H_8

J. Martinet

Theorem 5.1. of [M1] shows that quaternion extensions play a crucial role in the study of conductors and root numbers of symplectic characters. Only a few results, mainly due to Fröhlich, are known.

The aim of this section is to describe one of them, which concerns normal extensions N of $\mathbb{Q}$ with Galois group G isomorphic to the quaternion group H_8 of order 8. Such an extension will be called briefly a quaternion field, and we shall restrict ourselves to the case of a tamely ramified extension (i.e. 2 is not ramified in $N/\mathbb{Q}$).

Write $H_8 = \langle\sigma,\tau\rangle$ with relations $\sigma^4 = 1$, $\tau^2 = \sigma^2$, $\tau\sigma\tau^{-1} = \sigma^{-1}$, and imbed H_8 in the field of quaternions by $\sigma \longmapsto i$ and $\tau \longmapsto j$. Then the reduced trace defines a character χ, with values $\chi(1) = 2$, $\chi(\sigma^2) = -2$ and $\chi(s) = 0$ for $s \neq 1, \sigma^2$. This character is the unique irreducible character of degree 2 of H_8. We write W_N or W

for the Artin root number $W(\chi)$.

Since $N/\mathbb{Q}$ is tamely ramified, the ring O_N of integers of N is a projective module over $\mathbb{Z}[G]$. Now, the projective class group of $\mathbb{Z}[H_8]$ is of order 2 (see below). We define an invariant U_N (or simply U) of N by putting $U_N = +1$ or -1 according to whether O_N has a trivial image in this group or not.

Theorem 1 (Fröhlich) - $W_N = U_N$.

We shall define in a quite natural way a local invariant $U_{N,v}$ (or U_v) for every place v of $\mathbb{Q}$, with $U_v = 1$ almost everywhere and $U = \prod_v U_v$. Let $W_{N,v}$ (or W_v) be the local root number $W(\chi_v)$. Theorem 1. will be a consequence of the following local result we are going to prove.

Theorem 2 - $W_{N,v} = U_{N,v}$ for every place v of $\mathbb{Q}$.

For the details omitted in the proofs, the reader is referred to [M] and [F].

§1. $\mathbb{Z}[G]$-modules

Let M be a projective $\mathbb{Z}[G]$-module. Assume M is of

rank 1 (i.e. $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is free with one generator over $\mathbb{Q}[G]$), and define $M' = \{x \in M \mid x = \sigma^2 x\}$ and $M'' = \{x \in N \mid x + \sigma^2 x = 0\}$. Then, M' (resp. M'') can be given a structure of projective module over $\mathbb{Z}' = \mathbb{Z}[G]/(1 - \sigma^2)$ (resp. $\mathbb{Z}'' = \mathbb{Z}[G]/(1 + \sigma^2)$). Let $g = G/\{1,\sigma^2\}$. Then g is isomorphic to Klein's four group, and $\mathbb{Z}'$ is isomorphic to $\mathbb{Z}[g]$, whereas $\mathbb{Z}''$ is isomorphic to the ring $\mathbb{Z}[1,i,j,k]$ of integral quaternions. For both the rings $\mathbb{Z}'$ and $\mathbb{Z}''$, every projective module is free. Let now Φ (resp. ψ) be a basis for M' over $\mathbb{Z}'$ (resp. for M'' over $\mathbb{Z}''$). It is easily verified that Φ and ψ are well defined up to the sign and the conjugacy by an element of G. The following proposition is easy.

Proposition 3 The bases Φ and ψ can be chosen in such a way that one of the following congruences holds:

a) $\Phi \equiv \psi \mod 2M$

b) $\Phi \equiv \Phi\psi + \tau\psi + \sigma\tau\Phi \mod 2M$.

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

Proposition 3 implies that there are exactly 2

isomorphism classes of rank 1 projective $\mathbb{Z}[G]$-modules. But it can be proved for the particular group H_8 that given a free module F and a projective module P over $\mathbb{Z}[H_8]$, then $P \oplus F$ is free if and only if P is (cf. [M], §2). Hence, the projective class group of $\mathbb{Z}[G]$ is of order 2, and we identify this group with $\{-1, +1\}$.

