Acta Mathematica et Informatica Universitatis Ostraviensis

Martin Epkenhans
On vanishing theorems for trace forms

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 69--85

Persistent URL: http://dml.cz/dmlcz/120519

Acta Mathematica et Informatica Universitatis Ostraviensis 6 (1998) 69–85

On vanishing theorems for trace forms

Martin Epkenhans

Abstract: There are monic polynomials $p_n(X)$ with integer coefficients and with the property that they annihilate all non-singular quadratic forms of dimension n in the Witt ring $W(K)$ of a field K. The roots of $p_n(X)$ are integers of absolute value $\leq n$. Let $tr_{L/K} : L \to K : x \mapsto trace_{L/K}(x^2)$ denote the trace form of the finite separable field extension L/K of degree n. P.E. Conner proved that the 'positive half' of $p_n(X)$ (i.e. the product of linear factors of $p_n(X)$ with non-negative roots) already annihilates the trace form of L/K. If we only consider trace forms with given Galois group $\mathcal{G}$, then we get much better results. In general we get polynomials of lower degree, which depends on the Galois number of $\mathcal{G}$.

These results on trace forms come from identities in the Burnside ring $\mathcal{B}(\mathcal{G})$ of $\mathcal{G}$ and translate into Witt ring identities by Springer's theorem. We will discuss these results and give some new identities in $\mathcal{B}(\mathcal{G})$ which give rise to vanishing theorems for trace forms.

Key Words: quadratic forms, trace forms, Burnside ring

Mathematics Subject Classification: 11E04

1. Introduction

We consider vanishing polynomials for classes M of quadratic forms. Define

$$I_M := \{f(X) \in \mathbb{Z}[X] \mid f(\psi) = 0 \in \mathrm{W}(K) \text{ for all } \psi \in M, \text{ where } \psi \text{ is a form over } K\}.$$

Here $\mathrm{W}(K)$ denotes the Witt ring over the field K. We easily observe that I_M is an ideal, the *vanishing ideal of* M. Let us first give some examples. For $\mathrm{n} \in \mathbb{N}$ set

$$\begin{aligned} L_n(X) &= X(X^2 - 2^2)(X^2 - 4^2)\dots(X^2 - n^2) && \text{if } n \text{ is even,} \\ L_n(X) &= (X^2 - 1^2)(X^2 - 3^2)\dots(X^2 - n^2) && \text{if } n \text{ is odd.} \end{aligned}$$

Lewis [7] discovered that $L_n(\psi) = 0 \in \mathrm{W}(K)$ for any quadratic form ψ of dimension n over the field K of characteristic $\neq 2$. Later on we prove that $L_n(X)$ already generates the vanishing ideal of all these quadratic forms.

Let L/K be a finite and separable extension of fields of characteristic $\neq 2$. With it we associate the *trace form* which is defined by $tr_{L/K} : L \to K : x \mapsto tr_{L/K}x^2$. Let $C_n(X) := \prod_{k \geq 0, L_n(k)=0}(X - k)$ be the 'non-negative' part of $L_n(X)$. P.E.

Conner proved $C_n(\psi) = 0 \in \mathrm{W}(K)$ for any quadratic form ψ over K which is isometric to a trace form of a field extension of degree n over K. Further $C_n(X)$ generates the corresponding vanishing ideal.

From Beaulieu and Palfrey [2] we know the following refinement of Conner's result. Let $f(X) \in K[X]$ be an irreducible and separable polynomial with Galois group $\mathcal{G} = Gal(f)$ over K. Then the Galois number t_f of $f(X)$ is defined to be the least natural number j so that any j roots of $f(X)$ generate a splitting field of $f(X)$ over the ground field K (see [2]). Let n be the degree of $f(X)$. Then

$$B_n(X) := (X - n) \cdot \prod_{k=0, k \equiv n \bmod 2}^{t_f - 1} (X - k) \in \mathbb{Z}[X]$$

annihilates the trace form of $K[X]/(f)$ over K. In general $B_n(X)$ does not generate the corresponding vanishing ideal.

The aim of this note is to investigate the latter vanishing ideal. We know by an old result of Sylvester that the signatures of the trace form are always non-negative. This explains why Conner's polynomial $C_n(X)$ has no negative roots. We will show that signatures play an important role in this context.

2. Notation

Let us fix some notations. We only consider fields of characteristic $\neq 2$. Let K be a field. Then $< a_1, \ldots, a_n >$ is the diagonal form $a_1 X_1^2 + \ldots + a_n X_n^2$ over K. The m-fold sum of the quadratic form ψ is denoted $m \times \psi$. The trace form of L/K is written $< L/K >$, resp $< L >$ if no confusion arise. $\mathrm{ord}(\sigma)$, $\mathrm{ord}(\mathcal{G})$ is the order of the group element σ, resp. the group $\mathcal{G}$. We denote the cardinality of a set M by $\sharp M$.

3. The vanishing ideal

Let us reconsider the examples given in the introduction. Our first lemma contains some information on I_M.

Lemma 1. *Consider a class M of quadratic forms.*

1. *Let $\psi \in M$ be a quadratic form over a formally real field K. With $s = \mathrm{sign}(\psi)$ for some signature homomorphism* sign : $W(K) \to \mathbb{Z}$ *we get*

$$I_M \subset (X - s) \cdot \mathbb{Z}[X].$$

2. *Let $\psi \in M$ be a quadratic form of dimension n over K. Then*

$$I_M \subset (X - n) \cdot \mathbb{Z}[X].$$

Proof. 1. Let $f(X) \in I_M$. Then $f(\psi) = 0$ gives $\mathrm{sign}(f(\psi)) = 0 = f(\mathrm{sign}(\psi))$. Hence s is a root of $f(X)$.

2. Replace the signature homomorphism by the dimension. □

Proposition 1. (Conner,Lewis) *Let $n \in \mathbb{N}$.*

1. *The vanishing ideal of the class Q_n of quadratic forms of dimension n is a principal ideal generated by $L_n(X)$.*
2. *The vanishing ideal of the class T_n of trace forms of dimension n is a principal ideal generated by $C_n(X)$.*

Proof. As already mentioned in the introduction $L_n(X) \in I_{Q_n}$ and $C_n(X) \in I_{T_n}$ (see [2], [7]). For each $s \in \{-n, \ldots, n\}$ with $s \equiv n \mod 2$ there is a quadratic form of dimension n over $\mathbb{Q}$ having signature s. Hence

$$(L_n(X)) \subset I_{Q_n} \subset \bigcap_{s=-n, s\equiv n \mod 2}^{n} (X - s) \cdot \mathbb{Z}[X] \subset (L_n(X)).$$

2. We use the classification of rational trace forms given in [5] Theorem 1 and 3. Hence for any $s \in \{0, \ldots, n\}, s \equiv n \mod 2$ there is a trace form ψ over $\mathbb{Q}$ of dimension n having signature s. This gives $I_{T_n} \subset (C_n(X))$. □

4. The Burnside ring $\mathcal{B}(\mathcal{G})$

Beaulieu, Palfrey and Conner proved their results as follows: They formulate identities in the Burnside ring $\mathcal{B}(\mathcal{G})$ and translate these identities via a homomorphism of Springer into the Witt ring. We will briefly recall the definition of the Burnside ring. Let $\mathcal{H} < \mathcal{G}$ be finite groups. We denote the action of $\mathcal{G}$ on the left cosets $\mathcal{G}/\mathcal{H} = \{a\mathcal{H}, a \in \mathcal{G}\}$ by $(\mathcal{G}, \mathcal{G}/\mathcal{H})$. This action gives rise to a permutation character denoted $\chi_{\mathcal{H}}^{\mathcal{G}} = \chi_{\mathcal{H}}$.

Definition 1. *Let $\mathcal{G}$ be a finite group. The Burnside ring $\mathcal{B}(\mathcal{G})$ of $\mathcal{G}$ is a free abelian group. The set*

$\{\chi_{\mathcal{H}} \mid \mathcal{H}$ runs over a set of representatives of conjugacy classes of subgroups of $\mathcal{G}\}$

is a free set of generators of $\mathcal{B}(\mathcal{G})$. The multiplication is induced by the tensor product of the underlying representations. Hence

$$\chi_{\mathcal{H}} \cdot \chi_{\mathcal{U}} = \bigoplus_{\sigma \in \mathcal{H}\backslash\mathcal{G}/\mathcal{U}} \chi_{\mathcal{H} \cap \sigma\mathcal{U}\sigma^{-1}},$$

where the sum runs over a set of representatives of the double cosets in $\mathcal{H}\backslash\mathcal{G}/\mathcal{U}$.

