ILLINOIS JOURNAL OF MATHEMATICS
Volume 35, Number 1, Spring 1991

A GENERALIZATION OF FRÖHLICH'S THEOREM TO WILDLY RAMIFIED QUATERNION EXTENSIONS OF Q

BY

SEYONG KIM

1. Introduction

Let N/K be a finite normal extension of number fields and let $G = \mathrm{Gal}(N/K)$. By E. Noether's theorem (cf. [5, p. 26–27]), the ring of integers o_N of N is projective as a G-module if and only if N/K is at most tamely ramified. In [14], M. Taylor proved that in this case, $(o_N) - [K: \mathbf{Q}](\mathbf{Z}[G]) = W_{N/K}$ where (o_N) is the class of o_N in $K_0(\mathbf{Z}[G])$ and $W_{N/K}$ is the Cassou-Noguès Fröhlich class of N/K (cf. [2, p. 18–19], [5]). The group $K_0(\mathbf{Z}[G])$ is the Grothendieck group of all finitely generated G-modules of finite projective dimension and the class $W_{N/K}$ is defined by means of the Artin root numbers of the irreducible symplectic representations of G.

Let rank: $K_0(\mathbf{Z}[G]) \to \mathbf{Z}$ be the homomorphism by

$$\mathrm{rank}((A)) = \mathrm{rank}_{\mathbf{Q}[G]} \mathbf{Q} \otimes_{\mathbf{Z}} A$$

if A is finitely generated and of finite projective dimension. The class group $\mathrm{Cl}(\mathbf{Z}[G])$ of G is defined to be the kernel of rank. In [3], T. Chinburg defined Galois invariants $\Omega(N/K, i)$ of N/K in $\mathrm{Cl}(\mathbf{Z}[G])$ and proved that $\Omega(N/K, 2) = (o_N) - [K: \mathbf{Q}](\mathbf{Z}[G])$ for all N/K which are at most tamely ramified.

Since both classes, $\Omega(N/K, 2)$ and $W_{N/K}$, are defined for all N/K, and not only for those which are tamely ramified, one may ask the following question.

QUESTION (Chinburg [3]). Is $\Omega(N/K, 2) = W_{N/K}$ for all N/K?

Here we will prove the following result.

THEOREM 1. *Suppose that $K = \mathbf{Q}$ and that G is isomorphic to the quaternion group H_8 of order eight. If there are at least two places over the prime 2 in N then $\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}}$.*

The techniques of this paper apply as well to the case in which there is exactly one place over the prime 2 in N. We believe that further computation will determine whether the conclusion of the theorem holds in this case.

Received December 6, 1988

If the prime 2 is at most tamely ramified in N then it is unramified and there exist at least two places over the prime 2. In this case Theorem 1 was proved by A. Fröhlich in [6]. Fröhlich's theorem began the line of development leading to Taylor's theorem; see Fröhlich's book [5, Chapter I]. Theorem 1 is a step towards proving $\Omega(N/K, 2) = W_{N/K}$ for all N/K, including those which are wildly ramified.

The first step in proving Theorem 1 is to prove a general formula for $\Omega(N/K, 2)$ which is useful for computation; see Proposition 2.4 and the remark following it.

Theorem 1 will be proved by combining the ideas from Fröhlich's original proof for tamely ramified H_8-extensions of $\mathbf{Q}$, as presented in J. Martinet's paper [7], with the ideas of Chinburg's paper [3]. The key idea will be defining o'_N, a projective G-module which has finite index in o_N, which can be used to compare $\Omega(N/\mathbf{Q}, 2)$ with $W_{N/\mathbf{Q}}$.

This paper is based on my Ph.D. thesis. I would like to thank my thesis advisor, Ted Chinburg, for his help and guidance.

II. $\Omega(N/K, 2)$

Let N/K be a finite normal extension of number fields with $G = \mathrm{Gal}(N/K)$. In this section we define o'_N, a projective G-module which has finite index in o_N, in order to compare $\Omega(N/\mathbf{Q}, 2)$ with $W_{N/\mathbf{Q}}$ when $G = \mathrm{Gal}(N/\mathbf{Q}) \cong H_8$. In general, $\Omega(N/K, 2)$ will be the sum of the class $(o'_N) - [K: \mathbf{Q}](\mathbf{Z}[G])$ in $\mathrm{Cl}(\mathbf{Z}[G])$ with factors indexed by the places of K which are wildly ramified in N, these factors depending however on the choice of o'_N; see Proposition 2.4 and the remark following it.

For each finite place w of K, let $v = v(w)$ be a place of N lying over w and define o'_v as follows.

o'_v = a free $o_w[G_v]$-module which has finite index in o_v if N/K is wildly ramified at v.
$o'_v = o_v$ otherwise.

Here, N_v is the completion of N at the place v, o_v (resp. o_w) is the ring of integers in N_v (resp. K_w) and G_v is the decomposition group of v.

For all G_v-modules A we define $\mathrm{Ind}_{G_v}^G A = \mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} A$. If $v = v(w)$ and A is a submodule of N_v, we may regard $\mathrm{Ind}_{G_v}^G A$ as a G-submodule of $\oplus_{v'|w} N_{v'}$ via the natural isomorphism

$$\mathrm{Ind}_{G_v}^G N_v = \mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} N_v \cong \bigoplus_{v'|w} N_{v'}.$$

We regard N as a submodule of $\oplus_{v'|w} N_{v'}$ by means of the diagonal homomorphism.

DEFINITION 2.1. Let $o'_N = \bigcap_w \{N \cap \mathrm{Ind}_{G_v}^G o'_v$: w ranges over all finite places of K and $v = v(w)\}$.

Remark. By [10, Theorem 5.3], $o_w \otimes_{o_K} o'_N = \mathrm{Ind}_{G_v}^G o'_v$. If v is at most tamely ramified, then by [5, p. 26–27], o_v is a free $o_w[G_v]$-module. By construction, o'_v is a free $o_w[G_v]$-module for all $v = v(w)$. Hence o'_N is a locally free $o_K[G]$-module, and it is a projective G-module which has finite index in o_N.

Now as in [3, Section II, p. 352–353] we may assume that, by enlarging S if necessary, S is a finite set of places in N, stable under G, for which the following is true:

(a) *S contains the archimedean places S_∞ of N and those places which are ramified over K. The S-class number of every subfield of N containing K is 1.*

(b) *The set S_f of finite places in S is non-empty. There are integers $z, m \in o_K$ which are units outside of S such that*

$$zo'_N \subseteq Fr \subseteq mo'_N \subseteq mo_N$$

where Fr is a free $\mathbf{Z}[G]$-submodule of finite index in o'_N.

(c) exp: $mo_N \to \oplus\{N_v^*: v \in S_f\}$ *is a well-defined injection, where*

$$\exp = \bigoplus \{\exp_v : v \in S_f\} \quad and \quad \exp_v(x) = \sum_{n=0}^{\infty} x^n/n!$$

for all x in the additive group N_v^+ of N_v which are sufficiently close to zero.

Define $\overline{\exp}(Fr)$ to be the closure of the image of Fr under exp, and let $S_{f,0} = \{v(w)$: w is a place of K lying under a place in $S_f\}$. Then $S_{f,0}$ is a set of representatives for the G-orbits in S_f.

The following results are simple consequences of work of T. Chinburg in [3, Lemma 5.1].

LEMMA 2.2 (Chinburg). *For $v \in S_{f,0}$ define $\tilde{U}_v(1)$ as follows:*

$$\tilde{U}_v(1) = \begin{cases} \exp_v(mo'_v) & \text{if } v \text{ is wildly ramified over } K, \\ U_v(1) & \text{otherwise,} \end{cases}$$

where $U_v(1)$ is the group of principal units in o_v^*. The group $\overline{\exp}(Fr)$ is contained in

$$\tilde{J}(1) = \bigoplus \left\{ \mathrm{Ind}_{G_v}^G \tilde{U}_v(1) : v \in S_{f,0} \right\}.$$

The G-module $\tilde{J}(1)/\overline{\exp}(Fr)$ is finite and of finite projective dimension and has class $(o'_N) - [K: \mathbf{Q}](\mathbf{Z}[G])$ in $K_0(\mathbf{Z}[G])$.

Proof. The lemma is a consequence of the following observations:

(i) $\exp(\overline{mo'_N})/\,\overline{\exp}(Fr) = \exp(\overline{mo'_N})/\exp(\overline{Fr}) \cong \overline{mo'_N}/\,\overline{Fr} \cong mo'_N/Fr$, where $\overline{Fr}$ (resp. $\overline{mo'_N}$) denotes the closure of Fr (resp. mo'_N) in $\oplus\{o_v: v \in S_f\}$, and $\cong$ denotes an isomorphism of G-modules.
(ii) $(mo'_N) = (o'_N)$ and $(Fr) = [K\colon \mathbf{Q}](\mathbf{Z}[G])$ in $K_0(\mathbf{Z}[G])$.
(iii) $\tilde{J}(1)/\exp(\overline{mo'_N}) = \oplus\{\mathrm{Ind}_{G_v}^{G}(\tilde{U}_v(1)/\exp_v(mo'_v))\colon v \in S_{f,0}\}$.
(iv) If $v \in S_{f,0}$ is wildly ramified then $\tilde{U}_v(1) = \exp_v(mo'_v)$ by definition.
(v) If $v \in S_{f,0}$ is not wildly ramified, then $\tilde{U}_v(1) = U_v(1)$ and $o'_v = o_v$. The argument of [1, p. 285–288] shows that if $\exp_v$ is well defined on mo_v, then $\exp_v(mo_v) = 1 + mo_v$. Hence $\tilde{U}_v(1)/\exp_v(mo'_v) = U_v(1)/(1 + mo_v)$ if v is not wildly ramified. By [3, Lemma 5.1], $U_v(1)/(1 + mo_v)$ is finite and of finite projective dimension with trivial class in $K_0(\mathbf{Z}[G_v])$.
(vi) From (iii)–(v) we see that $\tilde{J}(1)/\exp(\overline{mo'_N})$ is finite and of finite projective dimension as a G-module with trivial class in $K_0(\mathbf{Z}[G])$. Now Lemma 2.2 follows from this and observations (i) and (ii).

