Journal de Théorie des Nombres
de Bordeaux **12** (2000), 423–435

Ramifications minimales

par Georges GRAS

Résumé. Nous appliquons à la notion d'extension (cyclique de degré p) à ramification minimale, les techniques de "réflexion" qui permettent une caractérisation très simple de ces extensions à l'aide d'un corps gouvernant.

Abstract. We apply, for the notion of extension (cyclic of degree p) with minimal ramification, the technics of "reflection" which allow a very simple characterization of these extensions by mean of a governing field.

Ce texte propose une approche nouvelle de l'étude de la ramification dans $\overline{K}^{\text{ab}}{}_{[p]}/K$, la p-sous-extension maximale d'exposant p de la clôture abélienne $\overline{K}^{\text{ab}}$ du corps de nombre K, notamment par l'étude des possibilités de ramification des extensions cycliques de degré p de K en vue de la caractérisation des "plus petits discriminants" (ce problème général concerne surtout les extensions non galoisiennes et repose sur des méthodes géométriques, mais dans le cas abélien la théorie du corps de classes reste prépondérante ; pour le cas général se reporter à [M1] et à la bibliographie qu'il contient).

Le principe consiste à construire une extension de Kummer de la forme $Q_1 = K_1\left(\sqrt[p]{Y}\ \right)$ (le corps gouvernant), où $K_1 = K(\mu_p)$ et où Y est un invariant numérique ne dépendant que de K, et de montrer que l'on a la propriété suivante : pour un ensemble T fini de places finies de K, l'existence d'une extension cyclique de degré p de K, totalement ramifiée en T et non ramifiée en dehors de T, dépend simplement de la décomposition des éléments de T dans Q_1/K_1.

De façon précise, une telle extension existe si et seulement s'il existe des éléments $\sigma_{1,v}$ du groupe de décomposition $\delta_{1,v}$ de v dans Q_1/K_1, avec $\sigma_{1,v} \neq 1$ si $\delta_{1,v} \simeq U_v/U_v^p$ (où U_v désigne le groupe des unités du complété de K en v), tels que $\prod_{v\in T} \sigma_{1,v} = 1$.

Cette formulation qui "échange" ramification et décomposition est typique des méthodes de "réflexion" qui utilisent la dualité kummérienne à

Manuscrit reçu le 28 février 2000.

l'origine des "théorèmes de réflexion" que nous avons détaillé dans [G2]. Elle permet alors de résoudre tout problème de ramification (comme celui des extensions à ramifications minimales) d'une façon très naturelle qui élimine complètement le caractère très technique de tout problème lié à la ramification, même abélienne .

Cette étude emprunte au chapitre V de [G1] qui repose sur les résultats de la théorie du corps de classes qui y sont développés ; signalons l'existence d'un travail de Jacques Martinet [M2] qui étudie les extensions quadratiques relatives à ramification minimale en vue d'obtenir des petits discriminants.

Je remercie Jacques Martinet de m'avoir communiqué ses textes non publiés ainsi que Henri Cohen pour l'invitation à ce Colloque qui a influencé une partie de ce travail.

1. Introduction

Désignons par Pl_0 l'ensemble des places finies du corps de nombres K et par Pl_∞^{r} celui des places à l'infini réelles ; si $v \in Pl_0$, on désigne par $\mathfrak{p}_v$ l'idéal premier qui lui correspond. Nous fixons un nombre premier p et distinguons, dans Pl_0, le sous-ensemble Pl_p formé des places "sauvages" (i.e. divisant p) et celui, Pl_{mod}, formé des places "modérées".

Soit $S = S_0 \cup S_\infty \subset Pl_0 \cup Pl_\infty^{\mathrm{r}}$ un ensemble fini de places non complexes de K. Si l'on se donne un ensemble fini $T = T_p \cup T_{\mathrm{mod}}$ ($T_p = T \cap Pl_p$, $T_{\mathrm{mod}} = T \setminus T_p$), disjoint de S_0, formé de places finies de K, on peut se demander s'il existe une extension cyclique L, de degré p de K, S-décomposée et telle que (en termes d'indices de ramification dans L/K) :

$$e_v = p \text{ pour tout } v \in T, \quad e_v = 1 \text{ pour tout } v \notin T,$$

une telle extension étant dite T-totalement ramifiée, S-décomposée [1].

