MÉMOIRES DE LA S. M. F.

A. FRÖHLICH

The Galois module structure of algebraic integer rings in fields with generalised quaternion group

Mémoires de la S. M. F., tome 37 (1974), p. 81-86

<http://www.numdam.org/item?id=MSMF_1974__37__81_0>

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France,
Mémoire 37, 1974, p. 81-86

THE GALOISMODULE STRUCTURE OF ALGEBRAIC INTEGER RINGS IN FIELDS WITH GENERALISED QUATERNION GROUP

by

A. FRÖHLICH

-:-:-:-

Let K and N be algebraic number fields, i.e., extensions of finite degree of the field Q of rational numbers, with N a normal extension of K with Galois group $Gal(N/K) = \Gamma$. Let $\mathfrak{O}$ and $\mathfrak{D}$ be the rings of algebraic integers in K, and in N respectively. Then $\mathfrak{D}$ is a module over the group ring $\mathfrak{O}(\Gamma)$, and we are interested in the global structure of this module. One knows (Theorem of Emmy Nöther) that $\mathfrak{D}$ is locally free over $\mathfrak{O}(\Gamma)$ (hence locally free of rank 1), if and only if N/K is at most tamely ramified. We assume this to be the case, so that we have fixed the local structure of $\mathfrak{D}$ over $\mathfrak{O}(\Gamma)$. It is then convenient to introduce the <u>classgroup</u> $\mathfrak{C}(\mathfrak{O}(\Gamma))$ of $\mathfrak{O}(\Gamma)$. This classifies the locally free rank one $\mathfrak{O}(\Gamma)$-modules to within stable isomorphism. Here two such modules M and M^1 are stably isomorphic, if there is a free $\mathfrak{O}(\Gamma)$-module F of finite rank, so that $M \oplus F = M^1 \oplus F$. We denote by $[\mathfrak{D}]$ the class in $\mathfrak{C}(\mathfrak{O}(\Gamma))$ of the module $\mathfrak{D}$. We wish to determine $[\mathfrak{D}]$. What is known in this direction so far concerns special cases, although it is possible to define general invariants of an arithmetic nature, which can be used to describe $[\mathfrak{D}]$, to unify the known results and to get more general theorems. This will be done elsewhere. Here I shall again consider a particular situation which leads to rather interesting results and problems.

Let now $K = Q$, i.e., $\mathfrak{O} = Z$. Write H_{4m} for the (generalised) quaternion group of order $4m$. We consider tamely ramified extensions N/Q with $Gal(N/Q) = H_8$. One knows that $\mathfrak{C}(Z(H_8))$ is of order 2, and in fact there are exactly two isomorphism classes of rank one $Z(H_8)$-modules. Martinet (cf. [4]) derived a handy algorithm to find $[\mathfrak{D}]$, and he computed examples both for $\mathfrak{D}$ to be free, and for $\mathfrak{D}$ to be locally free but not free. We now define an invariant U_N of tamely ramified fields N with $Gal(N/Q) = H_8$, taking values ± 1, by observing that we have an isomorphism

(1) $$\theta : \mathfrak{a}(Z(H_8)) \cong \pm 1 ,$$

and setting

(2) $$\theta([\mathfrak{O}]) = U_N .$$

We next define a second such invariant. First, let more generally N/K be a normal extension of algebraic number fields with arbitrary Galois group $Gal(N/K) = \Gamma$. Let ψ be any character of Γ, in the sense of representation theory over the complex numbers. The extended Artin L-series then satisfies a functional equation

$$\Lambda(s, N/K, \psi) = W(N/K, \psi)\Lambda(1-s, N/K, \bar{\psi}) ,$$

where $\bar{\psi}$ is the complex conjugate of ψ, and where the "root number" $W(N/K, \psi) = W(\psi)$ has absolute value 1. If $\psi = \bar{\psi}$ is real valued, then one knows that $W(\psi) = \pm 1$.

Now return to the case $K = Q$, $Gal(N/Q) = H_8$. All characters of H_8 are real valued, and by the multiplicativity of root numbers under character addition, it suffices to consider only irreducible ψ. Moreover for real Abelian, i.e., quadratic or trivial characters one knows that the value of the root number is 1. This just leaves the unique two-dimensional irreducible character ψ_8 of H_8, and we define

$$W(N/Q, \psi_8) = W_N .$$

Then I proved (cf. [1]) :

Theorem 1. <u>If</u> N/Q <u>is tamely ramified</u>, $Gal(N/Q) = H_8$, <u>then</u> $U_N = W_N$.