All references to cohomology in this paper will be to Tate cohomology.

DEFINITION 2.3. For $v \in S$ let $\alpha_v \in H^2(G_v, N_v^*)$ be the local canonical class at v. If $v \in S_{f,0}$, let $\tilde{N}_v(1) = N_v^*/\tilde{U}_v(1)$ and let

$$h_v\colon \mathrm{Ext}^2_{G_v}(\mathbf{Z}, N_v^*) \to \mathrm{Ext}^2_{G_v}(\mathbf{Z}, \tilde{N}_v(1))$$

be the homomorphism induced by the quotient homomorphism $N_v^* \to \tilde{N}_v(1)$.

It is shown by Chinburg in [3, proof of Lemma 5.1] that if v is at most tamely ramified in N/K, then the G_v-module $U_v(1)$ is of finite projective dimension. If v is wildly ramified in N/K, then

$$\tilde{U}_v(1) = \exp_v(mo'_v)$$

is also of finite projective dimension because mo'_v is isomorphic to $\exp_v(mo'_v)$ as a G_v-module and because mo'_v is free over $o_w[G_v]$. Thus the quotient homomorphism $N_v^* \to \tilde{N}_v(1)$ induces an isomorphism in cohomology. Now cup product with the class

$$h_v(\alpha_v) \in \mathrm{Ext}^2_{G_v}(\mathbf{Z}, \tilde{N}_v(1))$$

induces an isomorphism between the cohomology of $\mathbf{Z}$ and that of $\tilde{N}_v(1)$ after a dimension shift of two. This is because cup product with

$$\alpha_v \in \mathrm{Ext}^2_{G_v}(\mathbf{Z}, N_v^*)$$

induces such an isomorphism between the cohomology of $\mathbf{Z}$ and that of N_v^*

and because the quotient homomorphism $N_v^* \to \tilde{N}_v(1)$ induces an isomorphism in cohomology (see the diagram below).

$$\begin{array}{ccc} H^i(G_v, \mathbf{Z}) & \xrightarrow{\cup \alpha_v} & H^{i+2}(G_v, N_v^*) \\ \| & & \downarrow \\ H^i(G_v, \mathbf{Z}) & \xrightarrow{\cup h_v(\alpha_v)} & H^{i+2}(G_v, \tilde{N}_v(1)). \end{array}$$

Since $\tilde{N}_v(1)$ is finitely generated, the mapping cylinder construction of [11, p. 56–57] now yields an exact sequence

$$(2.1) \qquad 0 \to \tilde{N}_v(1) \to A_{1,v} \to A_{2,v} \to \mathbf{Z} \to 0$$

of finitely generated G_v-modules with extension class

$$h_v(\alpha_v) \in \mathrm{Ext}^2_{G_v}(\mathbf{Z}, \tilde{N}_v(1))$$

in which $A_{1,v}$ and $A_{2,v}$ are of finite projective dimension.

The following result is a consequence of Lemma 2.2 and the results of Chinburg in [3, Proposition 5.1].

PROPOSITION 2.4 (Chinburg). *For $v \in S_{f,0}$ we define*

$$\Omega_v = (A_{1,v}) - (A_{2,v})$$

in $K_0(\mathbf{Z}[G_v])$ where $A_{i,v}$ are the modules in (2.1). *Then $\Omega_v \in \mathrm{Cl}(\mathbf{Z}[G_v])$. Let*

$$\mathrm{Ind}^G_{G_v} \Omega_v = (\mathrm{Ind}^G_{G_v} A_{1,v}) - (\mathrm{Ind}^G_{G_v} A_{2,v})$$

in $K_0(\mathbf{Z}[G])$. Then $\Omega(N/K, 2) = (o_N') - [K\colon \mathbf{Q}](\mathbf{Z}[G]) + \Sigma\{\mathrm{Ind}^G_{G_v} \Omega_v\colon v \in S_{f,0}$ and v is wildly ramified over $K\}$.

Remark. (1) It is not difficult to see that any effect on the class

$$(o_N') - [K\colon \mathbf{Q}](\mathbf{Z}[G])$$

caused by different choices of o_v' is balanced by the opposite effect on the last term in the formula. Thus the right hand side of the formula is indeed an invariant of Galois extension N/K.

(2) For all cases considered in this paper, the term $\mathrm{Ind}_{G_v}^{G}\,\Omega_v$ in the formula will be zero.

When N/K is a tame extension, Proposition 2.4 is nothing but Theorem 3.2 in [3]. In fact Proposition 2.4 may be proved by the same arguments as those of [3, p. 366–367]. We summarize these arguments after reviewing some definitions and results in [3].

Proof of Proposition 2.4. We begin by extending Definition 2.3 to infinite places. For $v \in S_\infty$ let W_v be a finitely generated G_v-submodule of N_v^* for which

(i) *W_v contains the group of S-units $U = U_{N,S}$ of N and W_v/U is torsion free, and*

(ii) *the inclusion of W_v into N_v^* induces an isomorphism in G_v-cohomology.*

The existence of such a module was proved in [3, Lemma 2.1]. For $v \in S_\infty$, let $\tilde{N}_v(1) = W_v$ and let $h_v\colon \mathrm{Ext}_{G_v}^2(\mathbf{Z}, N_v^*) \to \mathrm{Ext}_{G_v}^2(\mathbf{Z}, \tilde{N}_v(1))$ be the inverse of the cohomology isomorphism induced by the inclusion of W_v into N_v^*.

Then, by [3, Proposition 5.1], there is an exact sequence

$$0 \to \tilde{N}_v(1) \to A_{1,v} \to A_{2,v} \to \mathbf{Z} \to 0 \tag{2.2}$$

of finitely generated G_v-modules with extension class

$$h_v(\alpha_v) \in \mathrm{Ext}_{G_v}^2\big(\mathbf{Z}, \tilde{N}_v(1)\big)$$

in which $A_{1,v}$ and $A_{2,v}$ are of finite projective dimension. Let $S_{\infty,0}$ be a set of representatives for the G-orbits in S_∞. For $v \in S_{\infty,0}$, as for the case $v \in S_{f,0}$, we define

$$\Omega_v = (A_{1,v}) - (A_{2,v}) \quad \text{and} \quad \mathrm{Ind}_{G_v}^{G}\,\Omega_v = \big(\mathrm{Ind}_{G_v}^{G} A_{1,v}\big) - \big(\mathrm{Ind}_{G_v}^{G} A_{2,v}\big)$$

in $K_0(\mathbf{Z}[G])$ where $A_{1,v}$ and $A_{2,v}$ are the modules in (2.2).

Let now Y be the free abelian group on S, and define the exact sequences (X), (U), and $(U)_f$, which is a finitely generated approximating sequence to (U) (cf. [3, Section III]), as follows:

$$(X) \qquad 0 \to X \to Y \xrightarrow{\partial} \mathbf{Z} \to 0$$

$$(U) \qquad 0 \to U \to J \to C \to 0$$

$$(U)_f \qquad 0 \to U \to J_f \to C_f \to 0,$$

where $\partial(v) = 1$ for $v \in S$,
$U = U_{N,S}$ is the group of S-units of N,
$J = J_{N,S}$ is the group of S-ideles,
$C = C_N$ is the idele class group of N,
$J_f = J_0 \oplus \oplus\{\mathrm{Ind}_{G_v}^{G} W_v \colon v \in S_{\infty,0}\}$
$J_0 = \oplus\{N_v^* \colon v \in S_f\}/\overline{\exp(Fr)}$ and
$C_f = J_f/U$.

In [3, Corollary 2.1] Chinburg constructed a unique class

$$(\alpha)_f \in H^2(G, \mathrm{Hom}((X), (U)_f))$$

from the Tate canonical class

$$(\alpha) \in H^2(G, \mathrm{Hom}((X), (U)))$$

(see [12] for the definition of $\mathrm{Hom}((X), (U))$ and the class (α)). Let $(\alpha)_{2,f} \in H^2(G, \mathrm{Hom}(Y, J_f)) = \mathrm{Ext}_G^2(Y, J_f)$ be the second canonical projection of $(\alpha)_f$ as in [3]. Then there is an exact sequence of finitely generated modules

$$(2.3) \qquad 0 \to J_f \to \tilde{A}_1 \to \tilde{A}_2 \to Y \to 0$$

with extension class $(\alpha)_{2,f}$ in which the $\tilde{A}_i$ are of finite projective dimension. By definition

$$(2.4) \qquad \Omega(N/K, 2) = (\tilde{A}_1) - (\tilde{A}_2) - \tilde{r}(\mathbf{Z}[G]) \quad \text{in } K_0(\mathbf{Z}[G])$$

for some integer $\tilde{r}$.

Let $\tilde{E}$ be the module $\tilde{J}(1)/\overline{\exp(Fr)}$ in Lemma 2.2. The sequence (2.3), by push out, gives rise to an exact sequence of finitely generated modules

$$(2.5) \qquad 0 \to J_f/\tilde{E} \to \tilde{A}_1/E \to \tilde{A}_2 \to Y \to 0$$

with extension class

$$\alpha_{\tilde{E}} \in \mathrm{Ext}_G^2\left(Y, J_f/\tilde{E}\right),$$

the image of

$$(\alpha)_{2,f} \in \mathrm{Ext}_G^2(Y, J_f)$$

under the homomorphism induced by the quotient homomorphism $J_f \to J_f/\tilde{E}$. From (2.3) and Lemma 2.2, $\tilde{A}_1/\tilde{E}$ has finite projective dimension.