Pratiquement la réponse est contenue (via la théorie du corps de classes) dans l'étude numérique des groupes de S-classes généralisées $Cl_{\mathfrak{m}}^S$ (quotient du groupe des idéaux fractionnaires étrangers à T par le sous-groupe engendré par S_0 et par les idéaux principaux de la forme (x) pour $x \equiv 1 \bmod \mathfrak{m}$ et positif sur $Pl_\infty^{\mathrm{r}} \setminus S_\infty$), puisque pour $\mathfrak{m} = \prod_{v \in T} \mathfrak{p}_v^{m_v}$ assez gros, le p-corps de rayon S-décomposé $K(\mathfrak{m})^S(p)$ contient toutes les "solutions" relatives à T et S ; ceci est possible en utilisant PARI et les techniques effectives de [CDO], [Co1] et [Co2].

Mais dans ce point de vue "groupes de classes généralisées", les calculs sont à reprendre dès que l'on modifie T et l'on ne voit pas comment **caractériser** les parties T pouvant convenir pour le problème posé.

[1] Comme dans [J], la ramification ne concerne que les places finies, le comportement des places à l'infini dans l'extension considérée étant imposé par la décomposition de S_∞.

Nous allons construire un corps gouvernant permettant de caractériser les solutions T au moyen de conditions arithmétiques simples, en y adjoignant la S-décomposition qui, comme d'habitude, modifie très peu les raisonnements.

La notion de corps gouvernant a été introduite par Stevenhagen dans [St] où l'on trouve une étude de ce type de problème basée sur la notion d'extension de groupe, et qui est donc de nature cohomologique ; de même , dans [N], Neukirch traite de façon approfondie le “problème du plongement” dont les obstructions mettent en jeu de tels corps gouvernants.

La méthode que nous proposons est par contre d'une extrême simplicité ; cependant, si elle donne une bonne description de ces extensions (particulièrement adaptée à l'utilisation du théorème de Čebotarev), elle ne les construit pas et pour cela on devra utiliser [Co1], [Fi] entre autres.

2. Construction d'un corps gouvernant

On fixe un ensemble fini $S = S_0 \cup S_\infty \subset Pl_0 \cup Pl_\infty^{\mathrm{r}}$ de places non complexes de K, l'idée étant que l'on fera varier $T = T_p \cup T_{\mathrm{mod}}$ comme ensemble fini, disjoint de S_0, tel que la condition (trivialement nécessaire) $\mathrm{N}\mathfrak{p}_v \equiv 1 \bmod p$ pour tout $v \in T_{\mathrm{mod}}$, soit satisfaite.

2.1 Notations. (i) On désigne par H_T^S l'extension abélienne T-ramifiée S-décomposée maximale de K ; par exemple H^S est le corps de classes de Hilbert S-décomposé qui donne le corps de classes de Hilbert au sens restreint $H = H^{\mathrm{res}}$, pour $S = \emptyset$, et le corps de classes de Hilbert au sens ordinaire $H^{Pl_\infty^{\mathrm{r}}} = H^{\mathrm{ord}}$, pour $S = Pl_\infty^{\mathrm{r}}$.

Si v est une place finie, on désigne par $(U_v^{(i)})_{i \geq 0}$ la filtration habituelle du groupe des unités U_v du complété K_v de K en cette place et par i_v le plongement de K dans K_v.

On fixe $\mathfrak{m} = \prod\limits_{v \in T} \mathfrak{p}_v^{m_v}$ assez gros de telle sorte que l'on ait $U_v^{(m_v)} \subseteq U_v^p$ pour tout $v \in T$ (on vérifie qu'alors $K(\mathfrak{m})^S(p)$ contient la sous-extension maximale d'exposant p de H_T^S/H^S) ; on pose :

$$A = \mathrm{Gal}(H_T^S/K), \quad B = \mathrm{Gal}(H_T^S/H^S).$$

(ii) On désigne par $E_{\mathfrak{m}}^S$ le groupe des S-unités congrues à 1 modulo $\mathfrak{m}$ (on notera que pour $S_\infty = \emptyset$, on obtient le groupe $E_{\mathfrak{m}}^{S_0 \mathrm{pos}}$ des S_0-unités totalement positives congrues à 1 modulo $\mathfrak{m}$, le cas ordinaire s'obtenant avec $S_\infty = Pl_\infty^{\mathrm{r}}$).

