Cohomology operations in Milnor K-theory mod ℓ, transfer of quadratic forms and Stiefel-Whitney invariants

Timo Keller

March 5, 2017

Abstract

This article arose from the question if there is a Grothendieck-Riemann-Roch style formula for the Stiefel-Whitney invariants of quadratic forms with the Scharlau transfer $s_* : \widehat{W}(L) \to \widehat{W}(K)$ on the quadratic forms side and corestriction $\mathrm{cor} : \mathrm{H}^{**}(L) \to \mathrm{H}^{**}(K)$ on the Galois cohomology or, equivalently, the norm map $\mathrm{N}_{L/K} : \mathrm{K}^{\mathrm{M}}_{**}(L)/2 \to \mathrm{K}^{\mathrm{M}}_{**}(K)/2$ on the Milnor K-theory side, respectively. The answer is negative, but we prove a partial formula. To this end, we classify all cohomology operations in Milnor K-theory mod ℓ. Furthermore, we calculate some trace forms.

Keywords: Quadratic forms over general fields; cohomology theory; Milnor K-theory

MSC 2010: 11E04, 20G10, 19D45

1 Introduction

Let L/K be a finite separable field extension and $q \in \widehat{W}(L)$ be a quadratic form. According to Kahn [Kah84], there is the following relation between $w(\mathrm{Tr}(q))$ and $w(q)$:

$$w(\mathrm{Tr}(q)) = \mathscr{N}(w(q)) \cdot w(\mathrm{Tr}(\langle 1 \rangle))^{\dim q}$$

Here, $\mathscr{N}$ is Evens' [Eve63] multiplicative norm $\mathscr{N} : \mathrm{H}^{**}(L) \to \mathrm{H}^{**}(K)$, $\dim q$ is the dimension of q and $w(\mathrm{Tr}(\langle 1 \rangle))$ the absolute Stiefel-Whitney invariant of the trace form of L/K.

According to this formula, the calculation of $w(\mathrm{Tr}(q))$ is split up into two parts: On the one hand, one has to find an easy formula for the multiplicative norm $\mathscr{N}$ (see Theorem 4.3), one the other hand, one has to calculate $w(\mathrm{Tr}(\langle 1 \rangle))$ (see Theorem 5.9). In the special case $q \in \hat{I}^n$, the problem simplifies because of $\dim q = 0$ to

$$w(\mathrm{Tr}(q)) = \mathscr{N}(w(q))$$

and there is an easy *partial* Riemann-Roch formula:

Theorem 1 (Theorem 4.3). *Let $n \geq 1$, $t = 2^{n-1}$. Then one has, for all $q \in \hat{I}^n_L$ and all Scharlau transfers $s : L \to K$,*

$$w_k(s(q)) = \mathrm{cor}(w_k(q))$$

for all k not divisible by t and for $k = t$. Here, both sides are 0 if k is not divisible by t.

For the first Stiefel-Whitney invariant, there were already results by Bourbaki. Serre [Ser84] considered the second Stiefel-Whitney invariant and obtained a formula in 1984. Since then, there had been no further results.

The Grothendieck-Riemann-Roch formula is

$$\mathrm{ch}(f_*(\alpha)) \cdot \mathrm{Td}(T_Y) = f_*(\mathrm{ch}(\alpha) \cdot \mathrm{Td}(T_X)).$$

One can ask if there is a similar formula for the absolute Stiefel-Whitney invariants in place of the Chern class and the transfer Tr and the corestriction in place of the push-forward:

$$F(w(\mathrm{Tr}_{L/K}(q))) = \mathrm{cor}(G(w(q)))$$

with F, G cohomology operations in Milnor K-theory mod 2 in place of the product with a Todd class. To this end, we classify all cohomology operations in Milnor K-theory mod ℓ in Theorem 2.4, and show that for certain local fields, if such a formula holds, all these cohomology operations have to be trivial on H^2 in section 3.

Notation. Denote the cokernel of $A \xrightarrow{n} A$ by A/n and its kernel by $A[n]$. Denote Milnor K-theory of a field K by $\mathrm{K}_i^{\mathrm{M}}(K)$ and $\mathrm{K}_*^{\mathrm{M}}(K) = \oplus_{i\geq 0}\mathrm{K}_i^{\mathrm{M}}(K)$ and $\mathrm{K}_{**}^{\mathrm{M}}(K) = \prod_{i\geq 0}\mathrm{K}_i^{\mathrm{M}}(K)$. Quadratic forms are denoted by $\langle a_1, \dots, a_n\rangle$, and for $a_i \in K^\times$ the Pfister form $\langle\langle a_1, \dots, a_n\rangle\rangle = \prod_{i=1}^n(\langle 1, -a_i\rangle)$. For a field K, let $\mathrm{H}^i(K) = \mathrm{H}^i(K, \mathbf{Z}/2)$ be Galois cohomology, $\mathrm{H}^*(K) = \oplus_{i\geq 0}\mathrm{H}^i(K)$ and $\mathrm{H}^{**}(K) = \prod_{i\geq 0}\mathrm{H}^i(K)$. Canonical isomorphisms are often denoted by "=". Denote the Grothendieck-Witt ring of a field K by $\widehat{W}(K)$ with fundamental ideal $\hat{I}_K$ and its Witt ring by $W(K)$. Write $i_{L/K}$ for the morphism $\mathrm{K}_i^{\mathrm{M}}(K) \to \mathrm{K}_i^{\mathrm{M}}(L)$ on Milnor K-theory induced by a field extension L/K. For a finite separable field extension L/K denote the transfer $W(L) \to W(K)$ resp. $\widehat{W}(L) \to \widehat{W}(K)$ by $\mathrm{Tr}_{L/K}$. Denote the absoulte Stiefel-Whitney invariant by $w : \widehat{W}(K) \to \mathrm{K}_{**}^{\mathrm{M}}(K)/2 = \mathrm{H}^{**}(K)$ (the equality by the Milnor conjecture) and its graded components by w_i.

2 Cohomology operations in Milnor K-theory mod ℓ

Definition 2.1. *Let ℓ be prime. A* **cohomology operation of type $(1, n; \ell)$** *is a natural transformation $\mathrm{K}_m^{\mathrm{M}}(-)/\ell \to \mathrm{K}_n^{\mathrm{M}}(-)/\ell$ of functors from the category of fields to the category of Abelian groups.*

For $x \in \mathrm{K}_n^{\mathrm{M}}(K)/\ell$, let $x \cdot -$ be the cohomology operation $F(L) : \mathrm{K}_m^{\mathrm{M}}(L)/\ell \to \mathrm{K}_n^{\mathrm{M}}(L)/\ell, a \mapsto i_{L/K}(x) \cdot a$ of type $(*, * + n; \ell)$ on the category of fields over K.

Obviously, $x \cdot -$ is indeed a cohomology operation of type $(*, * + n; \ell)$.

Lemma 2.2. *Let $x \in \mathrm{K}_n^{\mathrm{M}}(K)/\ell$. If the natural transformation $x \cdot -$ is 0, one has $x = 0$.*

Proof. If $\partial_t(\{t\} \cdot i_{K(t)/K}(x)) = x \neq 0$ (the equality by [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2), then $\{t\} \cdot i_{K(t)/K}(x) \neq 0$, hence also $x \neq 0$. □

I thank Charles Vial who sketched large parts of the following proof to me.

Theorem 2.3. *Let ℓ be prime and K be a perfect field of characteristic $\neq \ell$. For $n \in \mathbf{Z}$, the group of cohomology operations of type $(1, n; \ell)$ for the category of fields over K is isomorphic to $\mathrm{K}_{n-1}^{\mathrm{M}}(K)/\ell$, with isomorphism given by $x \mapsto (x \cdot -)$.*

Proof. Let K be a perfect field of characteristic $\neq \ell$ and k/K a field extension. Let F be a cohomology operation of type $(1, n; \ell)$.

First, assume $n \geq 1$.

Let $\pi \in K[t]$ be a monic irreducible polynomial $\neq 0, t$, and $K(t)_\pi$ the completion of $K(t)$ with respect to the discrete valuation defined by (π) and $\kappa = K[t]/(\pi)$ the corresponding residue class field. By [Mil70], p. 327, Lemma 2.6 and [GS06], p. 189, Corollary 7.1.10 and by the assumption on the characteristic, there is an isomorphism $(s_\pi, \partial_{(\pi)}) : \mathrm{K}_*^{\mathrm{M}}(K(t)_\pi)/\ell \to \mathrm{K}_*^{\mathrm{M}}(\kappa)/\ell \oplus \mathrm{K}_{*-1}^{\mathrm{M}}(\kappa)/\ell$. Since K is perfect, there is by [Mat86], p. 215 ff., Theorem 28.3 (iii), (iv) a coefficient field for κ in the valuation ring of $K(t)_\pi$ containing K. Let $i_{K(t)_\pi/\kappa}$ be the morphism induced by this inclusion. From the definition of s_π, it follows that $s_\pi \circ i_{K(t)_\pi/\kappa} = \mathrm{id}$. Thus, the sequence

$$0 \longrightarrow \mathrm{K}_*^{\mathrm{M}}(\kappa)/\ell \xrightarrow{i_{K(t)_\pi/\kappa}} \mathrm{K}_*^{\mathrm{M}}(K(t)_\pi)/\ell \xrightarrow{\partial_{(\pi)}} \mathrm{K}_{*-1}^{\mathrm{M}}(\kappa)/\ell \longrightarrow 0$$

is exact: The left hand morphism is injective, since s_π is a retract of $i_{K(t)_\pi/\kappa}$. If $\partial_{(\pi)}(x) = 0$ for $x \in \mathrm{K}_*^{\mathrm{M}}(K(t)_\pi)/\ell$, let $x' = i_{K(t)_\pi/\kappa}(s_\pi(x))$. Because of $s_\pi \circ i_{K(t)_\pi/\kappa} = \mathrm{id}$, one has $s_\pi(x') = s_\pi(x)$. From [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2, it follows that $\partial_{(\pi)} \circ i_{K(t)_\pi/\kappa} = 0$ since $i_{K(t)_\pi/\kappa}$ has image in the coefficient field $\kappa \subset K(t)_\pi$ of $K(t)_\pi \cong \kappa((s))$, and so consists of units and 0. Hence, $\partial_{(\pi)}(x') = 0$. Summing up, one has $(s_\pi, \partial_{(\pi)})(x) = (s_\pi, \partial_{(\pi)})(x')$, so $x = x' \in \mathrm{im}(i_{K(t)_\pi/\kappa})$ since $(s_\pi, \partial_{(\pi)})$ is an isomorphism.

Applying the natural transformation F, which commutes with the field inclusion, one gets the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{K}_1^{\mathrm{M}}(\kappa)/\ell & \xrightarrow{i_{K(t)_\pi/\kappa}} & \mathrm{K}_1^{\mathrm{M}}(K(t)_\pi)/\ell & \xrightarrow{\partial_{(\pi)}} & \mathrm{K}_0^{\mathrm{M}}(\kappa)/\ell & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F(\kappa)} & & \downarrow{\scriptstyle F(k_\pi)} & & & & \\
0 & \longrightarrow & \mathrm{K}_n^{\mathrm{M}}(\kappa)/\ell & \xrightarrow{i_{K(t)_\pi/\kappa}} & \mathrm{K}_n^{\mathrm{M}}(K(t)_\pi)/\ell & \xrightarrow{\partial_{(\pi)}} & \mathrm{K}_{n-1}^{\mathrm{M}}(\kappa)/\ell & \longrightarrow & 0
\end{array}$$

Consider the element $\{t\} \in \mathrm{K}_1^{\mathrm{M}}(K(t))/\ell$ and its inclusion in $K(t)_\pi$. Because of $(\pi) \neq (0), (t)$, t is a unit in the valuation ring of $K(t)$ and hence $\partial_{(\pi)}(i_{K(t)_\pi/K(t)}(\{t\})) = 0$ by definition of $\partial_{(\pi)}$ [Mil70], p. 322 ff., Lemma 2.1

and Lemma 2.2. It follows from the exactness of the upper row that $i_{K(t)_\pi/K(t)}(\{t\})$ comes from an element of $\mathrm{K}_1^{\mathrm{M}}(\kappa)/\ell$, so $F(K(t)_\pi)(i_{K(t)_\pi/K(t)}(\{t\}))$ comes by the commutativity of the left square from an element of $\mathrm{K}_n^{\mathrm{M}}(\kappa)/\ell$. Hence, by the exactness of the lower row,

$$\partial_{(\pi)}(F(K(t)_\pi)(i_{K(t)_\pi/K(t)}(\{t\}))) = 0.$$

Now,

$$\partial_{(\pi)}(F(K(t)_\pi)(i_{K(t)_\pi/K(t)}(\{t\}))) = \partial_{(\pi)}(i_{K(t)_\pi/K(t)}(F(K(t))(\{t\})))$$

since F is a natural transformation. Finally, one has

$$\partial_{(\pi)} \circ i_{K(t)_\pi/K(t)} = \partial_{(\pi)} : \mathrm{K}_*^{\mathrm{M}}(K(t))/\ell \to \mathrm{K}_{*-1}^{\mathrm{M}}(\kappa)/\ell$$

by [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2.

