WITT RINGS OF COMPLETE SKEW FIELDS

ANDRZEJ SŁADEK

In 1982 T. Craven generalized the definition of Witt ring from fields to skew fields. The main aim of this paper is to survey Witt rings of skew fields complete relative to discrete valuation. We prove that if A is a complete skew field with the residue class field E of characteristic not 2, then the Witt ring W(A) is isomorphic to the group ring $(W(E)\mathfrak{A}(E_{\sigma}))[\Delta]$, where Δ is the two-element group, $\mathfrak{A}(E_{\sigma})$ is the ideal of W(E) generated by all elements of the form $\langle 1, -d \rangle$, $d \in \{\sigma(x)x^{-1}; x \in E^{-}\}E^{-2}$ and σ is the automorphism of E induced by the inner automorphism $x \mapsto \pi x \pi^{-1}$ of A determined by the uniformizer π of A. When A is commutative, then it turns out to be the well known Springer's Theorem. The case of dyadic skew fields is also considered. We show that if A is a finite dimensional division algebra over a dyadic field, then every binary form over A is universal.

1. Preliminaries. Throughout this paper A will denote a skew field of characteristic not 2. As far as terminology and notation connected with forms over A is concerned, we use here basically those of [1, 8]. Let us recall the most important. We shall denote by G = G(A) the factor group $A^{\cdot}/S(A)$, where S(A) is the subgroup of the multiplicative group A' generated by squares. Of course G(A) is an elementary 2-group and it plays the same role as a square class group in the commutative case. The elements of G(A) will be denoted by $\langle d \rangle$, for $d \in A^{\cdot}$ and we shall use an abbreviation $\langle d_1, \ldots, d_n \rangle$ for the element $\langle d_1 \rangle + \cdots + \langle d_n \rangle$ of the integral group ring Z[G(A)]. Any element $\langle d_1, \ldots, d_n \rangle$ is said to be a form (over A) of dimension n.

The Witt-Grothendieck ring of A is the ring WG(A) = Z[G(A)]/J(A), where J(A) is the ideal if the integral group ring Z[G(A)] generated by all elements of the form $\langle 1, d \rangle - \langle 1 + d, d(1 + d) \rangle$, for $d \in A$, $d \neq -1$. The Witt ring of A is the ring W(A) = Z[G(A)]/I(A), where I(A) is the ideal of Z[G(A)] generated by J(A) and $\langle 1, -1 \rangle$.

The forms $\varphi = \langle a_1, \dots, a_n \rangle$ and $\psi = \langle b_1, \dots, b_n \rangle$ are called *isometric*, written $\varphi \cong \psi$, if their images in WG(A) coincide. A form φ is called *isotropic* if $\varphi \cong \psi + \langle 1, -1 \rangle$, for some form ψ .

Note that if A is a field, then the definitions presented above agree with the usual definitions in [3].

In this paper A will be provided with a discrete valuation v called here just a valuation. The objects: valuation ring, valuation ideal, group of units and residue class skew field will be denoted by O = O(v), P = P(v), U = U(v) and E = E(v), respectively. The image of $a \in O$ in E will be denoted by $\kappa(a)$. We will confine our consideration to the case when E is a field.

The main objects of our attention are skew fields complete with respect to a fixed valuation v. Look through the fundamental examples:

EXAMPLE 1.1. Let A be a central division algebra over a local field F and let deg A = n. Then the standard valuation w of F extends uniquely to the valuation v of A by the rule v(x) = (1/n)w(N(x)), where $N: A \to F$ is the reduced norm map. Moreover E(v) is an extension of E(w) of degree n.

EXAMPLE 1.2. Let F be a field and let σ be a fixed automorphism of F. We write $F_{\sigma}((t))$ for the skew field of twisted formal power series $\sum_{i=n}^{\infty} a_i t^i$, $a_i \in F$, $n \in Z$, which are added in the usual way and multiplied by using Cauchy product formula and the convention: $tat^{-1} = \sigma(a)$, for $a \in F$. The skew field $F_{\sigma}((t))$ can be equipped with a valuation v by putting v(f) = n if $f = \sum_{i=n}^{\infty} a_i t^i$, $a_n \neq 0$. It is a routine matter to check that E(v) = F.

The standard reference for information about valued skew fields and examples presented above is Pierce's book [5].

