Sums of units in function fields II - The extension problem

Christopher Frei April 26, 2010

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 [5], 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 cannot be written as a sum of at most N units. This 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

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, 9, 11], 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. [5, 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 [7] and [8]. 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 [8], 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.

Theorem 1. 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 1 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, \ldots, 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 1. Let K be a perfect field not of characteristic 2 and $a \in K \setminus \{0\}$. 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 [8].

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 $K \setminus \{0\}$ are units in $K[x, x^{-1}]$, and the lemma is proved. \square

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 1.

Proposition 1. 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 $a \in K \setminus \{0\}$ 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 1, 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 [8]), 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 P 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 29 from [10]).

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 [6] 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 1.

Proposition 2. 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 [8] 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

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

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

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

Therefore, Proposition III.7.8 from [8] 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 2. 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, such 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

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

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 $(\bigcap_{P \notin S} \mathcal{O}_P)[X]$. 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 $\mathcal{O}_S \setminus \mathfrak{P}$. 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 2 (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:

Corollary 1. 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 1 and 2, we need to ensure that we can always find an a as required. This is accomplished by the following lemma.

Lemma 3. 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 $a \in K_0 \setminus \{0\}$, 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 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 1

It is enough to prove Theorem 1 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 some 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

$$v_R(t) = 1,$$

 $v_{R'}(t) = |S| - 1,$
 $v_P(t) = -1,$ for all $P \in S \setminus \{Q\},$ and
 $v_P(t) \ge 0,$ for all places $P \notin S \cup \{R, R'\}.$

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 [8]) 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 3 permits us to find a finite extension $K_0|K$ and some $a \in K_0 \setminus \{0\}$, such that the zeros of t - 2a and t + 2a in $K_0(t)$ are unramified in K_0F . By Corollary 1, 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 1 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 $F_1|K_1, \ldots, F_n|K_n$ 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 $i \in \{0, \ldots, n\}$:

- $\mathcal{O}_i = K_i[t, s_1, \dots, s_i, t_{i+1}, \dots t_n, x_0, x_1, \dots, x_i]$, where x_0, \dots, 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, \ldots, 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 $F_{i-1}|K_{i-1}$. 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, $\mathcal{O}_{i-1} = K_{i-1}[t, s_1, \ldots, s_i, t_{i+1}, \ldots, t_n, x_0, \ldots, x_{i-1}]$.

Since s_i is not a p-th power in F_{i-1} , it is a separating element of $F_{i-1}|K_{i-1}$. By Lemma 3, there is some finite extension $K_i|K_{i-1}$ and some $a \in K_i \setminus \{0\}$ 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 1, 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 $F_i|K_i$.

Recall that \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 1, 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 2 (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

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

as desired. The elements x_0, \ldots, 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, \ldots, 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 1 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 take Proposition 2 instead of Proposition 1.

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. to appear in Monatsh. Math.
- [5] M. Jarden and W. Narkiewicz. On sums of units. *Monatsh. Math.*, 150(4):327–332, 2007.
- [6] J. Neukirch. Algebraic number theory, volume 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999.

- [7] M. Rosen. Number theory in function fields, volume 210 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.
- [8] H. Stichtenoth. Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin, 1993.
- [9] R. F. Tichy and V. Ziegler. Units generating the ring of integers of complex cubic fields. *Colloq. Math.*, 109(1):71–83, 2007.
- [10] O. Zariski and P. Samuel. *Commutative algebra. Vol. 1.* Graduate Texts in Mathematics, No. 28. Springer-Verlag, New York, 1975.
- [11] 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