Summing up, one gets

$$\partial_{(\pi)}(F(K(t))(\{t\})) = 0$$

for all $(\pi) \neq (0), (t)$. Hence, by [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2

$$x = F(K(t))(\{t\}) - \{t\} \cdot i_{K(t)/K}(\partial_{(t)}(F(K(t))(\{t\})))$$

has residue 0 at all places $\neq (0)$ residue 0: At the places $(\pi) \neq (0), (t)$ because

$$\partial_{(\pi)}(F(K(t))(\{t\})) = 0$$

and

$$\partial_{(\pi)}(\{t\} \cdot i_{K(t)/K}(\partial_{(t)}(F(K(t))(\{t\}))) = 0$$

by [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2, since t is a unit in the valuation ring associated to (π) and $\partial_{(t)}(F(K(t))(\{t\}))$ is a sum of products of units in the valuation ring (since $K^\times$ is a subset of the units of the valuation ring); at the place (t), since by [Mil70], p. 322 ff., Lemma 2.1 and Lemma 2.2

$$\partial_{(t)}(\{t\} \cdot i_{K(t)/K}(\partial_{(t)}(F(K(t))(\{t\})))) = \partial_{(t)}(F(K(t))(\{t\})).$$

Hence, by [Mil70], p. 325 ff., Theorem 2.3

$$x = i_{K(t)/K}(b) \in \mathrm{im}(i_{K(t)/K} : \mathrm{K}_{n-1}^{\mathrm{M}}(K)/\ell \to \mathrm{K}_{n-1}^{\mathrm{M}}(K(t))/\ell).$$

Let

$$a = \partial_{(t)}(F(K(t))(\{t\}) \in \mathrm{K}_{n-1}^{\mathrm{M}}(K[t]/(t))/\ell = \mathrm{K}_{n-1}^{\mathrm{M}}(K)/\ell.$$

It follows that $F(\{t\}) = \{t\} \cdot i_{K(t)/K}(b) + i_{K(t)/K}(b)$. By Step 1 in [Via08], p. 12 f., one has $F = (a \cdot -) + b$. Since F is additive, we get $b = 0$.

Summing up, it follows that for the category of fields over K, every cohomology operation of type $(1, n; \ell)$ is equal to a $x \cdot -$. Conversely, $x \cdot -$ is obviously a cohomology operation of type $(1, n; \ell)$. For different x, one gets by Lemma 2.2 different cohomology operations, hence the claim.

The case $n \leq 0$ is trivial: If $n < 0$, obviously, every operation is trivial, and also $\mathrm{K}_{n-1}^{\mathrm{M}}(K)/\ell = 0$ by definition. If $n = 0$, let L/K be a field extension and $\{a\} \in \mathrm{K}_1^{\mathrm{M}}(L)/\ell$. Then

$$\begin{aligned} i_{L(\sqrt[\ell]{a})/L}(F(L)(\{a\})) &= F(L(\sqrt[\ell]{a}))(i_{L(\sqrt[\ell]{a})/L}(\{a\})) \\ &= F(L(\sqrt[\ell]{a}))(\ell \cdot \{\sqrt[\ell]{a}\}) \\ &= F(L(\sqrt[\ell]{a}))(0) \\ &= 0. \end{aligned}$$

But $i_{L(\sqrt[\ell]{a})/L} : \mathbf{Z}/\ell = \mathrm{K}_0^{\mathrm{M}}(L)/\ell \to \mathrm{K}_0^{\mathrm{M}}(L(\sqrt[\ell]{a}))/\ell = \mathbf{Z}/\ell$ is the identity, so $F(L)(\{a\}) = 0$. Summing up, one gets $F = 0$, and one also has $\mathrm{K}_{-1}^{\mathrm{M}}(K)/\ell = 0$ by definition. □

Theorem 2.4. *Let ℓ be prime and K be a perfect field of characteristic $\neq \ell$. Let $m, n \geq 0$ be integers.*

The group of cohomology operations of type $(m, n; \ell)$ for the category of fields over K is isomorphic to $\mathrm{K}_{n-m}^{\mathrm{M}}(K)/\ell$, the isomorphism given by $x \mapsto (x \cdot -)$.

Proof. Let K be a perfect field of characteristic $\neq \ell$. Let F be a cohomology operation of type $(m, n; \ell)$.

If $m = 0$, one has $F(L)(a) = F(L)(i_{L/K}(a)) = i_{L/K}(F(K)(a))$ for all field extensions L/K and $a \in \mathrm{K}_0^{\mathrm{M}}(K)/\ell = \mathbf{Z}/\ell = \mathrm{K}_0^{\mathrm{M}}(L)/K$ since $i_{L/K}$ is the identity in degree 0. So F is determined by $F(K)$, and since $\mathrm{K}_0^{\mathrm{M}}(K)/\ell$ is generated by 1, by $x = F(K)(1) \in \mathrm{K}_n^{\mathrm{M}}(K)/\ell$. Hence, $F = x \cdot -$. Conversely, this gives an operation.

Now let $m \geq 1$. There is a natural transformation $(\mathrm{K}_1^{\mathrm{M}}(-)/\ell)^{\otimes_{\mathbf{Z}} m} \to \mathrm{K}_m^{\mathrm{M}}(-)/\ell$ induced by the multilinear map $(\mathrm{K}_1^{\mathrm{M}}(-)/\ell)^{\times m} \to \mathrm{K}_m^{\mathrm{M}}(-)/\ell$ given by multiplication. So F lifts to a natural transformation $(\mathrm{K}_1^{\mathrm{M}}(-)/\ell)^{\otimes_{\mathbf{Z}} m} \to \mathrm{K}_n^{\mathrm{M}}(-)/\ell$.

Lemma 2.5. *Let $m \geq 1$, ℓ be prime and K a perfect field of characteristic $\neq \ell$. Every natural transformation $F : (\mathrm{K}_1^{\mathrm{M}}(-)/\ell)^{\otimes_{\mathbf{Z}} m} \to \mathrm{K}_n^{\mathrm{M}}(-)/\ell$ from the category of fields over K to the category of Abelian groups is the linear extension of $x_1 \otimes \cdots \otimes x_m \mapsto x \cdot \prod_{i=1}^m x_m$ mit $x \in \mathrm{K}_{n-m}^{\mathrm{M}}(K)$.*

Proof. We prove the lemma by induction over m. Since tensor products are generated by pure tensors, it suffices to consider the action of F on these. The case $m = 1$ is Theorem 2.3.

Let L be a field extension of K and $y \in (\mathrm{K}_1^{\mathrm{M}}(L)/\ell)^{\otimes_{\mathbf{Z}}(m-1)}$. The natural transformation $F(- \otimes y) : \mathrm{K}_1^{\mathrm{M}}(-)/\ell \to \mathrm{K}_n^{\mathrm{M}}(-)/\ell$ on the category of fields over L is by the case $m = 1$ of the form $F(- \otimes y) = x_{y,L} \cdot -$ with a unique $x_{y,L} \in \mathrm{K}_{n-1}^{\mathrm{M}}(L)/\ell$. The assignment $(y, L) \mapsto x_{y,L}$ (it is an assignment by uniqueness) is a natural transformation $(\mathrm{K}_1^{\mathrm{M}}(-)/\ell)^{\otimes_{\mathbf{Z}}(m-1)} \to \mathrm{K}_{n-1}^{\mathrm{M}}(-)/\ell$ (additivity is clear, and naturality since F is natural) and thus by induction hypothesis of the claimed form. ☐

If $x_i + x_j = 1$ for $1 \leq i < j \leq m$, $x_1 \otimes \cdots \otimes x_m$ is in the kernel of this natural transformation. Hence, it factors through $\mathrm{K}_m^{\mathrm{M}}(-)/\ell$.

Summing up, every cohomology operation of type $(m, n; \ell)$ on the category of fields over K is equal to $x \cdot -$. Conversely, $x \cdot -$ is a cohomology operation. For different x, by Lemma 2.2, one gets different cohomology operations. Hence, the claim follows. ☐

Vial [Via08] also considered non-additive operations on Milnor K-theory mod ℓ, but from his results it is not obvious which operations are additive.

Corollary 2.6. *Let ℓ be prime and K a perfect field of charateristic $\neq \ell$ and let $\mathrm{K}_i^{\mathrm{M}}(K)/\ell = 0$ for $i \gg 0$.*

Then, every natural transformation $\mathrm{K}_*^{\mathrm{M}}(-)/\ell \to \mathrm{K}_*^{\mathrm{M}}(-)/\ell$ of functors from the category of fields over K to the category of graded Abelian groups is of the form $(x_0, x_1, \ldots) \mapsto \sum_{i \geq 0} x_i a_i$ with $x_i \in \mathrm{K}_*^{\mathrm{M}}(K)/\ell$.

Proof. This follows from the universal property of the direct sum and the direct product and Theorem 2.4 since $\mathrm{K}_*^{\mathrm{M}}(K)/\ell = \mathrm{K}_{**}^{\mathrm{M}}(K)/\ell$ because of $\mathrm{K}_i^{\mathrm{M}}(K)/\ell = 0$ for $i \gg 0$. ☐

Corollary 2.7. *Voevodsky's operations Sq^i und P^i from [Voe03] vanish on Milnor K-theory mod ℓ for $\ell \neq p = \operatorname{char} K > 0$ and $i > 1$ or ($i = 1$ and $\ell \nmid (p-1)$).*

Proof. These operations define cohomology operations of type $(*, *+i; \ell)$ over the perfect field $\mathbf{F}_p$ and $\mathrm{K}_i^{\mathrm{M}}(\mathbf{F}_p)/\ell = 0$ for $i > 1$ or ($i = 1$ and $\ell \nmid (p-1)$) by [Mil70], p. 321. ☐

3 The counterexample

The question arises if there is a Grothendieck-Riemann-Roch style formula for the Stiefel-Whitney invariants of a quadratic form:

$$w(\mathrm{Tr}_{L/K}(q)) = \mathrm{cor}(w(q) \cdot c)$$

We answer this question negatively: The counterexample for the Grothendieck-Riemann-Roch formula is as follows: Let K be a p-adic local field with $p > 2$ such that $-1 \neq (K^\times)^2$ and consider $L = K(\sqrt{-1})$. Then all cohomology operations F, G such that

$$w(\mathrm{Tr}_{L/K}(q)) = F\,\mathrm{cor}(G(w(q))) \quad \text{or}$$
$$F(w(\mathrm{Tr}_{L/K}(q))) = \mathrm{cor}(G(w(q))$$

are trivial on H^2 as can be seen by examining all possibilities with a computer program. By Corollary 2.6, these are all of the form $(x_0, x_1, x_2, \ldots) \mapsto \sum a_i x_i$ for $a_i \in \mathrm{K}_*^{\mathrm{M}}(K)/2$.

