zero characteristic as well as in positive characteristic.

Theorem 3. *Let R be the ring of S-integers of an algebraic function field in one variable over a perfect field, where $S \neq \emptyset$ is a finite set of places. Then, for each positive integer n, there exists an element of R that can not be written as a sum of at most n units of R. In particular, we have $u(R) \geq \omega$.*

We will later discuss criteria which show that in the number field case as well as in the function field case, both possibilities $u(R) = \omega$ and $u(R) = \infty$ occur.

3 The qualitative problem

Problem A. *[24, Problem A] Give a criterion for an algebraic extension K of the rationals to have the property that its ring of integers R has unit sum number $u(R) \leq \omega$.*

Jarden and Narkiewicz provided some easy examples of infinite extensions of $\mathbb{Q}$ with $u(R) \leq \omega$: By the Kronecker-Weber theorem, the maximal Abelian extension of $\mathbb{Q}$ has this property. Further examples are the fields of all algebraic numbers and all real algebraic numbers.

More criteria are known for algebraic number fields of small degree. Here, the only possibilities for $u(R)$ are ω and ∞, by Theorem 1. For quadratic number fields, Belcher [3], and later Ashrafi and Vámos [2], proved the following result:

Theorem 4. *[3, Lemma 1][2, Theorems 7, 8] Let $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, be a quadratic number field with ring of integers R. Then $u(R) = \omega$ if and only if*

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.

A similar result for purely cubic fields was found by Tichy and Ziegler [33].

Theorem 5. *[33, Theorem 2] Let d be a cubefree integer and R the ring of integers of the purely cubic field $\mathbb{Q}(\sqrt[3]{d})$. Then $u(R) = \omega$ if and only if*

1. d is squarefree, $d \not\equiv \pm 1 \mod 9$, and $d+1$ or $d-1$ is a perfect cube, or

2. $d = 28$.

Filipin, Tichy and Ziegler used similar methods to handle purely quartic complex fields $\mathbb{Q}(\sqrt[4]{d})$. Their criterion [11, Theorem 1.1] states that $u(R) = \omega$ if and only if d is contained in one of six explicitly given sets.

As a first guess, one could hope to get information about the unit sum number of the ring of integers of a number field K by comparing the regulator and the discriminant of K. In personal communication with the authors, Martin Widmer pointed out the following sufficient criterion for the simple case of complex cubic fields:

Proposition 6. *(Widmer) If R is the ring of integers of a complex cubic number field K then $u(R) = \omega$ whenever the inequality*

$$|\Delta_K| > (e^{\frac{3}{4}R_K} + e^{-\frac{3}{4}R_K})^4 \tag{1}$$

holds. Here, Δ_K is the discriminant and R_K is the regulator of K.

Proof. Regard K as a subfield of the reals, and let $\eta > 1$ be a fundamental unit, so $R_K = \log \eta$. Since K contains no roots of unity except ± 1, the ring of integers R is generated by its units if and only if $R = \mathbb{Z}[\eta]$. By the standard embedding $K \to \mathbb{R} \times \mathbb{C} \simeq \mathbb{R}^3$, we can regard R and $\mathbb{Z}[\eta]$ as lattices in $\mathbb{R}^3$ and compare their determinants. Let $\eta' = x + iy$ be one of the non-real conjugates of η. We get $u(R) = \omega$ if and only if

$$2^{-1}\sqrt{|\Delta_K|} = \left| \det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix} \right|.$$

Since the right-hand side of the above equality is always a multiple of the left-hand side, we have $u(R) = \omega$ if and only if

$$\sqrt{|\Delta_K|} > \left| \det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix} \right|.$$

Clearly, $\eta^{-1} = \eta'\overline{\eta'} = x^2 + y^2$, whence $|x|$, $|y| \leq \eta^{-1/2}$. With this in mind, a simple computation shows that the right-hand side of the above inequality is at most $\eta^{-3/2} + 2 + \eta^{3/2}$, so (1) implies that $u(R) = \omega$. □

To see that condition (1) is satisfied in infinitely many cases, we consider the complex cubic fields $K_N = \mathbb{Q}(\alpha_N)$, where α_N is a root of the polynomial

$$f_N = X^3 + NX + 1, \tag{2}$$

with a positive integer N such that $4N^3 + 27$ is squarefree. By [7], infinitely many such N exist. We may assume that $\alpha_N \in \mathbb{R}$. From (2), we get

$$\frac{N^2}{N^3 + 1} < -\alpha_N = \frac{1}{\alpha_N^2 + N} < 1/N.$$

Since $-1/\alpha_N$ is a unit of the ring of integers of K_N, and $N < -1/\alpha_N < N + 1/N^2$, we have $R_K \leq \log(N + 1/N^2)$. The discriminant $-4N^3 - 27$ of f_N is squarefree by hypothesis, so $|\Delta_K| = 4N^3 + 27$. Now we see by a simple computation that (1) holds.

In the function field case, Frei [14] investigated quadratic extensions of rational global function fields.

Theorem 7. *[14, Theorem 2] Let K be a finite field, and F a quadratic extension field of the rational function field $K(x)$ over K. Denote the integral closure of $K[x]$ in F by R. Then the following two statements are equivalent.*

1. *$u(R) = \omega$*

2. *The function field $F|K$ has full constant field K and genus 0, and the infinite place of $K(x)$ splits into two places of $F|K$.*

This criterion can also be phrased in terms of an element generating F over $K(x)$. If, for example, K is the full constant field of F and of odd characteristic then we can write $F = K(x, y)$, where $y^2 = f(x)$ for some separable polynomial $f \in K[x] \setminus K$. Then we get $u(R) = \omega$ if and only if f is of degree 2 and its leading coefficient is a square in K ([14, Corollary 1]).

Theorem 7 holds in fact for arbitrary perfect base fields K. An alternative proof given at the end of [14] implies the following stronger version:

Theorem 8. *Let $F|K$ be an algebraic function field in one variable over a perfect field K. Let S be a set of two places of $F|K$ of degree one, and denote by R the ring of S-integers of $F|K$. Then $u(R) = \omega$ if and only if $F|K$ is rational.*

All of the rings R investigated above have in common that their unit groups are of rank at most one. Currently, there are no known nontrivial criteria for families of number fields (or function fields) whose rings of integers have unit groups of higher rank. We consider it an important direction to find such criteria.

Pethő and Ziegler investigated a modified version of Problem A, where one asks whether a ring of integers has a power basis consisting of units [39, 29]. For example, Ziegler proved the following:

Theorem 9. *[39, Theorem 1] Let $m > 1$ be an integer which is not a square. Then the order $\mathbb{Z}[\sqrt[4]{m}]$ admits a power basis consisting of units if and only if $m = a^4 \pm 1$, for some integer a.*

Since analogous results are already known for negative m [40] and for the rings $\mathbb{Z}[\sqrt[d]{m}]$, $d < 4$ [3, 33], Theorem 9 motivates the following conjecture:

Conjecture. *[39, Conjecture 1] Let $d \geq 2$ be an integer and $m \in \mathbb{Z} \setminus \{0\}$, and assume that $\sqrt[d]{m}$ is an algebraic number of degree d. Then $\mathbb{Z}[\sqrt[d]{m}]$ admits a power basis consisting of units if and only if $m = a^d \pm 1$, for some integer a.*

For rings R with $u(R) = \omega$, Ashrafi [1] investigated the stronger property that every element of R can be written as a sum of k units for all sufficiently large integers k. Ashrafi proved that this is the case if and only if R does not have $\mathbb{Z}/2\mathbb{Z}$ as a factor, and applied this result to rings of integers of quadratic and complex cubic number fields.

Let R be an order in a quadratic number field. Ziegler [38] found various results about representations of elements of R as sums of S-units in R, where S is a finite set of places containing all Archimedean places.

Another variant of Problem A asks for representations of algebraic integers as sums of distinct units. Jacobson [23] proved that in the rings of integers of the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, every element is a sum of distinct units. His conjecture that these are the only quadratic number fields with that property was proved by Śliwa [30]. Belcher [3, 4] investigated cubic and quartic number fields. A recent article by Thuswaldner and Ziegler [32] puts these results into a more general framework: they apply methods from the theory of arithmetic dynamical systems to additive unit representations.

4 The extension problem

Problem B. *[24, Problem 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?*

If K is an Abelian number field, that is, $K|\mathbb{Q}$ is a Galois extension with Abelian Galois group, then we know by the Kronecker-Weber theorem that K is contained in a cyclotomic number field $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$, which is obviously generated by its units. Problem B was completely solved by Frei [13]:

Theorem 10. *[13, Theorem 1] For any number field K, there exists a number field L containing K, such that the ring of integers of L is generated by its units.*

The proof relies on finding elements of the ring of integers of K with certain properties via asymptotic counting arguments, and then using these properties to generate easily manageable quadratic extensions of K in which those elements are sums of units of the respective rings of integers. The field L is then taken as the compositum of all these quadratic extensions.

Prior to this, with an easier but conceptually similar argument, Frei [15] answered the function field version of Problem B:

Theorem 11. *[15, Theorem 2] Let $F|K$ be an algebraic function field over a perfect field K, and R the ring of S-integers of F, for some finite set $S \neq \emptyset$*

of places. Then there exists a finite extension field F' of F such that the integral closure of R in F' is generated by its units.

5 The quantitative problem

Problem C. *[24, Problem C] Let K be an algebraic number field. Obtain an asymptotic 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.*

As Jarden and Narkiewicz noticed, Lemma 2 and Szemerédi's theorem (see [19]) imply that

$$\lim_{x\to\infty} \frac{N_k(x)}{x} = 0,$$

for any fixed k.

A similar question has been investigated by Filipin, Fuchs, Tichy, and Ziegler [11, 12, 16]. We state here the most general result [16]. Let R be the ring of S-integers of a number field K, where S is a finite set of places containing all Archimedean places. Two S-integers α, β are *associated*, if there exists a unit ε of R such that $\alpha = \beta\varepsilon$. For any $\alpha \in R$, we write

$$N(\alpha) := \prod_{\nu\in S} |\alpha|_\nu.$$

Fuchs, Tichy and Ziegler investigated the counting function $u_{K,S}(n, x)$, which denotes the number of all classes $[\alpha]$ of associated elements α of R with $N(\alpha) \leq x$ such that α can be written as a sum

$$\alpha = \sum_{i=1}^{n} \varepsilon_i,$$

where the ε_i are units of R and no subsum of $\varepsilon_1 + \cdots + \varepsilon_n$ vanishes. The proof uses ideas of Everest [8], see also Everest and Shparlinski [9].

Theorem 12. *[16, Theorem 1] Let $\varepsilon > 0$. Then*

$$u_{K,S}(n, x) = \frac{c_{n-1,s}}{n!} \left(\frac{\omega_K (\log x)^s}{\mathrm{Reg}_{K,S}} \right)^{n-1} + o((\log x)^{(n-1)s-1+\varepsilon}),$$

as $x \to \infty$. Here, ω_K is the number of roots of unity of K, $\mathrm{Reg}_{K,S}$ is the S-regulator of K, and $s = |S| - 1$. The constant $c_{n,s}$ is the volume of the polyhedron

$$\{(x_{11}, \ldots, x_{ns}) \in \mathbb{R}^{ns} \mid g(x_{11}, \ldots, x_{ns}) < 1\},$$

with

$$g(x_{11},\dots,x_{ns}) = \sum_{i=1}^{s} \max\{0, x_{1i},\dots,x_{ni}\} + \max\left\{0, -\sum_{i=1}^{s} x_{1i},\dots,-\sum_{i=1}^{s} x_{ni}\right\}.$$

The values of the constant $c_{n,s}$ are known in special cases from [16]:

	n				
s	1	2	3	4	5
1	2	3	4	5	6
2	3	15/4	7/2	45/16	
3	10/3	7/3	55/54		
4	35/12	275/32			
5	21/10				

Furthermore, $c_{n,1} = n+1$ and $c_{1,s} = \frac{1}{s!}\binom{2s}{s}$.

In the following we calculate the constant $c_{n,s}$ for $n > 1$ and $s = 2$. This constant is the volume of the polyhedron

$$V = \{(x,y) \in \mathbb{R}^n \times \mathbb{R}^n : g(x,y) < 1\},$$

with

$$g(x,y) = \max_i \{0, x_i\} + \max_i \{0, y_i\} + \max_i \{0, -x_i - y_i\},$$

where $x = (x_1,\dots,x_n)$, $y = (y_1,\dots,y_n)$.

For any K, L, $M \in \{1,\dots,n\}$ we consider the sets

$$V_{K,L,M} = \left\{(x,y) \in \mathbb{R}^{2n} : x_i \le x_K,\ y_i \le y_L,\ x_M + y_M \le x_i + y_i,\ g(x,y) < 1\right\}.$$

Clearly the union of these sets is V and the intersection of any two of them has volume zero. Thus

$$c_{n,2} = \sum_{K=1}^{n}\sum_{L=1}^{n}\sum_{M=1}^{n} I_{K,L,M},$$

where $I_{K,L,M}$ is the volume of $V_{K,L,M}$. For the values of $I_{K,L,M}$ we distinguish three cases:

(i) K, L, M are pairwise distinct;

(ii) exactly two of the indices K, L, M are equal;

(iii) $K = L = M$.