Springer's Theorem Let N/K be a Galois extension with Galois group $G(N/K)$. Then

$$\chi_{\mathcal{H}} \mapsto < N^{\mathcal{H}} >, \mathcal{H} < \mathcal{G}$$

extends uniquely to a ring homomorphism

$$h_{N/K} : \mathcal{B}(G(N/K)) \to \mathrm{W}(K).$$

For details see [2].

We very briefly sketch the proof of the vanishing result given in [2]. Let $f(X) \in K[X]$ be an irreducible and separable polynomial with $\mathcal{G} = Gal(f)$ and let N be a splitting field of $f(X)$ over K. Set $\mathcal{H} = G(N/(K[X]/(f)))$. We get $B_n(< K[X]/(f) >) = B_n(h_{N/K}(\chi_{\mathcal{H}})) = h_{N/K}(B_n(\chi_{\mathcal{H}}))$. Since $B_n(X)$ already annihilates $\chi_{\mathcal{H}}$ in $\mathcal{B}(\mathcal{G})$ we are done.

Next we define the class of quadratic forms we are interested in.

Definition 2. *Let $\mathcal{H} < \mathcal{G}$ be finite groups. Then $M(\mathcal{G}, \mathcal{H})$ denotes the class of all quadratic forms ψ such that there is an irreducible and separable polynomial $f \in K[X]$ with Galois group $Gal(f) \simeq \mathcal{G}$ and such that*

1. *the action of $Gal(f)$ on the roots of $f(X)$ is equivalent to the action of $\mathcal{G}$ on $\mathcal{G}/\mathcal{H}$.*
2. *ψ and the trace form of $K[X]/(f)$ over K are isometric.*

Note that we restrict ourselves implicitly to faithful actions. The following example shows that in general $B_n(X)$ does not generate $I_{M(\mathcal{G},\mathcal{H})}$. Let N/K be a Galois extension of odd degree. Then $< L >\simeq [L : K]\times < 1 >$ for any intermediate field L of N/K. Hence $g(X) = X - [L : K] = X - [\mathcal{G} : G(N/L)]$ is a vanishing polynomial for $< L >$, which implies $g(X) \in I_{M(\mathcal{G},\mathcal{H})}$. Now $B_n(X)$ has degree 1 if and only if $t_f = 1$, which means $N = L$.

Next we investigate the intersection of the kernels of all homomorphisms $h_{N/K}$ with $G(N/K) \simeq \mathcal{G}$ to get more information on $I_{M(\mathcal{G},\mathcal{H})}$.

Definition 3. *The trace ideal $\mathcal{T}(\mathcal{G})$ of a finite group $\mathcal{G}$ in $\mathcal{B}(\mathcal{G})$ is defined to be the intersection of all kernels $\ker(h_{N/K})$, where N/K runs over all Galois extensions N/K of fields of characteristic $\neq 2$ with $G(N/K) \simeq \mathcal{G}$.*

5. The signatures

Let $f(X) \in K[X]$ be an irreducible and separable polynomial. Then the signature value of the trace form of $K[X]/(f)$ over K equals the number of real roots of $f(X)$. A root α of $f(X)$ is real if and only if α is fixed by the complex conjugation. This motivates the following definition

Definition 4. *Let $\sigma \in \mathcal{G}$ be an element of order ≤ 2 and let $\mathcal{H} < \mathcal{G}$. Then*

$$sign_\sigma \chi_{\mathcal{H}} = \sharp\{\text{fixpoints of } (<\sigma>, \mathcal{G}/\mathcal{H})\}$$

is the 'signature' of $\chi_{\mathcal{H}}$ induced by σ. Of course, $\text{sign}_\sigma \chi_{\mathcal{H}} = \chi_{\mathcal{H}}(\sigma)$. Hence sign_σ extends uniquely to a ring homomorphism $\text{sign}_\sigma : \mathcal{B}(\mathcal{G}) \to \mathbb{Z}$. In our context of quadratic forms it is more enlightening to look at $\chi_{\mathcal{H}}(\sigma)$ as a signature value than just a character value. The virtual degree of $\chi_{\mathcal{H}}$ equals $\text{sign}_{id}(\chi_{\mathcal{H}})$. Hence it also fits into this concept.

As usual $C_{\mathcal{G}}(\sigma)$ denotes the centralizer of σ in $\mathcal{G}$. Let $\mathcal{G}\sigma = \{\rho^{-1}\sigma\rho \mid \rho \in \mathcal{G}\}$ be the set of conjugates of σ in $\mathcal{G}$.

Proposition 2. *Let $\mathcal{H} < \mathcal{G}$ be finite groups and let $\sigma \in \mathcal{G}$ be an element of order ≤ 2. Then*

$$\operatorname{sign}_\sigma \chi_{\mathcal{H}} = \frac{ord(C_{\mathcal{G}}(\sigma))\sharp\mathcal{G}\sigma \cap \mathcal{H}}{ord(\mathcal{H})} = \frac{[\mathcal{G} : \mathcal{H}]\sharp\mathcal{G}\sigma \cap \mathcal{H}}{\sharp\mathcal{G}\sigma}.$$

Proof. Consider the action of $< \sigma >$ on $\mathcal{G}/\mathcal{H}$. Then $\rho\mathcal{H}$ is a fixpoint if and only if $\rho^{-1}\sigma\rho \in \mathcal{H}$. We apply proposition 16.5 in [1]. Let s be the number of conjugacy classes of $\mathcal{H}$ whose members are conjugate in $\mathcal{G}$ to σ. If $s = 0$, then $\operatorname{sign}_\sigma \chi_{\mathcal{H}} = \chi_{\mathcal{H}}(\sigma) = 0 = \sharp\mathcal{G}\sigma \cap \mathcal{H}$. Otherwise, let $h_1, \ldots, h_s$ be representatives of these conjugacy classes of $\mathcal{H}$. Since $\chi_{\mathcal{H}}^{\mathcal{H}}$ is trivial, we get

$$\begin{aligned}
\chi_{\mathcal{H}}^{\mathcal{G}} &= \sharp C_{\mathcal{G}}(\sigma) \cdot \sum_{i=1}^{s} \frac{\chi_{\mathcal{H}}^{\mathcal{H}}(h_i)}{C_{\mathcal{H}}(h_i)} = \frac{\sharp C_{\mathcal{G}}(\sigma)}{\operatorname{ord}(\mathcal{H})} \cdot \sum_{i=1}^{s} [\mathcal{H} : C_{\mathcal{H}}(h_i)] \\
&= \frac{\sharp C_{\mathcal{G}}(\sigma)}{\operatorname{ord}(\mathcal{H})} \cdot \sum_{i=1}^{s} \mathcal{H}h_i \\
&= \frac{\sharp C_{\mathcal{G}}(\sigma)}{\operatorname{ord}(\mathcal{H})} \sharp\mathcal{G}\sigma \cap \mathcal{H}.
\end{aligned}$$

□

Before we are able to apply lemma 1 in this situation we have to give a new realization result for trace forms.

Proposition 3. *Let $\mathcal{H} < \mathcal{G}$ be finite groups. Suppose $\mathcal{G}$ acts faithfully on $\mathcal{G}/\mathcal{H}$. Set $n := [\mathcal{G} : \mathcal{H}]$ and let $\sigma \in \mathcal{G}$ be an element of order ≤ 2. Then there is an algebraic number field $K \subset \mathbb{R}$ and an irreducible polynomial $f(X) \in K[X]$ such that*

1. *the action of $Gal(f(X))$ on the roots of $f(X)$ is equivalent to the action of $\mathcal{G}$ on $\mathcal{G}/\mathcal{H}$ and*
2. *σ corresponds to the complex conjugation on the splitting field of $f(X)$ over K.*

Hence

$$\operatorname{sign}_K < K[X]/(f(X)) >= \operatorname{sig}_{:\sigma} \chi_{\mathcal{H}}.$$

Proof. 1. $\operatorname{ord}(\sigma) = 2$. If σ generates $\mathcal{G}$, set $K = \mathbb{Q}$ and $f(X) = X^2 + 1$.
Now let $\operatorname{ord}(\mathcal{G}) = 2m \geq 4$. Consider the quadratic form

$$\psi = (m-1) \times <1, -1> \perp <1, -2>$$

over $\mathbb{Q}$. By Theorem 1 and 3 in [5] there is a field extension $L/\mathbb{Q}$ with trace form ψ and such that the normal closure $N \subset \mathbb{C}$ of L has Galois group $\mathfrak{S}_n$ over $\mathbb{Q}$. Let $\alpha \in L$ be a primitive element of $L/\mathbb{Q}$ and let $M := \{\alpha_1, \overline{\alpha}_1 \ldots, \alpha_m, \overline{\alpha}_m\}$ be the set of conjugates of $\alpha = \alpha_1$. Here $\bar{}$ denotes the complex conjugation. Observe that no conjugate of α is real since $\operatorname{sign}_{\mathbb{Q}} < L >= \operatorname{sign}_{\mathbb{Q}} \psi = 0$. Let $\phi : \mathcal{G} \to M$ be a bijection such that for any $a \in \mathcal{G}$ we have $\overline{\phi(a)} = \phi(\sigma(a))$. Let $\iota : \mathcal{G} \hookrightarrow S(\mathcal{G}) \tilde{\to} S(M) \tilde{\to} G(N/\mathbb{Q})$ be the induced embedding. Then $\iota(\sigma)$ is the complex conjugation on N. Set $K := N^{\iota(\mathcal{G})}$. Since $\iota(\sigma) \in \iota(\mathcal{G})$ the field K is real. Next

define $F := N^{\iota(\mathcal{H})}$ and let $f(X) \in K[X]$ with $K[X]/(f(X)) \simeq F$. Then N is a splitting field of $f(X)$ over K since the action of $\mathcal{G}$ on $\mathcal{G}/\mathcal{H}$ is faithful.