A partir de la suite exacte classique (cf. [G1, ch. III, § 1.1.3, i]) :

$$1 \to E^S/E_{\mathfrak{m}}^S \xrightarrow{i_T} \bigoplus_{v \in T} U_v/U_v^{(m_v)} \xrightarrow{\rho} \mathrm{Gal}(K(\mathfrak{m})^S/H^S) \to 1,$$

que l'on écrit sous la forme :

$$1 \to i_T(E^S) \to \bigoplus_{v\in T} U_v/U_v^{(m_v)} \xrightarrow{\rho} \mathrm{Gal}(K(\mathfrak{m})^S/H^S) \to 1,$$

et dans laquelle ρ est l'application de réciprocité globale, on déduit la suite exacte :

$$1 \to i_{T,1}(E^S) \to \bigoplus_{v\in T} U_v/U_v^p \xrightarrow{\rho_1} B/B^p \to 1,$$

où $i_{T,1}$ est l'application composée :

$$i_{T,1} : K_T^\times \xrightarrow{i_T} \bigoplus_{v\in T} U_v \to \bigoplus_{v\in T} U_v/U_v^p.$$

On a $i_{T,1} = (i_{v,1})_{v\in T}$ en un sens évident.

(iii) Si G est un groupe abélien fini, on désigne par G^* le groupe dual $\mathrm{Hom}(G, \mathbb{C}^\times)$, et pour tout homomorphisme de groupes $h : G \to G'$, on désigne par :

$$h^* : G'^* \to G^*$$

l'application duale définie par :

$$h^*(\chi')(\sigma) = \chi'(h(\sigma)),$$

pour tout $\chi' \in G'^*$ et tout $\sigma \in G$.

2.2 Rappels. (dualité kummérienne). Soit $K_1 = K(\mu_p)$ et soit $Q_1 = K_1(\sqrt[p]{X})$, où X est un sous-groupe de $K_1^\times$ contenant $K_1^{\times p}$ et tel que $W = X/K_1^{\times p}$ soit fini (par la suite X sera de la forme $YK_1^{\times p}$ où Y est un sous-groupe de $K^\times$ contenant $K^{\times p}$; on sait que pour un exposant premier on a $W \simeq Y/Y \cap K_1^{\times p} = Y/K^{\times p}$).

On pose $G_1 = \mathrm{Gal}(Q_1/K_1)$. Alors l'application :

$$G_1 \to W^*$$

qui à $\sigma \in G_1$ associe $\chi_\sigma \in W^*$ défini par $\chi_\sigma(\overline{\alpha}) = \frac{\sigma(\sqrt[p]{\overline{\alpha}})}{\sqrt[p]{\overline{\alpha}}}$ pour tout $\overline{\alpha} \in W$, est un isomorphisme canonique ; l'application inverse est ainsi définie : si $\chi \in W^*$, il existe $\overline{\beta} \in W$ tel que $W = \langle\overline{\beta}\rangle \mathrm{Ker}(\chi)$ et l'image de χ est l'unique générateur σ_χ de $\mathrm{Gal}(Q_1/K_1(\sqrt[p]{\mathrm{Ker}(\chi)}))$ tel que $\frac{\sigma_\chi(\sqrt[p]{\overline{\beta}})}{\sqrt[p]{\overline{\beta}}} = \chi(\overline{\beta})$.

2.3 Approche par la théorie du corps de classes. Les hypothèses et notations sont celles de (2.1, i).

Soit M/H^S la sous-extension (p-élémentaire) de H_T^S/H^S fixe par $C = B \cap A^p$; on a le schéma suivant :

$$\begin{tikzcd}
H^S \arrow[r, dash, "p"] \arrow[d, dash] \arrow[rrr, dotted, dash, bend left, "B"] & M_1 \arrow[r, dash, "N"] \arrow[d, dash] & M \arrow[r, dash, "C"] \arrow[d, dash] & H_T^S \arrow[dl, dotted, dash, bend left, "A^p"] \\
H^S[p] \arrow[r, dash] \arrow[d, dash] & {} \arrow[r, dash] \arrow[d, dash] & H_T^S[p] \arrow[d, dash] & \\
K \arrow[r, dash] & L_1 \arrow[r, dash] & L &
\end{tikzcd}$$

