Functiones et Approximatio
XXVIII (2000), 243–252

Dedicated to Professor W. Staś on the occasion of his 75th birthday

WITT RINGS OF GLOBAL FUNCTION FIELDS

Alfred Czogała

Abstract: We give an explicit description of Witt rings of of global function fields.
Keywords: Global function fields; Witt rings.

1. Introduction

A fundamental problem in the algebraic theory of quadratic forms over a field K is to determine the structure of the Witt ring $W(K)$ of the field K and to classify fields with respect to isomorphism type of their Witt rings. Two fields with isomorphic Witt rings are said to be *Witt equivalent.*

For global fields the Witt equivalence has been completely described in [4] in terms of the following local-global principle.

1.1. *Two global fields K and L are Witt equivalent if and only if there is a bijective matching of primes of K and L such that the completions of K and L at corresponding places are Witt equivalent.*

As a result one obtains a very simple criterion for the Witt equivalence of global function fields.

1.2. *Two global function fields K and L of characteristic different from 2 are Witt equivalent if and only if they have the same level.*

Thus we have definitive answers to the problem of comparing Witt rings of global fields. This, however, does not mean that we can explicitly describe the structure of the Witt ring of all global fields. An explicit description of the Witt ring of the rational number field $\mathbb{Q}$ has been found in [1]. Here we will give a similar description of Witt rings of global function fields. This will be accomplished by adapting the approach presented in [1] to the function field case.

Global function fields having different levels have non-isomorphic Witt rings. Thus we will consider fields with level one or two separately.

1991 Mathematics Subject Classification: Primary 11E81; Secondary 11E12.

2. Preliminaries

From now on K denotes a global function field of characteristic different from 2 with finite constant field $\mathbb{F}$, i.e. K is a finite extension of the field $\mathbb{F}(X)$, where X is transcendental over $\mathbb{F}$. From [2, p. 45 and p. 304] it follows that the level $s(K)$ of the field K is equal to 1, when $|\mathbb{F}| \equiv 1 \pmod 4$ and is equal to 2, when $|\mathbb{F}| \equiv 3 \pmod 4$. We use Ω_K for the set of all primes of K. For $\mathfrak{p} \in \Omega_K$ we write $(\ .\ )_{\mathfrak{p}}$ for the $\mathfrak{p}$-adic Hilbert symbol.

Following [4] we consider the collection Γ_K of finite even-order subsets of Ω_K. The symmetric difference $A + B = (A \cup B) \setminus A \cap B$ of two elements of Γ_K again lies in Γ_K and $(\Gamma_K, +)$ is an infinite elementary abelian 2-group, the zero element being the empty set. For $a, b \in \dot{K}$ let

$$(a|b) = \{\mathfrak{p} \in \Omega_K \ :\ (a,b)_{\mathfrak{p}} = -1\}.$$

From the Hilbert's Reciprocity Law (see [3, p. 190]) it follows that $(a|b) \in \Gamma_K$ for each $a, b \in \dot{K}$. As a direct consequence of the properties of the Hilbert symbols we obtain the following:

Proposition 2.1. *For all* $a, b, c \in \dot{K}$ *and* $x, y \in \dot{\mathbb{F}}$,

(1) $(a|b) = (b|a)$,
(2) $(ab|c) = (a|c) + (b|c)$,
(3) $(ac^2|b) = (a|b)$,
(4) $(a|a) = (-1|a)$,
(5) $(a|-a) = \emptyset, \quad (a|1-a) = \emptyset, \quad (x|y) = \emptyset$.

We recall now some notions and facts connected with the Witt ring of K.