My attack on this problem was encouraged by Serre, who had computed U_N and W_N in one case where they both have value -1, followed by Armitage, who altogether computed twelve examples. I also showed that W_N takes each of the values ± 1 infinitely often, even with further arithmetic "boundary conditions" imposed (cf. [1]).

This theorem is rather surprising. The proof is based on a good arithmetic classification of the fields N, which essentially goes back to papers of mine of twenty years ago, but it does not give any real insight into why such a theorem should hold. Some other alternative proof would therefore be desirable.

Another problem is that of a possible generalisation of Theorem 1. Before one can formulate a conjecture one has to get good definitions of the invariants U_N and W_N and this itself involves serious and interesting problems. I shall here concentrate on W_N .

For the root numbers our original procedure for H_8 will not work. We shall call $\psi = \psi_{4m}$ *a quaternion character of order* $4m$ if it is an irreducible real valued character of H_{4m} of degree 2 , corresponding to a faithful representation of H_{4m} . There are such characters (for $m > 1$ of course), and, for given m , they are all conjugate over Q . In general one cannot expect that for any two such characters the root numbers coincide. In fact, we have

Theorem 2. *There is a unique field* N *containing* $Q(\sqrt{5})$ *with* $Gal(N/Q) = H_{20}$, *so that* $N/Q(\sqrt{5})$ *has conductor* 55 . *There are exactly two quaternion characters* ψ *and* ψ' *of order* 20 , *and for this field* N

$$W(N/Q,\psi) = -W(N/Q,\psi') .$$

Note however that N/Q is wildly ramified. In fact we do get

Theorem 3. *Let* N/K *be a normal extension with* $Gal(N/K) = H_{4m}$. *If* N/K *is tamely ramified, then the values of the root numbers* $W(N/K,\psi)$, *for all quaternion characters of order* $4m$ *coincide*.

Using this theorem we can now define, for a tamely ramified field N/Q with $Gal(N/Q) = H_{4m}$, the invariant W_N as the common value of the $W(N(Q,\psi))$, for ψ a quaternion character of order $4m$.

We shall say a few words about the background to Theorems 2 and 3. If $Gal(N/K) = H_{4m}$ then we have a field tower $K \subset E \subset N$, where E is quadratic over K , N cyclic over E . Let ϕ be the idele class character of

K , for which $E = K_\phi$ is the class field. Let χ be an idele class character of E with $N = E_\chi$. Viewed as a character of $Gal(N/E)$, this χ will induce a quaternion character ψ of order $4m$ of $Gal(N/K)$, and all such quaternion characters are given in this manner. Moreover, we ave $W(N/K,\psi) = W(\chi)$, and the various Abelian characters χ , with $N = E_\chi$, are all conjugate over Q . Finally, the fact that χ induces a quaternion character is expressed exactly in the equation $\chi | C_K = \phi$, where $\chi | C_K$ is the restriction of χ to the idele class group C_K of K. We thus have to compare root numbers of Abelian characters which are conjugate over Q.

Let Q^{cyc} be the maximal cyclotomic field inside the field of complex numbers. The Galois group $Gal(Q^{cyc}/Q)$ can be identified with $\prod_p U_p$ (product over all finite primes), where U_p is the group of p-adic units. This Galois group acts in a natural manner both on the Abelian characters and on their root numbers. Namely if η is an r-th root of unity, and $un \equiv 1 (\mathrm{mod}\ r)$, with $n \in Z$, then $\eta^u = \eta^n$. For $u \in \prod_p U_p$, $a \in Q^*$ define $(\frac{u}{a})$ by

$$(\frac{u}{a}) = \prod_p (\frac{u,a}{p})_2 \quad \text{(product of Hilbert symbols)},$$

or equivalently

$$(\frac{u}{a}) = \sqrt{a}^{\,u}/\sqrt{a} .$$

We then have

Theorem 4. <u>For any Abelian character</u> χ <u>of an algebraic number field</u> E, <u>and for</u> $u \in \prod_p U_p = Gal(Q^{cyc}/Q)$,

$$W(\chi)^u = W(\chi^u)\chi^u(u)(\frac{u}{Nf(\chi)})(\frac{u}{c(\chi)}) ,$$

<u>where</u> $Nf(\chi)$ <u>is the absolute norm of the conductor</u> $f(\chi)$, <u>and where</u> $c(\chi) = (-1)^{\gamma}$, γ <u>being the number of real places of</u> E <u>at which</u> χ <u>is ramified.</u>

