Computing generators of the tame kernel of a global function field

Annegret Weng*

Johannes Gutenberg-Universität, Fachbereich Mathematik, Staudingerweg 9, 55128 Mainz, Germany

Received 21 June 2004; accepted 22 December 2005
Available online 27 June 2006

Abstract

The group $K_2$ of a curve $C$ over a finite field is equal to the tame kernel of the corresponding function field. We describe two algorithms for computing generators of the tame kernel of a global function field. The first algorithm uses the transfer map and the fact that the $\ell$-torsion can easily be described if the ground field contains the $\ell$th roots of unity.

The second method is inspired by an algorithm of Belabas and Gangl for computing generators of $K_2$ of the ring of integers in a number field.

We finally give the generators of the tame kernel for some elliptic function fields.

Keywords: Algorithmic number theory; K-theory; Global function fields

1. Introduction

Let $k = \mathbb{F}_q$ be the finite field with $q$ elements and let $F/k$ be a function field in one variable, i.e. a finite extension of the rational function field $k(x)$. We assume that $k$ is the full constant field of $F$.

By the Theorem of Matsumoto, we have

$$K_2(F) = F^* \otimes F^*/(g \otimes (1 - g) : g \in F^*, g \neq 1).$$

(In fact, this holds for any field $F$ and can serve as a definition of $K_2(F)$ for a field $F$.)
Let \([g, h]\) denote the image of \(g \otimes h\) in \(K_2(F)\). For any place \(v\) in \(F\) with residue field \(k_v\), we define the tame symbol

\[
K_2(F) \xrightarrow{\partial_v} k_v^* : \quad \partial_v([g, h]) = (-1)^{v(g)v(h)} \frac{g^{v(h)}}{h^{v(g)}} \mod v.
\]

The tame kernel is defined by

\[
\ker_F = \bigcap_v \ker(\partial_v).
\]

The cokernel of \(\prod_v \partial_v\) in \(\prod_v k_v^*\), where the product runs over all places \(v\) in \(F\), has cardinality \(q - 1\) (Moore, 1968). Thus, once we know the tame kernel we also get a description of \(K_2(F)\).

The tame kernel is equal to \(K_2(C)\) where \(C\) is the curve corresponding to \(F\) (Quillen, 1973). More generally, for any finite set \(S\) of places of \(F\) we can define \(\ker_{F,S} = \bigcap_{v \notin S} \ker(\partial_v)\). We then have \(\ker_{F,S} = K_2(\mathcal{O}_S)\) where \(\mathcal{O}_S\) denotes the set of \(S\)-integers in \(F\).

There exist several papers on \(\ker_F\) for \(F\) a number field. Somehow, the function field case seems to be easier (cf. Section 2), but there are some questions which have been answered in the number field case but are still open for function fields.

One of those questions concerns the explicit computation of generators for \(\ker_F\). We discuss two methods for computing generators of \(\ker_F\) (see Sections 3.2 and 5). The first method uses the transfer map and results given by Suslin and Tate. The second method uses the fact that \(\ker_F\) can be generated by elements \(\sum_i \{g_i, h_i\}\) where \(g_i\) and \(h_i\) are \(S\)-units where \(S\) is a finite set of places of bounded degree. This has already been proven by Bass and Tate (1973). They also give an upper bound for the degree \(t\) of the places in \(S\) but it is not completely explicit. We will give an explicit bound for the case where the function field has at least two \(k\)-rational places of degree one and we describe how to compute generators of \(\ker_F\) using ideas by Bass and Tate (1973) and Belabas and Gangl (2004). As examples, we give the generators of \(\ker_F\) for some elliptic function fields.

**Notation.** For the rest of the text we fix the following notation: Let \(k\) be the finite field \(\mathbb{F}_q\) with \(q\) elements and let \(\overline{k}\) be a fixed algebraic closure. We write \(F\) for the global function field of a curve \(C\) of genus \(g\) defined over \(k\). Set \(F_\infty = F\overline{k}\). The group of \(k\)-rational (resp. \(\overline{k}\)-rational) points of the Jacobian \(J\) of \(C\) is denoted by \(J(k)\) (resp. \(J(\overline{k})\)).

### 2. The order and structure of the tame kernel

In contrast to the number field case, the order and structure of the tame kernel of a global function field are much easier to obtain.

By Tate (1970) we have the following theorem.

**Theorem 2.1.** With the notation as introduced above, there exists a non-canonical isomorphism between \(\ker_F\) and the \((1 - \phi q)\)-torsion points in the Jacobian \(J(\overline{k})\) where \(\phi\) is the Frobenius endomorphism on \(J\).

We draw some easy consequences from **Theorem 2.1**. The zeta function of the function field \(F/k\) of a curve \(C\) of genus \(g\) can be written in the form

\[
Z(T) = \frac{L_F(T)}{(1 - T)(1 - qT)}
\]
where \( L_F(T) \in \mathbb{Z}[T] \) is a polynomial of degree \( 2g \). The polynomial \( L_F(T) \) is called the \( L \)-polynomial of the function field \( F \). It factors over \( \mathbb{C} \) in the form

\[
2g \prod_{i=1}^{2g} (1 - \alpha_i T)
\]

where \( \alpha_1, \ldots, \alpha_{2g} \) are algebraic integers satisfying \( |\alpha_i| = \sqrt{q} \). Moreover, \( L_F(1) = \# \ker (1 - \phi : J(\bar{k}) \to J(\bar{k})) = \# J(k) \) where \( J(k) \) is the group of \( k \)-rational points on the Jacobian of \( C \).

The order of the tame kernel, \( \# \ker F \), is now given by

\[
\deg (1 - \phi q) = \prod_{i=1}^{2g} (1 - q \alpha_i) = L_F(q).
\]

We deduce \( \# \ker F \equiv 1 \mod q \).

We can also derive information on the group structure.

**Corollary 2.1.** The group \( \ker F \) of a global function field of genus \( g \) has at most \( 2g \) cyclic factors.

This follows from a well-known fact about the kernel of the multiplication-by-\( m \) map on an abelian variety, in particular on the Jacobian of the curve \( C \).

**Example 2.1.** Let \( F_E \) be the function field of an elliptic curve \( E \). We have \( \#E(\mathbb{F}_q) = q + 1 - t \) where \( t \) is the trace of the Frobenius endomorphism. Then \( L_{F_E}(T) = qT^2 - tT + 1 \) and \( \# \ker_{F_E} = q^3 + 1 - tq \). Therefore, if we know the number of points on the elliptic curve over \( \mathbb{F}_q \), we can determine the order of \( \ker_{F_E} \).