2. Products of squares. Let v be a discrete valuation of A. In the sequel π will denote a fixed element of $P \setminus P^2$. It means that $v(\pi)$ generates the group $v(A^{\cdot})$. The correspondence $u \mapsto \pi u \pi^{-1}$ for $u \in U$ induces an automorphism σ of the field E. This automorphism determines a σ -invariant subgroup $E_{\sigma} = \{\sigma(x)x^{-1}; x \in E^{\cdot}\}E^{\cdot 2}$ of the group E^{\cdot} containing all squares. It is not difficult to check that $\sigma^k(x)x^{-1} \in E_{\sigma}$, for every $x \in E^{\cdot}$ and $k \in Z$.

Every element of A can be uniquely presented in the form $u\pi^k$, $u \in U$ and $k \in Z$, whereas every product of squares can be uniquely presented as $u\pi^{2k}$, $u \in U \cap S(A)$, $k \in Z$.

THEOREM 2.1. If A is complete with respect to v and char $E \neq 2$, the following conditions are equivalent:

- (i) $u \in U \cap S(A)$,
- (ii) $u \in U$ and $\kappa(u) \in E_{\sigma}$,
- (iii) $u \in U$ and u is a product of three squares.

Proof. (i) \Rightarrow (ii). Let us assume that $u \in U$ and $u = a_1^2 \dots a_n^2$, where $a_1, \dots, a_n \in A^*$. We induct on n. For n = 1 the assertion is obvious, so assume n > 1. If $u_1 = (a_1a_2)^2a_3^2 \dots a_n^2$, then $u_1 \in U$ and u_1 satisfies the inductive assumption. Clearly $\kappa(u) = \kappa(uu_1^{-1})\kappa(u_1)$ and so that the inductive step would be done it suffices to show that $\kappa(uu_1^{-1}) \in E_{\sigma}$. Let $a_1 = x\pi^k$, $a_2 = y\pi^l$, where $x, y \in U$ and $k, l \in Z$. Then

$$\kappa(uu_1^{-1}) = \kappa(a_1^2 a_2^2 (a_1 a_2)^{-2}) = \kappa(a_1^2 a_2 a_1^{-1} a_2^{-1} a_1^{-1})$$

= $\kappa(x \pi^k x \pi^k y \pi^l \pi^{-k} x^{-1} \pi^{-l} y^{-1} \pi^{-k} x^{-1})$
= $\sigma^k(\kappa(x) \sigma^{-l}(\kappa(x^{-1})) \sigma^k(\kappa(y)) \kappa(y^{-1})) \in E_{\sigma}$

(ii) \Rightarrow (iii). Suppose $u \in U$ and $\kappa(u) = \sigma(\kappa(x))\kappa(x^{-1})\kappa(y^2) = \kappa(\pi x \pi^{-1} x^{-1} y^2)$, for some $x, y \in U$. Consider the polynomial $\Phi = X^2 - u(x^{-1}\pi)^2\pi^{-2}$ in O[X]. The polynomials $\kappa(\Phi)$ and $\kappa(\Phi')$ are relatively prime and $\kappa(\Phi)(\kappa(x^{-1}y)) = 0$. By Hensel's Lemma (cf. [5, p. 324]) there exists $z \in O$ such that $\kappa(z) = \kappa(x^{-1}y)$ and $\Phi(z) = 0$. Then $u = z^2\pi^2(x^{-1}\pi)^{-2}$.

(iii) \Rightarrow (i). Obvious.

REMARK 2.2. It is worth noticing that if $E_{\sigma} = E^{\cdot 2}$, then (iii) of the previous theorem can be replaced by (iii') $u \in U$ and u is a square.

COROLLARY 2.3. Under the assumption of Theorem 2.1 the correspondence $u\pi^k \mapsto (\kappa(u), k + 2Z)$ determines the group isomorphism $G(A) \rightarrow E^{*}/E_{\sigma} \times Z/2Z$.

COROLLARY 2.4. Keep the assumption of Theorem 2.1. Let u, w be units and let $s_1 = x\pi^{2k}, s_2 = y\pi^{2l}$, where $x, y \in U \cap S(A)$ and $k, l \in Z$. Then

(i) if $us_1 + ws_2 \neq 0$, then $\langle us_1 + ws_2 \rangle$ is equal to $\langle u \rangle$, $\langle w \rangle$ or $\langle ux + wy \rangle$ when k < l, k > l or k = l, respectively.