The third case is simple. Since $x_i \le x_K$, $y_i \le y_K$ implies $x_i + y_i \le x_K + y_K$ we obtain $x_i + y_i = x_K + y_K$. Thus $V_{K,K,K}$ has volume zero.

We only have to consider the remaining cases (i) and (ii). Clearly,

$$c_{n,2} = n(n-1)(n-2)I_{1,2,3} + 3n(n-1)I_{1,1,2}.$$

5.i Calculation of $I_{1,2,3}$

This case can only happen if $n \geq 3$. The inequalities $x_3 + y_3 \leq x_i + y_i$ give us lower bounds for x_i and y_i and we always have the upper bounds $x_i \leq x_1$ and $y_i \leq y_2$. Hence we have

$$x_3 + y_3 - x_i \leq y_i \leq y_2$$

and

$$x_i \leq x_1.$$

Note that

$$g(x,y) = \max\{0, x_1\} + \max\{0, y_2\} + \max\{0, -x_3 - y_3\}.$$

We integrate with respect to the y_i's, $i \neq 2, 3$ and obtain

$$I_{1,2,3} = \int\cdots\int_{\substack{x_3+y_3-x_i\leq y_i\leq y_2\\ x_i\leq x_1,\ g(x,y)<1}} dxdy = \int\cdots\int_{\substack{x_3+y_3\leq x_2+y_2\\ x_3+y_3-y_2\leq x_i\leq x_1\\ y_3\leq y_2,\ g(x,y)<1}} \prod_{j\neq 2,3}(y_2 - x_3 - y_3 + x_j)dxdy_2dy_3.$$

Next we integrate over the x_i's, $i \neq 1, 2, 3$ and obtain

$$I_{1,2,3} = \int\cdots\int_{\substack{x_2,x_3\leq x_1,\ y_3\leq y_2\\ x_3+y_3\leq x_2+y_2\\ g(x,y)<1}} \frac{1}{2^{n-3}}(y_2 - x_3 - y_3 + x_1)^{2n-5}dx_1dx_2dx_3dy_2dy_3.$$

For the values of $g(x, y)$ we consider the following cases depending on the signs of x_1, y_2 and $-x_3 - y_3$:

r	x_1	y_2	$-x_3 - y_3$	$g(x,y)$
1	≥ 0	< 0	< 0	x_1
2	< 0	≥ 0	< 0	y_2
3	< 0	< 0	≥ 0	$-x_3 - y_3$
4	≥ 0	≥ 0	< 0	$x_1 + y_2$
5	≥ 0	< 0	≥ 0	$x_1 - x_3 - y_3$
6	< 0	≥ 0	≥ 0	$y_2 - x_3 - y_3$
7	≥ 0	≥ 0	≥ 0	$x_1 + y_2 - x_3 - y_3$

According to the table we split the integral into seven parts:

$$I_{1,2,3} = \sum_{r=1}^{7} I_{1,2,3}^{(r)}.$$

One can calculate these integrals with the help of a computer algebra system. We just give the final expressions:

$$\begin{aligned} I_{1,2,3}^{(1)} = I_{1,2,3}^{(2)} = I_{1,2,3}^{(3)} &= \frac{2}{n(2n-1)(n-1)2^n}, \\ I_{1,2,3}^{(4)} = I_{1,2,3}^{(5)} = I_{1,2,3}^{(6)} &= \frac{2}{n(n-1)2^n}, \\ I_{1,2,3}^{(7)} &= \frac{2}{n2^n}. \end{aligned}$$

In conclusion we have

$$I_{1,2,3} = \frac{2(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

5.ii Calculation of $I_{1,1,2}$

We proceed in the same way as in the other case. We have the same bounds

$$x_2 + y_2 - x_i \le y_i \le y_1$$

and

$$x_i \le x_1.$$

We integrate first with respect to the y_i's and then with respect to the x_i's, $i \neq 1, 2$, and obtain

$$\begin{aligned} I_{1,1,2} = & \underset{\substack{x_2+y_2-y_1 \le x_i \le x_1 \\ y_2 \le y_1,\, g(x,y)<1}}{\int \cdots \int} \prod_{j \neq 1,2} (y_1 - x_2 - y_2 + x_j) dx dy_1 dy_2 = \\ = & \underset{\substack{x_2 \le x_1,\, y_2 \le y_1 \\ g(x,y)<1}}{\int \cdots \int} \frac{1}{2^{n-2}} \left(y_1 - x_2 - y_2 + x_1\right)^{2n-4} dx_1 dx_2 dy_1 dy_2. \end{aligned}$$

Proceeding as in the previous section we again split the integral into seven parts $I_{1,1,2}^{(r)}$, $r = 1, \ldots, 7$, and obtain:

$$\begin{aligned} I_{1,1,2}^{(1)} = I_{1,1,2}^{(2)} = I_{1,1,2}^{(3)} &= \frac{1}{n(2n-1)(n-1)2^n}, \\ I_{1,1,2}^{(4)} = I_{1,1,2}^{(5)} = I_{1,1,2}^{(6)} &= \frac{1}{n(n-1)2^n}, \\ I_{1,1,2}^{(7)} &= \frac{1}{n2^n}. \end{aligned}$$

Hence

$$I_{1,1,2} = \frac{(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

Conclusion. *The value of $c_{n,2}$ is*

$$\frac{(n+1)(2n+1)}{2^n}.$$

Remark. *The computation of $c_{n,s}$ for $s > 2$ seems to be more difficult and might be considered later.*

6 Matrix rings

6.1 Matrix rings over arbitrary rings

Let R be any ring with 1. We say that two elements $a, b \in R$ are equivalent ($a \sim b$) if there exist two units $u, v \in R^\times$ such that $b = uav$. Vámos [34, Lemma 1] already noticed the following simple fact.

Lemma 13. *Let R be a ring and $a, b \in R$. If $a \sim b$ then, for all $k \geq 1$, a is k-good if and only if b is k-good.*

We consider the ring $M_n(R)$ of $n \times n$ matrices, with $n \geq 2$, over an arbitrary ring R with 1. As usual $GL_n(R)$ denotes the group of units of $M_n(R)$.

For $a \in R$ the matrix $E_n(a, i, j)$, i, $j \in \{1, \ldots, n\}$, $i \neq j$, is the $n \times n$ matrix with 1 entries on the main diagonal, a as the entry at position (i, j) and 0 elsewhere. We call this kind of matrices *elementary matrices* and denote by $E_n(R)$ the subgroup of $GL_n(R)$ generated by elementary matrices, permutation matrices and $-I$, where I is the identity matrix of $M_n(R)$.

Let us consider a more specific kind of k-goodness introduced by Vámos [34].

Definition. *A square matrix of size n over R is strongly k-good if it can be written as a sum of k elements of $E_n(R)$. The ring $M_n(R)$ is strongly k-good if every element is strongly k-good.*

The following lemma is Lemma 1 from [21] and Lemma 5 from [34].

Lemma 14. *Let R be a ring and $n \geq 2$. Then any diagonal matrix in $M_n(R)$ is strongly 2-good.*

A ring R is called an *elementary divisor ring* (see [25]) if every matrix in $M_n(R)$, $n \geq 2$, can be diagonalized. Lemma 14 implies that, in this case, $M_n(R)$ is 2-good. In particular, if any matrix in $M_n(R)$ can be diagonalized using only matrices in $E_n(R)$ then $M_n(R)$ is strongly 2-good.

The following two remarks can be deduced without much effort from the proof of Lemma 14 that is given in [34].

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then the representation of a matrix in $M_n(R)$ as a sum of two units is never unique.*

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then every element of $M_n(R)$ has a representation as a sum of two distinct units.*

As we have already mentioned, Henriksen [21] proved that $M_n(R)$, where R is any ring, is 3-good. Henriksen's result was generalized by Vámos [34] to arbitrary dimension:

Theorem 15. *[34, Theorem 11] Let R be a ring and let F be a free R-module of rank α, where $\alpha \geq 2$ is a cardinal number. Then the ring of endomorphisms E of F is 3-good.*

If α is finite and R is 2-good or an elementary divisor ring then E is 2-good. If R is any one of the rings $\mathbb{Z}[X]$, $K[X,Y]$, $K\langle X,Y\rangle$, where K is a field, then $u(E) = 3$. Here $K\langle X,Y\rangle$ is the free associative algebra generated by X, Y over K.

To prove that a matrix ring over a certain ring has unit sum number 3, Vámos used the following proposition.

Proposition 16. *[34, Proposition 10] Let R be a ring, $n \geq 2$ an integer and let $L = Ra_1 + \cdots + Ra_n$ be the left ideal generated by the elements $a_1, \ldots, a_n \in R$. Let A be the $n \times n$ matrix whose entries are all zero except for the first column which is $(a_1, \ldots, a_n)^T$. Suppose that*

1. *L cannot be generated by fewer than n elements, and*

2. *zero is the only 2-good element in L.*

Then A is not 2-good.

We now apply Lemma 14 to a special case. Let R be a ring and suppose there exists a function

$$f : R \setminus \{0\} \to \mathbb{Z}_{\geq 0},$$

with the following property: for every $a, b \in R$, $b \neq 0$, there exist $q_1, q_2, r_1, r_2 \in R$ such that

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{where} \quad r_1 = 0 \text{ or } f(r_1) < f(b), \\ a &= b q_2 + r_2, \quad \text{where} \quad r_2 = 0 \text{ or } f(r_2) < f(b). \end{aligned}$$

Then we say that R has *left and right Euclidean division.*

The next theorem is a generalization of the well known fact that every square matrix over a Euclidean domain is diagonalizable. The proof strictly follows the line of the one in the commutative case (see Section 3.5 of [18]), hence it is omitted.

Theorem 17. *Let R be a ring with left and right Euclidean division and $n \geq 2$. For every $A \in M_n(R)$ there exist two matrices $U, V \in E_n(R)$ such that*

$$UAV = D,$$

where D is a diagonal matrix.

Corollary. *Let R be a ring with left and right Euclidean division and $n \geq 2$. Then $M_n(R)$ is strongly 2-good.*

We apply the previous result to the special case of quaternions. Consider the quaternion algebra

$$Q = \left\{ a + bi + cj + dk \mid a,\ b,\ c,\ d \in \mathbb{Q},\ i^2 = -1,\ j^2 = -1,\ k = ij = -ji \right\}.$$

Definition. *The ring of Hurwitz quaternions is defined as the set*

$$H = \left\{ a + bi + cj + dk \in Q \quad \text{s. t.} \quad a, b, c, d \in \mathbb{Z} \quad \text{or} \quad a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

For basic properties about Hurwitz quaternions see [5, Chapter 5].

In Q the ring of Hurwitz quaternions plays a similar role as maximal orders in number fields.

The units of H are the 24 elements ± 1, $\pm i$, $\pm j$, $\pm k$ and $(\pm 1 \pm i \pm j \pm k)/2$, so $u(H) = \omega$.

It is well known that H has left and right Euclidean division. Therefore, we get the following corollary.

Corollary. *For $n \geq 2$, $M_n(H)$ is strongly 2-good.*

6.2 Matrix rings over Dedekind domains

Let R be a ring and A an $r \times c$ matrix. The *type* of A is the pair (r, c) and the *size* of A is $\max(r, c)$. Let A_1 and A_2 be matrices of type (r_1, c_1) and (r_2, c_2), respectively. The *block diagonal sum* of A_1 and A_2 is the block diagonal matrix

$$diag(A_1, A_2) = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix},$$

of type $(r_1 + r_2, c_1 + c_2)$. A matrix of positive size is *indecomposable* if it is not equivalent to the block diagonal sum of two matrices of positive size.

In 1972 Levy [26] proved that, for a Dedekind domain R, the class number, when it is finite, is an upper bound to the number of rows and columns in every indecomposable matrix over R. Vámos and Wiegand [35] generalized Levy's result to Prüfer domains (under some technical conditions) and applied it to the unit sum problem.

Theorem 18. *(see [35, Theorem 4.7]) Let R be a Dedekind domain with finite class number c. For every $n \geq 2c$, $M_n(R)$ is 2-good.*

Unfortunately we do not know a criterion. The only sufficient condition we know for a matrix not to be 2-good is given by Proposition 16. For rings R of algebraic integers this proposition is of limited use. Since ideals in Dedekind domains need at most 2 generators, condition (1) can be fulfilled only for $n = 2$. Concerning condition (2) it is not hard to see that, if the unit group is infinite, there is a nonzero sum of two units in every nonzero ideal in a ring of algebraic integers. Therefore we can apply Proposition 16 only to the non-PID complex quadratic case.

Corollary. *[35, Example 4.11] Let R be the ring of integers of $\mathbb{Q}(\sqrt{-d})$, where $d > 0$ is squarefree and R has class number $c > 1$. Then $u(M_2(R)) = 3$ and $u(M_n(R)) = 2$ for every integer $n \geq 2c$.*

Question A. *[35, Example 4.11] With the hypotheses of the previous corollary, what is the value of $u(M_n(R))$ for $3 \leq n < 2c$?*

Question B. *[35, Question 4.12] If R is any ring of algebraic integers with class number c, what is the value of $u(M_n(R))$ for $2 \leq n < 2c$?*

Acknowledgements

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13. C. Frei is supported by the Austrian Science Foundation (FWF) project S9611-N23.