On the other hand, the arguments of [3, p. 366–367] show that by inducing from G_v to G the sequences (2.1) and (2.2) and then summing the resulting sequences over $v \in S_0 = S_{f,0} \cup S_{\infty,0}$, we arrive at a sequence

$$(2.6) \qquad 0 \to J_f/\tilde{E} \to A_1 \to A_2 \to Y \to 0$$

with extension class $\alpha_{\tilde{E}}$ in which the A_i are finitely generated and of finite projective dimension.

Since (2.5) and (2.6) have the same extension class, by [4, Proposition 5.1],

$$(2.7) \qquad (\tilde{A}_1/\tilde{E}) - (\tilde{A}_2) = (A_1) - (A_2) \quad \text{in } K_0(\mathbf{Z}[G]).$$

By construction and [3, Proposition 5.1],

$$\begin{aligned}(2.8)\quad (A_1) - (A_2) &= \sum\left\{\mathrm{Ind}_{G_v}^G \Omega_v : v \in S_0\right\} \\ &= \sum\left\{\mathrm{Ind}_{G_v}^G \Omega_v : v \in S_{f,0} \text{ and } v \text{ is wildly ramified}\right\} \\ &\quad + r(\mathbf{Z}[G]) \text{ in } K_0(\mathbf{Z}[G])\end{aligned}$$

for some integer r. From (2.4), (2.7), (2.8) and Lemma 2.2,

$$\begin{aligned}(2.9)\quad \Omega(N/K,2) &= (\tilde{E}) + (A_1) - (A_2) - \tilde{r}(\mathbf{Z}[G]) \\ &= [(o_N') - [K:\mathbf{Q}](\mathbf{Z}[G])] \\ &\quad + \sum\left\{\mathrm{Ind}_{G_v}^G \Omega_v : v \in S_{f,0} \text{ and } v \text{ is wildly ramified}\right\} \\ &\quad + (r - \tilde{r})(\mathbf{Z}[G]) \text{ in } K_0(\mathbf{Z}[G]).\end{aligned}$$

Since all the classes but $(r - \tilde{r})(\mathbf{Z}[G])$ in the last equation are in $\mathrm{Cl}(\mathbf{Z}[G])$, we conclude that $r = \tilde{r}$.

III. $W_{N/\mathbf{Q}}$

We define a quaternion field N to be a finite normal extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(N/\mathbf{Q})$ isomorphic to the quaternion group H_8 of order eight. From now on we restrict ourselves to quaternion fields.

In this case $\mathrm{Cl}(\mathbf{Z}[G])$ may be identified with $\{\pm 1\}$ because $\mathrm{Cl}(\mathbf{Z}[H_8])$ has order two. With this identification, the class $W_{N/\mathbf{Q}}$ is equal to the Artin root number $W(\chi_{N/\mathbf{Q}}) = \pm 1$ where $\chi_{N/\mathbf{Q}}$ is the character of the unique two dimensional irreducible symplectic representation of $G \cong H_8$. The question in Section 1 now becomes:

QUESTION. Is $\Omega(N/\mathbf{Q},2) = W(\chi_{N/\mathbf{Q}}) = \pm 1$ for all quaternion fields N?

Notation. From now on we denote by K the biquadratic subfield of a quaternion field N. We abbreviate $\chi_{N/\mathbf{Q}}$ by χ and we write

$$H_8 = \langle \sigma, \tau : \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle.$$

J. Martinet proved the following results in [7] (see also [6]).

LEMMA 3.1 (Fröhlich, Martinet). *Let N be a quaternion field. For each place $t \neq 2$ of $\mathbf{Q}$, define α_t and β_t as follows:*
$\alpha_t = 1$ if t is not ramified in $K/\mathbf{Q}$ (in particular, $\alpha_\infty = 1$);
$\alpha_p = (2/p)$ for a finite prime $p \neq 2$ ramified in $K/\mathbf{Q}$;

$$\beta_\infty = \varepsilon(N) = \begin{cases} +1 & \text{if } N \text{ is totally real} \\ -1 & \text{if } N \text{ is totally imaginary}; \end{cases}$$

$\beta_p = 1$ if p is unramified in $N/\mathbf{Q}$
$\beta_p =$ image of p mod 4 $= (-1)^{(p-1)/2}$ if p is ramified in $N/\mathbf{Q}$.
Then the local root number $W(\chi_t) = W_t = \alpha_t\beta_t = \pm 1$, where χ_t is the restriction of χ to the decomposition group G_v for a place v of N over t.

DEFINITION 3.2. For the place $t = 2$ of $\mathbf{Q}$, we define $\alpha_2 = 1$ and $\beta_2 = W(\chi_2) = W_2$ so that $\alpha_2\beta_2 = W_2$.

The following result is clear from the lemma.

PROPOSITION 3.3 (Fröhlich, Martinet). *Let*

$$D_0 = \prod_{\substack{p \neq 2, \\ p \mid d_{K/\mathbf{Q}}}} p,$$

i.e., the product of all odd primes ramified in K. Then

$$W_{N/\mathbf{Q}} = 1 \text{ if and only if } \left(\frac{2}{D_0}\right) \equiv W_2\varepsilon(N) \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p \mod 4$$

and

$$W_{N/\mathbf{Q}} = -1 \text{ if and only if } \left(\frac{2}{D_0}\right) \equiv -W_2\varepsilon(N) \prod_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \mod 4$$

where $d_{N/\mathbf{Q}}$ (*resp.* $d_{K/\mathbf{Q}}$) *is the discriminant of the field* N (*resp.* K).

Proof. All local factors are ± 1 and $+1$ except for finitely many places t. Since $W_{N/\mathbf{Q}} = W(\chi) = \Pi_t W(\chi_t)$ (cf. [8] or [13]),

$$\begin{aligned} W_{N/\mathbf{Q}} = 1 &\Leftrightarrow \prod_t W(\chi_t) = 1 \\ &\Leftrightarrow \prod_t (\alpha_t \beta_t) = 1 \\ &\Leftrightarrow \left(\prod_t \alpha_t\right)\left(\prod_t \beta_t\right) = 1 \\ &\Leftrightarrow \prod_t \alpha_t = \prod_t \beta_t \\ &\Leftrightarrow \left(\frac{2}{D_0}\right) = W_2\varepsilon(N) \prod_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \mod 4. \end{aligned}$$

Later we shall use the following results in [7 or 9] on projective $\mathbf{Z}[G]$-modules where $G = H_8$.

LEMMA 3.4 (Martinet). *Let* M *be a projective* G*-module of rank one. Define*

$$M^+ = \{x \in M : \sigma^2 x = x\} \quad \text{and} \quad M^- = \{x \in M : \sigma^2 x = -x\}.$$

Then M^+ (*resp.* M^-) *is a free module over* $\mathbf{Z}^+$ (*resp. over* $\mathbf{Z}^-$), *where*

$$\mathbf{Z}^+ = \mathbf{Z}[G]/(1-\sigma^2) \cong \mathbf{Z}[g] \text{ for } g = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$$

and

$$\mathbf{Z}^- = \mathbf{Z}[G]/(1+\sigma^2) \cong \mathbf{Z}[1, i, j, k],$$

the ring of integral quaternions.

PROPOSITION 3.5 (Martinet). *Let* M, M^+ *and* M^- *be as in Lemma* 3.4. *Let* ϕ *and* ψ *be bases for* M^+ *and* M^- *over* $\mathbf{Z}^+$ *and* $\mathbf{Z}^-$, *respectively.*

(1) ϕ *and* ψ *are well defined up to sign and the multiplication by an element of* G.

(2) *ϕ and ψ can be chosen in such a way that one of the following congruences holds*:

(a) $\psi \equiv \phi \bmod 2M$

(b) $\psi \equiv \sigma\phi + \tau\phi + \sigma\tau\phi \bmod 2M$.

Moreover, for a given module M, only one of the congruences (a) *and* (b) *is possible, and M is free if and only if* (a) *holds.*

Now let $N/\mathbf{Q}$ be an H_8-extension. From now on we fix an isomorphism $G = \mathrm{Gal}(N/\mathbf{Q}) \cong H_8$ and identify G with H_8 via this isomorphism. For a place v of N over the prime 2, let I_v be the inertia subgroup and G_v the decomposition subgroup of the place v. We denote the order of a group H by $\#H$. In the remainder of this paper, we shall prove $\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}}$ for the following cases:

$\#I_v = \#G_v = 2$ in Section IV

$\#I_v = 2$ and $\#G_v = 4$ in Section V

$\#I_v = \#G_v = 4$ in Section VI.

IV. The case in which $\#I_v = \#G_v = 2$

Lemma 4.1. *There are exactly six non-isomorphic ramified extensions of $\mathbf{Q}_2$ of degree two. These are the extensions $E = \mathbf{Q}_2(\sqrt{c})$ where $c =$* 3, 7, 2, 6, 10 *or* 14.

Proof. Consider all Kummer 2-extensions of degree two. Among them these are all that are ramified.

Now let N be an H_8-extension of $\mathbf{Q}$ with both the inertia subgroup I_v and the decomposition subgroup G_v of order two, i.e., $I_v = G_v = \{1, \sigma^2\} \subset G = H_8$ where v is a place of N over the prime 2. Let K be the biquadratic subfield of N and let $w = w(v)$ be the place of K under v. In this case we may identify N_v (resp. K_w) with $E = \mathbf{Q}_2(\sqrt{c})$ (resp. $\mathbf{Q}_2$) for one of the values of c listed in Lemma 4.1 by means of an embedding of N into $\overline{\mathbf{Q}}_2$ which induces the place v, where $\overline{\mathbf{Q}}_2$ denotes an algebraic closure of $\mathbf{Q}_2$. With this identification, we note that $o_w = \mathbf{Z}_2$ and $o_v = o_E = \mathbf{Z}_2[\sqrt{c}]$.

We define a projective G-module o'_N as follows.

