Marzena Ciemała
On the Milnor exact sequence for global function fields

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 8 (2000), No. 1, 25--31

Persistent URL: http://dml.cz/dmlcz/120556

Acta Mathematica et Informatica Universitatis Ostraviensis 8 (2000) 25–31

On the Milnor exact sequence for global function fields

Marzena Ciemała

Abstract: A new proof is given for the exactness of the Milnor sequence for the rational function field $\mathbb{F}(x)$ over a finite field $\mathbb{F}$. As a consequence an explicit construction of the generators of the cyclic direct summands of the Witt group $W(\mathbb{F}(x))$ is presented.

Key Words: Rational function fields; Milnor's exact sequence

Mathematics Subject Classification: Primary 11E81; Secondary 11E12

1. Introduction

For a field F of characteristic different from two the structure of the Witt group of quadratic forms over the rational function field $F(x)$ can be described in terms of Milnor's exact sequence provided we know the Witt groups $W(F)$ and $W(K)$ for all finite extensions K/F (see [3], p. 265). The proof of Milnor's theorem as presented in [3] Chapter 9.3 uses some techniques coming from K-theory. On the other hand the proof of the much more general result given in [4] Cor. (3.3), p. 93 (for the Witt group of a Dedekind domain and the Witt group of its field of quotients) is based on the arithmetic theory of lattices.

In this paper we consider rational function fields with finite fields of constants and give a proof of Milnor's theorem using only purely quadratic form theory arguments. These include Hasse Principle and Hilbert Reciprocity. Our proof makes it possible to write down an explicit decomposition of the Witt group $W(\mathbb{F}(x))$ into direct sum of cyclic groups. That is, we show how to find the generators of the cyclic summands in a decomposition of the Witt group $W(\mathbb{F}(x))$ into direct sum of cyclic groups.

This project follows closely the work of K. Szymiczek [5], who gave a proof of Milnor's theorem for the rational number field based on the Hasse Principle.

2. Milnor's theorem

Let $\mathbb{F}$ be a finite field of odd characteristic, Ω the set of all monic irreducible polynomials in the ring $\mathbb{F}[x]$, and $E := \mathbb{F}(x)$ the rational function field over $\mathbb{F}$. For every $\pi \in \Omega$ by E_π (resp. $\bar{E}_\pi$) we denote the completion (resp. the residue class field) of the field E under π-adic valuation.

The Milnor sequence combines two maps, the natural ring homomorphism $i : W(\mathbb{F}) \to W(E)$, and $\partial : W(E) \to \bigoplus_{\pi\in\Omega} W(\bar{E}_\pi)$ called the boundary homomorphism. Let $\partial_\pi : W(E) \to W(E_\pi) \to W(\bar{E}_\pi)$ be the composition of the natural homomorphism with the second residue homomorphism defined as follows

$$\partial_\pi\langle a_1, \dots a_n, \pi b_1, \dots , \pi b_s\rangle = \langle \bar{b}_1, \dots , \bar{b}_s\rangle$$

where $a_i, b_j \in \mathbb{F}[x]$, $\pi \nmid a_i$, $\pi \nmid b_j$ for $i \in \{1, \dots , n\}$, $j \in \{1, \dots , s\}$ and $\bar{b}$ is the image of $b \in \mathbb{F}[x]$ under canonical projection on $\bar{E}_\pi$. Then we define

$$\partial := (\partial_\pi)_{\pi\in\Omega}.$$

Now we can state Milnor's theorem for global rational function fields.

Theorem 2.1. *The following sequence is split exact*

$$0 \longrightarrow W(\mathbb{F}) \xrightarrow{\ i\ } W(E) \xrightarrow{\ \partial\ } \bigoplus_{\pi\in\Omega} W(\bar{E}_\pi) \longrightarrow 0. \tag{1}$$

We give a proof in §3, and in §4 we discuss the decomposition of the Witt group $W(\mathbb{F}(x))$ into an internal direct sum of cyclic subgroups. In an Appendix we summarize the results on quadratic and Hilbert reciprocity needed in the proof.