§2. Quaternion fields

A quaternion field contains three quadratic subfields k_1, k_2, k_3 with respective discriminants d_1, d_2, d_3, and a biquadratic subfield K with discriminant $d_1 d_2 d_3$, the compositium of the k_i's. We define a positive integer D by $D^2 = d_1 d_2 d_3$. Write $N = K(\sqrt{M})$ for some $M \in K$ (one can take $M = \psi^2$ with the notation of §1 applied to the G-module O_N). Let m be a square free integer such that $\mathbb{Q}(\sqrt{m})$ is none of the k_i's. By elementary considerations of group theory, one proves that $N(\sqrt{m})$ contains besides N a unique quaternion field, say N_m, and that any quaternion field containing K is of the form N_m for some m. Clearly, $N_m = K(\sqrt{Mm})$. Moreover, N_m is a tamely ramified extension of $\mathbb{Q}$ if and only if $m \equiv 1 \bmod 4$.

Now let p be an odd prime number. Since the extensions

N/k_i are cyclic, if p is ramified in $K/\mathbb{Q}$, then every prime above p in K is ramified in N/K. Hence, for every prime factor p of m, either p is ramified in $K/\mathbb{Q}$ and has ramification index equal to 4 for both the fields N and N_m, or p is not ramified in K and is ramified in one and only one of the fields N, N_m, with ramification index 2. Hence, every quaternion field is of the form N_m for some m, where N is a "pure" quaternion field in the sense of [F], namely: every prime number ramified in $N/\mathbb{Q}$ is ramified in $K/\mathbb{Q}$.

We shall need in the sequel to know under what conditions a biquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ can be imbedded in a quaternion field (cf. [F]).

Proposition 4 A necessary and sufficient condition for K to be a subfield of a quaternion field is that the following condition holds for every place p of $\mathbb{Q}$:

$$(-1, d_1)_p \ (-1, d_2)_p \ (d_1, d_2)_p = +1.$$

Note that there is no condition for an unramified p. If p is the place at infinity, the above relation simply means that K must be totally real. If p splits in some quadratic subfield of K and is ramified in the others, it

simply means that p must be congruent to 1 mod 4.

The following proposition can be deduced from proposition 4.

Proposition 5 Let m be a square free integer. In order that $k = \mathbb{Q}(\sqrt{m})$ should be a quadratic subfield of a quaternion field, it is necessary and sufficient that m be positive and not congruent to -1 mod 8.

§3. The invariant U_N

Recall that $U_N = +1$ if O_N is a free $\mathbb{Z}[G]$-module and $U_N = -1$ otherwise. Put $\varepsilon(N) = +1$ if N is totally real and $\varepsilon(N) = -1$ if N is totally imaginary. Choose Φ and ψ as in §1 for the G-module O_N. Then,

$$\psi \equiv \Phi \bmod 2 \Rightarrow \Phi^2 \equiv \psi^2 \bmod 4 \Rightarrow \mathrm{Tr}_{K/\mathbb{Q}}(\phi^2) \equiv \mathrm{Tr}_{K/\mathbb{Q}}(\psi^2) \bmod 4,$$

whereas

$$\Phi \equiv \sigma\psi + \tau\psi + \tau\sigma\psi \bmod 2 \Rightarrow \mathrm{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv -\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2) \bmod 4.$$

Hence, $U_N = +1 \Leftrightarrow \mathrm{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv \mathrm{Tr}_{K/\mathbb{Q}}(\psi^2) \bmod 4$.

