JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FLORENCE SORIANO

Extensions cycliques de degré ℓ de corps de nombres ℓ-réguliers

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994), p. 407-420

<http://www.numdam.org/item?id=JTNB_1994__6_2_407_0>

Journal de Théorie des Nombres
de Bordeaux **6** *(1994), 407–420*

Extensions cycliques de degré ℓ de corps de nombres ℓ-réguliers.

par FLORENCE SORIANO

ABSTRACT. – We determine all cyclic extensions L of prime degree ℓ over a ℓ-regular number field K containing the ℓ-roots of unity which are also l-regular. We classify these extensions according to the ramification index of the wild place $\mathcal{L}$ in L/K and to the ℓ-valuation of the relative class number $h_{L/K}$ (which is the quotient h_L/h_K of the ordinary class numbers of L and K).

We study the case where the ℓ is odd prime, since the even case was studien by R. BERGER. Our genus theory methods rely essentially on G. GRAS and J.-F JAULENT's results.

1. Introduction

Soit ℓ un nombre premier impair et soit K un corps de nombres contenant une racine primitive $\ell^{ième}$ de l'unité ζ. D'après G. GRAS et J.-F JAULENT (cf. [GJ]) nous avons :

1.1 DÉFINITION. *Le corps de nombres K est dit ℓ-régulier lorsque la ℓ-partie $R_2(K)$ du noyau des symboles réguliers dans $K_2(K)$ est nulle.*

En fait, comme nous avons supposé ici que K contient les racines $\ell^{ièmes}$ de l'unité, la notion de ℓ-régularité se trouve coïncider avec celle de la ℓ-rationnalité introduite par T. NGUYEN QUANG DO et H. MOVAHHEDI (cf. [JN]). Plus précisément, d'après [GJ], nous avons :

1.2 THÉORÈME. *Soit K un corps de nombres contenant ζ, les assertions suivantes sont équivalentes :*

(i) Le groupe de $\mathcal{G}\mathrm{al}(M/K)$ de la ℓ-extension abélienne ℓ- ramifiée ∞-décomposée maximale de K est un $\mathbb{Z}_\ell$-module libre de rang $c_K + 1$, où c_K désigne le nombre de places complexes de K.

(ii) Le corps K vérifie la conjecture de Leopoldt (pour le nombre premier ℓ), et le sous-module de torsion $\mathcal{T}_K$ de $\mathcal{G}\mathrm{al}(M/K)$ est nul.

Manuscrit reçu le 15 Février 1994, version définitive le 20 Décembre 1994.

(iii) Le corps K possède une unique place $\mathcal{L}$ au dessus de ℓ, et son ℓ-groupe des ℓ-classes Cl'_K d'idéaux est nul.

(iv) Le corps de nombres K est ℓ-régulier.

Les corps ℓ-réguliers contenant les racines $\ell^{ièmes}$ de l'unité forment une classe de corps particulièrement intéressants du point de vue de l'arithmétique puisqu'ils vérifient simultanément les conjectures de Leopoldt et de Gross pour des raisons purement algébriques alors même qu'ils ne sont nullement abéliens (en général) ni même galoisiens sur $\mathbb{Q}$.

Nous nous proposons ici de déterminer toutes les extensions L d'un corps ℓ-régulier K, cycliques et ℓ-régulières, puis de les classifier en fonction de l'indice de ramification de la place sauvage $\mathcal{L}$ de K dans L et de la ℓ-valuation du nombre $h_{L/K}$ de classes relatives. Nous nous plaçons ici dans le cas où ℓ est impair, le cas (ℓ=2) ayant été traité par R. BERGER dans [B]. Notre point de départ est le résultat suivant établi dans [GJ]:

1.3 THÉORÈME. *Soit K un corps de nombres contenant ζ, et soit L une ℓ-extension galoisienne de K, les propriétés suivantes sont équivalentes :*

(i) Le corps L est ℓ-régulier.

(ii) Le corps K est ℓ-régulier, et l'ensemble S des places de K qui se ramifient modérément dans l'extension L/K est primitif (autrement dit les logarithmes de Gras $\ell g(\mathfrak{p})$ des places de S forment une $\mathbb{Z}_\ell$-base d'un sous-module pur du groupe de Galois de la composée Z des $\mathbb{Z}_\ell$-extensions de K).

Remarque. les places $\mathfrak{p}$ de la caractérisation *(ii)* ci-dessus sont donc nécessairement des places ultramétriques étrangères à ℓ. Nous les appelons modérées dans ce qui suit, par opposition avec la place sauvage $\mathcal{L}$.

1.4 DÉFINITION. *Lorsque l'ensemble des places de K qui se ramifient modérément dans l'extension L/K est primitif, on dit que L/K est primitivement ramifiée.*

Le théorème de Čebotarev montre que tout ensemble primitif de places de K de cardinal $s_K < 1 + c_K + \delta_K$, où δ_K est le défaut de la conjecture de Leopoldt, peut être complété d'une infinité de façons en un ensemble S primitif maximal. Comme $\mathcal{G}al(Z/K)$ est un $\mathbb{Z}_\ell$-module libre de rang $c_K + 1 + \delta_K$, et que tout corps de nombres régulier vérifie la conjecture de Leopoldt, le cardinal d'un tel S dans ce cas est toujours $1 + c_K$.

