Astérisque

ALBRECHT FRÖHLICH

Rings of integers in tame extensions as Galois module

Astérisque, tome 41-42 (1977), p. 31-33

<http://www.numdam.org/item?id=AST_1977__41-42__31_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.31-33

RINGS OF INTEGERS IN TAME EXTENSIONS AS GALOIS MODULES

par

Albrecht FRÖHLICH

-:-:-:-

For detailed statement, background and proofs see "Arithmetic and Galois module structure for tame extensions" (to appear in Crelle). See also "Galois module structure" (Proceedings of the Durham Symposium).

(1) Let Γ be a finite group, represented as Galois group of a normal extension N/K of number fields (always of finite degree over $\mathbb{Q}$). Assume N/K to be tame. Then the ring $\mathfrak{O}$ of algebraic integers in N as a module over the integral group ring $Z(\Gamma)$ is projective, and thus defines an element $(\mathfrak{O})_{Z(\Gamma)}$ of the class group $Cl(Z(\Gamma))$.

Let R_Γ be the additive group of virtual characters of Γ. Write $\Omega_{\mathbb{Q}}$ for $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in the complex field. Let $J(\bar{\mathbb{Q}})$ be the limit or union of idele groups $J(E)$ of all number fields $E \subset \bar{\mathbb{Q}}$. Then $Cl(Z(\Gamma))$ can be written as a quotient of $Hom_{\Omega_{\mathbb{Q}}}(R_\Gamma, J(\bar{\mathbb{Q}}))$, and the problem of determining $(\mathfrak{O})_{Z(\Gamma)}$ is solved by finding an element $g \in Hom_{\Omega_{\mathbb{Q}}}(R_\Gamma, J(\mathbb{Q}))$ which represents $(\mathfrak{O})_{Z(\Gamma)}$. Such a g is given by

$$(1) \qquad g(\chi) = \tau(N/K, \chi) \, . \prod_\sigma (a \mid \chi^{\sigma^{-1}})^\sigma , \qquad \text{for all } \chi \in R_\Gamma .$$

Here (i) $\tau(N/K, \chi)$ is the Galois Gauss sum for χ. (ii) $\{a^\gamma\}$ is a basis ("normal basis") of N/K, and for $T : \Gamma \to GL_n(\bar{\mathbb{Q}})$ a representation with character χ the resolvent is defined by

$$(a|\chi) = \det\left(\sum_{\gamma} a^{\gamma} T(\gamma)^{-1}\right)$$

the definition being extended to all $\chi \in R_\Gamma$ by linearity. (iii) $\{\sigma\}$ is a right transversal of $\Omega_K = \mathrm{Gal}(\overline{Q}/K)$ in Ω_Q.

A character χ is simplectic if some corresponding representation is symplectic. Let R_Γ^s be the subgroup of R_Γ generated by the symplectic characters. For $\chi \in R_\Gamma^s$ the root number $W(N/K, \chi)$ has values ± 1, and with g as in (1), $W(N/K, \chi) g(\chi)$ is totally positive. This together with the representation (1) implies that $(\mathfrak{O})_{Z(\Gamma)}$ lies in the so-called Kernel group $D(Z(\Gamma))$. In other words if $\mathfrak{M}$ is maximal oder of $Q(\Gamma)$, containing $Z(\Gamma)$ then $\mathfrak{O}\mathfrak{M}$ is stably free over $\mathfrak{M}$. For $K = Q$ this was conjectured by Martinet.

(2) For the kernel group we have the representation

$$(2) \qquad D(Z(\Gamma)) = \mathrm{Hom}^+_{\Omega_Q}(R_\Gamma, U(\overline{Q}))/\mathrm{Hom}^+_{\Omega_Q}(R_\Gamma, Y(\overline{Q})) \ \mathrm{Det}\, U(Z(\Gamma)).$$

Here $U(\overline{Q})$ is the union or limit of the groups of unit ideles $U(E)$, and $Y(\overline{Q})$ that of the groups of global units $Y(E)$ in number fields $E \subset Q$. The Hom^+ indicates that the images $f(\chi)$ for $\chi \in R_\Gamma^s$ should always be real and positive at infinity. $U(Z(\Gamma)) = \mathbb{R}(\Gamma)^* \times \prod_p Z_p(\Gamma)^*$, where $\mathbb{R}$ is the field of real numbers, and where $*$ stands for the multiplicative group of invertible elements. Moreover if $T : \Gamma \to GL_n(\overline{Q})$ is a reperesentation of Γ, we extend this to $T : Q(\Gamma)^* \to GL_n(\overline{Q})$ and then write $\det T(\lambda) = \det_\chi(\lambda)$, for $\lambda \in Q(\Gamma)^*$. This extends to $\lambda \in U(Z(\Gamma))$ and to $\chi \in R_\Gamma$. Write $\mathrm{Det}(\lambda)(\chi) = \det_\chi(\lambda)$. Then $\mathrm{Det}(\lambda) \in \mathrm{Hom}^+_{\Omega_Q}(R_\Gamma, U(\overline{Q}))$, and $\mathrm{Det}\, U(Z(\Gamma))$ is the group of these $\mathrm{Det}(\lambda)$.