Every Witt class $\varphi \in W(K)$ can be represented by the diagonalized form $\langle a_1, a_2, \ldots, a_n\rangle$ where $a_1, a_2, \ldots, a_n \in \dot{K}$. In [2, p. 49] we find the following representation of $W(K)$,

$$W(K) \cong \mathcal{F}/\mathcal{R}$$

where $\mathcal{F}$ is the commutative ring generated by the symbols $\langle a\rangle$, $a \in \dot{K}$ and $\mathcal{R}$ is the ideal generated by the elements

$$\begin{aligned}
&\langle 1\rangle - 1,\\
&\langle 1\rangle + \langle -1\rangle,\\
&\langle ab\rangle - \langle a\rangle \cdot \langle b\rangle, \qquad (a, b \in \dot{K}),\\
&\langle a\rangle + \langle b\rangle - \langle a+b\rangle \cdot (1 + \langle ab\rangle), \qquad (a, b, a+b \in \dot{K}).
\end{aligned}$$

By the universal property of the free commutative ring we obtain

Corollary 2.2. *Let P be a commutative ring and let $\rho : \dot{K} \to P$ be the map satisfying the following conditions:*

(1) $\rho(1) = 1$,
(2) $\rho(-1) = -1$,
(3) $\rho(ab) = \rho(a)\rho(b), \qquad (a, b \in \dot{K})$,
(4) $\rho(a) + \rho(b) = \rho(a+b)(1 + \rho(ab), \qquad (a, b, a+b \in \dot{K})$.

Then there exists a unique ring homomorphism $\Theta : W(K) \to P$ *with* $\Theta(\langle a\rangle) = \rho(a)$.

The fundamental ideal $I(K)$ consisting of Witt classes of even rank, is the unique ideal of index 2 in the Witt ring $W(K)$. There exists a unique ring isomorphism $e : W(K)/I(K) \cong \mathbb{Z}_2$. The field K is not formally real, so the ring $W(K)$ is a local ring and $I(K)$ is the unique maximal ideal of $W(K)$ (see [2, Corollary 5.6]). The ideal $I(K)$ is additively generated by the forms $\langle 1, -a\rangle$ (where $a \in \dot{K}$), so its square $I^2(K)$ is additively generated by the forms $\langle 1, -a\rangle \otimes \langle 1, -b\rangle = \langle 1, -a, -b, ab\rangle$ (where $a, b \in \dot{K}$).

The discriminant map disc : $W(K) \to \dot{K}/\dot{K}^2$ induces a group isomorphism $d : I(K)/I^2(K) \cong \dot{K}/\dot{K}^2$ sending the coset of the form $\langle 1, -a\rangle$ to the square class of a (see [2, Corollary 2.3]).

From [2, p. 172] it follows that $I^3(K) = 0$ and the Hasse-Witt invariant induces a group isomorphism of $I^2(K)$ onto the 2-torsion subgroup $\mathrm{Br}_2(K)$ of the Brauer group of K. This isomorphism sends the Witt class of the form $\langle 1, -a, -b, ab\rangle$ to the class of the quaternion algebra $(a, b)_K$. Every class in $\mathrm{Br}_2(K)$ is represented by simple quaternion algebra (see [2, p. 171]). The theorem of Brauer-Albert-Hasse-Noether shows that class of $(a, b)_K$ is completely determined by the set $(a|b)$ of primes where it is nonsplit. Therefore, there exists a group isomorphism $w : I^2(K) \cong \Gamma_K$ such that $w(\langle 1, -a, -b, ab\rangle) = (a|b)$.

For $a \in \dot{K}$ we write $\hat{a}$ for the square class $a\dot{K}^2$ and we denote $(\hat{a}|\hat{b}) = (a|b)$.

3. Witt rings of global function fields with level 2

In this section we describe the Witt ring of K in the case when $s(K) = 2$. In this case -1 is a non-square in K. Fix a subgroup K_0 of index 2 in the group $\dot{K}$ such that $-1 \notin K_0$. Then we have the decomposition of the square class group of the field K,

$$\dot{K}/\dot{K}^2 = \{\hat{1}, -\hat{1}\} \oplus K_0/\dot{K}^2.$$

We set

$$V(K) = \mathbb{Z}_4 \times K_0/\dot{K}^2 \times \Gamma_K.$$

We define addition and multiplication in $V(K)$ by

$$(n, \hat{a}, A) + (m, \hat{b}, B) = (n + m, \hat{a}\hat{b}, A + B + (a|b)),$$

$$(n, \hat{a}, A) \cdot (m, \hat{b}, B) =$$

$$(nm, \hat{a}^m\hat{b}^n, mA + nB + \frac{m(m-1)}{2}(a|a) + \frac{n(n-1)}{2}(b|b) + (mn+1)(a|b)).$$