To this end, we describe $\mathrm{K}_*^{\mathrm{M}}(K)/2$ as follows:

(a) $q \equiv 1 \pmod 4$

$(\cdot,\cdot)_2$	1	π_K	ζ	$\pi_K\zeta$
1	$+1$	$+1$	$+1$	$+1$
π_K	$+1$	$+1$	-1	-1
ζ	$+1$	-1	$+1$	-1
$\pi_K\zeta$	$+1$	-1	-1	$+1$

(b) $q \equiv 3 \pmod 4$

$(\cdot,\cdot)_2$	1	π_K	ζ	$\pi_K\zeta$
1	$+1$	$+1$	$+1$	$+1$
π_K	$+1$	-1	-1	$+1$
ζ	$+1$	-1	$+1$	-1
$\pi_K\zeta$	$+1$	$+1$	-1	-1

Table 1 – The Hilbert symbol $(\cdot,\cdot)_2$ in p-adic local fields with residue field $\mathbf{F}_q$

Theorem 3.1. *Let $p > 2$ be prime, $K/\mathbf{Q}_p$ be a local field with ring of integers $\mathcal{O}_K$ and residue field $\mathbf{F}_q$. Let $\pi_K \in \mathcal{O}_K$ be a uniformiser and $\zeta \in \mu_{q-1} \subset \mathcal{O}_K$ be a primitive $(q-1)$-th root of unity. Then, one has*

$$\begin{aligned}
\mathrm{H}^0(K) &= \mathbf{Z}/2,\\
\mathrm{H}^1(K) &= K^\times/2 = \langle \pi_K \rangle /2 \times \langle \zeta \rangle /2 \cong \mathbf{F}_2^2,\\
\mathrm{H}^2(K) &= \frac{1}{2}\mathbf{Z}/\mathbf{Z} = \mu_2,\\
\mathrm{H}^i(K) &= 0, i > 2.
\end{aligned}$$

The cup product $\mathrm{H}^1(K) \times \mathrm{H}^1(K) \to \mathrm{H}^2(K)$ is given by the Hilbert symbol $(\cdot,\cdot)_2$, see table 1. The cup products in other dimensions are trivial for dimension reasons or $\mathrm{H}^0(K) \times \mathrm{H}^i(K) \to \mathrm{H}^i(K), (x, y) \mapsto x \cdot y$ (x-fold summing of y).

Let L/K be a finite field extension. Then the restriction on H^2 is given by multiplication with $[L : K]$ and the corestriction by identity, the restriction on H^1 is induced by the inclusion and the corestriction is induced by the field norm, finally, the restriction on H^0 the identity and the corestriction multiplication by $[L : K]$.

Proof. The statement on H^0 is clear, and the statement on H^1 follows from [Neu92], p. 142, (5.3) and p. 145 f., (5.7) (i). For the claims on $\mathrm{H}^i(K)$ for $i > 1$ see [NSW00] p. 323, (7.1.8) (ii).

The description of the cup product as a Hilbert symbol can be found in [Koc70], p. 88, Satz 8.12. The table for the Hilbert symbol can be calculated using [Neu92], p. 353, (3.4). As an example, we give the calculation for $(\pi_K, \pi_K)_2$:

$$\begin{aligned}
(\pi_K, \pi_K)_2 &= \omega\left((-1)^{1\cdot 1}\frac{\pi_K^1}{\pi_K^1}\right)^{(q-1)/2}\\
&= \omega(-1)^{(q-1)/2}\\
&= (-1)^{(q-1)/2}\\
&= \begin{cases} +1, & q \equiv 1 \pmod 4\\ -1, & q \equiv 3 \pmod 4, \end{cases}
\end{aligned}$$

where ω is the Teichmüller character (see [Neu92], p. 252).

For the claim regarding restriction and corestriction on H^2 see [NSW00], p. 322, (7.1.4). For H^0 the claims are clear, and for H^1, they follow from the compatibility of δ in the long exact sequence associated to the Kummer sequence with res and cor ([NSW00], p. 46 f., (1.5.2), p. 48, (1.5.4) and (1.5.5)) and because the restriction on H^0 is given by inclusion and the corestriction by the norm:

$$\begin{array}{ccccc}
L^\times & \xrightarrow{\delta} & \mathrm{H}^1(L) & \longrightarrow & \mathrm{H}^1(L, (L^{\mathrm{sep}})^\times) = 0\\
{\scriptstyle \mathrm{cor}=\mathrm{N}_{L/K}}\downarrow & & {\scriptstyle \mathrm{cor}}\downarrow & & \\
K^\times & \xrightarrow{\delta} & \mathrm{H}^1(K) & \longrightarrow & \mathrm{H}^1(K, (K^{\mathrm{sep}})^\times) = 0,
\end{array}$$

and analogously for the restriction. □

4 The multiplicative norm and Stiefel-Whitney invariants

All fields (except our coefficient ring $\mathbf{Z}/2$) are assumed to have characteristic $\neq 2$. First, we partially calculate Evens' multiplicative norm [Eve63] generalising *loc. cit.*, p. 63, Theorem 1. Let us recall briefly the construction of the multiplicative norm $\mathscr{N}\colon \mathrm{H}^{**}(H) \to \mathrm{H}^{**}(G)$ for $H \leq G$ an open subgroup of finite index n of a profinite group G in the case of $\mathbf{Z}/2$-coefficients, which carry the trivial G-action.

Let $\tau_1, \ldots, \tau_n$ be a system of left coset representatives of G/H. The choice of the $(\tau_i)_{i=1}^n$ induces an injection $\Phi : G \hookrightarrow S_n \wr H$ in the wreath product $S_n \wr H = H^n \rtimes S_n$, called the monomial representation.

In the following, all tensor products are taken over $\mathbf{Z}/2$. If $C_\bullet$ is a complex of $\mathbf{Z}/2[H]$-modules, $(C_\bullet)^{\otimes n}$ becomes a complex of $\mathbf{Z}/2[S_n \wr H]$-modules via

$$(\sigma_1 \times \sigma_2 \times \ldots \times \sigma_n)(a_1 \otimes a_2 \otimes \ldots \otimes a_n) = \sigma_1 a_1 \otimes \sigma_2 a_2 \otimes \ldots \otimes \sigma_n a_n, \quad \sigma_i \in H$$
$$\pi(a_1 \otimes a_2 \otimes \ldots \otimes a_n) = a_{\pi^{-1}(1)} \otimes a_{\pi^{-1}(2)} \otimes \ldots \otimes a_{\pi^{-1}(n)}, \quad \pi \in S_n.$$

Pulling back with the monomorphism Φ, $(C_\bullet)^{\otimes n}$ becomes a complex of $\mathbf{Z}/2[G]$-modules. Let $P_\bullet \overset{\varepsilon}{\to} \mathbf{Z}/2 \to 0$ and $R_\bullet \overset{\eta}{\to} \mathbf{Z}/2 \to 0$ be a $\mathbf{Z}/2[H]$-projective, respectively a $\mathbf{Z}/2[S_n]$-projective resolution of $\mathbf{Z}/2$. Then

$$R_\bullet \otimes (P_\bullet)^{\otimes n} \overset{\eta \otimes \varepsilon^{\otimes n}}{\to} \mathbf{Z}/2 \to 0$$

is a $\mathbf{Z}/2[S_n \wr H]$-projective resolution of $\mathbf{Z}/2$. Let $f = (f_i)$, $f_i : P_i \to \mathbf{Z}/2$ be a cocycle representing a cohomology class $\alpha = (\alpha_i) \in \mathrm{H}^{**}(H)$. Then the **multiplicative norm** $\mathscr{N}(\alpha) \in \mathrm{H}^{**}(G)$ is defined as the cohomology class represented by $\Phi^*(1 \wr f^{\otimes n})$, where

$$1 \wr f^{\otimes n} := \eta \otimes f^{\otimes n} \in \mathrm{Hom}_{\mathbf{Z}/2[S_n \wr H]}(R_\bullet \otimes (P_\bullet)^{\otimes n}, \mathbf{Z}/2).$$

One checks that this is well-defined. Note that since our coefficient module $\mathbf{Z}/2$ is a commutative ring of characteristic 2, we do not have to worry about signs.

Theorem 4.1. *Let G be a profinite group with open subgroup H of index $n = [G : H]$. Assume $x \in \mathrm{H}^{**}(H)$ can be written as $x = 1 + x_t + \sum_{j>t} x_j$, with $t > 0$ and $x_j \in \mathrm{H}^j(H)$. Then one has*

$$\mathscr{N}(x) = 1 + \mathrm{cor}_G^H(x_t) + \sum_{k>t} \mathscr{N}_k(x) \quad \text{with } \mathscr{N}_k(x) \in \mathrm{H}^k(G),$$

where in the sum only such k can occur which can be written as a sum with at most n summands of j such that $x_j \neq 0$.

Proof. First assume G finite. Let $P_\bullet \overset{\varepsilon}{\to} \mathbf{Z}/2 \to 0$ and $R_\bullet \overset{\eta}{\to} \mathbf{Z}/2 \to 0$ be as above.

Choose a cocycle $f = (f_i)$, $f_i : P_i \to \mathbf{Z}/2$ representing x. One can assume $f_i = 0$ for those i such that $x_i = 0$. Then, obviously, $1 \wr f^{\otimes n} = \eta \otimes f^{\otimes n}$ is trivial in degrees which cannot be written as a sum with (at most) n summands of j such that $x_j \neq 0$. (It does not matter if we write "at most" or not since $x_0 = 1 \neq 0$.)

One has $\mathscr{N}_t(x) = \mathscr{N}_t(1 + x_t)$, and this is equal to $\mathrm{cor}_G^H(x_t)$ by [CTVE+03], p. 118 f., Theorem 6.3.5 6.

Reduce the general case to this using projective limits. □

Next, we partially calculate the Stiefel-Whitney invariants of quadratic forms from the n-th power of the fundamental ideal $\hat{I}_K \subset \widehat{W}(K)$:

Proposition 4.2. *Let K be a field of characteristic $\neq 2$, $n \geq 1$, $t = 2^{n-1}$ and $q \in \hat{I}_K^n$. Then $w_k(q) \neq 0$ can only occur if $t \mid k$. Further, $w_t(\langle \alpha \rangle \cdot q) = w_t(q)$ for all $\alpha \in K^\times$.*

Proof. According to [Lam05], p. 28, Proposition 1.2, $\hat{I}_K$ is additively generated by forms $\langle a \rangle - \langle 1 \rangle, a \in K^\times$. Therefore, every $q \in \hat{I}_K^n$ is a sum of forms of type $\langle a \rangle q$, where $q = \prod_{i=1}^n (\langle a_i \rangle - \langle 1 \rangle)$. For the Stiefel-Whitney invariants of such a form one has

$$\begin{aligned} w\left(\langle a \rangle \prod_{i=1}^n (\langle a_i \rangle - \langle 1 \rangle)\right) &= w\left((\langle a \rangle - \langle 1 \rangle) \prod_{i=1}^n (\langle a_i \rangle - \langle 1 \rangle) + \prod_{i=1}^n (\langle a_i \rangle - \langle 1 \rangle)\right) \\ &= (1 + \underbrace{\{a, a_1, \ldots, a_n\} \cdot \{-1\}^{2t-n-1}}_{\text{in degree } 2t})^{\pm} (1 + \underbrace{\{a_1, \ldots, a_n\} \cdot \{-1\}^{t-n}}_{\text{in degree } t})^{\mp} \end{aligned}$$

according to [Mil70], p. 329, Lemma 3.2 and the Whitney summation formula. Because of the formula for the geometric series, terms $\neq 0$ can occur only in degrees divisible by t. One has

$$w\left(\langle a\rangle \prod_{i=1}^{n}(\langle a_i\rangle - \langle 1\rangle)\right) = 1 + \underbrace{\{a_1,\ldots,a_n\}\cdot\{-1\}^{t-n}}_{\text{in degree } t} + \ldots,$$

where ... denotes the omission of terms in degrees $> t$. Hence

$$\begin{aligned} w_t\left(\langle a\rangle \prod_{i=1}^{n}(\langle a_i\rangle - \langle 1\rangle)\right) &= \{a_1,\ldots,a_n\}\cdot\{-1\}^{t-n} \\ &= w_t\left(\prod_{i=1}^{n}(\langle a_i\rangle - \langle 1\rangle)\right) \quad \text{by } \textit{loc. cit.}\text{, p. 329, Lemma 3.2.} \end{aligned}$$