2. Let $\sigma = id$. Set $\psi = (n-1)\times$ <1>$\perp$<2> and proceed as above. □

Now we are ready to determine an ideal $\mathfrak{a}$ with $I_{M(\mathcal{G},\mathcal{H})} \subset \mathfrak{a}$.

Definition 5. *Let $\mathcal{H} < \mathcal{G}$ be finite groups. Set*

$$q_{\mathcal{G},\mathcal{H}}(X) := \prod_{k \in \{\mathrm{sign}_\sigma \chi_\mathcal{H} \mid \sigma \in \mathcal{G}, \mathrm{ord}(\sigma) \leq 2\}} (X - k).$$

Let $K(\mathcal{H}) = \cap_{\sigma \in \mathcal{G}} \sigma \mathcal{H} \sigma^{-1}$, then $\mathcal{G}$ acts faithfully on $\mathcal{G}/\mathcal{H}$ if and only if $K(\mathcal{H}) = 1$.

Corollary 1. *For finite groups $\mathcal{H} < \mathcal{G}$ with $K(\mathcal{H}) = 1$ we get*

$$I_{M(\mathcal{G},\mathcal{H})} \subset (q_{\mathcal{G},\mathcal{H}}(X)).$$

6. The rank formula

This section contains the main result of this note. It implies that the trace ideal is a submodule of the kernel of the total signature homomorphism and both modules have the same rank. Hence their quotient is finite.

Theorem 1. *Let $\mathcal{G}$ be a finite group and let $RC_2(\mathcal{G})$ be a set of representatives of conjugacy classes of elements of order ≤ 2 in $\mathcal{G}$. Then*

$$\mathrm{rank}(T(\mathcal{G})) = \mathrm{rank}(\mathcal{B}(\mathcal{G})) - \sharp RC_2(\mathcal{G}).$$

Definition 6. *For a finite group $\mathcal{G}$ let*

$$L(\mathcal{G}) = \cap_{\sigma \in RC_2(\mathcal{G})} \ker(\mathrm{sign}_\sigma)$$

be the kernel of the total signature homomorphism. Let $RC(\mathcal{G})$ be a set of representatives of the conjugacy classes of subgroups of $\mathcal{G}$.

Lemma 2.

1. $L(\mathcal{G})$ is a submodule of $\mathcal{B}(\mathcal{G})$ of rank $\mathrm{rank}(\mathcal{B}(\mathcal{G})) - \sharp RC_2(\mathcal{G})$.

2. $T(\mathcal{G}) \subset L(\mathcal{G})$.

Proof. 1. $L(\mathcal{G})$ is given by the system of linear equations

$$\sum_{\mathcal{H} \in RC(\mathcal{G})} \mathrm{sign}_\sigma \chi_\mathcal{H} \cdot x_\mathcal{H} = 0, \ \sigma \in RC_2(\mathcal{G}).$$

By proposition 2 the rank of this system equals the number of conjugacy classes of elements of order ≤ 2.

2. follows from proposition 3. □

Obviously the rank formula of theorem 1 is equivalent to the existence of some $a \in \mathbb{N}$ with $a \cdot L(\mathcal{G}) \subset T(\mathcal{G})$. The proof of theorem 1 is organized as follows. First we consider groups of odd order. In section 3 we reduce our approach to 2-groups. After dealing with elementary abelian 2-groups we finally show in section 7 that $T(\mathcal{G})$ has finite index in $L(\mathcal{G})$ for any finite 2-group.

Proposition 4. *Let $\mathcal{G}$ be a group of odd order. Then*

$$T(\mathcal{G}) = L(\mathcal{G}).$$

Hence rank$(T(\mathcal{G}))$ = rank$(B(\mathcal{G}))$ − 1.

Proof. Let N/K be a Galois extension with Galois group $G(N/K) \simeq \mathcal{G}$. Let L be an intermediate field of N/K. Then $<L>= [L : K]\times <1>$ (see [3][cor. I.6.5]. Let $X = \sum_{\mathcal{H}\in \mathrm{RC}(\mathcal{G})} m_{\mathcal{H}} \cdot \chi_{\mathcal{H}}$. Then $h_{N/K}(X) = \sum_{\mathcal{H}\in \mathrm{RC}(\mathcal{G})} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}]\times <1>$. Since ord$(\mathcal{G})$ is odd, $L(\mathcal{G})$ is defined by the equation $\sum_{\mathcal{H}\in \mathrm{RC}(\mathcal{G})} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] = 0$ (see proposition 2). □

7. Some consequences

We first give some consequences of the rank formula.

Corollary 2. *Let $\mathcal{H} < \mathcal{G}$ be finite groups. Then there exists some $l \in \mathbb{N}_0$ with*

$$(2^l \cdot q_{\mathcal{G},\mathcal{H}}(X)) \subset I_{M(\mathcal{G},\mathcal{H})} \subset (q_{\mathcal{G},\mathcal{H}}(X)).$$

Hence $2^l \cdot q_{\mathcal{G},\mathcal{H}}(X)$ is a polynomial of minimal degree in $I_{M(\mathcal{G},\mathcal{H})}$.

Proof. $q_{\mathcal{G},\mathcal{H}}(X)$ lies in $L(\mathcal{G})$ since signatures are ring homomorphisms. Now apply theorem 1 and observe that the only torsions in the Witt ring are 2-torsions. □

We conclude that $I_{M(\mathcal{G},\mathcal{H})}$ is a principal ideal if and only if $2^l \cdot q_{\mathcal{G},\mathcal{H}}(X)$ generates $I_{M(\mathcal{G},\mathcal{H})}$ for some $l \in \mathbb{N}_0$. The next corollary gives a relation between our polynomials.

Corollary 3. *Let $\mathcal{H} < \mathcal{G}$ be finite groups with $K(\mathcal{G}) = 1$. Then $q_{\mathcal{G},\mathcal{H}}(X)$ divides $B_{\mathcal{G},\mathcal{H}}(X)$.*

Proof. The definition of the Galois number gives

$$\max\{\mathrm{sign}_\sigma \chi_{\mathcal{H}}, \mathrm{ord}(\sigma) = 2\} \leq \max\{\chi_{\mathcal{H}}(\tau), \tau \in \mathcal{G}, \tau \neq 1\} = t_{\mathcal{G}} - 1.$$

□

By lemma 1 in [2] equality holds for any 2-group $\mathcal{G}$. We abbreviate $\chi_{<\tau>} = \chi_\tau$ if $\tau \in \mathcal{G}$ is an element of order ≤ 2.

Example 1. *Let $\mathcal{G} = M(16) =< \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^5 >$ be the modular group of order 16. Set $\mathcal{H} =< \tau >$. Then $q_{\mathcal{G},\mathcal{H}} = X(X-4)(X-8)$ and*

$B_{\mathcal{G},\mathcal{H}} = X(X-2)(X-4)(X-8)$. *Further* $I_{M(\mathcal{G},\mathcal{H})}$ *is a principal ideal with generator* $q_{\mathcal{G},\mathcal{H}}$.

Proof. $M(16)$ has three involutions: $\rho := \sigma^4, \tau$ and $\tau\rho = \sigma\tau\sigma^{-1}$. Proposition 2 gives $\operatorname{sign}_\tau \chi_\tau = 4$ and $\operatorname{sign}_\rho \chi_\tau = 0$. Hence $t_{\mathcal{G}} = 5$. From $\chi_{\mathcal{H}}^2 = 4\chi_{\mathcal{H}} + 2\chi_1$ and $\chi_1\chi_{\mathcal{H}} = 8\chi_1$ we conclude $q_{\mathcal{G},\mathcal{H}}(\chi_{\mathcal{H}}) = 0$ which implies the assertion. □

Example 2. *Consider the natural action of the alternating group* $\mathfrak{A}_n$ *on* n *points. Set* $\mathcal{H} = \mathfrak{A}_{n-1}$. *Then* $\operatorname{sign}_\sigma \chi_{\mathcal{H}} \equiv n \mod 4$, *since any involution is a product of an even number of disjoint transpositions. Therefore the degree of* $q_{\mathcal{G},\mathcal{H}}$ *is about half the degree of the polynomial* $B_n(X) = C_n(X)$.

