Tatra Mt. Math. Publ. **20** (2000), 1–9

Tatra Mountains
Mathematical Publications

WITT EQUIVALENCE OF GLOBAL FUNCTION FIELDS

Marzena Ciemała — Kazimierz Szymiczek

ABSTRACT. We summarize what is known about the Witt equivalence of global function fields and give new direct proofs in the case of global rational function fields.

1. Introduction

Two fields K and L are said to be *Witt equivalent* when their Witt rings WK and WL of symmetric bilinear forms are isomorphic. For global fields the Witt equivalence has been completely described in [PSCL] in terms of a local-global principle. This reads as follows.

Theorem 1.1. *Two global fields K and L are Witt equivalent if and only if their places can be matched bijectively so that the completions of K and L at corresponding places are Witt equivalent.*

An immediate consequence of Theorem 1.1 is the following classification theorem for global function fields (cf. [S1, Theorems (1.1), (1.3)]). Here for a nonreal field K we write $s(K)$ for the level of K (the minimal number of terms in a representation of -1 as a sum of squares in K).

Theorem 1.2. *Let K be a finite extension of the rational function field $\mathbb{F}(X)$, where $\mathbb{F}$ is a finite field.*

(a) *If* char $K = 2$, *then K is Witt equivalent to $\mathbb{F}_2(X)$ and is not Witt equivalent to any field of characteristic different from two.*

(b) *If* char $K \neq 2$, *then $s(K) \leq 2$, and K is Witt equivalent either to $\mathbb{F}_5(X)$ or to $\mathbb{F}_3(X)$ depending on whether $s(K) = 1$ or 2.*

While this final classification theorem for global function fields appears to be quite simple, its proof depends on the machinery of [PSCL].

2000 Mathematics Subject Classification: Primary 11E81; Secondary 11E12.
Keywords: rational function fields, Witt equivalence of fields.

In this paper we prove Theorem 1.1 for global *rational* function fields of odd characteristic, and then we get also Theorem 1.2 in that case. Our proof is direct and more elementary but it is not radically simpler than the one in [PSCL]. Even though rational function fields are the simplest among global fields in many respects they retain the characteristic features of all global fields such as the existence of infinitely many primes and infinitely many square classes. These make the comparison of Witt rings relatively complicated and make it unlike that an elementary proof exists for Theorem 1.1 in the case of global rational function fields. We comment on that at the end of the paper. As explained in [S1] the classification result in case of characteristic two easily follows from the results of the paper [BM] and so we will not discuss it here.

2. Preliminaries

For a global rational function field $K = \mathbb{F}_P(X)$, where $\mathbb{F}_P$ is a finite field of $P = p^k$ elements and of characteristic p, we write Ω_K for the set of all monic irreducible polynomials over $\mathbb{F}_P$. Notice that the elements in the set $\Omega_K \cup \{\infty\}$ correspond bijectively to the primes of the field K, that is, to the equivalence classes of valuations on K. For $\pi \in \Omega_K \cup \{\infty\}$ we write K_π for the completion of K at the prime π. The completions are formal power series fields over finite fields. We have $K_\infty = \mathbb{F}_P\big((X^{-1})\big)$, and for $\pi \in \Omega_K$ and $\deg \pi = m$, we have $K_\pi = \mathbb{F}_{P^m}\big((\pi)\big)$. Observe that $K_X = \mathbb{F}_P\big((X)\big)$ and $K_\infty = \mathbb{F}_P\big((X^{-1})\big)$ are isomorphic fields, hence they are Witt equivalent. The following classification results are well known.

Lemma 2.1. *For finite fields $\mathbb{F}_P$ and $\mathbb{F}_Q$ of odd characteristics the following statements are equivalent.*

(a) *$\mathbb{F}_P$ and $\mathbb{F}_Q$ are Witt equivalent.*

(b) $s(\mathbb{F}_P) = s(\mathbb{F}_Q)$.

(c) $P \equiv Q \pmod 4$.

Moreover, $s(\mathbb{F}_P) = 1$ *when* $P \equiv 1 \pmod 4$ *and* $s(\mathbb{F}_P) = 2$ *when* $P \equiv 3 \pmod 4$.