dans lequel $H_T^S[p]$ est le sous-corps de H_T^S fixe par A^p, $H^S[p] = H^S \cap H_T^S[p]$ est fixe par $B\,A^p$; ainsi M est le composé direct, sur $H^S[p]$, de H^S et $H_T^S[p]$, et comme $\mathrm{Gal}(H_T^S[p]/K)$ est un $\mathbb{F}_p$-espace vectoriel, il existe $L \subseteq H_T^S[p]$ tel que $H_T^S[p]$ soit le composé direct de L et $H^S[p]$, donc tel que M soit le composé direct, sur K, de L et H^S (on notera que $H_T^S[p]/K$ (resp. $H^S[p]/K$) est bien la sous-extension maximale p-élémentaire de H_T^S/K (resp. H^S/K)).

On a supposé implicitement $H_T^S[p]$ distinct de $H^S[p]$, sinon le problème est trivialement impossible (on verra en (2.3.5) ce que ce cas signifie).

2.3.1 Lemme. *Une condition nécessaire et suffisante pour qu'il existe une extension L_1, cyclique de degré p, T-totalement ramifiée, S-décomposée, est qu'il existe un hyperplan N de B/C tel que :*

$$B/C = N + I_v C/C, \ \textit{pour tout } v \in T,$$

où $I_v \subseteq B$ est le groupe d'inertie de v dans H_T^S/K (noter que la somme est directe pour les places modérées, mais non nécessairement pour les places sauvages car leur groupe d'inertie peut ne pas être cyclique).

Démonstration. Si L_1 existe, il est clair que $N = \mathrm{Gal}(M/M_1)$, où $M_1 = L_1 H^S$, est un hyperplan de B/C puisque L_1 est linéairement disjointe de H^S/K pour $T \neq \emptyset$, et donc $[M_1 : H^S] = p$; ensuite, pour chaque $v \in T$, $I_v C/C$ est le groupe d'inertie de v dans M/H^S et ce groupe n'est pas contenu dans N puisque L_1/K, donc M_1/H^S, est totalement ramifiée en v. Donc $N + I_v C/C = B/C$.

Réciproquement, s'il existe un hyperplan N de B/C tel que $B/C = N + I_v C/C$ pour tout $v \in T$, alors nécessairement la sous-extension M_1/H^S fixe par N est T-totalement ramifiée puisque $I_v C/C$ est le groupe d'inertie de v dans M/H^S et n'est pas contenu dans N.

Comme M est le composé direct, sur K, de H^S et L, M_1 se redescend en une extension $L_1 \subseteq L$ de K, cyclique de degré p et T-totalement ramifiée (S-décomposée par construction). □

Nous allons traduire (2.3.1) en termes d'invariants numériques du corps K ; pour cela on établit la suite exacte importante suivante que l'on trouve déjà dans [Š] relativement à l'étude de la p-extension T-ramifiée maximale de K (cf. [G1, ch. I, § 4.5, iii]) :

2.3.2 Lemme. *On a la suite exacte :*

$$1 \to i_{T,1}(Y_T^S) \to \bigoplus_{v\in T} U_v/U_v^p \stackrel{\widetilde{\rho}_1}{\to} B/C \to 1,$$

où $\widetilde{\rho}_1$ est le composé (surjectif) :

$$\bigoplus_{v\in T} U_v/U_v^p \stackrel{\rho_1}{\to} B/B^p \to B/C,$$

$$Y_T^S = \{\alpha \in K_T^{\times p} K_T^{\times \Delta_\infty},\ (\alpha) = \mathfrak{a}^p\, \mathfrak{a}_{S_0},\ \mathfrak{a} \in I_T,\ \mathfrak{a}_{S_0} \in \langle S_0\rangle\},$$

où $\Delta_\infty = Pl^{\mathrm{r}}_\infty \setminus S_\infty$, où $K_T^{\times\Delta_\infty}$ est l'ensemble des $x \in K^\times$ étrangers à T et positifs sur Δ_∞, et où $i_{T,1}$ est définie en (2.1, ii).