References

[1] N. Ashrafi. A finer classification of the unit sum number of the ring of integers of quadratic fields and complex cubic fields. *Proc. Indian Acad. Sci. Math. Sci.*, 119(3):267–274, 2009.

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

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

[4] 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.

[5] J. H. Conway and D. A. Smith. *On quaternions and octonions: their geometry, arithmetic and symmetry.* A K Peters, Natick, Massachusetts, 2003.

[6] J. Dieudonné. La théorie de Galois des anneux simples et semi-simples. *Comment. Math. Helv.*, 21:154–184, 1948.

[7] P. Erdös. Arithmetical properties of polynomials. *J. London Math. Soc.*, 28:416–425, 1953.

[8] G. R. Everest. Counting the values taken by sums of S-units. *J. Number Theory*, 35(3):269–286, 1990.

[9] G. R. Everest and I. E. Shparlinski. Counting the values taken by algebraic exponential polynomials. *Proc. Amer. Math. Soc.*, 127(3):665–675, 1999.

[10] J.-H. Evertse and K. Győry. On the numbers of solutions of weighted unit equations. *Compositio Math.*, 66(3):329–354, 1988.

[11] 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.

[12] 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.

[13] C. Frei. On rings of integers generated by their units. *submitted.*

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

[15] C. Frei. Sums of units in function fields II - The extension problem. *to appear in Acta Arith.*

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

[17] B. Goldsmith, S. Pabst, and A. Scott. Unit sum numbers of rings and modules. *Q. J. Math.*, 49(195):331–344, 1998.

[18] F. M. Goodman. *Algebra: abstract and concrete.* SemiSimple Press, Iowa City, IA, 1998.

[19] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

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

[21] M. Henriksen. Two classes of rings generated by their units. *J. Algebra*, 31:182–193, 1974.

[22] B. Herwig and M. Ziegler. A remark on sums of units. *Arch. Math. (Basel)*, 79(6):430–431, 2002.

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

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

[25] I. Kaplansky. Elementary divisors and modules. *Trans. Amer. Math. Soc.*, 66:464–491, 1949.

[26] L. S. Levy. Almost diagonal matrices over Dedekind domains. *Math. Z.*, 124:89–99, 1972.

[27] R. C. Mason. Norm form equations. I. *J. Number Theory*, 22(2):190–207, 1986.

[28] R. C. Mason. Norm form equations. III. Positive characteristic. *Math. Proc. Camb. Philos. Soc.*, 99(3):409–423, 1986.

[29] A. Pethő and V. Ziegler. On biquadratic fields that admit unit power integral basis,. *submitted.*

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

[31] A. K. Srivastava. A survey of rings generated by units. *Ann. Fac. Sci. Toulouse Math. (6)*, 19, 2010.

[32] J. Thuswaldner and V. Ziegler. On linear combinations of units with bounded coefficients. *preprint.*

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

[34] P. Vámos. 2-good rings. *Q. J. Math.*, 56(3):417–430, 2005.

[35] P. Vámos and S. Wiegand. Block diagonalization and 2-unit sums of matrices over Prüfer domains. *to appear in Trans. Amer. Math. Soc.*

[36] B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk (2)*, 15:212–216, 1927.

[37] D. Zelinsky. Every linear transformation is a sum of nonsingular ones. *Proc. Am. Math. Soc.*, 5:627–630, 1954.

[38] V. Ziegler. The additive S-unit structure of quadratic fields. *to appear in Int. J. Number Theory.*

[39] V. Ziegler. On unit power integral bases of $\mathbb{Z}[\sqrt[4]{m}]$. *to appear in Period. Math. Hung.*

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

Technische Universität Graz
Institut für Analysis und Computational Number Theory
Steyrergasse 30, 8010 Graz, Austria
E-mail: barroero@math.tugraz.at, frei@math.tugraz.at, tichy@tugraz.at

Sums of units in function fields

Christopher Frei

Abstract

Let R be the ring of S-integers of an algebraic function field (in one variable) over a perfect field, where S is finite and not empty. It is shown that for every positive integer N there exist elements of R that can not be written as a sum of at most N units.

Moreover, all quadratic global function fields whose rings of integers are generated by their units are determined.

1 Introduction

The connection between the additive structure and the units of certain rings has achieved some attention in the last years. First investigations in this direction were made by Zelinsky [20], who showed that, except for one special case, every linear transformation of a vector space is a sum of two automorphisms, and Jacobson [11], who showed that in the rings of integers of the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ every element can be written as a sum of distinct units. Jacobson's work was extended by Śliwa [17], who proved that there are no other quadratic number fields with this property, and Belcher [2], [3], who investigated cubic and quartic number fields.

Goldsmith, Pabst and Scott [8], investigated similar questions, but without the requirement that the units be distinct. The following definition from [8] describes quite precisely how the units of a ring R additively generate R.

Definition 1. *Let R be a ring with identity and k a positive integer. An element $r \in R$ is called k-good if there are units $e_1, \ldots, e_k$ of R, such that*

The original publication is available at `http://www.springerlink.com`.
DOI: 10.1007/s00605-010-0219-7
2010 *Mathematics Subject Classification*: 12E30; 11R27; 11R58; 11R04
Key words and phrases: unit sum number, sums of units, function field

$r = e_1 + \cdots + e_k$. *If every element of* R *is* k*-good then we call the ring* k*-good as well.*

The unit sum number $u(R)$ *of* R *is defined as* $\min\{k \mid R \text{ is } k\text{-good }\}$, *if this minimum exists. If the minimum does not exist, but* R *is additively generated by its units, then we define* $u(R) := \omega$. *If the units do not generate* R *additively then we set* $u(R) := \infty$.

By convention, we put $n < \omega < \infty$, for every integer n. The case where R is the ring of integers of an algebraic number field has recently been of particular interest. The fact that no ring of integers of an algebraic number field can have a finite unit sum number was proved by Ashrafi and Vámos [1] in some special cases, and by Jarden and Narkiewicz [12] in the general case. It is also a consequence of a result obtained independently by Hajdu [9]. Our first theorem is an analogous result for rings of S-integers of algebraic function fields over perfect fields.

Regarding function fields, we use the notation from [16] and [18]. In particular, an algebraic function field over a field K is a finitely generated extension $F|K$ of transcendence degree 1. If K is a finite field then $F|K$ is called a global function field. The algebraic closure of K in F is called the (full) field of constants of $F|K$. Following [18], we regard the places of $F|K$ as the maximal ideals of discrete valuation rings of F containing K. In particular, the places P of $F|K$ correspond to (surjective) discrete valuations $v_P : F \to (\mathbb{Z} \cup \{\infty\})$ of F over K. Let n be a positive integer. We say that a place P of $F|K$ is a zero of an element $f \in F$ of order n, if $v_P(f) = n > 0$, and P is a pole of f of order n, if $v_P(f) = -n < 0$. If S is a finite set of places of $F|K$ then the ring $\mathcal{O}_S$ of S-integers of F is the set of all elements of F that have no poles outside of S. The S-units of F are the units of $\mathcal{O}_S$. As a consequence of the definition of $\mathcal{O}_S$, an element $f \in F$ is an S-unit if and only if $v_P(f) = 0$ for all places P outside of S. The pole [zero] divisor $(f)_\infty$ [$(f)_0$] of an element $f \in F^*$ is the sum of all poles [zeros] of f, taken with their respective multiplicities. The height $H(f)$ of f is defined as the degree of its zero divisor, or, equivalently, as the degree of its pole divisor:

$$\begin{aligned} H(f) := \deg(f)_0 &= \sum_P \max\{0, v_P(f) \deg P\} \\ &= -\sum_P \min\{0, v_P(f) \deg P\} = \deg(f)_\infty, \end{aligned}$$

where the sums run over all places P of $F|K$.

The following theorem is basically a consequence of Mason's classical work on unit equations in function fields [14], [15].

Theorem 1. *Let K be a perfect field, $F|K$ an algebraic function field, and $S \neq \emptyset$ a finite set of places of $F|K$. Denote by $\mathcal{O}_S$ the ring of S-integers of F. Then, for each positive integer N, there exists an element of $\mathcal{O}_S$ that can not be written as a sum of at most N units of $\mathcal{O}_S$. In particular, we have $u(\mathcal{O}_S) \geq \omega$.*

To show that both cases, ω and ∞, occur, we give a complete classification of the unit sum numbers of rings of integers of quadratic function fields over finite fields. The number field analogue of this result was found independently by Belcher [2] and Ashrafi and Vámos [1]. Results of this kind also exist for cubic and quartic number fields [5], [19], [21]. In the global function field case it turns out that the only quadratic function fields whose rings of integers have unit sum number ω are real quadratic function fields that are again rational.

Theorem 2. *Let K be a finite field, and F a quadratic extension field of the rational function field $K(x)$ over K. Denote the integral closure of $K[x]$ in F by $\mathcal{O}_F$. Then the following two statements are equivalent.*

(a) $u(\mathcal{O}_F) = \omega$.

(b) The function field $F|K$ has full constant field K and genus 0, and the infinite place of $K(x)$ splits into two places of $F|K$.

Of course, one can use Theorem 2 to obtain explicit criteria similar to those in [1], [2], [5], [19], [21]. If K is of odd characteristic then every quadratic extension field of the rational function field $K(x)$ with full constant field K is of the form $F = K(x, y)$, where y satisfies an equation $y^2 = f(x)$, for some separable polynomial $f \in K[X] \setminus K$. It is well known that F is of genus 0 if and only if $\deg f \in \{1, 2\}$, and that the infinite place of $K(x)$ splits in $F|K$ if and only if $\deg f$ is even and the leading coefficient of f is a square in K. We therefore get the following corollary.

Corollary 1. *Let K be a finite field of odd characteristic, and $F = K(x, y)$, where $K(x)$ is a rational function field over K and $y^2 = f(x)$, for some separable polynomial $f \in K[x] \setminus K$. Denote the integral closure of $K[x]$ in F by $\mathcal{O}_F$. Then the following two statements are equivalent.*

(a) $u(\mathcal{O}_F) = \omega$.

(b) The degree of f is 2 and the leading coefficient of f is a square in K.

If K is of characteristic 2 then every separable quadratic extension field of the rational function field $K(x)$ with full constant field K can be written as $F = K(x, y)$, where y satisfies a quadratic equation in Hasse normal form [10, p. 38]. That is,

$$y^2 + y = \frac{g(x)}{p_1(x)^{2n_1-1} \cdots p_m(x)^{2n_m-1}}, \tag{1}$$

where, $p_1, \ldots, p_m \in K[X]$ are monic irreducible polynomials and distinct from each other, $n_1, \ldots, n_m$ are positive integers, $g \in K[X]$ is not divisible by any of the p_i, and the infinite place of $K(x)$ is either no pole or a pole of odd order of the right-hand side of (1). (That is, the difference of the degrees of denominator and numerator is non-negative or odd.) We put $B := p_1^{n_1} \cdots p_m^{n_m}$, and $C := gp_1 \cdots p_m$ (cf. [13]). Then (1) becomes

$$y^2 + y = \frac{C(x)}{B(x)^2}. \tag{2}$$

Note that K is the full constant field of $F|K$ if and only if C is not constant. Using well-known properties of Artin-Schreier extensions of function fields (for example Proposition III.7.8. from [18]), we see that the function field $F|K$ is of genus 0 if and only if

$$\deg B = 0 \quad \text{and} \quad \deg C = 1 \tag{3}$$

or

$$\deg B = 1 \quad \text{and} \quad \deg C \leq 2. \tag{4}$$

In case (3) the infinite place of $K(x)$ is ramified in $F|K$, and in case (4) the infinite place of $K(x)$ splits in $F|K$ if and only if either $\deg C < 2$, or $\deg C = 2$ and the leading coefficient of C has the form a^2+a, for some $a \in K$. (These are exactly the cases where the projection of $y^2 + y + C(x)/B(x)^2$ to the polynomial ring over the residue class field of the infinite place of $K(x)$ is reducible.) We have shown the following analogue of Corollary 1.

Corollary 2. *Let K be a finite field of characteristic 2, and $F = K(x, y)$, where y satisfies an irreducible quadratic equation (2) in Hasse normal form. Denote the integral closure of $K[x]$ in F by $\mathcal{O}_F$. Then the following two statements are equivalent.*

(a) $u(\mathcal{O}_F) = \omega$.

(b) We have $\deg B = 1$ and either $\deg C \leq 1$, or $\deg C = 2$ and the leading coefficient of C is of the form $a^2 + a$, for some $a \in K$.

Note that if K is of characteristic 2 and $F|K(x)$ is an inseparable quadratic extension then it is purely inseparable, and the infinite place of $K(x)$ is ramified in $F|K$. Therefore, we have $u(\mathcal{O}_F) = \infty$ in this case.

In the number field case, quantitative problems in relation with sums of units have been objects of recent study. The question, how many non-associated algebraic integers with bounded norm in a number field can be written as a sum of exactly k units, has been investigated in [5], [6] and [7]. Similar considerations in the function field case would be of interest.