Therefore the claim is proven for forms of the type $\langle a\rangle \prod_{i=1}^{n}(\langle a_i\rangle - \langle 1\rangle)$. In the general case, the claim follows for sums $q_1 + \ldots + q_r$ of such forms by the Whitney summation formula: One has

$$w_i(q_1+\ldots+q_r) = \sum_{\substack{i_1+\ldots+i_r=i \\ 0\le i_j}} w_{i_1}(q_1)\cdots w_{i_r}(q_r),$$

and if $t \nmid i$, there is for $i_1 + \ldots + i_r = i$ a j with $t \nmid i_j$, so $w_{i_j}(q_j) = 0$. For $i = t$ one has

$$\begin{aligned} w_t(q_1+\ldots+q_r) &= \sum_{\substack{i_1+\ldots+i_r=t \\ 0\le i_j}} w_{i_1}(q_1)\cdots w_{i_r}(q_r) \\ &= \sum_{j=1}^{r} w_t(q_j), \end{aligned}$$

since for $i_1 + \ldots + i_r = t$, $0 \le i_j$ and $t \nmid i_j$ there is exactly one $i_j = t$ and the others equal 0. Hence

$$\begin{aligned} w_t(\langle\alpha\rangle\cdot(q_1+\ldots+q_r)) &= w_t(\langle\alpha\rangle\cdot q_1 + \ldots + \langle\alpha\rangle\cdot q_r) \\ &= \sum_{j=1}^{r} w_t(\langle\alpha\rangle\cdot q_j) \\ &= \sum_{j=1}^{r} w_t(q_j) \\ &= w_t(\langle\alpha\rangle\cdot(q_1+\ldots+q_r)) \end{aligned}$$

since the Stiefel-Whitney invariants of $\langle\alpha\rangle\cdot q_j$ vanish in degrees not divisible by t if q_j is of the form $\langle\alpha_j\rangle \prod_{i=1}^{n}(\langle a_{ij}\rangle - \langle 1\rangle)$, as we have seen above. □

Combining the above theorem with Kahn's formula [Kah84], p. 224, Théorème 2

$$w(\mathrm{Tr}(q)) = \mathscr{N}(w(q))\cdot w(\mathrm{Tr}(\langle 1\rangle))^{\dim q}$$

yields

Theorem 4.3. *Let $n \ge 1$, $t = 2^{n-1}$. Then one has, for all $q \in \hat{I}_L^n$ and all Scharlau transfers $s : L \to K$,*

$$w_k(s(q)) = \mathrm{cor}(w_k(q))$$

for all k not divisible by t and for $k = t$. Here, both sides are 0 if k is not divisible by t.

Proof. Let $q \in \hat{I}_L^n$. There is a unique $\alpha \in L^\times$ such that $s(x) = \mathrm{Tr}_{L/K}(\alpha \cdot x)$ for all $x \in L$. One has

$$\begin{aligned} w(s(q)) &= w_k(\mathrm{Tr}_{L/K}(\langle\alpha\rangle \cdot q)) \\ &= \mathscr{N}(w(\langle\alpha\rangle \cdot q)) \cdot w(\mathrm{Tr}_{L/K}(\langle 1\rangle))^{\dim\langle\alpha\rangle\cdot q} \\ &= \mathscr{N}(w(\langle\alpha\rangle \cdot q)) \\ &= \mathscr{N}\left(1 + \sum_{i=1}^{\infty} w_{ti}(q)\right) \quad \text{by Proposition 4.2.} \end{aligned}$$

Applying Theorem 4.1 yields the result. □

Remark 4.4. Let L/K be a quadratic extension. If one writes for $1 + x \in \mathrm{H}^{**}(L)$ the multiplicative norm as in in [Kah84], p. 230 f. as

$$\mathscr{N}(1 + x) = 1 + \mathscr{N}_1(x) + \mathscr{N}_2(x)$$

(for quadratic extensions there only occur $\mathscr{N}_i$ with $i \leq 2$ according to [Kah84], p. 230), where $\mathscr{N}_1$ is the corestriction, there is a method for calculating $\mathscr{N}_2(x)$ in low degrees $< 2n_2$:

Write $1 + x = 1 + \sum_{i\geq 1} x_i$ with $x_i \in \mathrm{H}^{n_1}(L)$, $1 = n_1 < n_2 < \ldots$. According to the addition formula [Kah84], p. 231, Proposition I.2.4. a) one has

$$\begin{aligned} \mathscr{N}_2(x) &= \mathscr{N}_2(x_1 + x_2 + \ldots) \\ &= \mathscr{N}_2((1 + x_1) + (1 + x_2 + \ldots)) \\ &= \mathscr{N}_2(1 + x_1) + \mathscr{N}_2(1 + x_2 + \ldots) + \\ &\qquad \mathrm{cor}((1 + x_1) \cdot (1 + x_2 + \ldots)) + \mathrm{cor}((1 + x_1)) \cdot \mathrm{cor}(1 + x_2 + \ldots), \end{aligned}$$

where the sum $\sum_{i>2} x_i$ is denoted by $\ldots$. Therefore, it suffices to calculate $\mathscr{N}_2(1 + x_1)$ and $\mathscr{N}_2(1 + x_2 + \ldots)$.

By the addition formula, one has $\mathscr{N}_2(1 + y) = \mathscr{N}_2(1) + \mathscr{N}_2(y) + \mathrm{cor}(1) \cdot \mathrm{cor}(y) + \mathrm{cor}(1 \cdot y)$, and $\mathscr{N}_2(1)$ can be calculated since $0 = \mathscr{N}(1 + 1) = 1 + \mathrm{cor}(1) + \mathscr{N}_2(1)$. Therefore, one has to determine $\mathscr{N}_2(x_1)$ and $\mathscr{N}_2(x_2 + \ldots)$.

But $\mathscr{N}(1 + x_1) = 1 + \mathrm{cor}(x_1) + \mathscr{N}_2(x_1)$ with $\mathscr{N}_i(x_1) \in \mathrm{H}^{in_1}(K)$ according to [Kah84], p. 230, so it suffices to calculate $\mathscr{N}(1 + x_1)$. If $x_1 = \{a\} \in \mathrm{K}_1^{\mathrm{M}}(L)/2$, then

$$\mathscr{N}(1 + x_1) = w(\mathrm{Tr}_{L/K}(\langle a\rangle)) \cdot (w(\mathrm{Tr}_{L/K}(\langle 1\rangle)))^{-1}$$

and the terms on the right hand side can for quadratic extensions be determined as follows: Write $L = K(\sqrt{c})/K$ and let $\alpha = a + b\sqrt{c} \in L^\times$. Then

$$w(\mathrm{Tr}_{L/K}(\langle\alpha\rangle)) \cong \begin{cases} 1 + \{-1\} + 0, & \text{if } a = 0 \\ 1 + \{c\,\mathrm{N}_{L/K}(\alpha)\} + \{2a, -c\,\mathrm{N}_{L/K}(\alpha)\}, & \text{if } a \neq 0. \end{cases}$$

Analogously, one can write $\mathscr{N}(1 + x_2 + \ldots) = 1 + \mathrm{cor}(x_2 + \ldots) + \mathscr{N}_2(x_2 + \ldots)$ and calculate the left hand side and hence $\mathscr{N}_2(x_2 + \ldots)$ using Theorem 4.1 in the relevant low degrees $< 2n_2$.

Note that Galois field extensions L/K of odd degree n pose no real problem, since for these the restriction $\mathrm{res} : \mathrm{H}^{**}(K) \to \mathrm{H}^{**}(L)$ is injective and by [CTVE$^+$03], p. 118, Theorem 6.3.5 4 one has

$$\mathrm{res} \circ \mathscr{N}(x) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma x.$$

5 Trace forms

Finally, we calculate the trace forms of special field extensions. This is motivated by work of Serre [Ser84]. There are applications to embedding problems [Ser92], p. 99, Corollary 9.2.3 and inverse Galois theory [MM99], p. 312 ff.

Proposition 5.1. *Let L/K be a finite separable field extension with Galois hull $\tilde{L}/K$.*

(i) If $[\tilde{L} : K]$ is odd, $\mathrm{Tr}_{L/K}(\langle 1\rangle) = [L : K]\,\langle 1\rangle$.

(ii) If L/K is Galois, one has $w(\mathrm{Tr}_{L/K}(\langle 1\rangle)) \equiv 1 \mod \ker(\mathrm{res}: \mathrm{K}^{\mathrm{M}}_{**}(K)/2 \to \mathrm{K}^{\mathrm{M}}_{**}(L)/2)$. *If $[\tilde{L}:K]$ is odd, we have* $w(\mathrm{Tr}_{L/K}(\langle 1\rangle)) = 1$.

Proof. (i): We first show the claim for $\tilde{L} = L$. By [Lam05], p. 210 f., Theorem 6.1, one has

$$r^*_{L/K}(\mathrm{Tr}_{L/K}(\langle 1\rangle_L)) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \langle 1\rangle_L^\sigma = [L:K]\,\langle 1\rangle_L = r^*_{L/K}([L:K]\,\langle 1\rangle_K)$$

because of $\langle 1\rangle_L^\sigma = \langle 1^{\sigma^{-1}}\rangle_L = \langle 1\rangle_L$, see [Lam05], p. 210. So by Springer's theorem [Sch84], p. 47, Corollary 5.4, $\mathrm{Tr}_{L/K}(\langle 1\rangle) = [L:K]\,\langle 1\rangle$.

Now let L/K be an arbitrary finite separable field extension with $[\tilde{L}:K]$ odd. Then one has

$$\begin{aligned}
[\tilde{L}:L]\,\langle 1\rangle \cdot [L:K]\,\langle 1\rangle &= [\tilde{L}:K]\,\langle 1\rangle\\
&= \mathrm{Tr}_{\tilde{L}/K}(\langle 1\rangle) \quad \text{as we have just shown}\\
&= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{\tilde{L}/L}(\langle 1\rangle))\\
&= \mathrm{Tr}_{L/K}([\tilde{L}:L]\,\langle 1\rangle)) \quad \text{as we have just shown}\\
&= [\tilde{L}:L]\,\mathrm{Tr}_{L/K}(\langle 1\rangle)), \quad \text{since } \mathrm{Tr}_{L/K} \text{ is a homomorphism.}
\end{aligned}$$

With [Sch84], p. 54, Corollary 6.5, the claim follows since $\dim([\tilde{L}:L]\,\langle 1\rangle) = [\tilde{L}:L]$ is odd.

(ii): The first claim follows from [Sha79], p. 301, Theorem 5.5 and $\mathscr{N}(w(\langle 1\rangle)) = \mathscr{N}(1) = 1$. If L/K is Galois of odd degree, the second claim follows from the first since the restriction is injective by [NSW00], p. 49, (1.5.7). In general, the second claim follows from (i) and $w([L:K]\,\langle 1\rangle) = (1+\{1\})^{[L:K]} = 1$. □

Proposition 5.2. *(i) Let $L/M/K$ be finite separable field extensions such that the Galois hull $\tilde{L}/M$ of L/M is of odd degree. Then one has* $\mathrm{Tr}_{L/K}(\langle 1\rangle) = [L:M]\,\mathrm{Tr}_{M/K}(\langle 1\rangle)$.

(ii) Let $L/M/K$ be finite separable field extensions with $\mathrm{Tr}_{L/M}(\langle 1\rangle) = \frac{[L:M]}{2}\,\langle 1,-1\rangle$ *totally hyperbolic. Then* $\mathrm{Tr}_{L/K}(\langle 1\rangle) = \frac{[L:K]}{2}\,\langle 1,-1\rangle$ *is totally hyperbolic.*

Proof. (i): One has

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\langle 1\rangle) &= \mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(\langle 1\rangle))\\
&= \mathrm{Tr}_{M/K}([L:M]\,\langle 1\rangle)) \quad \text{by Proposition 5.1 (i)}\\
&= [L:M]\,\mathrm{Tr}_{M/K}(\langle 1\rangle)), \quad \text{since } \mathrm{Tr}_{M/K} \text{ is a homomorphism.}
\end{aligned}$$

(ii) follows from the injectivity of the trace and [Lam05], p. 190, Corollary 1.4. □

Proposition 5.3. *Let $L/K, L'/K$ be finite separable field extensions contained in a common field (so the compositum LL' is defined) and $\tilde{L}/K$ the Galois hull of L/K. Assume $\tilde{L}\cap L' = K$.*

(i) One has $\mathrm{Tr}_{LL'/L'}(\langle 1\rangle_{LL'}) = r^*_{L'/K}(\mathrm{Tr}_{L/K}(\langle 1\rangle_L))$.