Note for the definition of $\chi^u(u)$ that u is a rational idele, hence an idele of E. The case relevant to us is given by the

Corollary. <u>If</u> $W(\chi) = \pm 1$ <u>then</u>

$$W(\chi)/W(\chi^u) = \chi^u(u)(\frac{u}{Nf(\chi)})(\frac{u}{c(\chi)}) .$$

Serre has pointed out that the formula of Theorem 4 yields a similar formula for non-Abelian characters, namely

$$(*) \qquad W(\psi)^u = W(\psi^u)\,\delta_\psi^u(u)(\frac{u}{Nf(\psi)})(\frac{u}{c(\psi)}) .$$

Here δ_ψ is the "determinant" of ψ, i.e. viewed as a character of a Galois group it is given by

$$\delta_\psi(\gamma) = \det T(\gamma) \ ,$$

if $\gamma \to T(\gamma)$ is a representation corresponding to ψ. Also $c(\psi) = \prod c_v(\psi)$, v running through the real places of the base field E, with $c_v(\psi) = (-1)^{n_v}$, where n_v is the number of eigenvalues -1 of the v-Frobenius element σ_v in a representation corresponding to ψ. In other words $c_v(\psi) = \delta_\psi(\sigma_v)$.

Note that formula (*) allows one to regain a result of Dwork's, in answer to a question of Hasse, on the field in which $W(\psi)$ lies.

To get Theorem 2 one takes $E = Q(\sqrt{5})$, with the appropriate χ of order 10, ramified at 5 and at 11. The operator u is then chosen to be $u_5 = 3_5$, $u_p = 1$ for $p \neq 5$.

Theorem 3 follows from an explicit formula for $W(\chi)$. Let $\mathfrak{d}$ be the discriminant of E/K and let $E = K(\Delta)$, $\Delta^2 \in K$, with Δ integral and square free at all prime divisors $\mathfrak{P}$ of $\mathfrak{d}$ in E. The part of (Δ) "prime to $\mathfrak{d}$" is then a fractionnal ideal $\mathfrak{a}$ in K. Let moreover f^* be the part of $f(\chi)$ "prime to $\mathfrak{d}$". f^* is an ideal in K. One then has

Theorem 5. <u>If</u> $N = \bar{E}_\chi$, $E = K_\phi$ <u>quadratic over</u> K, <u>and if</u> N/K <u>is tamely ramified and</u> $Gal(N/K) = H_{4m}$, <u>then</u>

$$W(\chi) = \left(\frac{2}{\mathfrak{d}}\right)\phi(f^*) \prod_{\mathfrak{P}|\mathfrak{d}} \chi_{\mathfrak{P}}(\Delta) \ .$$

Theorem 3 follows almost immediately. For, $W(\chi)$, $\left(\frac{2}{\mathfrak{d}}\right)$ and $\phi(f^*)$ clearly take only ± 1 as possible values, hence so does $\prod_{\mathfrak{P}|\mathfrak{d}} \chi_{\mathfrak{P}}(\Delta)$. Therefore replacing χ by χ^u will not alter anything.

The proofs of Theorems 2-5 are contained in reference [3] below.

-:-:-:-

BIBLIOGRAPHY

[1] A. FRÖHLICH - Artin root numbers and normal integral bases for Quaternion Fields, Inventions Math. 17, 143-166 (1972).

[2] A. FRÖHLICH and J. QUEYRUT - On the functionnal equation of the Artin L-function for characters of real representations. To appear in Inventiones Math.

[3] A. FROHLICH - The root numbers, conductors and representations of Artin for generalised quaternion groups. To appear.

[4] J. MARTINET - Modules sur l'algèbre du groupe quaternionen. Ann. Sci. de l'Ecole Normale Sup. 4(3) 399-408 (1971).

-:-:-:-

A. FRÖHLICH
University of London,
King's College,
Strand, LONDON, WC2R 2LS.