Astérisque

R. MASSY

Sur les bases normales d'entiers relatives

Astérisque, tome 198-199-200 (1991), p. 231-236

<http://www.numdam.org/item?id=AST_1991__198-199-200__231_0>

SUR LES BASES NORMALES D'ENTIERS RELATIVES

par

R. MASSY

Soit N/E une extension galoisienne finie de corps quelconques, de groupe de Galois $\Delta = Gal(N/E)$. On sait par le théorème de la base normale ([**1**], AV70) que N est un module libre de rang 1 sur l'algèbre du groupe Δ sur E. Lorsque N et E sont des corps de nombres, d'anneaux d'entiers respectifs O_N et O_E, on peut se poser la question de savoir si O_N est un module libre, nécessairement de rang 1, sur l'algèbre $O_E[\Delta]$ du groupe Δ sur O_E ; autrement dit, existe-t-il un entier $\vartheta \in O_N$ tel que O_N soit un O_E-module libre de base $\{\delta(\vartheta)\}_{\delta\in\Delta}$? Lorsqu'elle existe, une telle base est dite "base normale d'entiers" (BNE en abrégé) de N sur E.

Dans le cas absolu $E = \mathbf{Q}$, la question est résolue depuis peu par la théorie de Fröhlich et son école [**6**], dont le point culminant est la preuve par Taylor [**15**] de la conjecture de Fröhlich liant la structure de $\mathbf{Z}[\Delta]$-module de O_N au signe de la constante de l'équation fonctionnelle de la fonction L d'Artin associée aux caractères symplectiques de Δ.

En revanche, il n'y a pas actuellement de théorie satisfaisante dans le cas relatif $E \neq \mathbf{Q}$. La première étude systématique de ce cas est due à Brinkhuis qui démontre dans sa thèse [**2**], ainsi que dans des articles postérieurs ([**3**],[**4**]), des résultats de non-existence de BNE. A contrario, nous énonçons ici plusieurs conditions nécessaires et suffisantes d'existence de BNE relatives, avec en outre, lorsqu'elles sont vérifiées, des formules explicites permettant de calculer un générateur ϑ. Ces formules assurent la suffisance de nos conditions d'existence ; elles sont obtenues via celles de [**11**]. Quant à la nécessité de nos conditions, elle procède de la méthode de [**2**] : on ajoute une condition de module au problème de plongement classique. Plus précisément, on se donne une extension galoisienne finie de corps de nombres E/K, de groupe de Galois $Gal(E/K) = \Gamma$, et un groupe abélien Δ considéré comme Γ-module. A une classe de cohomologie $\epsilon \in H^2(\Gamma, \Delta)$ donnée, on peut alors associer les problèmes $(E/K, \epsilon)$ et $[E/K, \epsilon]$ définis comme suit.

Problème $(E/K,\epsilon)$: Existe-t-il au dessus de E un corps N, galoisien sur K, de groupe de Galois sur E s'identifiant à Δ, qui induise une extension de groupes $1 \to \Delta \hookrightarrow Gal(N/K) \to \Gamma \to 1$ de classe ϵ ? Lorsqu'elle existe, l'extension N/K est appelée "solution du problème résoluble $(E/K,\epsilon)$".

Problème $[E/K,\epsilon]$: Le problème $(E/K,\epsilon)$ est-il résoluble, et dans l'affirmative admet-il, en outre, une solution N/K telle que l'on ait une BNE de N sur E ?

Le but de cet article est de résoudre explicitement les problèmes $[E/K,\epsilon]$ sans spécifier le corps de base K comme cela se fait d'habitude (cf.[**2**] chap.8, [**7**], [**14**], [**9**], [**10**]...), ceci, pour une classe ϵ décrivant une extension cyclique d'ordre 4 ou diédrale (resp. quaternionienne) d'ordre 8. Dans toute la suite, le noyau Δ est d'ordre 2 : $\Delta = \{1,\delta\}$, et le groupe $\Gamma = Gal(E/K)$ est d'ordre 2 ou le groupe de Klein. Nos conditions d'existence de BNE sont obtenues sans rien supposer sur le corps de nombres K. Pour les conditions suffisantes, on fait l'hypothèse simplificatrice que K est de nombre de classe $h(K) = 1$, de façon à obtenir une formule de construction d'un générateur ϑ de la base existante.