Since an elliptic curve has genus \( g = 1 \) and \( \ker_{F_E} = K_2(\mathcal{O}_{F_E}) \) for \( \mathcal{O}_{F_E} \) the ring of integers, we have

**Lemma 2.1.** Let \( F_E \) be the function field of an elliptic curve defined over \( k = \mathbb{F}_q \). Then

\[
K_2(\mathcal{O}_{F_E}) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}
\]

where \( n_2 \mid n_1 \) and \( n_2 \mid q^3 - 1 \).

**Proof.** We only need to prove that \( n_2 \mid q^3 - 1 \). Let \( \phi \) be the Frobenius endomorphism on \( E \) and for every endomorphism \( \alpha \) of \( E \) let \( E[\alpha] \) be the group of \( \alpha \)-torsion points over the algebraic closure \( \bar{k} \).

We have to show that \( E[n_2] \subset E[\phi q - 1] \) implies \( n_2 \mid q^3 - 1 \).

The endomorphism ring \( \text{End}(E) \) of \( E \) is isomorphic to an order \( \mathcal{O} \) in an imaginary quadratic field or in a quaternion algebra. We identify every endomorphism with its image in \( \mathcal{O} \).

Suppose \( E[n_2] \subset E[\phi q - 1] \). Then \( \phi q - 1 \) must be divisible by \( n_2 \) in \( \mathcal{O} \).

First suppose \( \phi \in \mathbb{Z} \). Then \( n_2 \mid (\phi q - 1)(\phi q + 1) = q^3 - 1 \), since \( \text{Norm}_{\mathcal{O}\otimes \mathcal{O}/\mathbb{Q}}(\phi) = q \).

If \( \phi \not\in \mathbb{Z} \), consider

\[
\text{Tr}(\phi q - 1) = tq - 2 = q^3 - 1 - (q^3 + 1 - tq).
\]

Since \( \#K_2(\mathcal{O}_{F_E}) = q^3 + 1 - tq \) and \( \text{Tr}(\phi q - 1) \) are both divisible by \( n_2 \), the same is true for \( q^3 - 1 \). \( \square \)

To determine the group structure completely we also need some information on the endomorphism ring.
1. Let $E$ be an ordinary (i.e. non-supersingular) elliptic curve defined over $\mathbb{F}_q$ with Frobenius endomorphism $\phi$ and let $E[1 - \phi q]$ be the $(1 - \phi q)$-torsion points of $E$ over a fixed algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. We have

$$E[1 - \phi q] \simeq \text{End}(E)/(1 - \phi q)$$

where $\text{End}(E)$ is the endomorphism ring of $E$. Note that $\text{End}(E)$ can be identified with an imaginary quadratic order, since $E$ is ordinary. Let $f \in \mathbb{Z}$ be the conductor of $\text{End}(E)$, i.e. $\text{End}(E) = \mathbb{Z} + fw\mathbb{Z}$ where $\mathbb{Z} + w\mathbb{Z}$ is the maximal order in $\text{End}(E) \otimes \mathbb{Q}$. We identify $\phi$ with $a + bw$ for some integers $a, b$. Set $d = \gcd(aq - 1, bq)$ and let $d' = \frac{d}{\gcd(f, d)}$. Then $\ker_{F_E}$ is cyclic if and only if $d' = 1$. Otherwise, $\ker_{F_E} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ where $n_2 = d'$ and $n_2 | n_1$.

2. Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_q = \mathbb{F}_{p^r}$, i.e. $(t, q) \neq 1$. By Waterhouse (1969), we can distinguish the following cases:

(a) $t = 0$, $r$ odd or $p \neq 1 \mod 4$,
(b) $t^2 = aq$ where $a = 1, 2, 3$,
(c) $t = 2\sqrt{q}$ if $r$ is even.

For (b), we find that $\ker_{F_E}$ is cyclic. For (a), $\ker_{F_E}$ is either cyclic or has the structure $\mathbb{Z}/(q^2 - 1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In (c), $\ker_{F_E} \simeq \mathbb{Z}/(q\sqrt{q} - 1)\mathbb{Z} \times \mathbb{Z}/(q\sqrt{q} - 1)\mathbb{Z}$. The proof is analogous to the proof of Lemma 4.8 in Schoof (1987).

3. A first algorithm for computing generators

We use the notation introduced at the end of Section 1.

3.1. Elements of small order

For every endomorphism $\alpha$ let $J[\alpha]$ be the group of $\alpha$-torsion points in $J(\bar{k})$. The elements in $\ker_F$ of order $n$ | $(q - 1)$ can be described easily.

**Theorem 3.1.** Let $\ell$ be a prime divisor of $q - 1$. Then $J(k)$ and $\ker_F$ have the same number of $\ell$-torsion points.

**Proof.** If $q - 1 \equiv 0 \mod \ell$, then $1 - \phi q \equiv 1 - \phi \mod \ell$. The assertion follows since the structure of the group of $\ell$-torsion points in $J[1 - \phi]$ (resp. $J[1 - \phi q]$) does only depend on $\phi - 1 \mod \ell$ (resp. $\phi q - 1 \mod \ell$). □

We recall the following theorem from Tate (1976), Suslin (1987):

**Theorem 3.2.** Suppose $F$ contains a primitive $n$th root of unity $\zeta_n$.

1. Then each element of $K_2(F)$ of order $n$ can be represented by a symbol $\{\zeta_n, f\}$ with $f \in F^*$.
2. We have $\{\zeta_{n^k}, f\} = 1$ if and only if $f = cg^{n^k}$ for some $c \in k^*$ and $g \in F^*$.

By induction on the number of different prime factors of $n$ we can extend Theorem 3.2(2).

**Corollary 3.1.** Let $F$ be the function field of a curve $C$ defined over a finite field $k$ containing a primitive $n$th root of unity $\zeta_n$. Then $\{\zeta_n, f\} = 1$ if and only if $f = cg^n$ for some $c \in k^*$ and $g \in F^*$.

We can now give a description of the $n$-torsion elements in $\ker_{F_\infty}$ with $(n, q) = 1$ which allows us to deduce information on the $n$-torsion elements in $\ker_F$ for $n | (q - 1)$. 

Corollary 3.2. For \((n, q) = 1\), we identify \(J[n]\) with a set of \(\bar{k}\)-rational divisors \(\{D_1, \ldots, D_{n^2}\}\) of degree 0 of order \(n\) in the divisor class group of degree 0. Let \(f_i \in F_\infty\) such that \(nD_i = (f_i)\) and let \(\zeta_n \in F_\infty\) be a primitive \(nth\) root of unity.

