Can. J. Math., Vol. XL, No. 3, 1988, pp. 546-588

THE ADDITIVE CHARACTERS OF THE WITT RING OF AN ALGEBRAIC NUMBER FIELD

P. E. CONNER AND NORIKO YUI

1. Introduction. For an algebraic number field K there is a similarity between the additive characters defined on the Witt ring $W(K)$, [**20**], [**11**], [**17**], [**14**, p. 131], and the local root numbers associated to a real orthogonal representation of the absolute Galois group of K, [**18**], [**5**]. Using results of Deligne and of Serre, [**16**], we shall derive in (5.3) a formula expressing the value, at a prime in K, of the additive character on a Witt class in terms of the rank modulo 2, the stable Hasse-Witt invariant and the local root number associated to the real quadratic character defined by the square class of the discriminant. Thus we are able to separate out the contributions made to the value of the additive character by each of the standard Witt class invariants.

Upon a re-examination of the results of Deligne on local root numbers and those of Serre on trace forms, we can see that if E/K is a relative extension of number fields, then it is possible to express in a simple formula (6.2) the relation between the values of Weil's additive character $\gamma_p\langle E\rangle$, where $\langle E\rangle \in W(K)$ is the Witt class of the relative trace form from the extension and p is a prime divisor of K, and the local root number $W_p(K, \rho(E))$, where $\rho(E)$ is the real orthogonal representation of $\mathrm{Gal}(\bar{K}/K)$ induced by the trivial representation of the subgroup $\mathrm{Gal}(\bar{K}/E)$. This shows us explicitly how the local root numbers for $\rho(E)$ depend only on the Witt class $\langle E\rangle \in W(K)$ and the degree of E/K modulo 8.

In all of these considerations, it is to be expected that the prime 2 would have special features. It is natural to express this in terms of van der Blij's invariant, [**1**], [**14**, p. 25], and we carry out this in Sections 7 and 8 showing this invariant's connection with both additive characters and local root numbers.

We have included a section of examples (Section 10) to illustrate what these additive characters, and local root numbers, really look like in the Witt ring formalism. In fact, these examples may be regarded as one of the main points of this paper.

Langlands has introduced local root numbers for all complex representations of the absolute Galois group. Here we only treat certain real

Received January 15, 1987 and in revised form February 8, 1988. The second author was partially supported by a grant from Natural Sciences and Engineering Research Council of Canada during the preparation of this paper.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

orthogonal representations which occur naturally in connection with innerproduct spaces.

Fröhlich [7] has considered orthogonal representations of Galois groups, and the relation between the Hasse-Witt invariants of trace forms and the second Stiefel-Whitney classes associated with orthogonal representations, generalizing the results of Deligne [5] and of Serre [16]. There is no overlap with the present paper, as our discussions are centered around the additive characters of the Witt ring of an algebraic number field.

During the preparation of this paper, the first author was a visiting professor at the University of Geneva and the University of Regensburg, and the second author was a member of the Mathematical Sciences Research Institute, Berkeley, and was affiliated with the University of Toronto. Our thanks are due to Olga Taussky-Todd for her interest in this work and for her valuable comments, and to Robert Perlis for his continual interest and criticism for this work.

2. A local formula. We assume that $K/\mathbf{Q}_l$ is an extension of finite degree of the l-adic completion of the rationals at some finite prime l in $\mathbf{Q}$. If $\bar{K}/K$ is an algebraic closure of K then the finite extensions $F/K \subset \bar{K}/K$ are in one-to-one correspondence with the closed subgroups of finite index in the compact, profinite Galois group $\mathrm{Gal}(\bar{K}/K)$. Thus we may write

$$G(F) = \mathrm{Gal}(\bar{K}/F) \subset \mathrm{Gal}(\bar{K}/K).$$

In particular, we write $\mathrm{Gal}(\bar{K}/K) = G(K)$.

In his expository paper on local constants, [18], Tate shows that to every pair $(G(F), \rho)$, where ρ is a continuous finite-dimensional real orthogonal representation of $G(F)$, there is associated a root number, $W(F, \rho) \in \mathbf{C}^*$, which is a fourth root of unity. For a second such pair, $(G(F), \rho_1)$, the direct sum may be formed and

$$W(F, \rho + \rho_1) = W(F, \rho)W(F, \rho_1).$$

Hence we may assume that $W(F, \rho)$ is defined for virtual real orthogonal representations of $G(F)$.

Now $G(F) \subset G(K) = \mathrm{Gal}(\bar{K}/K)$ is a closed subgroup of finite index equal to the degree of F/K and so each virtual representation ρ of $G(F)$ will induce a virtual representation $(G(K), \mathrm{Ind}(\rho))$. If $\deg(\rho) = 0$ then

$$W(K, \mathrm{Ind}(\rho)) = W(F, \rho).$$

Deligne [5], [18, Section 3], made the following analysis of root numbers of real orthogonal representations. Associated to the virtual representation $(G(F), \rho)$ there is the determinant homomorphism

$$\det(\rho){:}G(F) \to \mathbf{Z}^* = \mathbf{Z}/2\mathbf{Z}.$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Since this is a degree 1 orthogonal representation (possibly trivial) it too has a root number, $W(F, \det(\rho))$. Then

$$W(F, \rho)/W(F, \det(\rho)) = \pm 1$$

and, under the isomorphism in Galois cohomology

$$H^2(G(F); \mathbf{Z}/2\mathbf{Z}) \cong Br_2(F) \cong \mathbf{Z}^*,$$

Deligne identifies this ratio with the ordinary second Stiefel-Whitney class of the virtual representation,

$$s_2(\rho) \in H^2(G(F); \mathbf{Z}/2\mathbf{Z}).$$

Next observe that through the identification

$$F^*/F^{**} \cong H^1(G(F); \mathbf{Z}/2\mathbf{Z}) \cong \mathrm{Hom}(G(F); \mathbf{Z}/2\mathbf{Z}) \cong \mathrm{Hom}(G(F), \mathbf{Z}^*)$$

we may canonically assign to each square class $\sigma \in F^*/F^{**}$ a corresponding degree 1 representation

$$\rho(\sigma): G(F) \rightarrow O(1)$$

defined by

$$\rho(\sigma)(g) = g(\sqrt{\sigma})/\sqrt{\sigma} \in \mathbf{Z}^* \quad \text{for all } g \in G(F).$$

As a corollary there will be assigned to $\sigma \in F^*/F^{**}$ a root number $W(F, \rho(\sigma))$. However, we can also define a real quadratic character

$$\chi(\sigma): F^* \rightarrow \mathbf{Z}^*$$

by $\chi(\sigma)(x) = (x, \sigma)_P$, where the Hilbert symbol is taken at the prime P in F. Then, as described in [**18**, p. 94], there is the root number $W(F, \chi(\sigma))$ of the real quadratic character. Naturally

$$W(F, \chi(\sigma)) = W(F, \rho(\sigma)),$$

and therefore we shall rephrase [**18**, Corollary 2, p. 126] as

(2.1) LEMMA. *For square classes σ, σ_1 in F^*/F^{**}*

$$W(F, \rho(\sigma\sigma_1)) = (\sigma, \sigma_1)_P W(F, \rho(\sigma)) W(F, \rho(\sigma_1)).$$

We shall now introduce Witt theory considerations. The Witt class of the trace form of the extension F/K will be denoted by $\langle F \rangle \in W(K)$, the Witt ring of the local field K. If a square class $\sigma \in F^*/F^{**}$ is used to scale the trace form of F/K then the resulting Witt class will be denoted by $\langle F(\sigma) \rangle \in W(K)$. We wish to prove

(2.2) THEOREM. *For $\sigma \in F^*/F^{**}$*

$$W(F, \rho(\sigma)) = c_p(\langle F(\sigma) \rangle - \langle F \rangle) W(K, \rho(N_{F/K}(\sigma))).$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

By $c_p(\langle F(\sigma)\rangle - \langle F\rangle) \in \mathbf{Z}^*$ we denote the stable Hasse-Witt invariant [**4**, p. 14-15], at the prime p in K of the difference element $\langle F(\sigma)\rangle - \langle F\rangle$ which lies in the fundamental ideal of the Witt ring $W(K)$.

The proof of (2.2) combines Deligne's analysis with the results of Serre on trace forms, [**16**], and will be completed after we prove Lemma (2.8).

To begin with there is the trivial degree 1 representation

$$1_F:G(F) \to O(1).$$

If $\deg(F/K) = n$ then this will induce a transitive permutation representation

$$\rho(F):G(F) \to S_n \subset O(n)$$

with degree n. This extension has a square class discriminant $d \in K^*/K^{**}$ and Serre noted that

$$\det(\rho(F)) = \rho(d).$$

That is, under

$$K^*/K^{**} \cong H^1(G(K), \mathbf{Z}/2\mathbf{Z}) \cong \mathrm{Hom}(G(K), \mathbf{Z}^*)$$

we may identify d with both the first Stiefel-Whitney class $s_1(\rho(F))$ and with $\det(\rho(F))$. Therefore by Deligne's theorem we can write

$$W(K, \rho(d))s_2(\rho(F)) = W(K, \rho(F)).$$

The main point now is that Serre proved that under the isomorphism

$$H^2(G(K); \mathbf{Z}/2\mathbf{Z}) \cong Br_2(K) \cong \mathbf{Z}^*$$

$s_2(\rho(F))$ is identified with the product $(2, d)_p h_p(F/K)$ where $h_p(F/K) \in \mathbf{Z}^*$ is the classical Hasse symbol at the prime p in K of the trace form of F/K. Thus far, by Deligne and Serre, we have

(2.3) LEMMA. *For a finite extension F/K*

$$W(K, \rho(F)) = (2, d)_p h_p(F/K)W(K, \rho(d)).$$

To bring in scaled trace forms we now introduce

$$\rho(F, \sigma) = \mathrm{Ind}(\rho(\sigma)):G(K) \to O(n)$$

for any square class $\sigma \in F^*/F^{**}$. This time Serre found that

$$\det(\rho(F, \sigma)) = \rho(N(\sigma)d),$$

that is,

$$s_1(\rho(F, \sigma)) = N(\sigma)d \in K^*/K^{**},$$

while

$$s_2(\rho(F, \sigma)) = (2, d)_p h_p(\sigma, F/K)$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

where $h_p(\sigma, F/K) \in \mathbf{Z}^*$ is now the classical Hasse symbol of the trace form of F/K scaled by σ. The factor $(2, d)_p$ is correct.

(2.4) LEMMA. *For* $\sigma \in F^*/F^{**}$

$$W(K, \rho(F, \sigma)) = (2, d)_p h_p(\sigma, F/K) W(K, \rho(N(\sigma)d)).$$

Next we note that

$$W(F, \rho(\sigma) - 1) = W(F, \rho(\sigma)).$$

But $\deg(\rho(\sigma) - 1) = 0$ so that

$$W(F, \rho(\sigma) - 1) = W(K, \mathrm{Ind}(\rho(\sigma) - 1)) = W(K, \rho(F, \sigma) - \rho(F)).$$

Consequently we may add the relation

(2.5) LEMMA. *For* $\sigma \in F^*/F^{**}$

$$W(K, \rho(F, \sigma)) = W(F, \rho(\sigma)) W(K, \rho(F)).$$

We now combine (2.1), (2.3), (2.4) and (2.5) into

(2.6) LEMMA. *For* $\sigma \in F^*/F^{**}$

$$W(F, \rho(\sigma)) = (N(\sigma), d)_p h_p(\sigma, F/K) h_p(F/K) W(K, \rho(N(\sigma))).$$

The reader will note that (2.6) involves the classical Hasse symbols of two different innerproduct spaces over K, while (2.2) states a formula which is in terms of the stable Hasse-Witt invariant of a difference element in the Witt ring of K. Clearly we need a conversion table between c_p and h_p. We denote by (V, b) an innerproduct space over K and by $\langle V, b\rangle \in W(K)$ the resulting Witt class.

(2.7) LEMMA. *For an innerproduct space* (V, b) *over* K

$$\begin{cases} h_p(V, b) = c_p\langle V, b\rangle & \text{if } \dim V \equiv 0, 1 \pmod 8 \\ h_p(V, b) = (-1, \mathrm{dis}\langle V, b\rangle)_p c_p\langle V, b\rangle & \text{if } \dim V \equiv 2, 3 \pmod 8 \\ h_p(V, b) = (-1, -1)_p c_p\langle V, b\rangle & \text{if } \dim V \equiv 4, 5 \pmod 8 \\ h_p(V, b) = (-1, -\mathrm{dis}\langle V, b\rangle)_p c_p\langle V, b\rangle & \text{if } \dim V \equiv 6, 7 \pmod 8). \end{cases}$$

We are now interested in the Scharlau transfer homomorphism [**4**, p. 35] and specifically in

$$T_{F/K}(\langle\sigma\rangle - \langle 1\rangle) = \langle F(\sigma)\rangle - \langle F\rangle$$

in the fundamental ideal $I \subset W(K)$. We note that

$$\mathrm{dis}\langle F(\sigma)\rangle = N(\sigma)\,\mathrm{dis}\langle F\rangle \in K^*/K^{**}$$

$$\mathrm{dis}(\langle F(\sigma)\rangle - \langle F\rangle) = N(\sigma) \in K^*/K^{**}.$$

Then from a direct computation, following the rules in [**4**, I.2.4], we find that

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$c_p(\langle F(\sigma)\rangle - \langle F\rangle) = (N(\sigma), \mathrm{dis}\langle F\rangle)_p c_p\langle F(\sigma)\rangle c_p\langle F\rangle.$$

Thus (2.2) will be an immediate corollary of (2.6) and

(2.8) LEMMA.

$$(N(\sigma), \mathrm{dis}\langle F\rangle)_p c_p\langle F(\sigma)\rangle c_p\langle F\rangle = (N(\sigma), d)_p h_p(\sigma, F/K) h_p(F/K).$$

Proof. If $\deg(F/K) \equiv 0$ or $1 \pmod 4$ then

$$\mathrm{dis}\langle F\rangle = d \in K^*/K^{**}$$

and from the conversion formula in (2.7) it follows immediately that

$$c_p\langle F(\sigma)\rangle c_p\langle F\rangle = h_p(\sigma, F/K) h_p(F/K).$$

Suppose that $\deg(F/K) \equiv 2$ or $3 \pmod 4$. Then

$$\mathrm{dis}\langle F\rangle = -d \quad \text{and} \quad \mathrm{dis}\langle F(\sigma)\rangle = -N(\sigma)d.$$

Now from (2.7)

$$\begin{aligned} h_p(\sigma, F/K) &= c_p\langle F(\sigma)\rangle(-1, N(\sigma)\,\mathrm{dis}\langle F\rangle)_p \\ &= c_p(\langle F(\sigma)\rangle)(-1, -N(\sigma)d)_p \end{aligned}$$

$$h_p(F/K) = c_p\langle F\rangle(-1, \mathrm{dis}\langle F\rangle)_p = c_p\langle F\rangle(-1, -d)_p.$$

Hence

$$h_p(\sigma, F/K) h_p(F/K) = c_p\langle F(\sigma)\rangle c_p\langle F\rangle(-1, N(\sigma))_p$$

and

$$\begin{aligned} (N(\sigma), d)_p h_p(\sigma, F/K) h_p(F/K) &= c_p\langle F(\sigma)\rangle c_p\langle F\rangle(-d, N(\sigma))_p \\ &= c_p\langle F(\sigma)\rangle c_p\langle F\rangle(\mathrm{dis}\langle F\rangle, N(\sigma))_p. \end{aligned}$$

The case $\deg(F/K) \equiv 6$ or $7 \pmod 8$ is similar and is left to the reader. This completes the proof of (2.2).

We close this section by pointing out

(2.9) COROLLARY. *For* $\sigma \in K^*/K^{**}$

$$W(K, \rho(F, \sigma)) = c_p(\langle F(\sigma)\rangle - \langle F\rangle) W(K, \rho(F)) W(K, \rho(N_{F/K}(\sigma))).$$

Proof. In (2.5) we noted that

$$W(K, \rho(F, \sigma)) = W(K, \rho(F)) W(F, \rho(\sigma))$$

so we simply apply (2.2).