Note that on the right of (2), the field $\overline{Q}$ can be replaced by a sufficiently large number field E. To obtain further information about $D(Z(\Gamma))$ and about the class $(\mathfrak{O})_{Z(\Gamma)}$ in it one has to use "congruences" on $U(E)$ together with restriction of maps to suitable subgroups of R_Γ, to get rid of the denominator in (2) coming from $\mathrm{Det}\, U(Z(\Gamma))$. This can be put under the heading of

A) Determinantal congruences

One is then left with the part of the denominator coming from $Y(\overline{Q})$, in other words one has to look at

B) Embedding of global in local units

To determine the image of $(\mathfrak{O})_{Z(\Gamma)}$ one has then to study

C) <u>Congruences on resolvents</u> $(a \mid \chi)$

and

D) <u>Congruences on Galois Gauss sums</u> $\tau(N/K, \chi)$.

(3) We give an example of this four-pronged attack on the problem. Let ℓ be a prime number, $\mathrm{Ker}\, d_\ell$ the kernel of "reduction mod ℓ" on R_Γ, or alternatively

$$\mathrm{Ker}\, d_\ell = [\chi \in R_\Gamma \mid \chi(\gamma) = 0 \text{ for } \ell\text{-regular } \gamma].$$

For E a big enough number field let V_ℓ be the multiplicative group of the residue class ring mod $\mathfrak{L}$ ($\mathfrak{L}$ = product of all prime ideals above ℓ). If $f \in \mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(Q))$ then write $r^s_\ell f$ for the composite map

$$R^s_\Gamma \cap \mathrm{Ker}\, d_\ell \longrightarrow R_\Gamma \longrightarrow U(\bar{Q}) \xrightarrow{\mathrm{mod}\, \mathfrak{L}} V_\ell .$$

Thus $r^s_\ell f \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R^s_\Gamma \cap \mathrm{Ker}\, d_\ell, V_\ell)$. If $\ell \nmid \mathrm{order}(\Gamma)$, the group on the right is null of course. Let

$$r^s f = \{r_\ell f\}_\ell \in \prod_{\ell \mid \mathrm{order}(\Gamma)} \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R^s_\Gamma \cap \mathrm{Ker}\, d_\ell, V_\ell).$$

Under the heading A) above we now get :

$$\mathrm{Det}\, U(Z(\Gamma)) \subset \mathrm{Ker}\, r^s .$$

Thus r^s yields a homomorphism

$$h^s : D(Z(\Gamma)) \longrightarrow E^s(\Gamma) = \prod_\ell \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R^s_\Gamma \cap \mathrm{Ker}\, d_\ell, V_\ell) / \mathbf{r}^s \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, Y(\bar{Q})).$$

The precise structure of $E^s(\Gamma)$ depends on the solution of problem B) above. But even without this we have under C) :

$$(a \mid \chi) \equiv 1 \pmod{\mathfrak{L}} \quad \text{if } \chi \in R^s_\Gamma \cap \mathrm{Ker}\, d_\ell$$

and under D)

$$\tau(N/K, \chi) \equiv 1 \pmod{\mathfrak{L}} \quad \text{if } \chi \in R^s_\Gamma \cap \mathrm{Ker}\, d_\ell .$$

Using this, one has the following result : $h^s((\mathfrak{D})_{Z(\Gamma)})$ is represented by a family of maps $f_\ell \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R^s_\Gamma \cap \mathrm{Ker}\, d_\ell, V_\ell)$ where for each ℓ and all $\chi \in R^s_\Gamma \cap \mathrm{Ker}\, d_\ell$,

$$f_\ell(\chi) = W(N/K, \chi) \mod \mathfrak{L} .$$

For further developments of the general method and further results see the lectures of Ph. Cassou-Noguès and of M. Taylor.

-:-:-:-

Albrecht FRÖHLICH
Univeristy of London King's College
Department of Mathematics
Strand London WC 2R 2LS