En résumé, on considère donc K un corps de nombres contenant ζ et

ℓ-régulier, et on retiendra qu'une extension L/K cyclique de degré ℓ est ℓ-régulière si et seulement s'il existe un ensemble primitif maximal S tel que L soit incluse dans la ℓ-extension $\overline{M}^S$ ℓ-élémentaire S-modérément ramifiée ∞-décomposée maximale de K.

2. Etude de la structure de $\mathcal{G}\mathrm{al}(\overline{M}^S/K)$ puis de $\mathcal{R}\mathrm{ad}(\overline{M}^S/K)$

2.1 Structure du groupe de Galois.

Désignons par M^S la ℓ-extension S-modérément ramifiée (∞-décomposée) maximale du corps de nombres K; nous avons évidemment:

$$\mathcal{G}\mathrm{al}(\overline{M}^S/K) \simeq \mathcal{G}\mathrm{al}(M^S/K)/\mathcal{G}\mathrm{al}(M^S/K)^\ell$$

D'après (cf. [JN] Th 2.3), nous avons donc:

$$\mathcal{G}\mathrm{al}(\overline{M}^S/K) \simeq \prod_{\mathfrak{p}\in S}(\mathcal{K}_\mathfrak{p}^\times/\mathcal{K}_\mathfrak{p}^{\times\ell}) \simeq \prod_{\mathfrak{p}\in S}(K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times\ell})$$

où $\mathcal{K}_\mathfrak{p}^\times$ désigne le ℓ-adifié du groupe multiplicatif $K_\mathfrak{p}^\times$ du complété en $\mathfrak{p}$ du corps de nombres K.

Et la décomposition canonique $K_\mathfrak{p}^\times \simeq \mu_\mathfrak{p}^\circ \times (1+\mathfrak{p}) \times \pi_\mathfrak{p}^{\mathbb{Z}}$ où $\mu_\mathfrak{p}^\circ$ est le groupe des racines de l'unité d'ordre $(N\mathfrak{p}-1)$ dans $K_\mathfrak{p}^\times$, et $\pi_\mathfrak{p}$ une uniformisante de $K_\mathfrak{p}$, nous donne alors l'isomorphisme :

$$\begin{aligned}\mathcal{G}\mathrm{al}(\overline{M}^S/K) &\simeq \prod_{\mathfrak{p}\in S}\left(\frac{\mu_\mathfrak{p}^\circ}{\mu_\mathfrak{p}^{\circ\ell}} \times \frac{(1+\mathfrak{p})}{(1+\mathfrak{p})^\ell} \times \pi_\mathfrak{p}^{\mathbb{Z}/\ell\mathbb{Z}}\right)\\ &\simeq \prod_{\mathfrak{p}\in S}\left(\frac{\mu_\mathfrak{p}^\circ}{\mu_\mathfrak{p}^{\circ\ell}} \times \pi_\mathfrak{p}^{\mathbb{Z}/\ell\mathbb{Z}}\right) \simeq \prod_{\mathfrak{p}\in S}\mathbb{F}_\ell^{2(1+c_K)})\end{aligned}$$

puisque le terme médian $\frac{(1+\mathfrak{p})}{(1+\mathfrak{p})^\ell}$ est trivial pour $\mathfrak{p} \nmid \ell$, et que $\mu_\mathfrak{p}^\circ$ contient évidemment les racines $\ell^{ièmes}$ de l'unité dès qu'il en est de même de K.

2.2 Proposition. *Si K est un corps de nombres ℓ-régulier qui contient les racines $\ell^{ièmes}$ de l'unité, pour tout ensemble ℓ-primitif maximal S de places modérées, le groupe de Galois $\mathcal{G}\mathrm{al}(\overline{M}^S/K)$ de la ℓ-extension S-modérément ramifiée maximale de K est un $\mathbb{F}_\ell$-espace vectoriel de dimension $2(1+c_K)$.*

2.3 STRUCTURE DE $\mathcal{R}\mathrm{ad}(\overline{M}^S/K)$.

Si ${E'}_S/{E'}_S{}^{\ell}$ est le quotient du groupe E'_S des $S \cup \{\mathcal{L}\}$- unités au sens ordinaire, par sa puissance $\ell^{ième}$, l'isomorphisme de dualité (cf. [GJ] Cor 4.2.) s'écrit aussi grâce au §2.1:

$$ {E'}_S/{E'}_S{}^{\ell} \simeq \prod_{\mathfrak{p}\in S} (\mathcal{K}_{\mathfrak{p}}^{\times}/\mathcal{K}_{\mathfrak{p}}^{\times\ell}) \simeq \mathcal{G}\mathrm{al}(\overline{M}^S/K). $$

Lorsque x est un représentant du groupe quotient ${E'}_S/{E'}_S{}^{\ell}$, l'extension $K(\sqrt[\ell]{x})$ est ∞-décomposée (puisque K est totalement imaginaire) et non ramifiée en dehors des places de S et de celles divisant ℓ. Le quotient ${E'}_S/{E'}_S{}^{\ell}$ est donc un sous-groupe du radical de l'extension $\overline{M}^S/K$. La théorie de KUMMER établissant une dualité entre les groupes $\mathcal{G}\mathrm{al}(\overline{M}^S/K)$ et $\mathcal{R}\mathrm{ad}(\overline{M}^S/K)$, de l'égalité des ordres nous obtenons enfin:

$$ \mathcal{R}\mathrm{ad}(\overline{M}^S/K) \simeq {E'}_S/{E'}_S{}^{\ell}. $$

2.4 THÉORÈME. *Soient K un corps de nombres ℓ-régulier contenant une racine primitive $\ell^{ième}$ de l'unité, $\mathcal{L}$ sa place sauvage, S un ensemble primitif maximal de places de K, il existe exactement $(\frac{\ell^{2(c_K+1)}-1}{\ell-1})$ extensions non triviales ℓ-régulières de degré ℓ.*

Ce sont exactement les extensions de la forme $K(\sqrt[\ell]{\sigma})$ où σ est un représentant de l'une quelconque des $(\ell^{2(c_K+1)} - 1)$ classes non triviales de $E'_S/E'_S{}^{\ell}$.