3. Algebraic number fields.

In this section we shall assume that K is an algebraic number field. If $\bar{K}/K$ is an algebraic closure of K then again we have a profinite absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ and the extensions of finite degree $E/K \subset \bar{K}/K$ are in one-to-one correspondence with the closed subgroups of finite index in $\mathrm{Gal}(\bar{K}/K)$:

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$G(E) = \mathrm{Gal}(\bar{K}/E) \subset \mathrm{Gal}(\bar{K}/K) = G(K).$$

To a virtual real orthogonal representation $(G(E), \rho)$ there is associated a collection of local root numbers $W_P(W, \rho)$, one for each prime P in E. These satisfy

1. $W_P(E, \rho)$ is a fourth root of unity,
2. $W_P(E, \rho) = 1$ for almost all primes,
3. $W_P(E, \rho) = 1$ for all complex infinite primes,
4. $W_P(E, \rho) = \pm 1$ for all primes at which -1 is a local square in the completion of E, and
5. $\prod_P W_P(E, \rho) = 1$.

This last, a reciprocity law for root numbers of real orthogonal representations, is the Fröhlich-Queyrut theorem which asserts that the global root number for a real orthogonal representation is always 1. If $(G(F), \rho)$ has $\deg(\rho) = 0$, then

$$W_p(K, \mathrm{Ind}(\rho)) = \prod_{P|p} W_P(E, \rho)$$

at each prime p in K. Furthermore, Deligne's analysis still applies. That is,

$$W_P(E, \rho)/W_P(E, \det(\rho)) = \pm 1$$

and these ratios can be regarded as a single element in $Br_2(E)$. Then this element is identified with

$$s_2(\rho) \in H^2(G(E); \mathbf{Z}/2\mathbf{Z}) \cong Br_2(E).$$

For a global square class $\sigma \in E^*/E^{**}$ we have at each completion of E, denoted by $E(P)$, the real quadratic character

$$\chi(\sigma): E(P)^* \rightarrow \mathbf{Z}^*$$

defined by $\chi(\sigma)(x) = (x, \sigma)_P$ (the Hilbert symbol) and we have naturally

$$W_P(E, \rho(\sigma)) = W(E(P), \chi(\sigma)).$$

The global version of (2.2) is

(3.1) THEOREM. *For $\sigma \in E^*/E^{**}$, and p a prime in K,*

$$c_p(\langle E(\sigma)\rangle - \langle E\rangle)W_p(K, \rho(N_{E/K}(\sigma))) = \prod_{P|p} W_P(E, \rho(\sigma)).$$

The proof will be facilitated by the following device.

(3.2) *Definition.* Let L be an algebraic number field, or a completion of an algebraic number field. For a Witt class X in the fundamental ideal I of $W(L)$ and for a prime P in L, introduce

$$v_P(X) = c_P(X)W_P(L, \rho(\mathrm{dis}(X))) \in \mathbf{C}^*.$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

We note in particular that for X, Y both in the fundamental ideal I of $W(L)$

$$\nu_P(X + Y) = \nu_P(X)\nu_P(Y).$$

This follows from the identities

$$\operatorname{dis}(X + Y) = \operatorname{dis}(X)\operatorname{dis}(Y)$$

$$c_P(X + Y) = (\operatorname{dis}(X), \operatorname{dis}(Y))_P c_P(X)c_P(Y)$$

and by (2.1)

$$W_P(L, \rho(\operatorname{dis}(X)\operatorname{dis}(Y)))$$
$$= (\operatorname{dis}(X), \operatorname{dis}(Y))_P W_P(L, \rho(\operatorname{dis}(X)))W_P(L, \rho(\operatorname{dis}(Y))).$$

We now return to (3.1). A prime p in K has extensions $P_1, \dots, P_r$ to E. These produce local extensions $E(P_j)/K(p)$ ($K(p)$ denotes the completion of K at p) together with local norms and local traces. We consider the image of $\langle\sigma\rangle - \langle 1\rangle$ in $W(E(P_j))$ and we apply the local Scharlau transfer:

$$T_{E(P_j)/K(p)}(\langle\sigma\rangle - \langle 1\rangle) = X_j \in I \subset W(K(p)).$$

But the image of

$$T_{E/K}(\langle\sigma\rangle - \langle 1\rangle) = \langle E(\sigma)\rangle - \langle E\rangle$$

in the fundamental ideal of $W(K(p))$ is equal to the sum $\sum_1^r X_j$. According to (2.2)

$$W_{P_j}(E, \rho(\sigma)) = W(E(P_j), \chi(\sigma))$$
$$= c_p(X_j)W(K(p), \chi(N_j(\sigma)))$$
$$= c_p(X_j)W(K(p), \rho(N_j(\sigma))).$$

Note here that $N_j(\sigma)$ is a local norm. But this can also be written as

$$W_{P_j}(E, \rho(\sigma)) = \nu_p(X_j).$$

Then

$$\nu_p(\langle E(\sigma)\rangle - \langle E\rangle) = \prod_1^r \nu_p(X_j) = \prod_1^r W_{P_j}(E, \rho(\sigma)).$$

Now

$$\operatorname{dis}(\langle E(\sigma)\rangle - \langle E\rangle) = N_{E/K}(\sigma)$$

so that

$$\nu_p(\langle E(\sigma)\rangle - \langle E\rangle) = c_p(\langle E(\sigma)\rangle - \langle E\rangle)W_p(K, \rho(N_{E/K}(\sigma)))$$

by definition. Thus (3.1) follows.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

To formulate (2.9) globally we recall the relation

$$W_p(K, \operatorname{Ind}(\rho(\sigma) - 1)) = W_p(K, \rho(E, \sigma) - \rho(E))$$
$$= \prod_{P|p} W_P(E, \rho(\sigma) - 1) = \prod_{P|p} W_P(E, \rho(\sigma)).$$

Hence we find

(3.3) COROLLARY. *For $\sigma \in E^*/E^{**}$*

$$W_p(K, \rho(E, \sigma)) = c_p(\langle E(\sigma) \rangle - \langle E \rangle) W_p(K, \rho(E)) W_p(K, \rho(N_{E/K}(\sigma)))$$

at each prime p in K.

Next we wish to show

(3.4) COROLLARY. *For a square class $\sigma \in K^*/K^{**}$ and a prime p in K*

$$\prod_{P|p} W_P(E, \operatorname{Res}(\rho(\sigma))) = (\sigma, \operatorname{dis}\langle E \rangle)_p W_p(K, \rho(\sigma))$$

if $\deg(E/K)$ *is odd, while if* $\deg(E/K)$ *is even then*

$$\prod_{P|p} W_P(E, \operatorname{Res}(\rho(\sigma))) = (\sigma, \operatorname{dis}\langle E \rangle)_p.$$

Proof. The square class $\sigma \in K^*/K^{**}$ corresponds to $\rho(\sigma): G(K) \to O(1)$. Then

$$\operatorname{Res}(\rho(\sigma)): G(E) \to O(1)$$

simply means that we consider σ as a square class in E^*/E^{**}. But then [**4**, I.6.1] asserts that

$$T_{E/K}(\langle \sigma \rangle - \langle 1_E \rangle) = (\langle \sigma \rangle - \langle 1_K \rangle)\langle E \rangle$$

in the fundamental ideal $I \subset W(K)$. By a simple calculation

$$c_p(T_{E/K}(\langle \sigma \rangle - \langle 1_E \rangle)) = (\sigma, \operatorname{dis}\langle E \rangle)_p$$

while

$$N_{E/K}(\sigma) = \sigma^{\deg(E/K)} \in K^*/K^{**}.$$

Finally we would like to connect (3.1) and (3.2) with the Scharlau transfer homomorphism $T: W(E) \to W(K)$.

(3.5) COROLLARY. *For $X \in I \subset W(E)$*

$$v_p(T_{E/K}(X)) = \prod_{P|p} v_p(X)$$

at every prime p in K.

Proof. Since $c_p(\langle\sigma\rangle - \langle 1\rangle) = 1$ for all primes in E we can begin by restating (3.1) in the form

$$v_p(T(\langle\sigma\rangle - \langle 1\rangle)) = \prod_{P|p} v_p(\langle\sigma\rangle - \langle 1\rangle).$$

Then for a general Witt class $X \in I \subset W(E)$ we choose a representative innerproduct space (V, b) over E with

$$\dim_E V = m \equiv 0 \pmod 8.$$

We assume that (V, b) is diagonalized with diagonal entries $\sigma_1, \dots, \sigma_m$. Then we write

$$\begin{aligned}\langle V, b\rangle - m\langle 1_E\rangle &= X - m\langle 1_E\rangle \\ &= (\langle\sigma_1\rangle - \langle 1_E\rangle) + \dots + (\langle\sigma_m\rangle - \langle 1_E\rangle).\end{aligned}$$

But

$$v_P(X - m\langle 1_E\rangle) = v_P(X)(v_P(2\langle 1_E\rangle))^{-m/2}$$

and since $m \equiv 0 \pmod 8$ we get

$$(v_P(2\langle 1_E\rangle))^{-m/2} = 1.$$

Thus we obtain

$$v_P(X - m\langle 1_E\rangle) = v_P(X)$$

and by a similar argument,

$$v_p(T(X) - m\langle E\rangle) = v_p(T(X)).$$

So now

$$X - m\langle 1_E\rangle = (\langle\sigma_1\rangle - \langle 1_E\rangle) + \dots + (\langle\sigma_m\rangle - \langle 1_E\rangle)$$

$$v_P(X) = \prod_1^m v_P(\langle\sigma_j\rangle - \langle 1_E\rangle)$$

while

$$v_p(T(X)) = \prod_1^m v_p(T(\langle\sigma_j\rangle - \langle 1_E\rangle)).$$

Then for each index j we have from (3.1)

$$v_p(T_{E/K}(\langle\sigma_j\rangle - \langle 1_E\rangle)) = \prod_{P|p} v_P(\langle\sigma_j\rangle - \langle 1_E\rangle).$$

Thus (3.5) is established.

To be complete we return to the local field $K/\mathbf{Q}_l$ and a finite extension F/K. Then from (2.2) we obtain

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

(3.6) COROLLARY. *For* $X \in I \subset W(F)$

$$v_p(T_{F/K}(X)) = v_P(X).$$

In Section 5 we shall show that the invariant introduced in (3.2) is simply the additive character [**14**, p. 131]

$$\gamma_P: W(L) \rightarrow \mathbf{C}^*.$$

4. Examples of local root numbers.

In this section we shall recall some known examples of local root numbers associated with real quadratic characters and then in the following sections we shall refer to these computations. We take the algebraic number field to be $\mathbf{Q}$ and for $\sigma \in \mathbf{Q}^*/\mathbf{Q}^{**}$ we are interested in $W_l(\mathbf{Q}, \rho(\sigma))$. First of all, we can write

$$W_l(\mathbf{Q}, \rho(\sigma)) = W(\mathbf{Q}_l, \chi(\sigma))$$

where the real quadratic character χ on $\mathbf{Q}_l^*$ is given by the Hilbert symbol

$$\chi(\sigma):\mathbf{Q}_l^* \rightarrow \mathbf{Z}^*, \quad x \rightarrow (x, \sigma)_l.$$

Thus we can refer to the description of $W(\mathbf{Q}_l, \chi(\sigma))$ in [**18**, p. 94]. We should keep in mind then that

$$W_\infty(\mathbf{Q}, \rho(\sigma)) = \begin{cases} 1 & \text{if } \sigma > 0 \\ -i & \text{if } \sigma < 0. \end{cases}$$

We can also say

(4.1) LEMMA. *If the rational prime l is unramified in* $\mathbf{Q}(\sqrt{\sigma})/\mathbf{Q}$ *then*

$$W_l(\mathbf{Q}, \rho(\sigma)) = 1.$$

Proof. The infinite prime is unramified in this quadratic extension if and only if $\sigma > 0$. If l is a finite rational prime unramified in $\mathbf{Q}(\sqrt{\sigma})/\mathbf{Q}$ then $\chi(\sigma):\mathbf{Q}_l^* \rightarrow \mathbf{Z}^*$ is an unramified character. Since the absolute different of $\mathbf{Q}_l/\mathbf{Q}_l$ is the unit ideal, it will follow that

$$W_l(\mathbf{Q}, \rho(\sigma)) = W(\mathbf{Q}_l, \chi(\sigma)) = 1.$$

Next we represent σ by a square-free rational integer n.

(4.2) LEMMA. *If l is an odd rational prime that divides n, then*

$$W_l(\mathbf{Q}, \rho(n)) = \begin{cases} (-n/l, l)_l & \textit{if } l \equiv 1 \pmod 4 \\ (-n/l, l)_l i & \textit{if } l \equiv 3 \pmod 4). \end{cases}$$

Proof. Since l is an odd rational prime dividing n the (local) conductor for the real quadratic character $\chi(n)$ at l is just $l\mathbf{Z}_l$ and the different of $\mathbf{Q}_l/\mathbf{Q}_l$ is the unit ideal. So following [**18**, p. 94] we put $l = d$ and thus

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$W_l(\mathbf{Q}, \rho(n)) = W(\mathbf{Q}_l, \chi(n)) = \frac{1}{\sqrt{l}}\left(\sum_{x=1}^{l-1} (x/l, n)_l e^{2\pi ix/l}\right).$$

Now

$$(x/l, n)_l = (xl, (n/l)l)_l = (l, (n/l)l)_l(x, (n/l)l)_l$$
$$= (-(n/l), l)_l(x, n/l)_l(x, l)_l = (-n/l, l)_l(x, l)_l.$$

We have used the fact that $(x, n/l)_l = 1$ because n/l and x are both local units at the odd prime l. Therefore

$$W_l(\mathbf{Q}, \rho(n)) = \frac{(-n/l, l)_l}{\sqrt{l}}\left(\sum_{x=1}^{l-1} (x, l)_l e^{2\pi ix/l}\right).$$

The lemma now follows from the well known value of the Galois-Gauss sum.

(4.3) LEMMA. *Let q be a fixed rational prime.*

1. *If $q \equiv 1 \pmod 4$, then $W_l(\mathbf{Q}, \rho(q)) = 1$ for all primes l in* $\mathbf{Q}$.

2. *If $q \equiv 3 \pmod 4$, then $W_2(\mathbf{Q}, \rho(q)) = i$, $W_q(\mathbf{Q}, \rho(q)) = -i$ and $W_l(\mathbf{Q}, \rho(q)) = 1$ otherwise*

3. *If $q = 2$, then $W_l(\mathbf{Q}, \rho(2)) = 1$ for all primes l in* $\mathbf{Q}$.

Proof. According to (4.1) we have $W_l(\mathbf{Q}, \rho(q)) = 1$ for all unramified primes in $\mathbf{Q}(\sqrt{q})/\mathbf{Q}$. Thus if $q = 2$ or $q \equiv 1 \pmod 4$ we see that

$$W_l(\mathbf{Q}, \rho(q)) = 1 \quad \text{for all primes } l \neq q.$$

But we have the reciprocity

$$\prod_l W_l(\mathbf{Q}, \rho(q)) = 1.$$

Now if $q \equiv 3 \pmod 4$ we use (4.2) to see that

$$W_q(\mathbf{Q}, \rho(q)) = (-1, q)_q i = -i.$$

Then

$$W_2(\mathbf{Q}, \rho(q)) = i \quad \text{and} \quad W_l(\mathbf{Q}, \rho(q)) = 1$$

otherwise.