Then the elements \(\{\zeta_n, f_i\}\) represent different \(n\)-torsion elements in \(\ker F_\infty\) and every \(n\)-torsion element can be represented by such a symbol.

Proof. From Corollary 2.1 and the fact that \(F_\infty\) has an algebraically closed constant field we deduce that \(\ker F_\infty[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}\). Hence, it is enough to show that we can reduce each symbol in \(\ker F_\infty\) to a symbol of the form \(\{\zeta_n, h\}\) for some \(h \in F\) to a symbol of the form \(\{\zeta_n, f_i\}\) where \(nD_i = (f_i)\).

If \(\{\zeta_n, h\} \in \ker F_\infty\) then \(\langle h \rangle = n \sum n_P P\) where \(\sum n_P P\) is a formal sum of \(\bar{k}\)-rational points \(P\) on \(C\) and the divisor \(\sum n_P P\) is an element of order \(n\) in the divisor class group of degree zero. The element is non-trivial if and only if \(\sum n_P P\) is a non-trivial \(n\)-torsion point. Hence, there exists some \(D_i\) such that \(\sum n_P P\) is linearly equivalent to \(D_i\), i.e. there exists a function \(h'\) with \((h') = \sum n_P P - D_i\). We have

\[\{\zeta_n, h\} = \{\zeta_n, f_i\} \cdot \left\{\zeta_n, \frac{h}{f_i}\right\} = \{\zeta_n, f_i\}\{\zeta_n, h^\prime\} = \{\zeta_n, f_i\}.\]

Now suppose that \(n\) divides \((q - 1)\) and \(\ker F\). In this case, we have \(L_F(1) \equiv L_F(q) \equiv 0 \mod n\). Hence, there exist an \(n\)-torsion element \(D\) in \(J(k)\) and a function \(f \in F\) such that \(nD = (f)\). Since \(D\) is non-trivial, \(f\) cannot be written in the form \(cg^n\) for some \(c \in k^*, g \in F^*\) and \(n \in \mathbb{N}\). We can construct a non-trivial \(n\)-torsion element \(\{\zeta_n, f\} \in \ker F\) where \(\zeta_n\) is a primitive \(n\)th root of unity in \(F\).

3.2. Computing generators via the transfer

From Corollary 3.2 we can already derive an algorithm for computing the generators for \(\ker F\).

For a finite constant field extension \(E/F\) let \(\text{tr}_{E/F} \) be the transfer \(K_2(E) \to K_2(F)\) (for the definition see Bass and Tate (1973), Chapter I, Section 5).

Lemma 3.1. Let \(\ell \neq 2\) be a prime. Suppose \(\ell \mid \#\ker F\). Let \(m\) be the smallest integer such that \(\ell \mid q^m - 1\). Then \(\ell \mid \#J(\mathbb{F}_{q^m})\). Furthermore, putting \(E = F\mathbb{F}_{q^m}\), there exists an \(\ell\)-torsion element \(\beta \in \ker E\) such that \(\text{tr}_{E/F}(\beta)\) is a non-trivial \(\ell\)-torsion element in \(\ker F\).

Proof. Let \(L_E\) be the \(L\)-polynomial of \(E\). Since \(q^m \equiv 1 \mod \ell\) we have

\[L_E(1) = L_E(q^m) \equiv 0 \mod \ell\]

and \(\#J(\mathbb{F}_{q^m})\) contains a non-trivial \(\ell\)-torsion element.

Let \(\alpha\) be a non-trivial \(\ell\)-torsion element of \(\ker F\). Since \(K_2(E) = K_2(F)^G\) (where \(G = \text{Gal}(F/E) \cong \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\) is the Galois group of the field extension \(F/E\), seeSuslin (1987), Corollary 5.3),\(\alpha\) can be identified with some \(\ell\)-torsion element \(\beta\) in \(K_2(E)\). We have \(\text{tr}_{E/F}(\beta) = \alpha^{|E:F|} = \alpha^m\). Now since \(m\) is chosen to be minimal, \(m\) is the order of \(q\) modulo \(\ell\). Hence \((m, \ell) = 1\) and \(\alpha^m\) is an element of precise order \(\ell\).

If \(\ell \mid q^m - 1\), we even have \(\phi - 1 \equiv \phi q^m - 1 \mod \ell\) in the endomorphism algebra of the Jacobian \(J(\mathbb{F}_{q^m})\). Hence, we can construct all \(\ell\)-torsion elements in \(K_2(E)\) using Corollary 3.2. Together with the transfer this gives us an algorithm for computing \(\ell\)-torsion elements in \(\ker F\).

There exists an algorithm for computing the transfer given by Rosset and Tate (1983). Unfortunately, the integer \(m\) is usually very large and the presentation of the elements in \(K_2(F)\) or \(\ker F\) becomes huge. We give an example in Section 6.
4. Bounds for computing the tame kernel

Let $F/k$ be a function field in one variable of genus $g \geq 1$. We assume that $F$ has at least two $k$-rational places of degree one. Let $v_\infty, v_2$ be such places of minimal norm, in particular $\deg(v_\infty) = \deg(v_2) = 1$.

In this section we determine a bound $t$ such that ker$_F$ can be given by elements of the form $\sum_i \{f_i, g_i\}$ where $f_i, g_i$ are S-units for the finite set $S$ of all places in $F$ of degree $\leq t$.

Let $S$ be such a set of cardinality $j$ containing the places $v_1 = v_\infty$ and $v_2, \ldots, v_j$ and let $S' = S \cup \{v\}$ for $v \notin S$. We denote the set of $S$-units (resp. $S'$-units) by $U$ (resp. $U'$).

As in the number field case (cf. Groenewegen (2004)), we set

$$K = (U \otimes U)/\langle a \otimes b : a, b \in U, a + b = 1 \text{ or } a + b = 0 \rangle$$

and

$$K' = (U' \otimes U')/\langle a \otimes b : a, b \in U', a + b = 1 \text{ or } a + b = 0 \rangle.$$ 

Let Im $K$ be the image of $K$ in $K'$.

The tame symbol $\partial_v$ induces a map $K'/\text{Im } K \rightarrow k_v^\times$. Then ker$_F$ is generated by certain $\sum_i \{f_i, g_i\}$ with $f_i, g_i \in U$ if this map is an isomorphism for all $v$ with $v \notin S$. Let $S$ be the set of all places of degree $\leq t$. From now on, we reserve the letter $t$ for the integer such that $S$ is the set of all places of degree $\leq t$. We will give conditions on $t$ under which the map $K'/\text{Im } K \rightarrow k_v^\times$ is bijective.