3. Proof

3.1. Surjectivity of the boundary homomorphism ∂

Since the residue class field $\bar{E}_\pi \cong \mathbb{F}[x]/\pi$ is a finite field of odd characteristic, for $\pi \in \Omega$ the group $W(\bar{E}_\pi)$ is the cyclic group of order 4 generated by $\langle \bar{1}\rangle$ when $s(\bar{E}_\pi) = 2$, or the Klein four-group generated by $\langle \bar{1}\rangle$ and $\langle \bar{u}\rangle$, $\bar{u} \in \dot{\bar{E}}_\pi \setminus \dot{\bar{E}}_\pi^{\,2}$ when $s(\bar{E}_\pi) = 1$. Here $s(\bar{E}_\pi)$ denotes the level of the field $\bar{E}_\pi$. This implies that the elements of the following set generate the cyclic direct summands of $\bigoplus_{\pi\in\Omega} W(\bar{E}_\pi)$:

$$A := \{\eta^\pi : \pi \in \Omega\} \cup \{\mu^\pi : \pi \in \Omega \quad \text{with} \quad s(\bar{E}_\pi) = 1\}, \tag{2}$$

where η^π and μ^π are elements of $\bigoplus_{\pi\in\Omega} W(\bar{E}_\pi)$ whose ρ-th coordinates satisfy

$$(\eta^\pi)_\varrho = \begin{cases} 0 & \text{for } \pi \neq \varrho, \\ \langle \bar{1}\rangle & \text{for } \pi = \varrho, \end{cases}$$

$$(\mu^\pi)_\varrho = \begin{cases} 0 & \text{for } \pi \neq \varrho, \\ \langle \bar{u}\rangle & \text{for } \pi = \varrho \text{ and some } \bar{u} \in \dot{\bar{E}}_\pi \setminus \dot{\bar{E}}_\pi^{\,2}. \end{cases}$$

To prove the surjectivity of ∂ it is sufficient to check that

$$A \subseteq im\ \partial.$$

First observe that $\eta^\pi \in im\ \partial$ for all $\pi \in \Omega$, since $\langle\pi\rangle \in W(E)$ satisfies $\partial\langle\pi\rangle = \eta^\pi$. To show that $\mu^\pi \in im\ \partial$ we fix a $\pi \in \Omega$ with $s(\bar{E}_\pi) = 1$.

We choose and fix an $a \in \dot{\mathbb{F}} \setminus \dot{\mathbb{F}}^2$. When -1 is not a square in $\mathbb{F}$ we set $a = -1$. Further, we choose $\rho \in \Omega$ satisfying the following conditions for the Legendre symbols:

$$\left(\frac{\pi}{\rho}\right) = \left(\frac{a}{\rho}\right) = -1.$$

There are infinitely many such ρ's (see [1] Lemma 2.3). Consider now the form

$$\varphi = \langle a\rho, \pi\rho\rangle \in W(E) \qquad \text{when} \quad s(E) = 1 \tag{3}$$

or

$$\varphi = \langle \rho, \pi\rho\rangle \in W(E) \qquad \text{when} \quad s(E) = 2. \tag{4}$$

In both cases we have

$$\partial_\pi(\varphi) = \langle\bar{\rho}\rangle \in W(\bar{E}_\pi).$$

We claim that $\bar{\rho}$ is a non-square in $\bar{E}_\pi$. Consider first the case $s(E) = 1$. Then also $s(\mathbb{F}) = 1$ and if $Q = |\mathbb{F}|$, then $Q \equiv 1 \pmod 4$ by [3] p. 304. Hence $\frac{Q-1}{2}$ is even and

$$-1 = \left(\frac{\pi}{\rho}\right) = \left(\frac{\rho}{\pi}\right) \tag{5}$$

by quadratic reciprocity law ([2] p. 103, see the Appendix). Hence $\bar{\rho}$ is a non-square in $\bar{E}_\pi$.

If $s(E) = 2$, then from $s(\bar{E}_\pi) = 1$ we conclude that the degree of π is even (see Appendix) and again by reciprocity we get (5). This proves our claim.