Example 3. *Suppose that the Galois number* $t_{\mathcal{G}}$ *equals 1. Then*

$$B_n(X) = X - n \quad \text{if } n \text{ is odd and}$$
$$B_n(X) = X(X-n) \quad \text{if } n \text{ is even.}$$

Further $\mathcal{H} = 1$. *We get* $B_n(X) = q_{\mathcal{G},\mathcal{H}}(X)$ *and* $I_{M(\mathcal{G},\mathcal{H})} = (B_n(X)) = (q_{\mathcal{G},\mathcal{H}}(X))$.

8. Reduction to 2-groups

We reduce the proof of theorem 1 via several maps to subgroups of $\mathcal{G}$.
For a subgroup $\mathcal{H}$ of $\mathcal{G}$ there is a ring homomorphism

$$\operatorname{res}_{\mathcal{G}}^{\mathcal{H}} : \mathcal{B}(\mathcal{G}) \to \mathcal{B}(\mathcal{H})$$

called the *restriction map*. It is defined by restricting the characters $\chi_{\mathcal{U}}^{\mathcal{G}}$ to $\mathcal{H}$. There is an additive but not multiplicative *corestriction* map

$$\operatorname{cor}_{\mathcal{H}}^{\mathcal{G}} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{G})$$

defined by $\operatorname{cor}_{\mathcal{H}}^{\mathcal{G}} \chi_{\mathcal{U}}^{\mathcal{H}} = \chi_{\mathcal{U}}^{\mathcal{G}}$. $\operatorname{cor}_{\mathcal{H}}^{\mathcal{G}} \chi_{\mathcal{U}}^{\mathcal{H}} = \chi_{\mathcal{U}}^{\mathcal{G}}$ is known to be the induced character of $\chi_{\mathcal{U}}^{\mathcal{H}}$ (see [6] Chapter 4 Theorem 4.2).

Let $\mathcal{H}$ be a normal subgroup of $\mathcal{G}$. Then the canonical projection $\mathcal{G} \to \mathcal{G}/\mathcal{H}$ induces the *inflation map*

$$\inf_{\mathcal{H}}^{\mathcal{G}} : \mathcal{B}(\mathcal{G}/\mathcal{H}) \to \mathcal{B}(\mathcal{G}),$$

which is a ring homomorphism. If $\mathcal{H} < \mathcal{U} < \mathcal{G}$, then $\inf_{\mathcal{H}}^{\mathcal{G}}(\chi_{\mathcal{U}/\mathcal{H}}^{\mathcal{G}/\mathcal{H}}) = \chi_{\mathcal{U}}^{\mathcal{G}}$. We now give the connection of these maps in the category of Burnside rings and several maps between Witt rings.

Lemma 3. *Let* N/K *be a finite Galois extension with* $G(N/K) = \mathcal{G}$ *and let* $\mathcal{H}$ *be a subgroup of* $\mathcal{G}$.

1. Let $\sigma \in \mathcal{H}$ *be an element of order* ≤ 2. *Then*

$$\begin{array}{ccc} B(G) & \xrightarrow{sign_\sigma} & \mathbb{Z} \\ {\scriptstyle res_G^H}\downarrow & \nearrow_{sign_\sigma} & \\ B(H) & & \end{array}$$

commutes.

2. *Let* $s^* : W(K) \to W(N^H)$ *be the lifting homomorphism. Then*

$$\begin{array}{ccc} B(G) & \xrightarrow{h_{N/K}} & W(K) \\ {\scriptstyle res_G^H}\downarrow & & \downarrow{\scriptstyle s^*} \\ B(H) & \xrightarrow{h_{N/N^H}} & W(N^H) \end{array}$$

and

$$\begin{array}{ccc} B(H) & \xrightarrow{h_{N/N^H}} & W(N^H) \\ {\scriptstyle cor_H^G}\downarrow & & \downarrow{\scriptstyle tr_{N^H/K}} \\ B(G) & \xrightarrow{h_{N/K}} & W(K) \end{array}$$

commute.

3. *Let* H *be a normal subgroup of* G. *Then*

$$\begin{array}{ccc} B(G/H) & \xrightarrow{h_{N^H/K}} & W(K) \\ {\scriptstyle inf_H^G}\downarrow & \nearrow_{h_{N/K}} & \\ B(G) & & \end{array}$$

commutes.

Hence the restriction map in the Burnside ring plays the role of the lifting of quadratic forms in the Witt ring and the corestriction corresponds to the Scharlau transfer.

Proof. 1. is obvious.

2. Set $L := N^H$. Then

$$\begin{aligned} h_{N/L}(\operatorname{res}_G^H(\chi_U^G)) &= h_{N/L}\Big(\sum_{\sigma\in H\backslash G/U} \chi^H_{H\cap\sigma U\sigma^{-1}}\Big) = \perp_{\sigma\in H\backslash G/U} h_{N/L}(\chi^H_{H\cap\sigma U\sigma^{-1}}) \\ &= \perp_{\sigma\in H\backslash G/U} < N^{H\cap\sigma U\sigma^{-1}}/L > = \perp_{i=1,\dots,r} < L[X]/(f_i)/L > \\ &= < (K[X]/(f)) \otimes L/L > = s^* \circ h_{N/K}(\chi_U^G), \end{aligned}$$

where $K[X]/(f) \simeq L$ and $f = f_1 \cdots f_r$ is the decomposition of f into prime factors over L.

Let $\mathcal{U} < \mathcal{H} < \mathcal{G}$. Then

$$h_{N/K} \circ \operatorname{cor}^{\mathcal{G}}_{\mathcal{H}}(\chi^{\mathcal{H}}_{\mathcal{U}}) = h_{N/K}(\chi^{\mathcal{G}}_{\mathcal{U}}) =< N^{\mathcal{U}} >= tr_{N^{\mathcal{H}}/K} < N^{\mathcal{U}}/N^{\mathcal{H}} > = tr_{N^{\mathcal{H}}/K}(h_{N/N^{\mathcal{H}}}(\chi^{\mathcal{H}}_{\mathcal{U}})).$$

3. Let $\mathcal{H} < \mathcal{U} < \mathcal{G}$. Then

$$h_{N/K}(\operatorname{inf}^{\mathcal{G}}_{\mathcal{H}}(\chi^{\mathcal{G}/\mathcal{H}}_{\mathcal{U}/\mathcal{H}})) = h_{N/K}(\chi^{\mathcal{G}}_{\mathcal{U}}) =< N^{\mathcal{U}} >=< (N^{\mathcal{H}})^{\mathcal{U}/\mathcal{H}} >= h_{N^{\mathcal{H}}/K}(\chi^{\mathcal{G}/\mathcal{H}}_{\mathcal{U}/\mathcal{H}}).$$

□

Lemma 4. *Let $\mathcal{H} < \mathcal{G}$ be finite groups.*

1. Then $res^{\mathcal{H}}_{\mathcal{G}}(L(\mathcal{G})) \subset L(\mathcal{H})$.

2. Let $[\mathcal{G} : \mathcal{H}]$ be odd.

(a) Then $res^{\mathcal{H}}_{\mathcal{G}}(\chi) \in L(\mathcal{H})$ if and only if $\chi \in L(\mathcal{G})$.

(b) $res^{\mathcal{G}}_{\mathcal{H}}(\chi) \in \mathcal{R}(\mathcal{H})$ gives $\chi \in \mathcal{R}(\mathcal{G})$.

3. $cor^{\mathcal{G}}_{\mathcal{H}}(\mathcal{R}(\mathcal{H})) \subset \mathcal{R}(\mathcal{G})$.

4. If $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$ then $inf^{\mathcal{G}}_{\mathcal{H}}(\mathcal{R}(\mathcal{G}/\mathcal{H})) \subset \mathcal{R}(\mathcal{G})$.

