THEORIE DES NOMBRES
BESANÇON

Années 1979-1980
et 1980-1981

A PROPOS DU GENRE DE L'ANNEAU DES ENTIERS D'UNE EXTENSION

Anne-Marie BERGÉ

A PROPOS DU GENRE DE L'ANNEAU

DES ENTIERS D'UNE EXTENSION

par A.-M. BERGÉ

Pour tout corps de nombres global ou local F, nous notons O_F son anneau d'entiers ou de valuation.

Soit N/F une extension galoisienne de corps de nombres, de groupe de Galois G. Pour décrire le genre de O_N considéré comme module sur l'algèbre $O_F[G]$, nous cherchons à définir canoniquement un idéal fractionnaire I de $O_F[G]$ représentant ce genre, c'est-à-dire localement isomorphe à O_N. La considération du cas des extensions modérément ramifiées (cf. [6]) et du cas des extensions absolument abéliennes (cf. [5]) a orienté les recherches vers l'ordre* associé à O_N dans l'algèbre $F[G]$, seul ordre susceptible d'appartenir au genre de O_N. Nous savons maintenant que cet invariant ne convient pas (cf. [1]). Nous nous proposons ici d'analyser les obstructions que l'on rencontre à diverses étapes de réduction, en les reliant à un mauvais comportement fonctoriel de l'ordre associé, comportement que nous étudions d'abord dans un contexte plus général.

§ 1 - Ordre associé et changement de groupe ou de corps de base

Soit A l'algèbre d'un groupe fini sur un corps local, et soit M un module sur un ordre de A, de rang déterminé. Nous notons

---

* idéal fractionnaire contenant 1 et multiplicativement stable.

$\Lambda(M,A)$ l'ordre associé à M dans A, c'est-à-dire l'ensemble des éléments de A qui opèrent dans M. C'est le comportement de cet ordre lors de changements standards de A que nous étudions maintenant.

Tout au long de ce paragraphe, K désigne un corps local dont nous notons simplement $O = O_K$ l'anneau de valuation, et G est un groupe fini.

1. Extension des scalaires

Soient $\overline{K}$ une extension finie de K, $\overline{O} = O_{\overline{K}}$ son anneau de valuation, et soit M un $O[G]$-module de rang déterminé.

Le produit tensoriel $\overline{O} \otimes_O M$ est muni, de façon naturelle, d'une structure de module sur l'algèbre $\overline{O}[G]$ (identifiée à $\overline{O} \otimes_O O[G]$). Le O-module $\overline{O}$ étant libre et de type fini, on obtient immédiatement :

$$(1) \qquad \Lambda\left(\overline{O} \otimes_O M, \overline{K}[G]\right) = \overline{O} \otimes_O \Lambda\left(M, K[G]\right).$$

Il en résulte un transport de structure :

Proposition 1. Pour que $\overline{O} \otimes_O M$ soit projectif sur son ordre dans $\overline{K}[G]$, il faut et il suffit que M soit projectif sur son ordre dans $K[G]$.

Notons qu'une telle extension des scalaires, appliquée à un corps, détruit en général sa structure de corps (comme d'ailleurs cela se produit pour les complétions semi-locales), et nous cherchons à revenir au cas d'un corps. Pour cela, nous étudions maintenant la transition à un facteur direct et le passage inverse :

2. Passage à un sous-groupe et induction

Rappelons les considérations élémentaires que nous avons appliquées dans [2] à l'étude des complétions semi-locales :

Soit H un sous-groupe de G, et soit M un $O[H]$-module de rang déterminé. Le module induit $O[G] \otimes_{O[H]} M$ (ou plus simplement $G \underset{H}{\otimes} M$) est muni d'une structure naturelle de module sur $O[G]$. Comme le retour au facteur direct M conserve notre invariant -à savoir la projectivité sur l'ordre associé - (cf. [2]), nous nous limitons à l'induction proprement dite.

Clairement, elle "conserve les isomorphismes". En particulier, si M est isomorphe à un idéal fractionnaire I de $O[H]$, alors le $O[G]$-module $G \underset{H}{\otimes} M$ est isomorphe à l'idéal fractionnaire $G \underset{H}{\otimes} I$ de $O[G]$.