2 Proof of Theorem 1

Let $\tilde{K}$ be the full constant field of $F|K$. Since the places of the function fields $F|K$ and $F|\tilde{K}$ are the same, we may assume without loss of generality that $K = \tilde{K}$. We start with the case where K is of characteristic 0.

2.1 Characteristic 0

The main tool for our proof is a finiteness result on S-unit equations by Mason [14, Lemma 2].

Lemma 1. *Let K be an algebraically closed field of characteristic 0, $F|K$ an algebraic function field, and S a finite set of places of $F|K$. Suppose that u_1, ..., u_k are S-units in F such that $u_1 + \cdots + u_k = 1$, and no proper subset of $\{1, u_1, \ldots, u_k\}$ is K-linearly dependent. Then we have $H(u_i) \leq A(k)$, for all $1 \leq i \leq k$ and a constant $A(k)$ that depends only on k, S, and $F|K$.*

Mason even provides an explicit formula for the bound $A(k)$, which was improved by Brownawell and Masser [4]. For our purpose, however, the above lemma is sufficient. Suppose that every element of $\mathcal{O}_S$ is a sum of at most N S-units, for some integer $N > 1$. Choose some non-constant S-integer r that is not an S-unit, and denote the set of zeros of r by T. Obviously, r is an $(S \cup T)$-unit, and there is some place $P \in T \setminus S$.

For every positive integer n, there exists some $2 \leq k \leq N$, and S-units ε_1, ..., $\varepsilon_k \in \mathcal{O}_S^*$, such that

$$\varepsilon_1 + \cdots + \varepsilon_k = r^n,$$

and no proper subset of $\{\varepsilon_1, \ldots, \varepsilon_k, r^n\}$ is K-linearly dependent. Therefore, we have

$$\varepsilon_1/r^n + \cdots + \varepsilon_k/r^n = 1, \tag{5}$$

for $(S \cup T)$-units ε_1/r^n, …, ε_k/r^n, and still no proper subset is K-linearly dependent.

For some algebraically closed field $\Phi \supset F$, let $\overline{K}$ be the algebraic closure of K in Φ. We put $F' := F\overline{K}$ and regard the constant field extension $F'|\overline{K}$ of $F|K$. Let S' be the set of all places of $F'|\overline{K}$ lying over places in $(S \cup T)$.

Then (5) is an S'-unit equation in $F'|\overline{K}$. Since F and $\overline{K}$ are linearly disjoint over K (see, for example, [18, Proposition III.6.1]), all requirements of Lemma 1 are satisfied. Therefore,

$$H(\varepsilon_1/r^n) \leq A(k) \leq A := \max\{A(2), \ldots, A(N)\}. \tag{6}$$

On the other hand, we have $H(\varepsilon_1/r^n) \geq |v_{P'}(\varepsilon_1/r^n)| = nv_{P'}(r) \geq n$, for any place P' of $F'|\overline{K}$ lying over P. Here we used that ε_1 is an S-unit and $P \notin S$, whence $v_P(\varepsilon_1) = 0$. If n is chosen big enough, this contradicts (6).

2.2 Positive characteristic

The case of positive characteristic p is similar in spirit, but a little bit more technical. The main problem is that, due to the Frobenius homomorphism, the height of solutions of unit equations is no longer bounded. For if

$$u_1 + \cdots + u_k = 1$$

is a solution of such a unit equation then

$$u_1^{p^l} + \cdots + u_k^{p^l} = 1$$

as well, for any positive integer l. Again, we use a result by Mason. The following lemma is a special form of Lemma 1 from [15].

Lemma 2. *Let K be an algebraically closed field of positive characteristic p, and $K(z)|K$ a rational function field. Let F be a finite separable extension of $K(z)$, and denote by $\mathcal{O}_F$ the integral closure of $K[z]$ in F.*

For each positive integer k, there exist bounds $M(k)$, $A(k) \in \mathbb{R}$, depending only on $F|K(z)$ and k, such that the following holds: Let $(u_1, \ldots, u_k) \in (\mathcal{O}_F^*)^k$ be a solution of the unit equation

$$u_1 + \cdots + u_k = 0,$$

such that no proper subsum on the left-hand side vanishes. Then there are non-negative integers m, $t(1)$, …, $t(m)$, a non-zero constant $\eta \in K$, and units η_1, …, $\eta_m \in \mathcal{O}_F^*$, such that

$$u_2/u_1 = \eta \prod_{j=1}^{m} \eta_j^{p^{t(j)}}.$$

Moreover, we have $m \leq M(k)$, and $H(\eta_j) \leq A(k)$, for all $1 \leq j \leq m$. (As usual, the empty product is interpreted as 1.)

Additionally, we use the following elementary number-theoretical lemma.

Lemma 3. *Let p, M, A be positive integers. Then there exist infinitely many positive integers n that can not be written in the form*

$$n = -\sum_{j=1}^{m} p^{t(j)} k_j, \tag{7}$$

with any integer $0 \leq m \leq M$, integers k_j with $|k_j| \leq A$, and non-negative integers $t(j)$.

Proof. Let T be any positive integer and R_T the set of residue classes of all positive integers of the form (7) modulo p^T. Each residue class in R_T has a representative of the form

$$-\sum_{j=1}^{M} p^{s(j)} k_j,$$

with k_j as in the lemma, and integers $s(j) \in \{0, \ldots, T-1\}$. Obviously, there are at most $(T(2A+1))^M$ such representatives, which is a polynomial in T. On the other hand, there are p^T residue classes modulo p^T. If T is chosen big enough then not all residue classes modulo p^T are in R_T, and the lemma follows immediately. □ □

Let N be a positive integer. We construct an element of $\mathcal{O}_S$ that can not be written as a sum of at most N units of $\mathcal{O}_S$.

Choose some place P of $F|K$ that is not in S. The strong approximation theorem permits us to find an S-integer $r \in \mathcal{O}_S$ with $v_P(r) = 1$. Let T be the set of zeros of r. Then r is obviously an $(S \cup T)$-unit, but no S-unit.

For some algebraically closed field $\Phi \supset F$, let $\overline{K}$ be the algebraic closure of K in Φ, and put $F' := F\overline{K}$. We regard the constant field extension $F'|\overline{K}$ of $F|K$.

Let S' be the set of all places of $F'|\overline{K}$ lying over places in $(S \cup T)$, and choose some places $Q \in S'$ and R, $R' \notin S'$ of $F'|\overline{K}$. By the strong approximation theorem, we can find an element $z \in F'$ that satisfies the conditions

$$\begin{aligned}
&v_R(z) = 1,\\
&v_{R'}(z) = |S'| - 1,\\
&v_W(z) = -1, \text{ for all } W \in S' \smallsetminus \{Q\}, \text{ and}\\
&v_W(z) \geq 0, \text{ for all places } W \notin S' \cup \{R, R'\}.
\end{aligned}$$

Since the principal divisor of z must have degree 0, it follows that $v_Q(z) < 0$. Therefore, the poles of z are exactly the elements of S'. Moreover, z is not a p-th power, since p does not divide $v_R(z) = 1$. It follows that F' is separable over $\overline{K}(z)$ (use, for example, Proposition III.9.2 (d) from [18]) and the integral closure of $\overline{K}[z]$ in F' is exactly $\mathcal{O}_{S'}$, the ring of S'-integers of F'.

For any positive integer k, let $M(k)$, $A(k)$ be the constants from Lemma 2, for the function field extension $F'|\overline{K}(z)$. In Lemma 3, put

$$M := \max\{M(k) \mid 2 \leq k \leq N{+}1\}, \quad \text{and} \quad A := \max\{A(k) \mid 2 \leq k \leq N{+}1\},$$

and choose some positive integer n that can not be written in the form (7).

We claim that the element $r^n \in \mathcal{O}_S$ can not be written as a sum of at most N units of $\mathcal{O}_S$. Suppose otherwise; then there is some $2 \leq k \leq N$ and units $\varepsilon_1, \ldots, \varepsilon_k \in \mathcal{O}_S^*$, such that

$$\varepsilon_1 + \cdots + \varepsilon_k = r^n,$$

and no proper subsum on the left-hand side vanishes. Therefore, we get

$$-r^n + \varepsilon_1 + \cdots + \varepsilon_k = 0,$$

for $(S \cup T)$-units $-r^n$, $\varepsilon_1, \ldots, \varepsilon_k$, and still no proper subsum vanishes. Regarded as elements of F', the summands on the left-hand side are S'-units. Lemma 2 implies that there exist an integer $0 \leq m \leq M$, non-negative integers $t(1), \ldots, t(m)$, a constant $\eta \in \overline{K}^*$, and S'-units $\eta_1, \ldots, \eta_m \in \mathcal{O}_{S'}^*$, such that $H(\eta_j) \leq A$, for all $1 \leq j \leq m$, and

$$\varepsilon_1/r^n = -\eta \prod_{j=1}^{m} \eta_j^{p^{t(j)}}. \tag{8}$$

Let $P' \in S'$ be a place of $F'|\overline{K}$ lying over P. Since K is perfect, constant field extensions are unramified, and thus $v_{P'}(r) = 1$. We consider (8) in the P'-adic valuation:

$$-n = v_{P'}(\varepsilon_1/r^n) = \sum_{j=1}^{m} p^{t(j)} v_{P'}(\eta_j).$$

Since $|v_{P'}(\eta_j)|$ are bounded by $H(\eta_j) \leq A$, we found a representation (7), contrary to our choice of n. This completes the proof of Theorem 1.

3 Proof of Theorem 2

3.1 *(b)* implies *(a)*

To show that *(b)* implies *(a)*, we prove a more general proposition.

Proposition 1. *Let $K(x)$ be a rational function field over any perfect field K, $n \geq 2$ an integer, and $S = \{P_1, \ldots, P_n\}$ a set of n distinct places of $K(x)$ of degree one. Denote by $\mathcal{O}_S$ the ring of S-integers of $K(x)$. Then $u(\mathcal{O}_S) = \omega$.*

Proof. By Theorem 1, we have $u(\mathcal{O}_S) \geq \omega$, hence it is enough to show that every element of $\mathcal{O}_S$ is a sum of S-units. This is clear for $0 \in \mathcal{O}_S$. Let $f \in \mathcal{O}_S \setminus \{0\}$ be a non-zero element. The pole divisor of f has the form

$$(f)_\infty = v_1 P_1 + \cdots + v_n P_n,$$

with non-negative integers v_1, …, v_n. If $H(f) = 0$ then f is a constant and nothing is left to prove. Assume that $H(f) > 0$, that is, at least one of the v_i is positive. We construct an S-unit $u \in \mathcal{O}_S^*$, such that either $f = u$ or $H(f - u) < H(f)$. Then the proposition follows by induction.

Without loss of generality, we assume that $v_1 > 0$. By exchanging the generating element x, if necessary, we can always assure that P_1 is the infinite place of $K(x)$. Let $x - \alpha_i \in K[x]$ be the monic local parameter for P_i, for each $2 \leq i \leq n$. Then f is of the form

$$f = g(x) \cdot (x - \alpha_2)^{-v_2} \cdots (x - \alpha_n)^{-v_n},$$

where $g \in K[X] \setminus \{0\}$ is some polynomial. Since $-v_1 = v_{P_1}(f)$ is the difference of the degrees of denominator and numerator of f, we have $-v_1 = v_2 + \cdots + v_n - \deg g$. Therefore, g is of degree $v_1 + \cdots + v_n$. Let λ be the leading coefficient of g, and put $u := \lambda(x - \alpha_2)^{v_1}$. Then u is an S-unit, and we get

$$f - u = \frac{g - \lambda(x - \alpha_2)^{v_1 + v_2}(x - \alpha_3)^{v_3} \cdots (x - \alpha_n)^{v_n}}{(x - \alpha_2)^{v_2} \cdots (x - \alpha_n)^{v_n}}.$$

The degree of the numerator is smaller than the degree of g. Therefore, we have $v_{P_1}(f - u) > -v_1$. Also, $v_{P_i}(f - u) \geq -v_i$, for $2 \leq i \leq n$, and $v_P(f - u) \geq 0$, for all places $P \notin S$. Therefore, we have either $f - u = 0$ or $H(f - u) < H(f)$. This concludes our proof. □ □

Now assume *(b)* and let $S := \{P_1, P_2\}$ be the set of infinite places of $F|K$. Then both P_1 and P_2 are of degree one, so F is a rational function field over K. The integral closure of $K[x]$ in F is exactly the ring of S-integers $\mathcal{O}_S$ of F, whence *(a)* follows from Proposition 1.

3.2 *(a)* implies *(b)*

If K is not the full constant field of $F|K$ then $F|K(x)$ is a constant field extension (since it is of degree 2). Thus, $F = \tilde{K}(x)$, where $\tilde{K}$ is the full constant field of $F|K$. Since then $\mathcal{O}_F = \tilde{K}[x]$, the units of $\mathcal{O}_F$ are constants, so $u(\mathcal{O}_F) = \infty$. Therefore, K is the full constant field of $F|K$. We treat the cases of even and odd characteristic separately.

