MÉMOIRES DE LA S. M. F.

J. MARTINET

Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois

Mémoires de la S. M. F., tome 25 (1971), p. 123-126

<http://www.numdam.org/item?id=MSMF_1971__25__123_0>

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 123 à 126

ANNEAU DES ENTIERS D'UNE EXTENSION GALOISIENNE CONSIDERE COMME MODULE SUR L'ALGEBRE DU GROUPE DE GALOIS

par

Jacques MARTINET

-:-:-:-

§ 1. - Problèmes posés

Nous nous donnons un anneau de Dedekind A, de corps des fractions K, et une extension galoisienne L de K. Notons G le groupe de Galois de L/K et B la clôture intégrale de A dans L. Le groupe de Galois G opère sur B, et B se trouve ainsi muni d'une structure de module à gauche sur l'algèbre $A[G]$ du groupe G sur A.

Problème. - Etudier la structure de B en temps que $A[G]$-module.

En temps que A-module, B est de type fini, sans torsion. De plus, le $K[G]$-module $B \otimes_A K$ est libre, avec un générateur : il est en effet isomorphe à L, ce qui permet d'appliquer le théorème de la base normale de E. Noether. De manière générale, nous dirons qu'un $A[G]$-module M est de rang 1 si M est un A-module sans torsion de type fini et si $M \otimes_A K$ est libre avec un générateur.

Les premiers résultats obtenus sur ce problème l'ont été dans le cas où A est l'anneau $\mathbb{Z}$ des entiers rationnels et G est un groupe abélien.

Hilbert dans son traité ([1]), démontre en effet le résultat suivant : "Tout corps abélien C de degré M dont le discriminant D est premier avec M possède une base normale" (théorème 132).

Par base normale, on entend une base formée des conjugués d'un élément. Dire que B/A possède une base normale revient donc à dire que B est un $A[G]$-module libre avec un générateur. Ce résultat n'est pas le glus général possible ; nous reviendrons là-dessus au paragraphe suivant.

§ 2. - Modules projectifs sur $A[G]$

Nous allons tout d'abord chercher à obtenir des conditions portant tant sur l'anneau A que sur le groupe G permettant d'affirmer que B est libre sur l'anneau $A[G]$. Une condition nécessaire est bien entendu que B soit un $A[G]$-module projectif. Or on peut prouver sans difficulté le :

THEOREME. - Pour que B soit un A[G]-module projectif, il faut et il suffit que l'extension L/K soit modérément ramifiée. (voir[3], théorème II-1).

Revenons au théorème 132 de Hilbert. On peut sans difficulter aménager la démonstration donnée par Hilbert de façon à obtenir ce théorème de la base normale pour toute extension abélienne de $\mathbb{Q}$ modérément ramifiée. Le principe d'une démonstration est le suivant : le théorème de Kronecker-Weber prouve que l'on peut plonger une telle extension dans un corps cyclotomique L' . L'extension donnée étant modérément ramifiée, on peut choisir L' de façon que L'/$\mathbb{Q}$ soit modérément ramifiée. Le théorème 132 est évident pour un tel corps ; si θ' est une base normale de L' , on vérifie que $\theta = \mathrm{Tr}_{L'/L}(\theta')$ est une base normale de L . Il est clair que lorsque G n'est pas abélien ou encore losque A n'est plus l'anneau Z des entiers (par exemple lorsque A est un anneau d'entiers algébriques), le théorème de Kronecker-Weber ne s'applique plus ; la méthode de démonstration que nous avons brièvement décrite ne peut donc plus être employée.

Une méthode naturelle pour attaquer le problème est de définir des invariants caractérisant à un isomorphisme près les A[G]-modules projectifs de rang 1 , et de calculer ces invariants dans le cas d'une extension. Ainsi, on démontre le

THEOREME. - Soit A un anneau principal, p un nombre premier impair et G le groupe diédral d'ordre 2p . On suppose que $A/_{pA}$ et $A/_{2A}$ sont isomorphes respectivement au corps $\mathbb{Z}/_{p\mathbb{Z}}$ et $\mathbb{Z}/_{2\mathbb{Z}}$. Alors, si L/K est modérément ramifiée, B est libre sur A[G] ([3] , théorème VI-5).

Le principe de la démonstration est le suivant : notons σ et τ deux générateurs de G , d'ordres respectifs p et 2 et vérifiant par conséquent la relation $\tau\sigma\tau^{-1} = \sigma^{-1}$. Si M est un A[G]-module projectif de rang 1 , on vérifie que M^{τ} , ensemble des éléments de M invariants par τ , est stable par $\sigma + \sigma^{-1}$. On peut donc munir $M^{\tau}/_{M}G$ d'une structure de module sur l'anneau $A_o = \dfrac{A[\sigma+\sigma^{-1}]}{(1+\sigma+\ldots+\sigma^{p-1})}$. Cet anneau est en fait un anneau de Dedekind, isomorphe à l'anneau $A[\omega + \omega^{-1}]$, ω désignant une racine primitive p-ième de l'unité. Le A_o-module $M^{\tau}/_{M}G$ est isomorphe à un idéal de A_o , dont la classe est l'invariant cherché, caractérisant M à un isomorphisme près.