Definition 4.2. Let

$$o'_v = \{a + b\sqrt{c} : a \equiv b \bmod 2 \text{ and } a, b \in \mathbf{Z}_2\} = \mathbf{Z}_2[G_v](1 + \sqrt{c}).$$

As in Definition 2.1, let o'_N be the unique submodule of o_N such that

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} o'_N = \mathrm{Ind}_{G_v}^{G} o'_v = \mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} o'_v$$

and

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} o'_N = \mathbf{Z}_p \otimes_{\mathbf{Z}} o_N \quad \text{for } p \neq 2.$$

Remark 4.3. (1) By the remark following Definition 2.1, o'_N is projective.
(2) From the semi-local construction of o'_N we have

$$(o_N : o'_N) = (o_v : o'_v)^4 = 16 \quad \text{and} \quad o'_N \cap K = 2o_K.$$

Define $(o'_N)^+ = (x \in o'_N : \sigma^2 x = x\}$ and $(o'_N)^- = \{x \in o'_N : \sigma^2 x = -x\}$. Then by Lemma 3.4,

$$(o'_N)^+ = o'_N \cap K = \mathbf{Z}^+ \phi' \quad \text{and} \quad (o'_N)^- = \mathbf{Z}^- \psi'$$

where ϕ' (resp. ψ') is a free basis over $\mathbf{Z}^+$ (resp. $\mathbf{Z}^-$).

PROPOSITION 4.4. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = \mathbf{Q}_2(\sqrt{c})$ and $K_w = \mathbf{Q}_2$.*
(1) *For $c = 3$ or 7,*

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 4 \bmod 16$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 4 \bmod 16.$$

(2) *For $c = 2$ or 10,*

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32.$$

(3) *For $c = 6$ or 14,*

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32.$$

Proposition 4.4 will be a consequence of the following lemma and Proposition 3.3. Let k_i, $i = 1, 2, 3$, be quadratic subfields of the biquadratic field K and let $d_i = d_{k_i/\mathbf{Q}}$, the discriminant of k_i. Then $d_i \equiv 1 \bmod 4$ since $K/\mathbf{Q}$ is at most tamely ramified in this case. Also

$$d_{K/\mathbf{Q}} = d_1 d_2 d_3 = D_0^2 \quad \text{where } D_0 = \prod_{\substack{p \neq 2, \\ p \mid d_{K/\mathbf{Q}}}} p,$$

i.e., the product of all odd primes ramified in K.

LEMMA 4.5.

(a) $$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) = 1 + d_1 + d_2 + d_3 \equiv 4\left(\frac{2}{D_0}\right) \equiv \pm 4 \bmod 16.$$

(b) $$\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) = \begin{cases} \varepsilon(N) 4 \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p \equiv \pm 4 \bmod 16 & \text{for } c = 3 \text{ or } 7 \\ \varepsilon(N) 8 \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p \equiv \pm 8 \bmod 32 & \text{otherwise} \end{cases}$$

(*see Lemma* 3.1 *for the definition of* $\varepsilon(N)$).

Proof of Lemma 4.5. (a) Let $o_K' = (o_N')^+ = o_N' \cap K$. By Remark 4.3 $o_K' = 2 o_K$, and $\phi' = 2\phi$ for a normal basis ϕ for o_K. Since

$$\phi_0 = \left(1 + \sqrt{d_1} + \sqrt{d_2} \pm \sqrt{d_3}\right)/4$$

is a normal basis for o_K and ϕ is determined up to sign and multiplication by an element of $G = H_8$ by Prop. 3.5,

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) = 4\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) = 4\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi_0^2) = 1 + d_1 + d_2 + d_3.$$

Now (a) is a consequence of the congruence

$$\frac{1 + d_1 + d_2 + d_3}{4} \equiv \left(\frac{2}{D_0}\right) \mod 4,$$

which follows from the fact that if $AB \equiv BC \equiv CA \equiv 1 \bmod 4$ then

$$\frac{1 + AB + BC + CA}{4} \equiv \left(\frac{2}{|ABC|}\right) \mod 4,$$

the proof of which is straightforward together with the definition

$$\left(\frac{2}{|ABC|}\right) = 1 \quad \text{for } |ABC| = 1.$$

(b) Note that both $\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2)$ and $\varepsilon(N)$ have the same sign. This is because ψ'^2 is totally positive if N is real and because ψ'^2 is totally negative otherwise. By using the same arguments as in [9, III] or [7, §3], we have $\mathrm{disc}_{N/\mathbf{Q}}(o'_N) = \mathrm{disc}_{K/\mathbf{Q}}(o'_K)[\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2)]^4$ where disc denotes the discriminant. We thus have

$$d_{N/\mathbf{Q}} = d_{K/\mathbf{Q}}\left[\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2)\right]^4 \quad \text{since } (o_N : o'_N) = (o_K : o'_K) = 16.$$

Now again as in [9, III] or [7, §3], we can use ramification groups to compute $d_{N/\mathbf{Q}}/d_{K/\mathbf{Q}}$, from which (b) follows.

We now prove Proposition 4.4.

Proof of Proposition 4.4. By Proposition 3.3,

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \left(\frac{2}{D_0}\right) \equiv W_2\varepsilon(N) \prod_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \mod 4$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \left(\frac{2}{D_0}\right) \equiv -W_2\varepsilon(N) \prod_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \mod 4.$$

Since

$$\left(\frac{2}{D_0}\right) \equiv \frac{1 + d_1 + d_2 + d_3}{4} \mod 4$$

by Lemma 4.5, Proposition 4.4 now follows from Lemma 4.5 and the following results on local root numbers.

Claim.

$$W_2 = \begin{cases} 1 & \text{for } c = 2 \text{ or } 10 \\ -1 & \text{otherwise.} \end{cases}$$

Proof of Claim. Let χ_2 be the restriction of χ to G_v where χ is the character of the unique two-dimensional irreducible representation of $G = H_8$. Then $\chi_2 = \lambda_2 + \bar{\lambda}_2$ for the non-trivial character λ_2 of G_v. We thus have

$W_2 = W(\chi_2) = W(\lambda_2)W(\bar{\lambda}_2) = \lambda_2(-1)$ where (-1) is the image of (-1) under the Artin map: $\mathbf{Z}_2^* \to I_v = \{1, \sigma^2\}$ (see, for example, [8] or [13]). Since $\mathrm{Norm}_{E/\mathbf{Q}_2}(1+\sqrt{c}) = 1 - c \equiv -1 \bmod 8$ for $c = 2$ or 10 since $(\mathbf{Z}_2^*)^2 = 1 + 8\mathbf{Z}_2$ is contained in the norm group,

$$(-1) \in \mathrm{Norm}_{E/\mathbf{Q}_2}(E^*) \quad \text{for } c = 2 \text{ or } 10.$$

Furthermore these are the only such cases. This is because the conductor of λ_2 is $1 + 4\mathbf{Z}_2$ for $c = 3$ or 7 and because the conductor of λ_2 is $1 + 8\mathbf{Z}_2$ with $\mathrm{Norm}_{E/\mathbf{Q}_2}(1+\sqrt{c}) \equiv 3 \bmod 8$ for $c = 6$ or 14.

PROPOSITION 4.6. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = \mathbf{Q}_2(\sqrt{c})$ and $K_w = \mathbf{Q}_2$.*

(1) *For $c = 3$ or 7,*

$$\text{(a)} \quad \psi' \equiv \phi' \bmod 2o_N' \Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16,$$

$$\text{(b)} \quad \psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N' \Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16.$$

(2) *For $c = 2$ or 10,*

$$\text{(a)} \quad \psi' \equiv \phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32,$$

$$\text{(b)} \quad \psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32$$

(3) *For $c = 6$ or 14,*

$$\text{(a)} \quad \psi' \equiv \phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32,$$

$$\text{(b)} \quad \psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32.$$

Before proving Proposition 4.6, we note these corollaries.

COROLLARY 4.7. *The projective G-module o_N' given in Definition 4.2 is free if and only if*

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16 \text{ for } c = 3 \text{ or } 7,$$

$$2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32 \text{ for } c = 2 \text{ or } 10$$

and

$$2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32 \textit{ for } c = 6 \textit{ or } 14.$$

Proof. Combine Propositions 3.5 and 4.6.

COROLLARY 4.8. *Theorem 1 is true if the inertia and decomposition groups of v each has order two.*

Proof. Since $\mathrm{Cl}(\mathbf{Z}[G_v])$ is trivial in this case, $\Omega(N/\mathbf{Q}, 2) = (o_N') - (\mathbf{Z}[G])$ by virtue of Proposition 2.4. Recall that $(o_N') - (\mathbf{Z}[G]) = 1 \in \mathrm{Cl}(\mathbf{Z}[G]) = \{\pm 1\}$ if and only if o_N' is free as G-module. Corollary 4.8 now results from Proposition 4.4 and Corollary 4.7.

Proof of Proposition 4.6. (a) Let $\psi' = \phi' + 2x$ for some $x \in o_N'$. Since $(o_N')^+ = o_K' = 2o_K$ by Remark 4.3, we may set $\phi' = 2\phi$, and $\psi' = 2\psi$ where ϕ, $\psi \in o_N$ and ϕ is a normal basis for o_K. It suffices to show that

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 + \psi^2) \equiv 0 \bmod 4 \text{ for case } (1),$$

$$\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 - \psi^2) \equiv \bmod 8 \text{ for case } (2)$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 + \psi^2) \equiv 0 \bmod 8 \text{ for case } (3).$$

Denote by x_v the image of x under the embedding of N into $E = \mathbf{Q}_2(\sqrt{c})$ which has been identified with N_v. It is clear from the relations $\sigma^2\phi = \phi$ and $\sigma^2\psi = -\psi$ that $\sigma^2\phi_v = \phi_v$ and $\sigma^2\psi_v = -\psi_v$. Therefore in $o_v = o_E = \mathbf{Z}_2[\sqrt{c}]$, $\phi_v = a$ and $\psi_v = b\sqrt{c}$ for some $a, b \in o_w = \mathbf{Z}_2$. Furthermore the condition $\psi - \phi = x \in o_N'$ gives rise to the condition $\psi_v - \phi_v = x_v \in o_v'$, which implies by Definition 4.2 that $-a \equiv b \bmod 2$.

