ACTA ARITHMETICA
LIV (1989)

Generating functions of finitely generated Witt rings

by

WINFRIED SCHARLAU (Münster)

1. Introduction. Let K be a field of characteristic not 2 and with finitely many square classes. Let a_n denote the number of isometry classes of n-dimensional anisotropic quadratic forms over K, and $\hat{a}_n$ the number of isometry classes of arbitrary n-dimensional forms. The *generating functions* of K are the following power series

$$\hat{Z}_K(x) = \hat{Z}(x) = 1 + \hat{a}_1 x + \hat{a}_2 x^2 + \dots,$$

$$Z_K(x) = Z(x) = 1 + a_1 x + a_2 x^2 + \dots$$

The purpose of this note is to study the properties of these functions and to see how they reflect the theory of quadratic forms over K. In particular, we will find classes of fields for which the following statement holds:

(1.1) *Let r be the number of orderings of K. Then*

$$\hat{Z}(x) = \hat{p}(x)(1-x)^{-r-1}$$

for a suitable polynomial $\hat{p}(x)$. That is, $\hat{Z}(x)$ is a rational function with $x = 1$ as its only pole.

For example, this statement is true for pythagorean fields. In this case we have in addition the following functional equation

$$Z(1/x) = (-1)^r Z(x).$$

These results indicate that $Z(x)$ and $\hat{Z}(x)$ are interesting invariants of the field K and reflect a substantial part of the theory of quadratic forms over K. Nevertheless the Witt ring $W(K)$ of K remains a rather inaccessable and mysterious combinatorial object about which only little is known.

We will use the standard terminology and some well-known facts from the theory of quadratic forms. For this we refer to [4].

Acknowledgement. This work was done during a stay at the University of Katowice. I am grateful for the support by the Polish Academy of Science

(PAN) and the Deutsche Akademische Austauschdienst (DAAD), for the hospitality of the University at Katowice, and for useful conversations with the members of the algebra group there.

2. Remarks, comments, examples.

(2.1) It is easy to see that it is sufficient to consider one of the functions $Z(x)$, $\hat{Z}(x)$. In fact, the obvious equation $\hat{a}_n = a_n + \hat{a}_{n-2}$ yields the equation

$$\hat{Z}(x)(1-x^2) = Z(x).$$

Then statement (1.1) gets the following form

$$Z(x) = (1+x)\hat{p}(x)(1-x)^{-r}.$$

(2.2) The following statements are equivalent:
(i) $Z(x)$ is a polynomial.
(ii) K is not formally real.
(iii) The Witt ring $W(K)$ is finite.

In this case the conjecture is true almost trivially. In particular, $Z(x)$ is a multiple of $(1+x)$ since the number of even-dimensional anisotropic forms is equal to the number of odd-dimensional ones.

(2.3) If K is real-closed, for example $K = \boldsymbol{R}$, then

$$Z(x) = 1+2x+2x^2+ \ldots = \frac{1+x}{1-x}.$$

(2.4) Let K be a local field with residue class field k and assume char $(k) \neq 2$. Then the following equation is an easy consequence of Springer's well-known theorem

$$Z_K(x) = (Z_k(x))^2.$$

(2.5) It is obvious that the functions $Z(x)$ and $\hat{Z}(x)$ can be defined in the abstract setting of "quaternionic structures", "Cordes schemes", or "abstract Witt rings" (see [6], [3]). Similar remarks as above can be made. In particular (2.4) clarifies the behaviour of $Z(x)$ under the "group ring construction".

(2.6) The formulation used in the introduction seems a particularly nice way to state (1.1). But note that (1.1) is equivalent to the following statements:

(A) There exists an N such that for $n > N$ the coefficients $\hat{a}_n$ satisfy the following recursive relation

$$\hat{a}_n - \binom{r+1}{1}\hat{a}_{n-1} + \binom{r+1}{2}\hat{a}_{n-2} - \ldots + (-1)^{r+1}\hat{a}_{n-r-1} = 0.$$

(In fact, this is the nth coefficient of the polynomial $\hat{p}(x)$.)

(B) There exists an N and a polynomial $\hat{f}(t)$ of degree r such that $\hat{a}_n = \hat{f}(n)$ for $n > N$.