Il suffit alors de démontrer que cette classe est la classe principale lorsque M est la clôture untégrale B de A dans L pour obtenir le fait que B est libre sur A[G].

§ 3. - Extensions cycliques de degré premier

Dans ce paragraphe, G désigne un groupe cyclique de degré premier impair p et A un anneau principal. On note ω une racine primitive p-ième de l'unité, A' l'anneau $A[\omega]$ et $K' = K(\omega)$ le corps des fractions de A'. Soit M un $A[G]$-module de rang 1. Etant donné un caractère χ non trivial de G à valeurs dans K', on munit $M/_{M}G$ d'une structure de module sur A' en posant, pour tout σ de G et tout x de M, $\chi(\sigma) . x = \sigma x$ modulo M^G. Le quotient $M/_{M}G$ est alors isomorphe à un idéal de A', dont la classe sera appelée classe de M $(C(M))$.

On suppose que $A/_{pA}$ est un corps. On peut vérifier que

- ou bien M est projectif sur $A[G]$
- ou bien M peut être muni d'une structure de module sur l'ordre maximal $\mathfrak{O}$ de A dans $K[G]$, (et dans ce cas, M est évidemment projectif sur $\mathfrak{O}$.

Un $\mathfrak{O}$-module M de rang 1 est caractérisé à un isomorphisme près par sa classe $C(M)$. Il en est de même pour un module projectif sur $A[G]$ si l'on fait l'hypothèse supplémentaire que $A/_{pA}$ est un corps à p-éléments (voir par exemple D.S. Rim [5]). On peut, dans le cas d'une extension cyclique L de K ayant G pour groupe de galois, étudier la classe $C(B)$ de la clôture intégrale B de A dans L. On montre par exemple que $C(B)$ est une "classe relative", c'est-à-dire en posant $K_o = K(\omega+\omega^{-1})$, vérifiant l'égalité $N_{K/K_o}(C(B)) = 1$. Mais il est faux, en général, que $C(B) = 1$. Ainsi, pour $p = 3$, on prouve que toute classe d'idéaux de A' est de la forme $C(B)$ pour une extension L de K convenable. Ainsi, contrairement à ce qui se passe dans le cas d'une extension diédrale, des conditions purement algébriques portant sur l'anneau A ne semblent pas devoir entraîner un théorème de base normale. Pour d'autres résultats dans le cas $p = 3$, voir [4].

§ 4. - Les extensions qui ne sont pas modérément ramifiées

Nous conservons les notations du paragraphe 1. Lorsque l'extension L/K n'est pas modérément ramifiée, nous avons vu, au paragraphe 2, que B n'était pas un $A[G]$-module projectif, et que, par conséquent, B ne pouvait pas posséder de base normale.

Considérons alors l'anneau $\mathfrak{O} = \{\lambda \in K[G] \mid \lambda B \subset B\}$.

On vérifie sans peine que $\mathfrak{O}$ est un ordre de A dans $K[G]$, et que B ne peut être un module libre sur un ordre $\mathfrak{O}'$ de $K[G]$ que si $\mathfrak{O}' = \mathfrak{O}$.

Léopoldt ([2], Hauptsatz) a démontré le

THEOREME. - Lorsque A est l'anneau $\mathbb{Z}$ des entiers rationnels et l'extension L/K est abélienne, B est un module libre sur l'ordre $\mathfrak{O}$.

La démonstration repose sur le théorème de Kronecker-Weber, tout comme celle du théorème 132 de Hilbert, mais les difficultés sont beaucoup plus considérables.

On peut prouver, dans le cas général, où K est de caractéristique 0 , que l'ordre est égal à A[G] si et seulement si l'extension L/K est modérément ramifiée, ce qui fait apparaître le résultat de Hilbert comme un cas particulier du théorème de Léopoldt.

On peut se poser le problème de savoir si B est toujours un module projectif sur $\mathfrak{O}$. Hormis dans les cas couverts par le théorème de Léppoldt, il semble qu'on ne sache rien sur cette question.

-:-:-:-

BIBLIOGRAPHIE

[1] D. HILBERT. - Théorie des corps de nombres algébriques. Paris (1915).

[2] H.W. LEOPOLDT. - Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers. Jour. reine angew. Math. 201 (1959) pp. 119-149.

[3] J. MARTINET. - Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p . Annales de l'Institut Fourier, 19, 1, (1969) pp. 1-80.

[4] J. MARTINET et J.J. PAYAN. - Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne. Jour. reine angew. Math. 228 (1967) pp. 15-37.

[5] D.S. RIM. - Modules over finite groups. Ann. of Math. 69 (1959) pp. 700-712.

-:-:-:-

Faculté des Sciences de Bordeaux
Département de Mathématiques
351, cours de la Libération
33 - Talence (France)