(ii) One has $\mathrm{Tr}_{LL'/K}(\langle 1\rangle_{LL'}) = \mathrm{Tr}_{L/K}(\langle 1\rangle_L)\cdot \mathrm{Tr}_{L'/K}(\langle 1\rangle_{L'})$.

Proof. Because of $\tilde{L}\cap L' = K$, one has an isomorphism $LL' \cong L\otimes_K L'$ of L'-algebras, so the characteristic polynomial of $x^i\cdot -$ as a K-endomorphism of L equals the characteristic polynomial of $x^i\cdot -$ as an L'-endomorphism of LL' since the latter map is the base change by L' of the former map. In particular, $\mathrm{Tr}_{L/K}(x^ix^j) = \mathrm{Tr}_{LL'/L'}(x^ix^j)$, and one gets (i), since the x^i are a K-basis of L resp. a L'-basis of LL' for $0 \le i < \deg(f)$.

Applying the projection formula [Sch84], p. 48, Theorem 5.6 to (i), one gets by the transitivity of the trace

$$\begin{aligned}
\mathrm{Tr}_{LL'/K}(\langle 1\rangle_{LL'}) &= \mathrm{Tr}_{L'/K}(\mathrm{Tr}_{LL'/L'}(\langle 1\rangle_{LL'})) \quad \text{because of the transitivity}\\
&= \mathrm{Tr}_{L'/K}(r^*_{L'/K}(\mathrm{Tr}_{L/K}(\langle 1\rangle_L))\cdot\langle 1\rangle_{L'}) \quad \text{by (i)}\\
&= \mathrm{Tr}_{L/K}(\langle 1\rangle_L)\cdot \mathrm{Tr}_{L'/K}(\langle 1\rangle_{L'}) \quad \text{by the projection formula,}
\end{aligned}$$

hence (ii). □

Lemma 5.4. *Let (V,q) be a regular quadratic form over a field K, $W \subset V$ a totally isotropic K-subspace and $U \subset V$ a K-subspace with $W^\perp = W \oplus U$. Then there is a K-subspace W' of V with $\dim_K(W) = \dim_K(W')$, $W \oplus W'$ totally hyperbolic and $(W \oplus W') \perp U$.*

Proof. Let $e_1, \ldots, e_m$ be a K-basis of W. If $\dim_K(W) = 0$, one can take $W' = \{0\}$. So assume $m \geq 1$.

We inductively construct vectors $e'_1, \ldots, e'_m$ with $B_q(e_i, e'_j) = \delta_{ij}$ and $B_q(e'_i, U) = \{0\}$. Then $W' = \langle\{e'_1, \ldots, e'_m\}\rangle$ works: One has $W \cap W' = \{0\}$ because since W is totally isotropic, one has $W \cap W' \subset W^\perp \cap W' = \{0\}$, as just shown. The e'_i are linearly independent since if $v = \sum \lambda_i e'_i = 0$, one has $0 = B_q(e_i, v) = \lambda_i$ for all i. Thus $W \oplus W'$ is totally hyperbolic by [Sch84], p. 12 f., Theorem 4.5 (with respect to the basis $e_1, \ldots, e_m, e'_1, \ldots, e'_m$ with $C = I_n$ because of $B_q(e_i, e'_j) = \delta_{ij}$ and the upper left square equal to 0 since W is totally isotropic; here, $W \oplus W'$ is regular by [Sch84], p. 7, Corollary 3.2 and [Lam05], p. 4, Proposition 1.2 since the matrix of B_q equals

$$\begin{pmatrix} 0 & I_n \\ I_n & * \end{pmatrix}$$

and is hence invertible). Further, one has $B_q(W \oplus W', U) \subset B_q(W, U) + B_q(W', U) = \{0\} + \{0\} = \{0\}$ since $U \subset W^\perp$ and $B_q(W', U)$ by construction of the e'_i. One has $(W \oplus W') \cap U = \{0\}$: For $v = \sum \lambda_i e_i + \sum \lambda'_i e'_i \in (W \oplus W') \cap U$, one has $0 = B_q(e_i, v) = \lambda'_i$ for all i because of $v \in U \subset W^\perp$ and since $B_q(e_i, e_j) = 0$ because of W totally isotropic and $B_q(e_i, e'_j) = \delta_{ij}$. Hence, $v = \sum \lambda_i e_i$. Thus, $0 = B_q(e'_i, v) = \lambda_i$ for all i because of $B_q(W', U) = \{0\}$ and $B_q(e'_i, e_j) = \delta_{ij}$, so $v = 0$. Summing up, one has $(W \oplus W') \perp U$.

Now for the construction of the e'_i.

Assume $U^\perp \subset \langle\{e_1\}\rangle^\perp$. Applying the inclusion-reversing $(-)^\perp$, it follows from [Sch84], p. 9, Lemma 3.11 and Corollary 3.12 that $\langle\{e_1\}\rangle \subset U$, a contradiction. Hence, there is $e'_1 \in U^\perp \setminus \langle\{e_1\}\rangle^\perp$. After division of e'_1 by $B_q(e_1, e'_1) \neq 0$ (since $e'_1 \notin \langle\{e_1\}\rangle^\perp$), one can assume $B_q(e_1, e'_1) = 1$. One has $B_q(e'_1, U) = \{0\}$ because of $e'_1 \in U^\perp$.

Assume that for $1 \leq i < i_0 \leq m$, the e'_i are already constructed. Let $U_{i_0} = \langle\{e_j : j < i_0\}\rangle \oplus U$. Assume $U_{i_0}^\perp \subset \langle\{e_{i_0}\}\rangle^\perp$. Applying the inclusion-reversing $(-)^\perp$, it follows from [Sch84], p. 9, Lemma 3.11 and Corollary 3.12 that $\langle\{e_{i_0}\}\rangle \subset U_{i_0}$, a contradiction. Hence, there is $e'_{i_0} \in U_{i_0}^\perp \setminus \langle\{e_{i_0}\}\rangle^\perp$. After division of e'_{i_0} by $B_q(e_{i_0}, e'_{i_0}) \neq 0$ (since $e'_{i_0} \notin \langle\{e_{i_0}\}\rangle^\perp$), one can assume $B_q(e_{i_0}, e'_{i_0}) = 1$. Further, one has $B_q(e_j, e'_{i_0}) = 0$ for $1 \leq j < i_0$ because of $e'_{i_0} \in U_{i_0}^\perp \subset \langle\{e_j : j < i_0\}\rangle^\perp$ and $B_q(e'_{i_0}, U) = \{0\}$ because of $e'_{i_0} \in U_{i_0}^\perp \subset U^\perp$. □

Lemma 5.5. *Let $k \geq 1$ and K a field with $\operatorname{char} K \nmid k$. Let*

$$f(X) = \alpha \prod_{i=1}^{m} (X - \alpha_i) \in K[X],$$
$$g(X) = \beta \prod_{i=1}^{n} (X - \beta_i) \in K[X]$$

be two polynomials. Then

$$\operatorname{res}(f(X^k), g(X^k)) = (-1)^{(k+1)mn} \operatorname{res}(f(X), g(X))^k.$$

Proof. We calculate in the algebraic closure of K. Let ζ be a primitive k-th root of unity ($\operatorname{char} K \nmid k$) and $\alpha_i^{\frac{1}{k}}, \beta_j^{\frac{1}{k}}$ fixed k-th roots of α_i, β_j. The factorisation of $f(X^k)$ in $\bar{K}$ is

$$f(X^k) = \alpha \prod_{i=1}^{m} \prod_{a=1}^{k} (X - \zeta^a \alpha_i^{\frac{1}{k}})$$

and analogously for $g(X^k)$. Hence, by [Bos03], S. 177, Korollar 9

$$\begin{aligned}
\operatorname{res}(g(X^k), h(X^k)) &= \alpha^{kn}\beta^{km}\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{a,b=1}^{k}(\zeta^a\alpha_i^{\frac{1}{k}} - \zeta^b\beta_j^{\frac{1}{k}}) \\
&= \alpha^{kn}\beta^{km}\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{a,b=1}^{k}\zeta^a(\alpha_i^{\frac{1}{k}} - \zeta^{b-a}\beta_j^{\frac{1}{k}}) \\
&= \alpha^{kn}\beta^{km}\prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{a=1}^{k}\zeta^a(\alpha_i - \beta_j) \\
&= (\alpha^n\beta^m)^k\prod_{i=1}^{m}\prod_{j=1}^{n}\zeta^{\frac{k(k+1)}{2}}(\alpha_i - \beta_j)^k \\
&= \zeta^{\frac{k(k+1)}{2}mn}\operatorname{res}(g,h)^k,
\end{aligned}$$

If k is odd, one has $\zeta^{\frac{k(k+1)}{2}} = (\zeta^k)^{\frac{k+1}{2}} = 1$, and if k is even, one has $\zeta^{\frac{k(k+1)}{2}} = (\zeta^{\frac{k}{2}})^{k+1} = (-1)^{k+1}$. Hence, the sign equals $(-1)^{(k+1)mn}$. □

Lemma 5.6. *Let $k \geq 1$ and K be a field. Let $f(X) = X^n + \sum_{i=0}^{n-1} a_iX^i$ be a polynomial. Then the discriminant of $f(X^k)$ equals*

$$(-1)^{\frac{kn(kn-1)}{2}}\left(\operatorname{res}(f,f')\right)^k k^{kn}a_0^{k-1}.$$

Proof. If $\operatorname{char} K \mid k$, one has $(f(X^k))' = kX^{k-1}f'(X^k) = 0$ and hence its discriminant equals 0 by [Bos03], p. 173. So one can assume $\operatorname{char} K \nmid k$.

By [Bos03], S. 177, Korollar 10, one has $\operatorname{disc}(f(X^k)) = (-1)^{\frac{kn(kn-1)}{2}}\operatorname{res}(f(X^k),(f(X^k))')$.

We calculate in the algebraic closure of K. By [Bos03], S. 177, Korollar 9, one has

$$\begin{aligned}
\operatorname{res}(f(X^k), k) &= k^{kn}, \\
\operatorname{res}(f(X^k), X^{k-1}) &= \prod_{f(\alpha)=0}\prod_{i=1}^{k}\left(\zeta^i\alpha^{\frac{1}{k}}\right)^{k-1} \\
&= \left(\prod_{f(\alpha)=0}\zeta^{\frac{k(k+1)}{2}}\alpha\right)^{k-1} \\
&= \left((-1)^{n(k+1)}\prod_{f(\alpha)=0}\alpha\right)^{k-1} \qquad \text{because of } \zeta^{\frac{k(k+1)}{2}} = (-1)^{k+1} \\
&= (-1)^{n(k+1)(k-1)}\left((-1)^n a_0\right)^{k-1} \\
&= (-1)^{n(k-1)}\cdot(-1)^{n(k-1)}\cdot a_0^{k-1} \quad \text{because of } k^2-1 \equiv k-1 \pmod 2 \\
&= a_0^{k-1},
\end{aligned}$$

where ζ is a primitive k-th root of unity ($\operatorname{char} K \nmid k$) and $\alpha^{\frac{1}{k}}$ is a fixed k-th root of α. The equality $\zeta^{\frac{k(k+1)}{2}} = (-1)^{k+1}$ is known from the proof of Lemma 5.5.

Hence,

$$\begin{aligned}
\operatorname{res}(f(X^k),(f(X^k))') &= \operatorname{res}(f(X^k), kX^{k-1}f'(X^k)) \\
&= \operatorname{res}(f(X^k),k)\operatorname{res}(f(X^k),X^{k-1})\operatorname{res}(f(X^k),f'(X^k)) \\
&= k^{kn}a_0^{k-1}(-1)^{(k+1)n(n-1)}\left(\operatorname{res}(f,f')\right)^k \quad \text{by Lemma 5.5} \\
&= k^{kn}a_0^{k-1}\left(\operatorname{res}(f,f')\right)^k \quad \text{because of } n(n-1) \equiv 0 \pmod 2
\end{aligned}$$

because of $\operatorname{res}(f,g_1g_2) = \operatorname{res}(f,g_1)\operatorname{res}(f,g_2)$ (cf. [Bos03], S. 177, proof of Korollar 9).