3.2.1 Odd characteristic

Let $p \geq 3$ be the characteristic of K. In this case, we always have $F = K(x, y)$, for some y in F, satisfying an equation

$$y^2 = f(x),$$

with a separable polynomial $f \in K[X] \setminus K$. We have $\mathcal{O}_F = K[x, y]$, since the separability of f implies non-singularity of the affine curve $Y^2 = f(X)$.

The following two lemmata use the notation of the preceding paragraph. The first one is the function field analogue of Lemma 1 from [2] and Theorem 7 from [1].

Lemma 4. *The ring of integers $\mathcal{O}_F$ is generated by units as a $K[x]$-module if and only if there is some $\mu \in K^*$ such that $f + \mu$ is a square in $K[X]$.*

In this case, the unit group $\mathcal{O}_F^*$ is of rank 1 and there is a fundamental unit of the form $a(x) + y$, for some $a \in K[X]$.

Proof. Our proof is basically the same as Belcher's proof of the number field case. First, assume that $f + \mu = g^2$, for some $\mu \in K^*$ and $g \in K[X]$. This implies that

$$(g(x) + y)(g(x) - y) = g(x)^2 - f(x) = \mu \in K^*,$$

whence $g(x)+y$, $g(x)-y$ are units in $\mathcal{O}_F$. Therefore, $y = (g(x)+y) - g(x) \cdot 1$ is a $K[x]$-linear combination of units of $\mathcal{O}_F$, and since $\mathcal{O}_F$ is generated by $\{1, y\}$ as a $K[x]$-module, we conclude that $\mathcal{O}_F$ is generated as a $K[x]$-module by its units.

Now assume that $\mathcal{O}_F$ is generated by its units as a $K[x]$-module. By Dirichlet's unit theorem (for a version that holds in global function fields see Proposition 14.2 from [16]), the group $\mathcal{O}_F^*/K^*$ is a free abelian group of rank 0 or 1. Rank 0 can not happen, since then the group of units in $\mathcal{O}_F$ would be exactly K^*, which generates only $K[x]$ as a $K[x]$-module. Therefore, we have a fundamental unit $a(x) + b(x)y$, with some a, $b \in K[X]$, b monic, and every unit of $\mathcal{O}_F$ is of the form

$$\lambda(a(x) + b(x)y)^n,$$

with some constant $\lambda \in K^*$ and some integer n. Since the norm of $a(x)+b(x)y$ is a unit of $K[x]$, hence an element of K^*, we have

$$(a(x)+b(x)y)^{-1} = \kappa(a(x)-b(x)y),$$

for some $\kappa \in K^*$. Let us write y as a $K[x]$-linear combination of units:

$$y = g_0(x) + \sum_{i=1}^{k_1} g_i(x)(a(x)+b(x)y)^{n_i} + \sum_{i=1}^{k_2} h_i(x)(a(x)-b(x)y)^{m_i},$$

where k_1, k_2 and all n_i, m_i are positive integers, and all g_i, $h_i \in K[X]$. Expanding the right-hand side yields an equation of the form

$$y = g(x) + h(x)b(x)y,$$

with polynomials g, $h \in K[X]$. By comparing the coefficient of y, we get $b(x) \in K[x]^* = K^*$, whence $b = 1$. Since the norm of $a(x)+y$ is a unit in $K[x]$, we get $a^2 - f = \mu \in K^*$, and f is of the desired form. □ □

Lemma 5. *Let $a \in K[X]$, such that $a(x)+y$ is a unit of $\mathcal{O}_F$. For any non-negative integer n, define polynomials a_n, $b_n \in K[X]$ via $a_n(x)+b_n(x)y := (a(x)+y)^n$. Then $\deg f$ is even, and for every positive integer n, we have*

$$\deg a_n = n(\deg f)/2 \quad \textit{and} \quad \deg b_n = (n-1)(\deg f)/2. \tag{9}$$

Proof. Induction on n proves that a_n, b_n are given by the recursive formulas

$$a_{n+1} = aa_n + b_n f \quad \text{and} \quad b_{n+1} = ab_n + a_n, \tag{10}$$

with starting values $a_0 = 1$, $b_0 = 0$.

Since $N(a(x)+y) = a(x)^2 - f$ is a constant, it follows that f is of even degree, and $\deg a = (\deg f)/2$. From $a_n(x)^2 - b_n(x)^2 f = N(a(x)+y)^n \in K^*$ we get, for all positive integers n,

$$\deg b_n = \deg a_n - (\deg f)/2, \tag{11}$$

and

$$\text{the leading coefficients of } a_n^2 \text{ and } b_n^2 f \text{ coincide.} \tag{12}$$

By (11) and the recursion formulas (10),

$$\deg a_{n+1} \le \deg a_n + (\deg f)/2 \quad \text{and} \quad \deg b_{n+1} \le \deg b_n + (\deg f)/2, \tag{13}$$

for all positive integers n.

We first prove (9) for the cases where n is a power of 2. We have already seen that the assertion holds for $n = 2^0 = 1$. Since

$$(a_{2^{l+1}}(x) + b_{2^{l+1}}(x)y) = (a(x) + y)^{2^{l+1}} = (a_{2^l}(x) + b_{2^l}(x)y)^2,$$

we get

$$a_{2^{l+1}} = a_{2^l}^2 + b_{2^l}^2 f \quad \text{and} \quad b_{2^{l+1}} = 2a_{2^l}b_{2^l}.$$

By (11) and by induction, we have $\deg a_{2^l}^2 = \deg b_{2^l}^2 f = 2^{l+1}(\deg f)/2$. Assertion (12) and the fact that $p \neq 2$ imply that $\deg a_{2^{l+1}} = 2^{l+1}(\deg f)/2$. Also,

$$\deg b_{2^{l+1}} = \deg a_{2^l} + \deg b_{2^l} = (2^{l+1} - 1)(\deg f)/2.$$

Now let n be an arbitrary positive integer and find the positive integer l, such that $2^{l-1} \leq n < 2^l$. We already know that

$$\deg a_{2^{l-1}} = 2^{l-1}(\deg f)/2 \quad \text{and } \deg a_{2^l} = 2^l(\deg f)/2.$$

By $(n - 2^{l-1})$ applications of (13), we get $\deg a_n \leq n(\deg f)/2$. Suppose that we have $\deg a_n < n(\deg f)/2$. Then $(2^l - n)$ applications of (13) lead to $\deg a_{2^l} < 2^l(\deg f)/2$, a contradiction.

This and (11) yield the desired result. □ □

Assume *(a)*. We have already seen that K is the full constant field of $F|K$. Clearly, F is generated by its units as a $K[x]$-module. Now Lemma 4 implies that $\deg f$ is even, that the unit group $\mathcal{O}_F^*$ is of rank 1, and that a fundamental unit is of the form $a(x) + y$, for some $a \in K[X]$.

Let a_n, b_n be as in Lemma 5. Then all units of $\mathcal{O}_F$ are given by

$$\lambda(a_n(x) + b_n(x)y), \quad \text{and} \quad \lambda(a_n(x) - b_n(x)y), \tag{14}$$

for $\lambda \in K^*$ and non-negative integers n. Every element of $K[x]$ is a sum of units and can thus be written as a K-linear combination of the $a_n(x)$. Since the degrees of all a_n are different from each other, and all divisible by $(\deg f)/2$, it follows that the degree of every polynomial in $K[X]$ is divisible by $(\deg f)/2$ as well, whence $\deg f = 2$. Therefore, the genus of $F|K$ is 0. It remains to show that the infinite place of $K(x)$ splits into two places of $F|K$. Let S be the set of places of $F|K$ lying over the infinite place of $K(x)$. Then $\mathcal{O}_F = \mathcal{O}_S$, the ring of S-integers of F. By Proposition 14.2 from [16], the unit group $\mathcal{O}_S^*$ is of rank $|S| - 1$. We already know that the rank of $\mathcal{O}_F^*$ is 1, hence the infinite place of $K(x)$ splits into two places of $F|K$.

3.2.2 Characteristic 2

The only thing left to consider is the case where K is of characteristic 2. We have already seen that K is the full constant field of $F|K$. Let g be the genus of $F|K$ and assume that

$$g > 0 \tag{15}$$

or that

$$\text{the infinite place of } K(x) \text{ is inert or ramified in } F|K. \tag{16}$$

We need to show that not every element of $\mathcal{O}_F$ is a sum of units. This is true if (16) holds. Indeed, we have already seen that, by Dirichlet's unit theorem, the unit group $\mathcal{O}_F^*$ is of rank $s-1$, where s is the number of places of $F|K$ lying over the infinite place of $K(x)$. If there is only one such place then this rank is 0, whence the unit group $\mathcal{O}_F^*$ only consists of torsion elements. Then $u(\mathcal{O}_F) = \infty$, since the torsion subgroup of $\mathcal{O}_F^*$ is exactly K^*, the group of non-zero constants.

Assume from now on that (15) holds and (16) does not hold. Then $F|K(x)$ must be a separable extension, since otherwise it is purely inseparable (as it is of degree 2) and therefore every place is ramified. Separable quadratic extension fields F of $K(x)$ with full constant field K and of genus $g > 0$, such that the infinite place of $K(x)$ splits in $F|K$, can always be written as $F = K(x, y)$, for some $y \in F$ that satisfies an equation

$$y^2 + B(x)y + C(x) = 0, \tag{17}$$

with polynomials B, $C \in K[X] \setminus \{0\}$ having the following properties: The polynomial B is monic, and every prime factor of B is a simple prime factor of C. Moreover, we have $\deg B = g+1$ and $\deg C < 2g+2$. This is a slightly modified version [13, Theorem 1] of the Hasse normal form for Artin-Schreier extensions [10, p. 38].

Let us first show that $\mathcal{O}_F = K[x, y]$. This holds if the affine curve given by (17) is non-singular. Let

$$B = \prod_{i=1}^{r} B_i^{n_i}$$

be the prime factor decomposition of B, with pairwise distinct monic irreducible polynomials $B_i \in K[X]$. Then the polynomial C is of the form

$$C = D \prod_{i=1}^{r} B_i,$$

with some non-zero polynomial $D \in K[X]$ that is not divisible by any B_i. Put $G = Y^2 + B(X)Y + C(X) \in K[X, Y]$. The partial derivatives of G are

$$G_X = B'(X)Y + C'(X) \quad \text{and} \quad G_Y = B(X).$$

Suppose that there are elements a, b in some algebraic extension of K, such that $G(a, b) = G_X(a, b) = G_Y(a, b) = 0$. Since $B(a) = 0$, there is some $1 \leq k \leq r$ with $B_k(a) = 0$. Therefore, $C(a) = 0$, and thus $b = 0$. Then $G_X(a, 0) = 0$ implies

$$0 = C'(a) = D'(a) \prod_{i=1}^{r} B_i(a) + D(a) \sum_{i=1}^{r} B_i'(a) \prod_{j \neq i} B_j(a) = D(a) B_k'(a) \prod_{j \neq k} B_j(a).$$

However, since D, B_k', and all B_j, for $j \neq k$, are relatively prime to B_k, the above product is not 0, a contradiction. Therefore, the affine curve given by (17) is non-singular, and $\mathcal{O}_F = K[x, y]$.

Note that the conjugate of y over $K(x)$ is $y + B(x)$. The following lemmata use the notation established in (17). The first one is the analogous result of Lemma 4.

Lemma 6. *The ring of integers $\mathcal{O}_F$ is generated by units as a $K[x]$-module if and only if there is some $\mu \in K^*$ such that the polynomial $Y^2 + B(x)Y + C(x) + \mu \in K[x][Y]$ has a root in $K[x]$.*

In this case, the unit group $\mathcal{O}_F^*$ is of rank 1, and there is some polynomial $a \in K[X]$ such that $a(x) + y$ is a fundamental unit.

Proof. The proof is similar to the proof of Lemma 4. Assume first that there is some $\mu \in K^*$ and a root $a(x) \in K[x]$ of $Y^2 + B(x)Y + C(x) + \mu$. Then

$$(a(x) + y)(a(x) + B(x) + y) = a(x)^2 + a(x)B(x) + C(x) = \mu \in K^*,$$

whence $a(x) + y$ is a unit of $K[x, y] = \mathcal{O}_F$. Therefore, $y = (a(x) + y) + a(x) \cdot 1$ is a $K[x]$-linear combination of units. Since $\mathcal{O}_F$ is generated by $\{1, y\}$ as a $K[x]$-module, it is generated by its units as a $K[x]$-module.

Now assume that the ring of integers $\mathcal{O}_F$ is generated by its units as a $K[x]$-module. The same argument as in the proof of Lemma 4 shows that the unit group $\mathcal{O}_F^*$ is of rank 1, and that there is a fundamental unit $a(x) + b(x)y$, with polynomials a, $b \in K[X]$, b monic. Every element of $\mathcal{O}_F^*$ is of the form

$$\lambda(a(x) + b(x)y)^n,$$

with $\lambda \in K^*$ and $n \in \mathbb{Z}$. Since the norm of $a(x) + b(x)y$ is in K^*, we have

$$(a(x) + b(x)y)^{-1} = \kappa(a(x) + b(x)B(x) + b(x)y),$$

for some $\kappa \in K^*$. Let us express y as a $K[x]$-linear combination of units:

$$y = g_0(x) + \sum_{i=1}^{k_1} g_i(x)(a(x)+b(x)y)^{n_i} + \sum_{i=1}^{k_2} h_i(x)(a(x)+b(x)B(x)+b(x)y)^{m_i},$$

with positive integers k_1, k_2, n_i, m_i, and polynomials g_i, $h_i \in K[X]$. By comparing the coefficient of y, we get $b(x) \in K[x]^* = K^*$, whence $b = 1$. Since the norm of $a(x) + y$ is some $\mu \in K^*$, we have

$$\mu = (a(x)+y)(a(x)+B(x)+y) = a(x)^2 + a(x)B(x) + C(x),$$

as desired. □ □

Next, we prove an analogue of Lemma 5.