Proof. 1. follows from lemma 3 (1).
2. By Sylow's theorem we can choose $RC_2(\mathcal{G}) \subset RC_2(\mathcal{H})$. Now apply lemma 3 (1).
2b. By lemma 3 (2) we get $0 = h_{N/N^{\mathcal{H}}} \circ \operatorname{res}^{\mathcal{H}}_{\mathcal{G}}(\chi) = s^* \circ h_{N/K}(\chi)$. Hence $h_{N/K}(\chi) = 0$ since s^* is injective by a theorem of Springer.
3. $\chi \in \mathcal{R}_{\mathcal{H}}$ gives $h_{N/N^{\mathcal{H}}}(\chi) = 0 \in \mathrm{W}(N^{\mathcal{H}})$. By lemma 3 (2) we are done.
4. Let $\chi \in \mathcal{R}(\mathcal{G}/\mathcal{H})$. Then $h_{N/K} \circ \operatorname{inf}^{\mathcal{G}}_{\mathcal{H}}(\chi) = h_{N^{\mathcal{H}}/K}(\chi) = 0$.
Now we are ready to reduce our approach to 2-groups. □

Lemma 5. (Reduction Lemma) *The rank formula of theorem 1 holds for a finite group $\mathcal{G}$ if it holds for any 2-Sylow group $\mathcal{G}_2$ of $\mathcal{G}$.*
Proof. By the assumption there is some $a \in \mathbb{N}$ with $a \cdot L(\mathcal{G}_2) \subset \mathcal{R}(\mathcal{G}_2)$. Let $\chi \in L(\mathcal{G})$. Then $\operatorname{res}^{\mathcal{G}_2}_{\mathcal{G}}(\chi) \in L(\mathcal{G}_2)$ by lemma 4 (2a). We get $\operatorname{res}^{\mathcal{G}_2}_{\mathcal{G}}(a\chi) = a \cdot \operatorname{res}^{\mathcal{G}_2}_{\mathcal{G}}(\chi) \in a \cdot L(\mathcal{G}_2) \subset \mathcal{R}(\mathcal{G}_2)$. Hence $a\chi \in \mathcal{R}(\mathcal{G})$ by lemma 4 (2b). □

9. The trace ideal of some 2-groups

Proposition 5. *Let $\mathcal{G}$ be a cyclic group of order $2^l \geq 2$. Then*

$$T(\mathcal{G}) = \{\sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}\chi_{\mathcal{H}} \mid \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}[\mathcal{G} : \mathcal{H}] = 0, m_1 = 0, \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \equiv 0 \colon mod \colon 2\}.$$

Hence $L(\mathcal{G})/T(\mathcal{G}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Proof. a) $L(\mathcal{G})$ is given by the equations

$$\sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] = 0 \tag{1}$$

$$\sum_{\mathcal{H}<\mathcal{G}, 2| \operatorname{ord}(\mathcal{H})} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] = 0.$$

Since $\operatorname{ord}(\mathcal{G}) = 2^l \geq 2$, the system (1) is equivalent to

$$m_1 = 0, \quad \sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq 1} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] = 0. \tag{2}$$

b) Set $K_0 := \mathbb{Q}(\sqrt{-1})$. For every $l \geq 1$ there is a cyclic extension N/K_0 of degree 2^l. Let $D \in K_0$ such that $K_0(\sqrt{D})/K_0$ is the unique quadratic subextension of N/K_0. Let $\chi = \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \chi_{\mathcal{H}} \in \mathcal{B}(\mathcal{G})$. Then $\det_{K_0} h_{N/K_0}(\chi) = D^m$, where $m = \sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq\mathcal{G}} m_{\mathcal{H}}$. Therefore

$$\sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq\mathcal{G}} m_{\mathcal{H}} \equiv \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \equiv 0 \colon \operatorname{mod} \colon 2$$

if $\chi \in \mathcal{T}(\mathcal{G})$ ($m_{\mathcal{G}}$ is even by (1)).
c) Now let $\chi \in L(\mathcal{G})$ with $\sum_{\mathcal{H}<\mathcal{G}, 2|[\mathcal{G}:\mathcal{H}]} m_{\mathcal{H}}$ is even. Let N/K be any Galois extension with Galois group $\mathcal{G}$ and $D = \det_K <N>$. From corollary 4 in [4] we get

$$\begin{aligned} h_{N/K}(\chi) &= \sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq 1} m_{\mathcal{H}} \times <N^{\mathcal{H}}> \\ &= m_{\mathcal{G}} \times <1> \perp \sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq 1, \mathcal{G}} m_{\mathcal{H}} \times (<2, 2D> \perp ([\mathcal{G} : \mathcal{H}] - 2) \times <1>) \\ &= \sum_{\mathcal{H}<\mathcal{G}, \mathcal{H}\neq 1} m_{\mathcal{H}} [\mathcal{G} : \mathcal{H}] \times <1> = 0, \end{aligned}$$

since $<2D, 2D> = <1, 1>$ if $l \geq 2$. □
Let $\mathbf{e}_2(a)$ be the exponent of 2 in $a \in \mathbb{Z}$.

Proposition 6. *Let $\mathcal{G}$ be an elementary abelian 2-group of order 2^n. Then*

$$\mathit{rank}(\mathcal{T}(\mathcal{G})) = \mathit{rank}(\mathcal{B}(\mathcal{G})) - \sharp RC_2(\mathcal{G}).$$

Further $\mathcal{T}(\mathcal{G})$ is determined by the system of linear equations given by

$$\sum_{\mathcal{H}<\mathcal{G}, \sigma\in\mathcal{H}} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] = 0, \quad \sigma \in \mathcal{G}, \ \mathit{ord}(\sigma) \leq 2$$

$$\sum_{\mathcal{H}<\mathcal{U}, \, \mathbf{e}_2([\mathcal{G}:\mathcal{H}])\equiv 0(2)} m_{\mathcal{H}} \equiv 0(2), \quad \mathcal{U} < \mathcal{G}, [\mathcal{G} : \mathcal{U}] = 2.$$

$L(\mathcal{G})/\mathcal{T}(\mathcal{G})$ has exponent 2.

Proof. 1) By proposition 2 we get

$$L(\mathcal{G}) = \{\sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}\chi_{\mathcal{H}} \mid \sum_{\mathcal{H}<\mathcal{G},\sigma\in\mathcal{H}} m_{\mathcal{H}}[\mathcal{G}:\mathcal{H}] = 0, \sigma \in \mathcal{G},\ \mathrm{ord}(\sigma) \leq 2\}.$$

Further $\mathcal{T}(\mathcal{G}) \subset L(\mathcal{G})$.
2) Let N/K be a Galois extension with $G(N/K) \simeq \mathcal{G}$. Then $N = K(\sqrt{a_1}, \ldots, \sqrt{a_n})$ for some $a_1, \ldots, a_n \in K^\star$. There are exactly $2^n - 1$ different subfields F of N/K with $[F : K] = 2$. These fields are given by $F = K(\sqrt{\alpha})$, where $\alpha = a_1^{e_1} \cdots a_n^{e_n}$ with $e_1, \ldots, e_n \in \{0, 1\}$, not all 0.
3) Let L be an arbitrary intermediate field of N/K with $[L : K] = 2^m \geq 2$. Then L is the compositum of its quadratic subextensions. Hence $L = K(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$ with $\alpha_1, \ldots, \alpha_m \in M := \{a_1^{e_1} \cdots a_n^{e_n} \mid (e_1, \ldots, e_n) \in \{0,1\}^n - \{(0, \ldots, 0)\}\}$. We further observe

$$<N>=<2^n> \otimes <<-a_1, \ldots, -a_n>>=<2^n> \otimes(<1>\perp\perp_{\alpha\in M}<\alpha>)$$

and

$$<L>=<2^m> \otimes <<-\alpha_1, \ldots, -\alpha_m>>=<2^m> \otimes(<1>\perp \psi_0),$$

where the coefficients of ψ_0 can be taken from M. Hence $<2^m> \otimes <L>$ is a subform of $<2^n> \otimes <N>$. Further the coefficients of $<2^m> \otimes <L>$ form a set of representatives of $L^\star/K^{\star 2}$, i.e. of the subextensions of L/K of degree ≤ 2 over K. Let $\chi = \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}\chi_{\mathcal{H}} \in L(\mathcal{G})$. Then

$$h_{N/K}(\chi) = \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \times <N^{\mathcal{H}}>= \sum_{\alpha\in M\cup\{1\}} (n_\alpha \times <\alpha>\perp m_\alpha \times <2\cdot\alpha>)$$

with multiplicities $n_\alpha, m_\alpha \in \mathbb{Z}$. We now determine these multiplicities.
a) Let $\mathcal{H} < \mathcal{G}, \alpha \in M$. Set $2^m = [\mathcal{G} : \mathcal{H}]$. Then $2^m \cdot \alpha$ is a coefficient of $<N^{\mathcal{H}}>$ if and only if $K(\sqrt{\alpha}) \subset N^{\mathcal{H}}$ if and only if $\mathcal{H} \subset G(N/K(\alpha)) =: \mathcal{G}_\alpha$. Hence

$$h_{N/K}(\chi) = \sum_{\alpha\in M\cup\{1\}} (\sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 0(2)} m_{\mathcal{H}} \times <\alpha> \perp \sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 1(2)} m_{\mathcal{H}} \times <2\cdot\alpha>)$$

b) Assertion: $\sum_{\mathcal{H}<\mathcal{G}_\alpha} m_{\mathcal{H}} = 0$ for all $\alpha \in M \cup \{1\}$.
Proof. i) Add the 2^n linear equations which define $L(\mathcal{G})$. We get

$$\begin{aligned} 0 &= \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] + \sum_{\sigma\in\mathcal{G},\ \mathrm{ord}(\sigma)=2} (\sum_{\mathcal{H}<\mathcal{G},\sigma\in\mathcal{H}} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}]) \\ &= \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} \cdot [\mathcal{G} : \mathcal{H}] + \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}(\ \mathrm{ord}(\mathcal{H}) - 1) \cdot [\mathcal{G} : \mathcal{H}] \\ &= 2^n \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}, \end{aligned}$$

since there are exactly $\mathrm{ord}(\mathcal{H}) - 1$ elements of order 2 in $\mathcal{G}$ which are contained in $\mathcal{H}$. Hence

$$\sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} = 0. \qquad \text{(I)}$$