Plus précisément, si $\mathcal{L}$ est la place sauvage de K, si les $\{\pi_j; j = 1, \cdots, c_K + 2\}$ sont les $(c_K + 2)$ uniformisantes associées aux places de $S \cup \{\mathcal{L}\}$ de K, puis si $\{u_j; j = 1, \cdots, c_K - 1\}$ est un système de $(c_K - 1)$ unités fondamentales de K, les extensions L cherchées sont les extensions de la forme :

$$ L = K\left(\sqrt[\ell]{\zeta^i \times \Big(\prod_{j=1}^{c_K+2} \pi_j^{k_j}\Big) \times \Big(\prod_{j=1}^{c_K-1} u_j^{l_j}\Big)} \right) $$

où les entiers i, k_j et l_j sont non simultanément multiples de ℓ, et tels qu'aucun $(2c_K + 2)$-uplet $(i; k_j; l_j)$ ne soit proportionnel à un autre.

3. Les extensions L/K non modérément ramifiées

Désormais, L/K est une extension cyclique de degré ℓ, non ramifiée en les places modérées, de corps de nombres ℓ-réguliers contenant une racine primitive $\ell^{ième}$ ζ de l'unité. Le lemme d'approximation simultanée par les S-unités (cf [JN], Cor. 4.3), nous donne l'isomorphisme :

$$K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times\ell} \simeq E'_S/{E'_S}^{\ell};$$

ce qui nous permet de considérer le quotient du groupe des ℓ-unités par le sous groupe de ses puissances $\ell^{ièmes}$ (soit $E'_K/{E'_K}^{\ell}$) comme un sous-groupe de $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times\ell}$. Il existe ainsi une classe $\beta = cl(\tau)$ de $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times\ell}$ vérifiant : $L = K(\sqrt[\ell]{\tau})$. Par suite, notons G le groupe de Galois de l'extension L/K et h_L^G l'ordre du ℓ-groupe des classes ambiges de L. L'extension L/K étant ℓ-régulière, les classes d'idéaux de L sont engendrées par la classe de la seule place sauvage, et sont ainsi des classes ambiges. La formule des classes ambiges:

$$h_L^G = h_K \times \frac{\prod_{\mathfrak{p}\nmid\infty} e_{\mathfrak{p}}(L/K) \times \prod_{\mathfrak{p}\mid\infty} d_{\mathfrak{p}}(L/K)}{[L:K] \times (E_K : E_K \cap N_{L/K})}$$

où $e_{\mathfrak{p}}(L/K)$ est l'indice de ramification de la place finie $\mathfrak{p}$ dans L/K,

$d_{\mathfrak{p}}(l/K)$ est le degré de l'extension locale $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ associée à la place infinie $\mathfrak{p}$ de K,

E_K est le groupe des unités de K, et $N_{L/K}$ est le groupe des normes dans L/K,

devient donc:

$$h_L = h_K \times \frac{e_{\mathcal{L}}(L/K)}{\ell \times (E_K : E_K \cap N_{L/K})}$$

3.1 LEMME. *Les unités de K sont toutes normes globales dans l'extension L/K.*

Preuve. Si $\mathfrak{p}$ est une place ultramétrique modérée, alors $\mathfrak{p}$ est non ramifiée, si bien que d'après la théorie du corps de classes locale, les unités de K sont normes locales en $\mathfrak{p}$. On déduit de la formule du produit que toute unité est norme locale partout et donc norme globale de l'extension L/K.

La formule des classes ambiges devenue $h_L = h_K \times \frac{e_{\mathcal{L}}(L/K)}{\ell}$, nous amène à considérer deux cas :

1^{er} cas : $\ell \nmid h_K$, de sorte que $\mathcal{L}$ est ramifiée dans l'extension L/K et on a $(h_L = h_K)$.

$2^{ième}$ cas : $\ell | h_K$, le groupe de Galois Cl_K de la ℓ-extension abélienne maximale non ramifiée ∞-décomposée C de K n'est pas trivial. Ainsi, puisque l'extension C n'est pas confondue avec le corps de nombres K, et qu'elle est de plus contenue dans la ℓ-extension ℓ-ramifiée maximale M de K qui coïncide avec la composée Z des $\mathbb{Z}_\ell$-extensions de K, elle contient une unique sous-extension cyclique de degré ℓ, non ramifiée et donc inerte en $\mathcal{L}$, et nous avons $(h_L = h_K/\ell)$.

3.2 THÉORÈME. *Soit L/K une extension cyclique de degré ℓ, non ramifiée en dehors de ℓ, de corps de nombres ℓ-réguliers, contenant une racine primitive $\ell^{ième}$ de l'unité. Alors il existe une classe $cl(\tau)$ non triviale de $E'_K/{E'_K}^{\ell}$, telle qu'on ait $L = K(\sqrt[\ell]{\tau})$. Deux cas se présentent alors :*

(i) Pour $(\ell \nmid h_K)$, la place sauvage $\mathcal{L}$ est toujours ramifiée dans L/K et on a $(h_L = h_K)$ donc $(\ell \nmid h_L)$.