Le détail des démonstrations, qui sont assez techniques, est donné en [**12**].

1. Conditions nécessaires de résolubilité des problèmes $[E/K,\epsilon]$

Dans cette section, K est un corps de nombres quelconque.

- Si $E = K(\sqrt{a})/K, a \in K$, est une extension quadratique, on note ϵ_{-1} la classe non nulle de $H^2(\Gamma,\Delta)$. Dire que le problème $[E/K,\epsilon_{-1}]$ est résoluble signifie qu'au dessus de E, il existe un corps N, extension cyclique de degré 4 de K, et admettant une BNE sur E.
- Si $E = K(\sqrt{a},\sqrt{b})/K$, $a \in K$, $b \in K$, est une extension biquadratique, soient σ,τ les générateurs de Γ définis par les égalités

$$\sigma(\sqrt{a})/\sqrt{a} = \tau(\sqrt{b})/\sqrt{b} = -1,\ \sigma(\sqrt{b})/\sqrt{b} = \tau(\sqrt{a})/\sqrt{a} = 1.$$

On note ϵ_0 (resp. ϵ_1) la classe de cohomologie d'une extension $1 \to \Delta \hookrightarrow G \to \Gamma \to 1$ de groupe G diédral d'ordre 8, d'unique sous-groupe cyclique d'ordre 4 engendré par un relèvement dans G du produit $\sigma\tau$ (resp. de groupe G quaternionien d'ordre 8). Dire que le problème $[E/K,\epsilon_0]$ (resp. $[E/K,\epsilon_1]$) est résoluble signifie qu'au dessus de E, il existe un corps N, cyclique sur $K(\sqrt{ab})$, extension galoisienne de K de groupe $Gal(N/K)$ diédral (resp. quaternionien) d'ordre 8, et admettant une BNE sur E.

Remarque. Les classes $\epsilon_{-1}, \epsilon_0, \epsilon_1$ s'expriment au moyen de cup-produits définis par a et b. Dans les notations de [**11**], on a

$$\epsilon_{-1} = ((a))_E\ ,\ \epsilon_0 = (a,b)_E\ ,\ \epsilon_1 = ((ab))_E + (a,b)_E.$$

On note $A^\times$ le groupe des inversibles d'un anneau A.

THÉORÈME 1. *(1) Pour que le problème* $[E = K(\sqrt{a})/K, \epsilon_{-1}]$ *soit résoluble, il faut que la condition* (BNE_{-1}) *suivante soit vérifiée :*
(BNE_{-1}) *Il existe une unité de* E *:* $u \in O_E^\times$*, congrue à 1 modulo 2 :* $u \equiv 1\, mod 2O_E$*, de norme* $N_{E/K}u = -1$.

La condition (BNE_{-1}) *est équivalente à la condition*
$(BNE_{-1})'$ *Il existe un entier* $t \in O_K$ *tel que* $E = K(\sqrt{1+4t^2})$.
(2) Pour que le problème $[E = K(\sqrt{a}, \sqrt{b})/K, \epsilon_n]$ *(*$n \in \{0,1\}$ *fixé) soit résoluble, il faut que la condition* (BNE_n) *suivante soit vérifiée :*
(BNE_n) *Il existe des unités* $u \in O_E^\times, v \in O_E^\times$*, de* E*, telles que l'on ait*

$$u \equiv 1\, mod 2O_E,\ u\sigma(u) = (-1)^n\ ;\ v \equiv 1\, mod 2O_E,\ v\tau(v) = (-1)^n$$
$$\tau(u)/u = -\sigma(v)/v.$$

On voit donc que ces conditions ne s'expriment qu'en termes des unités du corps E.

Idée de la démonstration. Etant donnée une extension de groupes $1 \to \Delta \hookrightarrow G \xrightarrow{\pi} \Gamma \to 1$ de classe $\epsilon \in H^2(\Gamma, \Delta)$, on se place dans "l'algèbre de groupe tordue" $\widehat{E[G]}$ de G sur E définie comme étant le E-espace vectoriel de base les éléments de G muni de la multiplication $eg \cdot e'g' = e\pi(g)(e')gg'$ $(e, e' \in E; g, g' \in G)$. Soit $O_E[\Delta]^\times G$ le sous-groupe multiplicatif de $\widehat{E[G]}^\times$ constitué des produits ηg où $\eta \in O_E[\Delta]^\times$ et $g \in G$. La démonstration consiste à traduire les propriétés des cup-produits définissant les classes $\epsilon_n (n \in \{-1, 0, 1\})$ (cf.[**11**]) au moyen de l'implication suivante : si le problème $[E/K, \epsilon]$ est résoluble, la suite exacte