P r o o f. See [L, p. 45 and p. 304]. □

Lemma 2.2. *Let $K = \mathbb{F}_P(X)$ and $L = \mathbb{F}_Q(X)$ be global rational function fields each of odd characteristic. Let $\pi \in \Omega_K \cup \{\infty\}$ and $\rho \in \Omega_L \cup \{\infty\}$ be any primes of K and L, respectively. The following statements are equivalent.*

(a) *The completions K_π and L_ρ are Witt equivalent.*

(b) $s(K_\pi) = s(L_\rho)$.

Moreover, if $\pi \in \Omega_K$ *and* $\rho \in \Omega_L$, $\deg \pi = m$, $\deg \rho = n$, *then each* (a) *and* (b) *is equivalent to*

(c) $P^m \equiv Q^n \pmod 4$.

P r o o f. Each completion K_π is a local field with four square classes. The equivalence of (a) and (b) follows from [S2, Appendix B.10.7, p. 468]. And using Lemma 2.1 we get

$$(c) \iff s(\mathbb{F}_{P^m}) = s(\mathbb{F}_{Q^n}) \iff s\big(\mathbb{F}_{P^m}((\pi))\big) = s\big(\mathbb{F}_{Q^n}((\rho))\big) \iff (b).$$

□

Lemma 2.3. *Let* $\mathbb{F}$ *be a finite field of odd characteristic and let* $K = \mathbb{F}(X)$ *be the rational function field over* $\mathbb{F}$. *Let* $\alpha_1, \dots, \alpha_n \in \mathbb{F}[X]$ *be a finite set of polynomials multiplicatively independent in the group of square classes* K^*/K^{*2}. *For any* $\varepsilon_1, \dots, \varepsilon_n$ *in* $\{\pm 1\}$ *there are infinitely many polynomials* $\pi \in \Omega_K$ *satisfying*

$$\left(\frac{\alpha_1}{\pi}\right) = \varepsilon_1, \dots, \left(\frac{\alpha_n}{\pi}\right) = \varepsilon_n .$$

P r o o f. This is an analog of a well known result in number fields (see [He, Satz 147, Satz 169]). We discuss the proof in the Appendix at the end of the paper. □

3. Witt equivalence of rational function fields

For global rational function fields K and L we consider the following six properties.

(A) K and L are Witt equivalent.

(B) $s(K) = s(L)$.

(C) There is a bijective map $T\colon \Omega_K \to \Omega_L$ such that for all $\pi \in \Omega_K$ we have $\deg \pi \equiv \deg T\pi \pmod 2$ and K_π and $L_{T\pi}$ are Witt equivalent.

(D) There is a bijective map $T\colon \Omega_K \cup \{\infty\} \to \Omega_L \cup \{\infty\}$ such that K_π and $L_{T\pi}$ are Witt equivalent for all $\pi \in \Omega_K \cup \{\infty\}$.

(E) There is a bijective map $T\colon \Omega_K \to \Omega_L$ such that for all $\pi, \rho \in \Omega_K$,

$$\rho \in K_\pi^{*2} \iff T\rho \in L_{T\pi}^{*2} \qquad \text{and} \qquad -1 \in K_\pi^{*2} \iff -1 \in L_{T\pi}^{*2}.$$

(F) There is a Hilbert-symbol equivalence (t, T) between K and L such that

$$t(\pi K^{*2}) = T\pi\, L^{*2} \qquad \text{for all} \quad \pi \in \Omega_K .$$

The property (D) expresses the fact that K and L are *locally* Witt equivalent. Theorems 1.1 and 1.2 assert that for global function fields we have (A) $\iff$ (D), and in case of odd characteristic (A) $\iff$ (B), respectively. We will prove that for global rational function fields of odd characteristic the six properties are pairwise equivalent.

THEOREM 3.1. *Let $K = \mathbb{F}_P(X)$ and $L = \mathbb{F}_Q(X)$ be global rational function fields of odd characteristic. Then*

$$(\mathrm{A}) \iff (\mathrm{B}) \iff (\mathrm{C}) \iff (\mathrm{D}) \iff (\mathrm{E}) \iff (\mathrm{F}).$$

Proof. We will prove the Theorem in three steps. First we show that (A) $\Rightarrow$ (B), then (B) $\Rightarrow$ (C) $\Rightarrow$ (D) $\Rightarrow$ (B), and in the final step we prove (B) $\Rightarrow$ (E) $\Rightarrow$ (F) $\Rightarrow$ (A).