Theorem 3.1. *$V(K)$ is a commutative ring with identity.*

Proof. We notice that the zero element 0 in $V(K)$ is $(0, \hat{1}, \emptyset)$, the identity 1 in $V(K)$ is $(1, \hat{1}, \emptyset)$ and the opposite element to $(n, \hat{a}, A)$ is $-(n, \hat{a}, A) =$

$(-n,\, \hat{a},\, A+(-1|a))$. It is a routine matter to check the remaining axioms. The additive order of the identity element in $V(K)$ is equal to 4. ∎

Let $J(K)$ be the set of all $(n,\, \hat{a},\, A) \in V(K)$ such that $n=0$ or 2. It is easy to verify that $J(K)$ is an ideal of $V(K)$. For every $\alpha = (n,\, \hat{a},\, A) \in V(K) \setminus J(K)$ we have $\alpha + 1 \in J(K)$, so the index of $J(K)$ in $V(K)$ is equal to 2. Thus, there exists a unique isomorphism $f : V(K)/J(K) \to \mathbb{Z}_2$.

Proposition 3.2. *The ring $V(K)$ is a local ring and $J(K)$ is the unique maximal ideal of $V(K)$,*

Proof. Let's observe that the equality $(n,\, \hat{a},\, A)^4 = (0,\, \hat{1},\, (a|a))^2 = 0$ holds for every $(n,\, \hat{a},\, A) \in J(K)$. For each $\alpha \in V(K) \setminus J(K)$ the element $\alpha + 1$ belongs to $J(K)$, hence $0 = (1+\alpha)^4 = \alpha\beta + 1$ for some element $\beta \in V(K)$. Therefore, α is invertible in $V(K)$. ∎

Proposition 3.3.

(i) $J^2(K) = \{\, (0,\, \hat{1},\, A) \,:\, A \in \Gamma_K \,\}$,
(ii) $J^3(K) = 0$.

Proof. (i) The inclusion $\subseteq$ is obvious. For the reverse inclusion, let $A \in \Gamma_K$. From [3, 71:19] it follows that there exists $a \in \dot{K}$ such that $(-1|a) = A$. Since $(-1|\pm a) = (-1|a)$ we can assume $a \in K_0$. Then $(2,\, \hat{1},\, \emptyset) \cdot (2,\, \hat{a},\, \emptyset) = (0,\, \hat{1},\, A)$, so $(0,\, \hat{1},\, A) \in J^2(K)$. The proof of (ii) is easy. ∎

Corollary 3.4. *The map $v : J^2(K) \to \Gamma_K$ such that $v((0,\, \hat{1},\, A)) = A$ is a group isomorphism.*

Consider the map $g : \dot{K}/\dot{K}^2 \to J(K)/J^2(K)$,

$$g(\hat{a}) = \begin{cases} (0,\, \hat{a},\, \emptyset) + J^2(K) & \text{if } a \in K_0 \\ (2,\, -\hat{a},\, \emptyset) + J^2(K) & \text{if } a \notin K_0. \end{cases}$$

Lemma 3.5. *The map g is a group isomorphism.*

Proof. It is easy to verify that g is a group homomorphism. From the definition of g we deduce that $g(\hat{a}) = J^2(K)$ if and only if $a \in K_0$ and $\hat{a} = \hat{1}$. Suppose $(n,\, \hat{a},\, A)$ is an element of $J(K)$. If $n=0$, then $(0,\, \hat{a},\, A) + J^2(K) = (0,\, \hat{a},\, \emptyset) + J^2(K) = g(\hat{a})$, and next, if $n=2$, then $(2,\, \hat{a},\, A) + J^2(K) = (2,\, \hat{a},\, \emptyset) + J^2(K) = g(-\hat{a})$, because $-a \notin K_0$. ∎

Lemma 3.6. *If $\alpha \in g(\hat{a})$, $\beta \in g(\hat{b})$, then $\alpha\beta = (0,\, \hat{1},\, (a|b))$.*