Now we compute the image of φ under ∂_ρ. In the first case we have

$$\partial_\rho(\varphi) = \langle\bar{a}, \bar{\pi}\rangle \in W(\bar{E}_\rho).$$

Here $\bar{a}$ and $\bar{\pi}$ are non-squares in $\bar{E}_\rho$, hence they belong to the same square class of $\bar{E}_\rho$. Thus $\partial_\rho(\varphi) = \langle\bar{a}, \bar{a}\rangle = 0 \in W(\bar{E}_\rho)$, since $s(\bar{E}_\rho) = s(E_\rho) = s(E) = 1$. It follows that $\partial(\varphi) = \mu^\pi$.

In the second case (when ϕ is given by (4)) we have

$$\partial_\rho(\varphi) = \langle\bar{1}, \bar{\pi}\rangle = \langle\bar{1}, -\bar{1}\rangle = 0 \in W(\bar{E}_\rho),$$

since -1 is a non-square in $\bar{E}_\rho$ and $\bar{\pi}$ is also a non-square in $\bar{E}_\rho$, and so $\bar{\pi}$ and $-\bar{1}$ are in the same square class of $\bar{E}_\rho$. It follows $\partial(\varphi) = \mu^\pi$, as required.

This proves that each μ^π belongs to the image of ∂ and so $A \subset im\ \partial$.

3.2. Splitting ∂

Recall that the elements of the set A (see (2)) generate the direct summands of the group $\bigoplus_{\pi\in\Omega} W(\bar{E}_\pi)$. Hence there is a unique group homomorphism

$$\sigma : \bigoplus_{\pi\in\Omega} W(\bar{E}_\pi) \to W(E)$$

such that for all $\pi \in \Omega$,

$$\sigma(\eta^\pi) = \langle\pi\rangle, \quad \sigma(\mu^\pi) = \varphi,$$

where φ is defined by (3) or (4) when $s(E) = 1$ or $s(E) = 2$, respectively. Then we have $\partial \circ \sigma = \mathrm{id}$. Hence σ splits ∂.

3.3. Exactness at $W(E)$

We only need to prove that $\ker \partial \subseteq im\ i$ since the opposite inclusion is obvious. We take an anisotropic quadratic form φ over E with $\langle\varphi\rangle \in \ker\partial$. To prove that $\langle\varphi\rangle \in im\ i$ we will use induction on $k = \dim\varphi$. Observe that three-dimensional forms over $\mathbb{F}$ are isotropic, hence there are no three-dimensional anisotropic forms in $im\ i$. Thus we will have to show that there are no anisotropic forms φ in $\ker\partial$ of dimension greater than 2. Accordingly, the proof splits into two parts. First we consider the dimensions $k = 1, 2$, and then we prove by induction that there are no anisotropic forms of dimension ≥ 3 in $\ker\partial$. We begin with a lemma.

Lemma 3.1. *Let $f_1, \dots, f_k \in \mathbb{F}[x] \setminus \{0\}$. If $\langle f_1, \dots, f_k\rangle$ belongs to the kernel of the homomorphism ∂, then there exists an element $a \in \dot{\mathbb{F}}$ such that*

$$f_1 \cdots f_k \dot{E}^2 = a\dot{E}^2.$$

Proof. Without loss of generality we can assume that each of the polynomials f_i is square-free, that is, not divisible by the square of any irreducible polynomial. Assume now that $\partial\langle f_1, \dots, f_k\rangle = 0$. Hence $\partial_\pi\langle f_1, \dots, f_k\rangle = 0$ for all $\pi \in \Omega$. If the product $f_1 \cdots f_k$ is not a constant, then take any $\pi \in \Omega$ dividing the product. Renumbering the f_i's if necessary, we can write

$$\langle f_1, \dots, f_k\rangle = \langle \pi f_1', \dots, \pi f_l', f_{l+1}, \dots, f_k\rangle,$$

where $\pi \nmid f_i', \pi \nmid f_j$ for all $i = 1, \dots, l$ and $j = l+1, \dots, k$. Hence

$$\partial_\pi\langle f_1, \dots, f_k\rangle = \langle \bar{f}_1', \dots, \bar{f}_l'\rangle = 0.$$