We add the following

(4.4) LEMMA. *If l is an odd rational prime then*

$$W_l(\mathbf{Q}, \rho(-1)) = 1 \quad \textit{while}$$

$$W_\infty(\mathbf{Q}, \rho(-1)) = -i \quad \textit{and} \quad W_2(\mathbf{Q}, \rho(-1)) = i.$$

With (2.1), it is in principle possible to determine $W_l(\mathbf{Q}, \rho(n))$ from (4.3) and (4.4) for any square-free integer n.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

5. Gauss sums associated to a Witt class. To complete the formalism we shall now take up the additive characters

$$\gamma_l: W(\mathbf{Q}) \to \mathbf{C}^*.$$

These appeared first in [**20**] and were involved in Weil's reciprocity formula. Their relation to the Witt ring was explored in [**11**] and in [**17**]. These additive characters were included in the discussion of Milgram's theorem in [**14**, p. 131]. We shall sketch a viewpoint suitable to our purposes.

For l a finite rational prime, we want to describe a Witt group $W_q(\mathbf{Q}_l/\mathbf{Z}_l)$ of finite innerproduct spaces together with quadratic refinements. We therefore consider all pairs (A, q) where

1. A is a finite $\mathbf{Z}_l$-module (finite abelian l-group)
2. $q:A \to \mathbf{Q}_l/\mathbf{Z}_l$ is a quadratic map, that is,

$$q(\lambda a) = \lambda^2 q(a) \quad \text{for all } \lambda \in \mathbf{Z}_l, a \in A$$

3. $B(a_1, a_2) = q(a_1 + a_2) - q(a_1) - q(a_2) \in \mathbf{Q}_l/\mathbf{Z}_l$ is a $\mathbf{Z}_l$-bilinear and symmetric finite innerproduct space structure on A with values in $\mathbf{Q}_l/\mathbf{Z}_l$.

Such a pair (A, q) is Witt trivial if and only if there is a subgroup $N \subset A$ for which $N^\perp = N$ and $q_{|N}:N \to \mathbf{Q}_l/\mathbf{Z}_l$ is trivial. In the usual way we obtain a group, $Wq(\mathbf{Q}_l/\mathbf{Z}_l)$, of Witt classes with

$$\langle A, q\rangle + \langle A_1, q_1\rangle = \langle A \oplus A_1, q \oplus q_1\rangle$$
$$-\langle A, q\rangle = \langle A, -q\rangle.$$

First we note that if l is an odd prime then the embedding

$$\mathbf{Z}_l/l\mathbf{Z}_l \to \mathbf{Q}_l/\mathbf{Z}_l; \ \lambda \to \lambda/l$$

induces an isomorphism

$$W(\mathbf{Z}_l/l\mathbf{Z}_l) \cong Wq(\mathbf{Q}_l/\mathbf{Z}_l).$$

The point is that for l odd, $2 \in \mathbf{Z}_l^*$ and therefore every finite innerproduct space structure with values in $\mathbf{Q}_l/\mathbf{Z}_l$ has a unique quadratic refinement.

Now to the pair (A, q) we assign

$$\gamma_l(A, q) = \frac{1}{\sqrt{\#(A)}}\left(\sum_{a \in A} \exp(2\pi i q(a))\right).$$

This is a Witt class invariant and defines a homomorphism

$$\gamma_l: Wq(\mathbf{Q}_l/\mathbf{Z}_l) \to \mathbf{C}^*.$$

Next we can introduce a boundary homomorphism

$$\partial_l: W(\mathbf{Q}_l) \to Wq(\mathbf{Q}_l/\mathbf{Z}_l).$$

Let (V, b) be an innerproduct space over $\mathbf{Q}_l$. We choose a $\mathbf{Z}_l$-lattice $L \subset V$ such that

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$b(v, w) \in \mathbf{Z}_l \quad \text{for all } v, w \text{ in } L$$

$$b(v, v) \in 2\mathbf{Z}_l \quad \text{for all } v \text{ in } L.$$

Introduce

$$L^\# = \{x \text{ if } x \in V, b(x, L) \subset \mathbf{Z}_l\}.$$

Then $L \subset L^\#$ and on the quotient group $L^\#/L$ the quadratic refinement is defined by

$$q(a) = b(x, x)/2 \in \mathbf{Q}_l/\mathbf{Z}_l$$

where a denotes a coset of L in $L^\#$ and $x \in L^\#$ is any representative of that coset. We then define

$$\partial_l\langle V, b\rangle = \langle L^\#/L, q\rangle \in Wq(\mathbf{Q}_l/\mathbf{Z}_l).$$

Now from the composition

$$W(\mathbf{Q}_l) \rightarrow Wq(\mathbf{Q}_l/\mathbf{Z}_l) \rightarrow \mathbf{C}^*$$

we obtain

$$\gamma_l: W(\mathbf{Q}_l) \rightarrow \mathbf{C}^*.$$

This is an additive character in the sense that

$$\gamma_l(X + Y) = \gamma_l(X)\gamma_l(Y).$$

In particular, if $X \in W(\mathbf{Q})$ then $\gamma_l(X)$ is defined for all finite primes in $\mathbf{Q}$. Clearly $\gamma_l(X) = 1$ for almost all finite primes. Then by Milgram's theorem

$$\prod_{l \text{ finite}} \gamma_l(X) = \exp(2\pi i \operatorname{sgn}(X)/8).$$

Thus if we define, for $X \in W(\mathbf{Q})$,

$$\gamma_\infty(X) = \exp(-2\pi i \operatorname{sgn}(X)/8)$$

the desired reciprocity is produced. This is Weil Reciprocity.

For any algebraic number field E we can, at each prime P in E, define

$$\gamma_P: W(E) \rightarrow \mathbf{C}^*.$$

Introduce the local extension $E(P)/\mathbf{Q}_l$ and the local Scharlau transfer

$$T_{E(P)/\mathbf{Q}_l}: W(E(P)) \rightarrow W(\mathbf{Q}_l).$$

Then $\gamma_P: W(E) \rightarrow \mathbf{C}^*$ is the composition

$$W(E) \rightarrow W(E(P)) \rightarrow W(\mathbf{Q}_l) \xrightarrow{\gamma_l} \mathbf{C}^*.$$

Now we refer back to the definition (3.2) as we now wish to prove

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

(5.1) THEOREM. *Let $X \in I \subset W(\mathbf{Q})$ be any element in the fundamental ideal of the Witt ring of the rationals. Then*

$$\gamma_l(X) = (-2, \operatorname{dis}(X))_l\, v_l(X)$$

at every prime l in $\mathbf{Q}$.

Proof. We shall first consider the case $l = \infty$. For $X \in I \subset W(\mathbf{Q})$, we have, by the definition,

$$\gamma_\infty(X) = (-i)^{\operatorname{sgn}(X)/2}.$$

Now

$$v_\infty(X) = c_\infty(X) W_\infty(\mathbf{Q}, \rho(\operatorname{dis}(X))).$$

However we know the following [**4**, I.2.3]

$$\begin{cases} c_\infty(X) = 1 \text{ and } \operatorname{dis}(X) > 0 & \text{if and only if } \operatorname{sgn}(X) \equiv 0 \pmod 8 \\ c_\infty(X) = -1 \text{ and } \operatorname{dis}(X) < 0 & \text{if and only if } \operatorname{sgn}(X) \equiv 2 \pmod 8 \\ c_\infty(X) = -1 \text{ and } \operatorname{dis}(X) > 0 & \text{if and only if } \operatorname{sgn}(X) \equiv 4 \pmod 8 \\ c_\infty(X) = 1 \text{ and } \operatorname{dis}(X) < 0 & \text{if and only if } \operatorname{sgn}(X) \equiv 6 \pmod 8. \end{cases}$$

Furthermore,

$$W_\infty(\mathbf{Q}, \rho(\operatorname{dis}(X))) = \begin{cases} 1 & \text{if } \operatorname{dis}(X) > 0 \\ -i & \text{if } \operatorname{dis}(X) < 0. \end{cases}$$

The above discussions culminate in the formula

$$v_\infty(X) = (i)^{\operatorname{sgn}(X)/2}$$

and consequently

$$\gamma_\infty(X) = (-1)^{\operatorname{sgn}(X)/2} v_\infty(X).$$

Now we only need to point out that

$$\begin{aligned} \operatorname{sgn}(X)/2 \equiv 0 \pmod 2 \quad & \text{if and only if } \operatorname{dis}(X) > 0 \\ & \text{if and only if } (-2, \operatorname{dis}(X))_\infty = 1 \end{aligned}$$

and that

$$\begin{aligned} \operatorname{sgn}(X)/2 \equiv 1 \pmod 2 \quad & \text{if and only if } \operatorname{dis}(X) < 0 \\ & \text{if and only if } (-2, \operatorname{dis}(X))_\infty = -1. \end{aligned}$$

Thus we have disposed of the infinite prime $l = \infty$.

Next we must specialize to $X = \langle n \rangle - \langle 1 \rangle$ where n is a square-free rational integer. Then

$$c_l(X) \equiv 1 \quad \text{and} \quad \operatorname{dis}(X) = n \in \mathbf{Q}^*/\mathbf{Q}^{**}.$$

Let us comment on $\gamma_l(X)$. If l is an odd rational prime which does not divide n then $\partial_l(X) = 0$ in $Wq(\mathbf{Q}_l/\mathbf{Z}_l)$ so that $\gamma_l(X) = 1$. However, by (4.1) we also have

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$W_l(\mathbf{Q}, \rho(n)) = \nu_l(X) = 1$$

and certainly

$$(-2, n)_l = (-2, \operatorname{dis}(X))_l = 1.$$

Thus we find for $X = \langle n \rangle - \langle 1 \rangle$

$$1 = \gamma_l(X) = (-2, \operatorname{dis}(X))_l\, \nu_l(X)$$

for all odd rational primes which do not divide n.

But now suppose that l is an odd rational prime which does divide n. Since $\partial_l(\langle n \rangle - \langle 1 \rangle) = \partial_l \langle n \rangle$ it is enough to compute $\gamma_l \langle n \rangle$. The anisotropic representative of $\partial_l \langle 4n \rangle = \partial_l \langle n \rangle$ is $A = \mathbf{Z}_l / l\mathbf{Z}_l$ with

$$q(\lambda) = \frac{2(n/l)\lambda^2}{l} \in \mathbf{Q}_l / \mathbf{Z}_l.$$

Thus $\gamma_l(\langle n \rangle - \langle 1 \rangle)$ is

$$\frac{1}{\sqrt{l}}\left(\sum_{\lambda \in \mathbf{Z}_l / l\mathbf{Z}_l} \exp(2\pi i (2(n/l)\lambda^2))/l \right).$$

The Gauss sum is evaluated in [**12**, p. 85]. The answer is

$$\gamma_l(\langle n \rangle - \langle 1 \rangle) = \begin{cases} (2(n/l), l)_l & \text{if } l \equiv 1 \pmod 4 \\ (2(n/l), l)_l i & \text{if } l \equiv 3 \pmod 4. \end{cases}$$

If we recall (4.2) it is natural to write

$$(2(n/l), l)_l = (-2, l)_l(-n/l, l)_l.$$

Clearly

$$(-2, l)_l = (-2, n)_l = (-2, \operatorname{dis}(X))_l.$$

Thus for $X = \langle n \rangle - \langle 1 \rangle$ we have shown that

$$\gamma_l(X) = (-2, \operatorname{dis}(X))_l\, \nu_l(X)$$

for $l = \infty$ and l any odd rational prime. Then $l = 2$ is simply included by reciprocity. Thus (5.1) has actually been established for $\langle \sigma \rangle - \langle 1 \rangle$ where $\sigma \in \mathbf{Q}^*/\mathbf{Q}^{**}$ is any square class.

So next suppose that $X \in I \subset W(\mathbf{Q})$ is a general Witt class in the fundamental ideal of $W(\mathbf{Q})$. As before we choose a representative innerproduct space (V, b) over $\mathbf{Q}$ with $\dim_{\mathbf{Q}} V = m \equiv 0 \pmod 8$. Assuming that (V, b) is diagonalized we can write

$$\begin{aligned} \langle V, b \rangle - m\langle 1 \rangle &= X - m\langle 1 \rangle \\ &= (\langle \sigma_1 \rangle - \langle 1 \rangle) + \ldots + (\langle \sigma_m \rangle - \langle 1 \rangle) \end{aligned}$$

for suitable square classes σ_j. But $m \equiv 0 \pmod 8$, so $m\langle 1 \rangle \in I^3$. Hence we find

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$\gamma_l(X - m\langle 1\rangle) = \gamma_l(X)$$
$$\mathrm{dis}(X - m\langle 1\rangle) = \mathrm{dis}(X)$$
$$\nu_l(X - m\langle 1\rangle) = \nu_l(X).$$

Thus we have

$$\gamma_l(X) = \prod_l \gamma_l(\langle\sigma_j\rangle - \langle 1\rangle)$$

and

$$(-2, \mathrm{dis}(X))_l\, \nu_l(X) = \prod_l (-2, \sigma_j)_l\, \nu_l(\langle\sigma_j\rangle - \langle 1\rangle).$$

This completes the proof of (5.1).

Even though we used reciprocity in the proof of (5.1), if we note that $W(\mathbf{Q}) \to W(\mathbf{Q}_l) \to 0$ is an epimorphism that preserves the rank modulo 2, then we can add

(5.2) Corollary. *For* $X \in I \subset W(\mathbf{Q}_l)$

$$\gamma_l(X) = (-2, \mathrm{dis}(X))_l\, \nu_l(X).$$

We would like to see (5.1) remains valid for any algebraic number field E and we can use (5.2) to do this. For $E(P)/\mathbf{Q}_l$ let us just write

$$T{:}\, W(E(P)) \to W(\mathbf{Q}_l)$$

rather than $T_{E(P)/\mathbf{Q}_l}$. For $X \in I \subset W(E)$ then by definition $\gamma_p(X) = \gamma_l(T(X))$, while by (3.6) $\nu_P(X) = \nu_l(T(X))$. Now

$$\mathrm{dis}(T(X)) = N_{E(P)/\mathbf{Q}_l}(\mathrm{dis}(X)) \in \mathbf{Q}_l^*/\mathbf{Q}_l^{**}$$

so

$$(-2, \mathrm{dis}(X))_P = (-2, \mathrm{dis}(T(X)))_l.$$

We then apply (5.1) to find

$$\gamma_P(X) = (-2, \mathrm{dis}(X))_P \nu_P(X).$$

Actually we shall find it more useful to have

(5.3) Corollary. *For any prime P in the algebraic number field E and any Witt class* $X \in W(E)$,

1. *If* $\mathrm{rk}(X) \equiv 0 \pmod 2$ *then*

$$\gamma_P(X) = (-2, \mathrm{dis}(X))_P c_P(X) W_P(E, \rho(\mathrm{dis}(X))).$$

2. *If* $\mathrm{rk}(X) \equiv 1 \pmod 2$ *then*

$$\gamma_P(X) = (-2, \mathrm{dis}(X))_P c_P(X) W_P(E, \rho(\mathrm{dis}(X)))\gamma_P\langle 1_E\rangle.$$

Proof. Only the second assertion needs a comment. If $\mathrm{rk}(X) \equiv 1 \pmod 2$ we write

$$X = (X - \langle 1_E \rangle) + \langle 1_E \rangle$$

so

$$\gamma_P(X) = \gamma_P(X - \langle 1_E \rangle)\gamma_P\langle 1_E \rangle.$$

Then using the rules in [**4**, I.2.4] we calculate

$$\mathrm{dis}(X) = \mathrm{dis}(X - \langle 1_E \rangle)$$

$$c_P(X) = c_P(X - \langle 1_E \rangle)$$

and apply part 1 to $X - \langle 1_E \rangle$.

We have made extensive use of Deligne's analysis of local root numbers of real orthogonal representations [**5**], [**18**, Section 3]. An analogous result for the additive characters follows immediately from (5.3).

(5.4) *Exercise.* Show that if $\mathrm{rk}(X) \equiv 1 \pmod 2$ then

$$\gamma_P(X) = c_P(X)\gamma_P(\langle \mathrm{dis}(X) \rangle)$$

while if $\mathrm{rk}(X) \equiv 0 \pmod 2$ then

$$\gamma_P(X)\gamma_P\langle 1_E \rangle = c_P(X)\gamma_P(\langle \mathrm{dis}(X) \rangle).$$

We shall close this section by disposing of the invariant introduced in (3.2).