(2.7) To make the last remark more explicit we recall the notion of Eulerian polynomials: There exist polynomials $A_k(x)$, $k = 0, 1, 2, \ldots$ of degree k so that

$$\sum_{n=0}^{\infty} n^k x^n = A_k(x)(1-x)^{-k-1}.$$

The first are

$$A_0 = 1, \quad A_1(x) = x, \quad A_2(x) = x^2+x, \quad A_3(x) = x^3+4x^2+x,$$
$$A_4(x) = x+11x^2+11x^3+x^4.$$

They satisfy the recursion formula

$$A_{k+1}(x) = x(A_k'(x)(1-x)+(k+1)A_k(x)),$$

in particular, all $A_k(x)$, $k > 0$, are multiples of x. From the recursion formula follows easily that the $A_k(x)$ are symmetric:

$$x^{k+1}A_k(1/x) = A_k(x).$$

(2.8) Let K be a pythagorean SAP-field (see Section 4 for the definition) with exactly r orderings. Since all signatures of a quadratic form have the parity of the dimension, n-dimensional forms can have at most $(n+1)^r$ different total signatures. SAP implies that all these can be realized, and pythagorean then means $\hat{a}_n = (n+1)^r$. Therefore

$$\hat{Z}(x) = \sum_{n=0}^{\infty}(n+1)^r x^n = \frac{1}{x}\sum_{n=0}^{\infty} n^r x^n = x^{-1}A_r(x)(1-x)^{-r-1}.$$

In particular, (1.1) is true in this case.

3. Products and elementary Witt rings. Let K_1, K_2 be fields (or corresponding abstract objects, see (2.5)) with generating functions

$$\hat{Z}_1(x) = 1+\hat{a}_1x+\hat{a}_2x^2+ \ldots,$$
$$\hat{Z}_2(x) = 1+\hat{b}_1x+\hat{b}_2x^2+ \ldots$$

Let K be a field representing the product of K_1, K_2 in the sense of the abstract theory (see [2], [6]). If

$$\hat{Z}(x) = 1+\hat{c}_1x+\hat{c}_2x^2+ \ldots$$

is its generating function, then it follows at once from the properties of the product that $\hat{c}_n = \hat{a}_n\hat{b}_n$. Therefore

$$\hat{Z}(x) = \hat{Z}_1(x)\cdot\hat{Z}_2(x)$$

where the dot-product $\cdot$ of two (formal) power series is defined by coefficient-wise multiplication. Moreover, if the $\hat{a}_n$ satisfy a polynomial law of degree r (in the sense of (2.6) (B) and the $\hat{b}_n$ one of degree s, then the $\hat{c}_n$ satisfy a polynomial law of degree $r+s$. Thus (1.1) is true for $\hat{Z}(x)$ if it is true for $\hat{Z}_1(x)$ and $\hat{Z}_2(x)$.

Changing somewhat the usual definition, let us call a quaternionic structure (or an abstract Witt ring) of *elementary type* if it is obtained from non-real structures and the structure of the real-closed field $\boldsymbol{R}$ by an iteration of the group ring construction and the product construction. Then we get

(3.1) PROPOSITION. *Statement* (1.1) *is true for Witt rings of elementary type.*

Proof. By (2.2) and (2.3) the statement is true for the non-real and real-closed "building blocks" of the elementary constructions. By (2.4) it is preserved by the group ring construction. The same is true for the product by the above remarks. ∎

(3.2) COROLLARY. *Statement* (1.1) *is true for pythagorean fields.*

Proof. It is well known ([1], [2], [5]), but non-trivial, that the quaternionic structure of a pythagorean field is of elementary type. ∎

As mentioned in the introduction, more can be said in this case:

(3.3) THEOREM. *Assume that K is pythagorean with r orderings. Then the generating function of K satisfies the following functional equation*

$$Z(1/x) = (-1)^r Z(x).$$

Proof. In view of the equation

$$Z(x) = \frac{\hat{p}(x)(1+x)}{(1-x)^r}$$

we have to show that the polynomial $p(x) = \hat{p}(x)(1+x)$ is symmetric of degree r:

$$p(x) = x^r p(1/x).$$

To prove this statement we use again the fact that the quaternionic structure of K is of elementary type. The assertion is true for $\boldsymbol{R}$. Obviously it is preserved by group ring extensions. So it remains to show that the assertion is preserved under the product construction. Assume that the coefficients $\hat{a}_n$ satisfy a polynomial law of degree r:

$$\hat{a}_n = \hat{f}(n), \quad \hat{f}(t) \in \boldsymbol{Q}[t] \text{ of degree } r.$$