The form $\langle \bar{f}_1', \dots, \bar{f}_l'\rangle$ is hyperbolic which implies that its dimension is even. Hence $l = 2t$ for some $t \in \mathbb{N}$ and $\pi^{2t} \mid f_1 \cdots f_k$. Since the polynomials f_i are square-free, the product $f_1 \cdots f_k$ is not divisible by any higher power of π. Thus the product $f_1 \cdots f_k$ is a square up to a constant $a \in \dot{\mathbb{F}}$. □

Consider the case $k = 1$. If $\partial\langle f_1\rangle = 0$, then by the Lemma there is an $a \in \dot{\mathbb{F}}$ such that $f_1\dot{E}^2 = a\dot{E}^2$. Hence $\langle f_1\rangle = \langle a\rangle \in im\ i$.

Now consider the case when $k = 2$. So assume $\partial\langle f_1, f_2\rangle = 0$. According to the Lemma, $\langle f_1, f_2\rangle = \langle f, af\rangle$ for a nonzero square-free polynomial f in $\mathbb{F}[x]$ and an $a \in \dot{\mathbb{F}}$. Write φ for the quadratic form (f, af). We are going to prove that $\varphi \cong (1, a)$ over E. For this it is sufficient to show that φ represents 1 over all completions E_π of E.

If φ is isotropic over E_π for some $\pi \in \Omega \cup \{\infty\}$ then clearly $1 \in D_{E_\pi}(\varphi)$. So let us assume $\pi \in \Omega$ and φ_π is anisotropic. We claim that then $\pi \nmid f$. For otherwise there is $f' \in \mathbb{F}[x]$ such that $\pi f' = f$ and this implies $\langle \bar{f}', \bar{a}\bar{f}'\rangle = \partial_\pi\langle f, af\rangle = 0$. Hence $(\bar{f}', \bar{a}\bar{f}')$ would be isotropic over the residue class field and so φ would be isotropic over E_π (see [3] Prop. 1.9(1), p. 147).

Thus we have $\varphi_\pi = (u_1, u_2)$ with u_1, u_2 units in E_π. By [3] Cor. 2.5(2), p. 150, the ternary form $(u_1, u_2, -1)$ is isotropic over E_π, hence (u_1, u_2) represents 1 over E_π, as required.

We have shown that 1 is represented by φ in all completions E_π except possibly E_∞. By Hilbert Reciprocity (see the Appendix), 1 is also represented over E_∞. Then, by Hasse principle, 1 is represented by φ over E, and so $\varphi \cong (1, a)$ over E. Thus $\langle\varphi\rangle \in im\ i$, as required.

Now let $k \geq 3$. We will prove by induction on k that there are no k-dimensional anisotropic forms in $\ker\partial$. First consider the case $k = 3$. So let φ be 3−dimensional anisotropic form over E with $\partial\langle\varphi\rangle = 0$. By the Lemma we can assume that $\varphi = (f_1, f_2, af_1f_2)$, where f_1, f_2 are square-free polynomials in $\mathbb{F}[x]$ and $a \in \dot{\mathbb{F}}$. Since $\partial_\pi\langle f_1, f_2, af_1f_2\rangle = 0$, the first or the second residue form of φ is isotropic, hence the form φ is isotropic over every E_π, $\pi \in \Omega$ by [3] Prop. 1.9(2), p. 147. By Hilbert Reciprocity, φ is also isotropic over E_∞. Hence, by Hasse principle, it is isotropic over E, a contradiction. So there are no 3−dimensional anisotropic forms φ with $\partial\langle\varphi\rangle = 0$.

Assume now $k \geq 4$. Let φ be a k−dimensional anisotropic form over E such that $\partial\langle\varphi\rangle = 0$. Consider the form $\psi = (1) \perp \varphi$. The dimension of ψ is at least five, so the form is isotropic over any completion of E ([3] Thm. 2.2(2), p. 149]. By the Hasse principle, ψ is isotropic over E, and so $-1 \in D_E(\varphi)$. Thus there is an anisotropic form φ' satisfying $\varphi \cong (-1) \perp \varphi'$. Obviously we have $\dim\varphi' = k - 1$ and $0 = \partial\langle\varphi\rangle = \partial\langle\varphi'\rangle$. By induction hypothesis φ' is isotropic, hence φ is isotropic as well, a contradiction.