Proposition 6 a) $\mathrm{Tr}_{K/\mathbb{Q}}(\Phi^2) \equiv \dfrac{1+d_1+d_2+d_3}{4} \bmod 4.$

b) $\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2) \equiv \varepsilon(N) \prod_{\substack{p \text{ ramified} \\ \text{in } N/\mathbb{Q}}} p \bmod 4.$

Proof a) We may choose for Φ any normal basis of $K/\mathbb{Q}$. Taking $\Phi = \frac{1+\sqrt{d_1}+\sqrt{d_2}+\sqrt{d_3}}{4}$ gives immediately a).

b) We first remark that ψ^2 is totally positive if N is real and totally negative otherwise. Hence $\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2)$ and $\varepsilon(N)$ have the same sign. To find the ideal of $\mathbb{Z}$ generated by $\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2)$, we compute the discriminant $D(N/\mathbb{Q})$ of $N/\mathbb{Q}$ in two ways. On the one hand, write for the bilinear form $T = \mathrm{Tr}_{N/\mathbb{Q}}(xy)$ the direct sum decomposition $T = T' \oplus T''$, where $T' = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ on $N' = K$ and $T'' = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ on $N'' = \{x \in N \mid x + \sigma^2 x = 0\}$. This gives the formula $D(N/\mathbb{Q}) = D(K/\mathbb{Q})(\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2))^4$. On the other hand, we can use ramification groups to compute $D(N/\mathbb{Q})$. This gives the formula $D(N/\mathbb{Q}) = \prod_{\substack{p \text{ ramified} \\ \text{in } N/\mathbb{Q}}} p^4 \prod_{\substack{p \text{ ramified} \\ \text{in } K/\mathbb{Q}}} p^2$, and b) is proved.

We identify now $(\mathbb{Z}/4\mathbb{Z})^*$ with $\{-1, +1\}$, and write α_N or α for the image $\mathrm{Tr}_{K/\mathbb{Q}}(\Phi^2)$ and β_N or β for the image of $\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2)$ in $\{-1, +1\}$. Hence, $U_N = \alpha_N \beta_N$.

There is quite a natural decomposition of β as a product

of local terms $\beta_{N,v} = \beta_v$, namely:

$\beta_\infty = \varepsilon(N)$

$\beta_p = 1$ if p is unramified

β_p = image of p mod 4 $= (-1)^{(p-1)/2}$ if p is ramified.

Then, $\beta_v = 1$ almost everywhere, and $\beta = \prod_v \beta_v$.

It is less obvious to find what to choose for the α_v's. We use a remark of Fröhlich (cf. [F], §7): $\frac{1+d_1+d_2+d_3}{4} \equiv (\frac{2}{D})$ mod 4, where D^2 is the discriminant of $K/\mathbb{Q}$. We now define the α_v's:

$\alpha_v = +1$ if v is not ramified in $K/\mathbb{Q}$ (in particular, $\alpha_\infty = +1$)

$\alpha_p = (\frac{2}{p})$ for a finite prime p ramified in $K/\mathbb{Q}$.

Then, $\alpha_v = +1$ almost everywhere, and $\alpha = \prod_v \alpha_v$. Moreover, α_v depends only on the field K.

We know define local terms for U_N by $U_{N,v} = U_v = \alpha_v \beta_v$. Then, $U_v = +1$ almost everywhere and $U = \prod_v U_v$.

§4. Some computations of the invariant U_N

Let p be a prime number. Write $p' = (-1)^{(p-1)/2} p$, and assume that $\mathbb{Q}(\sqrt{p'})$ is not one of the fields k_i. Given a quaternion field N, we compare the local invariants of N and $N' = N_{p'}$. The proof of the following proposition is obvious

from the definition of the α_v's and β_v's.

Proposition 7

(i) $\beta_{N',\infty} = (-1)^{(p-1)/2}\beta_{N,\infty}$

(ii) $\beta_{N',p} = (-1)^{(p-1)/2}\beta_{N,p}$ if p is unramified in $K/\mathbb{Q}$

(iii) $\beta_{N',q} = \beta_{N,q}$ otherwise

(iv) $\alpha_{N',v} = \alpha_{N,v}$ for all v.