Summing up, the claim follows. □

Corollary 5.7. *Let $k \geq 1$ and K be a field. Let $n > 1$. Then the discriminant of $X^{kn} + a_k X^k + a_0 \in K[X]$ equals*

$$(-1)^{\frac{kn(kn-1)}{2}} \left[(1-n)^{n-1} a_k^n + n^n a_0^{n-1}\right]^k a_0^{k-1} k^{kn}.$$

Proof. For $k = 1$ see [Bos03], S. 181, Aufgabe 3 (ii). For the general case, set $f(X) = X^n + a_k X + a_0$ and apply Lemma 5.6. □

Theorem 5.8. *Let $L = K(a)/K$ be a finite separable field extension of degree $n > 1$ with minimal polynomial $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in K[X]$ of a over K. Then the bilinear form associated to the trace form $\mathrm{Tr}_{L/K}(\langle 1 \rangle)$ with respect to the basis $1, a, a^2, \ldots, a^{n-1}$ is given by the matrix $(a_{ij})_{i,j=0}^{n-1}$ with $a_{ij} = t_{i+j} = \mathrm{Tr}_{L/K}(a^{i+j})$, where the t_i are recursively determined by*

$$\begin{aligned} t_0 &= n, \\ t_i &= -\left(i a_{n-i} + \sum_{j=1}^{i-1} a_{n-i+j} t_j\right), \quad i > 0. \end{aligned}$$

Here $a_n = 1$ and $a_i = 0$ for $i < 0$. For $i > n$, the formula simplifies to

$$t_i = -\sum_{j=i-n}^{i-1} a_{n-i+j} t_j.$$

Proof. One has

$$\left(\sum_{i=0}^{n-1} x_i a^i\right)^2 = \sum_{i=0}^{n-1} x_i^2 a^{2i} + 2 \sum_{0 \leq i < j \leq n-1} x_i x_j a^{i+j}$$

for $x_i \in K$. Applying $\mathrm{Tr}_{L/K}$, one gets

$$\mathrm{Tr}_{L/K}(\langle 1 \rangle)(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i^2 \,\mathrm{Tr}_{L/K}(a^{2i}) + 2 \sum_{0 \leq i < j \leq n-1} x_i x_j \,\mathrm{Tr}_{L/K}(a^{i+j}). \tag{5.1}$$

We show $\mathrm{Tr}_{L/K}(a^i) = t_i$.

Let A be the matrix of the K-endomorphism $L \to L, x \mapsto ax$ with respect to the basis $1, a, a^2, \ldots, a^{n-1}$. Then $\mathrm{Tr}_{L/K}(a^i) = \mathrm{Tr}(A^i)$. Because of $f(A) = 0$, one has

$$\begin{aligned} (X - A) \sum_{i=0}^{n-1} \left(\sum_{j=i}^{n-1} a_{j+1} A^{j-i}\right) X^i &= \sum_{i=1}^{n} \left(\sum_{j=i-1}^{n-1} a_{j+1} A^{j-i+1}\right) X^i - \sum_{i=0}^{n-1} \left(\sum_{j=i}^{n-1} a_{j+1} A^{j-i+1}\right) X^i \\ &= X^n - \sum_{j=0}^{n-1} a_{j+1} A^{j+1} + \sum_{i=1}^{n-1} a_i X^i \\ &= (f(X) - a_0) - (f(A) - a_0) \\ &= f(X). \end{aligned}$$

Applying for $x \in \bar{K} \setminus \sigma(A)$ ($\sigma(A)$ the set of eigenvalues of A in $\bar{K}$) the homomorphism $\mathrm{M}_n(K[X]) \to \mathrm{M}_n(\bar{K}), X \mapsto x I_n = x$ and multiplying with $(x - A)^{-1}$ (x is no eigenvector of A) and taking the trace, yields

$$\sum_{i=0}^{n-1} \left(\sum_{j=i}^{n-1} a_{j+1} \,\mathrm{Tr}(A^{j-i})\right) x^i = \mathrm{Tr}((x - A)^{-1} f(x)). \tag{5.2}$$

Let $T \in \mathrm{GL}_n(\bar{K})$ with TAT^{-1} an upper triangular matrix with diagonal entries x_i, where $f(x) = \prod_{i=1}^n (x - x_i)$. Then

$$\begin{aligned} \mathrm{Tr}((x-A)^{-1}f(x)) &= \mathrm{Tr}((x-A)^{-1})f(x) \\ &= \mathrm{Tr}(T(x-A)^{-1}T^{-1})f(x) \\ &= \mathrm{Tr}((x-TAT^{-1})^{-1})f(x) \\ &= f(x)\sum_{i=1}^n (x-x_i)^{-1}. \end{aligned}$$

But

$$\begin{aligned} f(x)\sum_{i=1}^n (x-x_i)^{-1} &= \left(\prod_{j=1}^n (x-x_i)\right)\left(\sum_{i=1}^n (x-x_i)^{-1}\right) \\ &= \sum_{i=1}^n \prod_{j\neq i} (x-x_j) \\ &= f'(x). \end{aligned}$$

Plugging into (5.2), one gets

$$\sum_{i=0}^{n-1}\left(\sum_{j=i}^{n-1} a_{j+1}\,\mathrm{Tr}(A^{j-i})\right)x^i = f'(x) = \sum_{i=0}^{n-1}(i+1)a_{i+1}x^i$$

for infinitely many $x \in \bar{K}$. One gets a polynimial with infinitely many zeroes, hence this equals 0, and comparing coefficients, one gets

$$\sum_{j=i}^{n-1} a_{j+1}\,\mathrm{Tr}(A^{j-i}) = (i+1)a_{i+1}$$

for all $0 \leq i \leq n-1$, which yields after an index shift

$$\sum_{j=1}^{n-i} a_{j+i}\,\mathrm{Tr}(A^{j-1}) = (i+1)a_{i+1} \tag{5.3}$$

for all $0 \leq i \leq n-1$.

For $i = n-1$, one gets from (5.3)

$$\mathrm{Tr}(A^0) = a_n\,\mathrm{Tr}(A^0) = na_n = n = t_0.$$

Hence (5.3) simplifies to

$$na_{i+1} + \sum_{j=2}^{n-i} a_{j+i}\,\mathrm{Tr}(A^{j-1}) = (i+1)a_{i+1},$$

so after subtraction of na_{i+1} and index shift

$$\mathrm{Tr}(A^{n-i}) + \sum_{j=1}^{n-i-1} a_{j+i}\,\mathrm{Tr}(A^j) = -(n-i)a_i \tag{5.4}$$

for all $1 \leq i \leq n$.

Now $\mathrm{Tr}_{L/K}(a^i) = t_i$ for $i \leq n$ follows from induction: For $i = n-2$, one gets from (5.4) $a_{n-1}\,\mathrm{Tr}(A^0) + a_n\,\mathrm{Tr}(A^1) = (n-1)a_{n-1}$, so

$$t_1 = -a_{n-1} = ((n-1)-n)a_{n-1} = (n-1)a_{n-1} - a_{n-1}\,\mathrm{Tr}(A^0) = a_n\,\mathrm{Tr}(A^1) = \mathrm{Tr}(A^1).$$

Assume $\mathrm{Tr}_{L/K}(a^i) = t_i$ is shown for $1 \le i < i_0 \le n$. Then

$$\begin{aligned} t_{i_0} &= -\left(i_0 a_{n-i_0} + \sum_{j=1}^{i_0-1} a_{n-i_0+j} t_j \right) \\ &\overset{\text{Vor.}}{=} -\left(i_0 a_{n-i_0} + \sum_{j=1}^{i_0-1} a_{n-i_0+j} \mathrm{Tr}(A^j)) \right) \\ &\overset{(5.4)}{=} -\big(i_0 a_{n-i_0} - \mathrm{Tr}(A^{i_0}) - i_0 a_{n-i_0} \big) \\ &= \mathrm{Tr}(A^{i_0}) \end{aligned}$$

using (5.4) with $0 \le i = n - i_0 < n - 1$.

Assume $\mathrm{Tr}_{L/K}(a^i) = t_i$ to be shown for all $i < i_0$ and $i_0 > n$. Then

$$\begin{aligned} 0 &= f(A)A^{n-i_0} \\ &= \sum_{j=0}^{n} a_j A^{n-i_0+j} \\ &= \sum_{j=i_0-n}^{i_0} a_{n-i_0+j} A^j \\ &= \sum_{j=i_0-n}^{i_0-1} a_{n-i_0+j} A^j + A^{i_0} \end{aligned}$$

and taking the trace and using the induction hypothesis yields $\mathrm{Tr}_{L/K}(a^{i_0}) = t_{i_0}$. □

Theorem 5.9. *Let $L = K(a)/K$ be a finite separable field extension of degree $kn > 1$ with minimal polynomial $f(X) = X^{kn} + a_k X^k + a_0 \in K[X]$ of a over K. Let*

$$c(f) = (1-n)^{n-1} a_k^n + n^n a_0^{n-1}.$$

Note that $\mathrm{disc}(f) = (-1)^{\frac{kn(kn-1)}{2}} c(f)^k a_0^{k-1} k^{kn}$.

(1) Let $n = 2, k = 1$ and $\mathrm{char}\, K \ne 2$. Then one has

$$\begin{aligned} \mathrm{Tr}_{L/K}(\langle 1 \rangle) &= \big\langle 2, 2(a_1^2 - 4a_0) \big\rangle = \langle 2, 2\,\mathrm{disc}(f) \rangle \quad \text{and} \\ w(\mathrm{Tr}_{L/K}(\langle 1 \rangle)) &= 1 + \{\mathrm{disc}(f)\} + \{2, -\mathrm{disc}(f)\}. \end{aligned}$$

(2) Let $n > 2, k = 1$. Let $\mathrm{char}\, K \nmid n$. If $a_1 = 0$ and $n > 2$, then

$$\mathrm{Tr}_{L/K}(\langle 1 \rangle) = \begin{cases} \langle n \rangle + \frac{n-1}{2} \langle 1, -1 \rangle, & n \text{ odd} \\ \langle n, -na_0 \rangle + \frac{n-2}{2} \langle 1, -1 \rangle, & n \text{ even.} \end{cases}$$

(3) Let $k = 1$, $a_k \ne 0$ and $n > 2$. Let $\mathrm{char}\, K \nmid n(n-1)$ and $a_1 \ne 0$ if n is odd. Then one has

$$\mathrm{Tr}_{L/K}(\langle 1 \rangle) = \begin{cases} \Big\langle n, (1-n)a_1, n(1-n)a_1(-1)^{\frac{n-3}{2}} \mathrm{disc}(f) \Big\rangle + \frac{n-3}{2} \langle 1, -1 \rangle, & n \text{ odd} \\ \Big\langle n, (-1)^{\frac{n-2}{2}} n\, \mathrm{disc}(f) \Big\rangle + \frac{n-2}{2} \langle 1, -1 \rangle, & n \text{ even.} \end{cases}$$

(4) Let $n = 2, k > 1$ and $a_k \ne 0$. Let $\mathrm{char}\, K \nmid 2k$. Then one has

$$\mathrm{Tr}_{L/K}(\langle 1 \rangle) = \begin{cases} \langle 2k, -2kc(f), -ka_k, ka_k a_0 c(f) \rangle + (k-2) \langle 1, -1 \rangle, & k \text{ even} \\ \langle 2k, -2kc(f) \rangle + (k-1) \langle 1, -1 \rangle, & k \text{ odd.} \end{cases}$$

(5) Let $n > 2, k > 1$ and $a_k \ne 0$. Let $\mathrm{char}\, K \nmid kn(n-1)$. Then one has $\mathrm{Tr}_{L/K}(\langle 1 \rangle) =$

$$\begin{cases} \langle kn, k(1-n)a_k, -a_0 kc(f), -n(1-n)a_k kc(f) \rangle + \big(\frac{k}{2}n - 2\big) \langle 1, -1 \rangle, & k \text{ even, } n \text{ odd} \\ \langle kn, k(1-n)a_k, -ka_0 a_k, -kn(1-n) \rangle + \big(\frac{k}{2}n - 2\big) \langle 1, -1 \rangle, & k \text{ even, } n \text{ even} \\ \langle kn, -c(f)kn \rangle + \frac{kn-2}{2} \langle 1, -1 \rangle, & k \text{ odd, } n \text{ even} \\ \langle kn, k(1-n)a_k, -c(f)kn(1-n)a_k \rangle + (\frac{kn-3}{2}) \langle 1, -1 \rangle, & k \text{ odd, } n \text{ odd.} \end{cases}$$