(5.5) Corollary. *For $X \in I \subset W(E)$*

$$\gamma_P(\langle -2 \rangle X) = \nu_P(X).$$

Proof. Again from [**4**, I.2.4], since $\mathrm{rk}(X) \equiv 0 \pmod 2$ we find

$$\mathrm{dis}(\langle -2 \rangle X) = \mathrm{dis}(X)$$

$$c_P(\langle -2 \rangle X) = (-2, \mathrm{dis}(X))_P c_P(X).$$

Then by (5.3)

$$\begin{aligned} \gamma_P(\langle -2 \rangle X) &= (-2, \mathrm{dis}(X))_P(-2, \mathrm{dis}(X))_P c_P(X) W_P(E, \rho(\mathrm{dis}(X))) \\ &= c_P(X) W_P(E, \rho(\mathrm{dis}(X))) \\ &= \nu_P(X). \end{aligned}$$

6. Local root numbers and additive characters. We shall need a small computation.

(6.1) Lemma. *For any algebraic number field E,*

$$(\gamma_P\langle 1_E \rangle)^2 = W_P(E, \rho(-1)), \quad (\gamma_P\langle 1_E \rangle)^4 = (-1, -1)_P$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$\gamma_P(\langle 1_E\rangle)^6 = (-1, -1)_P W_P(E, \rho(-1)).$$

Proof. We write

$$\gamma_P(\langle 1_E\rangle)^2 = \gamma_P(2\langle 1_E\rangle).$$

Then $2\langle 1_E\rangle$ is represented by $\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$, so by direct calculation

$$\operatorname{dis} 2\langle 1_E\rangle = -1 \in E^*/E^{**}$$

$$c_P(2\langle 1_E\rangle) = (-1, -1)_P.$$

Thus by (5.4)

$$\begin{aligned}\gamma_P(\langle 1_E\rangle)^2 &= (-2, -1)_P(-1, -1)_P W_P(E, \rho(-1))\\ &= (2, -1)_P W_P(E, \rho(-1))\\ &= W_P(E, \rho(-1)).\end{aligned}$$

But then

$$(\gamma_P\langle 1_E\rangle)^4 = W_P(E, \rho(-1))^2 = (-1, -1)_P.$$

Thus we have used (2.1) again. Finally

$$\gamma_P(\langle 1_E\rangle)^6 = (\gamma_P\langle 1_E\rangle)^4(\gamma_P\langle 1_E\rangle)^2.$$

Suppose now that K is an algebraic number field and that E/K is a relative extension of degree n. Then we have the transitive permutation representation

$$\rho(E): G_K \to S_n \subset O(n)$$

which is induced from the trivial degree 1 representation of the subgroup $G_E = \operatorname{Gal}(\bar{K}/E) \subset \operatorname{Gal}(\bar{K}/K) = G_K$. There is also the Witt class of the relative trace form of E/K, $\langle E\rangle \in W(K)$.

(6.2) THEOREM. *If E/K is a relative extension of degree n then at every prime p in K*

$$\gamma_p\langle E\rangle W_p(K, \rho(E)) = (\gamma_p\langle 1_K\rangle)^n.$$

Proof. If we combine the results of Deligne with those of Serre we may begin by writing

$$W_p(K, \rho(E)) = (2, d)_p h_p(E/K) W_p(K, \rho(d))$$

where $d = \operatorname{Dis}(E/K) \in K^*/K^{**}$. Then from (5.4) we also have

$$\gamma_p\langle E\rangle = \begin{cases}(-2, \operatorname{dis}\langle E\rangle)_p c_p\langle E\rangle W_p(K, \rho(\operatorname{dis}\langle E\rangle)) & n \equiv 0 \pmod 2\\ (-2, \operatorname{dis}\langle E\rangle)_p c_p\langle E\rangle W_p(K, \rho(\operatorname{dis}\langle E\rangle))\gamma_p\langle 1_K\rangle & n \equiv 1 \pmod 2\end{cases}$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

where

$$\mathrm{dis}\langle E\rangle = (-1)^{n(n-1)/2}d \in K^*/K^{**}.$$

Let us first note that, since $(2, -1)_p \equiv 1$,

$$(2, d)_p = (2, \mathrm{dis}\langle E\rangle)_p$$

and therefore

$$(-2, \mathrm{dis}\langle E\rangle)_p(2, d)_p = (-1, \mathrm{dis}\langle E\rangle)_p.$$

Next we turn to the product $W_p(K, \rho(\mathrm{dis}\langle E\rangle))W_p(K, \rho(d))$. For $n \equiv 0$, 1 (mod 4), $\mathrm{dis}\langle E\rangle = d$, while for $n \equiv 2$, 3 (mod 4), $\mathrm{dis}\langle E\rangle = -d$. We simply apply (2.1) to find

$$W_p(K, \rho(\mathrm{dis}\langle E\rangle))W_p(K, \rho(d))$$
$$= \begin{cases} (-1, \mathrm{dis}\langle E\rangle)_p & n \equiv 0, 1 \pmod 4 \\ W_p(K, \rho(-1)) & n \equiv 2, 3 \pmod 4. \end{cases}$$

Finally we must refer back to the conversion formulas in (2.7). Using these, we find

$$c_p\langle E\rangle h_p(E/K)$$
$$= \begin{cases} 1 & n \equiv 0, 1 \pmod 8 \\ (-1, \mathrm{dis}\langle E\rangle)_p & n \equiv 2, 3 \pmod 8 \\ (-1, -1)_p & n \equiv 4, 5 \pmod 8 \\ (-1, -\mathrm{dis}\langle E\rangle)_p = (-1, -1)_p(-1, \mathrm{dis}\langle E\rangle)_p & n \equiv 6, 7 \pmod 8. \end{cases}$$

We can now read off the product $\gamma_p\langle E\rangle W_p(K, \rho(E))$ with the aid of (6.1). The result is

$$\begin{cases} 1 = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 0 \pmod 8 \\ \gamma_p\langle 1_K\rangle = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 1 \pmod 8 \\ W_p(K, \rho(-1)) = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 2 \pmod 8 \\ W_p(K, \rho(-1))\gamma_p\langle 1_K\rangle = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 3 \pmod 8 \\ (-1, -1)_p = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 4 \pmod 8 \\ (-1, -1)_p\gamma_p\langle 1_K\rangle = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 5 \pmod 8 \\ (-1, -1)_pW_p(K, \rho(-1)) = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 6 \pmod 8 \\ (-1, -1)_pW_p(K, \rho(-1))\gamma_p\langle 1_K\rangle = (\gamma_p\langle 1_K\rangle)^n & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

This completes the proof of (6.2).

Associated with $\rho(E):G_K \rightarrow O(n)$ there is an extended Artin L-function. This is the Dedekind zeta-function of E with Γ-factors. Thus when we

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

consider $W_p(K, \rho(E))$ we have the local root numbers associated to the Dedekind zeta-function considered as the Artin L-series of the real orthogonal representation $\rho(E)$. We have shown explicitly how the local root numbers $W_p(K, \rho(E))$ depend only on the Witt class $\langle E \rangle$ of the relative trace form of E/K and the degree modulo 8 of this relative extension.

For example suppose that E/K has $\langle E \rangle = 0 \in W(K)$. Then $\deg E/K = n$ is even and at every prime p in K,

$$W_p(K, \rho(E)) = (\gamma_p\langle 1_K \rangle)^n.$$

In fact, for any integer $n \equiv 0 \pmod 2$, there are many extensions E/K of degree n with $\langle E \rangle = 0 \in W(K)$.

The factor $\gamma_p\langle 1_K \rangle$ is not generally easy to determine. For each rational prime l we can say

$$\gamma_l\langle K \rangle = \prod_{p|l} \gamma_p\langle 1_K \rangle.$$

For $K = \mathbf{Q}$ the formula is given as follows:

$$\gamma_2\langle 1_{\mathbf{Q}} \rangle = \xi = \exp(2\pi i/8),$$

$$\gamma_\infty\langle 1_{\mathbf{Q}} \rangle = \xi^{-1}, \quad \text{and}$$

$$\gamma_l\langle 1_{\mathbf{Q}} \rangle = 1 \quad \text{otherwise.}$$

For $\sigma \in E^*/E^{**}$ we also have the scaled Witt class $\langle E(\sigma) \rangle \in W(K)$ and $W_p(K, \rho(E, \sigma))$. We can deal with this case as follows. Using (3.3) we write

$$W_p(K, \rho(E, \sigma)) = c_p(\langle E(\sigma) \rangle - \langle E \rangle) W_p(K, \rho(N(\sigma))) W_p(K, \rho(E)).$$

Then

$$\gamma_p(\langle E(\sigma) \rangle) = \gamma_p(\langle E(\sigma) \rangle - \langle E \rangle)\gamma_p\langle E \rangle$$

and applying (5.4) to $\langle E(\sigma) \rangle - \langle E \rangle \in I \subset W(K)$, we have

$$\gamma_p(\langle E(\sigma) \rangle)$$
$$= (-2, N(\sigma))_p c_p(\langle E(\sigma) \rangle - \langle E \rangle) W_p(K, \rho(N(\sigma)))\gamma_p\langle E \rangle.$$

Now note from (2.1) that

$$W_p(K, \rho(N(\sigma)))^2 = (-1, N(\sigma))_p$$

and then

$$(-2, N(\sigma))_p(-1, N(\sigma))_p = (2, N(\sigma))_p.$$

Thus we find

(6.3) COROLLARY. *If E/K is a relative extension of degree n, then for any square class σ in E^*/E^{**}*

$$\gamma_p(\langle E(\sigma)\rangle)W_p(K, \rho(E, \sigma)) = (2, N_{E/K}(\sigma))_p(\gamma_p\langle 1_K\rangle)^n.$$

As an example take $\sigma = -1 \in E^*/E^{**}$. Now

$$(2, N_{E/K}(-1))_p \equiv 1 \quad \text{and} \quad \langle E(-1)\rangle = -\langle E\rangle,$$

so we find

$$W_p(K, \rho(E, -1)) = (\gamma_p\langle E\rangle)^2 W_p(K, \rho(E)).$$

If -1 is a square in E it is easy to see that $2\langle E\rangle = 0 \in W(K)$.

7. Van der Blij's invariant. We denote by $\mathbf{Z}_{(2)} \subset \mathbf{Q}$, the localization, without completion, of the ring of rational integers at 2. There is then the Witt ring $W(\mathbf{Z}_{(2)})$ of innerproduct spaces over the local ring $\mathbf{Z}_{(2)}$. There is a Knebusch short exact sequence

$$0 \rightarrow W(\mathbf{Z}_{(2)}) \rightarrow W(\mathbf{Q}) \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow 0.$$

The (split) epimorphism

$$\partial_2 : W(\mathbf{Q}) \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow 0$$

is given by

$$\partial_2(X) = \operatorname{ord}_2(\operatorname{dis}(X)) \pmod 2$$

for all $X \in W(\mathbf{Q})$.

A natural ring homomorphism

$$\beta : W(\mathbf{Z}_{(2)}) \rightarrow \mathbf{Z}/8\mathbf{Z} \rightarrow 0$$

was introduced by van der Blij [**1**], [**14**, p. 25]. We shall briefly recall the definition. Let (V, b) be an innerproduct space over $\mathbf{Z}_{(2)}$. Then there is an element $u \in V$, called a characteristic class, which is unique modulo $2V$ and for which

$$b(x, x) \equiv b(u, x) \pmod{2\mathbf{Z}_{(2)}}$$

for all $x \in V$. Now $b(u, u)$ is well defined in $\mathbf{Z}_{(2)}/8\mathbf{Z}_{(2)} \cong \mathbf{Z}/8\mathbf{Z}$. That is, if u is replaced by $u + 2v$ then

$$b(u + 2v, u + 2v) = b(u, u) + 4b(u, v) + 4b(v, v).$$

But $b(u, v) + b(v, v) \equiv 0 \pmod{2\mathbf{Z}_{(2)}}$ so that

$$b(u + 2v, u + 2v) \equiv b(u, u) \pmod{8\mathbf{Z}_{(2)}}.$$

Then $b(u, u) \in \mathbf{Z}/8\mathbf{Z}$ is a Witt class invariant and defines a ring homomorphism

$$\beta : W(\mathbf{Z}_{(2)}) \rightarrow \mathbf{Z}/8\mathbf{Z} \rightarrow 0.$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

We also point out that the van der Blij invariant can be defined on the Witt ring $W(\mathbf{Z}_2)$ of the ring $\mathbf{Z}_2 \subset \mathbf{Q}_2$ of 2-adic integers. For $X \in W(\mathbf{Z})$, the Witt ring of innerproduct spaces over the ring $\mathbf{Z}$, there is a well known congruence

$$\beta(X) \equiv \operatorname{sgn}(X) \pmod 8.$$

However for $X \in W(\mathbf{Z}_{(2)})$ we can only say that

$$\beta(X) \equiv \operatorname{sgn}(X) \equiv \operatorname{rk}(X) \pmod 2.$$

We have the additive character

$$\gamma_2 : W(\mathbf{Q}_2) \rightarrow \mathbf{C}^*$$

and for $X \in W(\mathbf{Z}_2)$ we shall give a direct proof of the relation between $\beta(X)$ and $\gamma_2(X)$ [**1**] from the definition of β.

(7.1) LEMMA. *For a Witt class* $X \in W(\mathbf{Z}_2)$

$$\gamma_2(X) = \xi^{\beta(X)}$$

where $\xi = \exp(2\pi i/8)$ *is a primitive* 8*-th root of unity.*

Proof. We represent X by an innerproduct space (V, b) over $\mathbf{Z}_2$. In particular, V is a free $\mathbf{Z}_2$-module of finite rank. Then $\partial_2(X) \in Wq(\mathbf{Q}_2/\mathbf{Z}_2)$ is represented as follows. Put $A = V/4V$ and denote the quotient homomorphism by $\nu : V \rightarrow A$. Then the quadratic map $q : A \rightarrow \mathbf{Q}_2/\mathbf{Z}_2$ is defined by

$$q(\nu(x)) = b(x, x)/8 \in \mathbf{Q}_2/\mathbf{Z}_2.$$

This refines the innerproduct space structure on A with values in $\mathbf{Q}_2/\mathbf{Z}_2$ given by

$$B(\nu(x), \nu(y)) = b(x, y)/4 \in \mathbf{Q}_2/\mathbf{Z}_2.$$

We denote by $\mathcal{K} \subset V$ the kernel of

$$x \rightarrow b(x, u) \equiv b(x, x) \in \mathbf{Z}_2/2\mathbf{Z}_2.$$

Then $\mathcal{K} = V$ if and only if $u \in 2V$, if and only if $b(x, x) \in 2\mathbf{Z}_2$ for all $x \in V$. In that case $\beta(X) = 0 \in \mathbf{Z}/8\mathbf{Z}$ and (V, b) already has a quadratic refinement, $x \rightarrow b(x, x)/2$. Thus $\partial_2(X) = 0 \in Wq(\mathbf{Q}_2/\mathbf{Z}_2)$ and hence

$$\gamma_2(X) = 1 = \xi^0 = \xi^{\beta(X)}.$$

Thus we now assume that $u \notin 2V$. Then $\mathcal{K} \subset V$ has index 2 and there is an element, $x_0 \in V$, unique modulo $\mathcal{K}$, for which

$$b(x_0, x_0) \equiv b(u, x_0) \equiv 1 \pmod{2\mathbf{Z}_2}.$$

We now embed $V/2V$ into A by $x \rightarrow \nu(2x) = 2\nu(x)$. We denote the image by $N \subset A$, thus $N = 2A$. Clearly $2V \subset \mathcal{K}$ so we denote by $K \subset N$ the image of $\mathcal{K}$ under $x \rightarrow \nu(2x) = 2\nu(x)$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Now clearly $\#(N)^2 = \#(A)$ and

$$B(\nu(2x), \nu(2y)) = 4b(x, y)/4 = 0 \in \mathbf{Q}_2/\mathbf{Z}_2.$$

Thus $N = N^{\perp}$. We also note $q_{|K}:K \rightarrow \mathbf{Q}_2/\mathbf{Z}_2$ is trivial, since

$$b(\nu(2x), \nu(2x))/8 = b(x, x)/2 = 0$$

in $\mathbf{Q}_2/\mathbf{Z}_2$ for all $x \in \mathscr{K}$.