Démonstration. En effet, sous la condition (2.1, i), on a l'isomorphisme de la théorie du corps de classes :

$$A/A^p \simeq \mathcal{C}\ell_{\mathfrak{m}}^S/(\mathcal{C}\ell_{\mathfrak{m}}^S)^p \simeq I_T/P_{T,\mathfrak{m}}^{\Delta_\infty}\langle S_0\rangle I_T^p,$$

où $P_{T,\mathfrak{m}}^{\Delta_\infty}$ est l'ensemble des idéaux principaux (x) pour $x \in K_{T,\mathfrak{m}}^{\times\Delta_\infty} = \{\alpha \in K^\times,\quad \alpha \equiv 1 \bmod \mathfrak{m},\quad \alpha \text{ positif sur } \Delta_\infty\}$, dans lequel l'image de B est donnée par celle de $P_T^{\Delta_\infty}\langle S_0\rangle$, ce qui donne :

$$P_T^{\Delta_\infty}\langle S_0\rangle P_{T,\mathfrak{m}}^{\Delta_\infty}\langle S_0\rangle I_T^p/P_{T,\mathfrak{m}}^{\Delta_\infty}\langle S_0\rangle I_T^p \simeq P_T^{\Delta_\infty}\,.\,\langle S_0\rangle I_T^p/P_{T,\mathfrak{m}}^{\Delta_\infty}\,.\,\langle S_0\rangle I_T^p \simeq B/C.$$

On a ensuite la suite exacte :

$$1 \to Y_T^S/Y_{T,\mathfrak{m}}^S \to K_T^{\times p}K_T^{\times\Delta_\infty}/K_T^{\times p}K_{T,\mathfrak{m}}^{\times\Delta_\infty} \to P_T^{\Delta_\infty}\,.\,\langle S_0\rangle I_T^p/P_{T,\mathfrak{m}}^{\Delta_\infty}\,.\,\langle S_0\rangle I_T^p \to 1,$$

où :

$$Y_{T,\mathfrak{m}}^S = \{\alpha \in K_T^{\times p} K_{T,\mathfrak{m}}^{\times \Delta_\infty},\ (\alpha) = \mathfrak{a}^p\, \mathfrak{a}_{S_0},\ \mathfrak{a} \in I_T,\ \mathfrak{a}_{S_0} \in \langle S_0\rangle\},$$

et dans laquelle on remplace (en utilisant le théorème d'approximation) $K_T^{\times p}K_T^{\times\Delta_\infty}/K_T^{\times p}K_{T,\mathfrak{m}}^{\times\Delta_\infty} = K_T^{\times\Delta_\infty}/K_T^{\times p}K_{T,\mathfrak{m}}^{\times\Delta_\infty}$ par :

$$\bigoplus_{v\in T} U_v/U_v^pU_v^{(m_v)} = \bigoplus_{v\in T} U_v/U_v^p,$$

et $Y_T^S/Y_{T,\mathfrak{m}}^S$ par $i_{T,1}(Y_T^S)$. □

2.3.3 Remarques. Il est très important pour la suite de remarquer que $K^{\times p}Y_T^S$ ne dépend pas de T car on a :

$$K^{\times p}Y_T^S = Y^S = \{\alpha \in K^{\times p}K^{\times\Delta_\infty},\ (\alpha) = \mathfrak{a}^p\,\mathfrak{a}_{S_0},\ \mathfrak{a} \in I,\ \mathfrak{a}_{S_0} \in \langle S_0\rangle\}.$$

On observera également que Y^S contient le groupe E^S des S-unités et que l'on a la suite exacte :

$$1 \to E^SK^{\times p}/K^{\times p} \to Y^S/K^{\times p} \to \mathcal{C}\ell^S{}_{[p]}/c\ell^S(P) \to 1,$$

où $\mathcal{C}\ell^S{}_{[p]}$ est le sous-groupe des S-classes annulées par p et où P est le groupe des idéaux principaux au sens ordinaire. Elle montre que :

$$Y^S = K^{\times p} E^S$$

si et seulement si $\mathcal{C}\ell^S{}_{[p]} = c\ell^S(P)$; pour $p \neq 2$ on a $\mathcal{C}\ell^S{}_{[p]} = c\ell^S(P)$ si et seulement si $(\mathcal{C}\ell^{S_0})_p = 1$ et pour $p = 2$, $\mathcal{C}\ell^S{}_{[2]} = c\ell^S(P)$ si et seulement si :

$$|\mathcal{C}\ell^S{}_{[2]}| = \frac{2^{|\Delta_\infty|}}{|\mathrm{sgn}_{\Delta_\infty}(E^{S_0 \mathrm{ord}})|},$$

où $\mathrm{sgn}_{\Delta_\infty}$ est la signature pour le support Δ_∞, une condition suffisante (valable pour tout p) étant que $(\mathcal{C}\ell^{S_0 \mathrm{ord}})_p = 1$.