Lemma 7. *Let $a \in K[X]$, such that $a(x) + y$ is a unit of $\mathcal{O}_F$. For any non-negative integer n, define polynomials a_n, $b_n \in K[x]$ via $a_n(x) + b_n(x)y := (a(x)+y)^n$. Then we have, for every positive integer n,*

$$\deg a_n \le n \deg B \quad \textit{and} \quad \deg b_n = (n-1)\deg B. \tag{18}$$

Proof. Induction on n proves that a_n, b_n are given by the recursive formulas

$$a_{n+1} = aa_n + b_nC \quad \text{and} \quad b_{n+1} = ab_n + a_n + b_nB, \tag{19}$$

with starting values $a_0 = 1$, $b_0 = 0$.

Since $\deg C < 2g + 2 = 2\deg B$, and

$$a(x)^2 + B(x)a(x) + C(x) = (a(x)+y)(a(x)+B(x)+y) = N(a(x)+y) \in K^*, \tag{20}$$

we get $\deg a \le \deg B$.

First consider the case where $\deg a < \deg B$. Then $\deg C = \deg B + \deg a$. We use induction to prove the following (in)equalities for every positive integer n:

$$\deg a_n < \deg b_n + \deg B \quad \text{and} \quad \deg b_{n+1} = \deg b_n + \deg B. \tag{21}$$

First one checks (21) directly for $n = 1$. Assume that both (in)equalities hold for n. Then we have $a_{n+1} = aa_n + b_nC$, and $\deg a + \deg a_n < \deg a + \deg b_n + \deg B = \deg b_n + \deg C$. Therefore,

$$\begin{aligned}\deg a_{n+1} &= \deg b_n + \deg C = \deg b_n + \deg a + \deg B\\ &= \deg b_{n+1} + \deg a < \deg b_{n+1} + \deg B.\end{aligned}$$

Similarly,

$$\deg b_{n+2} = \deg(ab_{n+1} + a_{n+1} + b_{n+1}B) = \deg b_{n+1} + \deg B.$$

The desired result (18) now follows by induction from (21).

Now assume that $\deg a = \deg B$. From (20), we have $\deg(a^2 + aB) = \deg C < 2 \deg B$, and thus $\deg(a + B) < \deg B = \deg a$. This time, we prove the following equalities for all positive integers n:

$$\deg a_n = \deg a_{n-1} + \deg a \quad \text{and} \quad \deg b_n = \deg a_{n-1}. \tag{22}$$

Again, we check the case $n = 1$ directly. Assume (22) holds for n. Then

$$\deg b_{n+1} = \deg((a + B)b_n + a_n) = \deg a_n,$$

since $\deg((a+B)b_n) < \deg a+\deg b_n = \deg a+\deg a_{n-1} = \deg a_n$. Moreover,

$$\deg a_{n+1} = \deg(aa_n + b_nC) = \deg a_n + \deg a,$$

since $\deg b_n + \deg C = \deg a_n - \deg a + \deg C < \deg a_n + \deg a$.

From the first equality of (22), we deduce inductively that $\deg a_n = n \deg B$, whence the second equality of (22) implies $\deg b_n = (n - 1) \deg B$.

□ □

Suppose that every element of $\mathcal{O}_F$ is a sum of units. Let $a(x) + y$ be the fundamental unit from Lemma 6, and a_n, b_n the polynomials from Lemma 7. Then all units of $\mathcal{O}_F$ are of the form

$$\lambda(a_n(x) + b_n(x)y), \quad \text{or} \quad \lambda(a_n(x) + b_n(x)B(x) + b_n(x)y),$$

for constants $\lambda \in K^*$ and non-negative integers n. Since the degrees of the b_n are all distinct from each other, the only way to represent elements of $K[x]$ as sums of units is as K-linear combinations of the

$$(a_n(x) + b_n(x)y) + (a_n(x) + b_n(x)B(x) + b_n(x)y) = b_n(x)B(x).$$

Since $\deg(b_nB) = n \deg B$, and $\deg B = g+1 > 1$, there is no way to represent x as such a linear combination, which is a contradiction. This completes our proof.

Added in proof: There is a simpler way to prove that *(a)* implies *(b)* in Theorem 2, which the author was not aware of when submitting this article. We sketch the argument here:

Suppose that $u(\mathcal{O}_F) = \omega$. By Dirichlet's unit theorem, the torsion-free part of the unit group of $\mathcal{O}_F$ is of rank at most 1. Since $\mathcal{O}_F$ is generated by its units as a ring, the rank is 1. It follows that

$$\mathcal{O}_F = K[\varepsilon, \varepsilon^{-1}],$$

for some fundamental unit $\varepsilon \in \mathcal{O}_F$. Since the quotient field of $\mathcal{O}_F$ is F, we get $F = K(\varepsilon)$, which shows that $F|K$ is of genus 0 and has full constant field K. The fact that the infinite place of $K(x)$ splits into two places of $F|K$ follows in the same way as in Section 3.

The proof shown in Section 3, while being significantly longer and more technical than the above argument, has its own merits, especially Lemmata 4 and 6, which show an additional function field analogy of the unit sum number problem in number fields.

Acknowledgements

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

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] W. D. Brownawell and D. W. Masser. Vanishing sums in function fields. *Math. Proc. Camb. Philos. Soc.*, 100(3):427–434, 1986.

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

[8] B. Goldsmith, S. Pabst, and A. Scott. Unit sum numbers of rings and modules. *Q. J. Math.*, 49(195):331–344, 1998.

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

[10] H. Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *J. reine angew. Math.*, 172:37–54, 1935.

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

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

[13] D. Le Brigand. Real quadratic extensions of the rational function field in characteristic two. In *Arithmetic, geometry and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 143–169. Soc. Math. France, Paris, 2005.

[14] R. C. Mason. Norm form equations. I. *J. Number Theory*, 22(2):190–207, 1986.

[15] R. C. Mason. Norm form equations. III. Positive characteristic. *Math. Proc. Camb. Philos. Soc.*, 99(3):409–423, 1986.

[16] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

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

[18] H. Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

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

[20] D. Zelinsky. Every linear transformation is a sum of nonsingular ones. *Proc. Am. Math. Soc.*, 5:627–630, 1954.

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

Technische Universität Graz
Institut für Analysis und Computational Number Theory
Steyrergasse 30, 8010 Graz, Austria
E-mail: frei@math.tugraz.at
`http://www.math.tugraz.at/~frei`

Sums of units in function fields II - The extension problem

Christopher Frei

Abstract

In 2007, Jarden and Narkiewicz raised the following question: Is it true that each algebraic number field has a finite extension L such that the ring of integers of L is generated by its units (as a ring)? In this article, we answer the analogous question in the function field case.

More precisely, it is shown that for every finite non-empty set S of places of an algebraic function field $F|K$ over a perfect field K, there exists a finite extension $F'|F$, such that the integral closure of the ring of S-integers of F in F' is generated by its units (as a ring).

1 Introduction

In their paper [7], Jarden and Narkiewicz proved that, for every finitely generated integral domain R of characteristic 0 and every positive integer N, there exists an element of R that can not be written as a sum of at most N units. This also follows from a result obtained by Hajdu [6], and applies in particular to the case where R is a ring of integers of an algebraic number field. The author recently showed an analogous result for the case where R is a ring of S-integers of an algebraic function field of one variable over a perfect field [4].

A related question is whether or not a ring R is generated by its units. If we take R to be a ring of integers of an algebraic number or function field, both possibilities occur. Complete classifications have been found in many special cases, including rings of integers of quadratic number fields [1, 2] and

Accepted for publication by Acta Arith.

2010 *Mathematics Subject Classification*: Primary 11R58; Secondary 11R27.

Key words and phrases: function field, sums of units, generated by units

certain types of cubic and quartic number fields [3, 11, 13], and rings of S-integers of quadratic function fields [4]. All of these results have in common that the unit group of the ring in question is of rank 1. The author is not aware of any general results for rings of integers whose unit groups have higher rank.

Among other problems, Jarden and Narkiewicz asked the following question, which was later called the extension problem.

Problem 1. *[7, Problem 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.*

This is of course true for finite abelian extensions of $\mathbb{Q}$, since those are contained in cyclotomic number fields by the Kronecker-Weber theorem, and the ring of integers of a cyclotomic number field is generated by a root of unity. The scope of this paper is an affirmative answer to the function field version of Problem 1. Let us fix some basic notation before we state the theorem.

Regarding function fields, we use the notation from [9] and [10]. In particular, an algebraic function field over a field K is a finitely generated extension $F|K$ of transcendence degree 1. The algebraic closure of K in F is called the (full) constant field of $F|K$. An element $t \in F$ is called a separating element for $F|K$, if the extension $F|K(t)$ is finite and separable. Following [10], we regard the places P of $F|K$ as the maximal ideals of discrete valuation rings $\mathcal{O}_P$ of F containing K. In particular, the places correspond to (surjective) discrete valuations $v_P : F \to \mathbb{Z} \cup \{\infty\}$ of F over K. Let n be a positive integer. We say that a place P of $F|K$ is a zero of an element $f \in F$ of order n, if $v_P(f) = n > 0$, and P is a pole of f of order n, if $v_P(f) = -n < 0$. If S is a finite set of places of $F|K$ then the ring $\mathcal{O}_S$ of S-integers of F is the set of all elements of F that have no poles outside of S. Moreover, we write $K^\times := K \smallsetminus \{0\}$.

Theorem 2. *Let K be a perfect field, $F|K$ an algebraic function field over K, and $S \neq \emptyset$ a finite set of places of $F|K$. Let $\mathcal{O}_S$ be the ring of S-integers of F. Then there exists a finite extension $F'|F$ such that the integral closure of $\mathcal{O}_S$ in F' is generated by its units (as a ring).*

The basic idea to prove Theorem 2 is the following: First, choose a finite set $\{t, t_1, \ldots, t_n\}$ of generators of $\mathcal{O}_S$ over K. Then, for each $1 \leq i \leq n$, iteratively construct a finite extension $F_i|F$ such that

(I.) t, t_1, …, t_i are sums of units in the integral closure of $\mathcal{O}_S$ in F_i, and

(II.) the integral closure of $\mathcal{O}_S$ in F_i is generated by units as a ring extension of $\mathcal{O}_S$.

Then the integral closure of $\mathcal{O}_S$ in F_n is generated by units and sums of units as an extension of K, thus it is generated by its units. Section 2 provides the tools to construct the extension fields F_i. In Section 3, everything is put together.

2 Auxiliary results

The following lemma illustrates the idea explained at the end of the introduction.

Lemma 3. *Let K be a perfect field not of characteristic 2 and $a \in K^\times$. Consider the extension of rational function fields $K(x)|K(t)$, where $t = x + a^2/x$. Then the integral closure of $K[t]$ in $K(x)$ is $K[x, x^{-1}]$, which is generated (as a ring) by its units.*

The only places of $K(t)$ that are ramified in $K(x)$ are the zeros of $t - 2a$ and $t + 2a$, both with ramification index 2.

Proof. The minimal polynomial of x over $K(t)$ is $X^2 - tX + a^2$, whence $K(x) = K(t, y)$, with $y^2 = t^2 - 4a^2$. (Here we used the assumption that K is not of characteristic 2.) One can verify the assertions about ramification directly or use Proposition III.7.3 from [10].

Obviously, x and x^{-1} are integral over $K[t]$, and $K[t] \subseteq K[x, x^{-1}]$. Since $K[x, x^{-1}]$, as a ring of fractions of the principal ideal domain $K[x]$, is integrally closed, it is the integral closure of $K[t]$ in $K(x)$. Obviously, x, x^{-1} and all elements of $K^\times$ are units in $K[x, x^{-1}]$, and the lemma is proved. □

The main step in the construction of the extension fields F_i is carried out in the following proposition, which is the most important component of our proof of Theorem 2.

Proposition 4. *Let K be a perfect field not of characteristic 2, $F|K$ an algebraic function field with full constant field K, t a separating element of $F|K$, and $\mathcal{O}$ the integral closure of $K[t]$ in F. Assume that there is some $a \in K^\times$ such that the zeros of $t + 2a$ and $t - 2a$ in $K(t)$ are unramified in $F|K(t)$.*

Let $F' := F(x)$, where x is a root of the polynomial $f := X^2 - tX + a^2$, and let $\mathcal{O}'$ be the integral closure of $K[t]$ in F'. Then K is the full constant field of $F'|K$, x is a unit in $\mathcal{O}'$, $t = x + a^2/x$, and $\mathcal{O}' = \mathcal{O}[x]$.