In addition $\nu(u) \notin N$ but $\nu(u) \in K^{\perp}$. Then $\nu(2x_0) \in N$ but $\nu(2x_0) \notin K$. The index of K in N is 2, $\#(K)\#(K^{\perp}) = \#(A) = \#(N)^2$. Thus $K \subset N \subset K^{\perp}$ and $\#(K^{\perp}/K) = 4$. Since $q_{|K}$ is trivial on K there is naturally induced a quadratic map $q:K^{\perp}/K \rightarrow \mathbf{Q}_2/\mathbf{Z}_2$ and

$$\partial_2(X) = \langle A, q\rangle = \langle K^{\perp}/K, q\rangle \in Wq(\mathbf{Q}_2/\mathbf{Z}_2).$$

Now $\nu(2x_0)$ has a non-trivial image in $K^{\perp}/K$ as does $\nu(u)$. Hence to compute $\gamma_2(K^{\perp}/K, q)$, we write

$$\gamma_2(K^{\perp}/K, q) = \frac{1}{\sqrt{4}}\{1 + \exp(2\pi i q(\nu(2x_0))) + \exp(2\pi i q(\nu(u))) + \exp(2\pi i q(\nu(u + 2x_0)))\}.$$

Then

$$q(\nu(2x_0)) = 4b(x_0, x_0)/8 = b(x_0, x_0)/2 = 1/2 \in \mathbf{Q}_2/\mathbf{Z}_2$$

and hence

$$\exp(2\pi i q(\nu(2x_0))) = -1.$$

Now $q(\nu(u)) = b(u, u)/8 \in \mathbf{Q}_2/\mathbf{Z}_2$ so that

$$\exp(2\pi i q(\nu(u))) = \xi^{\beta(X)}.$$

Finally

$$q(\nu(u) + \nu(2x_0)) = b(u + 2x_0, u + 2x_0)/8 = b(u, u)/8 \in \mathbf{Q}_2/\mathbf{Z}_2$$

and hence $q(\nu(u) + \nu(2x_0)) = \xi^{\beta(X)}$ also.

Thus

$$\gamma_2(X) = \gamma_2(K^{\perp}/K, q) = \xi^{\beta(X)}$$

as required.

As an immediate consequence of a Knebusch exact sequence, we have

(7.2) Lemma. *For a Witt class $X \in W(\mathbf{Q})$ the following statements are equivalent*

1. $X \in W(\mathbf{Z}(2))$,
2. $\partial_2(X) = \mathrm{ord}_2(\mathrm{dis}(X)) \equiv 0 \pmod 2$,
3. *there is an odd rational integer N for which* $\mathrm{dis}(X) = N \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

It is important to recognize here that N is unique up to sign and residue class mod 8.

We shall also need

(7.3) LEMMA. *If N is an odd rational integer then*

$$(-2, N)_2 W_2(\mathbf{Q}, \rho(N)) = \xi^{N-1} = \exp(2\pi i(N - 1)/8).$$

Proof. We need only be concerned with the values of N modulo 8; that is, $N = 1, 3, 5$ and 7. We know

$$(-2, 1)_2 = (-2, 3)_2 = 1, \quad \text{and} \quad (-2, 5)_2 = (-2, 7)_2 = -1.$$

Then from (4.3)

$$W_2(\mathbf{Q}, \rho(1)) = W_2(\mathbf{Q}, \rho(5)) = 1$$
$$W_2(\mathbf{Q}, \rho(3)) = W_2(\mathbf{Q}, \rho(7)) = i.$$

Thus

$$(-2, N)_2 W_2(\mathbf{Q}, \rho(N)) = i^{(N-1)/2} = \xi^{N-1}.$$

We shall use the lemmas to derive Satz 2 of [**3**] in a Witt ring formulation.

(7.4) THEOREM. *Suppose $X \in W(\mathbf{Z}_{(2)})$ and N is any odd rational integer for which* $\operatorname{dis}(X) = N \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

1. *If* $\operatorname{rk}(X) \equiv 1 \pmod 2$, *then* $\beta(X) \equiv N \pmod 4$ *and*

$$(-1)^{(\beta(X)-N)/4} = c_2(X) \in \mathbf{Z}^*.$$

2. *If* $\operatorname{rk}(X) \equiv 0 \pmod 2$, *then* $\beta(X) \equiv N - 1 \pmod 4$ *and*

$$(-1)^{(\beta(X)-N+1)/4} = c_2(X) \in \mathbf{Z}^*.$$

Proof. We use (5.3) to write

$$\gamma_2(X) = \begin{cases} (-2, N)_2 c_2(X) W_2(\mathbf{Q}, \rho(N))\xi & \text{if } \operatorname{rk}(X) \equiv 1 \pmod 2 \\ (-2, N)_2 c_2(X) W_2(\mathbf{Q}, \rho(N)) & \text{if } \operatorname{rk}(X) \equiv 0 \pmod 2). \end{cases}$$

By (7.1) $\gamma_2(X) = \xi^{\beta(X)}$, while by (7.3)

$$(-2, N)_2 W_2(\mathbf{Q}, \rho(N)) = \xi^{N-1}.$$

Thus for $\operatorname{rk}(X) \equiv 1 \pmod 2$

$$\xi^{\beta(X)-N} = c_2(X) \in \mathbf{Z}^*$$

and for $\operatorname{rk}(X) \equiv 0 \pmod 2$

$$\xi^{\beta(X)-N+1} = c_2(X) \in \mathbf{Z}^*.$$

Since $c_2(X) = \pm 1$ and $\xi^4 = -1$ the exponents of ξ must be divisible by 4.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Thus for $X \in W(\mathbf{Z}_{(2)})$, or $W(\mathbf{Z}_2)$, we have a determination of the van der Blij invariant $\beta(X) \in \mathbf{Z}/8\mathbf{Z}$ in terms of the other Witt class invariants: rank (mod 2), discriminant (mod squares) and the value of the stable Hasse-Witt invariant $c_2(X) \in \mathbf{Z}^*$. In dealing with trace forms it is not uncommon to encounter examples where the van der Blij invariant is obviously defined, but where its direct determination would be inefficient. Then (7.4) can be quite useful in such cases.

Here is an elementary illustration. Let $-N$ be any square free rational integer which is odd and take the quadratic extension $E = \mathbf{Q}(\sqrt{-N})/\mathbf{Q}$. We have the Witt class $\langle E\rangle \in W(\mathbf{Q})$ of the trace form, but $\text{dis}\langle E\rangle = N \in \mathbf{Q}^*/\mathbf{Q}^{**}$ so that $\beta\langle E\rangle \in \mathbf{Z}/8\mathbf{Z}$ is defined. Fortunately we know $c_l\langle E\rangle = (-2, N)_l$ at all primes l in $\mathbf{Q}$. Thus $\beta\langle E\rangle \equiv N - 1 \pmod 4$ and

$$(-1)^{(\beta\langle E\rangle - N+1)/4} = (-2, N)_2.$$

Thus we find

$$\beta\langle E\rangle = \begin{cases} 2 \in \mathbf{Z}/8\mathbf{Z} & \text{if } N \equiv 3 \pmod 4) \\ 0 \in \mathbf{Z}/8\mathbf{Z} & \text{if } N \equiv 1 \pmod 4). \end{cases}$$

We noted that for $X \in W(\mathbf{Z}_{(2)})$ we could only say that

$$\beta(X) \equiv \text{sgn}(X) \pmod 2.$$

However, if we bring in the other Witt invariants we can produce the more precise [**13**]

(7.5) COROLLARY. *Suppose $X \in W(\mathbf{Z}_{(2)})$ and N is an odd rational integer for which* $\text{dis}(X) = N \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

1. *If $N > 0$ then* $\beta(X) - \text{sgn}(X) \equiv N - 1 \pmod 4$ *and*

$$(-1)^{(\beta(X)-\text{sgn}(X)-N+1)/4} = c_2(X)c_\infty(X).$$

2. *If $N < 0$ then* $\beta(X) - \text{sgn}(X) \equiv N + 1 \pmod 4$ *and*

$$(-1)^{(\beta(X)-\text{sgn}(X)-N-1)/4} = c_2(X)c_\infty(X).$$

Proof. We observe first that if $N > 0$ then

$$(-2, N)_\infty W_\infty(\mathbf{Q}, \rho(N)) = (1)(1) = 1$$

while if $N < 0$,

$$(-2, N)_\infty W_\infty(\mathbf{Q}, \rho(N)) = (-1)(-i) = i = \xi^2.$$

From

$$\begin{aligned} \gamma_\infty(X) &= \xi^{-\text{sgn}(X)} \\ &= \begin{cases} (-2, N)_\infty c_\infty(X) W_\infty(\mathbf{Q}, \rho(N)) & \text{if } \text{rk}(X) \equiv 0 \pmod 2) \\ (-2, N)_\infty c_\infty(X) W_\infty(\mathbf{Q}, \rho(N))\xi^{-1} & \text{if } \text{rk}(X) \equiv 1 \pmod 2) \end{cases} \end{aligned}$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

we derive four relations

$$\begin{cases} \xi^{-\operatorname{sgn}(X)} = c_\infty(X) & \text{if } N > 0 \text{ and } \operatorname{rk}(X) \equiv 0 \pmod 2 \\ \xi^{1-\operatorname{sgn}(X)} = c_\infty(X) & \text{if } N > 0 \text{ and } \operatorname{rk}(X) \equiv 1 \pmod 2 \\ \xi^{-2-\operatorname{sgn}(X)} = c_\infty(X) & \text{if } N < 0 \text{ and } \operatorname{rk}(X) \equiv 0 \pmod 2 \\ \xi^{-1-\operatorname{sgn}(X)} = c_\infty(X) & \text{if } N < 0 \text{ and } \operatorname{rk}(X) \equiv 1 \pmod 2). \end{cases}$$

Using (7.4) we see that if $\operatorname{rk}(X) \equiv 0 \pmod 2$ then

$$\xi^{\beta(X)-N+1} = c_2(X)$$

so that

$$c_2(X)c_\infty(X) = \begin{cases} \xi^{\beta(X)-\operatorname{sgn}(X)-N+1} & \text{if } N > 0 \\ \xi^{\beta(X)-\operatorname{sgn}(X)-N-1} & \text{if } N < 0. \end{cases}$$

If $\operatorname{rk}(X) \equiv 1 \pmod 2$

$$\xi^{\beta(X)-N} = c_2(X)$$

and

$$c_2(X)c_\infty(X) = \begin{cases} \xi^{\beta(X)-\operatorname{sgn}(X)-N+1} & \text{if } N > 0 \\ \xi^{\beta(X)-\operatorname{sgn}(X)-N-1} & \text{if } N < 0. \end{cases}$$

Since $c_2(X)c_\infty(X) = \pm 1$ the exponents of ξ are divisible by 4.

8. The invariants $W_2(\mathbf{Q}, \rho(E))$ and $\beta\langle E\rangle$.

In this section we shall consider algebraic number fields $E/\mathbf{Q}$ for which

$$\operatorname{ord}_2(\operatorname{Dis}(E/\mathbf{Q})) \equiv 0 \pmod 2.$$

Thus $\beta\langle E\rangle \in \mathbf{Z}/8\mathbf{Z}$ is defined and we shall relate van der Blij's invariant of the absolute trace form of $E/\mathbf{Q}$ to the local root number $W_2(\mathbf{Q}, \rho(E))$.

(8.1) PROPOSITION. *If $E/\mathbf{Q}$ is an extension of degree n with*

$$\operatorname{ord}_2(\operatorname{Dis}(E/\mathbf{Q})) \equiv 0 \pmod 2$$

then

$$W_2(\mathbf{Q}, \rho(E)) = (i)^{(n-\beta\langle E\rangle)/2}.$$

Proof. From (6.2) we have

$$\gamma_2\langle E\rangle W_2(\mathbf{Q}, \rho(E)) = \xi^n$$

while (7.1) asserts that $\gamma_2\langle E\rangle = \xi^{\beta\langle E\rangle}$. Since $n \equiv \beta\langle E\rangle \pmod 2$ we may conclude

$$W_2(\mathbf{Q}, \rho(E)) = (i)^{(n-\beta\langle E\rangle)/2}.$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Thus we have an expression for $W_2(\mathbf{Q}, \rho(E))$ in terms of van der Blij's invariant and $\deg(E/\mathbf{Q})$ when $\mathrm{ord}_2(\mathrm{Dis}(E/\mathbf{Q}))$ is even.

Next we shall specialize further to extensions in which the rational prime 2 is no more than tamely ramified. We first prove a local result.

(8.2) LEMMA. *Suppose $F/\mathbf{Q}_2$ is a local extension of the 2-adic rationals which is no more than tamely ramified. Then $\beta\langle F\rangle \in \mathbf{Z}/8\mathbf{Z}$ is well-defined and*

$$\beta\langle F\rangle \equiv \deg(F/\mathbf{Q}_2) \pmod 8.$$

Proof. First there is a Knebusch short exact sequence

$$0 \to W(\mathbf{Z}_2) \to W(\mathbf{Q}_2) \overset{\partial_2}{\to} W(\mathbf{Z}/2\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} \to 0.$$

Since $F/\mathbf{Q}_2$ is no more than tamely ramified we have

$$\partial_2\langle F\rangle = \mathrm{ord}_2(\mathrm{dis}\langle F\rangle) \equiv 0 \pmod 2)$$

and therefore $\langle F\rangle \in W(\mathbf{Z}_2)$, so we can refer to $\beta\langle F\rangle$. We then split F into two extensions, $K/\mathbf{Q}_2$ which is unramified of degree $f \geqq 0$ and F/K which is a totally ramified extension of odd degree $e \geqq 1$. Then $e \cdot f = \deg(F/\mathbf{Q}_2)$.

Since F/K is totally and tamely ramified so it must be given by a polynomial $t^e - \pi$ for some local uniformizer $\pi \in \mathfrak{O}_K$, where $\mathfrak{O}_K$ denotes the ring of integers of K. But e is odd and hence by [**4**, III.4.1] the relative trace form of F/K represents $\langle e\rangle = \langle e\rangle\langle 1_K\rangle \in W(K)$. However, we already have the Witt class $\langle e\rangle \in W(\mathbf{Q}_2)$. Thus

$$T_{F/\mathbf{Q}_2}(1_F) = T_{K/\mathbf{Q}_2}(\langle e\rangle\langle 1_K\rangle) = \langle e\rangle\langle K\rangle = \langle F\rangle \in W(\mathbf{Q}_2).$$

Of course $\langle e\rangle$ and $\langle K\rangle$ both lie in $W(\mathbf{Z}_2)$ and hence

$$\beta\langle F\rangle = (\beta\langle e\rangle)(\beta\langle K\rangle) \in \mathbf{Z}/8\mathbf{Z}.$$

From the definition of van der Blij's invariant we see

$$\beta\langle e\rangle \equiv e \pmod 8$$

while it was noted in [**4**, III.8.1] that

$$\beta\langle K\rangle \equiv \deg(K/\mathbf{Q}_2) = f \pmod 8$$

for unramified local extensions. Thus we have

$$\beta\langle F\rangle \equiv e \cdot f = \deg(F/\mathbf{Q}_2) \pmod 8.$$

We add the following

(8.3) LEMMA. *If $E/\mathbf{Q}$ is an algebraic number field in which 2 is at most tamely ramified, then*

$$\beta\langle E\rangle \equiv \deg(E/\mathbf{Q}) \pmod 8.$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

If 2 is at most tamely ramified in $E/\mathbf{Q}$ then we can write $\mathrm{Dis}(E/\mathbf{Q}) = 4^j \cdot M$ for some $j \geqq 0$ and some odd rational integer M. Observe that $M \equiv 1 \pmod 4$.