Proof. If $a, b \in K_0$, then $\alpha = (0,\, \hat{a},\, \emptyset) + \gamma_1$ and $\beta = (0,\, \hat{b},\, \emptyset) + \gamma_2$ for some $\gamma_1, \gamma_2 \in J^2(K)$. Hence $\alpha\beta = (0,\, \hat{1},\, (a|b))$, because $J^3(K) = 0$. Now assume that $a \in K_0, b \notin K_0$. In this case $\alpha = (0,\, \hat{a},\, \emptyset) + \gamma_1$ and $\beta = (2,\, -\hat{b},\, \emptyset) + \gamma_2$ where $\gamma_1, \gamma_2 \in J^2(K)$. Similarly as above we have $\alpha\beta = (0,\, \hat{1},\, (a|a) + (a|-b)) =$

$(0,\, \hat{1},\, (a|b))$. Checking the statement when $a \notin K_0$, $b \notin K_0$ is done in analogous way. ∎

Now we proceed to constructing an isomorphism between $W(K)$ and $V(K)$. Consider the map $r : \dot{K} \to V(K)$,

$$r(a) = \begin{cases} (1,\, \hat{a},\, (a|a)) & \text{if } a \in K_0, \\ (-1,\, -\hat{a},\, \emptyset) & \text{if } a \notin K_0. \end{cases}$$

Proposition 3.7. *For all $a, b \in \dot{K}$,*

(1) $r(1) = 1$,
(2) $r(-1) = -1$,
(3) $r(ab) = r(a)r(b)$,
(4) $r(a) + r(b) = r(a+b)(1 + r(ab))$, *when* $a + b \neq 0$.

Proof. The first two assertions are clear. To verify (3) there are three cases to consider: $a, b \in K_0$ or $a \notin K_0$, $b \notin K_0$ or $a \in K_0$, $b \notin K_0$. Let's consider the last case. In this case $ab \notin K_0$ and we have $r(a)r(b) = (1,\, \hat{a},\, (a|a)) \cdot (-1,\, -\hat{b},\, \emptyset) = (-1,\, -\hat{ab},\, \emptyset) = r(ab)$. Verifying (3) in the remaining cases proceeds in an analogous way. Observe now that $r(a)^2 = 1$ for every $a \in \dot{K}$, so from (3) we obtain $r(a^2) = 1$.

Notice that if $a + b = 1$ then $r(a) + r(b) = 1 + r(ab)$. Indeed, it follows from Proposition 2.1 that $(a|b) = \emptyset$, so $(-a|-b) = (a|a) + (b|b)$. If $a \notin K_0$, $b \notin K_0$, then $r(a) + r(b) = (-1,\, -\hat{a},\, \emptyset) + (-1,\, -\hat{b},\, \emptyset) = (2,\, \hat{a}\hat{b},\, (-a|-b))$. On the other hand $ab \in K_0$, so $1 + r(ab) = (1,\, \hat{1},\, \emptyset)) + (1,\, \hat{ab},\, (ab|ab)) = (2,\, \hat{a}\hat{b},\, (ab|ab))$. Now it suffices to notice that $(ab|ab) = (-1|ab) = (a|a) + (b|b)$. The remaining cases are similar.

Assume $a + b = c \neq 0$. Then $ac^{-1} + bc^{-1} = 1$. From the above and (3) we have $r(ac^{-1}) + r(bc^{-1}) = 1 + r(abc^{-2}) = 1 + r(ab)$. On the other hand $r(ac^{-1}) + r(bc^{-1}) = r(c^{-1})(r(a) + r(b))$, so $r(c^{-1})(r(a) + r(b)) = 1 + r(ab)$. Multiplying the last equality by $r(c)$ and using (3) we obtain (4). ∎

From the above and Corollary 2.2 we obtain

Corollary 3.8. *There exists a unique ring homomorphism $\Phi : W(K) \to V(K)$ such that $\Phi(\langle a \rangle) = r(a)$ for all $a \in \dot{K}$.*

Lemma 3.9. *Let the homomorphism $\Phi : W(K) \to V(K)$ be as above. Then*

(1) $\Phi^{-1}(J(K)) = I(K)$,
(2) $\Phi^{-1}(J^2(K)) = I^2(K)$.