Now suppose $\alpha \neq 1$.
ii) From (1) we get

$$2^{n-1} \cdot \sum_{\mathcal{H}<\mathcal{G}_\alpha} m_{\mathcal{H}} = 2^{n-1} \cdot \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}} - \sum_{\sigma\in\mathcal{G}_\alpha,\ \mathrm{ord}(\sigma)=2} \sum_{\mathcal{H}<\mathcal{G},<\sigma>\subsetneq\mathcal{H}} m_{\mathcal{H}} \cdot [\mathcal{G}:\mathcal{H}]$$
$$= 2^{n-1} \cdot \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}} - \sum_{\mathcal{H}<\mathcal{G}} n_{\mathcal{H}} \cdot m_{\mathcal{H}} \cdot [\mathcal{G}:\mathcal{H}]$$

with multiplicities $n_{\mathcal{H}} \in \mathbb{N}_0$. Now $n_{\mathcal{H}} = 0$ if $\mathrm{ord}(\mathcal{H}) = 1, 2$. Let $\mathcal{H} < \mathcal{G}$ with $\mathrm{ord}(\mathcal{H}) > 2$. Then

$$n_{\mathcal{H}} = \sharp\{\sigma \in \mathcal{G}_\alpha \mid \mathrm{ord}(\sigma) = 2, \sigma \in \mathcal{H}\} = \sharp\{\sigma \in \mathcal{G}_\alpha \cap \mathcal{H} \mid \mathrm{ord}(\sigma) = 2\}$$
$$= \begin{cases} \mathrm{ord}(\mathcal{H}) - 1, & \text{if } \mathcal{H} \subset \mathcal{G}_\alpha \\ \frac{1}{2} \cdot \mathrm{ord}(\mathcal{H}) - 1, & \text{if } \mathcal{H} \not\subset \mathcal{G}_\alpha. \end{cases}$$

($\mathcal{G}_\alpha$ has index 2 in $\mathcal{G}$. Hence $\mathcal{H} \not\subset \mathcal{G}_\alpha$ gives $\mathcal{H} \cdot \mathcal{G}_\alpha = \mathcal{G}$. Now consider $\mathcal{H}, \mathcal{G}_\alpha, \mathcal{G}$ as $\mathbb{F}_2$-vector spaces and apply the dimension formula). We get

$$2^{n-1} \sum_{\mathcal{H}<\mathcal{G}_\alpha} m_{\mathcal{H}} = 2^{n-1} \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}} - \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}}(\ \mathrm{ord}(\mathcal{H}) - 1)[\mathcal{G}:\mathcal{H}]$$
$$- \sum_{\mathcal{H}<\mathcal{G},\mathcal{H}\not\subset\mathcal{G}_\alpha} m_{\mathcal{H}}(\frac{1}{2}\ \mathrm{ord}(\mathcal{H}) - 1)[\mathcal{G}:\mathcal{H}]$$
$$= (2^{n-1} - 2^n) \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}} + \sum_{\mathcal{H}<\mathcal{G}_\alpha,\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}}[\mathcal{G}:\mathcal{H}]$$
$$- 2^{n-1} \sum_{\mathcal{H}<\mathcal{G},\mathcal{H}\not\subset\mathcal{G}_\alpha} m_{\mathcal{H}} + \sum_{\mathcal{H}<\mathcal{G},\mathcal{H}\not\subset\mathcal{G}_\alpha} m_{\mathcal{H}}[\mathcal{G}:\mathcal{H}]$$
$$= -2^{n-1} \sum_{\mathcal{H}<\mathcal{G},\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}} + \sum_{\mathcal{H}<\mathcal{G},\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}}[\mathcal{G}:\mathcal{H}]$$
$$= \sum_{\mathcal{H}<\mathcal{G},\ \mathrm{ord}(\mathcal{H})\neq 2} m_{\mathcal{H}}([\mathcal{G}:\mathcal{H}] - 2^{n-1}) = \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}([\mathcal{G}:\mathcal{H}] - 2^{n-1})$$
$$= \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}}[\mathcal{G}:\mathcal{H}] - 2^{n-1} \sum_{\mathcal{H}<\mathcal{G}} m_{\mathcal{H}} = 0$$

by (1) and (I). This proves the assertion (b).
4) Let us continue with the computation of $h_{N/K}(\chi)$, where $\chi \in L(\mathcal{G})$. From assertion (b) we get

$$\sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 0(2)} m_{\mathcal{H}} \times <\alpha> + \sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 1(2)} m_{\mathcal{H}} \times <2\cdot\alpha>$$
$$= \sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 0(2)} m_{\mathcal{H}} \times <\alpha, -2\cdot\alpha>\ .$$

This gives

$$h_{N/K}(\chi) = <1, -2> \otimes (\sum_{\alpha\in M\cup\{1\}} k_\alpha \times <\alpha>),$$

where $k_\alpha = \sum_{\mathcal{H}<\mathcal{G}_\alpha, e_2([\mathcal{G}:\mathcal{H}])\equiv 0(2)} m_\mathcal{H}$. Since $2\times <1,-2>= 0$, we get

$$h_{N/K}(\chi) = <1,-2> \otimes (\sum_{\alpha\in M\cup\{1\}} \bar{k}_\alpha \times <\alpha>),$$

where $\bar{k}_\alpha \in \{0,1\}$ with $\bar{k}_\alpha \equiv k_\alpha$: mod: 2. Hence the Witt class $h_{N/K}(\chi)$ is represented by a subform of $<1,-2> \otimes <<-a_1,\dots,-a_n>>=<1,-2> \otimes <2^n> \otimes <N>$. It remains to prove the following:

Let $\chi \in \mathcal{T}(\mathcal{G})$, then $\bar{k}_\alpha = 0$ for all $\alpha \in \{1\}\cup M$.
Let $X_1,\dots,X_n$ be indeterminates. Then the quadratic form
$\psi = <<-X_1,\dots,-X_n>>$ over $K = \mathbb{Q}(X_1,\dots,X_n)$ does not represent 2. Let ψ_0 be a subform of ψ with $<1,-2> \otimes \psi_0 = 0$. Suppose $\psi_0 = <a> \perp \psi_1 \neq 0$. Then

$$<a> \otimes \psi_0 \simeq <2> \otimes <a> \otimes \psi_0 \simeq <2> \perp <2a> \otimes \psi_1.$$

Since $<a>$ is a similarity factor of ψ, the form $<a> \otimes \psi_0$ is a subform of ψ, which represents 2. But ψ does not represent 2. We conclude $\psi_0 = 0$. Therefore $h_{N/K}(\chi) = 0$ gives $\bar{k}_\alpha = 0$ for $\alpha \in \{1\}\cup M$. □

Next we give an example where $L(\mathcal{G})/\mathcal{T}(\mathcal{G})$ has exponent 4.