(8.4) COROLLARY. *If 2 is no more than tamely ramified in $E/\mathbf{Q}$ then*

$$W_2(\mathbf{Q}, \rho(E)) = 1 \quad \textit{and} \quad (2, \mathrm{Dis}(E/\mathbf{Q}))_2 = h_2(E/\mathbf{Q}).$$

Proof. As $\beta\langle E\rangle \equiv \deg(E/\mathbf{Q}) \pmod 8$, it follows from (8.1) that

$$W_2(\mathbf{Q}, \rho(E)) = 1.$$

Then $\mathrm{Dis}(E/\mathbf{Q}) = M \in \mathbf{Q}^*/\mathbf{Q}^{**}$ for some rational integer $M \equiv 1$ or $5 \pmod 8$. Thus by (4.3),

$$W_2(\mathbf{Q}, \rho(M)) = W_2(\mathbf{Q}, \rho(d)) = 1$$

and the second assertion follows from the identity

$$1 = W_2(\mathbf{Q}, \rho(E)) = (2, d)_2 h_2(E/\mathbf{Q}) W_2(\mathbf{Q}, \rho(d))$$

where $\mathrm{Dis}(E/\mathbf{Q}) = d \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

Recall that Hasse [**8**, p. 502] showed that if 2 is unramified in $E/\mathbf{Q}$, then

$$(2, \mathrm{Dis}(E/\mathbf{Q}))_2 = (-1)^s$$

where $s \geqq 0$ is the number of distinct prime factors of $2\mathfrak{O}_E$ which have even inertia degree. To include the possibility of tame ramification of 2 we now define an integer $t \geqq 0$ to be the number of distinct prime factors of $2\mathfrak{O}_E$ which have odd inertia degree and for which the ramification index is congruent to $\pm 5 \pmod 8$. Now we can state

(8.5) Hasse. *If $E/\mathbf{Q}$ is an algebraic number field in which 2 is no more than tamely ramified, then*

$$(2, \mathrm{Dis}(E/\mathbf{Q}))_2 = (-1)^{s+t} = h_2(E/\mathbf{Q})$$

where $s \geqq 0$ (resp. $t \geqq 0$) denotes the number of distinct prime factors of $2\mathfrak{O}_E$ with even inertia degree (resp. odd inertia degree and with ramification index $\equiv \pm 5 \pmod 8$).

Now the problem with (8.5) lies in the fact that while 2 is unramified in $E/\mathbf{Q}$ if and only if $\mathrm{Dis}(E/\mathbf{Q})$ is odd, we are unable to recognize the tame ramification of 2 from the value of $\mathrm{Dis}(E/\mathbf{Q})$ alone. In other words, we may have $\mathrm{Dis}(E/\mathbf{Q}) = 4^j \cdot M$, $j \geqq 0$ and $M \equiv 1 \pmod 4$ but even so 2 is wildly ramified. We shall take up some examples of this kind in Section 10. We now refer back to (7.4) and close this section by restating (8.4) in terms of Witt class invariants.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

(8.6) COROLLARY. *Suppose that $E/\mathbf{Q}$ is an extension of degree n in which 2 is at most tamely ramified. Let*

$$(-1)^{n(n-1)/2}\,\mathrm{Dis}(E/\mathbf{Q}) = 4^j \cdot N$$

for some $j \geqq 0$ and some odd rational integer N.

1. *If n is odd then* $n \equiv N \pmod 4$ *and*

$$(-1)^{(n-N)/4} = c_2\langle E\rangle.$$

2. *If n is even then* $n \equiv N - 1 \pmod 4$ *and*

$$(-1)^{(n-N+1)/4} = c_2\langle E\rangle.$$

(Note that the modulo 4 congruence conditions on N are equivalent to $(-1)^{n(n-1)/2}N = M \equiv 1 \pmod 4$.)

9. Values of the additive characters. Let K be any algebraic number field. Upon examination of (5.3) we can think of $\gamma_p(X)$ as a function $f(p) \in \mathbf{C}^*$ which to every prime p in K assigns a complex value satisfying

1. $f(p) = 1$ for almost all primes,
2. $f(p) = 1$ for all complex infinite primes,
3. $f(p)^2 = 1$ for all primes where -1 is a local square in the completion $K(p)$
4. $\prod_p f(p) = 1$, and
5. either $f(p)^4 = 1$ for all primes of K or

$$(f(p)\gamma_p\langle 1_K\rangle^{-1})^4 = 1 \text{ for all primes in } K.$$

In 5 the two alternatives are not mutually exclusive. It could happen that $(\gamma_p\langle 1_K\rangle)^4 = 1$.

(9.1) PROPOSITION. *If $f(p) \in \mathbf{C}^*$ is a function which satisfies* 1-5, *then there is a Witt class $X \in W(K)$ with $\gamma_p(X) = f(p)$ for all primes p in K.*

Proof. We offer the following argument based on (5.3). Suppose first that $f(p)^4 = 1$. We need a square class $d \in K^*/K^{**}$ such that

$$f(p)/W_p(K, \rho(d)) = \pm 1$$

for all primes p in K. If we have $f(p)^2 = 1$ already then we just take $d = 1$. Otherwise there is a finite set of primes, having even cardinality, $p_1, \ldots, p_{2k}$, where $f(p_j) = \pm i$. This set is finite by property 1 and is of even cardinality by the reciprocity property 4. In addition, by 3, none of the primes $p_1, \ldots, p_{2k}$ split in the quadratic extension $K(\sqrt{-1})/K$. We appeal to the realization of Hilbert symbols as stated in [**15**, 71:19a, p. 203] to guarantee the existence of $d \in K^*/K^{**}$ with

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$(d, -1)_{p_j} = -1 \quad \text{for } j = 1, \dots, 2k$$

$$(d, -1)_p = 1 \quad \text{for all other primes.}$$

Since $W_p(K, \rho(d))^2 = (-1, d)_p \in \mathbf{Z}^*$ we can be certain that

$$f(p)/W_p(K, \rho(d)) = \pm 1 \quad \text{for all primes } p \text{ in } K.$$

Now we must specify a Witt class $X \in I \subset W(K)$ as follows.

$$\mathrm{rk}(X) \equiv 0 \pmod 2$$

$$\mathrm{dis}(X) = d \in K^*/K^{**}$$

$$c_p(X) = (-2, d)_p f(p)/W_p(K, \rho(d)) \in \mathbf{Z}^*.$$

If K has orderings, then with respect to the order corresponding to a real infinite prime p_∞ we specify

$$\mathrm{sgn}_{p_\infty}(X) = \begin{cases} 0 & \text{if and only if } d > 0,\ c_{p_\infty}(X) = 1 \\ 2 & \text{if and only if } d < 0,\ c_{p_\infty}(X) = -1 \\ 4 & \text{if and only if } d > 0,\ c_{p_\infty}(X) = -1 \\ -2 & \text{if and only if } d < 0,\ c_{p_\infty}(X) = 1. \end{cases}$$

Such a Witt class exists uniquely and clearly by (5.3) $\gamma_p(X) = f(p)$ for all primes p in K.

If $(f(p)\gamma_p\langle 1_K\rangle^{-1})^4 = 1$ we apply the foregoing to find $X \in I \subset W(K)$ with

$$\gamma_p(X) = f(p)\gamma_p\langle 1_K\rangle^{-1}.$$

But then

$$\gamma_p(X + \langle 1_K\rangle) = f(p) \quad \text{for all } p \text{ in } K.$$

Now we comment on the ambiguous situation $(\gamma_p\langle 1_K\rangle)^4 = 1$. In that case we may take our realizing Witt class to have rank 0 or 1 mod 2. We note, however,

(9.2) LEMMA. *If K is an algebraic number field then*

$$(\gamma_p\langle 1_K\rangle)^4 = 1$$

if and only if K is totally complex and for every prime ideal $p|2$ the degree of the local extension $K(p)/\mathbf{Q}_2$ is even.

For example in $K = \mathbf{Q}(\sqrt{-3})/\mathbf{Q}$ we have a single dyadic prime and at that prime $\gamma_p\langle 1_K\rangle = i$. By contrast there are two dyadic primes in $K = \mathbf{Q}(\sqrt{-7})/\mathbf{Q}$ and the values of $\gamma_p\langle 1_K\rangle$ at each of these primes is $\xi = \exp(2\pi i/8)$. Of course we could have $\gamma_p\langle 1_K\rangle = 1$. The simplest example of this is $K = \mathbf{Q}(\sqrt{-1})/\mathbf{Q}$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

We shall consider two viewpoints in giving a brief summary of the relation between additive characters and local root numbers of real orthogonal representations. First we may turn to the integral group ring $\mathbf{Z}[K^*/K^{**}]$. From the embedding $K^*/K^{**} \rightarrow W(K)^*$ there results a ring homomorphism

$$\mathbf{Z}[K^*/K^{**}] \rightarrow W(K) \rightarrow 0.$$

On the other hand

$$K^*/K^{**} \cong \mathrm{Hom}(G(K), O(1))$$

will produce

$$\mathbf{Z}[K^*/K^{**}] \rightarrow R_0(G(K))$$

where $R_0(G(K))$ is the representation ring of the continuous, finite dimensional real orthogonal representations of $G(K)$.

For an element $\alpha \in \mathbf{Z}[K^*/K^{**}]$ let $X(\alpha) \in W(K)$, $\rho(\alpha) \in R_0(G(K))$ denote the associated Witt class and the associated virtual representation respectively. If $\epsilon(\alpha) \in \mathbf{Z}$ is the argumentation of α then

$$\epsilon(\alpha) = \deg(\rho(\alpha)) \quad \text{while} \quad \epsilon(\alpha) \equiv \mathrm{rk}(X(\alpha)) \pmod 2.$$

Then from (6.3) with $K = E$, we can derive the identity

(9.3) COROLLARY. *For* $\alpha \in \mathbf{Z}[K^*/K^{**}]$,

$$\gamma_p(X(\alpha))W_p(K, \rho(\alpha)) = (2, \mathrm{dis}(X(\alpha)))_p(\gamma_p\langle 1_K\rangle)^{\deg\rho(\alpha)}.$$

For the second point of view we consider the Burnside ring, $\mathrm{Burn}(G(K))$, of continuous representations of $G(K)$ as a finite group of permutations. Since a continuous homomorphism $\rho:G(K) \rightarrow S_n$ with image a transitive subgroup corresponds to a relative extension E/K with degree n we can define $\mathrm{Burn}(G(K)) \rightarrow W(K)$ by $\rho \rightarrow \langle E\rangle \in W(K)$, the Witt class of the trace form from E/K. It is not difficult to see that in fact

$$\mathrm{Burn}(G(K)) \rightarrow W(K) \rightarrow 0$$

is a ring epimorphism. Of course there is a ring homomorphism

$$\mathrm{Burn}(G(K)) \rightarrow R_0(G(K)).$$

For $\rho \in \mathrm{Burn}(G(K))$ let $X(\rho) \in W(K)$ be the corresponding Witt class of the virtual trace form. Then from (6.2) we have

(9.4) COROLLARY. *For* $\rho \in \mathrm{Burn}(G(K))$

$$\gamma_p(X(\rho))W_p(K, \rho) = (\gamma_p\langle 1_K\rangle)^{\deg(\rho)}.$$

10. Examples. We shall take up a few examples involving the absolute trace form of an algebraic number field. If $f(t) \in \mathbf{Z}[t]$ is a monic ir-

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

reducible polynomial then there is a simple extension E of $\mathbf{Q}$ defined by $f(t)$, i.e.,

$$E = \mathbf{Q}[t]/(f(t)).$$

While all of the Witt invariants of the absolute trace form of $E/\mathbf{Q}$ and hence the local root numbers $W_l(\mathbf{Q}, \rho(E))$ of a real orthogonal representation $\rho(E)$ of the absolute Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and ultimately the additive characters $\gamma_l\langle E\rangle$, can, in theory, be computed from the coefficients of $f(t)$, we can only present a few examples where these computations are carried out, in practice, with reasonable success. We state our results in the Witt ring formalism. The additive characters $\gamma_l\langle E\rangle$ are then determined by (5.3). The explicitly determined Witt invariants give some basic information on ramification properties of (rational) primes in E, and also on the possibilities of the Galois group of $f(t)$ over $\mathbf{Q}$.

We first fix the notation. For an irreducible polynomial $f(t) \in \mathbf{Q}[t]$, D_f and $\mathrm{Gal}(f)$ denote the discriminant of $f(t)$ and the Galois group of $f(t)$ over $\mathbf{Q}$, respectively. For the associated simple extension $E = \mathbf{Q}[t]/(f(t))$, N stands for its normal closure and $\mathrm{Gal}(N/\mathbf{Q}) = \mathrm{Gal}(f)$. Note that the field discriminant $\mathrm{Dis}(E/\mathbf{Q})$ differs from D_f by a square factor, that is,

$$D_f/\mathrm{Dis}(E/\mathbf{Q}) \in \mathbf{Q}^{**}.$$

We shall begin with some extensions of degree 4 over $\mathbf{Q}$. Choose a square-free rational integer m and set $F = \mathbf{Q}(\sqrt{m})/\mathbf{Q}$. If a, b are rational numbers for which $\sigma = a + b\sqrt{m}$ is not a square in F, then we introduce the degree 4 extension

$$E/\mathbf{Q} = F(\sqrt{\sigma})/F = \mathbf{Q}(\sqrt{a + b\sqrt{m}})/\mathbf{Q}.$$

The results are collected in the following

(10.1) PROPOSITION. *Let $E/\mathbf{Q}$ be the simple extension of degree 4 defined by the irreducible quartic*

$$f(t) = t^4 - 2at^2 + (a^2 - b^2m) \in \mathbf{Q}[t]$$

where m is a fixed square-free rational integer and a, b are rational numbers such that $a + b\sqrt{m}$ is not a square in $\mathbf{Q}(\sqrt{m})$. Then

1. $\mathrm{dis}\langle E\rangle = a^2 - b^2m \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

2. $$c_l\langle E\rangle = \begin{cases} (-1, -m)_l(a, -m(a^2 - b^2m))_l & \text{if } a \neq 0 \\ (-1, -m)_l & \text{if } a = 0 \end{cases}$$

for every prime l in $\mathbf{Q}$, including the infinite prime.

In particular,

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$c_l\langle E\rangle = \begin{cases} (-1, -1)_l(-1, a)_l & \textit{if } a \neq 0 \quad \textit{and} \quad \mathrm{Gal}(f) = C_4 \\ -1)_l(-1, a)_l(m, -a)_l & \textit{if } a \neq 0 \quad \textit{and} \quad \mathrm{Gal}(f) = V_4 \end{cases}$$

3. $$\mathrm{sgn}\langle E\rangle = \begin{cases} 0 & \textit{if } [a < 0, m > 0] \quad \textit{or} \quad a \geqq 0, m < 0] \\ 2 & \textit{if } [a > 0, m \geqq 0 \quad \textit{and} \quad a^2 - b^2m < 0] \\ 4 & \textit{if } [a > 0, m > 0 \quad \textit{and} \quad a^2 - b^2m > 0] \end{cases}$$

4. $$\gamma_l\langle E\rangle = \begin{cases} (-2a, a^2 - b^2m)_l(-a, -m)_l W_l(\mathbf{Q}, \rho(a^2 - b^2m)) & \textit{if } a \neq 0 \\ (2, -m)_l W_l(\mathbf{Q}, \rho(-m)) & \textit{if } a = 0 \end{cases}$$

for every prime l in $\mathbf{Q}$, including the infinite prime.

Furthermore, if 2 is unramified in $E/\mathbf{Q}$, then

5. $m \equiv 1 \pmod 4$, $a \not\equiv 0$, $a^2 - b^2m = M \in \mathbf{Q}^*/\mathbf{Q}^{**}$ *with*

$M \equiv 1 \pmod 4$ *and* $h_2(E/\mathbf{Q}) = (a, -mM)_2 = (2, M)_2$.