Proof. (1) Let's note first that, directly from the definition of the map r,

$$1 + r(-a) = \begin{cases} (0,\, \hat{a},\, \emptyset) & \text{if } a \in K_0, \\ (2,\, -\hat{a},\, (a|a)) & \text{if } a \notin K_0. \end{cases} \tag{$*$}$$

Hence $\Phi(\langle 1, -a \rangle) \in J(K)$. The ideal $I(K)$ is additively generated by the forms $\langle 1, -a \rangle$ (where $a \in \dot{K}$), so $I(K) \subseteq \Phi^{-1}(J(K))$. The ideal $I(K)$ is the unique maximal ideal of $W(K)$ and $\Phi^{-1}(J(K))$ is a proper ideal of $W(K)$, hence $\Phi^{-1}(J(K)) \subseteq I(K)$.

(2) The inclusion $\supseteq$ follows from $\Phi(I^2(K)) \subseteq (\Phi(I(K)))^2 \subseteq J^2(K)$.

Assume $\varphi \in \Phi^{-1}(J^2(K))$, then $\Phi(\varphi) \in J^2(K) \subseteq J(K)$. From (1) we have $\varphi \in \Phi^{-1}(J(K)) = I(K)$. Let $\hat{a}$ be the discriminant of the form φ, then the discriminant of $\varphi + \langle 1, -a\rangle$ is equal to 1, so $\varphi + \langle 1, -a\rangle \in I^2(K)$. Since $\Phi(\varphi)$ belongs to $J^2(K)$ and $\Phi(I^2(K)) \subseteq J^2(K)$, hence $1 + r(-a) = \Phi(\langle 1, -a\rangle) \in J^2(K)$. From $(*)$ it follows that $\hat{a} = \hat{1}$, so $\langle 1, -a\rangle = 0$. Therefore $\varphi \in I^2(K)$. ■

Lemma 3.10. *If $a, b \in \dot{K}$ then $v((1 + r(-a))(1 + r(-b))) = (a|b)$.*

Proof. Using $(*)$ we observe that $1 + r(-a) \in g(\hat{a})$ and $1 + r(-b) \in g(\hat{b})$. Thus the statement follows directly from Lemma 3.6. ■

Theorem 3.11. *The unique homomorphism $\Phi : W(K) \to V(K)$ such that $\Phi(\langle a\rangle) = r(a)$ is a ring isomorphism.*

Proof. From Lemma 3.9 it follows that Φ induces a ring homomorphisms Φ_1, Φ_2, Φ_3 which form a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & I(K)/I^2(K) \arrow[r] \arrow[d, "\Phi_2"] & W(K)/I^2(K) \arrow[r] \arrow[d, "\Phi_3"] & W(K)/I(K) \arrow[r] \arrow[d, "\Phi_1"] & 0 \arrow[d] \\
0 \arrow[r] & J(K)/J^2(K) \arrow[r] & V(K)/J^2(K) \arrow[r] & V(K)/J(K) \arrow[r] & 0
\end{tikzcd}$$

Since the diagram

$$\begin{tikzcd}
W(K)/I(K) \arrow[rr, "\Phi_1"] \arrow[dr, "e"'] & & V(K)/J(K) \arrow[dl, "f"] \\
& \mathbb{Z}_2 &
\end{tikzcd}$$

commutes and e and f are isomorphisms, hence Φ_1 is an isomorphism.