Part 1.

(A) $\Rightarrow$ (B). This follows from the fact that for a nonreal field K of level s the exponent of the additive group of the Witt ring WK equals $2s$ (see [L, Corollary 2.3, p. 303]).

Part 2.

(B) $\Rightarrow$ (C). Write $\Omega_K = \Omega_K^0 \cup \Omega_K^1$, where for $i = 0, 1$,

$$\Omega_K^i = \{\pi \in \Omega_K \colon \deg \pi \equiv i \pmod 2\}.$$

We also split the set Ω_L into the union of two subsets consisting of polynomials with the same parity of degrees, and then we choose arbitrary bijections

$$T_i \colon \Omega_K^i \to \Omega_L^i, \quad i = 0, 1.$$

We define $T \colon \Omega_K \to \Omega_L$ by setting $T = T_i$ on Ω_K^i. We show that the bijective map T satisfies (C). So let $\pi \in \Omega_K^i$ and $\deg \pi = m$, $\deg T\pi = n$ for some positive integers m and n of the same parity. Then, by Lemma 2.1, from $s(\mathbb{F}_P) = s(\mathbb{F}_Q)$ it follows that $P \equiv Q \pmod 4$, hence also $P^m \equiv Q^n \pmod 4$ and so, by Lemma 2.2, K_π and $L_{T\pi}$ are Witt equivalent, as desired.

(C) $\Rightarrow$ (D). We extend the given map T by putting $T(\infty) = \infty$. Take any $\pi \in \Omega_K$ of odd degree m. Then the corresponding $\rho = T\pi \in \Omega_L$ has also odd degree n, say, and K_π and L_ρ have the same levels. Hence $P^m \equiv Q^n \pmod 4$. Since m, n are odd, it follows that $P \equiv Q \mod 4$ and so we have $s(\mathbb{F}_P) = s(\mathbb{F}_Q)$. Hence $WK_\infty \cong W\mathbb{F}_P\big((X)\big) \cong W\mathbb{F}_Q\big((X)\big) \cong WL_\infty$, as required.

(D) $\Rightarrow$ (B). By the Lemma 2.2, $s(K_\pi) = s(L_{T\pi})$ for all $\pi \in \Omega_K \cup \{\infty\}$. Hence, by the Strong Hasse Principle, $s(K) = s(L)$.

Part 3.

(B) $\Rightarrow$ (E). We set up the bijective map satisfying (E) by induction bouncing forth and back between Ω_K and Ω_L. To start with take the polynomial $\pi_1 = X \in \Omega_K$. By definition we set $T(\pi_1) = \rho_1$, where $\rho_1 = X \in \Omega_L$. Then we have

$$K_{\pi_1} = \mathbb{F}_P((X)) \qquad \text{and} \qquad L_{\rho_1} = \mathbb{F}_Q((X)).$$

By (B), the fields $\mathbb{F}_P(X)$ and $\mathbb{F}_Q(X)$ have the same level, hence also K_{π_1} and L_{ρ_1} have the same level, and so $-1 \in K_{\pi_1}^{*2} \iff -1 \in L_{T\pi_1}^{*2}$ as required.

In the second step we pick up a polynomial ρ_2 of the lowest degree in $\Omega_L \setminus \{\rho_1\}$. Then we use Lemma 2.3 to find a $\pi_2 \in \Omega_K \setminus \{\pi_1\}$ satisfying

$$\left(\frac{\pi_1}{\pi_2}\right) = \left(\frac{\rho_1}{\rho_2}\right), \quad \left(\frac{-1}{\pi_2}\right) = \left(\frac{-1}{\rho_2}\right).$$

The next step is to pick up a polynomial π_3 of the lowest degree in the set $\Omega_K \setminus \{\pi_1, \pi_2\}$ and to find a $\rho_3 \in \Omega_L \setminus \{\rho_1, \rho_2\}$ satisfying

$$\left(\frac{\pi_1}{\pi_3}\right) = \left(\frac{\rho_1}{\rho_3}\right), \quad \left(\frac{\pi_2}{\pi_3}\right) = \left(\frac{\rho_2}{\rho_3}\right), \quad \left(\frac{-1}{\pi_3}\right) = \left(\frac{-1}{\rho_3}\right).$$