(ii) Pour $(\ell | h_K)$, il existe une unique extension L/K inerte en $\mathcal{L}$. Les autres telles extensions sont donc ramifiées en la place sauvage en $\mathcal{L}$.

4. Les extensions L/K ramifiées en une place modérée

A présent, on suppose que L/K est une extension cyclique de degré ℓ, ramifiée en au moins une place modérée, de corps de nombres ℓ-réguliers et contenant une racine primitive $\ell^{ième}$ ζ de l'unité. Il existe donc une classe $cl(\sigma) = \beta$ dans $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell} \backslash E'_K/{E'_K}^{\ell}$ telle que l'on ait $L = K(\sqrt[\ell]{\sigma})$. Notons que l'extension L/K étant ramifiée et de degré premier, l'ordre h_K divise h_L, et le nombre relatif de classes $h_{L/K}$ est un entier.

4.1 LEMME. *Sous ces hypothèses, si t désigne le nombre de places modérées ramifiées dans l'extension L/K, l'indice normique $(E_K : E_K \cap N_{L/K})$ est ℓ^{t-1}.*

4.2 PROPOSITION. *Toujours sous ces hypothèses, l'une des assertions suivantes est vérifiée:*

(i) La place sauvage $\mathcal{L}$ se ramifie dans L/K et $(h_{L/K} = \ell)$.

(ii) La place sauvage $\mathcal{L}$ est inerte dans l'extension L/K, et $(h_{L/K} = 1)$. Deux cas sont alors à envisager :

- *ou bien $(\ell | h_K)$, auquel cas $(\ell \mid h_L)$.*

• *ou bien* $(\ell \nmid h_K)$, *auquel cas* $(\ell \mid h_L)$ *si et seulement si* $\mathcal{L}$ *se ramifie dans l'extension* L/K.

Preuve de la Proposition : le lemme 4.1 et la formule des classes ambiges donnent l'égalité : $h_L = h_K \times e_{\mathcal{L}}(L/K)$, d'où la proposition.

Preuve du Lemme 4.1 : dans l'isomorphisme $E'_S/{E'_S}^{\ell} \simeq \prod_{\mathfrak{p}\in S}(K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times\ell})$, où S est un ensemble primitif maximal de places de K, toute classe d'unité globale x de $E'_K/{E'_K}^{\ell}$ peut être considéré comme un élément de $\prod_{\mathfrak{p}\in S}(\frac{\mu_{\mathfrak{p}}^{\circ}}{\mu_{\mathfrak{p}}^{\circ\ell}})$. Les places de S étant nécessairement modérées, dans la factorisation $U_{\mathfrak{p}}/U_{\mathfrak{p}}^{\ell}$ du groupe des unités de $K_{\mathfrak{p}}^{\times}$, l'élément x peut être identifié à un élément de $\prod_{\mathfrak{p}\in S} U_{\mathfrak{p}}/U_{\mathfrak{p}}^{\ell} \simeq \prod_{\mathfrak{p}\in S}\mu_{\mathfrak{p}}^{\circ}/\mu_{\mathfrak{p}}^{\circ\ell}$. Or, par la théorie du corps de classes locale, le groupe d'inertie de la place $\mathfrak{p}$ de S est isomorphe au quotient du groupe des unités $U_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$ par le sous groupe de ses normes dans l'extension locale $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Par conséquent, l'indice $(U_{\mathfrak{p}} : U_{\mathfrak{p}} \cap N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}})$ est égal à ℓ dès que $\mathfrak{p}$ est ramifié dans L/K, auquel cas $(U_{\mathfrak{p}} \cap N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = U_{\mathfrak{p}}^{\ell})$. Par suite, il résulte de l'isomorphisme entre radicaux kummériens :

$$E'_K/{E'}_K^{\ell} \simeq \prod_{\mathfrak{p}\in S}(\mu_{\mathfrak{p}}^{\circ}/\mu_{\mathfrak{p}}^{\circ\ell})$$

et de sa propriété de compatibilité avec la norme, que l'indice dans le groupe des ℓ-unités du sous-groupe des normes, est :

$$({E'}_K : {E'}_K \cap N_{L/K}) = \prod_{\mathfrak{p}\in S^{\circ}}(\mu_{\mathfrak{p}}^{\circ} : \mu_{\mathfrak{p}}^{\circ\ell}) = \ell^t$$

où S° est l'ensemble des places modérées de K, ramifiées dans l'extension L/K.

En d'autres termes, le quotient ${E'}_K/{E'}_K \cap N_{L/K}$ est un sous-espace de codimension t du $\mathbb{F}_\ell$-espace vectoriel ${E'}_K/{E'}_K^{\ell}$. Et son intersection $(E_K \cap N_{L/K})/{E_K}^{\ell}$ avec l'hyperplan $E_K/{E_K}^{\ell}$ est donc de codimension inférieure ou égale à $t+1$, de sorte que le $\mathbb{F}_\ell$-espace vectoriel $E_K/E_K \cap N_{L/K}$ est de dimension au moins égale à $t-1$ i.e. $(E_K : E_K \cap N_{L/K}) \geq \ell^{t-1}$.