Corollary 8

$U_{N'} = U_N$ if p is unramified in $K/\mathbb{Q}$

$U_{N'} = (-1)^{(p-1)/2}U_N$ otherwise.

Corollary 9 Let Δ be the discriminant of a quaternion field containing a biquadratic field K such that at least one prime number $p \equiv 3 \bmod 4$ is ramified in K. Then, exactly half of the quaternion fields with discriminant Δ have invariant $U_N = +1$.

Corollary 10 Let K be a biquadratic field such that every prime number ramified in $K/\mathbb{Q}$ is congruent to 1 mod 4. Then

the quaternion fields N containing K, if any, have the same invariant U_N.

Remark Let us call this invariant U_K. Using Dirichlet's theorem on primes in arithmetic progressions together with propositions 4 and 5, it is easy to show that there exist infinitely many fields K with $U_K = +1$ and infinitely many fields K with $U_K = -1$.

§5. Proof of theorem 2.

We must verify for every place v of $\mathbb{Q}$ the equality

$$U_{N,v} = W_{N,v}.$$

(i) $v = \infty$. If N is real, then $\alpha_v = \beta_v = W_v = +1$. If N is imaginary, then $\alpha_v = +1$, $\beta_v = -1$, hence, $U_v = -1$. Now, the only possible choice for a real Frobenius substitution is $\sigma_v = \sigma^2$. Hence,

$$n(\chi,v) = \frac{\chi(1) - \chi(\sigma^2)}{2} = 2 \text{ and } W_v = i^{-n(\chi,v)} = -1.$$

We now consider the case of a finite prime p. Let G_p be the local Galois group. If p splits in at least one quadratic subfield of N, then G_p is cyclic of order 1, 2 or 4. If p does not split in K, then p is ramified in $K/\mathbb{Q}$. Hence, p is odd, $G_p = G$ and the inertia group I_p is

cyclic of order 4. Let χ_p be the restriction of χ to G_p.

(ii) G_p is cyclic. Then, $\chi_p = \phi_p + \bar{\phi}_p$, where ϕ_p is a character of G_p of order equal to that of G_p. We thus have $W_p = W(\chi_p) = \phi_p(-1)$.

If $I_p = \{1\}$, then ϕ_p is unramified. Hence, $W_p = \phi_p(-1) = +1 = U_p$.

If I_p is of order 2, then the restriction of ϕ_p to the group of p-adic units is the quadratic character $x \mapsto (\frac{x}{p})$. Hence, $W_p = (\frac{-1}{p}) = (-1)^{(p-1)/2} = U_p$ since $\alpha_p = 1$ and $\beta_p = (-1)^{(p-1)/2}$.

If $I_p = G_p$, then the restriction of ϕ to the group of p-adic units is a biquadratic character. Hence, $p \equiv 1 \mod 4$ and $W_p = \phi_p(-1) = (-1)^{(p-1)/4}$. But $\alpha_p = 1$ and $\beta_p = (\frac{2}{p})$. Since $p \equiv 1 \mod 4$, $(\frac{2}{p}) = (-1)^{(p-1)/4}$ and $W_p = U_p$.

(iii) $G_p = G$. Let k_p be a quadratic subfield of the completion N_p of N, let $H = \mathrm{Gal}(N_p/k_p)$, and let ϕ_p be a character of H of order 4.

Then, $\chi_p = \phi_p^*$, the character of G induced by ϕ_p. Let ε_p be the character of G lifted from the non trivial character of G/H. Then, $1^* = 1 + \varepsilon_p$.