The following lemma is crucial for the remainder of this section.

**Lemma 4.1.** Let $v$, $U$, $U'$ be as above. Then, if $\deg v > g$, the sequence

$$0 \rightarrow U \rightarrow U' \xrightarrow{v} \mathbb{Z} \rightarrow 0$$

is exact.

**Proof.** Consider the divisor $D = -v + (\deg v + g)(\infty)$ of degree $g$ and let $L(D)$ be the corresponding Riemann–Roch space, i.e.

$$L(D) = \{ f \in F : w(f) \geq -w(D) \text{ for all places } w \text{ of } F \}.$$ 

By the theorem of Riemann and Roch for function fields (see e.g. Stichtenoth (1993), Section 1.5), there exists a function $f \in L(D)$. Since $f$ has a pole of order at most $\deg v + g$ at infinity and no poles elsewhere, its zero divisor has degree at most $\deg v + g$. If $\deg v > g$, we have $v(f) = 1$. \qed

Let $S$ be a set of places of degree $\leq t$ for some $r \in \mathbb{N}$ and let $U$ be the set of $S$-units. Let $v$ be a place of degree $t + 1$. Let $U'$ be the set of $(S \cup \{v\})$-units and set

$$\Pi = \{ \pi \in U' : v(\pi) = 1 \}.$$ 

Choose an element $\pi \in \Pi$ and consider $\theta : U \rightarrow K'/\text{Im } K$ given by $u \mapsto \{u, \pi\}$ and $\beta : U/(U \cap (1 + \Pi)) \rightarrow k_v^\times$ induced by the reduction $U \rightarrow k_v^\times : f \mapsto \overline{f}$. The map $\theta$ is surjective (see e.g. Bass and Tate (1973), p. 58). Moreover, we have $\partial_v(\{u, \pi\}) = \partial_v(\{u, \pi'\})$ for
all $\pi, \pi' \in \Pi$. As in the number field case (Groenewegen, 2004), we get a commutative triangle

\[
\begin{array}{ccc}
U / \langle U \cap (1 + \Pi) \rangle & \xrightarrow{\beta} & k_v^* \\
\downarrow{\theta} & & \downarrow{\beta} \\
K' / \text{Im } K & \xrightarrow{\partial_v} & k_v^*
\end{array}
\]

If $\beta$ is an isomorphism, then all maps are isomorphisms.

Hence, we would like to have a condition on $t$ such that the map

$\beta : U / \langle U \cap (1 + \Pi) \rangle \rightarrow k_v^*$

is an isomorphism for all $v$ with $\deg(v) \geq t + 1$.

We first consider surjectivity.

We have that $\beta$ is surjective if and only if there exists a set $E \subset U$ such that the map $E \times E \rightarrow k_v^*$ defined by $(a, b) \mapsto (\overline{b} - \overline{a})x$, where the bar denotes the reduction, is surjective.

Let $\mathcal{O}_F$ be the set of $v_\infty$-integers in $F$. Let $D$ be a finite subset of $\mathcal{O}_F$ and set $E = \{d_1 - d_2 | d_1, d_2 \in D, d_1 \neq d_2\}$.

**Lemma 4.2.** Let $N(v)$ be the norm of the place $v$. If

(i) $(\#D)^2 > N(v)$ and

(ii) $E \subset U$,

then the map $\beta$ is surjective.

**Proof.** Given $x \in k_v^*$, we have to solve $x = \frac{\overline{e}_1}{\overline{e}_2}$ for some $e_i \in E$. Consider the map

$\varphi_x : \mathcal{O}_F \times \mathcal{O}_F \rightarrow k_v^*$

$\varphi_x(a, b) = \overline{b} - \overline{a}x$.

By (i), $\varphi_x$ is not injective on $D \times D$, i.e. there exist $d, d' \in D \times D$ with $d \neq d'$ and $\varphi_x(d) = \varphi_x(d')$. Let $e = (e_1, e_2) \in E \times E$ be the componentwise difference of $d$ and $d'$. We have $\varphi_x(e) = 0$. Since $e \neq 0$ and $E \subset U$, there exists some component $e_i$ of $e$ such that $\overline{e}_i \neq 0$. From $\overline{e}_2 - \overline{e}_1 x = 0$, we easily see that both components are not equal to 0. We have $x = \frac{\overline{e}_2}{\overline{e}_1}$. □

Let $r \in \mathbb{N}$ and let $L_r = L(rv_\infty) = \{a \in \mathcal{O}_F : (a) \geq -rv_\infty\}$ be the vector space over $k$ of functions with at most one pole of order $r$ in $\infty$ and no other poles.

**Lemma 4.3.** Each element in $L_r$ has a divisor whose support lies in an extension of $k$ of degree at most $r$.

**Proof.** Obvious. □

**Theorem 4.1.** Let $s$ be an integer with $t \geq s$ and

$2(s + 1 - g) > \deg v > t$.

Then $D = L_s$ and $E = L_s - \{0\}$ satisfy the conditions in Lemma 4.2.

Consequence: Under the assumption of the theorem, the map $\beta$ is already surjective if we restrict to the set of functions of the form $f_1/f_2$ where $f_1, f_2 \in L_s$. 
Theorem and the

Let \( f \in \mathcal{L} \) be a function. Suppose one of the following additional conditions is satisfied:

1. \( 3s < 2 \deg(v) \) or
2. \( 3 \dim L_s > 2 \deg(v) \).

Given any \( u, u' \in k_v^* \) and \( u'' \) with \( uu' = u'' \) we have \( \gamma(u)\gamma(u') = \gamma(u'') \).
Proof. First assume 1: Then $\gamma(u) = \frac{f_1}{f_2}$, $\gamma(u') = \frac{f_1'}{f_2'}$ and $\gamma(u'') = \frac{f_2''}{f_2'}$ with $f_1, f_1', f_1'', f_2, f_2', f_2'' \in L$. We have $\deg(f_1 f_2' f_2'' - f_2 f_2' f_2'') < 2 \deg(v)$ and the assertion follows.

Now assume 2: Then we can assume that $\gamma(u)$ and $\gamma(u'')$ have the same denominator (see e.g. Lemma 12 in Groenewegen (2004)) and the assertion follows similarly to that of Proposition 13 in Groenewegen (2004). □

We now would like to construct a set of generators for $U/(U \cap (1 + II))$ and show that we have $\gamma \circ \beta = \text{id}$ on the generators. We recall Lemma 5.5 from Bass and Tate (1973):

**Lemma 4.6.** Let $\mathfrak{A}$ be an ideal in $\mathcal{O}_F$. Let $s$ be the least integer such that $s > \deg(\mathfrak{A}) + g - 1$. There is an $a \neq 0$ in $L_s \cap \mathfrak{A}$. We have $a\mathfrak{O}_F = \mathfrak{A}\mathfrak{B}$ where $\mathfrak{B}$ is in the inverse ideal class of $\mathfrak{A}$ and $\deg(\mathfrak{B}) \leq g$.