(ii) $\langle us_1 + w\pi s_2 \rangle$ is equal to $\langle u \rangle$ when $k \leq l$ and to $\langle w\pi \rangle$ otherwise.

Corollary 2.3 describes the group G(A) only if char $E \neq 2$. If A is a finite dimensional division algebra over a local field, then we can manage the problem of G(A) without excluding that offensive case of characteristic 2.

PROPOSITION 2.5. Let A be a central division algebra over a local field F and let $\dim_{\mathscr{F}} A < \infty$. Then the group homomorphism $N^*: G(A) \to G(F)$ induced by the standard norm map $N: A \to F$ is an isomorphism.

Proof. The map N^* is an epimorphism, because $N(A^{\cdot}) = F^{\cdot}$ (cf. [5, p. 341]). Now assume that $N(v) = x^2$, $x \in F^{\cdot}$. Let x = N(w), $w \in A^{\cdot}$. Then $N(v) = N(w^2)$. In our case the Reduced Whitehead Group $SK_1 = \ker N/[A^{\cdot}, A^{\cdot}]$ is trivial (cf. [2, p. 64]), so $vw^{-2} \in [A^{\cdot}, A^{\cdot}]$. The element v is a product of squares, because $[A^{\cdot}, A^{\cdot}] \subset S(A)$. We have just proved that N^* is a monomorphism. The proof is finished.

3. Witt ring of a complete non-dyadic skew field. In this section we assume that the characteristic of the residue class field E is different from 2.

Any form φ over A decomposes as $\varphi = \langle u_1, \ldots, u_n \rangle + \langle \pi \rangle \langle w_1, \ldots, w_m \rangle$, where $u_1, \ldots, u_n, w_1, \ldots, w_m \in U$.

PROPOSITION 3.1. Let $\varphi = \psi + \langle \pi \rangle \rho$, $\xi = \tau + \langle \pi \rangle \kappa$, where ψ , ρ , τ and κ are forms with entries in U. If φ and ξ are anisotropic, then $\varphi \cong \xi$ if and only if $\psi \cong \tau$ and $\rho \cong \kappa$.

Proof. If φ is isometric to ξ , then by [1, Lemma 4.10 and Remark 4.11b] there exists a sequence of isometric forms $\varphi = \psi_0 + \langle \pi \rangle \rho_0$, $\psi_1 + \langle \pi \rangle \rho_1, \ldots, \psi_s + \langle \pi \rangle \rho_s = \xi$ such that φ_i ($\varphi_i := \psi_i + \langle \pi \rangle \rho_i$) is obtained from φ_{i-1} as follows: exactly one binary subform of φ_{i-1} , say $\langle a_1, a_2 \rangle$, is replaced by $\langle a_1s_1 + a_2s_2, a_1a_2(a_1s_1 + a_2s_2) \rangle$, for some $s_1, s_2 \in S(A) \cup \{0\}$. Taking s as small as possible, by Corollary 2.4(ii), we have to avoid changes of binary forms, which are of the form $\langle u, w\pi \rangle$, where $u, w \in U$. Thus in each step the binary form to be changed must be a subform of ψ_{i-1} or ρ_{i-1} . It means that $\psi_0 \cong \psi_s$ and $\rho_0 \cong \rho_s$. The proof is finished. \Box

By the above Proposition it is necessary to answer the question about the isometry of forms with entries in U.

PROPOSITION 3.2. If $u_1, \ldots, u_n, w_1, \ldots, w_n \in U$, then $\langle u_1, \ldots, u_n \rangle \cong \langle w_1, \ldots, w_n \rangle$ if and only if $\langle \kappa(u_1), \ldots, \kappa(u_n) \rangle \equiv \langle \kappa(w_1), \ldots, \kappa(w_n) \rangle$ (mod $\mathfrak{A}(E_{\sigma})$), where $\mathfrak{A}(E_{\sigma})$ is the ideal in W(E) generated by all forms $\langle 1, -d \rangle, d \in E_{\sigma}$.