Proof. Denote the associated bilinear form to the trace form $\mathrm{Tr}_{L/K}(\langle 1\rangle)$ with respect to the basis $1, a, a^2, \ldots, a^{n-1}$ by the matrix $(a_{ij})_{i,j=0}^{n-1}$ with $a_{ij} = t_{i+j} = \mathrm{Tr}_{L/K}(a^{i+j})$. One first calculates from Theorem 5.8:

(i) Let $n = 2, k = 1$. Then one has

$$\begin{aligned} t_0 &= kn = 2,\\ t_1 &= -k(n-1)a_k = -a_1,\\ t_2 &= k(-2a_0 + a_k^2) = a_1^2 - 2a_0. \end{aligned}$$

(ii) Let $n = 2, k > 1$. Then one has

$$\begin{aligned} t_0 &= kn = 2k,\\ t_k &= t_{k(n-1)} = -k(n-1)a_k = -ka_k,\\ t_{2k} &= t_{kn} = k(a_k^2 - 2a_0),\\ t_{3k} &= t_{k(2n-1)} = ka_k((n+1)a_0 - a_k^2) = ka_k(3a_0 - a_k^2). \end{aligned}$$

(iii) Let $n > 2, k = 1$. Then one has

$$\begin{aligned} t_0 &= kn = n,\\ t_{n-1} &= t_{k(n-1)} = k(1-n)a_k = (1-n)a_1,\\ t_n &= t_{kn} = -kna_0 = -na_0,\\ t_{2(n-1)} &= t_{2(kn-1)} = k(n-1)a_k^2 = (n-1)a_1^2. \end{aligned}$$

(iv) Let $n > 2$ and $k \geq 2$. Then one has

$$\begin{aligned} t_0 &= kn,\\ t_{k(n-1)} &= k(1-n)a_k,\\ t_{kn} &= -kna_0,\\ t_{k(2n-2)} &= k(n-1)a_k^2,\\ t_{k(2n-1)} &= k(2n-1)a_0a_k. \end{aligned}$$

Then one diagonalises the symmetric matrix $(a_{ij})_{i,j=0}^{n-1}$:

By example, we show (5) since this is the most complicated case. We distinguish the cases k even and k odd. By example, we show the case k even. We distinguish the cases n odd resp. even. We show by example the case n odd.

Let $W \subset L$ the K-subspace spanned by $a^1, \ldots, a^{\frac{k}{2}(n-1)-1}$. Because of $0 < 2 \cdot 1 \leq 2(\frac{k}{2}(n-1)-1) < k(n-1)$ and $t_i = 0$ for $0 < i < k(n-1)$ by the calculation from (iv), one has $B_q(a^i, a^j) = \mathrm{Tr}(a^{i+j}) = t_{i+j} = 0$ for $1 \leq i, j \leq \frac{k}{2}(n-1) - 1$, so $B_q(W, W) = \{0\}$. Let $U = \langle\{1, a^{\frac{k}{2}(n-1)}, v_1, \ldots, v_k\}\rangle$ with

$$\begin{aligned} \lambda &= -\frac{\mathrm{Tr}(a^{kn})}{\mathrm{Tr}(a^{k(n-1)})} = \frac{na_0}{(1-n)a_k},\\ v_j &= \sum_{i=0}^{i_{\max}(j,k,n)} \lambda^i a^{k(n-i)-j}, j = 1, \ldots, k. \end{aligned}$$

Here, let $i_{\max}(j, k, n)$ be the maximal $i \geq 0$ with $k(n-i) - j \geq \frac{k}{2}(n-1) + 1$. One has

$$i_{\max}(j,k,n) = \left\lfloor \frac{n+1}{2} - \frac{j+1}{k} \right\rfloor.$$

Now assume n odd. Then, $\frac{n+1}{2} \in \mathbf{N}$ and hence

$$i_{\max}(j,k,n) = \frac{n+1}{2} - \left\lceil \frac{j+1}{k} \right\rceil.$$

Thus, $i_{\max}(j,k,n) = \frac{n-1}{2}$ for $1 \le j \le k-1$ and $i_{\max}(j,k,n) = \frac{n-3}{2}$ for $j = k$, and hence $k(n - i_{\max}(j,k,n)) - j = k \cdot \frac{n+1}{2} - j$ for $1 \le j \le k-1$ and $k(n - i_{\max}(j,k,n)) - j = k \cdot \frac{n+1}{2}$ for $j = k$.

Because of $0 < 1 \le \frac{k}{2}(n-1)-1 < k(n-1)$ and $0 < 1+\frac{k}{2}(n-1) \le \frac{k}{2}(n-1)-1+\frac{k}{2}(n-1) = k(n-1)-1 < k(n-1)$, one has with (iv) $\langle\{1, a^{\frac{k}{2}(n-1)}\}\rangle \subset W^\perp$. Let ($j = 1, \dots, k$, $m = 1, \dots, \frac{k}{2}(n-1)-1$) or ($m = 0, \frac{k}{2}(n-1)$ and $1 \le j \le \frac{k}{2}$).One has

$$\operatorname{Tr}(a^m v_j) = \sum_{i=0}^{i_{\max}(j,k,n)} \lambda^i \operatorname{Tr}(a^{k(n-i)-j+m}). \tag{5.5}$$

We want to show that this always equals 0. If $-j+m = kr$ (note that $r \ge 0$ because of $-j+m \ge -k+1 > -k$ bzw. $-j+m \ge -\frac{k}{2}+0 > -k$) the sum from (5.5) equals

$$\begin{aligned}&\lambda^r(\operatorname{Tr}(a^{kn}) + \lambda \operatorname{Tr}(a^{k(n-1)})) = \\ &\lambda^r\left(\operatorname{Tr}(a^{kn}) - \frac{\operatorname{Tr}(a^{kn})}{\operatorname{Tr}(a^{k(n-1)})} \cdot \operatorname{Tr}(a^{k(n-1)})\right) = \\ &\lambda^r \cdot 0 = 0,\end{aligned}$$

since in the sum (5.5), the exponent of a is at least equal to $k(n - \frac{n-1}{2}) - j + m = \frac{k}{2}(n+1) - j + m > \frac{k}{2}(n+1) - k = \frac{k}{2}(n-1) > 0$ and at most equal to $kn - 1 + \frac{k}{2}(n-1) = \frac{3}{2}kn - \frac{k}{2} - 1 = \frac{k}{2}(3n-1) - 1 < k(2n-2)$ as the latter inequality is equivalent to $-1 < \frac{k}{2}(n-3)$, which is satisfied for $n \ge 3$. So by (iv), only terms with $\operatorname{Tr}(a^{k(n-1)})$ and $\operatorname{Tr}(a^{kn})$ can be $\neq 0$. Both indeed occur since $i_{\max}(j,k,n) = \frac{n-1}{2} > 0$ for $1 \le j \le k-1$, and for $j = k$ one has $i_{\max}(j,k,n) = \frac{n-3}{2} > 0$ for $n > 3$. In the case $n = 3, j = k$ one has $1 \le m \le k-1$ and hence $k+1 \le -j+m \le k+(k-1) = 2k-1$, so $-j+m = kr$ cannot occur.

In the case $-j+m \not\equiv 0 \pmod k$, in the sum (5.5) only terms $\operatorname{Tr}(a^s)$ with $k \nmid s$ occur, so by (iv) all terms equal 0.

Summing up, one gets $U \subset W^\perp$.

The generators of U from above are linearly independent since the exponents of a in the sums for the v_j lie by definition of $i_{\max}(j,k,n)$ between $kn-1$ and $\frac{k}{2}(n-1)+1$ and for different $1 \le j \le k$ the exponents of a in the sum are all distinct since they are $\equiv -j \pmod k$ and the a^i for $0 \le i \le kn-1$ are a K-basis of L.

The sum $W + U$ is direct, and because of $\frac{k}{2}(n-1) - 1 + \dim_K(W^\perp) = \dim_K(W) + \dim_K(W^\perp) = kn$ ([Sch84], p. 9, Lemma 3.11 and Corollary 3.12) one has $\dim_K(W^\perp) = kn - (\frac{k}{2}(n-1)-1) = \frac{k}{2}(n+1)+1$. But since W is totally isotropic, one has $W \subset W^\perp$ und damit $W \oplus U \subset W^\perp$ with $\dim_K(W \oplus U) = (\frac{k}{2}(n-1)-1) + (k+2) = \frac{k}{2}(n+1)+1 = \dim_K(W^\perp)$, hence $W \oplus U = W^\perp$.

Let $W' \subset L$ as in Lemma 5.4. ($\operatorname{Tr}(\langle 1\rangle)$ is regular.) Then one has $\dim_K((W \oplus W') \perp U) = 2 \cdot (\frac{k}{2}(n-1)-1) + (k+2) = kn$, so $L = (W \oplus W') \perp U$. Hence $\operatorname{Tr}(\langle 1\rangle)$ equals $(\frac{k}{2}(n-1)-1) \cdot \langle 1, -1\rangle$ plus the trace form restricted to U. Now we diagonalise the latter.

Let $W_1 \subset U$ be the K-subspace spanned by $v_1, \dots, v_{k/2-1}$. One has $B_q(W_1, W_1) = \{0\}$ nach den Berechnungen von (iv): Writing $v_i v_j$ in the basis $a^0, \dots, a^{kn-1}$, only powers of a with exponents congruent to $-i-j \pmod k$ occur. Because of $1 \le i, j \le \frac{k}{2} - 1$ all exponents are $\not\equiv 0 \pmod k$. Hence, by (iv) the trace of $v_i v_j$ equals 0.

Because of $\frac{k}{2} - 1 + \dim_K(W_1^\perp) = \dim_K(W_1) + \dim_K(W_1^\perp) = \dim_K(U) = k+2$ ([Sch84], p. 9, Lemma 3.11 and Corollary 3.12) one has $\dim_K(W_1^\perp) = k + 2 - (\frac{k}{2} - 1) = \frac{k}{2} + 3$. But since W_1 is totally isotropic, one has $W_1 \subset W_1^\perp$ and hence $\dim_K(W_1^\perp / W_1) = (\frac{k}{2}+3) - (\frac{k}{2}-1) = 4$.

By (iv), one has (since all exponents of a are between $2(kn - \frac{k}{2}) = k(2n-1)$ and $2(k \cdot \frac{n+1}{2} - \frac{k}{2}) = kn$)

$$\begin{aligned} q(v_{k/2}) &= \operatorname{Tr}\left(\left[\sum_{i=0}^{\frac{n-1}{2}} \lambda^i a^{k(n-i)-\frac{k}{2}}\right]^2\right) \\ &= \operatorname{Tr}(a^{k(2n-1)}) + 2\lambda \operatorname{Tr}(a^{k(2n-2)}) + \lambda^{n-1} \operatorname{Tr}(a^{kn}) \\ &= k(2n-1)a_0 a_k + 2\lambda \cdot k(n-1)a_k^2 - \lambda^{n-1} kna_0 \\ &= k(2n-1)a_0 a_k + 2\frac{na_0}{(1-n)a_k} k(n-1)a_k^2 - \left(\frac{na_0}{(1-n)a_k}\right)^{n-1} kna_0 \end{aligned}$$

$$= -a_0 k \left[a_k + \left(\frac{n a_0}{(1-n)a_k} \right)^{n-1} n \right]$$
$$\equiv -a_0 k \left[(1-n)^{n-1} a_k^n + n^n a_0^{n-1} \right] \mod (K^\times)^2$$
$$= -a_0 k c(f).$$

In the last step we used that since n is odd, $[(1-n)a_k]^{n-1}$ is a square. The latter expression is $\neq 0$ because of $\operatorname{char} K \nmid k$ and Corollary 5.7.

Let $\tilde{U_1} = \langle \{1, a^{\frac{k}{2}(n-1)}, v_{k/2}\} \rangle$.One has $\tilde{U_1} \subset W_1^\perp$ because of $1, a^{\frac{k}{2}(n-1)} \in W_1^\perp$ and $v_{k/2} \in W_1^\perp$ since for $1 \leq i \leq \frac{k}{2} - 1$ one has $-\frac{k}{2} - i \not\equiv 0 \pmod{k}$, and hence $B_q(v_{k/2}, W_1) = \{0\}$.