Let $A_T = \{a \in F : w(a) \geq 0 \text{ for all } w \not\in T\}$ and let $P_w$ be the prime ideal corresponding to the place $w$.

As a consequence of Lemma 4.6, we can generate $U$ by $U_T$ where $T$ consists of all places of degree less than or equal to $g$ and by elements $\pi_w \in A_T$ such that $\pi_w A_T = P_w A_T$ one for each $w \in S - T$ (cf. Bass and Tate (1973), p. 78).

We first show injectivity on the set of elements $\pi_w$. We have $\beta(\pi_w) = \beta(f_1/f_2)$ for some $f_1, f_2 \in L_s$. To guarantee injectivity, we require $\deg(\pi_w f_2 - f_1) < 2 \deg(v)$, i.e.

$$t + g + s < 2 \deg(v).$$

Next we need a generating set $U_T$ of $T$-units where $T$ is the set of places of degree $\leq g$.

Let $\sum n_w \deg w$ be the degree of the divisor $\sum n_w w$ as usual and define the degree of a function $f \in F^*$ to be the degree of its divisor of zeros or, equivalently, the degree of its divisor of poles.

**Lemma 4.7.** Let $f \in U_T$ be a function of degree $\geq 3g$. There exist functions $h_1, h_2, h_3 \in U_T$ with $\deg(h_1), \deg(h_2) < \deg(f)$ and $\deg(h_3) \leq g + 1$ and an integer $m \geq 0$ such that $f = h_1 h_2 h_3^m$.

**Proof.** Since any function in $F^*$ is uniquely determined by its divisor up to an element in $k^*$, it suffices to show that we can write

$$(f) = (h_1) + (h_2) + m \cdot (h_3)$$

for some integer $m$ and functions $h_1, h_2, h_3 \in U_T$ with $\deg(h_1), \deg(h_2) \leq \deg(f)$ and $\deg(h_3) \leq g + 1$.

We use the fact that the function field $F$ has two $k$-rational places of degree one, the places $v_\infty$ and $v_2$. By the theorem of Riemann and Roch there exists a non-constant function $h_3 \in L((g + 1) \cdot v_\infty - v_2)$. The function $h_3$ has degree $\leq g + 1$, it lies in $U_T$ and it has a pole of order at least one at $v_\infty$. There exists an integer $m \geq 0$ such that $f/h_3^m$ has a pole of order at most $g$ at $v_\infty$ and such that $\deg(f/h_3^m) \leq \deg f$.

It remains to show that every function $f$ of degree $\geq 3g$ with a pole at most $g$ at $v_\infty$ has a divisor of the form

$$(f) = (h_1) + (h_2)$$

with $h_1, h_2 \in U_T$ with $\deg(h_1), \deg(h_2) \leq \deg(f)$. 
Suppose that the divisor of \( f \) is given by
\[
(f) = \sum_v n_v v - \sum_w n_w w, \quad n_v, n_w \geq 0
\]
with \( \sum_v n_v \deg(v) = \sum_w n_w \deg(w) \geq 3g \). Let \( D \) be a divisor of the form
\[
\sum_v m_v v - \sum_w m_w w, \quad n_v \geq m_v \geq 0, n_w \geq m_w \geq 0,
\]
with \( \sum m_w \deg w = d_1 < \deg(f) \) and \( \sum m_v \deg v = d_1 - g - \epsilon \) where \( 0 \leq \epsilon < g \). We can choose the divisor \( D \) such that
\[
\deg(f) - d_1 \leq g, \tag{4.1}
\]
and since \( f \) has a pole of order at most \( g \) at \( v_\infty \), we can assume that \( m_{v_\infty} = 0 \).

Consider the divisor
\[
D_0 = \sum_v m_v v + \epsilon \cdot v_\infty - \sum_w m_w w.
\]
Since the divisors \( \sum_w m_w w \) and \( \sum_v m_v v + \epsilon \cdot v_\infty \) do not have a common support, the divisor \(-D_0\) has degree \( g \).

By the theorem of Riemann and Roch, there exists a function \( h_1 \in L(-D_0) \). Suppose the divisor of \( h_1 \) is given by
\[
(h_1) = \sum_v m_v v + \epsilon \cdot v_\infty + \sum_\mu m_\mu \mu - \sum_w m_w w, \quad m_\mu \geq 0.
\]
Since \( \deg(\sum m_\mu \mu) \leq g \), we have \( h_1 \in U_T \). Moreover, \( \deg(h_1) \leq d_1 \).

The function \( h_2 = f/h_1 \) has divisor
\[
(f) - (h_1) = \sum (n_v - m_v)v - \sum (n_w - m_w)w - \epsilon \cdot v_\infty - \sum m_\mu \mu,
\]
and hence has degree at most \( \deg(f) - d_1 + g + \epsilon \). Using Eq. (4.1), we get
\[
\deg(f) - d_1 + g + \epsilon \leq 2g + \epsilon < 3g \leq \deg f. \quad \square
\]

This implies the following corollary.

**Corollary 4.2.** The set \( U_T \) is generated by functions of degree \( \leq 3g - 1 \).

We can now prove \( \gamma \circ \beta = \text{id} \) on a set of generators of \( U_T \).

**Lemma 4.8.** We have \( \gamma \circ \beta = \text{id} \) on the functions of degree \( \leq 3g - 1 \) if
\[
s + (4g - 1) < 2 \deg(v).
\]

**Proof.** Let \( f \) be a function of degree \( \leq 3g - 1 \). Then there exist \( f_1, g_1 \in L_s \) with \( \beta(f_1/g_1) = \beta(f) \). We have to show that the valuation of \( fg_1 - f_1 \) at \( v \) is at most 1.

By the theorem of Riemann and Roch there exists a function \( h \in L_{4g-1} \) such that the only poles of \( h \) lie in \( v_\infty \) and the poles of \( f \) are zeros of \( h \) (with the same multiplicities). We then have \( \partial = hf_1 - hf_1 \in L_{s+4g-1} \). Since \( s + 4g - 1 < 2 \deg v \), the valuation of \( \partial \) is at most 1. \( \square \)

We summarize all the conditions we obtained:

1. \( 2(s + 1 - g) > \deg v > t \),
2. \( s \leq t \),
3. \( t + g + s < 2 \deg(v) \),
4. (a) \( 3s < 2 \deg(v) \) or 
   (b) \( 3 \dim L_s > 2 \deg(v) \) (follows from \( 3(s + 1 - g) > 2 \deg(v) \)),
5. \( s + 4g - 1 < 2 \deg(v) \).