$$1 \to O_E[\Delta]^\times \hookrightarrow O_E[\Delta]^\times G \xrightarrow[\eta g \mapsto \pi(g)]{\pi'} \Gamma \to 1$$

est scindée, i.e., il existe un homomorphisme $\psi : \Gamma \to O_E[\Delta]^\times G$ tel que $\pi' \circ \psi = id_\Gamma$.

Si les problèmes $(E/K, \epsilon_{-1})$ et $(E/K, \epsilon_1)$ sont résolubles et admettent une solution N/K telle que N/E soit modérément ramifiée, l'extension E/K est nécessairement modérément ramifiée (cf. [8] §39). Il n'en est pas de même en général lorsque $[E/K, \epsilon_0]$ est résoluble. Cependant, pour uniformiser et simplifier, nous supposons désormais l'extension de base E/K modérément ramifiée lorsque la condition (BNE_0) du théorème 1 est vérifiée.

On est maintenant en mesure de répondre à la question naturelle de savoir si les conditions nécessaires du théorème 1 sont aussi suffisantes. La réponse est oui sur un corps K de nombre de classe 1.

2. Formules de construction de bases normales d'entiers

Dans cette section, K est un corps de nombres de nombre de classe $h(K) = 1$. Cette hypothèse est avant tout calculatoire, et permet par exemple de choisir les éléments $a, b \in K$ de façon que l'on ait les discriminants $D(K(\sqrt{c})/K) = cO_K, c \in \{a, b\}$. On a alors le

THÉORÈME 2. *(A) Pour qu'un problème $[E/K, \epsilon_n]$ soit résoluble, il faut et il suffit que la condition (BNE_n) du théorème 1 soit vérifiée ($n \in \{-1, 0, 1\}$).*
(B) On suppose qu'il en est ainsi. Soit U le groupe multiplicatif des éléments $k \in K^\times$ tels que l'on ait $ord_\wp((k-1)/4) \geq 0$ en tout idéal premier $\wp$ de K divisant $2O_K$, où $ord_\wp$ désigne la valuation en $\wp$.
(1) Une solution du problème $[E = K(\sqrt{a})/K, \epsilon_{-1}]$ est l'extension cyclique $N = E(\sqrt{x})/K$ définie par l'entier de E

$$x = p(2t + \sqrt{1 + 4t^2})\sqrt{a}$$

obtenu comme suit. On prend pour t, un entier de K tel que $E = K(\sqrt{1+4t^2})$ (cf. condition $(BNE_{-1})'$) ; et pour p, un irréductible de O_K ne se ramifiant pas dans E (resp. une unité de K quand elle existe) vérifiant

$$\alpha(1 - 2t)/p \in U$$

où α est un entier de K tel que $\alpha^2 a = 1 + 4t^2$.
(2) Une solution du problème $[E = K(\sqrt{a}, \sqrt{b})/K, \epsilon_n]$ ($n \in \{0, 1\}$ fixé) est l'extension $N = E(\sqrt{x})/K$, diédrale si $n = 0$, quaternionienne si $n = 1$, définie par l'entier de E

$$x = p\frac{\sqrt{a}}{\lambda}\left(\frac{\sqrt{b}}{d}\right)^n \eta v$$

obtenu comme suit. On prend : pour λ, un entier de $K(\sqrt{a})$ divisant $\sqrt{a}$ tel que $\lambda/\sigma(\lambda) = u\tau(u)$; pour η, une unité de $K(\sqrt{a})$ telle que $\lambda^2 = \eta\kappa$ où κ est un entier de K divisant a ; pour d, un p.g.c.d. de a/κ et de b ; et pour p, un irréductible de O_K ne se ramifiant pas dans E (resp. une unité de K quand elle existe) vérifiant

$$d^n\kappa c/p \in U \quad avec \quad c := Tr_{E/K}\left(\theta/\left(\sqrt{a}(\sqrt{b})^n\lambda v\right)\right)$$

où $Tr_{E/K}$ est la trace de E sur K, et θ un entier de E de trace 1 sur K. (3) Dans les notations précédentes, avec $\Delta = Gal(N/E)$, on a $O_N = O_E[\Delta]\vartheta$ et $O_N = O_E[\vartheta]$ pour l'entier $\vartheta = \frac{1}{2}(1+\sqrt{x})$.