C'est le monomorphisme η déduit des symboles de HASSE et établi dans [J] (p. 211, Th III.2.7) qui nous permet de conclure. En effet, si $\widetilde{\oplus} I_{\mathfrak{p}}(L/K)$ désigne la somme restreinte (à la formule du produit) des sous-groupes d'inertie de l'extension L/K, alors le monomorphisme induit par les symboles de Hasse $\eta : E_K/E_K \cap N_{L/K} \hookrightarrow \widetilde{\oplus} I_{\mathfrak{p}}(L/K)$, nous amène à considérer les deux cas suivants:

-ou bien la place sauvage $\mathcal{L}$ est inerte, auquel cas $(E_K : E_K \cap N_{L/K}) = \ell^{t-1}$.

-ou bien la place sauvage $\mathcal{L}$ est ramifiée, auquel cas $(E_K : E_K \cap N_{L/K})$ prend la valeur ℓ^{t-1} ou ℓ^t. En tenant compte de la régularité de K et L, la formule des classes ambiges nous permet d'écrire dans la seconde situation $h_{L/K} = 1$, si bien que les classes de la place sauvage de ces corps de nombres sont de même ordre; ce qui ne peut être en vertu de l'hypothèse de ramification de $\mathcal{L}$. Par suite, seule la première situation est envisageable.

5. Familles d'extensions de degrés ℓ de corps de nombres totalement imaginaires et ℓ-réguliers

De l'isomorphisme $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell} \simeq E'_S/E'^{\ell}_S$, il apparaît que le groupe E'_K/E'^{ℓ}_K peut être considéré comme un sous-groupe de $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell}$.

5.1 DÉFINITION. *Soit K un corps de nombres ℓ-régulier contenant une racine primitive $\ell^{\text{ième}}$ de l'unité ζ et soit β une classe de $(K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell})\backslash(E'_K/E'^{\ell}_K)$.*

Un corps de nombres L est dit "être membre de la famille β " (notée $Fam(\beta)$) si et seulement si $L = K(\sqrt[\ell]{\sigma})$, où σ est un représentant de la classe β dans $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell}$, est une extension de degré ℓ dans laquelle au moins une place modérée $\mathfrak{p}$ de K se ramifie.

5.2 THÉORÈME. *Soit K un corps de nombres ℓ-régulier et contenant une racine primitive $\ell^{\text{ième}}$ de l'unité ζ. Pour chaque classe β de $(K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell})\backslash(E'_K/E'^{\ell}_K)$, il existe une infinité de corps de nombres qui sont membres de la famille $Fam(\beta)$.*

La clé de la preuve du résultat précédent est le théorème suivant :

5.3 THÉORÈME. *Soient K un corps de nombres ℓ-régulier contenant une racine primitive $\ell^{\text{ième}}$ de l'unité ζ. Il existe un épimorphisme ϕ, de $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell}$ dans le groupe de Galois de la ℓ-extension $\overline{M}$ abélienne ℓ-élémentaire ℓ-ramifiée maximale. De plus, le noyau de ϕ est E'_K/E'^{ℓ}_K. Autrement dit, on a la suite exacte courte canonique:*

$$1 \longrightarrow E'_K/E'^{\ell}_K \longrightarrow K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times \ell} \overset{\phi}{\longrightarrow} \mathcal{G}\text{al}(\overline{M}/K) \longrightarrow 1$$

Preuve. la théorie du corps de classes locale nous donne le morphisme canonique de $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times\ell}$ dans le groupe de Galois de la ℓ-extension $\overline{M}$ abélienne ℓ-élémentaire ℓ-ramifiée maximale. Comme le groupe de Galois de la ℓ- extension M abélienne ℓ-ramifiée maximale (cf [J], p. 29.Ex I.1.17) est isomorphe à $\mathcal{I}_K/(\prod_{\mathfrak{q}|\ell}\mu_{\mathfrak{q}}).\mathcal{R}_K$ où

- $\mathcal{I}_K$ est le ℓ-adifié du groupe des idèles
- $\mu_{\mathfrak{q}}$ est le groupe des unités dans le complété en $\mathfrak{q}$ du corps de nombres K
- $\mathcal{R}_K$ est le groupe des idèles principaux de K,

nous obtenons par définition de $\overline{M}$,

$$\mathcal{G}\mathrm{al}(\overline{M}/K) \simeq \mathcal{G}\mathrm{al}(M/K)/\mathcal{G}\mathrm{al}(M/K)^{\ell}$$

$$\mathcal{G}\mathrm{al}(\overline{M}/K) \simeq \mathcal{I}_K/(\prod_{\mathfrak{q}|\ell}\mu_{\mathfrak{q}}).\mathcal{R}_K.{\mathcal{I}_K}^{\ell}$$

Or nous avons ici : $\mathcal{K}_{\mathcal{L}}^{\times} \bigcap (\prod_{\mathfrak{q}|\ell}\mu_{\mathfrak{q}})\mathcal{R}_K{\mathcal{I}_K}^{\ell} = s_{\mathcal{L}}(\mathcal{E}')\mathcal{K}_{\mathcal{L}}^{\times\ell}$, où $\mathcal{E}'$ est le tensorisé du groupe des ℓ-unités et $s_{\mathcal{L}}(\mathcal{E}')$ sa projection sur le tensorisé $\mathcal{K}_{\mathcal{L}}^{\times}$, ce qui nous permet d'établir l'isomorphisme suivant :

$$\mathcal{G}\mathrm{al}(\overline{M}/K) \simeq \mathcal{K}_{\mathcal{L}}^{\times}/s_{\mathcal{L}}(\mathcal{E}').\mathcal{K}_{\mathcal{L}}^{\times\ell}.$$

Le noyau de ϕ est clairement le quotient $s_{\mathcal{L}}(\mathcal{E}').\mathcal{K}_{\mathcal{L}}^{\times\ell}/\mathcal{K}_{\mathcal{L}}^{\times\ell}$ et est donc isomorphe à ${E'}_K/{E'}_K^{\ell}$.