**Theorem 4.2.** Let \( S \) be the set of places of degree less than or equal to \( t = 6g - 2 \) and let \( v \) be a place outside of \( S \). Then the map \( \beta = \beta_v \) is a bijection.

**Proof.** We get the same result no matter which of the two conditions we choose in 4.

Let us first assume (a):

Set \( t = \deg(v) - 1 \). We have

\[
3s < 2(t + 1) < 4(s + 1 - g).
\]

Note that \( 3s = 4s + 4 - 4g \) for \( s = 4g - 4 \). The inequality (4.2) has an integer solution for \( t \) if \( s \geq 4g - 2 \) and \( t \geq 6g - 2 \).

Now assume (b):

We have \( t + g + s < 2(t + 1) \), and hence \( t > g + s - 2 \). Moreover \( t < 2(s + 1 - g) \), and hence \( 2(g + s - 1) < 3(s + 1 - g) \). We have equality for \( s \geq 5g - 5 \). The inequality

\[
2(g + s - 1) < 2(t + 1) < 3(s + 1 - g)
\]

has an integer solution for \( t \) if \( s = 5g - 2 \) and \( t = 6g - 2 \). \( \square \)

**Corollary 4.3.** Let \( F \) be the function field of an elliptic curve over \( k \). The map \( \beta \) is already surjective if \( S \) contains all places of degree at most 2 and a bijection if we also include the places of degree at most 4.

5. The algorithm of Gangl and Belabas in the function field case

On the basis of the work by Bass and Tate (1973), Belabas and Gangl describe an algorithm for finding generators and relations of the tame kernel of a number field (Belabas and Gangl, 2004). We adopt this algorithm to the function field case and describe the necessary modifications in this section.

For a finite set \( T \) of places let \( K_2^T(F) \) denote the subgroup of \( K_2(F) \) given by symbols \( \{ f, g \} \) supported by \( T \)-units in \( F \). The algorithm consists of two steps:

1. Given a set \( S \) of finite places and a single place \( v \not\in S \) such that \( \ker_F \subset K_2^{S \cup \{v\}}(F) \), the algorithm tests whether already \( \ker_F \subset K_2^S(F) \). If this is the case, we can disregard \( v \) in the subsequent steps.

We start with the set \( S \) containing all finite places of degree \( \leq t \) where \( t \) is given by Theorem 4.2. We then try to reduce the set \( S \) by testing algorithmically for some \( v \in S \) if \( \partial_v : K'/\text{Im} K \xrightarrow{\partial_v} k_v^* \) is an isomorphism.

2. Once \( S \) is small enough we compute the kernel of

\[
K \rightarrow \bigoplus_{v \in S} k_v^*
\]

where \( U \) is the set of \( S \)-units and \( K = (U \otimes U)/(a \otimes b : a, b \in U, a + b = 1 \text{ or } a + b = 0) \).
5.1. Reduction of the set $S$

We can easily adopt Algorithm 3.1 (Belabas and Gangl, 2004) to the function field case. The algorithm tests whether $U_1 = \ker \beta$ for $U_1 = (1 + \pi U_S) \cap U_S$ where $\pi$ is a generator of the ideal corresponding to $v$ in $U_S$ (if such a generator exists). The algorithm is not always successful, i.e. if it outputs $U_1 = \ker \beta$, the equality holds. But it may happen that equality holds and the algorithm fails to detect it.

We now describe the algorithm in the function field case (in our pseudo-code notation we refer to magma-functions whenever they are available in order to abbreviate the discussion). For the description of algorithms computing $S$-units in function fields and linear systems $L(D)$ see Hess (2002, 2003).

**Algorithm 5.1** *(Reduction of the Number of Places in $S$).*

**Input:** A set $S$ of places, $v \not\in S$, $\ker F \subseteq K_2 \setminus \{v\}(F)$.

**Output:** Check whether $U_1 = \ker \beta$. If so, $\ker F \subset K_2 \setminus \{v\}(F)$. Otherwise return FAIL.

1. Compute a set $W$ (with $|W| = |S|$) of generators of $U_S$ using the function $\text{SUnits}(U_S)$.
2. If $v$ is not principal in $O_S$ return FAIL. Else compute a generator $\pi$ of $v$.
3. Compute the order $B$ of the subgroup of $k_v^*$ generated by $W \mod v$.
4. For small multiplicative combinations $t$ from generators in $W$, compute $\pi t_1, t_2 := \text{IsSUnit}(1 - \pi t)$.
   
   If $t_1$ is TRUE, $t_2$ is a vector representing $1 - \pi t$ on the generators of $W$. Collect relations until the rank of the relation matrix is equal to $|S|$ or a counter gets too big.
5. Let $H$ be the relation matrix. If $H$ has maximal rank and $\det(H) = B$ return TRUE, otherwise FALSE.

**Remark 5.1** *(About Computing the Generator).* Given $v$, set $D = (\deg(v) + g)v_\infty - v$. Then there exists a function $f \in L(D)$. If $f \in O_S$, this is a generator. If not, we can also try $D' = (\deg + g + s)v_\infty - v - \sum_{v' \in S} v'$ where $\deg(\sum_{v' \in S} v') = s$.

The complexity of this algorithm is fairly high if $S$ is large. There are other possibilities for reducing the set $S$ before using the algorithm above.

**Remark 5.2.**
1. If we consider the bounds in Section 4 carefully, we notice that the worst bound comes from Lemma 4.5. But in practice, it will not always be necessary to require equation (1) or (2) in Lemma 4.5 to ensure that $\gamma$ is a homomorphism. For a concrete example, we can use the computer to check the latter.

Suppose for example, that our function field is an elliptic function field $F_E$. By Corollary 4.3, $S$ should contain all places of degree $\leq 4$. If we show the homomorphism property for each place $v$ of degree 4, we can restrict $S$ to the places of degree $\leq 3$, since all other inequalities will be automatically satisfied.