Proof. The roots of $f \in \mathcal{O}[X]$ in F' are x and a^2/x, whence x is a unit in $\mathcal{O}'$. Obviously, $t = x + a^2/x$. If f is reducible over F then $x, a^2/x \in \mathcal{O}$, and the proposition holds trivially. Assume now that f is irreducible over F.

The field F' is the compositum of F and $K(x)$. Since the characteristic of K is not 2, the extension $F'|F$, and thus as well $F'|K(t)$ is separable. By Lemma 3, the only places of $K(t)$ that are ramified in $K(x)$ are the zeros of $t-2a$ and $t+2a$, both with ramification index 2.

Let P be a zero of $t+2a$ or $t-2a$ in $F'|K$. By Abhyankar's lemma (see, for example, Proposition III.8.9 from [10]), the ramification index of P over $K(t)$ is 2. Here, we used the assumption that the zeros of $t-2a$ and $t+2a$ in $K(t)$ are unramified in the extension $F|K(t)$. Therefore, the ramification index of P over F is 2.

Again by Abhyankar's lemma, every place Q of $F'|K$ that is not a zero of $t+2a$ or $t-2a$ is unramified over F.

Since there are ramified places in the extension $F'|F$, it is not a constant field extension, so K is the full constant field of $F'|K$.

We are left with the task of proving that $\mathcal{O}'=\mathcal{O}[x]$. Denote the different of $\mathcal{O}'|\mathcal{O}$ by $\mathfrak{D}$, and let $\delta(x)$ be the different of x, that is $\delta(x)=f'(x)=2x-t$. It is well known that $\mathcal{O}'=\mathcal{O}[x]$ if and only if $\mathfrak{D}$ is the principal ideal of $\mathcal{O}'$ generated by $\delta(x)$ (see, for example, Theorem V.11.29 from [12]).

Already knowing all ramification indices in the extension $F'|F$, we see that the different $\mathfrak{D}$ of $\mathcal{O}'|\mathcal{O}$ is the product of all prime ideals of $\mathcal{O}'$ dividing $(t+2a)$ or $(t-2a)$ (use, for example, Theorem III.2.6 from [8] and the assumption K is not of characteristic 2).

Since

$$\delta(x)^2=(2x-t)^2=t^2-4a^2=(t+2a)(t-2a),$$

the ideal of $\mathcal{O}'$ generated by $\delta(x)$ satisfies

$$(\delta(x))^2=\prod_{\mathfrak{P}|(t\pm 2a)}\mathfrak{P}^2=\left(\prod_{\mathfrak{P}|(t\pm 2a)}\mathfrak{P}\right)^2=\mathfrak{D}^2.$$

Here, $\mathfrak{P}$ ranges over all prime ideals of $\mathcal{O}'$ dividing $(t+2a)$ or $(t-2a)$. As we have already seen, the ramification index of each such $\mathfrak{P}$ over the prime ideal $(t+2a)$ [or $(t-2a)$] of $K[t]$ is 2. By unique ideal factorization, the ideal of $\mathcal{O}'$ generated by $\delta(x)$ is $\mathfrak{D}$. □

For function fields of characteristic 2, we use a slightly modified form of Proposition 4.

Proposition 5. *Let K be a perfect field of characteristic 2, $F|K$ an algebraic function field with full constant field K, t a separating element of $F|K$, and $\mathcal{O}$ the integral closure of $K[t]$ in F. Assume that there is some $a\in K$ such that the zero of $t+a$ in $K(t)$ is unramified in $F|K(t)$.*

Let $F' := F(x)$, where x is a root of the polynomial $f := X^2+(t+a)X+1$, and let $\mathcal{O}'$ be the integral closure of $K[t]$ in F'. Then K is the full constant field of $F'|K$, x is a unit in $\mathcal{O}'$, $t = x + 1/x + a$, and $\mathcal{O}' = \mathcal{O}[x]$.

Proof. Again, x is a unit in $\mathcal{O}'$, since x and $1/x$ are the roots of the monic polynomial $f \in \mathcal{O}[X]$. Clearly, $t = x + 1/x + a$. The proposition holds again trivially if f is reducible over F. Assume from now on that f is irreducible over F.

Putting $y := x/(t+a)$, we get $F' = F(x) = F(y)$ and $y^2 + y = 1/(t+a)^2$. We use Proposition III.7.8 from [10] to prove that the only places of $F|K$ that are ramified in F' are the zeros of $t + a$. Indeed, for each such zero P, we have

$$v_P\left(1/(t+a)^2 - (1/(t+a)^2 - 1/(t+a))\right) = v_P(1/(t+a)) = -1,$$

since P is unramified over $K(t)$. For each place Q of $F|K$ that is not a zero of $t + a$, we have

$$v_Q(1/(t+a)^2) \geq 0.$$

Therefore, Proposition III.7.8 from [10] implies that the places of $F|K$ that are ramified in F' are exactly the zeros of $t + a$, and that the respective ramification indices and different exponents are 2. We conclude that K is the full constant field of $F|K$ and that the different $\mathfrak{D}$ of $\mathcal{O}'|\mathcal{O}$ is of the form

$$\mathfrak{D} = \prod_{\mathfrak{P}|(t+a)} \mathfrak{P}^2.$$

Here, $\mathfrak{P}$ ranges over all prime ideals of $\mathcal{O}'$ dividing $(t + a)$. On the other hand, the different of x is $\delta(x) = f'(x) = t + a$, and the ideal of $\mathcal{O}'$ generated by $t + a$ is given by

$$(t+a) = \prod_{\mathfrak{P}|(t+a)} \mathfrak{P}^2 = \mathfrak{D}.$$

Note that the ramification index of every ideal $\mathfrak{P}$ of $\mathcal{O}'$ over the prime ideal $(t+a)$ of $K[t]$ is 2, since $(t+a)$ is unramified in F and the ramification index of $\mathfrak{P}$ over F is 2.

Therefore, $\mathfrak{D} = (\delta(x))$, which suffices to prove that $\mathcal{O}' = \mathcal{O}[x]$. □

The following lemma shows a way to enlarge $\mathcal{O}$, while still maintaining the property that $\mathcal{O}' = \mathcal{O}[x]$ from the previous propositions. The results are probably not new, but the author is not aware of an adequate reference. Recall that, for any place P of an algebraic function field, $\mathcal{O}_P$ denotes the discrete valuation ring with maximal ideal P.

Lemma 6. *Let $F|K$ be an algebraic function field with perfect constant field K, $F'|F$ a finite separable extension, and $x \in F'$ with $F' = F(x)$. Let $S \subseteq T$ be sets of places of $F|K$, and assume that x is integral over $\mathcal{O}_S$. Then we have:*

(a) If $\mathcal{O}_P[x]$ is integrally closed for all $P \notin S$ then $\mathcal{O}_S[x]$ is integrally closed as well.

(b) If $\mathcal{O}_S[x]$ is integrally closed then $\mathcal{O}_T[x]$ is integrally closed as well.

(c) If x is algebraic over K then $\mathcal{O}_T[x]$ is integrally closed.

Proof. Denote the integral closure of $\mathcal{O}_S$ in F' by $\mathcal{O}'$. Clearly, $\mathcal{O}_S[x] \subseteq \mathcal{O}'$. To prove *(a)*, we need to show that $\mathcal{O}_S[x] = \mathcal{O}'$. Let S' be the set of places of $F'|K$ lying over places in S. We have

$$\mathcal{O}' = \bigcap_{P' \notin S'} \mathcal{O}_{P'} = \bigcap_{P \notin S} \bigcap_{P'|P} \mathcal{O}_{P'} = \bigcap_{P \notin S} (\mathcal{O}_P[x]).$$

Here, P' denotes places of $F'|K$ and P denotes places of $F|K$. The third equality follows from the assumption that $\mathcal{O}_P[x]$ is integrally closed and the fact that x is integral over $\mathcal{O}_P$, for all $P \notin S$. Therefore, it is sufficient to show that

$$\bigcap_{P \notin S} (\mathcal{O}_P[x]) = \left(\bigcap_{P \notin S} \mathcal{O}_P \right) [x].$$

Clearly, the right-hand side of the above equality is included in the left-hand side. Now let f be an arbitrary element of $\bigcap_{P \notin S}(\mathcal{O}_P[x])$. Denote the degree $[F' : F]$ by n. Then, for each $P \notin S$, there is some polynomial $g_P \in \mathcal{O}_P[X]$ of degree smaller than n, with $f = g_P(x)$. Since $\{1, x, \ldots, x^{n-1}\}$ is a basis of $F'|F$, all g_P are equal and thus elements of $\left(\bigcap_{P \notin S} \mathcal{O}_P\right) [X]$. This shows the other inclusion.

To prove *(b)*, notice that, for all $P \notin S$, $\mathcal{O}_P$ is the localization of $\mathcal{O}_S$ at the unique prime ideal $\mathfrak{P}$ of $\mathcal{O}_S$ corresponding to the place P. Therefore, $\mathcal{O}_P[x]$ can be seen as ring of fractions of $\mathcal{O}_S[x]$ with denominators in the multiplicative set $\mathcal{O}_S \smallsetminus \mathfrak{P}$. Assume that $\mathcal{O}_S[x]$ is integrally closed. By the above argument, $\mathcal{O}_P[x]$ is integrally closed for all $P \notin S$, in particular for all $P \notin T$, so *(b)* follows from *(a)*.

The special case of *(b)* with $S = \emptyset$ is exactly *(c)*. □

As an immediate consequence of Lemma 6 *(c)* and the primitive element theorem, we get that finite constant field extensions have property (II.) from the overview presented at the end of Section 1 (see also the third paragraph of Remark 6.1.7 from [5] for a more general formulation):

Corollary 7. *Let $F|K$ be an algebraic function field with perfect constant field K, S a set of places of $F|K$, and $K'|K$ a finite extension. Then the integral closure of $\mathcal{O}_S$ in $K'F$ is $K'\mathcal{O}_S$.*

To use Propositions 4 and 5, we need to ensure that we can always find an a as required. This is accomplished by the following lemma.

Lemma 8. *Let $F|K$ be an algebraic function field with perfect constant field K, and $t \in F \setminus K$. Then there is a finite extension $K_0|K$ and an element $a \in K_0^\times$, such that the zeros of $t-a$ and $t+a$ in $K_0(t)$ are unramified in the extension $K_0F|K_0(t)$.*

If F is separable over $K(t)$ then K_0F is separable over $K_0(t)$.

Proof. The first part of the lemma clearly holds if K is infinite, since there are only finitely many ramified places in $F|K(t)$, so we can put $K_0 := K$.

In the general case, consider the algebraic closure $\overline{K}$ of K in some algebraically closed field $\Phi \supseteq F$ and the constant field extension $\overline{K}F|\overline{K}$ of $F|K$. Since $\overline{K}$ is infinite, we find some $a \in \overline{K}$, such that the zeros of $t-a$ and $t+a$ in $\overline{K}(t)$ are unramified in $\overline{K}F$. Put $K_0 := K(a)$. Then the zeros of $t-a$ and $t+a$ in $K_0(t)$ are unramified in K_0F, as desired. Indeed, let $\overline{P}'$ be a place of $\overline{K}F|\overline{K}$ lying over the zero P of, say, $t+a$ in $K_0(t)$. Put $P' := \overline{P}' \cap K_0F$ and $\overline{P} := \overline{P}' \cap \overline{K}(t)$. We know that $\overline{P}'|\overline{P}$ is unramified. From $\overline{P}'|\overline{P}|P$ and the fact that constant field extensions are unramified, it follows that $\overline{P}'|P$ is unramified. Now $\overline{P}'|P'|P$ implies that $P'|P$ is unramified.

The assertion regarding separability holds because if F is separable over $K(t)$ then K_0F is generated over $K_0(t)$ by separable elements. □

3 Proof of Theorem 2

For convenience, let us state the theorem again.

Theorem 2. *Let K be a perfect field, $F|K$ an algebraic function field over K, and $S \neq \emptyset$ a finite set of places of $F|K$. Let $\mathcal{O}_S$ be the ring of S-integers of F. Then there exists a finite extension $F'|F$ such that the integral closure of $\mathcal{O}_S$ in F' is generated by its units (as a ring).*

It is enough to prove Theorem 2 under the assumption that K is the full constant field of $F|K$, since then the general case follows as well.

Denote the characteristic of K by $p \geq 0$, and assume first that $p \neq 2$. We find a separating element t of $F|K$ such that $\mathcal{O}_S$ is the integral closure of $K[t]$ in F. To this end, choose places $Q \in S$ and R, $R' \notin S$ of $F|K$. By the strong approximation theorem, we can find an element $t \in F$ that satisfies the conditions

$$\begin{aligned} v_R(t) &= 1, \\ v_{R'}(t) &= |S| - 1, \\ v_P(t) &= -1, \text{ for all } P \in S \smallsetminus \{Q\}, \text{ and} \\ v_P(t) &\geq 0, \text{ for all places } P \notin S \cup \{R, R'\}. \end{aligned}$$

Since the principal divisor of t has degree 0, it follows that $v_Q(t) < 0$. Therefore, the poles of t are exactly the elements of S. Moreover, t is not a p-th power, since p does not divide $v_R(t) = 1$. It follows that F is separable over $K(t)$ (see, for example, Proposition III.9.2 (d) from [10]) and the integral closure of $K[t]$ in F is exactly $\mathcal{O}_S$.