Using these relations we now have

$$\phi_v^2 + \psi_v^2 = a^2 + b^2c \equiv a^2 - b^2 \equiv 0 \bmod 4 \text{ for case } (1),$$

$$2\phi_v^2 - \psi_v^2 = 2a^2 - b^2c \equiv 2a^2 - 2b^2 \equiv 0 \bmod 8 \text{ for case } (2)$$

and

$$2\phi_v^2 + \psi_v^2 = 2a^2 + b^2c \equiv 2a^2 - 2b^2 \equiv 0 \bmod 8 \text{ for case } (3).$$

We note that in each case the same congruence holds for any place t of N over the prime 2.

Therefore, for case (1),

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2+\psi^2) &= \sum_{t\mid 2}\mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(\phi^2+\psi^2)\\ &= \sum_{t\mid 2}(\phi_t^2+\psi_t^2)\\ &\equiv 0 \mod 4\end{aligned}$$

where t ranges over all the places of N over the prime 2 and $w(t)$ denotes the place of K under t. Similarly $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2-\psi^2)\equiv 0 \mod 8$ for case (2) and $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2+\psi^2)\equiv 0 \mod 8$ for case 3).

(b) Let $\psi' = \sigma\phi' + \tau\phi' + \sigma\tau\phi' + 2y$ for some $y \in o'_N$. As in (a) we set $\phi' = 2\phi$ and $\psi' = 2\psi$. Then

$$\psi = \sigma\phi + \tau\phi + \sigma\tau\phi + y = \mathrm{Tr}_{K/\mathbf{Q}}(\phi) - \phi + y = \pm 1 - \phi + y,$$

where the last equality results from the fact that

$$\phi_0 = \left(1+\sqrt{d_1}+\sqrt{d_2}\pm\sqrt{d_3}\right)/4$$

is a normal basis for o_K and $\phi = \pm g\phi_0$ for some $g \in G = H_8$ by Proposition 3.5.

It suffices to show that

$$\begin{aligned}&\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2-\psi^2)\equiv 0 \mod 4 \text{ for case } (1),\\ &\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2+\psi^2)\equiv 0 \mod 8 \text{ for case } (2)\end{aligned}$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2-\psi^2)\equiv 0 \mod 8 \text{ for case } (3).$$

By the same arguments as in (a), the conditions

$$-(\pm 1-\phi)+\psi = y \in o'_N, \qquad \sigma^2\phi = \phi \quad\text{and}\quad \sigma^2\psi = -\psi,$$

give rise to the relations,

$$-(\pm 1-\phi_v) = a, \qquad \psi_v = b\sqrt{c} \quad\text{and}\quad a \equiv b \mod 2 \text{ for some } a, b \in \mathbf{Z}_2.$$

Using these relations we now have

$$\begin{aligned}\phi_v^2-\psi_v^2 &= (a\pm 1)^2 - b^2c \equiv (a\pm1)^2+b^2 \equiv 1 \mod 4 \text{ for case } (1),\\ 2\phi_v^2+\psi_v^2 &= 2(a\pm1)^2+b^2c \equiv 2(a\pm1)^2+2b^2 \equiv 2 \mod 8 \text{ for case } (2),\end{aligned}$$

and

$$2\phi_v^2 - \psi_v^2 = 2(a \pm 1)^2 - b^2c \equiv 2(a \pm 1)^2 + 2b^2 \equiv 2 \bmod 8 \text{ for case } (3).$$

We note that in each case the same congruence also holds for any place t of N over the prime 2.

Therefore, for case (1),

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 - \psi^2) &= \sum_{t|2} \mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(\phi^2 - \psi^2) \\ &= \sum_{t|2} (\phi_t^2 - \psi_t^2) \\ &= \sum_{t|2} \mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(1) \\ &= \mathrm{Tr}_{K/\mathbf{Q}}(1) \\ &\equiv 0 \mod 4.\end{aligned}$$

Similarly, $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 + \psi^2) \equiv 0 \bmod 8$ for case (2) and $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 - \psi^2) \equiv 0 \bmod 8$ for case (3), which completes the proof of Proposition 4.6.

V. The case in which $\#I_v = 2$ and $\#G_v = 4$

LEMMA 5.1. *There are exactly three non-isomorphic cyclic extensions of $\mathbf{Q}_2$ of degree four with the inertia subgroup of order two. These are the extensions $E = F(\sqrt{c})$ where $F = \mathbf{Q}_2(\zeta)$, ζ is a primitive cube root of unity and*

$$c = (1 + 2)(1 + \zeta 2^2), 2(1 + \zeta 2^2) \text{ or } 2(1 + 2)(1 + \zeta 2^2).$$

Proof. By local class field theory there are exactly three non-isomorphic extensions of the above kind. Since $\mathbf{Q}_2(\zeta)$ is the only unramified extension of $\mathbf{Q}_2$ of degree two, each such extension must contain $F = \mathbf{Q}_2(\zeta)$. Consider all Kummer 2-extensions E of F of degree two such that

(i) $E/\mathbf{Q}_2$ is normal with $\mathrm{Gal}(E/\mathbf{Q}_2) \cong \mathbf{Z}/4\mathbf{Z}$ and

(ii) E is ramified over F.

These extensions are the ones listed in Lemma 5.1.

Let now N be an H_8-extension of $\mathbf{Q}$ with the inertia subgroup of order two and the decomposition subgroup of order four, say, $I_v = \{1, \sigma^2\}$ and $G_v = \langle\sigma\rangle \subset G = H_8$ where v is a place of N over the prime 2.

Let $w = w(v)$ be the placed of K under v. In this case, by means of an embedding of N into $\overline{\mathbf{Q}}_2$ which induces the place v, we may identify N_v (resp. K_w) with $E = F(\sqrt{c})$ (resp. F) for one of the values of c listed in

Lemma 5.1. With this identification, we note that $o_w = o_F = \mathbf{Z}_2[\zeta]$ and $o_v = o_E = o_F[\sqrt{c}\,]$.

We define a projective G-module o'_N as follows.

DEFINITION 5.2. Let

$$o'_v = \{a + b\sqrt{c} : a \equiv b \bmod 2 \text{ and } a, b \in o_F\}.$$

A simple computation shows that

$$\mathbf{Z}_2[G_v]\zeta(1 + \sqrt{c}\,) \subset o'_v$$

and that

$$(o_v : o'_v) = \big(o_v : \mathbf{Z}_2[G_v]\zeta(1 + \sqrt{c}\,)\big) = 4.$$

So $o'_v = \mathbf{Z}_2[G_v]\zeta(1 + \sqrt{c}\,)$. As in Definition 2.1, let o'_N be the unique submodule of o_N such that

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} o'_N = \mathrm{Ind}_{G_v}^{G} o'_v \quad \text{and} \quad \mathbf{Z}_p \otimes_{\mathbf{Z}} o'_N = \mathbf{Z}_p \otimes_{\mathbf{Z}} o_N \text{ for } p \neq 2.$$

Remark 5.3. (1) The same remark as 4.3 holds here with

$$(o_N : o'_N) = (o_v : o'_v)^2 = 16.$$

(2) We can define $(o'_N)^+$, $(o'_N)^-$, ϕ' and ψ' as above.

PROPOSITION 5.4. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = F(\sqrt{c}\,)$ and $K_w = F = \mathbf{Q}_2(\zeta)$.*

(1) *For $c = (1 + 2)(1 + \zeta 2^2)$,*

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 4 \bmod 16$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 4 \bmod 16.$$

(2) *For $c = 2(1 + \zeta 2^2)$,*

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32.$$

(3) *For* $c = 2(1+2)(1+\zeta 2^2)$,

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 8 \bmod 32.$$

Proposition 5.4 will be a consequence of the following Lemma and Proposition 3.3.

LEMMA 5.5.

(a) $\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) = 1 + d_1 + d_2 + d_3 \equiv \pm 4 \bmod 16$ *for all* c.

(b)

$$\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) = \begin{cases} 4\varepsilon(N) \prod\limits_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \equiv \pm 4 \bmod 16 & \text{for } c = (1+2)(1+\zeta 2^2) \\ 8\varepsilon(N) \prod\limits_{\substack{p\neq 2,\\ p\mid d_{N/\mathbf{Q}}}} p \equiv \pm 8 \bmod 32 & \text{otherwise}. \end{cases}$$

Proof of Lemma 5.5. (a) Let $o'_K = (o'_N)^+ = o'_N \cap K$. By Remark 5.3, $o'_K = 2o_K$. Since $K/\mathbf{Q}$ is at most tamely ramified in this case, (a) results from Lemma 4.5(a).

(b) This follows from the same arguments as in Lemma 4.5(b).

Proof of Proposition 5.4. We refer the reader to the proof of Proposition 4.4. With the same notation as there we prove only the following results on local root numbers.

Claim.

$$W_2 = \begin{cases} 1 & \text{for } c = 2(1+\zeta 2^2) \\ -1 & \text{otherwise} \end{cases}.$$

Proof of Claim. Let χ_2 be as above. Then $\chi_2 = \lambda_2 + \bar{\lambda}_2$ and $W_2 = W(\chi_2) = W(\lambda_2)W(\bar{\lambda}_2) = \lambda_2(-1)$, where λ_2 is a character of G_v of order four and (-1) is the image of (-1) under the Artin map. Since

$$\mathrm{Norm}_{E/\mathbf{Q}_2}(1 + \zeta\sqrt{c}) \equiv -1 \bmod 8 \quad \text{for } c = 2(1+\zeta 2^2)$$

and $(\mathbf{Z}_2^*)^2 = 1 + 8\mathbf{Z}_2$ is contained in the norm group,

$$(-1) \in \mathrm{Norm}_{E/\mathbf{Q}_2}(E^*) \text{ for } c = 2(1 + \zeta 2^2).$$

Furthermore, by local class field theory, this is the only such case which completes the proof of the claim.

