Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 463–466

Stably Free and Not Free Rings of Integers

Jean Cougnard

Let $N/\mathbb{Q}$ be a tame Galois extension of number fields with finite degree $[N : \mathbb{Q}]$ and Galois group G. One knows by the normal basis theorem that N is a free rank one $\mathbb{Q}[G]$-module. It is natural to look at the structure of the ring of integers $\mathcal{O}_N$ as a $\mathbb{Z}[G]$-module. The first known result is Hilbert's theorem which asserts that *If G is abelian and the discriminant of $N/\mathbb{Q}$ is prime to $[N : \mathbb{Q}]$ then $\mathcal{O}_N$ has a normal integral basis* ([Hi] satz 132); that is to say, there exists an algebraic integer $a \in N$ such that $\mathcal{O}_N$ has a basis made of the set $\{g(a) \mid g \in G\}$. The following result is E. Nœther's theorem which asserts that $\mathcal{O}_N$ is $\mathbb{Z}[G]$-projective if and only if $N/\mathbb{Q}$ is a tame extension; in fact Nœther's result shows that $\mathcal{O}_N$ is locally-free: for all prime p the extended module $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_N$ is $\mathbb{Z}_p[G]$-free with rank one. We can associate to $\mathcal{O}_N$ its image $[\mathcal{O}_N]$ in the projective class group $\mathrm{Cl}(\mathbb{Z}[G])$ of $\mathbb{Z}[G]$-modules; from now on, all the extensions will be tame. In 1968, J. Martinet proved that if G is a dihedral group of order $2p$, p an odd prime then $\mathcal{O}_N$ is $\mathbb{Z}[G]$-free. A few years after, in the case where $G = H_8$ (the quaternionic group of order 8), he was able to describe $\mathrm{Cl}(\mathbb{Z}[G]) \simeq \{\pm 1\}$ and to give a criterion for $\mathcal{O}_N$ free or not. Moreover, he produced rings of integers $\mathbb{Z}[G]$-free and not free ([Ma2]). Almost in the same time, Armitage gave examples of L-functions of quaternionic fields with a zero at $s = \frac{1}{2}$ ([A]).

Knowing the two results J-P. Serre did computations in [S] on examples and was surprised to see that the constant of the functional equation of the Artin L-series for the irreducible degree two character of $\mathrm{Gal}(N/\mathbb{Q})$ was 1 whenever $\mathcal{O}_N$ was free and -1 in the other cases. This was proved to be a theorem by A. Fröhlich [F1].

The following years A. Fröhlich proposed a nice conjecture finally established by M.J. Taylor [T]. We give a few notations before we state this theorem.

The first step was a description of the projective classgroup as a quotient of a group of equivariant maps from R_G (the group of characters

Received September 14, 1998

of the Galois group) to the idèles group of a sufficiently large field E. One can represent $\mathcal{O}_N$ in this group using a $\mathbb{Q}[G]$ basis of N and the $\mathbb{Z}_p[G]$-basis of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_N$. On the other hand one can construct a map from R_G to E by sending symplectic irreducible characters to $W(\chi)$ (the constant in the functional equation $L(s, \chi, N/\mathbb{Q})$) and the others on $+1$. The image $U_{N/\mathbb{Q}}$ of this map in $\mathrm{Cl}(\mathbb{Z}[G])$ is the Cassou-Noguès Fröhlich invariant (see [F2] for more details).

Theorem. *If $N/\mathbb{Q}$ is a tame Galois extension with Galois group G, we have in* $\mathrm{Cl}(\mathbb{Z}[G])$

$$[\mathcal{O}_N] = U_{N/\mathbb{Q}}.$$

This result has a lot of consequences. As symplectic characters are real we have $W(\chi) = \pm 1$ and so $U_{N/\mathbb{Q}}$ is of order 2.

Corollary. *If $N/\mathbb{Q}$ is a tame Galois extension with Galois group G, we have an isomorphism of $\mathbb{Z}[G]$-modules: $\mathcal{O}_N \bigoplus \mathcal{O}_N \cong \mathbb{Z}[G] \bigoplus \mathbb{Z}[G]$.*

When the class of a projective $\mathbb{Z}[G]$-module M is 0 in $\mathrm{Cl}(\mathbb{Z}[G])$ we can only say that $M \bigoplus \mathbb{Z}[G] \cong \mathbb{Z}[G] \bigoplus \mathbb{Z}[G]$; one says, in this case, that M is *stably free.* Unfortunately it is not always possible to cancel and to have $M \cong \mathbb{Z}[G]$ as was shown by R.G. Swan [Sw1]. Jacobinski has given sufficient conditions to allow cancellation: If G has no binary polyhedral quotient and $[M] = 0$ then $M \cong \mathbb{Z}[G]$. From this, we can deduce