The homomorphism Φ_2 together with the isomorphism g (c.f. Lemma 3.5) and the discriminant isomorphism d gives the following diagram

$$\begin{tikzcd}
I(K)/I^2(K) \arrow[rr, "\Phi_2"] \arrow[dr, "d"'] & & J(K)/J^2(K) \\
& \dot{K}/\dot{K}^2 \arrow[ur, "g"'] &
\end{tikzcd}$$

Let's observe that $g \circ d = \Phi_2$. Indeed, if $a \in K_0$, then $g(\hat{a}) = (0, \hat{a}, \emptyset) + J^2(K) = 1 + r(-a) + J^2(K)$. If $a \notin K_0$, then $g(\hat{a}) = (2, -\hat{a}, \emptyset) + J^2(K)$. But $(2, -\hat{a}, \emptyset) + J^2(K) = (2, -\hat{a}, (a|a)) + J^2(K)$, so $g(\hat{a}) = 1 + r(-a) + J^2(K)$. In both cases we have $g(\hat{a}) = 1 + r(-a) + J^2(K)$. Thus the diagram commutes. Since d and g are isomorphisms, hence Φ_2 is an isomorphism.

Now we can deduce that the homomorphism Φ_3 is an isomorphism, because Φ_1 and Φ_2 are isomorphisms.

The Lemma 3.9 implies that the homomorphism Φ induces a group homomorphism $\Phi_4 : I^2(K) \to J^2(K)$. This gives the following diagram which is commutative

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I^2(K) & \longrightarrow & W(K) & \longrightarrow & W(K)/I^2(K) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \Phi_4} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi_3} & & \downarrow \\
0 & \longrightarrow & J^2(K) & \longrightarrow & V(K) & \longrightarrow & V(K)/J^2(K) & \longrightarrow & 0.
\end{array}$$

From Lemma 3.10 it follows that the diagram

$$\begin{tikzcd}
I^2(K) \arrow[rr, "\Phi_4"] \arrow[dr, "w"'] & & J^2(K) \arrow[dl, "v"] \\
& \Gamma_K &
\end{tikzcd}$$

commutes. Since w and v are isomorphisms, hence Φ_4 is an isomorphism.

Finally, we note that Φ is an isomorphism, because Φ_4 and Φ_3 are isomorphisms. ∎

4. Witt rings of global function fields with level 1

Now we determine the structure of the Witt ring of K in the case $s(K) = 1$. Since -1 is a square in K we have $(a|a) = (-1|a) = \emptyset$ for every $a \in \dot{K}$. Let

$$V(K) = \mathbb{Z}_2 \times \dot{K}/\dot{K}^2 \times \Gamma_K$$

We define addition and multiplication in $V(K)$ in the following way

$$(n, \hat{a}, A) + (m, \hat{b}, B) = (n + m, \hat{a}\hat{b}, A + B + (a|b)),$$

$$(n, \hat{a}, A) \cdot (m, \hat{b}, B) = (nm, \hat{a}^m \hat{b}^n, mA + nB + (mn + 1)(a|b)).$$

Theorem 4.1. *$V(K)$ is a commutative ring with identity.*

Proof. We omit the proof. It is technically complicated but simpler than the proof of Theorem 3.1. We notice that the group $V(K)$ is an elementary abelian 2-group, the zero element 0 in $V(K)$ is $(0, \hat{1}, \emptyset)$ and the identity 1 in $V(K)$ is $(1, \hat{1}, \emptyset)$. ∎

Define

$$J(K) = \{ (0, \hat{a}, A) \in V(K) : \hat{a} \in \dot{K}/\dot{K}^2, A \in \Gamma_K \}$$

It is easy to verify that $J(K)$ is an ideal in $V(K)$ and has index 2. Hence there exists a unique isomorphism $f : V(K)/J(K) \to \mathbb{Z}_2$.

Proposition 4.2. *The ring $V(K)$ is a local ring and $J(K)$ is the unique maximal ideal of $V(K)$.*

Proof. For every $\alpha \in V(K) \setminus J(K)$ we have $\alpha = (1, \hat{a}, A)$, hence $\alpha^2 = 1$. Therefore, α is invertible in $V(K)$. ■

Proposition 4.3.

(i) $J^2(K) = \{ (0, \hat{1}, A) : A \in \Gamma_K \}$,
(ii) $J^3(K) = 0$.

Proof. For the proof of (1) it suffices to notice that $(0, \hat{a}, A)(0, \hat{b}, B) = (0, \hat{1}, (a|b))$ and for every $C \in \Gamma_K$ there exist $a, b \in \dot{K}$ such that $(a|b) = C$ (c.f. [3, 71:19]). The statement (ii) is obvious. ■

Corollary 4.4.