The vectors form an orthogonal basis of $\tilde{U_1}$ since $\operatorname{Tr}(1 \cdot a^{\frac{k}{2}(n-1)} = 0 = \operatorname{Tr}(1 \cdot v_{k/2})$ as all exponents of a are $\not\equiv 0 \pmod{k}$, and $\operatorname{Tr}(a^{\frac{k}{2}(n-1)} \cdot v_{k/2}) = 0$.

Let $0 \neq \tilde{v} \in W_1^\perp$ such that $(\tilde{U_1} \oplus \langle \{\tilde{v}\} \rangle) \oplus W_1 = W_1^\perp$. (it exists since $\dim_K(W_1^\perp / (\tilde{U_1} \oplus W_1)) = (\frac{k}{2} + 3) - (3 + \frac{k}{2} - 1) = 1$. Let $U_1 = \tilde{U_1} \oplus \langle \{\tilde{v}\} \rangle$. By construction, one has $U_1 \oplus W_1 = W_1^\perp$. Let $v \in U_1$ be the vector obtained by applying the Gram-Schmidt orthogonalisation to $\tilde{v}$ with respect to $1, a^{\frac{k}{2}(n-1)}, v_{k/2}$. This is possible since $q(1), q(a^{\frac{k}{2}(n-1)}), q(v_{k/2})$ are all $\neq 0$.

Let $W_1' \subset U$ as in Lemma 5.4 (applied to $(q|_U, U)$ with $W_1^\perp = W_1 \oplus U_1$. $(U, q|_U)$ is regular: (L, q) is regular and $L = U \perp (W \oplus W')$. Now apply [Sch84], p. 10, Lemma 3.14 (iii).) Hence $q|_U$ equals $(\frac{k}{2} - 1) \cdot \langle 1, -1 \rangle$ plus the trace form restricted to U_1.

Summing up, one has $q = (W \oplus W') \perp (W_1 \oplus W_1') \perp U_1 = (\frac{k}{2}(n-1) - 1) \langle 1, -1 \rangle + (\frac{k}{2} - 1) \langle 1, -1 \rangle + q|_{U_1} = (\frac{k}{2}n - 2) \langle 1, -1 \rangle + q|_{U_1}$. It remains to calculate $q|_{U_1}$.

Since the basis vectors frome above together with v form an orthogonal basis, one obtains

$$q|_{U_1} = \left\langle q(1), q(a^{\frac{k}{2}(n-1)}), q(v_{k/2}), q(v) \right\rangle$$
$$= \left\langle kn, k(1-n)a_k, q(v_{k/2}), (-1)^{\frac{k}{2}n-2} \frac{\operatorname{disc}(f)}{n(1-n)a_k \cdot q(v_{k/2})} \right\rangle$$
$$= \left\langle kn, k(1-n)a_k, q(v_{k/2}), (-1)^{\frac{k}{2}n-2} \frac{(-1)^{\frac{k}{2}} a_0}{n(1-n)a_k \cdot q(v_{k/2})} \right\rangle$$
$$= \left\langle kn, k(1-n)a_k, q(v_{k/2}), (-1)^{\frac{k}{2}(n+1)-1} \frac{a_0}{n(1-n)a_k a_0 k c(f)} \right\rangle$$
$$= \langle kn, k(1-n)a_k, -a_0 k c(f), -n(1-n)a_k k c(f) \rangle.$$

Here, we used that if $\operatorname{Tr}_{L/K}(\langle 1 \rangle) = \langle a_1, \ldots, a_{n-1}, a_n \rangle$, $a_n \equiv \operatorname{disc}(f) / \prod_{i=1}^{n-1} a_i \mod (K^\times)^2$ ([Bos03], S. 179 f., Satz 11 and [Sch84], p. 37, Remark 2.2), $\frac{k}{2}(n+1) \equiv 0 \pmod{2}$ und $\operatorname{disc}(f) \equiv (-1)^{\frac{k}{2}} a_0 \mod (K^\times)^2$ by Corollary 5.7 because of k even, n odd. □

Margit Angermeier [Ang13] and Ramona Schiller [Sch13] extend in their master theses the above work to minimal polynomials of the form

$$X^{kn} + a_{2k} X^{2k} + a_k X^k + a_0$$

for $k \geq 1$ and $n > 2$.

From these calculations, one easily derives their Stiefel-Whitney invariants. In the case (2) of Theorem 5.9, if $\mu_n \subset K$, then L/K is normal, and for n odd together with the fact that the trace form of a Galois extension of odd degree $[L : K]$ is equal to $[L : K] \langle 1 \rangle$ by Proposition 5.1, one gets relations in $\mathrm{K}_*^{\mathrm{M}}(K)/2$:

$$1 = w(\operatorname{Tr}_{L/K}(\langle 1 \rangle))$$
$$= w(\{n\} + \frac{n-1}{2} \langle 1, -1 \rangle)$$
$$= 1 + \{(-1)^{\frac{n-1}{2}} n\} + \sum_{i=2}^{(n+1)/2} \{(-1)^{\binom{(n-1)/2}{i}} n^{\binom{(n-1)/2}{i-1}}\} \cdot \{-1\}^{i-1}.$$

For example, it follows that $\sqrt{(-1)^{(n-1)/2} n} \in K$ (this result is usually proven using Gauss sums).

In the top degree $\frac{n+1}{2}$ it follows that $\{n\} \cdot \{-1\}^{(n-1)/2} = 0$. The relations have the following interpretation for quadratic forms.

Proposition 5.10. *Let $n > 1$, $a_1, \dots, a_n \in K^\times$. The following are equivalent:*

(i) $\{a_1, \dots, a_n\} = 0 \in \mathrm{K}_n^{\mathrm{M}}(K)/2$

(ii) $\langle\langle a_1, \dots, a_n \rangle\rangle$ *is totally hyperbolic.*

(iii) $\langle\langle a_1, \dots, a_n \rangle\rangle$ *is isotropic.*

(iv) a_n *is represented by* $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle$.

Proof. (i) $\iff$ (ii): By the Milnor conjecture on quadratic forms [OVV00] (note that this is easier for $n = 2$ and already proved in [Mil70]; furthermore, we only need injectivity on *pure* symbols), one has $\{a_1, \dots, a_n\} = 0 = \{1, \dots, 1\}$ if and only if $\langle\langle a_1, \dots, a_n \rangle\rangle \equiv \langle\langle 1, \dots, 1 \rangle\rangle = 2^{n-1} \langle 1, -1 \rangle \mod I^{n+1}$. This is by [Lam05], p. 353, Corollary 5.4 equivalent to $\langle\langle a_1, \dots, a_n \rangle\rangle \equiv \langle\langle 1, \dots, 1 \rangle\rangle = 0 \in W(K)$.

(ii) $\iff$ (iii): a totally hyperbolic form is isotropic, and for the converse see [Lam05], p. 319, Theorem 1.7.

(iii) $\implies$ (iv): By assumption, there is $0 \neq (v_1, v_2) \in K^{2^{n-1}} \times K^{2^{n-1}}$ with

$$\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_1) - a_n \langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_2) = 0.$$

If $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_1)$ or $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_2)$ equals 0, $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle$ is isotropic (since v_1, v_2 are not both 0), hence totally hyperbolic by [Lam05], p. 319, Theorem 1.7, and thus represents a_n. Otherwise, there is $v_3 \in K^{2^{n-1}}$ with

$$\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_3) = \frac{\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_1)}{\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v_2)} = a_n,$$

since Pfister forms are multiplicative by [Sch84], p. 144, Corollary 1.5 (if a form q is anisotropic, one has $D(q) = G(q)$ with the notation from p. 142, and $G(q)$ is obviously a group; if q is hyperbolic, $D(q) = K^\times$ by [Sch84], p. 12 f., Theorem 4.5). Hence, in all cases $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle$ represents a_n.

(iii) $\impliedby$ (iv): By assumption, there is $v \in K^{2^{n-1}}$ with $a_n = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v)$ (denote $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v) = q(v)$ by $q = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle$), so

$$\begin{aligned} \langle\langle a_1, \dots, a_n \rangle\rangle(v, (1, 0, \dots)) &= \langle\langle a_1, \dots, a_{n-1} \rangle\rangle(v) - a_n \langle\langle a_1, \dots, a_{n-1} \rangle\rangle(1, 0, \dots) \\ &= a_n - a_n \\ &= 0. \end{aligned}$$

□

Acknowledgements. I thank Uwe Jannsen, Moritz Kerz and Charles Vial for helpful discussions, and the Studienstiftung des deutschen Volkes for financial and ideational support.

References

[Ang13] Angermeier, Margit: *Über die Diskriminanten und Spurmatrizen von Körpererweiterungen mit spärlich besetzten Minimalpolynomen*. master thesis, Universität Regensburg 2013.

[Bos03] Bosch, Siegfried: *Algebra*. Springer-Lehrbuch, fünfte Auflage, Springer 2003.

[CTVE+03] Carlson, John F.; Townsley, Lisa; Valero-Elizondo, Luis et al.: *Cohomology Rings of Finite Groups*. Kluwer Academic Publishers 2003.

[Eve63] Evens, Leonard: *A generalization of the transfer map in the cohomology of groups*. In: Trans. Amer. Math. Soc., **108** (1963), 54–65.

[GS06] Gille, Philippe und Szamuely, Tamás: *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics, 101, Cambridge University Press 2006.

[Kah84] Kahn, Bruno: *Classes de Stiefel-Whitney de Formes quadratiques et de représentations galoisiennes réelles*. In: Invent. Math., **78** (1984), 223–256.

[Koc70] Koch, Helmut: *Galoissche Theorie der p-Erweiterungen*. VEB Deutscher Verlag der Wissenschaften 1970.

[Lam05] Lam, Tsit-Yuen: *Introduction to Quadratic Forms Over Fields*. Graduate Studies in Mathematics 67, American Mathematical Society 2005.

[Mat86] Matsumura, Hideyuki: *Commutative ring theory*. Cambridge Studies in Advanced Mathematics, 8, Cambridge University Press 1986.

[Mil70] Milnor, John: *Algebraic K-Theory and Quadratic Forms*. In: Invent. Math., **9** (1970), 318–344.

[MM99] Malle, Gunter und Matzat, Heinrich: *Inverse Galois theory*. Springer Monographs in Mathematics, Springer-Verlag 1999.

[Neu92] Neukirch, Jürgen: *Algebraische Zahlentheorie*. Springer-Verlag 1992.

[NSW00] Neukirch, Jürgen; Schmidt, Alexander und Wingberg, Kay: *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften, Vol. 323, Springer-Verlag 2000.

[OVV00] Orlov, Dmitry; Vishik, Alexander und Voevodsky, Vladimir: *An exact sequence for* $\mathrm{K}_*^{\mathrm{M}}/2$ *with applications to quadratic forms*. Preprint, 2000. URL http://www.math.uiuc.edu/K-theory/0454/.

[Sch84] Scharlau, Winfried: *Quadratic and Hermitian Forms*. Grundlehren der mathematischen Wissenschaften 270, Springer-Verlag 1984.

[Sch13] Schiller, Ramona: *Über die Bestimmung der Spurformen und Stiefel-Whitney-Invarianten von Körpererweiterungen mit spärlich besetzten Minimalpolynomen*. master thesis, Universität Regensburg 2013.

[Ser84] Serre, Jean-Pierre: *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$. In: Comment. Math. Helvetici, **59** (1984), 651–676.

[Ser92] ——— *Topics in Galois Theory*. Research Notes in Mathematics, Volume 1, Jones and Bartlett Publishers 1992.

[Sha79] Shapiro, Jack M.: *A Riemann-Roch type theorem for the Witt and Milnor rings of a field*. In: J. Pure Appl. Algebra, **15** (1979), 293–304.

[Via08] Vial, Charles: *Operations in Milnor K-theory*. Preprint, 2008. URL http://www.math.uiuc.edu/K-theory/0881/.

[Voe03] Voevodsky, Vladimir: *Reduced power operations in motivic cohomology*. In: Publ. Math. Inst. Hautes Études Sci., **98** (2003), 1–57.

Timo Keller, Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-Mail address: firstname.lastname@uni-bayreuth.de