Proof. Consider in Z[G(A)] the element

 $T := \langle u, w \rangle - \langle us_1 + ws_2, uw(us_1 + ws_2) \rangle,$

where $s_1, s_2 \in S(A) \cup \{0\}$, $us_1 + ws_2 \neq 0$. By Corollary 2.4, if T is not 0 in Z[G(A)], then there exist $x_1, x_2 \in U \cap S(A)$ such that T =

$$\langle u, w \rangle - \langle ux_1 + wx_2, uw(ux_1 + wx_2) \rangle$$
. Then
 $\kappa(T) := \langle \kappa(u), \kappa(w) \rangle - \langle \kappa(us_1 + ws_2), \kappa(uw(us_1 + ws_2)) \rangle$

is equal in Z[G(E)] to

$$\langle \kappa(u) \rangle (\langle 1 \rangle - \langle \kappa(x_1) \rangle) + \langle \kappa(w) \rangle (\langle 1 \rangle - \langle \kappa(x_2) \rangle) + (\langle \kappa(ux_1), \kappa(wx_2) \rangle - \langle \kappa(ux_1) + \kappa(wx_2), \kappa(uw) (\kappa(ux_1) + \kappa(wx_2)) \rangle).$$

By Theorem 2.1, $\kappa(T)$ determines in W(E) an element of $\mathfrak{A}(E_{\sigma})$. Lemma 4.10 and Remark 4.11b of [1] gives us the implication \Rightarrow .

Now assume that $\langle \kappa(u_1), \ldots, \kappa(u_n) \rangle \equiv \langle \kappa(w_1), \ldots, \kappa(w_n) \rangle$ (mod $\mathfrak{A}(E_{\sigma})$). Thus, by Theorem 2.1, we have

$$\langle \kappa(u_1),\ldots,\kappa(u_n)\rangle - \langle \kappa(w_1),\ldots,\kappa(w_n)\rangle = \sum_{i=1}^k \langle \kappa(x_i)\rangle\langle 1,\kappa(-d_i)\rangle$$

(in W(E)), where $d_i \in U \cap S(A)$, $x_i \in U$. Then $\langle \kappa(u_i) \rangle = \kappa(u_i) \rangle + \langle \kappa(x_i) \rangle - \kappa(x_i)$

$$\langle \kappa(u_1), \dots, \kappa(u_n) \rangle + \langle \kappa(x_1), \dots, \kappa(x_k) \rangle \cong \langle \kappa(u_1), \dots, \kappa(u_n) \rangle + \langle \kappa(x_1d_1), \dots, \kappa(x_kd_k) \rangle \cong \langle \kappa(w_1), \dots, \kappa(w_n) \rangle + \langle \kappa(x_1), \dots, \kappa(x_k) \rangle.$$

Using the Piece Equivalence Theorem and going with the binary changes up to A it is easy to show that

$$\langle u_1,\ldots,u_n\rangle + \langle x_1,\ldots,x_k\rangle \cong \langle w_1,\ldots,w_n\rangle + \langle x_1,\ldots,x_k\rangle.$$

The cancelation law gives us $\langle u_1, \ldots, u_n \rangle \cong \langle w_1, \ldots, w_n \rangle$. The proof is finished.

Immediately from Proposition 3.1 and Proposition 3.2 we obtain the main result:

THEOREM 3.3. If A is complete with respect to a descrete valuation v and char $E(v) \neq 2$, then the Witt ring W(A) is isomorphic to the group ring $(W(E)/\mathfrak{A}(E_{\sigma}))[\Delta]$, where Δ is the group of order 2.

Proof. If $\Delta = \{1, g\}$, then the correspondence

$$\langle u_1, \dots, u_n \rangle + \langle \pi \rangle \langle w_1, \dots, w_n \rangle \mapsto \langle \kappa(u_1), \dots, \kappa(u_n) \rangle + g \langle \kappa(w_1), \dots, \kappa(w_n) \rangle, u_i, w_j \in U, \langle u_1, \dots, u_n \rangle, \langle w_1, \dots, w_n \rangle$$

anisotropic, determines the isomorphism $W(A) \to (W(E)/\mathfrak{A}(E_{\sigma}))[\Delta]$. \Box

COROLLARY 3.4. If char $F \neq 2$ and $\sigma \in \operatorname{Aut} F$, then $W(F_{\sigma}((t))) \cong (W(F)/\mathfrak{A}(F_{\sigma}))[\Delta]$.