Idée de la démonstration. On montre d'abord, par les théorèmes de [**11**], que si la condition (BNE_n) est vérifiée, le problème $(E/K, \epsilon_n)$ est résoluble ($n \in \{-1, 0, 1\}$). On sait qu'un tel problème admet nécessairement une solution modérément ramifiée N'/K (cf.[**13**], Theorem(6-6)). On affine ensuite les formules de [**11**] de façon à ce qu'elles fournissent un élément $x' \in E$ tel que $N' = E(\sqrt{x'})$. Puis l'on fait varier la solution N'/K jusqu'à trouver un entier $x = ke^2x'$ de E, $k \in K^\times, e \in E^\times$, congru à $1 \bmod 4O_E$, tel que l'idéal xO_E soit un produit d'idéaux premiers distincts ou O_E lui-même. L'extension $N = E(\sqrt{x})/K$ est alors une solution du problème $[E/K, \epsilon_n]$.

Soulignons que les extensions du théorème 2 sont de "bonnes" solutions au sens de Fröhlich (cf.[**5**] Theorem 3, [**6**] p. 230) : leur ramification n'augmente que très peu celle de l'extension de base. En effet,

COROLLAIRE. *Quand $h(K) = 1$, les problèmes $[E/K, \epsilon_n](n \in \{-1, 0, 1\})$ résolubles admettent toujours une solution N/K telle que les irréductibles de O_K qui se ramifient dans N soient ceux qui se ramifient dans E, à l'exception d'au plus l'un d'entre eux.*

C'est clair par nos formules car la ramification n'augmente que si le facteur p n'est pas une unité de K. L'existence des irréductibles p se prouve par le corps de classes.

Signalons pour terminer que dans le cas particulier $K = \mathbb{Q}$, on retrouve les résultats de plusieurs auteurs : Brinkhuis, Fröhlich, M-N. Gras,... .

REFERENCES

[1] N. BOURBAKI, "Algèbre, Chapitres 4 à 7," Masson, Paris, 1981.

[2] J. BRINKHUIS, "Embedding problems and Galois modules," Doctoral Dissertation, Leiden, 1981.

[3] J. BRINKHUIS, *Normal integral bases and embedding problems*, Math. Ann. **264** (1983), 537-543.

[4] J. BRINKHUIS, *Normal integral bases and complex conjugation*, J. reine angew. Math. **375/376** (1987), 157-166.

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

[6] A. FRÖHLICH, "Galois Module Structure of Algebraic Integers," Ergebnisse der Math. 3,1,Springer-Verlag, Berlin, 1983.

[7] M.-N. GRAS, *Bases d'entiers dans les extensions cycliques de degré 4 de* $\mathbf{Q}$, Sém. Théorie des Nombres, Bordeaux (1982/83), exp. 11.

[8] E. HECKE, "Lectures on the Theory of Algebraic Numbers," Graduate Texts Math.77, Springer-Verlag, New York, 1981.

[9] F. KAWAMOTO, *On normal integral bases*, Tokyo J. Math. **7** (1984), 221-231.

[10] F. KAWAMOTO, *Remark on "On normal integral bases"*, Tokyo J. Math. **8** (1985), 275.

[11] R. MASSY, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), 508-535.

[12] R. MASSY, *Bases normales d'entiers relatives quadratiques*, J. Number Theory, à paraître.

[13] J. NEUKIRCH, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59-116.

[14] K. OKUTSU, *Construction of relative integral basis of* $\mathbf{Q}(\sqrt[\ell]{a}, \zeta_\ell)$ *over* $\mathbf{Q}(\zeta_\ell)$ *(in Japanese)*, Seisūron Kenkyūshūkai hōkokushū, in Kyushu University (1982).

[15] M.J. TAYLOR, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41-79.

Richard Massy
Département de Mathématiques
Université de Valenciennes
Le Mont Houy
F-59326 VALENCIENNES Cedex
FRANCE

(reçu le 30 octobre 1989)