Preuve du Théorème 5.2. Soit β une classe du groupe quotient $K_{\mathcal{L}}^{\times}/K_{\mathcal{L}}^{\times\ell}$; il résulte de l'uniforme répartition des automorphismes de Frobenius $\left(\frac{\overline{M}/K}{\mathfrak{p}}\right)$ dans le groupe de Galois de l'extension $\overline{M}/K$, et de l'épimorphisme donné par le théorème 5.3, qu'à la classe $\phi(\beta)$ correspond une infinité de places modérées $\mathfrak{p}$. Si de plus β n'appartient pas à ${E'}_K/{E'}_K^{\ell}$, son image dans le groupe de Galois $\mathcal{G}\mathrm{al}(\overline{Z}/K) = \mathcal{G}\mathrm{al}(\overline{M}/K) \simeq \mathcal{K}_{\mathcal{L}}^{\times}/s_{\mathcal{L}}(\mathcal{E}').\mathcal{K}_{\mathcal{L}}^{\times\ell}$ n'est pas triviale. Par suite, l'automorphisme de Frobenius $\left(\frac{\overline{M}/K}{\mathfrak{p}}\right)$ ne fixe pas la ℓ-extension $\overline{Z}$, si bien que le premier modéré $\mathfrak{p}$ est ℓ-primitif et peut être complété en un ensemble primitif maximal de K.

6. Classification des extensions cycliques de degré ℓ

On considère à présent les extensions L/K cycliques de degré ℓ, de corps de nombres ℓ-réguliers contenant ζ une racine primitive $\ell^{ième}$ de l'unité, ramifiées en au moins une place modérée de K.

6.1 PROPOSITION. *Soit K un corps de nombres ℓ-régulier contenant une racine primitive $\ell^{ième}$ de l'unité ζ,*

- *si $(\ell \nmid h_K)$, alors la place $\mathcal{L}$ est inerte dans les membres L de l'une de ces familles, et se ramifie dans toute autre famille.*
- *si $(\ell | h_K)$, alors la place $\mathcal{L}$ se ramifie dans les membres de toutes les familles d'extensions.*

Preuve : Plaçons nous d'abord dans le cas où $(\ell \nmid h_K)$; en considérant $E_K^S/{E_K^S}^\ell$ comme un hyperplan de l'espace vectoriel $K_\mathcal{L}^\times/{K_\mathcal{L}^\times}^\ell$, nous sommes assurés de l'existence de ℓ applications linéaires de $K_\mathcal{L}^\times/{K_\mathcal{L}^\times}^\ell$, triviales sur l'hyperplan $E_K^S/{E_K^S}^\ell$ et à valeurs dans le groupe μ_ℓ des racines $\ell^{ièmes}$ de l'unité. Par suite, si $[.,.]_\mathcal{L}$ désigne la puissance $(m_\mathcal{L}/\ell)-ième$ du symbole de Hilbert en la place sauvage $\mathcal{L}$, $m_\mathcal{L}$ étant l'ordre du groupe $\mu_\mathcal{L}$ des racines de l'unité de $K_\mathcal{L}$ d'ordre une puissance de ℓ, $[\beta,.]_\mathcal{L}$ est l'une des ℓ applications linéaires cherchées et est de plus, non partout triviale. Notons que la classe β ne peut appartenir au quotient ${E'}_K/{{E'}_K}^\ell$, puisque les extensions $K(\sqrt[\ell]{\tau})$, où τ est un représentant d'une classe du groupe ${E'}_K/{{E'}_K}^\ell$, sont ramifiées en la place sauvage $\mathcal{L}$. Les autres applications linéaires sont clairement les symboles $[\beta^i,.]$, pour les i variant de 2 à ℓ, d'où l'unicité et l'existence d'une seule famille d'extensions dont les membres $L = K(\sqrt[\ell]{\sigma})$, où β est la classe de σ dans $K_\mathcal{L}^\times/{K_\mathcal{L}^\times}^\ell$, sont inertes en la place sauvage.

Supposons à présent, $(\ell | h_K)$; alors $\mathcal{L}$ est inerte dans une seule extension non triviale de la forme $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe de ${E'}_K/{{E'}_K}^\ell$. En raisonnant comme dans le cas précédent, on voit que la place sauvage $\mathcal{L}$ est ramifiée dans les membres de toutes familles d'extensions.

6.2 THÉORÈME. *Soit K un corps de nombres ℓ-régulier contenant une racine primitive $\ell^{ième}$ de l'unité.*

La liste complète des extensions L cycliques ℓ-régulières et de degré ℓ sur K comprend:

- *d'une part les $\frac{\ell^{c_K+1}-1}{\ell-1}$ extensions $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe du groupe ${E'}_K/{{E'}_K}^\ell$, dans lesquelles aucun premier modéré*

de K se ramifie.