Now we shall consider a monic irreducible trinomial of the form

$$f(t) = t^n + at^k + b \in \mathbf{Z}[t] \quad \text{with } n \geqq 2 \text{ and } 1 \leqq k \leqq p - 1.$$

We confine ourselves to the discussions on the following cases:

1. $k = 1$, $n \geqq 2$ arbitrary,
2. $k = 2$, $n \geqq 5$ odd, and
3. $k = 3$, $n = 7$.

In the case $k = 1$, all of the Witt invariants of $\langle E\rangle$ can be computed effectively from $f(t)$. In fact, these computations have been carried out by [**4**, VI] for n odd, and by [**16**, Appx. II] for n arbitrary. The results are formulated in the Witt ring formalism as follows.

(10.2) PROPOSITION. *Let $f(t) = t^n + at + b \in \mathbf{Z}[t]$ be an irreducible trinomial of degree $n \geqq 2$. Then the following are valid.*

1. $$\mathrm{dis}\langle E\rangle = (-1)^{n(n-1)/2}D_f = \begin{cases} n^nb^{n-1} + (n-1)^{n-1}a^n & \textit{if } n \equiv 1 \pmod 2 \\ n^nb^{n-1} - (n-1)^{n-1}a^n & \textit{if } n \equiv 0 \pmod 2. \end{cases}$$

2. $$c_l\langle E\rangle = \begin{cases} (\mathrm{dis}\langle E\rangle, 1 - n)_l & \textit{if } n \equiv 1 \pmod 2 \\ (\mathrm{dis}\langle E\rangle, -n)_l & \textit{if } n \equiv 0 \pmod 2 \end{cases}$$

for every prime l in $\mathbf{Q}$, including the infinite prime.

3. $$\mathrm{sgn}\langle E\rangle = \begin{cases} 0 & \textit{if } \mathrm{dis}\langle E\rangle > 0 \quad \textit{and} \quad n \equiv 0 \pmod 2 \\ 1 & \textit{if } \mathrm{dis}\langle E\rangle > 0 \quad \textit{and} \quad n \equiv 1 \pmod 2 \\ 2 & \textit{if } \mathrm{dis}\langle E\rangle < 0 \quad \textit{and} \quad n \equiv 0 \pmod 2 \\ 3 & \textit{if } \mathrm{dis}\langle E\rangle < 0 \quad \textit{and} \quad n \equiv 1 \pmod 2). \end{cases}$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Combining (10.2) with (8.6), we obtain

(10.3) COROLLARY. *Under the same hypotheses as in* (10.2), *assume that* 2 *is at most tamely ramified in* $E/\mathbf{Q}$. *Then the following hold.*

1. $\mathrm{dis}\langle E\rangle = (-1)^{n(n-1)/2}D_f = 4^j \cdot N$

for some integer $j \geqq 0$ *and some odd integer* N. *In particular*, $N = \mathrm{dis}\langle E\rangle \in \mathbf{Q}^*/\mathbf{Q}^{**}$.

2. *If* n *is odd, then* $n \equiv N \pmod 4$ *and*

$$(-1)^{(n-N)/4} = (N, 1-n)_2 = c_2\langle E\rangle.$$

3. *If* n *is even, then* $n \equiv N - 1 \pmod 4$ *and*

$$(-1)^{(n-N+1)/4} = (N, -n)_2 = c_2\langle E\rangle.$$

Note that properties listed in (10.3) are necessary conditions for 2 to be at most tamely ramified in E. Thus, if any one of the conditions is not satisfied then 2 will be wildly ramified in E.

For irreducible trinomials

$$f(t) = t^n + at^k + b \in \mathbf{Z}[t] \quad \text{with } n \geqq 5 \text{ odd and } k \geqq 2$$

the computations of the Witt invariants of $\langle E\rangle$ become increasingly involved. We state our results for these cases without proofs.

(10.4) PROPOSITION. *Let* $f(t) = t^n + at^2 + b \in \mathbf{Z}[t]$ *be an irreducible trinomial of odd degree* $n \geqq 5$. *Then the following are valid.*

1. $\mathrm{dis}\langle E\rangle = (-1)^{n(n-1)/2}D_f = 4(n-2)^{n-2}a^nb + n^nb^{n-1}$.

2. $c_l\langle E\rangle = (n\,\mathrm{dis}\langle E\rangle, -2(n-2))_l$

for every prime l *in* $\mathbf{Q}$, *including the infinite prime.*

$$3.\ \mathrm{sgn}\langle E\rangle = \begin{cases} 1 & \textit{if } \mathrm{dis}\langle E\rangle > 0 \\ 3 & \textit{if } \mathrm{dis}\langle E\rangle < 0. \end{cases}$$

Furthermore, assume that 2 *is at most tamely ramified in* $E/\mathbf{Q}$. *Then*

4. $\mathrm{Dis}(E/\mathbf{Q}) = 4^j \cdot N$ *for some integer* $j \geqq 0$ *and an odd integer* N *such that* $N = \mathrm{dis}\langle E\rangle \in \mathbf{Q}^*/\mathbf{Q}^{**}$, $N \equiv n \pmod 4$ *and*

$$(-1)^{(n-N)/4} = c_2\langle E\rangle = (n\,\mathrm{dis}\langle E\rangle, -2(n-2))_2.$$

Now we consider a septimic trinomial of the form

$$f(t) = t^7 + at^3 + b \in \mathbf{Z}[t].$$

(10.5) PROPOSITION. *Let* $f(t) = t^7 + at^3 + b \in \mathbf{Z}[t]$ *be an irreducible septimic trinomial over* $\mathbf{Q}$. *Then the following assertions hold*:

1. $\mathrm{dis}\langle E\rangle = (-1)^{n(n-1)/2}D_f = 7^7b^6 + 3^34^4a^7b^2$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

2. $c_l\langle E\rangle = (-3, \operatorname{dis}\langle E\rangle)_l$

for every prime l in $\mathbf{Q}$, including the infinite prime.

3. $\operatorname{sgn}\langle E\rangle = \begin{cases} 1 & \textit{if } \operatorname{dis}\langle E\rangle > 0 \\ 3 & \textit{if } \operatorname{dis}\langle E\rangle < 0. \end{cases}$

Furthermore, assume that 2 is no more than tamely ramified in $E/\mathbf{Q}$. Then

4. $\operatorname{dis}\langle E\rangle = -D_f = 4^j \cdot N$ *for some integer $j \geqq 0$ and an odd integer $N \equiv 7 \pmod 8$.*

Proof. Only statement 4 needs an explanation. To show that $N \equiv 7 \pmod 8$, we only need the observation that $N \equiv 7 \equiv 3 \pmod 4$ and therefore $c_2\langle E\rangle = (-3, N)_2 = 1$. Since

$$(-1)^{(7-N)/4} = c_2\langle E\rangle$$

it now follows that $N \equiv 7 \pmod 8$.

Continuing along in the same vein, it seems reasonable to call for the determination of the invariants of the Witt class of the absolute trace form of the algebraic number field E defined by an irreducible trinomial $f(t) = t^n + at^k + b \in \mathbf{Z}[t]$ in general. In particular, for $n = p$ an odd prime, the most subtle invariant of $\langle E\rangle$ is the stable Hasse-Witt invariant $c_l\langle E\rangle$ at a rational prime l, and should take a reasonably simple form. We should state this as

(10.6) QUESTION. *Let $f(t) = t^p + at^k + b \in \mathbf{Z}[t]$ be an irreducible trinomial of prime degree $p \geqq 5$ and $1 \leqq k \leqq p - 1$. Then is*

$$c_l\langle E\rangle = (p \operatorname{dis}\langle E\rangle, k(k - p))_l$$

for every prime l in $\mathbf{Q}$, including the infinite prime?

(This is true for $k = 1, 2$ and if $p = 7$ also for $k = 3$.)

The absolute trace form of the algebraic number field E defined by a polynomial of the type

$$f(t) = t^n + at^k + \ldots + b \in \mathbf{Z}[t]$$

where n, k are positive integers such that $k \leqq (n + 1)/3$, was studied in [**19**]. The stable Hasse-invariants $c_l\langle E\rangle$ and the additive characters $\gamma_l\langle E\rangle$ could be determined explicitly incorporating the results in [**19**].

For irreducible polynomials of odd prime degree $f(t) \in \mathbf{Z}[t]$, explicitly determined Witt invariants would produce the first screening test in deciding the solvability of the Galois group $\operatorname{Gal}(f)$. For the possibilities of $\operatorname{Gal}(f)$, we have

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

(10.7) LEMMA ([**6**] and [**2**]). *Let $f(t) \in \mathbf{Z}[t]$ be an irreducible polynomial of prime degree $p \geqq 5$. Then the possible Galois groups*, Gal(f), *are the following*:

1. Gal(f) *is solvable* (*so* Gal(f) *is a Frobenius group F_{pr} of degree p with* $r|p - 1$).

2. Gal(f) $= A_p$ *or* S_p.

3. Gal(f) $= PSL(2, 7)$ *if* $p = 7$.

4. Gal(f) $= PSL(2, 11)$ *or* M_{11} *if* $p = 11$.

5. $PSL(2, p - 1) \subseteq$ Gal(f) $\subseteq P\Gamma L(2, p - 1)$ *if* $p = 1 + 2^e > 5$ *is a Fermat prime.*

In particular, if $p \neq 7, 11$ *or a Fermat prime* >5, *then* Gal(f) *is either solvable or* A_p *or* S_p.

Now we add some trace form considerations. The knowledge of the stable Hasse-Witt invariants of the Witt class of the absolute trace form of the simple extension $E = \mathbf{Q}[t]/(f(t))$ contains significant information about the Galois group of $f(t)$. In fact, we have

(10.8) THEOREM. *Let $f(t) \in \mathbf{Z}[t]$ be any irreducible polynomial of prime degree $p \geqq 5$.*

1. *If* $p \equiv 3 \pmod 4$ *and if there is a rational prime* $l \equiv 1 \pmod 8$ *with* $c_l\langle E\rangle = -1$, *then* Gal(f) *is not solvable.*

2. *If* $p \equiv 5 \pmod 8$ *and if there is a rational prime* $l \equiv 1 \pmod 4$ *with* $c_l\langle E\rangle = -1$, *then* Gal(f) *is not solvable.*

3. *If* $p \equiv 1 \pmod 8$ *and if there is any rational prime l with* $c_l\langle E\rangle = -1$, *then* Gal(f) *is not solvable.*

Proof. We examine the argument of [**4**, VI.3] carefully. Let N be the normal closure of E over $\mathbf{Q}$. If Gal(f) is solvable then Gal(f) is a Frobenius group F_{pr} with $r|p - 1$. Let $2^t\|r$ and let L be the unique subfield of L of degree 2^t over $\mathbf{Q}$. Then by [**4**, VI.3.7], we have

$$\langle E\rangle = \langle 1\rangle + ((p - 1)/2^t)\langle L\rangle, \quad \mathrm{sgn}\langle E\rangle = 1 \text{ or } p$$

and

$$\mathrm{dis}\langle E\rangle \neq 1 \text{ in } \mathbf{Q}^*/\mathbf{Q}^{**} \quad \text{if } (p - 1)/2^t \equiv 1 \pmod 2$$
$$\mathrm{dis}\langle E\rangle = 1 \text{ in } \mathbf{Q}^*/\mathbf{Q}^{**} \quad \text{if } (p - 1)/2^t \equiv 0 \pmod 2.$$

1. Assume that $p \equiv 3 \pmod 4$. Then r could be odd, in which case $\langle E\rangle = p\langle 1\rangle$ and $c_l\langle E\rangle = 1$ for every prime $l \equiv 1 \pmod 8$. If $t = 1$ then $L/\mathbf{Q}$ is quadratic and we find

$$\mathrm{dis}\langle L\rangle = -D_f = \mathrm{dis}\langle E\rangle \neq 1 \quad \text{in } \mathbf{Q}^*/\mathbf{Q}^{**}$$

and we easily compute

$$c_l\langle E\rangle = \begin{cases} (-2, -D_f)_l & \text{if } p \equiv 3 \pmod 8 \\ (2, -D_f)_l & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

for every prime l in $\mathbf{Q}$. Obviously, $c_l\langle E\rangle = 1$ for all primes $l \equiv 1 \pmod 8$. Therefore, if there is at least one prime $l \equiv 1 \pmod 8$ for which $c_l\langle E\rangle = -1$, then $\mathrm{Gal}(f)$ cannot be a solvable group.

2. Assume that $p \equiv 5 \pmod 8$. We use [**4**, VI.3.10]. In this case, we have only to consider $t = 1$ or $t = 2$. If $t = 1$, then $\langle E\rangle = \langle 1\rangle + 2\langle L\rangle$ and $c_l\langle E\rangle = (-1, \mathrm{dis}\langle E\rangle)_l$ for every prime l in $\mathbf{Q}$. Clearly, $c_l\langle E\rangle = 1$ for all primes $l \equiv 1 \pmod 4$. Now assume that $t = 2$. Then $\langle E\rangle = \langle 1\rangle + \langle L\rangle$, and $c_l\langle L\rangle = (-1, a)_l$ for some rational number a (cf. Proposition (10.1)). It immediately follows that $c_l\langle E\rangle = c_l\langle L\rangle = 1$ for all primes $l \equiv 1 \pmod 4$. Therefore, if there is at least one prime $l \equiv 1 \pmod 4$ for which $c_l\langle E\rangle = -1$, then $\mathrm{Gal}(f)$ cannot be a solvable group.

3. Now assume that $p \equiv 1 \pmod 8$. If $(p - 1)/2^t$ is odd then $L/\mathbf{Q}$ is a cyclic extension of degree $2^t \geqq 8$. For such extensions it is known that $\mathrm{Dis}(L/\mathbf{Q}) = \mathrm{dis}\langle L\rangle$ is a norm from $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$. Thus

$$(2, \mathrm{Dis}(L/\mathbf{Q}))_l \equiv 1$$

for all primes l in $\mathbf{Q}$. On the other hand, Kahn [**10**] showed that the second Stiefel-Whitney class of the regular representation of C_{2^t}, the cyclic group of order 2^t, is trivial if $t \geqq 3$. Then by Serre's Theorem, we have

$$h_l(L/\mathbf{Q}) = (2, \mathrm{Dis}(L/\mathbf{Q}))_l \equiv 1.$$

Since $\deg(L/\mathbf{Q}) \equiv 0 \pmod 8$, it follows that

$$c_l\langle E\rangle = c_l\langle L\rangle \equiv 1.$$

If $(p - 1)/2^t$ is even then we write

$$(p - 1)/2^t = 2^i(2m + 1) \quad \text{for some } m \geqq 0.$$

Now it could happen that $\deg(L/\mathbf{Q}) = 4$. But if so, $i \geqq 1$ and $c_l(2\langle L\rangle) \equiv 1$ for a cyclic extension of degree 4. If $\deg(L/\mathbf{Q}) = 2$ then $i \geqq 2$ and surely $c_l(4\langle L\rangle) \equiv 1$ for a cyclic extension of degree 2. Therefore, if there is any prime l with $c_l\langle E\rangle = -1$, then $\mathrm{Gal}(f)$ cannot be a solvable group.

The point of the above discussions is that (10.7) combined with the explicit knowledge of stable Hasse-Witt invariants $c_l\langle E\rangle$ asserts that $\mathrm{Gal}(f)$ must be one of the nonsolvable groups listed in (10.7).

We should note

(10.9) COROLLARY. *Let $f(t) \in \mathbf{Z}[t]$ be a monic irreducible polynomial of prime degree $p \equiv 5 \pmod 8$ whose Galois group is solvable. If either*

1. $\mathrm{sgn}\langle E\rangle = 1$ *and* $D_f \equiv 1 \pmod 8$, *or*
2. $\mathrm{sgn}\langle E\rangle = p$ *and* $D_f \equiv 5 \pmod 8$,

then there are an odd number of rational primes $l \equiv 3 \pmod 4$ for which $c_l\langle E\rangle = -1$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Furthermore, N contains a unique cyclic subfield $L/\mathbf{Q}$ of degree 2 if D_f is a square, and of degree 4 if D_f is not a square, and these are exactly the rational primes $l \equiv 3 \pmod 4$ that ramify in $L/\mathbf{Q}$.