2. (cf. Belabas and Gangl (2004)) Let $U$ denote the $S$-units and suppose that $v$ is principal, i.e. $v = (\pi)$ in the ring of $S$-integers. Let $U_1$ be equal to $(1 + \pi U) \cap U$. From Proposition 1, p. 430 in Bass and Tate (1973) we easily derive the following criterion:

Suppose that $W$, $C$ and $G$ are subsets of $U$ such that

(a) $W \subset CU_1$ and $W$ generates $U$,
(b) $CG \subset CU_1$ and $\beta(G)$ generates $k_v^*$,
(c) $1 \in C \cap \ker \beta \subset U_1$.

then $U_1 = \ker \beta$ and $\delta_v$ is bijective.
We take \( W \) to be a set of generators, \( G = \{ \alpha \} \) for any \( \alpha \) with \( \langle \beta(\alpha) \rangle = k^*_v \), and take \( C \) to be a set of equivalence classes of \( k^*_v \), i.e. \( C \) should be minimal with respect to the property \( C = k^*_v \).

Condition (c) is then trivial.

Let \( m(W) \) (resp. \( m(C) \), \( m(G) \)) be the maximal degrees of the elements in \( W \) (resp. \( C \), \( G \)). If \( m(W) + m(C) < 2 \deg v \) and \( 2m(C) + m(G) < 2 \deg v \), then (a) and (b) are satisfied.

Otherwise we have to check the conditions for our choice of \( W \), \( C \) and \( G \) explicitly.

### 5.2. Computation of the generators

We now describe the computation of the generators of \( \ker F \). The algorithms are completely analogous to the Algorithms 5.1 and 5.2 in Belabas and Gangl (2004).

**Algorithm 5.2 (Computing Generators of \( \ker F \)).**

**Input:** A set \( S \) of places, a basis \((w_i)\) for the \( S \)-units.

**Output:** A lattice \( \Lambda \) of full rank in \( U_S \otimes U_S \) generated by \( x_i \otimes (1 - x_i) \) for certain \( x_i \) with determinant as small as possible.

1. Let \( w_{ij} = w_i \otimes w_j \) be a generating set of \( U_S \otimes U_S \). We include all relations \( 2w_{ij} = 0 \) into \( \Lambda \).

2. We include \( u \otimes (1 - u) \) for multiplicative combinations \( u = \prod w_i^{e_i} \in U_S \) for bounded \( e_i \) where \( 1 - u \) is also in \( U_S \). We stop searching for more combinations if the rank of \( \Lambda \) is \(|S|^2\) and the determinant stabilizes.

3. Return \( \Lambda \).

**Remark 5.3.** For the second step, we can use the following theorem (Mason, 1983; Silverman, 1984): Let \( u, v \) be \( S \)-units satisfying

\[
u + v = 1.
\]

Then either \( u, v \in \overline{k}^* \) or \( \deg_s(u) \leq 2g - 2 + |S| \) where \( \deg_s(u) \) denotes the separable degree of \( u \).

We can use this fact to modify our algorithm. It is now only necessary to consider products of \( S \)-units of degree less than or equal to \( 2g - 2 + |S| \) when producing the relation lattice in Algorithm 5.2. This allows us to enumerate all relations deterministically.

**Algorithm 5.3** computes a group of which \( \ker F \) is a quotient (cf. Belabas and Gangl (2004)).

Given two matrices

\[
A = (a_{ij})_{1 \leq i \leq s_C, 1 \leq j \leq s_A} \quad \text{and} \quad B = (b_{ij})_{1 \leq i \leq s_C, 1 \leq j \leq s_B},
\]

let \((A|B)\) be the \( s_C \times (s_A + s_B) \) matrix \( C \) given by \( c_{ij} = a_{ij} \) if \( j \leq s_A \) and \( c_{ij} = b_{i, j - s_A} \) if \( j > s_A \).

**Algorithm 5.3 (Computing a Group of which \( \ker F \) is a Quotient).**

**Input:** A lattice \( \Lambda \) as above.

**Output:** A presentation for a finite abelian group \( \widetilde{\ker F} \) of which \( \ker F \) is a quotient.

1. Order the places in \( S \), i.e. \( S = \{ v_1, \ldots, v_{|S|} \} \). For all \( v \in S \) do the following
   
   (a) Compute a generator \( g_v \) of the cyclic group \( k^*_v \).
   
   (b) For all \( w_{ij} \) compute \( n_{v,ij} \) such that \( \partial_v(w_{ij}) = g_v^{n_{v,ij}} \).

2. Compute the integer kernel \( M \) of the matrix

\[
\left( (n_{v,ij})_{v,ij} | \text{diag}(N(v) - 1) \right)_{v}
\]
where \( \text{diag}(N(v) - 1)_v \) denotes the \(|S| \times |S|\)-diagonal matrix whose \( i \)th diagonal entry is equal to \( N(v_i) - 1 \).

3. Compute the integer kernel of the matrix \((\widetilde{M}|M_A)\).

Let \( \begin{pmatrix} Y \\ Z \end{pmatrix} \) be the kernel. The SNF of \( Y \) gives the elementary divisors of \( \widetilde{\ker} F \).

**Remark 5.4.** 1. (Computation of the generators) Suppose that the column vectors of \( \widetilde{M} \) contain a basis of the kernel of \( \partial \) and the column vectors of \( M_A \) contain a basis of the relation lattice. Suppose that the columns of \( Y \) contain the integer kernel of the matrix \((\widetilde{M}|M_A)\). The columns of \( \widetilde{MY} \) represent the intersection \( \ker \partial \cap \Lambda \).

Let \( Y_S \) be the Smith normal form and \( Y_1, Y_2 \) be such that \( Y_1 \cdot Y \cdot Y_2 = Y_S \). Then, \( Y_1^{-1}Y_SY_2^{-1} = Y \) and \( \widetilde{MY}_1^{-1} \) is the basis of the kernel of \( \partial \) which corresponds to the Smith normal form. This means that the columns of the matrix \( \widetilde{MY}_1^{-1} \) represent the generators of \( \widetilde{\ker} F \) which correspond to the elementary divisors.

2. (Eliminating elements from the relation lattice) Sometimes we can include additional relations in the relation lattice.

**Lemma 5.1.** Given an abelian group \( G \) and subgroups \( H_1, H_2 \) and \( H \) such that \( H_1 \subseteq H \) and \([H : H_1] = \ell^k\). Suppose \( \ell \nmid |H_2/(H_2 \cap H_1)| \), then

\[
H_2/(H_2 \cap H_1) \simeq H_2/(H_2 \cap H).
\]

**Proof.** The map

\[
\varphi : H_2/(H_2 \cap H_1) \rightarrow H_2/(H \cap H_2)
\]

is obviously surjective. Its kernel is equal to \((H_2 \cap H)/(H_2 \cap H_1)\). The group \((H_2 \cap H)H_1/H_1\) is a subgroup of \( H/H_1 \) and as such has order \( \ell^k' \) for some \( k' \leq k \). But by the isomorphism theorem for groups

\[
(H_2 \cap H)H_1/H_1 \simeq (H_2 \cap H)/(H_2 \cap H \cap H_1) = (H_2 \cap H)/(H_2 \cap H_1).
\]

So the kernel is \( \ell \)-primary, but since \( \ell \nmid |H_2/(H_2 \cap H_1)| \) it must be equal to 0. \( \Box \)

We can use Lemma 5.1 as follows: The 2-torsion of \( \ker F \) can sometimes be computed by hand. So we concentrate on the odd part of \( \ker F \). This allows us to include the relations \( w \otimes w = 1 \) in the relation lattice.