On va utiliser la suite exacte duale de (2.3.2) :

$$1 \to (B/C)^* \xrightarrow{\widetilde{\rho}_1^*} (\bigoplus_{v \in T} U_v/U_v^p)^* \to (i_{T,1}(Y_T^S))^* \to 1.$$

En remarquant que, par la caractérisation des groupes d'inertie,

$$\widetilde{\rho}_1(U_v/U_v^p) = I_v C/C, \text{ pour tout } v \in T,$$

on a les équivalences suivantes, toujours sous l'hypothèse $B/C \neq 1$:

(i) Il existe un hyperplan N de B/C tel que :

$$B/C = N + I_v C/C, \text{pour tout } v \in T,$$

donc tel que :

$$B/C = N + \widetilde{\rho}_1(U_v/U_v^p), \text{ pour tout } v \in T \ ;$$

(ii) il existe $\psi_1 \in (B/C)^*$ tel que :

$$\psi_1(\widetilde{\rho}_1(U_v/U_v^p)) \neq 1, \text{ pour tout } v \in T,$$

donc tel que, par dualité :

$$\widetilde{\rho}_1^*(\psi_1)(U_v/U_v^p) \neq 1, \text{ pour tout } v \in T \ ;$$

(iii) il existe $\varphi_1 = \prod_{v \in T} \varphi_{1,v}$, avec $\varphi_{1,v} \in (U_v/U_v^p)^*$, tel que :

$$\varphi_1 \in \mathrm{Im}(\widetilde{\rho}_1^*), \text{ et } \varphi_{1,v} \neq 1 \text{ pour tout } v \in T \ ;$$

(iv) il existe $\varphi_1 = \prod_{v \in T} \varphi_{1,v}$, $\varphi_{1,v} \neq 1$ pour tout $v \in T$, tel que :

$$i_{T,1}(Y_T^S) \subseteq \mathrm{Ker}(\varphi_1) \ ;$$

(v) il existe des $\varphi_{1,v} \in (U_v/U_v^p)^*$, $\varphi_{1,v} \neq 1$ pour tout $v \in T$, tels que :

$$\prod_{v \in T} \varphi_{1,v}(y_v) = 1,$$

pour tout $(y_v)_{v \in T} = i_{T,1}(y) = (i_{v,1}(y))_{v \in T}$, $y \in Y_T^S$.
Ceci termine la partie "directe" de l'étude.

On considère maintenant le corps :

$$Q_{1(S)} = K_1\Big(\sqrt[p]{Y^S}\,\Big),\ \text{où } K_1 = K(\mu_p).$$

Son radical est donc $Y^S K_1^{\times p}/K_1^{\times p} \simeq Y^S/K^{\times p}$.
La théorie de Kummer montre que $Q_{1(S)}/K_1$ est $P\ell_p \cup \langle S_0\rangle$-ramifiée et Δ_∞-décomposée.

Donnons-nous maintenant $T = T_p \cup T_{\mathrm{mod}}$, non vide, disjointe de S_0, vérifiant $\mathrm{N}\mathfrak{p}_v \equiv 1 \bmod p$ pour tout $v \in T_{\mathrm{mod}}$.
D'après (2.3.3), on a aussi :

$$Q_{1(S)} = K_1\Big(\sqrt[p]{Y_T^S}\,\Big).$$

Pour chaque place $v \in T$, on considère :

$$V_{v,1}^S = \{y \in Y^S,\ i_v(y) \in K_v^{\times p}\} \text{ et } \delta_{1,v}^S = \mathrm{Gal}\Big(Q_{1(S)}/K_1\Big(\sqrt[p]{V_{v,1}^S}\,\Big)\Big)$$

(en notant que l'on a $V_{v,1}^S = K^{\times p}\{y \in Y_T^S,\ i_{v,1}(y) = 1\}$) ; il est clair que $\delta_{1,v}^S$ est le groupe de décomposition, dans $Q_{1(S)}/K_1$, d'une place arbitraire de K_1 au-dessus de v (ce groupe ne dépend que de v).