(1) *The map $v : J^2(K) \to \Gamma_K$ such that $v((0, \hat{1}, A)) = A$ is a group isomorphism.*
(2) *The map $g : \dot{K}/\dot{K}^2 \to J(K)/J^2(K)$, such that $g(\hat{a}) = (0, \hat{a}, \emptyset) + J^2(K)$ is a group isomorphism.*

Proposition 4.5. *Assume $r : \dot{K} \to V(K)$, is defined by $r(a) = (1, \hat{a}, \emptyset)$. Then for all $a, b \in \dot{K}$,*

(1) $r(1) = 1$,
(2) $r(ab) = r(a)r(b)$,
(3) $r(a) + r(b) = r(a+b)(1 + r(ab))$, *when* $a + b \neq 0$.

Proof. It is easy to check. ■

From the above and Corollary 2.2 we obtain

Corollary 4.6. *There exists a unique ring homomorphism $\Phi : W(K) \to V(K)$ such that $\Phi(\langle a \rangle) = r(a)$ for all $a \in \dot{K}$.*

Lemma 4.7. *Let the homomorphism $\Phi : W(K) \to V(K)$ be as above. Then*

(1) $\Phi^{-1}(J(K)) = I(K)$,
(2) $\Phi^{-1}(J^2(K)) = I^2(K)$.

Proof. Let's observe that $1 + r(-a) = 1 + r(a) = (0, \hat{a}, \emptyset)$ for every $a \in \dot{K}$. Thus we can obtain (1) and (2) as in the proof of Lemma 3.9 ■

Lemma 4.8. *If $a, b \in \dot{K}$ then $v((1 + r(a))(1 + r(b))) = (a|b)$.*

Proof. We compute directly $(1 + r(a))(1 + r(b)) = (0, \hat{1}, (a|b))$. ■

Theorem 4.9. *The unique homomorphism $\Phi : \dot{W}(K) \to V(K)$, described in Corollary 4.6, is a ring isomorphism.*

Proof. Arguments are the same as in the proof of Theorem 3.10. ■

5. Remarks on Witt equivalence of global function fields

The descriptions of Witt rings presented in previous sections allow us to study Witt equivalence of global function fields without using the notions and methods of algebraic theory of quadratic forms. To illustrate this we prove a certain necessary and sufficient condition for Witt equivalence. This condition is used in the paper [4] as a starting point for the proof of statement 1.1.

Theorem 5.1. *Two global function fields K and L of characteristic different from 2 are Witt equivalent if and only if there exist group isomorphisms*

$$t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2 \quad \text{and} \quad u : \Gamma_K \to \Gamma_L$$

such that

(1) $t(-\hat{1}) = -\hat{1}$,

(2) $u((\hat{a}|\hat{b})) = (t\hat{a}|t\hat{b})$ *for all* $\hat{a}, \hat{b} \in \dot{K}/\dot{K}^2$.

Proof. Assume K and L are Witt equivalent. Then there exists a ring isomorphism $\Psi : V(K) \to V(L)$. The order of the ring identity element in the additive group of $V(K)$ is equal to 2, when $s(K) = 1$ and is equal to 4 when $s(K) = 2$. Therefore we have $s(K) = s(L)$.

The ideals $J(K)$ and $J(L)$ are the unique maximal ideals in $V(K)$ and $V(L)$, respectively (see Proposition 3.2 and Proposition 4.2). Hence $\Psi(J(K)) = J(L)$, and so also $\Psi(J^2(K)) = J^2(L)$. The isomorphism Ψ induces a group isomorphism $\Psi_1 : J(K)/J^2(K) \to J(L)/J^2(L)$ and we have the commutative diagram

$$\begin{array}{ccc} J(K)/J^2(K) & \xrightarrow{\Psi_1} & J(L)/J^2(L) \\ \uparrow{\scriptstyle g_K} & & \uparrow{\scriptstyle g_L} \\ \dot{K}/\dot{K}^2 & \xrightarrow{t} & \dot{L}/\dot{L}^2 \end{array}$$

where $t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$, $t = g_L^{-1} \circ \Psi_1 \circ g_K$. Of course t is a group isomorphism.