Mais la propriété pour I d'être un ordre peut, lorsque G n'est pas abélien, être détruite par l'induction. Introduisons, pour toute la suite, les notations suivantes :

Pour $g \in G$, $\lambda = \sum_s a_s \, s \in K[G]$, et $U \subset K[G]$, on pose :

$$^g\lambda = \sum_s a_s \, g s g^{-1}, \quad ^gU = \{^g\lambda, \lambda \in U\}, \quad ^GU = \bigcap_{g \in G} {}^gU.$$

La formule générale donnant l'ordre associé au module induit s'écrit alors :

$$(2) \qquad \Lambda\left(G \underset{H}{\otimes} M, K[G]\right) = {}^G\left(G \underset{H}{\otimes} \Lambda\left(M, K[H]\right)\right).$$

Nous nous bornons désormais au cas où <u>H est un sous-groupe distingué de G</u>. Le groupe G opère alors dans l'algèbre $K[H]$ $\left(\text{par } \lambda \to {}^g\lambda\right)$, et la formule (2) devient :

$$(2^*) \qquad \Lambda\left(G \underset{H}{\otimes} M, K[G]\right) = G \underset{H}{\otimes} {}^G\Lambda\left(M, K[H]\right).$$

D'où, immédiatement la

<u>Proposition 2.</u> Pour que le G-module $O[G] \underset{O[H]}{\otimes} M$ soit projectif sur son ordre dans $K[G]$, il faut et il suffit que M soit projectif sur l'ordre ${}^G\Lambda\left(M, K[H]\right)$ de $K[H]$.

Dans le cas où G est abélien, ou bien dans le cas où $\Lambda\left(M, K[H]\right) = O[H]$, et d'une façon générale dans le cas où l'ordre

$\Lambda(M, K[H])$ est stable sous l'action $\lambda \to {}^g\lambda$ de G, l'induction conserve notre invariant. Cela peut aussi se produire dans d'autres circonstances (par exemple lorsque ${}^G\Lambda(M, K[H])$ est un ordre héréditaire). Cependant, lorsque le sous-groupe H est abélien, on obtient une contrainte sur l'ordre $\Lambda(M, K[H])$:

$$(2') \qquad \forall g \in G, \qquad {}^g\Lambda(M, K[H]) = \Lambda(M, K[H]).$$

(conséquence immédiate de la proposition 2, puisque ${}^G\Lambda(M, K[H])$ est un ordre "propre").

3. Passage aux groupes quotient

Ici encore, H désigne un sous-groupe distingué de G. L'idempotent

$$e_H = \frac{1}{\operatorname{card} H} \sum_{h \in H} h$$

appartient alors au centre de l'algèbre $K[G]$, et nous identifions les algèbres $K[G/H]$ et $e_H K[G]$.

Soit M un $O[G]$-module de rang déterminé. On peut définir, de façon naturelle, un module $e_H M$ sur $e_H O[G] = O[G/H]$. On a trivialement l'inclusion

$$(3) \qquad e_H \Lambda(M, K[G]) \subset \Lambda(e_H M, K[G/H]),$$

et la

Proposition 3. Si M est projectif (resp. libre) sur son ordre dans $K[G]$, alors $e_H M$ est projectif (resp. libre) sur l'ordre $e_H \Lambda(M, K[G])$ de $K[G/H]$.

Ici encore, nous voyons apparaître une obstruction liée à l'écart entre les deux membres de (3). Plus précisément, si nous supposons le quotient G/H abélien, nous obtenons une contrainte sur l'ordre associé :

$$(3') \qquad e_H \Lambda(M, K[G]) = \Lambda(e_H M, K[G/H]).$$

<u>Remarque</u> : Soit $G = H_1 \ltimes H_2$ le produit semi-direct du sous-groupe H_1 par le sous-groupe distingué H_2. Nous pouvons déduire de (3') une condition d'induction de H_1 à G (même lorsque H_1 n'est pas distingué dans G). En effet, le $O[H_1]$-module M est isomorphe à $e_{H_2}\left(G \underset{H_1}{\otimes} M\right)$.

2 - Application à l'arithmétique

On sait que l'on peut ramener l'étude d'une extension galoisienne de corps de nombres à celle d'extensions galoisiennes de corps locaux, quitte à élargir la notion de représentant "canonique" à certains idéaux fractionnaires induits (pour certaines places sauvages) par des ordres (cf. [2]).

Soit donc L/K une extension galoisienne de corps locaux, de groupe de Galois G. Nous étudions la réduction à des extensions intermédiaires.

1. Soit d'abord $F = L^H$ le sous-corps fixé par un sous-groupe distingué de G. C'est une extension galoisienne de K, de groupe de Galois G/H. La condition d'inflation (3'), appliquée au module $M = O_L$, fournit une contrainte sur l'ordre associé à O_L, et par là sur la ramification, à l'origine de nombreux contre-exemples.