PROPOSITION 5.6. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = F(\sqrt{c})$ and $K_w = F = \mathbf{Q}_2(\zeta)$.*

(1) *For $c = (1 + 2)(1 + \zeta 2^2)$,*

(a) $\psi' \equiv \phi' \bmod 2o_N' \Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16,$

(b) $\psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N'$
$\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16.$

(2) *For $c = 2(1 + \zeta 2^2)$,*

(a) $\psi' \equiv \phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32.$

(b) $\psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N'$
$\Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32.$

(3) *For $c = 2(1 + 2)(1 + \zeta 2^2)$,*

(a) $\psi' \equiv \phi' \bmod 2o_N' \Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32$

(b) $\psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N'$
$\Rightarrow 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32.$

Before proving Proposition 5.6, we note these corollaries.

COROLLARY 5.7. *The projective G-module o_N' which is defined in 5.2, is free if and only if*

$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 16$ *for* $c = (1 + 2)(1 + \zeta 2^2),$
$2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32$ *for* $c = 2(1 + \zeta 2^2)$

and

$$2\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) \equiv -\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 32 \text{ for } c = 2(1 + 2)(1 + \zeta 2^2)$$

respectively.

Proof. Combine Propositions 3.5 and 5.6

COROLLARY 5.8. *Theorem* 1 *is true if the inertia and decomposition groups of v have orders two and four respectively.*

Proof. Since $\mathrm{Cl}(\mathbf{Z}[G_v])$ is trivial in this case, $\Omega(N/\mathbf{Q},2) = (o'_N) - (\mathbf{Z}[G])$ by Proposition 2.4. Recall that $(o'_N) - (\mathbf{Z}[G]) = 1 \in \mathrm{Cl}(\mathbf{Z}[G]) = \{\pm 1\}$ if and only if o'_N is free as G-module. Corollary 5.8 now results from Proposition 5.4 and Corollary 5.7.

Proof of Proposition 5.6. (a) This part of the proof is the same as that of Proposition 4.6 with the following modifications:

$$E = F(\sqrt{c}), \qquad o_v = o_E = o_F[\sqrt{c}] \quad \text{and} \quad o_w = o_F = \mathbf{Z}_2[\zeta].$$

(b) Let $\psi' = \sigma\phi' + \tau\phi' + \sigma\tau\phi' + 2y$ for some $y \in o'_N$. As in the proof of part (a) of Proposition 4.6 we set $\phi' = 2\phi$ and $\psi' = 2\psi$. Then

$$\psi = \sigma\phi + \tau\phi + \sigma\tau\phi + y = \mathrm{Tr}_{K/\mathbf{Q}}(\phi) - \phi + y = \pm 1 - \phi + y$$

where the last equality results from the fact that $\phi_0 = (1 + \sqrt{d_1} + \sqrt{d_2} \pm \sqrt{d_3})/4$ is a normal basis for o_K and $\phi = \pm g\phi_0$ for some $g \in G = H_8$ by Proposition 3.5.

It suffices to show that

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 - \psi^2) \equiv 0 \bmod 4 \text{ for case } (1),$$
$$\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 + \psi^2) \equiv 0 \bmod 8 \text{ for case } (2)$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 - \psi^2) \equiv 0 \bmod 8 \text{ for case } (3).$$

By the same arguments as in part (a) of Proposition 4.6, the conditions $-(\pm 1 - \phi) + \psi = y \in o'_N$, $\sigma^2\phi = \phi$ and $\sigma^2\psi = -\psi$ give rise to the relations, $-(\pm 1 - \phi_v) = a$, $\psi_v = b\sqrt{c}$ and $a \equiv b \bmod 2$ for some $a, b \in o_F = o_w$.

Using these relations we now have

$$\begin{aligned} \phi_v^2 - \psi_v^2 &= \phi_v^2 - b^2c \equiv \phi_v^2 + b^2 \equiv \phi_v^2 + a^2 \\ &\equiv 2\phi_v^2 + 2\phi_v + 1 \bmod 4 \text{ for case } (1), \\ 2\phi_v^2 + \psi_v^2 &= 2\phi_v^2 + b^2c \equiv 2(\phi_v^2 + b^2) \\ &\equiv 2(2\phi_v^2 + 2\phi_v + 1) \bmod 8 \text{ for case } (2) \end{aligned}$$

and

$$2\phi_v^2 - \psi_v^2 = 2\phi_v^2 - b^2c \equiv 2(\phi_v^2 + b^2)$$
$$\equiv 2(2\phi_v^2 + 2\phi_v + 1) \bmod 8 \text{ for case (3).}$$

We note that in each case the same congruence holds for any place t of N lying over the prime 2.

Therefore, for case (1),

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 - \psi^2) &= \sum_{t|2} \mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(\phi^2 - \psi^2) \\ &= \sum_{t|2} \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_t^2 - \psi_t^2) \\ &\equiv \sum_{t|2} \mathrm{Tr}_{F/\mathbf{Q}_2}(2\phi_t^2 + 2\phi_t + 1) \\ &= \mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 + 2\phi + 1) \\ &= 0 \bmod 4.\end{aligned}$$

Similarly, $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 + \psi^2) \equiv 0 \bmod 8$ for case (2) and $\mathrm{Tr}_{K/\mathbf{Q}}(2\phi^2 - \psi^2) \equiv 0 \bmod 8$ for case (3), which completes the proof of Proposition 5.6.

VI. The case in which $\#I_v = \#G_v = 4$

LEMMA 6.1. *There are exactly eight non-isomorphic totally ramified cyclic extensions of $\mathbf{Q}_2$ of degree four. These are the extensions $E = F(\sqrt{c})$ where $F = \mathbf{Q}_2(\pi)$, $\pi = \sqrt{2}$ or $\sqrt{10}$ and*

$$c = \pi(1+\pi), \pi(1+\pi)(1+\pi^4), \pi(1+\pi)(1+\pi^3) \text{ or}$$
$$\pi(1+\pi)(1+\pi^3)(1+\pi^4).$$

Proof. By local class field theory there are exactly eight non-isomorphic extensions of the above kind. For each $\pi = \sqrt{2}$ or $\sqrt{10}$, consider all Kummer 2-extensions E of F of degree two such that

(1) $E/\mathbf{Q}_2$ is normal with $\mathrm{Gal}(E/\mathbf{Q}_2) \cong \mathbf{Z}/4\mathbf{Z}$ and
(2) E is ramified over F.

These extensions are the ones listed in Lemma 6.1. Since these are all different from each other, the conclusion of Lemma 6.1 follows.

Now let N be an H_8-extension of $\mathbf{Q}$ with both the inertia subgroup I_v and decomposition subgroup G_v of order four, say, $I_v = G_v = \langle\sigma\rangle \subset G = H_8$ where v is a place of N over the prime 2. Let $w = w(v)$ be the place of K under v, where K is the biquadratic subfield of N. In this case, by means of an embedding of N into $\overline{\mathbf{Q}}_2$ which induces the place v, we may identify N_v (resp. K_w) with $E = F(\sqrt{c})$ (resp. F) for one of the values of c and π listed in Lemma 6.1 respectively. With this identification, we note that $o_w = o_F = \mathbf{Z}_2[\pi]$ and $o_v = o_E = o_F[\sqrt{c}]$.

We define a projective G-module o_N' as follows.

DEFINITION 6.2. Let

$$o_v' = o_E' = \mathbf{Z}_2[G_v](1 + \pi + \sqrt{c}) \subset o_v = o_E = o_F[\sqrt{c}].$$

As in Definition 2.1, let o_N' be the unique submodule of o_N such that

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} o_N' = \mathrm{Ind}_{G_v}^{G} o_v' \quad \text{and} \quad \mathbf{Z}_p \otimes_{\mathbf{Z}} o_N' = \mathbf{Z}_p \otimes_{\mathbf{Z}} o_N \text{ for } p \neq 2.$$

Remark 6.3. (1) By the remark following Definition 2.1, o_N' is projective.
(2) Since $\sigma\sqrt{c} / \sqrt{c} = u_1 + u_2\pi$ and $u_i \equiv 1 \bmod 2\mathbf{Z}_2$, $(o_v : o_v') = 8$. From the semi-local construction of o_N' we have $(o_N : o_N') = (o_v : o_v')^2 = 64$.

As in previous sections let

$$(o_N')^+ = \{x \in o_N' : \sigma^2 x = x\} \quad \text{and} \quad (o_N')^- = \{x \in o_N' : \sigma^2 x = -x\}.$$

Then by Lemma 3.4,

$$(o_N')^+ = o_N' \cap K = \mathbf{Z}^+\phi' \quad \text{and} \quad (o_N')^- = \mathbf{Z}^-\psi'$$

where ϕ' (resp. ψ') is a free basis over $\mathbf{Z}^+$ (resp. $\mathbf{Z}^-$). Let k_i, $i = 1, 2, 3$, be quadratic subfields of K and let $d_i = d_{k_i/\mathbf{Q}}$, the discriminant of k_i. Without loss of generality, we may assume that the prime 2 splits in k_1. Then $k_1 = \mathbf{Q}(\sqrt{d_1})$ with $\mathrm{Gal}(N/k_1) = G_v = \langle\sigma\rangle$, $k_2 = \mathbf{Q}(\sqrt{d_2/4})$ and $k_3 = \mathbf{Q}(\sqrt{d_3/4})$.