Choose some non-constant elements $t_1, \ldots, t_n$ of $\mathcal{O}_S$, such that $\mathcal{O}_S = K[t, t_1, \ldots, t_n]$ (for example, let $\{t_1, \ldots, t_n\}$ be an integral basis of $\mathcal{O}_S$ over $K[t]$ and omit a possible constant).

Lemma 8 permits us to find a finite extension $K_0|K$ and some $a \in K_0^\times$, such that the zeros of $t - 2a$ and $t + 2a$ in $K_0(t)$ are unramified in K_0F. By Corollary 7, the integral closure of $\mathcal{O}_S$ in K_0F is $K_0\mathcal{O}_S = K_0[t, t_1, \ldots, t_n]$.

Proposition 4 yields a finite extension $F_0|K_0$ of $K_0F|K_0$, such that t is a sum of units in the integral closure $\mathcal{O}_0$ of $\mathcal{O}_S$ in F_0, and $\mathcal{O}_0 = K_0\mathcal{O}_S[x_0] = K_0[t, t_1, \ldots, t_n, x_0]$, for some unit x_0 of $\mathcal{O}_0$. Moreover, K_0 is the full constant field of $F_0|K_0$.

We inductively construct finite extensions $F_1|K_1$, …, $F_n|K_n$ of $F_0|K_0$ with the following properties. If $\mathcal{O}_i$ denotes the integral closure of $\mathcal{O}_S$ in F_i then we have, for $i \in \{0, \ldots, n\}$:

- $\mathcal{O}_i = K_i[t, s_1, \ldots, s_i, t_{i+1}, \ldots t_n, x_0, x_1, \ldots, x_i]$, where x_0, …, x_i are units of $\mathcal{O}_i$, and for all $1 \leq j \leq i$ there is some m with $s_j^{p^m} = t_j$.

- t, s_1, …, s_i are sums of units of $\mathcal{O}_i$.

- K_i is the full constant field of $F_i|K_i$.

For $i = 0$, the function field $F_0|K_0$ has all desired properties. Let $i \in \{1, \ldots, n\}$ and assume that we have constructed $F_{i-1}|K_{i-1}$. The figure on page 63 shows the relations between the rings and fields constructed in the following paragraphs.

Take the maximal non-negative integer m such that t_i is a p^m-th power in F_{i-1} (the maximum exists since t_i is not constant), and let s_i be the p^m-th root of t_i. Then $s_i \in \mathcal{O}_{i-1}$, since s_i has the same poles as t_i. Therefore, $\mathcal{O}_{i-1} = K_{i-1}[t, s_1, \ldots, s_i, t_{i+1}, \ldots, t_n, x_0, \ldots, x_{i-1}]$.

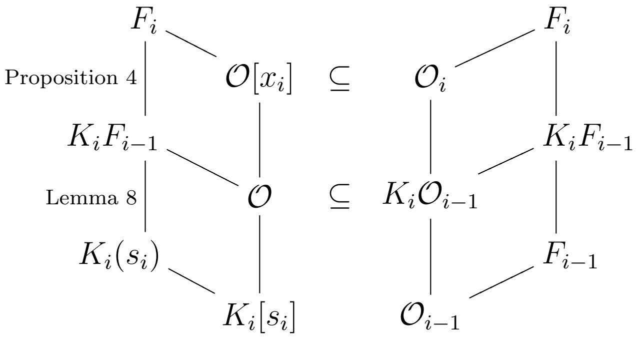

Figure 1: The rings and fields occurring in the induction step.

Since s_i is not a p-th power in F_{i-1}, it is a separating element of $F_{i-1}|K_{i-1}$ (again, we used Proposition III.9.2 (d) from [10]). By Lemma 8, there is some finite extension $K_i|K_{i-1}$ and some $a \in K_i^\times$ such that the zeros of $s_i - 2a$ and $s_i + 2a$ in $K_i(s_i)$ are unramified in K_iF_{i-1}, and K_iF_{i-1} is separable over $K_i(s_i)$.

Denote the integral closure of $K_i[s_i]$ in K_iF_{i-1} by $\mathcal{O}$. By Proposition 4, there is a finite extension $F_i|K_i$ of $K_iF_{i-1}|K_i$, such that the integral closure of $\mathcal{O}$ in F_i is $\mathcal{O}[x_i]$, for some unit x_i, and s_i is a sum of units in $\mathcal{O}[x_i]$. Moreover, K_i is the full constant field of $F_i|K_i$.

By our convention, $\mathcal{O}_i$ is the integral closure of $\mathcal{O}_S$ in F_i, and thus as well the integral closure of $\mathcal{O}_{i-1}$ in F_i. By Corollary 7, the integral closure of $\mathcal{O}_{i-1}$ in K_iF_{i-1} is $K_i\mathcal{O}_{i-1}$. Since $s_i \in \mathcal{O}_{i-1}$, we have $\mathcal{O} \subseteq K_i\mathcal{O}_{i-1}$. Let U be the set of poles of s_i in K_iF_{i-1}, and $V \supseteq U$ the set of poles of t in K_iF_{i-1}. Then $\mathcal{O} = \mathcal{O}_U$ and $K_i\mathcal{O}_{i-1} = \mathcal{O}_V$. Since $\mathcal{O}_U[x_i] = \mathcal{O}[x_i]$ is integrally closed, Lemma 6 *(b)* implies that $\mathcal{O}_V[x_i] = K_i\mathcal{O}_{i-1}[x_i]$ is integrally closed as well. Therefore, $K_i\mathcal{O}_{i-1}[x_i]$ is $\mathcal{O}_i$, the integral closure of $\mathcal{O}_{i-1}$ in F_i. We conclude that

$$\mathcal{O}_i = K_i[t, s_1, \ldots, s_i, t_{i+1}, \ldots, t_n, x_0, \ldots, x_i],$$

as desired. The elements x_0, …, x_{i-1} are units in $\mathcal{O}_i$, because they are units in $\mathcal{O}_{i-1} \subseteq \mathcal{O}_i$. Moreover, x_i is a unit in $\mathcal{O}_i$, since it is a unit in $\mathcal{O}[x_i] \subseteq \mathcal{O}_i$. Therefore, t, s_1, …, s_i are sums of units of $\mathcal{O}_i$, and the induction is complete.

Now put $F'|K' := F_n|K_n$, and Theorem 2 is proved whenever the characteristic of K is not 2. In characteristic 2, the proof is exactly the same as above, except that we always write a instead of $2a$ and use Proposition 5 instead of Proposition 4.

Acknowledgements

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

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] 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.

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

[5] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics.* Springer-Verlag, Berlin, third edition, 2008.

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

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

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

[9] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

[10] H. Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

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

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

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

Christopher Frei
Technische Universität Graz
Institut für Analysis und Computational Number Theory
Steyrergasse 30, 8010 Graz, Austria
E-mail: frei@math.tugraz.at
`http://www.math.tugraz.at/~frei`

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 generalize 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.

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

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

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 [5], [18], [22]. 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 σ_1, …, $\sigma_r : K\to\mathbb{R}$ and $2s$ distinct non-real embeddings σ_{r+1}, …, $\sigma_n : K\to\mathbb{C}$, 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

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

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 $\underline{x}=(x_1,\dots,x_n)\in\mathbb{R}^n$, 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

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

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 $\mathfrak{a}_1$, …, $\mathfrak{a}_k$ 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 $\mathcal{O}_K$,

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

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 $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ 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 $\eta \in \mathcal{O} \setminus K^2$. 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 (([20, 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

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

□

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

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

Therefore,

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

Put

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

and

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

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

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

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])

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

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

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

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,

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

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

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

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

Since

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

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

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

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], [20, Lemma 9.7])

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

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,

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

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

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

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

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

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. □

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

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

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 $\mathfrak{N}\mathfrak{P} \geq 5$ by the hypotheses of the proposition, but f is of degree 2, so $L(\mathfrak{P}) \leq 2$. If $2 \in \mathfrak{P}$ then we have $f \equiv X^2 \mod \mathfrak{P}$, whence $L(\mathfrak{P}) = 1$. On the other hand, $\mathfrak{N}\mathfrak{P} \geq 4$, 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 $\mathfrak{p}_1$, …, $\mathfrak{p}_k$ 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 $\mathfrak{a}\neq\mathcal{O}_K$, and $\mathfrak{a}\cap\mathcal{O}=\mathcal{O}$ if $\mathfrak{a}=\mathcal{O}_K$, since $\mathcal{O}$ is one-dimensional. As all $\mathfrak{p}_i$, $\mathfrak{p}_j$, $i\neq j$, are relatively prime, we get

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

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

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 $\mathfrak{N}\mathfrak{P}\ge 4$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ imply

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

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

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

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

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

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

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, [21, 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 $\eta \in \mathcal{O}_K^* \smallsetminus K^2$. 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 ω_1, …, ω_{i-1} have been chosen. If $\mathcal{O}^U[\omega_1, \dots, \omega_{i-1}] = \mathcal{O}_K$ then stop, otherwise put

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

Let ω_i be an element as in Proposition 4. Then

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

Therefore, the above process stops after $r \leq \log_2([\mathcal{O}_K : \mathcal{O}^U])$ steps, with elements ω_1, …, $\omega_r \in \mathcal{O}_K \smallsetminus \mathcal{O}^U$, such that $\mathcal{O}_K = \mathcal{O}^U[\omega_1, \dots, \omega_r]$. 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 $\{\beta_1, \dots, \beta_l\}$ over K,*
3. *L' has a relative integral basis $\{\beta'_1, \dots, \beta'_{l'}\}$ 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 $L_i := K(\alpha_1, \dots, \alpha_i)$ of K. We claim that L_i has an integral basis over K consisting of (not necessarily all) products of the form

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

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 $K(\alpha_i) \nsubseteq L_{i-1}$ 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 $\mathcal{O}_L = \mathcal{O}_K[\alpha_1, \dots, \alpha_r]$. With (17) and $\omega_i = \alpha_i + \eta\alpha_i^{-1}$, we get

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

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 [19].

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

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. The distribution of integral points in affine space. *in preparation.*

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

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

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

Christopher Frei
Technische Universität Graz
Institut für Analysis und Computational Number Theory
Steyrergasse 30, 8010 Graz, Austria
E-mail: frei@math.tugraz.at
`http://www.math.tugraz.at/~frei`

Curriculum Vitae

Personal information

Dipl.-Ing. Christopher Frei
Technische Universität Graz
Institut für Analysis und Computational Number Theory
Steyrergasse 30/II
8010 Graz
Austria

Telephone: +43 316 873 - 7620
Mobile phone: +43 699 11 22 89 45
E-mail: `frei@math.tugraz.at`
Homepage: `http://www.math.tugraz.at/~frei`

Date of birth: July 22, 1985
Place of birth: Graz, Austria

Education

2009 – now Doctoral program, Technical Mathematics, Graz University of Technology; doctoral thesis under supervision of Prof. Robert Tichy in the area of number theory

2008 – 2009 Master program, Mathematical Computer Science, Graz University of Technology; with honours

2004 – 2008 Bachelor program, Technical Mathematics, Graz University of Technology; with honours

Languages

German, English, French

Teaching Experience

2009 – now Exercise classes in symbolic computation, mathematics for electrical engineering, ordinary differential equations, linear algebra, and mathematical foundations of cryptography, Graz University of Technology

2006 – 2009 Teaching assistant for several mathematical courses, Graz University of Technology

Work Experience

2009 – now Project assistant, Graz University of Technology

2005 – 2007 Development of mathematical school teaching software for the EU-project “Learning Tools for Mathematics”

Attended Schools, Workshops, and Conferences

27th Journées Arithmétiques, Vilnius University, June 27 - July 1, 2011

Winter School Heights and Algebraic Numbers, March 2 - March 4, 2011, Eberhard-Karls-Universität, Tübingen

Rational Points - Theory & Experiment, May 25 - May 29, 2010, ETH Zürich

ESI May Seminar 2010 in Number Theory, May 2 - May 9, 2010, Erwin Schrödinger Institute, Vienna

ÖMG-DMV Congress 2009, September 20 - September 25, 2009, Graz University of Technology

Scientific Talks

27th Journées Arithmétiques, Vilnius University, June 28, 2011

Seminar for Doctorands, Graz University of Technology, March 25, 2011

Zahlentheoretisches Kolloquium, Graz University of Technology, March 11, 2011

Seminar on Number Theory and Algebra, University of Zagreb, November 24, 2010

Seminar for Doctorands, Graz University of Technology, April 30, 2010

Publications

Additive unit representations in global fields - A survey, with Fabrizio Barroero and Robert F. Tichy, submitted, arXiv:1102.0120

On rings of integers generated by their units, submitted, arXiv:1009.0447

Sums of units in function fields II: The extension problem, accepted by Acta Arith.

Sums of units in function fields, Monatsh. Math., DOI: 10.1007/s00605-010-0219-7

Non-unique factorization of polynomials over residue class rings of the integers, with Sophie Frisch, Comm. Algebra 39: 4, 1482-1490, 2011

July 26, 2011