Then for ρ_4 of the lowest degree in $\Omega_L \setminus \{\rho_1, \rho_2, \rho_3\}$ a $\pi_4 \in \Omega_K \setminus \{\pi_1, \pi_2, \pi_3\}$ is chosen satisfying

$$\left(\frac{\pi_1}{\pi_4}\right) = \left(\frac{\rho_1}{\rho_4}\right), \quad \left(\frac{\pi_2}{\pi_4}\right) = \left(\frac{\rho_2}{\rho_4}\right), \quad \left(\frac{\pi_3}{\pi_4}\right) = \left(\frac{\rho_3}{\rho_4}\right), \quad \left(\frac{-1}{\pi_4}\right) = \left(\frac{-1}{\rho_4}\right).$$

We continue the process and as a result we get a bijective map

$$T\colon \Omega_K \longrightarrow \Omega_L, \qquad T\pi_i = \rho_i, \quad i = 1, 2, \ldots$$

satisfying

$$\left(\frac{\pi_i}{\pi_j}\right) = \left(\frac{\rho_i}{\rho_j}\right) \quad \text{for all} \quad i < j \qquad \text{and} \qquad \left(\frac{-1}{\pi_i}\right) = \left(\frac{-1}{\rho_i}\right) \quad \text{for all} \quad i.$$

Observe that when $s = 2$ the map T preserves the parity of the degrees of the polynomials. Indeed,

$$(-1)^{\deg \pi_i} = \left(\frac{-1}{\pi_i}\right) = \left(\frac{-1}{\rho_i}\right) = (-1)^{\deg \rho_i}.$$

When $s = 1$, (B) and Lemma 2.1 imply that $\frac{P-1}{2} \equiv \frac{Q-1}{2} \equiv 0 \pmod 2$. Hence, by the quadratic reciprocity law (see [Ha, p. 103]),

$$\begin{aligned}\left(\frac{\pi_j}{\pi_i}\right) &= \left(\frac{\pi_i}{\pi_j}\right) \cdot (-1)^{\deg \pi_i \cdot \deg \pi_j \cdot \frac{P-1}{2}} \\ &= \left(\frac{\rho_i}{\rho_j}\right) \cdot (-1)^{\deg \rho_i \cdot \deg \rho_j \cdot \frac{Q-1}{2}} \\ &= \left(\frac{\rho_j}{\rho_i}\right).\end{aligned}$$

Thus we have shown that $\left(\frac{\pi_i}{\pi_j}\right) = \left(\frac{\rho_i}{\rho_j}\right)$ holds for all i, j. And this together with $\left(\frac{-1}{\pi_i}\right) = \left(\frac{-1}{\rho_i}\right)$ for all i, is just the condition (E) expressed in terms of residue class fields and Legendre's symbols.

(E) $\Rightarrow$ (F). K is the field of quotients of the unique factorization domain $\mathbb{F}_P[X]$, hence it follows that with $a \in \mathbb{F}_P^* \setminus \mathbb{F}_P^{*2}$,

$$K^*/K^{*2} = \{K^{*2}, aK^{*2}\} \oplus \bigoplus_{\pi \in \Omega_K} \{K^{*2}, \pi K^{*2}\}.$$

We define the square class group isomorphism $t\colon K^*/K^{*2} \to L^*/L^{*2}$ to be the unique group isomorphism satisfying

$$t(aK^{*2}) = bL^{*2} \qquad \text{and} \qquad t(\pi K^{*2}) = (T\pi)L^{*2},$$

where b is a non-square in $\mathbb{F}_Q$ and $\pi \in \Omega_K$.

We will prove that t and T preserve Hilbert symbols. First observe that for any $\sigma, \rho, \pi \in \Omega_K$,

$$(a, \sigma)_\pi = (b, T\sigma)_\pi \qquad \text{and} \qquad (\sigma, \rho)_\pi = (T\sigma, T\rho)_{T\pi}\,. \tag{3.1}$$

If $\sigma \neq \pi$ we have $(a, \sigma)_\pi = 1$ and $(b, T\sigma)_{T\pi} = 1$, and if $\sigma = \pi$, both symbols equal -1. To prove the second equality consider three cases.