Summing up we have shown that when $\langle\varphi\rangle \in \ker\partial$ and φ is anisotropic, then $\dim\varphi \leq 2$ and $\langle\varphi\rangle \in im\ i$.

4. The Witt group $W(\mathbb{F}(x))$

Since Milnor's sequence (1) is split exact it yields the decomposition of the Witt group $W(E)$ into the direct sum of the kernel and of the image of the boundary homomorphism ∂,

$$W(E) \cong W(\mathbb{F}) \oplus \bigoplus_{\pi\in\Omega} W(\bar{E}_\pi).$$

Alternatively, we get the internal direct sum decomposition

$$W(E) = \ker\partial \oplus im\ \sigma,$$

where σ is the injective group homomorphism splitting ∂, constructed in §3.2. In the decompositions given below we write $\mathbf{Z}_n\langle e\rangle$ for the cyclic group of order n generated by $\langle e\rangle$.

When $s(E)=1$, we have

$$W(E)=\mathbf{Z}_2\langle 1\rangle\oplus\mathbf{Z}_2\langle a\rangle\oplus\bigoplus_{\pi\in\Omega}(\mathbf{Z}_2\langle\pi\rangle\oplus\mathbf{Z}_2\langle\varphi\rangle),$$

where φ is chosen as in (3), and when $s(E)=2$, we have

$$W(E)=\mathbf{Z}_4\langle 1\rangle\oplus\bigoplus_{\pi\in\Omega,\ s(\bar{E}_\pi)=2}\mathbf{Z}_4\langle\pi\rangle\oplus\bigoplus_{\pi\in\Omega,\ s(\bar{E}_\pi)=1}(\mathbf{Z}_2\langle\pi\rangle\oplus\mathbf{Z}_2\langle\varphi\rangle),$$

where φ is chosen as in (4).

5. Appendix: Quadratic Reciprocity and Hilbert Reciprocity

We collect here some information on Legendre and Hilbert symbols, in particular we state all results used in this paper. The Legendre symbol and quadratic reciprocity law for rational function field over a finite field of constants is discussed in detail in [2] pp. 100–103 (even for n-th power residues). On the other hand Hasse omitted the discussion of Hilbert symbols and Hilbert Reciprocity for function fields. Actually, we have not found anything in the literature on that for the field $\mathbb{F}(x)$ (except for the discussion of the most general case of all global fields). While the case of a rational function field with finite field of constants is analogous to the case of rational number field, we nevertheless need precise formulation of the results and that is why we try to summarize them in this appendix. We retain the notation introduced in §2.

From [2] p. 103 we cite the Quadratic Reciprocity Law. For $\pi,\rho\in\Omega$, $\pi\neq\rho$ and $Q=|\mathbb{F}|$, we have

$$\left(\frac{\pi}{\rho}\right)\cdot\left(\frac{\rho}{\pi}\right)=(-1)^{\deg\pi\cdot\deg\rho\cdot\frac{Q-1}{2}}.$$

Further, if $a\in\dot{\mathbb{F}}\setminus\dot{\mathbb{F}}^2$, then

$$\left(\frac{a}{\pi}\right)=(-1)^{\deg\pi}. \tag{A1}$$

For if $n=\deg\pi$ is odd, then the field $\bar{E}_\pi=\mathbb{F}[x]/\pi$ has no quadratic subfields so that a remains a non-square in $\bar{E}_\pi$. On the other hand if the degree n is even, then by Galois theory $\bar{E}_\pi$ contains a quadratic extension of $\mathbb{F}$ and since $\mathbb{F}$ has only two square classes we must have $\mathbb{F}(\sqrt{a})\subseteq\bar{E}_\pi$. Hence a is a square in $\bar{E}_\pi$. In particular, if $s(E)=2$ and $s(\bar{E}_\pi)=1$, then the degree of π is even.