Proposition 7. *Let $\mathcal{G} = Q_8$ be the quaternion group of order 8. Then*

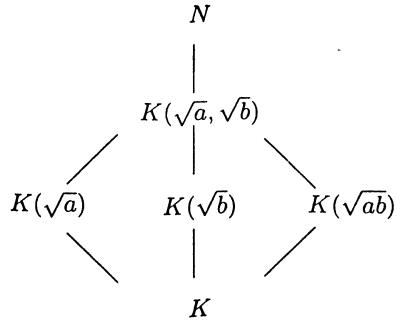
$$\mathcal{T}(\mathcal{G}) = \{\chi = \sum_{\mathcal{H}\in \mathrm{RC}(\mathcal{G})} m_\mathcal{H}\chi_\mathcal{H} \mid \chi \in L(\mathcal{G}),\ m_{\mathcal{H}_1} \equiv m_{\mathcal{H}_2} \equiv m_{\mathcal{H}_3} : \textit{mod}: 4 \text{ for all subgroups } \mathcal{H}_1,\mathcal{H}_2,\mathcal{H}_3 \text{ of order 4 in } Q_8\}.$$

Proof. We use the following facts: Q_8 contains a unique element σ of order 2. There are three subgroups $\mathcal{H}_1,\mathcal{H}_2,\mathcal{H}_3$ in Q_8 of order 4. They are not conjugate. All subgroups are normal subgroups.
Hence $L(Q_8)$ is defined by

$$\begin{aligned} m_\mathcal{G} + 2m_{\mathcal{H}_1} + 2m_{\mathcal{H}_2} + 2m_{\mathcal{H}_3} + 4m_{<\sigma>} + 8m_1 &= 0 \\ m_\mathcal{G} + 2m_{\mathcal{H}_1} + 2m_{\mathcal{H}_2} + 2m_{\mathcal{H}_3} + 4m_{<\sigma>} &= 0 \end{aligned}$$

This gives $m_1 = 0$ and $m_\mathcal{G} \equiv 0$: mod: 2.

Let N/K be a Galois extension with Galois group $G(N/K) \simeq Q_8$. Since $Q_8/<\sigma>$ is elementary abelian, the subextensions of N/K are as follows



with $a, b \in K^*$ such that $a, b \in N^{*2}$, but $a, b, ab \notin K^{*2}$. By Witt [8] we know $<1, a, b, ab> = 4\times <1>$. Hence $<K(\sqrt{a}, \sqrt{b})> = <<-a, -b>> = 4\times <1>$. Since $m_1 = 0$ we do not have to determine $h_{N/K}(\chi_1) = <N>$ (see [4]). We get

$$\begin{aligned} h_{N/K}(\chi) &= m_{\mathcal{G}}\times <1> \perp m_{\mathcal{H}_1}\times <2, 2a> \perp m_{\mathcal{H}_2}\times <2, 2b> \perp m_{\mathcal{H}_3}\times <2, 2ab> \\ &\quad \perp 4m_{<\sigma>}\times <1> \\ &= (m_{\mathcal{G}} + 4m_{<\sigma>})\times <1> \perp (m_{\mathcal{H}_1} + m_{\mathcal{H}_2} + m_{\mathcal{H}_3})\times <2> \\ &\quad \perp m_{\mathcal{H}_1}\times <2a> \perp m_{\mathcal{H}_2}\times <2b> \perp m_{\mathcal{H}_3}\times <2ab> \\ &= (m_{\mathcal{G}} + 4m_{<\sigma>} + m_{\mathcal{H}_1} + m_{\mathcal{H}_2} + m_{\mathcal{H}_3})\times <2> \\ &\quad \perp m_{\mathcal{H}_1}\times <2a> \perp m_{\mathcal{H}_2}\times <2b> \perp m_{\mathcal{H}_3}\times <2ab> \\ &= <-2> \otimes (m_{\mathcal{H}_1}\times <1, -a> \perp m_{\mathcal{H}_2}\times <1, -b> \perp m_{\mathcal{H}_3}\times <1, -ab>) \\ &= <-2> \otimes (\overline{m}_{\mathcal{H}_1}\times <1, -a> \perp \overline{m}_{\mathcal{H}_2}\times <1, -b> \perp \overline{m}_{\mathcal{H}_3}\times <1, -ab>), \end{aligned}$$

where $\overline{m}_{\mathcal{H}_j} \in \{0, 1, 2, 3\}$ with $\overline{m}_{\mathcal{H}_j} \equiv m_{\mathcal{H}_j} : \mathrm{mod}: 4$. From $<1, a, b, ab> = 4\times <1>$ we get $4\times <1, -a> = 4\times <1, -b> = 4\times <1, -ab> = 0$ and

$$\psi = <1, -a> \perp <1, -b> \perp <1, -ab> = 0 \tag{1}$$

Hence $h_{N/K}(\chi) = 0$ if $\overline{m}_{\mathcal{H}_1} = \overline{m}_{\mathcal{H}_2} = \overline{m}_{\mathcal{H}_3}$.

Now set $a = 6, b = 14$. Then $< 1, 6, 14, 21 > = 4\times < 1 > \in \mathrm{W}(\mathbb{Q})$. Hence $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ is contained in a Galois extension $N/\mathbb{Q}$ with Galois group Q_8. We further get $G(N(\sqrt{-1})/\mathbb{Q}(\sqrt{-1})) \simeq Q_8$. Consider the discriminant of $h_{N(\sqrt{-1})/\mathbb{Q}(\sqrt{-1})}(\chi)$. We get

$$\overline{m}_{\mathcal{H}_1} \equiv \overline{m}_{\mathcal{H}_2} \equiv \overline{m}_{\mathcal{H}_3} : \mathrm{mod}: 2 \text{ if } \chi \in \mathcal{T}(\mathcal{G}). \tag{2}$$

Let $\chi \in \mathcal{T}(\mathcal{G})$. Then (1) and (2) implies

$$h_{N/K}(\chi) = <-2> \otimes (a_1\times <1, -a> \perp a_2\times <1, -b> \perp a_3\times <1, -ab>)$$

with $a_1, a_2, a_3 \in \{0, 2\}$. Suppose $a_1 = a_2 \neq a_3$. By (1) we can assume $a_1 = a_2 = 0$. Since $6, 14, 21$ cannot be written as a sum of two rational squares we get $2\times <1, -21> \neq 0$. □

10. Proof of theorem 1

Let $\mathcal{J}_2(\mathcal{G})$ be the set of involutions of $\mathcal{G}$. For any subgroup $\mathcal{H}$ of $\mathcal{G}$ define

$$X^{\mathcal{G}}_{\mathcal{H}} := \mathrm{ord}(\mathcal{H})\chi^{\mathcal{G}}_{\mathcal{H}} - \chi^{\mathcal{G}}_1 + \sum_{\tau \in \mathcal{J}_2(\mathcal{H})} (\chi^{\mathcal{G}}_1 - 2\chi^{\mathcal{G}}_\tau)$$

and set

$$M_{\mathcal{G}} := \{X^{\mathcal{G}}_{\mathcal{H}} \mid \mathcal{H} \in RC(\mathcal{G}),\ \mathrm{ord}(\mathcal{H}) \neq 1, 2\}.$$

Consider involutions τ, τ' of $\mathcal{G}$. We know $\chi_\tau = \chi_{\tau'}$ if and only if $\tau' \in \mathcal{G}\tau$. From $\mathcal{J}_2(\mathcal{H}) = \mathcal{J}_2(\mathcal{G}) \cap \mathcal{H} = \cup_{\tau \in RC_2(\mathcal{G}), \tau \neq 1} \mathcal{G}\tau \cap \mathcal{H}$ we get

$$X^{\mathcal{G}}_{\mathcal{H}} = \mathrm{ord}(\mathcal{H})\chi^{\mathcal{G}}_{\mathcal{H}} - \chi^{\mathcal{G}}_1 + \sum_{\tau \in RC_2(\mathcal{G}), \tau \neq 1} \sharp(\mathcal{G}\tau \cap \mathcal{H})(\chi^{\mathcal{G}}_1 - 2\chi^{\mathcal{G}}_\tau).$$

Hence by proposition 2 $M_{\mathcal{G}}$ is a free subset of $L(\mathcal{G})$ consisting of $\operatorname{rank}(L(\mathcal{G}))$ elements.

Let $\mathcal{G}$ be a 2-group of order 2^l. We will prove by induction on the order of $\mathcal{G}$ that $M_{\mathcal{G}}$ is already contained in $\mathcal{R}(\mathcal{G})$.

1. Let $\mathcal{G}$ be an elementary abelian 2-group. Then all coefficients of $X_{\mathcal{H}}^{\mathcal{G}}$ are even. Hence proposition 6 gives $M_{\mathcal{G}} \subset \mathcal{R}(\mathcal{G})$.

2. Let $\mathcal{H}$ be a subgroup of $\mathcal{G}$ with $\mathcal{H} \neq \mathcal{G}$. Consider a maximal subgroup $\mathcal{U}$ of $\mathcal{G}$ which contains $\mathcal{H}$. Then $X_{\mathcal{H}}^{\mathcal{U}} \in \mathcal{R}(\mathcal{U})$ by the induction hypothesis. From lemma 4 (3) we get $X_{\mathcal{H}}^{\mathcal{G}} = \operatorname{cor}_{\mathcal{U}}^{\mathcal{G}}(X_{\mathcal{H}}^{\mathcal{U}}) \in \mathcal{R}(\mathcal{G})$.