If $\pi \neq \sigma$, $\pi \neq \rho$ both symbols equal 1.

If $\pi = \sigma$, $\pi \neq \rho$, we have

$$(\pi, \rho)_\pi = 1 \iff \rho \in K_\pi^{*2} \iff T\rho \in L_{T\pi}^{*2} \iff (T\pi, T\rho)_{T\pi} = 1\,.$$

If $\pi = \sigma$, $\pi = \rho$, we have

$$(\pi, \pi)_\pi = (\pi, -1)_\pi = (T\pi, -1)_{T\pi} = (T\pi, T\pi)_{T\pi}\,,$$

where in the middle we have used $(\pi, -1)_\pi = 1 \iff -1 \in K_\pi^{*2}$, and (E).

Now we consider the general case. Take $\alpha, \beta \in K^*$. Computing the Hilbert symbol $(\alpha, \beta)_\pi$ we can assume that α, β are separable polynomials, and then

$$\alpha = a^\varepsilon \prod \sigma_i\,, \quad \beta = a^\eta \prod \rho_j$$

for $\varepsilon, \eta \in \{0, 1\}$ and some $\sigma_i, \rho_j \in \Omega_K$. Then, using (3.1), we have

$$\begin{aligned}
(\alpha, \beta)_\pi &= \prod_j (a^\varepsilon, \rho_j)_\pi \prod_i (\sigma_i, a^\eta)_\pi \prod_{i,j} (\sigma_i, \rho_j)_\pi\,, \\
&= \prod_j (b^\varepsilon, T\rho_j)_{T\pi} \prod_i (T\sigma_i, b^\eta)_{T\pi} \prod_{i,j} (T\sigma_i, T\rho_j)_{T\pi}\,, \\
&= (t\alpha, t\beta)_{T\pi}\,.
\end{aligned}$$

This proves (F).

(F) $\Rightarrow$ (A). K and L are Hilbert-symbol equivalent and so they are Witt equivalent (by [PSCL, Corollary 1, p. 372]). $\square$

Remark 3.2. It is somewhat remarkable that we do not know any direct proof of (B) $\Rightarrow$ (A). The above proof interprets (B) in terms of local conditions and then laboriously constructs the Witt ring isomorphism between K and L. On the other hand, condition (E) shows that the Witt equivalence of K and L requires a perfect matching of the primes preserving the quadratic interdependences between all pairs of primes. So it is unlike that such a matching can be produced directly by declaring the action of T on Ω_K by a simple and concise formula. For instance, while (C) and (E) are equivalent conditions, preserving the parity of degrees of prime polynomials is by far insufficient to produce Hilbert equivalence in (F). For this we need much more refined matching in (E). So in any attempt to simplify the proof of (B) $\Rightarrow$ (A) we cannot hope for a radical simplification of the above proof.

Acknowledgment. We are grateful to Dr. A. Czogała for pointing out an oversimplification in an earlier version of the paper.

4. Appendix

Here we explain how a proof of Lemma 2.3 can be obtained in the case when $K = \mathbb{F}_p(X)$, p a prime, by using the method applied in the rational number field case by E. Hecke in [He, Satz 147]. Then we also deduce the result in full generality from [OM, 68:17].

The Dedekind zeta function $\zeta_k(s)$ of the quadratic extension $k = \mathbb{Q}(\sqrt{d})$ of the rational number field can be written as the product $\zeta_k(s) = \zeta(s)L(s)$, where $\zeta(s)$ is the Riemann zeta function and

$$L(s) = \prod_p \left(1 - \left(\frac{d}{p}\right)p^{-s}\right)^{-1},$$

the product running over all primes. From the limit formula for $\zeta(s)$ one then obtains

$$\lim_{s\to 1} L(s) = h\kappa > 0\,.$$

Hecke's proof of his Satz 147 is based solely on the fact that the limit $\lim\limits_{s\to 1} L(s)$ exists and is a positive number.