<u>Exemple</u>. Soient $p > 2$ et p' deux nombres premiers distincts, et $q = p^s$ une puissance de p. Le corps $N = \mathbb{Q}\left(\sqrt[q]{1}, \sqrt[q]{p'}\right)$ est une extension galoisienne de $\mathbb{Q}$, de groupe de Galois $G = H_1 \ltimes H_2$, où $F = N^{H_2} = \mathbb{Q}\left(\sqrt[q]{1}\right)$, et dans laquelle seul p est sauvagement ramifié. Soit $\mathfrak{P}$ un idéal premier de N au-dessus de p, et $\mathfrak{p}$ sa trace sur F.

$$\begin{tikzcd} N \arrow[d, dash] \arrow[d, bend right=60, dash, "H_2"'] \arrow[dd, bend left=60, dash, "G"] \\ F \arrow[d, dash] \arrow[d, bend right=60, dash, "H_1"'] \\ \mathbb{Q} \end{tikzcd} \qquad\qquad \begin{tikzcd} N_{\mathfrak{P}} \arrow[d, dash] \arrow[d, bend left=60, dash, "D_2"] \arrow[dd, bend right=60, dash, "D"'] \\ F_{\mathfrak{p}} \arrow[d, dash, "H_1"] \\ \mathbb{Q}_p \end{tikzcd}$$

- Si l'idéal $\mathfrak{p}$ n'est pas complètement décomposé dans N, et si l'on a $q \neq p$, l'extension $N_{\mathfrak{P}}/\mathbb{Q}_p$ ne vérifie pas la condition (3') relativement à la sous-extension cyclique $F_{\mathfrak{p}}/\mathbb{Q}_p$.

- Si au contraire $\mathfrak{p}$ est complètement décomposé dans N, c'est-à-dire si $N_{\mathfrak{P}} = F_{\mathfrak{p}}$, alors l'anneau de valuation $O_{N,\mathfrak{P}}$ est libre sur l'ordre maximal $\mathfrak{M}$ de $\mathbb{Q}_p[H_1]$, et le G-module $O_{N,p}$ est isomorphe à l'idéal $G \underset{H_1}{\otimes} \mathfrak{M}$, qui n'est projectif sur son ordre associé dans $\mathbb{Q}_p[G]$ que si $q = p$ (nous utilisons la remarque de § 1, 3.).

Prenons par exemple $q = 3^s$, et $p' = 53$ $\left(\text{donc } p' \equiv -1 \bmod 3^3\right)$. Il n'existe un ordre dans le genre de O_N que pour $s = 1$. Pour $s = 2$, on peut choisir comme représentant l'idéal fractionnaire I de $\mathbb{Q}[G]$ défini par $I_\ell = \mathbb{Z}_\ell[G]$ pour $\ell \neq 3$, et $I_\ell = G \underset{H_1}{\otimes} \mathfrak{M}$ pour $\ell = 3$. Pour $s \geq 3$, le problème reste ouvert ...

Dans l'exemple ci-dessus, les extensions $N_{\mathfrak{P}}/\mathbb{Q}_p$ sont totalement ramifiées. Nous consacrons le reste du paragraphe à la réduction du cas général à ce cas-là.

2. Soient T le sous-groupe d'inertie de G, et K_T le corps d'inertie. Posons $O = O_K$ et $O_T = O_{K_T}$.

La propriété de non-ramification de l'extension K_T/K intervient sous la forme suivante :

<u>Lemme</u>. Soit $\left(g(a)\right)_{g \in G/T}$ une base normale d'entiers de O_T sur O. Alors $\det\left[g g'(a)\right]$ est inversible dans O_T.

Démonstration : évidente dans l'extension résiduelle.

Nous notons provisoirement <u>$\tilde{L}$ le corps L considéré comme extension de K_T</u>. Pour étudier le passage de L/K à $\tilde{L}/K_T$ et inversement, nous introduisons la K_T-algèbre galoisienne $\overline{L} = K_T \underset{K}{\otimes} L$ (cf. [3]). L'isomorphisme canonique de $\overline{L}$ sur $G \underset{T}{\otimes} \widetilde{L}$ qui envoie $1 \otimes x$ sur $\sum_{g \in G/T} g \otimes g^{-1}(x)$ induit, d'après le lemme, un isomorphisme

$$(4) \qquad O_T \underset{O}{\otimes} O_L \xrightarrow{\sim} O_T[G] \underset{O_T[T]}{\otimes} O_{\widetilde{L}}$$

de $O_T[G]$-modules.