We write $\hat{f}(t)$ in the form

$$\hat{f}(t) = \sum_{i=0}^{r} \alpha_i (t+1)^i.$$

By the same computation as in (2.8) we get

$$\hat{p}(x) = \alpha_0 (1-x)^r + \sum_{i=1}^{r} \alpha_i \frac{1}{x} A_i(x)(1-x)^{r-i}.$$

Since $\hat{Z}(x) \neq 0$ if $\hat{f}(t) \neq 0$ it follows that the polynomials

$$(1-x)^r, \quad \frac{1}{x} A_1(x)(1-x)^{r-1}, \quad \ldots, \quad \frac{1}{x} A_r(x)$$

are linearly independent. Since the $\frac{1}{x} A_i(x)$ are symmetric (see (2.7)), it follows that $\hat{p}(x)$ is symmetric of degree $r-1$ if and only if

$$\alpha_0 = 0, \quad \alpha_{r-1} = \alpha_{r-3} = \ldots = 0.$$

If we now have two polynomials $\hat{f}(t)$, $\hat{g}(t)$ of degrees r and s satisfying this condition, then it follows at once that also their product satisfies this condition. ∎

4. SAP-fields. We consider now the very special class of SAP-fields. This means in our case (that is for fields with finitely many square classes) that for any collection of orderings $P_1, \ldots, P_k$ of K there exists an $\alpha \in K$ such that α is positive exactly at the orderings $P_1, \ldots, P_k$.

(4.1) LEMMA. *Let K be an SAP-field with orderings $P_1, \ldots, P_r$. Then there exists a number N with the following property: If $\dim(\varphi) > N$ and $\operatorname{sign}\varphi \geq -1$ for all orderings, then φ represents 1.*

Proof. Let $N > 2^q M$ where M is the maximal order of the torsion elements of $W(K)$. In a diagonalization of φ there appears a subform $M \times \langle \alpha \rangle$ with α not totally negative. Assume α is positive at P_i for $i \in I \neq \emptyset$. If α is negative at P_j there exists a subform $M \times \langle \beta \rangle$ with β positive at P_j. By SAP there exists an element γ which is positive exactly where α or β is positive. The forms $\langle \alpha, \beta \rangle$, $\langle \gamma, \alpha\beta\gamma \rangle$ have equal signatures. Therefore

$$M \times \langle \alpha, \beta \rangle \cong M \times \langle \gamma, \alpha\beta\gamma \rangle.$$

We continue in this way and find a totally positive subform $M \times \langle \delta \rangle$ of φ. Then

$$M \times \langle \delta \rangle \cong M \times \langle 1 \rangle$$

and we are finished. ∎

(4.2) PROPOSITION. *Statement* (1.1) *is true for SAP-fields.*

Proof. We shall prove the equivalent statement (2.6) (B). Let $\hat{A}_n$ be the set of isometry classes of n-dimensional forms so that $\hat{a}_n = |\hat{A}_n|$. Let

$$\sigma = (\sigma_1, \ldots, \sigma_r): \hat{W}(K) \to \boldsymbol{Z}^r$$

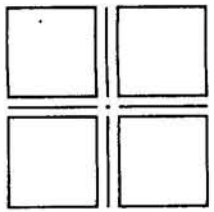
be the total signature map. For $\varphi \in \hat{A}_n$ we have

$$\sigma(\varphi) \in I_n = \{\tau \in \boldsymbol{R}^r \mid |\tau_i| \leq n, \ i = 1, \ldots, r\}.$$

For $\mathscr{R} = \{1, \dots, r\}$ we consider all ordered decompositions $\mathscr{D} = (Z, P, N)$, with $\mathscr{R} = Z \cup P \cup N$, in three disjoint subsets. The number of such $\mathscr{D}$ is

$$\sum_{j=0}^{r} \binom{r}{j} 2^{r-j}.$$

This yields a decomposition of I_n in disjoint subcubes $I_n(\mathscr{D})$



$$I_n(\mathscr{D}) = \{\tau \mid \tau_i = 0 \text{ for } i \in Z,\ \tau_i > 0 \text{ for } i \in P,\ \tau_i < 0 \text{ for } i \in N\}.$$