6. Some computational examples

We conclude with some examples. We compute a generator of \( \ker F \) for some elliptic function fields \( F \).

**6.1. Example for the algorithm in Section 3.2**

Consider the elliptic function field \( F_E \) over \( k = \mathbb{F}_3 \) given by

\[
y^2 = x^3 + x^2 + 2.
\]

It has three \( k \)-rational places and the order of \( \ker F_{E_k} \) is therefore equal to 25. We would like to construct a non-trivial element of order 5 in \( \ker F_{E_k} \) using the algorithm described in Section 3.2.
Note that $m = 4$ is the least positive integer such that $3^m = 1 \mod 5$. The elliptic curve over $\mathbb{F}_{3^4}$ contains the full 5-torsion group. It can be generated by two 5-torsion points, one already defined over $\mathbb{F}_{3^2}$. We take a 5-torsion point $P$ which cannot be defined over any smaller subfield of $\mathbb{F}_{3^2}$ and construct a function $f$ with divisor equal to $5P - 5P_\infty$. The element $\beta = \{\xi_5, f\}$ is an element of order 5 in ker$_{E, \mathbb{F}_{3^4}}$. Since $f$ cannot be defined over any smaller field than $\mathbb{F}_{3^4}$, the trace of $\beta$ is a non-trivial element $\alpha$ of ker$_{E, \mathbb{F}}$. For a certain choice of $P$, we find
\[
\alpha = \{(xy + x^3 + 2x^2 + 2)/(x^3 + 2), ((x^4 + 2x^3 + 2x)y + 2x^5 + 2x^4 + x^2)/(x^6 + x^3 + 1)\}
\]
\[
+ \{(((x^4 + 2x)y + x^5 + x^4 + 2x^2)/(x^6 + 2x^5 + 2x^4 + x^3 + x^2 + 1),
(x^6 + x^5 + x^4 + x^3 + 2x^2 + 1)xy + (x^3 + x^2 + 2)(x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 1))/((x \cdot (x^7 + x^6 + x^4 + 2x^3 + x)))\}.
\]
The result is not very satisfactory. Even for such a simple example (we just compute a 5-torsion element), the degree of the functions and the places at which they have positive valuation are large.

We next consider some examples derived using the second algorithm. We will see that even though the groups in the following examples are slightly larger, the results will be shorter.

6.2. Examples for the algorithm in Section 5

1. Let $p = 3$. Consider the elliptic function field $E_1$ given by the equation
\[y^2 = x^3 + 2x + 1.\]
The elliptic curve has seven points over $\mathbb{F}_p$. Hence, ker$_{E_1}$ is a cyclic group of order 37. Using the ideas in Remark 5.2, it is sufficient to consider the set of $S$-units where $S$ contains all places of degree $\leq 3$.

We now run Algorithm 5.1 and reduce $S$ to the set of places of degree $\leq 1$. Now using the algorithms in Section 5 we find a group of order 37.

Set
\[
w_2 = 1/(x^2 + 2) y + (x^2 + 1)/(x^2 + 2),
\]
\[
w_3 = 1/(x^2 + x + 1) y + (x^2 + 2x + 1)/(x^2 + x + 1) \text{ and}
\]
\[
w_4 = 1/(x^2 + x) y + 2/(x^2 + x).
\]
An element of order 37 is given by
\[
\{w_2, w_3, w_4\}.
\]

2. Let $p = 5$. Consider the elliptic function field $E_2$ given by the equation
\[y^2 = x^3 + 2x + 1.\]
The elliptic curve has seven points over $\mathbb{F}_p$. The group ker$_{E_2}$ must be cyclic of order 131. Using Remark 5.2, it is enough to consider the set $S$ where $S$ contains all places of degree $\leq 2$ and exactly four places of degree $\leq 3$. After running Algorithm 5.1, we are left with a set $S$ consisting of six places of degree one. Set
\[
\{w_1, \ldots, w_6\}
\]
\[
= \{1/(x^2 + 4x) y + (3x + 4)/(x^2 + 4x), 1/(x^2 + 2x) y + (2x + 1)/(x^2 + 2x),
2, 1/(x^2 + 3x + 1) y + (2x^2 + x + 4)/(x^2 + 3x + 1),
1/(x^2 + x + 3) y + (x^2 + 3x + 4)/(x^2 + x + 3), x/(x + 4)\}.
\]
An element of order 131 is given by
\[-\{w_1, w_6\} + \{w_2, w_6\} = \{w_2/w_1, w_6\}.
\]

3. Let \( q = 4 \) and consider the elliptic function field \( E_3 \) defined by
\[y^2 + x + \alpha y = x^3 + x^2 + \alpha \]
where \( \mathbb{F}_q = \mathbb{F}_2(\alpha) \). The elliptic curve defined over \( \mathbb{F}_q \) has six points. Hence, \( \ker_{E_3} \) is a cyclic group of order 69.

Using our algorithm, we find the generator
\[\{w_3, w_4 w_5\} + \{w_4 w_5, w_2\} + \{w_6, w_1 w_3\} + \{w_7, w_1\} = \{w_3/w_2, w_4 w_5\} + \{w_6, w_1 w_3\} + \{w_7, w_1\}\]
where
\[\{w_1, \ldots, w_7\} = \{(x + 1)/x, \alpha, 1/(x^2 + \alpha x + \alpha^2)y + (\alpha^2 x + 1)/(x^2 + \alpha x + \alpha^2), 1/(x^2 + \alpha x + \alpha^2)y + \alpha/(x^2 + \alpha x + \alpha^2), 1/(x^2 + x + 1)y + \alpha^2/(x + \alpha^2), (x + \alpha^2)/x, 1/(x^2 + \alpha x + \alpha^2)y + x^2/(x^2 + \alpha x + \alpha^2)\}.
\]

Acknowledgments

The author thanks the referees for valuable comments improving the paper.

References

Tate, J., 1970. Symbols in arithmetic. Actes, Congrès Int. Math. 1, 201–211.