Hence, $W((\chi_p - 1)^*) = W(\phi_p - 1)$, and therefore

$W(\chi_p) = W(\phi_p)\ W(\varepsilon_p)$. Take for k_p the field $\mathbb{Q}_p(\sqrt{(-1)^{(p-1)/2}p})$. Since $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})/\mathbb{Q}$ is ramified only at p, $W_p(\varepsilon_p)\ W_\infty(\varepsilon_p) = +1$. Hence, $W(\varepsilon_p) = +1$ for $p \equiv 1 \bmod 4$ and $W(\varepsilon_p) = +i$ for $p \equiv 3 \bmod 4$, a result known to Gauss! We thus have $W(\varepsilon_p)^2 = (-1)^{(p-1)/2} = \beta_p$. Now, an easy computation shows that the transfer Ver_G^H is not trivial.* This implies that the restriction of ϕ_p to $\mathbb{Q}_p^*$ is equal to ε_p. Since $\alpha_p = (\frac{2}{p}) = \phi_p(2)$, theorem 2 is a consequence of the following lemma.

Lemma 11 (Fröhlich, Queyrut) - Let K be a finite extension of a p-adic field. Let ε be a character of K^* of order 2 corresponding to a quadratic extension E of K. Let ϕ be a character of E^* whose restriction to K^* is ε. Assume that both ϕ and ε are ramified and tamely ramified. Then $W(\phi) = \phi(2)\ W(\varepsilon)$.

Proof Let v_K, v_E be the valuations of K, E respectively. Since ϕ and ε are ramified and tamely ramified, $v_K(\mathfrak{d}(\varepsilon)) = v_E(\mathfrak{d}(\phi)) = 1$.

With the notation of [M1] II, §2, we have the formulae

*Footnote: see Exercise 7.

$$W(\phi) = \frac{1}{\sqrt{N(\mathfrak{f}(\phi))}}\ \tau(\bar{\phi}) \quad \text{and} \quad W(\varepsilon) = \frac{1}{\sqrt{N(\mathfrak{f}(\varepsilon))}}\ \tau(\bar{\varepsilon}) ,$$

with :

$$\tau(\phi) = \sum_{x \in U_E/U_E^1} \phi(\tfrac{x}{c})\ \psi_E(\tfrac{x}{c}) \quad \text{and} \quad \tau(\varepsilon) = \sum_{x \in U_K/U_K^1} \varepsilon(\tfrac{x}{d})\ \psi_K(\tfrac{x}{d}) ,$$

where c generates $\mathcal{D}_{E/\mathbb{Q}_p}\mathfrak{f}(\phi)$ and d generates $\mathcal{D}_{K/\mathbb{Q}_p}\mathfrak{f}(\varepsilon)$.

Now, $v_E(\mathcal{D}_{E/K}) = 1$. Hence, $v_E(\mathcal{D}_{E/\mathbb{Q}_p}) = 1 + v_E(\mathcal{D}_{K/\mathbb{Q}_p}) = 1 + 2\, v_K(\mathcal{D}_{K/\mathbb{Q}_p})$, and $v_E(c) = 2v_K(d)$. We can therefore choose $c = d \in K$. Since E/K is totally ramified, the inclusion $K^* \subset E^*$ induces an isomorphism $U_K/U_K^1 \to U_E/U_E^1$. We can therefore choose the x's in U_K to compute $\tau(\phi)$. For such a choice for c and x, $\psi_E(\frac{x}{c}) = \psi_K(\frac{2x}{c})$. Hence,

$$\tau(\phi) = \bar{\phi}(2) \sum_{x \in U_K/U_K^1} \phi(\tfrac{2x}{d})\ \psi_K(\tfrac{2x}{d}) = \bar{\phi}(2)\ \tau(\varepsilon).$$

Since the conductors $\mathfrak{f}(\phi)$ and $\mathfrak{f}(\varepsilon)$ have the same absolute norm, $W(\phi) = \phi(2)\ W(\varepsilon)$,

Q.E.D.

REFERENCES

[F] A. Fröhlich - Artin Root Numbers and Normal Integral Bases for Quaternion Fields, Invent. Math., 17 (1972), 143-166.

[M] J. Martinet, Modules sur l'algèbre du groupe quaternionien, Ann. Sci. E.N.S., 4 (1971), 399-408.

[M1] J. Martinet, Character theory and Artin L-functions, Durham Symposium.