Now a parallel discussion of the Dedekind's zeta function for quadratic extension $\mathbb{F}_p(X)(\sqrt{D})$ of the rational function field $\mathbb{F}_p(X)$ over the prime field

$\mathbb{F}_p$ can be found in the analytical part of Artin's thesis [Ar]. He factorizes the zeta function

$$\mathbf{Z}(s) = \eta(s) \cdot \mathbf{L}(s),$$

with $\eta(s) = (1 - p^{1-s})^{-1}$ and

$$\mathbf{L}(s) = \prod_{\pi} \left(1 - \left(\frac{D}{\pi}\right) \cdot |\pi|^s\right)^{-1}.$$

Here π runs through monic irreducible polynomials in $\mathbb{F}_p[X]$ and $|\pi| = p^n$ where $n = \deg \pi$ ([Ar, p. 209]). He establishes the limit formula

$$\lim_{s \to 1} (s-1)\mathbf{Z}(s) = \frac{h}{\varkappa \log p} > 0,$$

where h is the class number and $\varkappa$ is a positive constant depending on the field ([Ar, p. 220]). Then, since $\lim_{s \to 1} (s-1)\eta(s) = 1/\log p$, it follows that

$$\lim_{s \to 1} \mathbf{L}(s) = \frac{h}{\varkappa \log^2 p} > 0.$$

Now Hecke's arguments apply to $\mathbf{L}(s)$ and give a proof of the Lemma 2.3 in the case when $\mathbb{F} = \mathbb{F}_p$ is the prime field of p elements.

Finally we notice that a purely algebraic proof of the Lemma 2.3 is given in [OM, 65:17]. In O'Meara's notation and terminology we write S for the set of spots on $K = \mathbb{F}(X)$ determined by irreducible polynomials not dividing the product $\alpha_1 \cdots \alpha_n$. Since the polynomials α_i are assumed to be multiplicatively independent in the group of square classes of K, their set can be extended to a set of generators $\alpha_1, \dots, \alpha_s$ of the group of units $\mathfrak{u}(S)$ modulo squares. Rearranging the α_i's if necessary we can assume that $\varepsilon_1 = \dots = \varepsilon_k = -1$ and $\varepsilon_{k+1} = \dots = \varepsilon_s = 1$. Then according to [OM, 65:17] there are infinitely many spots $\mathfrak{p}$ in S such that

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right) = -1, \quad \left(\frac{\alpha_1 \alpha_2}{\mathfrak{p}}\right) = \dots = \left(\frac{\alpha_1 \alpha_k}{\mathfrak{p}}\right) = \left(\frac{\alpha_{k+1}}{\mathfrak{p}}\right) = \dots = \left(\frac{\alpha_s}{\mathfrak{p}}\right) = 1.$$

The polynomials $\pi \in \Omega_K$ determining the spots $\mathfrak{p}$ satisfy the requirements of the Lemma 2.3.

REFERENCES

[Ar] ARTIN, E.: *Quadratische Körper im Gebiete der höheren Kongruenzen. II.*, Math. Zeitschr. **19** (1924), 207–246.

[BM] BAEZA, R.—MORESI, R.: *On the Witt-equivalence of fields of characteristic 2.*, J. Algebra **92** (1985), 446–453.

[Ha] HASSE, H.: *Number Theory*, Akademie Verlag, Berlin, 1979.

[He] HECKE, E.: *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

[L] LAM, T. Y.: *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, Mass, 1973.

[OM] O'MEARA, O. T.: *Introduction to Quadratic Forms*, Grundlehren der mathematischen Wissenschaften **117**., Springer-Verlag, Berlin, 1971.

[PSCL] PERLIS, R.—SZYMICZEK, K.—CONNER, P. E.—LITHERLAND, R.: *Matching Witts with global fields*, Contemp. Math. **155** (1994), 365–387.

[S1] SZYMICZEK, K.: *Witt equivalence of global fields*, Commun. Algebra **19** (1991), 1125–1149.

[S2] SZYMICZEK, K.: *Bilinear Algebra*, Gordon and Breach, Amsterdam, 1997.

Received September 10, 1999

Institute of Mathematics
University of Silesia
Bankowa 14
PL–40–007 Katowice
POLAND

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