(10.10) *Examples.* 1. Let

$$f(t) = t^5 - t^4 + 2t^3 - 5t^2 + t + 3 \in \mathbf{Z}[t].$$

Then $f(t)$ is irreducible over $\mathbf{Q}$ with $\mathrm{Gal}(f) = D_5$. We see that

$$\mathrm{sgn}\langle E\rangle = 1 \quad\text{and}\quad D_f = 3^4 79^2 \equiv 1 \pmod 8.$$

The primes 3 and 79 are both congruent to 3 (mod 4). However, only $79 \equiv -1 \pmod 5$ has the property that $c_{79}\langle E\rangle = -1$.

2. Consider the polynomial

$$f(t) = t^{13} - 8t^{12} + 16t^{11} - 27t^{10} + 38t^9 - 36t^8 + 22t^7 - 12t^6$$
$$+ 13t^5 - 19t^4 + 21t^3 - 15t^2 + 6t - 1 \in \mathbf{Q}[t].$$

Then $f(t)$ is irreducible over $\mathbf{Q}$ and $\mathrm{Gal}(f) = D_{13}$. We can compute that

$$\mathrm{sgn}\langle E\rangle = 1 \quad\text{and}\quad D_f = 5^4 41^2 263^6 \equiv 1 \pmod 8).$$

Only 263 is congruent to 3 (mod 4), and hence $c_{263}\langle E\rangle = -1$.

Finally we would like to discuss the question which suggested the need for the results (8.4) and (8.6). In [**4**, III.6] it was shown that every Witt class in $W(\mathbf{Q})$ with nonnegative signature can be represented by the absolute trace form of some algebraic number field. Then, upon reflection and consideration of some examples, the following is suggested, which we may state as a

(10.11) CONJECTURE. *If $X \in W(\mathbf{Q})$ is a Witt class for which* $\mathrm{sgn}(X) \geqq 0$ *and if l is a finite rational prime for which $\partial_l(X) = 0$ in $W(\mathbf{Z}/l\mathbf{Z})$, then there is an extension $E/\mathbf{Q}$ in which l is unramified and for which $\langle E\rangle = X$.*

In fact, this was raised as a further question in [**4**, III.9]. In trying to verify the statement in some elementary cases for which

$$\partial_2(X) = \mathrm{ord}_2(\mathrm{dis}(X)) \equiv 0 \pmod 2,$$

we came to realize that some relation between the Witt class invariants of the absolute trace form and the ramification of 2 was missing. This lead us to the discussions in Section 8, in particular, to (8.4) and (8.6).

For example, $0 \in W(\mathbf{Q})$ is obviously represented by the trace form from $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$. Yet 2 is wildly ramified in this extension. Since $\beta(0) = 0 \in \mathbf{Z}/8\mathbf{Z}$ we see by (8.6) that if $E/\mathbf{Q}$ is an extension in which 2 is unramified and for which $\langle E\rangle = 0 \in W(\mathbf{Q})$, then

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$$\deg(E/\mathbf{Q}) \equiv 0 \pmod 8).$$

Such an extension does exist. Less obvious, however, is the case of $2\langle 1\rangle$. Here the van der Blij invariant is 2 (mod 8) so the degree of such an extension $E/\mathbf{Q}$, in which 2 is unramified and for which $\langle E\rangle = 2\langle 1\rangle \in W(\mathbf{Q})$, must therefore be congruent to 2 (mod 8). No quadratic extension can represent $2\langle 1\rangle$. So the least possible degree of such an extension is 10.

We can give the affirmative answer to (10.11) with $l = 2$ and $X = 2\langle 1\rangle$.

(10.12) THEOREM. (a) *There exist monic irreducible polynomials* $f(t) \in \mathbf{Q}[t]$ *of degree* 5 *satisfying the following properties*:

1. D_f *is a square of an odd rational integer.*
2. $f(t)$ *has only one real root.*
3. $\mathrm{Gal}(f) = A_5$.

(b) *Let* $f(t) \in \mathbf{Q}[t]$ *be such a quintic polynomial. Let* $\{\alpha_i | i = 1, \dots, 5\}$ *be its roots in* $\mathbf{C}$. *Define a polynomial*

$$P_{10}(t) = \prod_{1 \leqq i < j \leqq 5} \{t - (\alpha_i + \alpha_j)\}.$$

Then

1. $P_{10}(t)$ *is irreducible over* $\mathbf{Q}$, *and*

$$E = \mathbf{Q}[t]/(P_{10}(t))$$

is a simple extension of degree 10 *over* $\mathbf{Q}$.

2. $\mathrm{Gal}(P_{10}) = A_5$.
3. $\mathrm{dis}\langle E\rangle = -1 \in \mathbf{Q}^*/\mathbf{Q}^{**}$.
4. $\mathrm{sgn}\langle E\rangle = 2$.
5. 2 *is unramified in* E.
6. $c_2\langle E\rangle = c_\infty\langle E\rangle = -1$, *and* $c_l\langle E\rangle = 1$ *for all odd primes* l *in* $\mathbf{Q}$.
7. $\langle E\rangle$ *represents the Witt class* $2\langle 1\rangle$ *in* $W(\mathbf{Q})$.

Proof. (a) We give some examples of quintic polynomials with the required properties. Put $F = \mathbf{Q}[t]/(f(t))$.

	$f(t)$	D_f	$\mathrm{sgn}\langle F\rangle$	$\mathrm{Gal}(f)$
I	$t^5-t^4+2t^3-3t^2+5t+1$	$17^2 59^2$	1	A_5
II	$t^5+t^4+4t^3-3t^2-3t+3$	$3^4 5^2 41^2$	1	A_5
III	$t^5+t^4-2t^3+t^2+t+1$	$3^4 23^2$	1	A_5

(b) 1. This was proved in **[9]**.

2. This follows from Proposition (I.1.6) in **[2]**.

3. $P_{10}(t)$ and its discriminant $D_{P_{10}}$ (and hence $\mathrm{dis}\langle E\rangle = -D_{P_{10}}$) are given as follows:

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

$f(t)$	$P_{10}(t)$	$D_{P_{10}}$
I	$t^{10}-4t^9+12t^8-25t^7+28t^6-43t^5+45t^4-8t^3-99t^2+109t-53$	$17^6 59^8 6427^2$
II	$t^{10}+4t^9+18t^8+37t^7+82t^6+51t^5-11t^4-164t^3-429t^2-189t-57$	$3^{22}5^6 7^2 23^2 41^6 313$
III	$t^{10}+4t^9-13t^7-4t^6+35t^5-27t^4-24t^3+27t^2+9t-9$	$3^{20}23^6 31^4$

In all cases, $P_{10}(t)$ is irreducible over $\mathbf{Q}$, and $\operatorname{dis}\langle E\rangle = -1$ in $\mathbf{Q}^*/\mathbf{Q}^{**}$.

4. As $f(t)$ has two pairs of conjugate imaginary roots, from its definition $P_{10}(t)$ has exactly two real roots. So $\operatorname{sgn}\langle E\rangle = 2$.

5. Since $D_{P_{10}}$ is a square of an odd rational integer, 2 is definitely unramified in $E/\mathbf{Q}$.

6. For $c_2\langle E\rangle$ use (8.6), taking $n = 10$ and $N = -1$. Then $c_2\langle E\rangle = (-1)^3 = -1$. For $c_\infty\langle E\rangle$ use (7.5) with $N = -1$. Then $c_2\langle E\rangle c_\infty\langle E\rangle = 1$ so that $c_\infty\langle E\rangle = -1$. The proof of $c_l\langle E\rangle = 1$ for all odd primes l is more involved. It suffices to show that $h_l(E/\mathbf{Q}) \equiv 1$ for all odd primes, since

$$c_l\langle E\rangle = h_l(E/\mathbf{Q})(-1, -1)_l = h_l(E/\mathbf{Q}).$$

We need the results of [**5**] and [**16**], which we recall briefly. Over the classifying space, $B(S_n)$, of S_n, there is the canonical n-plane bundle $l_n \to B(S_n)$. Since $S_n \subset O(n)$ there is a map $B(S_n) \to BO(n)$ unique up to homotopy. Then from the universal n-plane bundle $\xi_n \to BO(n)$ we simply pull back $l_n \to B(S_n)$. Now

$$H^*(B(S_n); \mathbf{Z}/2\mathbf{Z}) \cong H^*(S_n; \mathbf{Z}/2\mathbf{Z})$$

and thus the Stiefel-Whitney classes

$$s_j(l_n) \in H^j(B(S_n); \mathbf{Z}/2\mathbf{Z})$$

can be regarded as elements of $H^j(S_n; \mathbf{Z}/2\mathbf{Z})$. In particular,

$$s_2(l_n) \in H^2(S_n; \mathbf{Z}/2\mathbf{Z})$$

is e^*s_n in Serre's notation. If K is a field of characteristic $\neq 2$, then

$$H^1(G(K); \mathbf{Z}/2\mathbf{Z}) \cong K^*/K^{**} \quad \text{and} \quad H^2(G(K); \mathbf{Z}/2\mathbf{Z}) \cong Br_2(K).$$

Now a separable extension, F/K, of degree n, corresponds to a continuous homomorphism $\rho: G(K) \to S_n$ onto a transitive subgroup. In fact, this is $\rho(F)$. Then

$$\rho(F)^*(s_1(l_n)) \in H^1(G(K); \mathbf{Z}/2\mathbf{Z})$$

is the discriminant of F/K, $\operatorname{Dis}(F/K)$ (not the discriminant of $\langle F\rangle$), and

$$\rho(F)^*(s_2(l_n)) \in H^2(G(K); \mathbf{Z}/2\mathbf{Z}) \cong Br_2(K)$$

is not quite the classical Hasse invariant, but needs to be corrected by $(2, \operatorname{Dis}(F/K))$. (See [**16**, Theorem 1 and Remarks].)

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

Now we are ready to prove the assertion. Since S_5 is 2-transitive, there is an embedding $i:S_5 \hookrightarrow S_{10}$ whose image is a transitive subgroup. This induces the homomorphism

$$i^*:H^*(S_{10};\ \mathbf{Z}/2\mathbf{Z}) \rightarrow H^*(S_5;\ \mathbf{Z}/2\mathbf{Z}).$$

Now we need the following facts which were pointed out by V. Snaith:

$$i^*(s_1(l_{10})) = s_1(l_5), \quad \text{and}$$
$$i^*(s_2(l_{10})) = s_1(l_5) \cup s_1(l_5) = s_1(l_5)^2.$$

If Gal(f) is a 2-transitive subgroup of S_5, then $\rho(F):G(\mathbf{Q}) \rightarrow S_5$ is a homomorphism onto a 2-transitive subgroup. If we compose this with the embedding $i:S_5 \hookrightarrow S_{10}$ we obtain

$$\chi_F:G(\mathbf{Q}) \rightarrow S_{10}$$

whose image is a transitive subgroup of S_{10}, and this corresponds to an extension $E/\mathbf{Q}$ of degree 10. If we note that

$$\chi^*:H^*(S_{10};\ \mathbf{Z}/2\mathbf{Z}) \rightarrow H^*(G(\mathbf{Q});\ \mathbf{Z}/2\mathbf{Z})$$

factors into

$$H^*(S_{10};\ \mathbf{Z}/2\mathbf{Z}) \xrightarrow{i^*} H^*(S_5;\ \mathbf{Z}/2\mathbf{Z}) \xrightarrow{\rho(F)^*} H^*(G(\mathbf{Q});\ \mathbf{Z}/2\mathbf{Z})$$

we can immediately see that

$$\mathrm{Dis}(E/\mathbf{Q}) = \mathrm{Dis}(F/\mathbf{Q}) = D_f \in \mathbf{Q}^*/\mathbf{Q}^{**}.$$

Furthermore, at each prime l in $\mathbf{Q}$, we have

$$h_l(E/\mathbf{Q}) = (2, D_f)_l(-1, D_f)_l = (-2, D_f)_l.$$

Now we know that the polynomial $P_{10}(t)$ defines the extension $E/\mathbf{Q}$. Since Gal(f) $= A_5$ and D_f is a square of an odd integer, Dis($E/\mathbf{Q}$) is also a square, while

$$h_l(E/\mathbf{Q}) = (-2, D_f)_l \equiv 1$$

for all odd primes l in $\mathbf{Q}$.

7. We have constructed E in such a way that the Witt class of $\langle E\rangle$ indeed represents $2\langle 1\rangle$ in $W(\mathbf{Q})$.

We close this section with

(10.13) *Remark.* With the assumptions and notations of (10.12) in force, if Gal(f) is a 2-transitive subgroup of S_5, then

$$\begin{aligned} W_l(\mathbf{Q}, \rho(E) - \rho(F)) &= (-2, D_f)_l\, h_l(F/\mathbf{Q}) \\ &= h_l(E/\mathbf{Q})\, h_l(F/\mathbf{Q}) \end{aligned}$$

for every prime l in $\mathbf{Q}$.

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press

References

1. F. Van der Blij, *An invariant of quadratic forms* mod 8, Indag. Math. *21* (1959), 291-293.
2. A. Bruen, C. U. Jensen and N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory *24* (1986), 305-359.
3. J. W. S. Cassels, Über die Äquivalenz 2-*adischer quadratischer Formen*, Comment. Math. Helv. *37* (1962), 61-64.
4. P. E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, Series in Pure Math. *2* (World Scientific Publishing Co., Singapore, 1984).
5. P. Deligne, *Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale*, Invent. Math. *35* (1976), 299-316.
6. W. Feit, *Some consequences of the classification of finite simple groups*, AMS Proc. Symposia in Pure Math. *37* (1980), 175-181.
7. A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, Jour. Reine Angew. Math. *360* (1985), 351-360.
8. H. Hasse, *Number theory*, Grundlehren der math. Wissenschaften Bd. *229* (Springer-Verlag, Berlin-Heidelberg-New York, 1980).
9. C. U. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory *15* (1982), 347-375.
10. B. Kahn, *La deuxième classe de Stiefel-Whitney d'une représentation régulière I, II*, C.R. Acad. Sc. Paris, Serie I *297* (1983), 313-316 and (1983), 573-576.
11. M. Knebusch and W. Scharlau, *Quadratische Formen und quadratische Reziprozitätsgesetzè über algebraischen Zahlkörpern*, Math. Z *121* (1971), 346-368.
12. S. Lang, *Algebraic number theory* (Addison-Wesley Publishing Co., Reading, Massachusetts, 1968).
13. W. Ledermann, *An arithmetical property of quadratic forms*, Comment. Math. Helv. *33* (1959), 34-37.
14. J. W. Milnor and D. Husemoeller, *Symmetric bilinear forms*, Ergebnisse der Mathematik *73* (Springer-Verlag, Berlin-Heidelberg-New York, 1973).
15. O. T. O'Meara, *Introduction to quadratic forms*, Second Edition, Grundlehren der math. Wissenschaften 117 (Springer-Verlag, Berlin-Heidelberg-New York, 1971).
16. J.-P. Serre, *L'invariant de Witt de la* $\mathrm{Tr}(X^2)$, Comment. Math. Helv. *59* (1984), 651-676.
17. W. Scharlau, *Quadratic reciprocity laws*, J. Number Theory *4* (1972), 78-97.
18. J. Tate, *Local constants, algebraic number fields* (Academic Press Inc., New York, 1977), 89-131.
19. N. Vila, *Sobre la realitzacio de les extensions contrals del grup alternat com a grup de Galois sobre el cos dels racionals*, Thesis Univ. Auton. Barcelone (1983).
20. A. Weil, *Sur certains groupes d'opérateurs unitares*, Acta Math. *111* (1964), 143-211.

Louisiana State University,
Baton Rouge, Louisiana;
Queen's University,
Kingston, Ontario

https://doi.org/10.4153/CJM-1988-024-x Published online by Cambridge University Press