PROPOSITION 6.4. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = F(\sqrt{c})$ and $K_w = F = \mathbf{Q}_2(\pi)$.*

(1)

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 32 \bmod 128$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv -2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 32 \bmod 128,$$

for all the following four cases:

$$\pi = \sqrt{2} \quad \textit{and} \quad c = \pi(1+\pi),$$
$$\pi = \sqrt{2} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^4),$$
$$\pi = \sqrt{10} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^3),$$
$$\pi = \sqrt{10} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^3)(1+\pi^4)$$

(2)

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1+d_1) \equiv -2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 32 \bmod 128$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1+d_1) \equiv 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \equiv \pm 32 \bmod 128$$

for all the other four cases:

$$\pi = \sqrt{2} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^3),$$
$$\pi = \sqrt{2} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^3)(1+\pi^4),$$
$$\pi = \sqrt{10} \quad \textit{and} \quad c = \pi(1+\pi),$$
$$\pi = \sqrt{10} \quad \textit{and} \quad c = \pi(1+\pi)(1+\pi^4).$$

Proposition 6.4 will be a consequence of the following lemma and Proposition 3.3.

LEMMA 6.5.

(a) $d_1 \equiv 1 \bmod 8$ *and* $d_2/4 \equiv d_3/4 \equiv 2 \bmod 8$.

(b) $\dfrac{1 + d_1 + d_2/8 + d_3/8}{4} \equiv \left(\dfrac{2}{D_0}\right) \bmod 4$ *where* $D_0 = \prod_{\substack{p \neq 2,\\ p \mid d_{K/\mathbf{Q}}}} p$.

(c) $\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) = 4(1 + d_1 + d_2/4 + d_3/4)$.

(d) $\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) = \varepsilon(N)2^4 \prod_{\substack{p \neq 2,\\ p \mid d_{N/\mathbf{Q}}}} p$.

Proof of Lemma 6.5. (a) Since the prime 2 splits in k_1, $d_1 \equiv$ mod 8. It is shown by A. Fröhlich in [6, Theorem 3] that

$$(-1, d_1)_2(-1, d_2/4)_2(d_1, d_2/4)_2$$

should be equal to 1 for $K = k_1 k_2 = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2/4})$ the maximal abelian subfield of a quaternion field N, where the symbol $(\ , \ )_2$ is the Hilbert symbol. From this the congruence $d_2/4 \equiv d_3/4 \equiv 2 \bmod 8$ follows.

(b) Let d_0 be the greatest common divisor of d_1 and $d_2/4$ and let $d_1 = d_0 d_1'$, $d_2/4 = 2d_0 d_2'$ and $d_3/4 = 2d_1' d_2' \equiv 2 \bmod 8$. Then

$$\begin{aligned} \frac{1 + d_1 + d_2/8 + d_3/8}{4} &= \frac{1 + d_0 d_1' + d_0 d_2' + d_1' d_2'}{4} \\ &\equiv \left(\frac{2}{|d_0 d_1' d_2'|}\right) \\ &\equiv \left(\frac{2}{D_0}\right) \quad \bmod 4. \end{aligned}$$

(c) Let $o_K' = (o_N')^+ = o_N' \cap K$ and $H = \mathrm{Gal}(K/\mathbf{Q}) = \langle\bar{\sigma}\rangle x \langle\bar{\tau}\rangle \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

From the semi-local construction of o_N' (see Definition 6.2) we have

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} o_K' = \mathbf{Z}_p \otimes_{\mathbf{Z}} o_K \text{ for } p \neq 2$$

and

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} o_K' = \mathrm{Ind}_{H_w}^{H} o_w' = \mathbf{Z}[H] \otimes_{\mathbf{Z}[H_w]} o_w'$$

where $H_w = \langle\bar{\sigma}\rangle$ is the decomposition subgroup of the place w and $o_w' = o_v' \cap o_w$ which we can identify with $o_F' = o_E' \cap o_F = \mathbf{Z}_2[H_w]2(1 + \pi)$ by means of the embedding of N into $\overline{\mathbf{Q}}_2$ which induces the place v.

We note that o_K', as a free module over $\mathbf{Z}^+ = \mathbf{Z}[H]$, has

$$\phi_0' = \pm 1 + \sqrt{d_1} + \sqrt{d_2}/2 + \sqrt{d_3}/2$$

as a free generator. This results from the following conditions: for each irreducible character ξ of H, in order for ϕ' to be a free generator for o_K' over $\mathbf{Z}^+ = \mathbf{Z}[H]$, we must have

$$\mathrm{proj}_\xi \mathbf{Z}_p[H]\phi' = \mathrm{proj}_\xi(\mathbf{Z}_p \otimes_{\mathbf{Z}} o_K) \text{ for } p \neq 2$$

and

$$\mathrm{proj}_\xi \mathbf{Z}_2[H]\phi' = \mathrm{proj}_\xi(\mathbf{Z}[H] \otimes_{\mathbf{Z}[H_w]} o_w')$$

where $\mathrm{proj}_\xi = \frac{1}{4}\Sigma_{s \in H}\xi(s^{-1})s$, i.e., the idempotent corresponding to the irreducible character ξ.

Since by Proposition 3.5, $\phi' = \pm g\phi_0$ for some $g \in G = H_8$,

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) = \mathrm{Tr}_{K/\mathbf{Q}}(\phi_0'^2) = 4(1 + d_1 + d_2/4 + d_3/4).$$

(d) This follows from the same arguments as in Lemma 4.5(b). We just note here that

$$(o_K : o_K') = (o_w : o_w')^2 = (o_F : o_F')^2 = 64 = (o_N : o_N')$$

and that $\mathrm{ord}_2(d_{K/\mathbf{Q}}) = 6$ and $\mathrm{ord}_2(d_{N/\mathbf{Q}}) = 22$.

Proof of Proposition 6.4. By Proposition 3.3,

$$W_{N/\mathbf{Q}} = 1 \Leftrightarrow \left(\frac{2}{D_0}\right) \equiv W_2\varepsilon(N) \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p \bmod 4$$

and

$$W_{N/\mathbf{Q}} = -1 \Leftrightarrow \left(\frac{2}{D_0}\right) \equiv -W_2\varepsilon(N) \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p \bmod 4.$$

By Lemma 6.5,

$$\begin{aligned}\left(\frac{2}{D_0}\right) &\equiv \frac{1 + d_1 + d_2/8 + d_3/8}{4} \\ &\equiv \frac{\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2)/8 + (1 + d_1)/2}{4} \mod 4\end{aligned}$$

and

$$\varepsilon(N) \prod_{\substack{p \neq 2, \\ p \mid d_{N/\mathbf{Q}}}} p = \mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2)/16.$$

Therefore the proof of the proposition will be complete if we show the following results on local root numbers.

Claim.

$$W_2 = \begin{cases} 1 & \text{for all the four cases in (1)} \\ -1 & \text{otherwise.} \end{cases}$$

Proof of Claim. Let χ_2 be the restriction of χ to G_v where χ is the character of the unique two-dimensional irreducible representation of $G = H_8$. Then $\chi_2 = \lambda_2 + \bar{\lambda}_2$ for a character λ_2 of G_v of order four. We thus have

$$W_2 = W(\chi_2) = W(\lambda_2)W(\bar{\lambda}_2) = \lambda_2(-1)$$

where (-1) is the image of (-1) under the Artin map (see, for example, [8] or [13]). Since $(\mathbf{Z}_2^*)^4 = 1 + 2^4\mathbf{Z}_2$ is contained in the kernel of the Artin map in this case, λ_2 can be regarded as a character of

$$\mathbf{Z}_2^*/(\mathbf{Z}_2^*)^4 = (1 + 2\mathbf{Z}_2)/(1 + 2^4\mathbf{Z}_2) = \langle\bar{3}\rangle x \langle\bar{7}\rangle \cong \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

Furthermore $\lambda_2(3) = \pm i$ since $E/\mathbf{Q}_2$ is totally ramified. Therefore $(-1) \in \mathrm{Norm}_{E/\mathbf{Q}_2}(E^*)$ if and only if $7 \notin \mathrm{Norm}_{E/\mathbf{Q}_2}(E^*)$ since $(-1) \equiv 3^2 7 \bmod 16$.

The claim now results from the fact that

$$\mathrm{Norm}_{E/\mathbf{Q}_2}(1 + \sqrt{c}) \equiv 7 \bmod (1 + 2^4\mathbf{Z}_2)$$

for all the four cases in (2) and that there are exactly four cases for which 7 is in the norm group by local class field theory.

PROPOSITION 6.6. *Let $N/\mathbf{Q}$ be an H_8-extension with $N_v = E = F(\sqrt{c})$ and $K_w = F = \mathbf{Q}_2(\pi)$.*

(1) *For all the four cases in Proposition* 6.4 (1),

(a) $\psi' \equiv \phi' \bmod 2o_N' \Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 128$

(b) $\psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N'$

$$\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv -2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 128.$$

(2) *For all the other four cases in Proposition* 6.4 (2),

(a) $\psi' \equiv \phi' \bmod 2o_N'$

$$\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv -2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 128$$

(b) $\psi' \equiv \sigma\phi' + \tau\phi' + \sigma\tau\phi' \bmod 2o_N'$

$$\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \bmod 128.$$

Before proving Proposition 6.6, we note these corollaries.

COROLLARY 6.7. *The projective G-module o_N' which is defined in* 6.2, *is free if and only if*

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \quad \bmod 128$$

for all the four cases in Proposition 6.4 (1) *and*

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi'^2) + 4(1 + d_1) \equiv -2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi'^2) \mod 128$$

for the other four cases in Proposition 6.4 (2).

Proof. Combine Propositions 3.5 and 6.6.

COROLLARY 6.8. *Theorem* 1 *is true if the inertia and decomposition groups of v each has order four.*

Proof. This results from Propositions 6.4 and 2.4 and Corollary 6.7 by the same arguments as in the proof of Corollary 5.8.

Proof of Proposition 6.6. (a) Let $\psi' = \phi' + 2x$ for some $x \in o'_N$. Recall that $(o'_N)^+ = o'_K = \mathbf{Z}[H]\phi'$ and that $\phi'_0 = \pm 1 + \sqrt{d_1} + \sqrt{d_2}/2 + \sqrt{d_3}/2$ is one such generator. Since $\phi'_0 \in 2o_K$, o'_K is contained in $2o_K$, and we may set $\phi' = 2\phi$, $\phi'_0 = 2\phi_0$ and $\psi' = 2\psi$ where $\phi, \psi \in o_N$ and $\phi = \pm s\phi_0$ for some $s \in H = \mathrm{Gal}(K/\mathbf{Q})$.