The restriction of Ψ to $J^2(K)$ is a group isomorphism $\Psi_2 : J^2(K) \to J^2(L)$. Let $u : \Gamma_K \to \Gamma_L$, $u = v_L \circ \Psi_2 \circ v_K^{-1}$. Then u is a group isomorphism and gives the commutative diagram

$$\begin{array}{ccc} J^2(K) & \xrightarrow{\Psi_2} & J^2(L) \\ \downarrow{\scriptstyle v_K} & & \downarrow{\scriptstyle v_L} \\ \Gamma_K & \xrightarrow{u} & \Gamma_L \end{array}$$

Now we show that $t(-\hat{1}) = -\hat{1}$. This is clear, when $s(K) = 1$. Assume $s(K) = 2$. Notice that $\Psi_1(g_K(-1)) = \Psi_1((2, \hat{1}, \emptyset) + J^2(K)) = (2, \hat{1}, \emptyset) + J^2(L) = g_L(-1)$, because Ψ sends 2 to 2. Hence $t(-\hat{1}) = -\hat{1}$.

For the proof of the statement (2) choose $\alpha \in g_K(\hat{a})$ and $\beta \in g_K(\hat{b})$. Then $\Psi(\alpha) \in g_L(t\hat{a})$ and $\Psi(\beta) \in g_L(t\hat{b})$. From the Lemma 3.6 it follows that

$\alpha\beta = (0,\ \hat{1},\ (a|b))$ and $\Psi(\alpha)\Psi(\beta) = (0,\ \hat{1},\ (t\hat{a}|t\hat{b}))$. Therefore $\Psi((0,\ \hat{1},\ (a|b)) = (0,\ \hat{1},\ (t\hat{a}|t\hat{a}))$.

Now assume $t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$ and $u : \Gamma_K \to \Gamma_L$ are group isomorphisms satisfying (1) and (2). From (1) it follows that $s(K) = s(L)$.

If $s(K) = 2$ then we have the following decomposition of the square class group of L

$$\dot{L}/\dot{L}^2 = \{\hat{1}, -\hat{1}\} \oplus t(K_0/\dot{K}^2).$$

Let L_0 be the subgroup of the group $\dot{L}$ such that $t(K_0/\dot{K}^2) = L_0/\dot{L}^2$. Define a map $\Psi : (\mathbb{Z}_4,\ K_0/\dot{K}^2,\ \Gamma_K) \to (\mathbb{Z}_4,\ L_0/\dot{L}^2,\ \Gamma_L)$,

$$\Psi((n,\ \hat{a},\ A)) = (n,\ t\hat{a},\ u(A)).$$

When $s(K) = 1$ we define the map $\Psi : (\mathbb{Z}_2,\ \dot{K}/\dot{K}^2,\ \Gamma_K) \to (\mathbb{Z}_2,\ \dot{L}/\dot{L}^2,\ \Gamma_L)$ in a similar way setting

$$\Psi((n,\ \hat{a},\ A)) = (n,\ t\hat{a},\ u(A)).$$

It is easy to check that Ψ is a ring isomorphism $\Psi : V(K) \cong V(L)$. ■

Acknowledgment. I would like to thank Prof. K. Szymiczek for suggesting this problem and giving me useful comments concerning this subject.

References

[1] F. DeMeyer, D.Harrison, R. Miranda, *Quadratic forms over* $\mathbb{Q}$ *and Galois extensions of commutative rings*, Mem. Amer. Math. Soc. **77** (1989), no. 394.

[2] T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin, Reading Massachusetts, 1973.

[3] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer Verlag, Berlin Heidelberg New York Tokyo, 1973.

[4] R. Perlis, K. Szymiczek, P. E. Conner, R. Litherland, *Matching Witts with global fields*, Contemp. Math. **155** (1994), 365–387.

Address: Institute of Mathematics, Silesian University, ul. Bankowa 14, 40-007 Katowice, Poland

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