Corollary. *If $N/\mathbb{Q}$ is a tame Galois extension whose Galois group G has no binary polyhedral quotient and if $W(\chi) = +1$ for all the irreducible symplectic characters, we have an isomorphism of $\mathbb{Z}[G]$-modules: $\mathcal{O}_N \cong \mathbb{Z}[G]$, that is to say, $\mathcal{O}_N$ possesses a normal integral basis.*

Let $\mathrm{Isom}_1(\mathbb{Z}[G])$ be the set of isomorphism classes of rank one projective $\mathbb{Z}[G]$-modules; we have the map φ which send each (M) of $\mathrm{Isom}_1(\mathbb{Z}[G])$ to $\varphi((M)) = [M]$ in $\mathrm{Cl}(\mathbb{Z}[G])$. We can ask the following question: can we represent each element in $\varphi^{-1}(0)$ by a ring of integers? In [SW2], R.G. Swan has extensively studied cancellation for binary polyhedral groups. Among the numerous computations (made thanks to Pari [P]) we quote that for the product $G = H_8 \times C_2$ of a quaternionic group of order 8 by a cyclic group of order 2 the set $\mathrm{Isom}_1(\mathbb{Z}[G])$ has 40 elements and $\mathrm{Cl}(\mathbb{Z}[G]) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; in this case $\varphi^{-1}(0)$ has four elements (note sixteen is the smallest order for which exists a group where stably free doesn't imply free). We can prove

Theorem [C]. *If $G = H_8 \times C_2$, each of the four classes of rank one stably free $\mathbb{Z}[G]$-modules can be represented infinitely many times by a ring of integers.*

The ingredients to prove this results are the followings: The Witt's criterion to embed a biquadratic bicyclic extension in a quaternionic one, and Martinet's criterion to decide if the quaternionic extensions have or not a normal integral basis; Witt's construction of quaternionic extensions linked with Martinet's criterion allows us to construct normal integral basis of quaternionic extensions when they exist. It is then possible to use Swan's computations to decide what the class of $\mathcal{O}_N$ is in $\mathrm{Isom}_1(\mathbb{Z}[G])$. We refer to [C] for the details.

References

[A] J. V. ARMITAGE, Zeta functions with zero at $s = \frac{1}{2}$, Invent. Mat., **15** (1972), 199–205.

[C] J. COUGNARD, Anneaux d'entiers stablement libres sur $\mathbb{Z}[H_8 \times C_2]$, Journal de Théorie des nombres de Bordeaux, **10** (1998), 163–201.

[F1] A. FRÖHLICH, Artin root numbers and normal integral bases for quaternionic fields, Invent. Math., **17** (1972), 143–166.

[F2] A. FRÖHLICH, Galois module structure of algebraic integers, Ergeb. der Math. 3 Folge Band 1. Springer Verlag (1983).

[Hi] D. HILBERT, Die Theorie der algebraischen Zahlkörper, Jahr. ber. der deutschen Math., **4** (1897), 175–546.

[J] H. JACOBINSKI, Genera and decomposition of latticesover orders, Acta math., **121** (1968), 1–29.

[Ma1] J. MARTINET, Sur l'arithmétique d'une extension galoisienne à groupe de Galois diedral d'ordre $2p$, Ann. Inst. Fourier, **19** (1969), 1–80.

[Ma2] J. MARTINET, Modules sur l'algèbre du groupe quaternionien, Ann. Sci. Ecole Norm. sup., **4** (1971), 399–408.

[No] E. NOETHER, Normalbasis bei Körpern ohne höhere Verzweigung, J. reine und angew. Math., **167** (1932), 147–152.

[P] C. BATUT, D. BERNARDI, H. COHEN, M. OLIVIER, User's Guide to Pari-GP version 1.39–12 (1995).

[S] J-P. SERRE, lettre à Jacques Martinet.

[Sw1] R.G. SWAN, Projective modules over group rings and maximal orders, Ann. of Math., **76** (1962), 55–61.

[Sw2] R.G. SWAN, Projective modules over binary p yhedral groups, J. reine und angew. Math., **342** (1982), 66–172.

[T] M.J. TAYLOR, On Fröhlich conjecture for rings of integers of tame extensions, Invent. Math. (1983), 41–79.

ESA 6081 du CNRS
Structures Discrètes et Analyse Diophantienne
Esplanade de la Paix
F14032 CAEN cedex
E-mail address: cougnard@math.unicaen.fr