REMARK 3.5. Theorem 3.3 is a generalization of Springer's Theorem (cf. [3, p. 145]) from fields to skew fields.

REMARK 3.6. D. B. Shapiro and D. Leep [7] define the relation of G-equivalence denoted by \tilde{g} . In this section one can find out between lines the proof of the following fact: forms $\langle u_1, \ldots, u_n \rangle$ and $\langle w_1, \ldots, w_n \rangle$ with entries in U are isometric if and only if

$$\langle \kappa(u_1),\ldots,\kappa(u_n)\rangle \approx_{E_n} \langle \kappa(w_1),\ldots,\kappa(w_n)\rangle.$$

Thus the relation of E_{σ} -equivalence admits cancelation and by [7, Lemma 1.9] E_{σ} is a group with so called Piece Equivalence Property.

Now let us go on to the case of local skew fields. We mean a local skew field as a complete skew field with finite residue class field. Skew fields presented in Example 1.1 are local skew fields.

THEOREM 3.7. If A is a local skew field and the residue class field E of A has characteristic different from 2, then the Witt ring W(A) is isomorphic to the group ring $W(E)[\Delta]$, where Δ is the group of order 2.

Proof. Notice that if *E* is finite, then $E_{\sigma} = E^{\cdot 2}$, for every $\sigma \in \text{Aut } E$. Thus $\mathfrak{A}(E_{\sigma}) = \{0\}$ and the result follows from Theorem 3.3.

COROLLARY 3.8. If A is a finite dimensional division algebra over a non-dyadic local field F, then W(A) = W(K), where K is a maximal subfield of A, which is an unramified extension of the center of A.

Proof. The residue class fields of K and A coincide. The result follows from Theorem 3.7.

4. The dyadic case. Methods applied in the previous section are useless when the residue class field E of a skew field A has characteristic 2. To find a way to describe W(A) in the dyadic case we have to abandon comparisons of W(A) with Witt rings of fields connected in some way with A. The right way is to investigate the behaviour of binary forms over A.

DEFINITION 4.1. Let $\langle 1, a \rangle$ be a form over A. Define

$$D_A(1, a) = \{ s_1 + a s_2 \in A ; s_1, s_2 \in S(A) \cup \{0\} \}$$

and

$$D_A^*(1, a) = \{ c \in A^{\cdot}; \langle 1, a \rangle \cong \langle c, d \rangle, \text{ for some } d \in A^{\cdot} \}.$$

In the commutative case the sets defined above coincide. In the general case one can only prove that both contain S(A) and $D_A(1, a)$ is a subset of $D_A^*(1, a)$. It can happen that these sets differ. However, it turns out that $D_A^*(1, a)$ is a subgroup of A generated by $D_A(1, a)$ (for more details see [8]).

Throughout this section we assume that F, the center of a skew field A, is a finite extension of the 2-dic field Q_2 and $1 < \dim_F A < \infty$.

LEMMA 4.2. If K is a maximal subfield of A, that is $F \subset K \subset A$ and $[K:F] = \deg A$, then $K^{*}S(A) \subset D^{*}_{A}(1, a)$, for every $a \in K^{*}$.

Proof. Let us consider the homomorphism $i: G(K) \to G(A)$ induced by the inclusion $K \subset A$. If $[F:Q_2] = m$ and deg A = n, then $|G(F)| = 2^{m+2}$, whereas $|G(K)| = 2^{nm+2}$ (cf. [4, Th. 3.18]). Since, by Proposition 2.5, |G(A)| = |G(F)|, the homomorphism *i* cannot be a monomorphism and for $a \in K$ we have $D_A^*(1, a) = \bigcup \{D_A^*(1, ca); c \in \ker i\} \supset X$, where X is the subgroup of K generated by $\bigcup \{D_K(1, ca); c \in \ker i\}$. Every set $D_K(1, ca)$ is a subgroup of K of index 2 and $D_K(1, ca) \neq D_K(1, da)$ for $cK^{\cdot 2} \neq dK^{\cdot 2}$, so X = K.

LEMMA 4.3. If A_1 is a subalgebra of A and deg $A = 2 \deg A_1$, then the center $Z(A_1)$ of A_1 is equal to $F(\sqrt{d})$, for some $d \in F^* \setminus F^{\cdot 2}$ and $A^{\cdot 1}S(A) = N^{-1}(D_F(1, -d))$.