• *d'autre part $\frac{\ell^{2c_K+2}-\ell^{c_K+1}}{\ell-1}$ familles infinies d'extensions, dont les membres L se ramifient en au moins un premier modéré de K.*

• *Pour $(\ell \nmid h_K)$, les extensions $L = K(\sqrt[\ell]{\tau})$ où τ est un représentant d'une classe du groupe E'_K/E'^{ℓ}_K sont telles que la place sauvage $\mathcal{L}$ est ramifiée et que l'ordre h_L du groupe des classes de L n'est pas divisible par ℓ. De plus, il n'existe qu'une seule famille d'extensions dont les membres L sont inertes en $\mathcal{L}$ et de groupe de classes d'ordre h_L non divisible par ℓ. Pour toute autre famille, l'ordre h_L associé aux membres est un multiple de ℓ et la place sauvage est ramifiée.*

• *Pour $(\ell | h_K)$, il existe une unique extension non triviale et non ramifiée $L = K(\sqrt[\ell]{\tau})$ où nécessairement τ est un représentant d'une classe du groupe E'_K/E'^{ℓ}_K. Et l'ordre h_L de son groupe des classes est divisible par ℓ si et seulement si l'ordre h_K l'est par ℓ^2. Les autres extensions cycliques ℓ-ramifiées de degré ℓ, sont ramifiées en la place sauvage $\mathcal{L}$ et ont pour ordre h_L un multiple de ℓ. Enfin, les membres de toutes les familles se ramifient en la place sauvage $\mathcal{L}$ et eux aussi, ont pour ordre un multiple h_L de ℓ.*

Preuve : Si t désigne le nombre de diviseurs premiers modérés ramifiés dans l'extension L/K, par la formule des classes ambiges, nous obtenons:

$$\begin{cases} si \ \ (t \geq 1), \ h_L = h_K \times e_{\mathcal{L}}(L/K) \\ si \ (t = 0), \ h_L = \dfrac{h_K \times e_{\mathcal{L}}(L/K)}{\ell} \end{cases}$$

d'où le théorème.

7. L'exemple numérique ($K = \mathbb{Q}(\sqrt{-3})$) et ($\ell = 3$)

On sait dans ce cas que le corps de nombres K est 3-régulier (cf. [JN], Cor. 1.3) et que son anneau des entiers $\mathbb{Z}[j]$ est euclidien de sorte que son groupe des classes (au sens restreint comme au sens ordinaire) est trivial. Le théorème 6.2 nous permet alors de dresser les résultats suivants:

• il existe exactement $\frac{3^2-1}{3-1} = 4$ extensions L cycliques 3-régulières, de degré 3 sur K et telles qu'aucun premier modéré se ramifie. Il s'agit des quatre extensions:

$$L_1 = K(\sqrt[3]{j}), \ L_2 = K(\sqrt[3]{\sqrt{-3}}) = K(\sqrt[3]{3}),$$
$$L_3 = K(\sqrt[3]{j\sqrt{-3}}) \text{ et } L_4 = K(\sqrt[3]{j^2\sqrt{-3}}),$$

où j désigne une racine cubique non triviale de l'unité. Elles sont de plus ramifiées en la place sauvage et l'ordre de leur groupe des classes n'est pas multiple de 3.

• l'écriture de la liste des représentants des familles d'extensions, dont les membres L se ramifient en au moins un premier modéré de K, nous conduit à déterminer un ensemble S primitif maximal de K (nécessairement d'ordre $1 + c_K = 2$, cf. [GJ] p. 346, Sco. 1.2). Pour cela, nous notons $\mathfrak{p}$ et $\mathfrak{q}$ deux premiers modérés de K au dessus de 7 et 13, puis $\mathcal{D}\ell_K$ le tensorisé multiplicatif $\mathbb{Z}_3 \otimes_{\mathbb{Z}} D_K$ du groupe des diviseurs D_K de K. L'ensemble $S = \{\mathfrak{p}; \mathfrak{q}\}$ est primitif si et seulement si les classes des logarithmes de GRAS des uniformisantes globales associées $\pi_7 = 2+\sqrt{-3}$ et $\pi_{13} = 1+2\sqrt{-3}$ sont $\mathbb{F}_3$-linéairement indépendantes dans le $\mathbb{F}_3$-espace vectoriel $\log\ \mathcal{D}\ell_K/\ell\ \log\ \mathcal{D}\ell_K$. Ici, pour $(x \in \mathcal{L})$, le logarithme 3-adique vérifie la congruence :

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3}\ [mod\ \mathcal{L}^4]$$

et les calculs modulo $\mathcal{L}^4$:

$$\log {\pi_7}^2 = \log(1+4\sqrt{-3}) \equiv 4\sqrt{-3} + 24 - 64\sqrt{-3} \equiv -3 - 3\sqrt{-3}$$
$$\log \pi_{13} \equiv -3 + 3\sqrt{-3}$$

nous montrent alors que ces logarithmes sont effectivement indépendants dans $\mathcal{L}^2/\mathcal{L}^4 \simeq \mathbb{F}_3 \oplus \mathbb{F}_3$.

7.1 THÉORÈME. *Un système de représentants des extensions 3-régulières cycliques de degré 3 du corps de nombres $K = \mathbb{Q}(\sqrt{-3})$ est donné par les :*

$$L = K\Big(\sqrt[3]{j^i \times 3^k \times (1+2\sqrt{-3})^l \times (2+\sqrt{-3})^m}\ \Big),$$

où les entiers i, k, l, m ne sont pas simultanément multiples de 3 et tels qu'aucun 4-uplet (i,k,l,m) ne soit proportionnel à un autre.

Il s'agit donc à présent de déterminer la seule extension L non modérément ramifiée, inerte en la place sauvage $\mathcal{L}$ et dont l'existence est assurée par le théorème 6.2.