Correspondingly, one has

$$\hat{A}_n(\mathscr{D}) = \{\varphi \in \hat{A}_n \mid \sigma(\varphi) \in I_n(\mathscr{D})\},$$

$$\hat{a}_n(\mathscr{D}) = |\hat{A}_n(\mathscr{D})|, \quad \hat{a}_n = \sum_{\mathscr{D}} \hat{a}_n(\mathscr{D}).$$

Since K is SAP all $\hat{a}_n(\mathscr{D})$ with $I_n(\mathscr{D})$ of the same dimension (that is Z of the same cardinality) are equal. Hence

$$\hat{a}_n(j) := \sum_{|Z|=j} \hat{a}_n(\mathscr{D}) = \binom{r}{j} 2^{r-j} \hat{a}_n(\mathscr{D}_0)$$

for some $\mathscr{D}_0$ with $|Z| = j$. We distinguish the cases n even and n odd and note $\hat{a}_n(j) = 0$ if n is odd and $j > 0$. For n even we have

$$\hat{a}_n = \hat{a}_n(0) + \hat{a}_n(1) + \dots + \hat{a}_n(r).$$

We now study the growth of $\hat{a}_n$ for large n. For large even n we have

$$\begin{aligned} \hat{a}_n(r) &= \text{number of forms of total signature } 0 \\ &= \text{order of the torsion subgroup of } W(K) =: w. \end{aligned}$$

For n even we have

$$\hat{a}_{n+1} = 2^{r+1} \hat{a}_{n+1}(\mathscr{D}_+)$$

with $\mathscr{D}_+ = (\emptyset, \mathscr{R}, \emptyset)$, that is, $\hat{A}_n(\mathscr{D}_+)$ consists of all forms with totally positive signature. By (4.1) every such form can be written as $\langle 1 \rangle \perp \psi$, where $\psi \in \hat{A}_n$ has all signatures $\geqslant 0$. This leads to

$$\hat{a}_{n+1} = \hat{a}_n(0) + 2\hat{a}_n(1) + 4\hat{a}_n(2) + \dots + 2^r \hat{a}_n(r).$$

(The lower-dimensional cubes in $\hat{A}_n$ appear in $\hat{A}_{n+1}$ in all cubes they bound.) We now compute $\hat{a}_{n+2}$. Given $\mathscr{D}$, there exists a 2-dimensional form χ such that

$$\operatorname{sign}_i(\chi) = \begin{cases} 0 & \text{for } i \in Z, \\ 2 & \text{for } i \in P, \\ -2 & \text{for } i \in N. \end{cases}$$

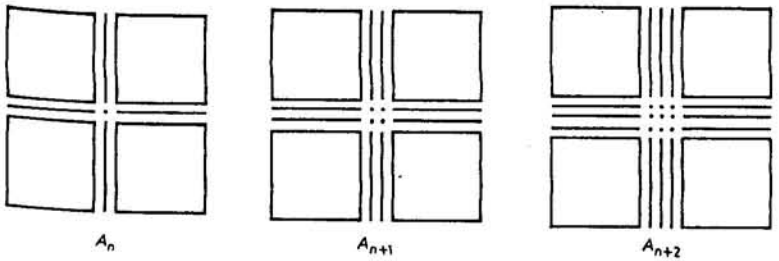
(Thus χ represents the "inner corner" of $I_{n+2}(\mathscr{D})$.) Again by (4.1) we can write every $\varphi \in \hat{A}_{n+2}(\mathscr{D})$ as $\varphi = \chi \perp \psi$ with $\psi \in \hat{A}_n(\mathscr{D}')$ where $\mathscr{D}' = \mathscr{D}$ or $\mathscr{D}'$ bounds $\mathscr{D}$. Similarly as above we get

$$\hat{a}_{n+2} = \hat{a}_n(0) + 3\hat{a}_n(1) + 9\hat{a}_n(2) + \dots + 3^r \hat{a}_n(r).$$

(A j-dimensional cube bounds 3^{r-j} higher-dimensional cubes including itself.) Continuing in this way we get

$$\hat{a}_{n+m} = \hat{a}_n(0) + (m+1)\hat{a}_n(1) + (m+1)^2 \hat{a}_n(2) + \dots + (m+1)^r \hat{a}_n(r).$$

This proves our claim. ∎



5. More remarks, comments, examples.

(5.1) Statement (1.1) claims in particular that the $\hat{a}_n$ grow like a polynomial of degree r (see (2.6)). This, in fact, can be shown directly:

There exist constants c, $C > 0$ such that

$$cn^r < \hat{a}_n < Cn^r.$$

Proof. As remarked in (2.8) there are at most $(n+1)^r$ possibilities for the total signature of an n-dimensional form. If w is the number of torsion forms, it follows that $\hat{a}_n \leqslant w(n+1)^r$ which gives the upper bound. The cokernel of the total signature map is torsion. Hence there are anisotropic forms $\varphi_1, \dots, \varphi_r$ representing a basis of $W(K)$/torsion. Let $d_i = \dim(\varphi_i)$ and $N = d_1 + \dots + d_r$. Then one has the following different forms of dimension $2nN$:

$$\perp_{i=1}^{r} 2n_i \times \varphi_i \perp (nN - \sum n_i d_i)\langle 1, -1 \rangle, \quad 0 \leqslant n_i \leqslant n.$$

Therefore

$$(n+1)^r \leqslant \hat{a}_{2nN} \leqslant \hat{a}_{2nN+1} \leqslant \ldots \leqslant \hat{a}_{2N(n+1)-1}$$

and hence

$$(2N)^{-r} n^r \leqslant \hat{a}_n. \blacksquare$$

(5.2) Only the first coefficients can be determined explicitly

$$\hat{a}_0 = 1,$$
$$\hat{a}_1 = |K^*/K^{*2}|,$$
$$\hat{a}_2 = ?,$$
$$\hat{a}_3 = |K^*/K^{*2}| \cdot \text{number of quaternion algebras.}$$

(5.3) The group K^*/K^{*2} acts by multiplication on the set A_n of isometry classes of n-dimensional anisotropic forms. The orbits are trivial or contain an even number of elements. This leads to some parity relations for the a_n:

(i) All a_{2m+1} are multiples of $2^q = |K^*/K^{*2}|$.

(ii) If a_n is odd then there exists an n-dimensional anisotropic form with $\varphi \cong \alpha\varphi$ for all α. In particular, φ is universal and of order 2 in the Witt group.

(iii) Only finitely many a_n can be odd.

(5.4) The same idea leads to a characterization of pythagorean fields: *K is pythagorean if and only if all a_n, $n > 0$, are even.*

Proof. Consider the action of ± 1 on $W(K)$. The fixed elements are precisely the elements of order 2. The field K is pythagorean if and only if the number of non-trivial anisotropic forms is not zero and then necessarily odd. This implies easily the assertion. ∎

(5.5) Recall that the Kaplansky radical of K is the following subgroup of K^*/K^{*2}

$$\{\alpha |\ (\alpha, \beta) \text{ splits for all } \beta\}.$$

An argument similar to the one above proves the following statement: *The Kaplansky radical is non-trivial if and only if a_2 is odd. In this case all a_n, $n \neq 0$, 2 are even.* ∎

(5.6) The above remarks indicate that the generating function contains a lot of information about K and $W(K)$. For finite fields one has always $Z(x) = (1+x)^2$. Hence the level and the structure of the Witt group are not determined by $Z(x)$. On the other hand all known counter examples can be reduced to this one by elementary constructions. Specifically one may ask whether the quaternionic structure of a pythagorean field is determined by $Z(x)$. (Note that the number of orderings is determined by (5.1).)

Note added in proof (February 1989). Conjecture (1.1) has been proved by M. Kula, Katowice. See his forthcoming paper.

References

[1] L. Bröcker, *Über die Anzahl der Anordnungen eines kommutativen Körpers*, Arch. Math. 29 (1977), 458–464.
[2] M. Kula, *Fields with prescribed quadratic form schemes*, Math. Z. 167 (1979), 201–212.
[3] M. Kula, L. Szczepanik and K. Szymiczek, *Quadratic form schemes and quaternionic schemes*, Preprint.
[4] T. Y. Lam, *The algebraic theory of quadratic forms*, Reading, Mass., 1973.
[5] M. Marshall, *Classification of finite spaces of orderings*, Canad. J. Math. 21 (1979), 320–330.
[6] —*Abstract Witt rings*, Queen's papers in Pure and App. Math. 57, Kingston 1980.

Katowice, Okt. 1987
MATH. INSTITUT
Einsteinstr. 62
D-4400 Münster

Received on 26.1.1988 (1779)