Proof. The first part of the statement follows from Double Centralizer Theorem [5, p. 231]. Now denote by $N_1: A_1 \to Z(A_1) = F_1$ the norm map of A_1 . Both, N and N_1 , are epimorphisms and $N_{|A_1|} = N_{F_1/F} \circ N_1$ (cf. [6, p. 298]). By Proposition 2.5 we have

$$A^{\cdot 1}S(A) = N^{-1}(N(A^{\cdot 1}S(A))) = N^{-1}(N_{F_1/F}(N_1(A^{\cdot 1})F^{\cdot 2}))$$
$$= N^{-1}(N_{F_1/F}(F^{\cdot 1})F^{\cdot 2}) = N^{-1}(D_F(1, -d)).$$

Now we can describe the Witt ring W(A). We shall do it in terms of the family of all sets $D_A^*(1, a)$, $a \in A^*$.

THEOREM 4.4. If A satisfies the assumptions made in this section, then every binary form over A is universal, that is $D_A^*(1, a) = A^*$, for every $a \in A^*$.

Proof. Let deg $A = l \cdot 2^k$, where l is odd and k is a non-negative integer. We use induction on k. First suppose k = 0. Let K be a maximal subfield of A. By Lemma 4.3, it suffices to show that $K^{\cdot}S(A) = A^{\cdot}$. Let $a \in A^{\cdot}$ and let deg A = 2s + 1. Then $a = N(a)(aN(a^{-1}))$ and $N(aN(a^{-1})) = N(a^{-1})^{2s} \in F^{\cdot 2}$. By Proposition 2.5, we have $aN(a^{-1}) \in S(A)$ and then $a \in F^{\cdot}S(A) \subset K^{\cdot}S(A)$.

Now assume $k \ge 1$. We have to show that $b \in D_A^*(1, a)$, for every $a, b \in A^*$. Let $a, b \in A^*$. Take $d \in F^* \setminus F^{*2}$ such that $N(a), N(b) \in D_F(1, -d)$. Choose in A a subfield $F_1 = F(\sqrt{d})$. It is possible by a slight modification of the argument used in [5, Ex. 4a, p. 341].

The centralizer A_1 of F_1 in A is a subalgebra of A and deg $A_1 = l \cdot 2^{k-1}$. By Lemma 4.3 and Proposition 2.5, elements a and b belong to $A^{-1}S(A)$. Thus, by the inductive assumption, we have $b \in D_A^*(1, a)$.

REMARK 4.5. Although Theorem 4.4 describes only behaviour of binary forms over A, it is not difficult to describe the Witt ring W(A). In the language of so-called quadratic schemes (cf. [9]) algebra A determines a radical scheme and W(A) can be easily constructed in the category of abstract Witt rings with help of products of indecomposable radical Witt rings. Moreover, there exists a field L such that W(A) is isomorphic to W(L).

References

- [1] T. C. Craven, Witt rings and orderings of skew fields, J. Algebra, 77 (1982), 74-96.
- P. Draxl and M. Kneser, SK₁ von Schiefkörpern, Lecture Notes in Math., vol. 778, Berlin-Heidelberg-New York, Springer Verlag 1980.
- [3] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin Addison-Wesley 1973.
- [4] M. Marshall, Abstract Witt Rings, Queen's Papers in Pure and Applied Math. No. 57, 1980.
- [5] R. S. Pierce, Associative Algebras, Springer Verlag 1982.
- [6] W. Scharlau, Quadratic and Hermitian Forms, Springer Verlag 1985.

- [7] D. B. Shapiro, and D. Leep, *Piecewise equivalence for quadratic forms*, Comm. Algebra, **11** (1983), 183-217.
- [8] A. Sładek, Witt rings of quaternion algebras, J. Algebra, 103 (1986), 267-272.
- [9] L. Szczepanik, Fields and quadratic form schemes with the index of radical not exceeding 16, Annales Math. Silesianae, 1(13), Prace naukowe Uniwersytetu Slaskiego, 663 (1985), 23-46.

Received November 7, 1986.

SILESIAN UNIVERSITY BANKOWA 14, 40 - 007 KATOWICE POLAND