Puisque $1-j$ est une uniformisante locale en 3, le groupe $(U^1_{\mathcal{L}} = 1+\mathcal{L})$ des unités principales de $K_{\mathcal{L}}$ apparaît aussi comme le produit direct du groupe des racines cubiques de l'unité par son sous-groupe $(U^2_{\mathcal{L}} = 1+\mathcal{L}^2)$. Comme on a par ailleurs $(U^2_{\mathcal{L}})^3 = U^4_{\mathcal{L}}$, le radical de l'extension abélienne maximale $K^{ab}_{\mathcal{L}}$ de $K_{\mathcal{L}}$ est donc donné par l'isomorphisme :

$$K^{\times}_{\mathcal{L}}/{K^{\times}_{\mathcal{L}}}^3 \simeq < j > \times U^2_{\mathcal{L}}/U^4_{\mathcal{L}} \times 3^{\mathbb{F}_3}.$$

Nous sommes ainsi conduits à considérer les caractères associés aux groupes successifs $< j >$, $3^{\mathbb{F}_3}$ et $U^2_{\mathcal{L}}/U^4_{\mathcal{L}}$ qui sont respectivement :

• ω le caractère cyclotomique (qui à tout générateur τ de G associe la racine -1),

• 1 le caractère unité (qui à τ associe +1),

• $1+\omega$ le caractère régulier.

Le radical non ramifié est donc $\alpha K_{\mathcal{L}}^{\times 3}/K_{\mathcal{L}}^{\times 3}$ où α est une classe de $(U_{\mathcal{L}}^2/U_{\mathcal{L}}^4)$ satisfaisant $(\alpha^\tau = \alpha^{-1})$ et que l'on peut imposer être égal à $\frac{1+3\sqrt{-3}}{1-3\sqrt{-3}}$ modulo $K_{\mathcal{L}}^{\times 3}$.
Ainsi, $\alpha \equiv (1+3\sqrt{-3})(1-3\sqrt{-3})^2 \equiv (1-3\sqrt{-3})(1+3\sqrt{-3})^2 \equiv 28(1+3\sqrt{-3})$.
L'écriture $(28 = 1+3^3 \in U_{\mathcal{L}}^6)$ permet enfin d'obtenir le radical : $\alpha \equiv (1+3\sqrt{-3})[mod\ K_{\mathcal{L}}^{\times 3}]$.

Il s'agit à présent de préciser pour lequel des quadruplets $(i;k;l;m)$ nous obtenons :

$$\alpha \equiv j^i \times 3^k \times (1+2\sqrt{-3})^l \times (1+4\sqrt{-3})^m \ [mod\ K_{\mathcal{L}}^{\times 3}].$$

Pour cela, nous écrivons modulo $\mathcal{L}^4$ les congruences successives :

$$\log \frac{\pi_{13}}{{\pi_7}^2} \equiv 6\sqrt{-3} \equiv \log (1+3\sqrt{-3})^2$$

si bien qu'il existe deux entiers i et k tels que :

$$(1+3\sqrt{-3})^2 \equiv \frac{\pi_{13}}{{\pi_7}^2} \times j^i \times 3^k \ [modK_{\mathcal{L}}^3].$$

L'entier k étant nécessairement nul, le dernier calcul :

$$j^i \equiv (1+3\sqrt{-3})^2 \frac{\pi_7^2}{\pi_{13}} \equiv 1+6\sqrt{-3}+4\sqrt{-3}-2\sqrt{-3} \equiv 1-\sqrt{-3} \equiv j^2,$$

montre que le radical α est aussi congru à $j^2 \frac{\pi_{13}}{{\pi_7}^2}$ soit $j^2\pi_{13}\pi_7$. En résumé, il vient donc :

7.2 THÉORÈME. *Les quatre extensions L non modérément ramifiées sont les extensions $L = K\left(\sqrt[3]{j^i\ 3^k}\right)$. Elles sont ramifiées en la place sauvage et l'ordre de leur groupe des classes n'est pas divisible par 3.*

Parmi les trente six autres extensions ramifiées en au moins une place modérée, seule l'extension $L = K\left(\sqrt[3]{j^2 \times (1+2\sqrt{-3}) \times (2+\sqrt{-3})}\right)$ est inerte en $\mathcal{L}$; de plus, l'ordre h_L de son groupe des classes n'est pas divisible par 3. Les trente cinq extensions restantes sont ramifiées en la place sauvage et l'ordre h_L de leur groupe des classes est un multiple de 3.

BIBLIOGRAPHIE

[B] R. BERGER, *Class number parity and unit signature*, Arch. Math. **59** (1993), 427–435.

[J] J.-F. JAULENT, *L'arithmétique des ℓ-extensions (Thèse)*, Publ. Math. Fac. Sci. Besançon, Théor. Nombres (1984/1985, 1985/1986 (1986)), 13–43, 163-178.

[JN] J.-F. JAULENT & T.NGUYEN QUANG DO, *Corps p-rationnels, corps p-réguliers, et ramification restreinte*, J. Théor. Nombres Bordeaux 5 (1994), 343–363.

[GJ] G. GRAS et J.-F. JAULENT, *Sur les corps de nombres réguliers*, Math.Z.202 (1989), 343–365.

[S] J.-P. SERRE, *Corps Locaux*, Hermann, Paris (1968), 17-34, 211–238.

Florence Soriano
Centre de Recherche en Mathématiques de Bordeaux
Université Bordeaux I
351, cours de la Libération
F-33405 Talence Cedex

e.mail : soriano@ceremab.u-bordeaux.fr