3. Claim: $X_{\mathcal{G}}^{\mathcal{G}} \in \mathcal{R}(\mathcal{G})$ for any non-elementary abelian 2-group $\mathcal{G}$.

Let $\mathcal{U}_1, \ldots, \mathcal{U}_m$ be the maximal subgroups of $\mathcal{G}$. Since $\mathcal{G}$ has at least order 4 each involution is contained in some $\mathcal{U}_i$. We get

$$\sum_{\tau \in \mathcal{J}_2(\mathcal{G})} (\chi_1^{\mathcal{G}} - 2\chi_\tau^{\mathcal{G}}) = \sum_{\mathcal{H}=\mathcal{U}_{i_1} \cap \ldots \cap \mathcal{U}_{i_r}} (-1)^{r+1} \sum_{\tau \in \mathcal{J}_2(\mathcal{H})} (\chi_1^{\mathcal{G}} - 2\chi_\tau^{\mathcal{G}}),$$

where the sum runs over the set of all non-empty subset of indices in $\{1, \ldots, m\}$. Let us consider $\sum_{\tau \in \mathcal{J}_2(\mathcal{H})}(\chi_1^{\mathcal{G}} - 2\chi_\tau^{\mathcal{G}})$ for any $\mathcal{H} = \mathcal{U}_{i_1} \cap \ldots \cap \mathcal{U}_{i_r}$. As usual, $\Phi(\mathcal{G})$ denotes the Frattini subgroup of $\mathcal{G}$. Let $\bar{\mathcal{H}}$ be the image of $\mathcal{H}$ under the canonical projection $\mathcal{G} \to \mathcal{G}/\Phi(\mathcal{G}) = \bar{\mathcal{G}}$. By the induction hypothesis and lemma 4 (3) we get $\operatorname{cor}_{\mathcal{H}}^{\mathcal{G}}(X_{\mathcal{H}}^{\mathcal{H}}) \in \mathcal{R}(\mathcal{G})$. This implies

$$\sum_{\tau \in \mathcal{J}_2(\mathcal{H})} (\chi_1^{\mathcal{G}} - 2\chi_\tau^{\mathcal{G}}) \equiv (\chi_1^{\mathcal{G}} - \operatorname{ord}(\mathcal{H})\chi_{\mathcal{H}}^{\mathcal{G}}) \bmod \mathcal{R}(\mathcal{G}).$$

Suppose $\bar{\mathcal{H}} \neq 1$. Since $\bar{\mathcal{H}}$ is a subgroup of the elementary abelian 2-group $\bar{\mathcal{G}} = \mathcal{G}/\Phi(\mathcal{G})$ we get from (1)

$$\begin{aligned}
\operatorname{ord}(\bar{\mathcal{H}})\chi_{\mathcal{H}}^{\mathcal{G}} &= \operatorname{cor}_{\mathcal{H}}^{\mathcal{G}} \circ \inf_{\mathcal{H}}^{\bar{\mathcal{H}}}(\operatorname{ord}(\bar{\mathcal{H}})\chi_{\bar{\mathcal{H}}}^{\bar{\mathcal{H}}}) \\
&\equiv \operatorname{cor}_{\mathcal{H}}^{\mathcal{G}} \circ \inf_{\mathcal{H}}^{\bar{\mathcal{H}}}(\chi_1^{\bar{\mathcal{H}}} - \sum_{\tau \in \mathcal{J}_2(\bar{\mathcal{H}})} (\chi_1^{\bar{\mathcal{H}}} - 2\chi_\tau^{\bar{\mathcal{H}}})) \\
&\equiv \operatorname{cor}_{\mathcal{H}}^{\mathcal{G}}(\chi_{\Phi(\mathcal{G})}^{\mathcal{H}} - \sum_{\tau \in \mathcal{J}_2(\bar{\mathcal{H}})} (\chi_{\Phi(\mathcal{G})}^{\mathcal{H}} - 2\chi_{\tau \cup \Phi(\mathcal{G})}^{\mathcal{H}})) \\
&\equiv \chi_{\Phi(\mathcal{G})}^{\mathcal{G}} - \sum_{\tau \in \mathcal{J}_2(\bar{\mathcal{H}})} (\chi_{\Phi(\mathcal{G})}^{\mathcal{G}} - 2\chi_{\tau \cup \Phi(\mathcal{G})}^{\mathcal{G}})) \bmod \mathcal{R}(\mathcal{G}).
\end{aligned}$$

Obviously, the last formula also holds for $\bar{\mathcal{H}} = 1$. We finally conclude

$$\begin{aligned}
X_{\mathcal{G}}^{\mathcal{G}} &= \operatorname{ord}(\mathcal{G})\chi_{\mathcal{G}}^{\mathcal{G}} - \chi_1^{\mathcal{G}} + \sum_{\mathcal{H}}(-1)^{r+1} \sum_{\tau\in\mathcal{J}_2(\mathcal{H})} (\chi_1^{\mathcal{G}} - \chi_\tau^{\mathcal{G}}) \\
&\equiv \operatorname{ord}(\mathcal{G})\chi_{\mathcal{G}}^{\mathcal{G}} - \chi_1^{\mathcal{G}} \\
&\quad + \sum_{\mathcal{H}}(-1)^{r+1}[\chi_1^{\mathcal{G}} - \operatorname{ord}(\Phi(\mathcal{G}))\chi_{\Phi(\mathcal{G})}^{\mathcal{G}} \\
&\quad + \operatorname{ord}(\Phi(\mathcal{G}))\cdot \sum_{\tau\in\mathcal{J}_2(\bar{\mathcal{H}})} (\chi_{\Phi(\mathcal{G})}^{\mathcal{G}} - 2\chi_{\tau\cup\Phi(\mathcal{G})}^{\mathcal{G}})] \\
&\equiv \operatorname{ord}(\mathcal{G})\chi_{\mathcal{G}}^{\mathcal{G}} - \operatorname{ord}(\Phi(\mathcal{G}))\chi_{\Phi(\mathcal{G})}^{\mathcal{G}} \\
&\quad + \operatorname{ord}(\Phi(\mathcal{G}))[\sum_{\mathcal{H}}(-1)^{r+1} \sum_{\tau\in\mathcal{J}_2(\mathcal{H})} (\chi_{\Phi(\mathcal{G})}^{\mathcal{G}} - 2\chi_{\tau\cup\Phi(\mathcal{G})}^{\mathcal{G}})] \\
&\equiv \operatorname{ord}(\Phi(\mathcal{G}))\cdot \inf_{\Phi(\mathcal{G})}^{\mathcal{G}}[(\operatorname{ord}(\bar{\mathcal{G}}))\chi_{\bar{\mathcal{G}}}^{\mathcal{G}} - \chi_1^{\mathcal{G}} + \sum_{\mathcal{H}}(-1)^{r+1} \sum_{\tau\in\mathcal{J}_2(\mathcal{H})} (\chi_1^{\bar{\mathcal{G}}} - 2\chi_\tau^{\bar{\mathcal{G}}}))] \\
&= \operatorname{ord}(\Phi(\mathcal{G}))\cdot \inf_{\Phi(\mathcal{G})}^{\mathcal{G}}(X_{\bar{\mathcal{G}}}^{\bar{\mathcal{G}}}) \equiv 0 \bmod \mathcal{R}(\mathcal{G})
\end{aligned}$$

Observe, that $\sum_{r=0}^{n}(-1)^r\binom{n}{r} = 0$ and that $\mathcal{G}$ is not elementary abelian. Hence $X_{\bar{\mathcal{G}}}^{\bar{\mathcal{G}}} \in \mathcal{R}(\bar{\mathcal{G}})$ by the induction hypothesis.

References

[1] J. Alperin and B. Bell. *Groups and Representations.* Graduate texts in mathematics. Springer, New York, 1995.

[2] P. Beaulieu and T. Palfrey. The Galois number. *Math. Ann.*, 309:81–96, 1997.

[3] P.E. Conner and R. Perlis. *A Survey of Trace Forms of Algebraic Number Fields.* World Scientific, Singapore, 1984.

[4] Christof Drees, Martin Epkenhans, and Martin Krüskemper. On the computation of the trace form of some Galois extensions. *J. Algebra*, 192:209–234, 1997.

[5] Martin Epkenhans and Martin Krüskemper. On Trace Forms of étale Algebras and Field Extensions. *Math. Z.*, 217:421–434, 1994.

[6] D. Gorenstein. *Finite Groups.* Harper and Row, New York, 1968.

[7] D. W. Lewis. Witt rings as integral rings. *Invent. Math.*, 90:631–633, 1987.

[8] Ernst Witt. Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. Reine Angew. Math.*, 174:237–245, 1936.

Author's address: Fb Mathematik, Universität-Gesamthochschule, D-33095 Paderborn

E-mail: martine@@uni-paderborn.de

Received: January 13, 1998