We write $(\alpha,\beta)_\pi$ for the π-adic Hilbert symbol for $\alpha,\beta\in E_\pi$ and π in $\Omega\cup\infty$. By definition, this equals 1 or -1 depending on whether or not the quadratic form (α,β) represents 1 over E_π.

For $\pi\in\Omega$, $f,g\in\mathbb{F}[x]$ with $\pi\nmid fg$, and $a\in\dot{\mathbb{F}}\setminus\dot{\mathbb{F}}^2$ we have

$$(\pi,f)_\pi=\left(\frac{f}{\pi}\right),\qquad(\pi,a)_\pi=-1,\qquad(f,g)_\pi=1.$$

For $\pi = \infty$, the crucial observation is that a monic polynomial is a square in E_∞ if and only if its degree is even. This follows from the identity

$$x^n + a_1 x^{n-1} + \cdots + a_n = \left(\frac{1}{x}\right)^{-n} \cdot (1 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n})$$

and from the fact that the expression in the parentheses is a square in the completion $E_\infty = \bar{E}_\pi((\frac{1}{x}))$. This leads to the following evaluation of the symbol for monic $f, g \in \mathbb{F}[x] \setminus \mathbb{F}$:

$$(f,g)_\infty = (-1)^{\deg f \cdot \deg g \cdot \frac{Q-1}{2}}.$$

This is clear when at least one of the polynomials has even degree. Otherwise, each f and g can be written as the product of $y := \frac{1}{x}$ and a square in E_∞, hence

$$(f,g)_\infty = (y,y)_\infty = (y,-1)_\infty.$$

Now it remains to notice that -1 is a square in E_∞ if and only if it is a square in $\mathbb{F}$ if and only if $\frac{Q-1}{2}$ is even.

For $\pi \in \Omega$ and $a \in \dot{\mathbb{F}} \setminus \dot{\mathbb{F}}^2$ we also have

$$(\pi, a)_\infty = (-1)^{\deg \pi}. \tag{A2}$$

Finally we state the Hilbert Reciprocity Law. It asserts that for any nonzero $f, g \in \mathbb{F}[x]$,

$$\prod_\sigma (f,g)_\sigma = 1.$$

Here σ runs over $\Omega \cup \infty$. The proof can be obtained by mimicking the proof in the rational number field case (see [2] pp. 95–96). We split f and g into irreducible factors and use multiplicativity of the Hilbert symbol to reduce the proof to the three cases: $(f,g) = (a,b), (\pi,a), (\pi,\rho)$, where $a, b \in \dot{\mathbb{F}}$ and $\pi, \rho \in \Omega$, $\pi \neq \rho$. In the first case all symbols $(a,b)_\sigma$ are equal to 1, in the second case the product reduces to $(\pi,a)_\pi \cdot (\pi,a)_\infty$ and this is 1 by (A1) and (A2). And in the third case the product reduces to

$$(\pi,\rho)_\pi \cdot (\pi,\rho)_\rho \cdot (\pi,\rho)_\infty = \left(\frac{\rho}{\pi}\right) \cdot \left(\frac{\pi}{\rho}\right) \cdot (-1)^{\deg \pi \cdot \deg \rho \cdot \frac{Q-1}{2}} = 1.$$

References

[1] M. Ciemała, and K. Szymiczek, *Witt equivalence of global function fields.* Tatra Mount. Math. Publ. (to appear).

[2] H. Hasse, *Number Theory.* Akademie Verlag, Berlin 1979

[3] T. Y. Lam, *The algebraic theory of quadratic forms.* W. A. Benjamin, Reading, Mass. 1973.

[4] J. Milnor, D. Husemoller, *Symmetric bilinear forms.* Springer, Berlin 1973.

[5] K. Szymiczek, *On the Milnor exact sequence for rational quadratic forms.* In: Number Theory in Progress. Editors K. Győry *et al.*, Proc. Int. Conf. Number Theory, pp. 531–537. Walter de Gruyter, Berlin-New York 1999.

Author's address: Institute of Mathematics, University of Silesia, Katowice, Poland

E-mail: mc@ux2.math.us.edu.pl

Received: August 2, 2000