En combinant alors les résultats des parties 1 et 2 du paragraphe 1 (et effectivement T est distingué dans G), on obtient une nouvelle preuve d'un résultat de Jacobinski

$$(5) \qquad \Lambda\left(O_L, K[G]\right) = O[G] \underset{O[T]}{\otimes} \Lambda\left(O_L, K[T]\right)$$

(cf. [4]), et le critère suivant :

<u>Théorème</u> : Pour que, dans l'extension L/K, O_L soit projectif sur son ordre dans $K[G]$, il faut et il suffit que, pour l'extension totalement ramifiée L/K_T, O_L soit projectif sur l'ordre

$${}^{G}\Lambda\left(O_L, K_T[T]\right).$$

Remarquons que cet ordre peut être obtenu autrement :

<u>Proposition 4</u>. On a ${}^{G}\Lambda\left(O_L, K_T[T]\right) = O_T \underset{O}{\otimes} \Lambda\left(O_L, K[T]\right)$.

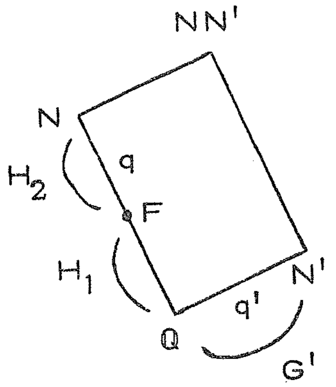
Démonstration : Dans le "twisted group ring" $K_T[G]$, qui opère dans L, l'ordre $\Lambda = \Lambda\left(O_L, K_T[T]\right)$ est invariant par conjugaison. L'ordre ${}^{G}\Lambda$ est donc égal à $G.\Lambda$, plus grand sous-anneau de Λ stable sous l'action suivante de G sur $K_T[T]$: Pour $g \in G$ et $\lambda = \sum_{t \in T} a_t t \in K_T[T]$, on pose $g.\lambda = \sum_t g(a_t)\, t$. On conclut grâce au lemme.

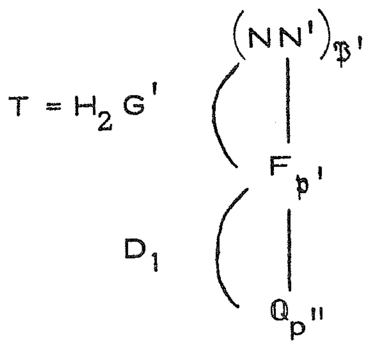
La condition d'induction (2') peut donc s'écrire, ici :

$$(2'') \qquad O_T \underset{O}{\otimes} \Lambda\left(O_L, K[T]\right) = \Lambda\left(O_L, K_T[T]\right),$$

ce qui généralise un résultat de [1] à l'origine des premiers exemples d'extensions de $\mathbb{Q}$ dépourvus d'une "bonne" structure galoisienne locale :

Exemple. Considérons le composé NN' du corps $N = \mathbb{Q}\left(\sqrt[q]{1}, \sqrt[q]{p'}\right)$ précédent par le sous-corps N' de $\mathbb{Q}\left(\sqrt[q']{1}\right)$, où $q' = p'^2$, qui est de degré p' sur $\mathbb{Q}$ (lorsque $p' = 2$, il convient de prendre $q' = p'^3$). On étudie le complété $(NN')_{p'}$ de NN' pour la valuation p'-adique.





Les extensions totalement ramifiées $(NN')_{\mathfrak{P}'}/F_{\mathfrak{p}'}$ auxquelles on est ramené ont une bonne structure galoisienne (il en irait autrement si nous remplacions p' par p'^2, les critères d'inflation (3') pouvant être en défaut pour q assez grand, cf. [1]). Mais nous rencontrons une obstruction pour le retour aux extensions $(NN')_{\mathfrak{P}'}/\mathbb{Q}_{p'}$, les conditions (2'') n'étant pas vérifiées lorsque $q > p'$, et dans ce cas encore, le problème de la recherche d'un bon représentant local reste entier ...

BIBLIOGRAPHIE

[1] A.-M. BERGÉ
Arithmétique d'une extension galoisienne à groupe d'inertie cyclique, Ann. Inst. Fourier, 28, 4 (1978), 17-44.

[2] A.-M. BERGÉ
Projectivité des anneaux d'entiers sur leurs ordres associés, Société Mathématique de France, Astérisque 61 (1979), 15-28.

[3] A. FRÖHLICH
Module conductors and module resolvents, Proc. London Math. Soc., 32 (1976) 279-321.

[4] H. JACOBINSKI
Über die Hauptordnung eines Körpers als Gruppenmodul, J. reine angew. Math., 213 (1963), 151-164.

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

[6] E. NOETHER
Normal basis bei Körpern ohn höhere Verzweigung, Jour. reine angew. Math., 167 (1932), 147-152.

Anne-Marie BERGÉ
U. E. R. de Mathématiques
et d'Informatique de l'Université
de Bordeaux I
351, Cours de la Libération
33405 Talence Cedex.