Let $\phi_1 = \pm s((\pm 1 + \sqrt{d_1})/2)$ and $\phi_2 = \pm s((\sqrt{d_2}/2 + \sqrt{d_3}/2)/2)$ so that $\phi = \phi_1 + \phi_2$, $\sigma\phi_1 = \phi_1$ and $\sigma\phi_2 = -\phi_2$. Then $1 + d_1 = \mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2)$. It now suffices to show that

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + \mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2) - 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \bmod 32 \text{ for case } (1)$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + \mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2) + 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \bmod 32 \text{ for case } (2).$$

Denote by x_v the image of x under the embedding of N into $E = F(\sqrt{c})$ which has been identified with N_v. It is clear from the relations $\sigma^2\phi = \phi$, $\sigma^2\psi = -\psi$, $\sigma\phi_1 = \phi_1$ and $\sigma\phi_2 = -\phi_2$ that

$$\sigma^2\phi_v = \phi_v, \qquad \sigma^2\psi_v = -\psi_v, \qquad \sigma\phi_{1,v} = \phi_{1,v} \quad \text{and} \quad \sigma\phi_{2,v} = -\phi_{2,v}.$$

Therefore in $o_v = o_E = o_F[\sqrt{c}]$, $\phi_v \in o_F$ and $\psi_v \in o_F\sqrt{c}$. Furthermore the condition $\psi - \phi = x \in o'_N$ gives rise to the condition

$$\psi_v - \phi_v = x_v \in o'_v = o'_E = \mathbf{Z}_2[G_v](1 + \pi + \sqrt{c}).$$

Let

$$\psi_v - \phi_v = x_v = (\alpha + \beta\sigma + \gamma\sigma^2 + \delta\sigma^3)(1 + \pi + \sqrt{c})$$

where α, β, γ, and $\delta \in \mathbf{Z}_2$. Then we have

$$-\phi_v = (\alpha + \beta + \gamma + \delta) + (\alpha + \gamma - \beta - \delta)\pi,$$
$$\psi_v = (\alpha - \gamma)\sqrt{c} + (\beta - \delta)(\sigma\sqrt{c}),$$
$$\phi_{1,v} = -(\alpha + \beta + \gamma + \delta) \quad \text{and} \quad \phi_{2,v} = -(\alpha + \gamma - \beta - \delta)\pi.$$

Now it is straightforward by using these relations to prove that

$$\mathrm{Tr}_{K_{w(v)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 - 2\psi^2) = \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_v^2 + \phi_{1,v}^2 - 2\psi_v^2)$$
$$\equiv 0 \bmod 32 \text{ for case } (1),$$

and

$$\mathrm{Tr}_{K_{w(v)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 + 2\psi^2) = \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_v^2 + \phi_{1,v}^2 + 2\psi_v^2)$$
$$\equiv 0 \bmod 32 \text{ for case } (2).$$

We note that for each case, the same congruence also holds for the other place of N lying over the prime 2.

Therefore, for case (1),

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + (1 + d_1) - 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) &= \mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 + \phi_1^2 - 2\psi^2) \\ &= \sum_{t|2} \mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 - 2\psi^2) \\ &\equiv 0 \mod 32\end{aligned}$$

where t ranges over all the places of N lying over the prime 2.

Similarly, for case (2),

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + (1 + d_1) + 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \mod 32,$$

which completes the proof of (a).

(b) Let $\psi' = \sigma\phi' + \tau\phi' + \sigma\tau\phi' + 2y$ for some $y \in o_N'$. As in (a) we set $\phi' = 2\phi$ and $\psi' = 2\psi$. Then

$$\psi = \sigma\phi + \tau\phi + \sigma\tau\phi + y = \mathrm{Tr}_{K/\mathbf{Q}}(\phi) - \phi + y = \pm 2 - \phi + y,$$

where the last equality results from the fact that

$$\phi = \pm s\phi_0 \quad \text{and} \quad \phi_0 = \left(\pm 1 + \sqrt{d_1} + \sqrt{d_2}/2 + \sqrt{d_3}/2\right)/2.$$

Since $\mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2) = 1 + d_1$, it suffices to show that

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + \mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2) + 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \bmod 32 \text{ for case (1)}$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + \mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2) - 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \bmod 32 \text{ for case (2)}.$$

Since $y \in o'_N$, $y_v \in o'_v = o'_E = \mathbf{Z}_2[G_v](1 + \pi + \sqrt{c})$. Let

$$y_v = (\alpha + \beta\sigma + \gamma\sigma^2 + \delta\sigma^3)(1 + \pi + \sqrt{c})$$

for some α, β, γ and $\delta \in \mathbf{Z}_2$. Then by the same arguments as in (a), the conditions

$$-(\pm 2 - \phi) + \psi = y \in o'_N, \qquad \sigma^2\phi = \phi, \qquad \sigma^2\psi = -\psi,$$
$$\sigma\phi_1 = \phi_1 \quad\text{and}\quad \sigma\phi_2 = -\phi_2$$

give rise to the relations,

$$-(\pm 2 - \phi)_v = (\alpha + \beta + \gamma + \delta) + (\alpha + \gamma - \beta - \delta)\pi,$$
$$\psi_v = (\alpha - \gamma)\sqrt{c} + (\beta - \delta)(\sigma\sqrt{c}),$$
$$-(\pm 2 - \phi_{1,v}) = \alpha + \beta + \gamma + \delta \quad\text{and}\quad \phi_{2,v} = (\alpha + \gamma - \beta - \delta)\pi.$$

Using these relations it is straightforward to prove that for case (1),

$$\begin{aligned}
&\mathrm{Tr}_{K_{w(v)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 + 2\psi^2)\\
&= \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_v^2 + \phi_{1,v}^2 + 2\psi_v^2)\\
&= \mathrm{Tr}_{F/\mathbf{Q}_2}(2\phi_{1,v}^2 + \phi_{2,v}^2 + 2\psi_v^2)\\
&\equiv 16\{(\alpha + \beta + \gamma + \delta)^2 + (\alpha + \beta + \gamma + \delta) + 1\}\\
&\equiv 16(\phi_{1,v}^2 + \phi_{1,v} + 1)\\
&= 8\,\mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_{1,v}^2 + \phi_{1,v} + 1) \quad \bmod 32.
\end{aligned}$$

Similarly, for case (2),

$$\mathrm{Tr}_{K_{w(v)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 - 2\psi^2) \equiv 8\,\mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_{1,v}^2 + \phi_{1,v} + 1) \quad \bmod 32.$$

We note that for each case, the same congruence also holds for the other place of N lying over the prime 2.

Therefore, for case (1),

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + (1+d_1) + 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) &= \mathrm{Tr}_{K/\mathbf{Q}}(\phi^2 + \phi_1^2 + 2\psi^2) \\
&= \sum_{t|2} \mathrm{Tr}_{K_{w(t)}/\mathbf{Q}_2}(\phi^2 + \phi_1^2 + 2\psi^2) \\
&= \sum_{t|2} \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_t^2 + \phi_{1,t}^2 + 2\psi_t^2) \\
&\equiv 8 \sum_{t|2} \mathrm{Tr}_{F/\mathbf{Q}_2}(\phi_{1,t}^2 + \phi_{1,t} + 1) \\
&= 8\,\mathrm{Tr}_{K/\mathbf{Q}}(\phi_1^2 + \phi_1 + 1) \\
&\equiv 8(1+d_1) + 16 + 8\,\mathrm{Tr}_{K/\mathbf{Q}}(1) \\
&\equiv 0 \mod 32.
\end{aligned}$$

Similarly for case (2), $\mathrm{Tr}_{K/\mathbf{Q}}(\phi^2) + (1+d_1) - 2\,\mathrm{Tr}_{K/\mathbf{Q}}(\psi^2) \equiv 0 \bmod 32$ and this completes the proof of Proposition 6.6.

REFERENCES

1. Z. BOREVICH and I. SHAFAREVICH, *Number theory*, Academic Press, New York, 1966.
2. T. CHINBURG, *The analytic theory of multiplicative Galois structure*, Mem. Amer. Math. Soc., 1989.
3. ______, *Exact sequences and Galois module structure*, Ann. of Math., vol. 121 (1985), pp. 351–376.
4. ______, *On the Galois structure of algebraic integers and S-units*, Invent. Math., vol. 74 (1983), pp. 321–349.
5. A. FRÖHLICH, *Galois module structure of algebraic integers*, Springer-Verlag, New York, 1983.
6. ______, *Artin root number and normal integral bases for quaternion fields*, Invent. Math., vol. 17 (1972), pp. 143–166.
7. J. MARTINET, "H_8" in *Algebraic number fields*, Proc. Durham Symp. 1975, Academic Press, London, 1977, pp. 525–538.
8. ______, "*Character theory and Artin L-functions*" Proc. Durham Symp. 1975, in *Algebraic number fields*, Academic Press, London, 1977, pp. 1–87.
9. ______, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sci. E.N.S., vol. 4 (1971), pp. 399–408.
10. I. REINER, *Maximal orders*, Academic Press, London, 1975.
11. J. TATE, *les Conjectures de Stark sur les fonctions L d'Artin en s = 0, Notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher*, Progress in Math., vol. 47, Birkhäuser, Boston, 1984.
12. ______, *The cohomology groups of tori in finite Galois extensions of number fields*, Nagoya Math. J., vol. 27, (1966), pp. 709–719.
13. ______, "Local constants" in *Algebraic number fields*, Proc. Durham Symp. 1975, Academic Press, London, 1977, pp. 89–131.
14. M.J. TAYLOR, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math., vol. 63 (1981), pp. 41–79.

IMPERIAL COLLEGE
LONDON