Montrons alors que la condition (v) est équivalente à :

(v′) il existe des éléments $\sigma_{1,v} \in \delta_{1,v}^S$, $\sigma_{1,v}$ d'ordre p si $\delta_{1,v}^S \simeq U_v/U_v^p$, tels que $\prod_{v\in T} \sigma_{1,v} = 1$.

– (v) $\Rightarrow$ (v′) : A chaque $\varphi_{1,v}$ on associe sa restriction à $i_{v,1}(Y_T^S)$ qui est un caractère $\chi_{1,v} \in (Y^S/K^{\times p})^* \simeq (Y_T^S/K_T^{\times p})^*$ défini par :

$$\chi_{1,v}(y) = \varphi_{1,v}(i_{v,1}(y)),\ \text{pour tout } y \in Y_T^S.$$

Par la dualité kummérienne, à $\chi_{1,v}$ correspond $\sigma_{1,v} \in \delta_{1,v}^S$ puisque $\mathrm{Ker}(\chi_{1,v})$ contient $V_{v,1}^S/K^{\times p}$.
On a alors, par hypothèse sur φ_1 :

$$\prod_{v\in T} \chi_{1,v}(y) = \prod_{v\in T} \varphi_{1,v}(i_{v,1}(y)) = 1,\ \text{pour tout } y \in Y_T^S\ ;$$

d'où $\prod_{v\in T} \sigma_{1,v} = 1$.
Si $\delta_{1,v}^S \simeq U_v/U_v^p$, la suite exacte :

$$1 \to V_{v,1}^S/K^{\times p} \to Y_T^S K^{\times p}/K^{\times p} \xrightarrow{i_{v,1}} i_{v,1}(Y_T^S) \subseteq U_v/U_v^p$$

montre que $i_{v,1}(Y_T^S) = U_v/U_v^p$, auquel cas $\sigma_{1,v} = 1$ voudrait dire $\chi_{1,v} = 1$, d'où $\varphi_{1,v} = 1$, ce qui est absurde.

– (v′) $\Rightarrow$ (v) : A chaque $\sigma_{1,v} \in \delta_{1,v}^S$ correspond $\chi_{1,v} \in (Y^S/K^{\times p})^* \simeq (Y_T^S/K_T^{\times p})^*$ et la relation $\prod_{v\in T} \sigma_{1,v} = 1$ conduit à $\prod_{v\in T} \chi_{1,v} = 1$. Comme

$\chi_{1,v}$ est trivial sur $V^S_{v,1}/K^{\times p}$, il définit un caractère de $i_{v,1}(Y^S_T) \subseteq U_v/U_v^p$ qui est donc prolongeable en un caractère $\varphi_{1,v} \in (U_v/U_v^p)^*$ que l'on peut prendre non trivial dès que $i_{v,1}(Y^S_T)$ est contenu strictement dans U_v/U_v^p, et on aura la relation :

$$(\prod_{v\in T} \varphi_{1,v})(y) = \prod_{v\in T} \varphi_{1,v}(i_{v,1}(y)) = \prod_{v\in T} \chi_{1,v}(i_{v,1}(y)) = \prod_{v\in T} \chi_{1,v}(y) = 1,$$

pour tout $y \in Y^S_T$.

Enfin si $i_{v,1}(Y^S_T) = U_v/U_v^p$, c'est que $\delta^S_{1,v} \simeq U_v/U_v^p$ et donc que $\varphi_{1,v} = \chi_{1,v}$ qui est non trivial par hypothèse.

On a donc obtenu le résultat suivant :

2.3.4 Théorème. *Soit K un corps de nombres, soit $S = S_0 \cup S_\infty \subset Pl_0 \cup Pl^{\mathrm{r}}_\infty$ un ensemble fini de places non complexes de K, et soit*

$$Y^S = \{\alpha \in K^{\times p}K^{\times \Delta_\infty},\ (\alpha) = \mathfrak{a}^p\mathfrak{a}_{S_0},\ \mathfrak{a} \in I,\ \mathfrak{a}_{S_0} \in \langle S_0\rangle\}.$$

On pose $Q_{1(S)} = K_1\left(\sqrt[p]{Y^S}\,\right)$, où $K_1 = K(\mu_p)$, et pour toute place finie v de K on désigne par $\delta^S_{1,v}$ le groupe de décomposition de v dans $Q_{1(S)}/K_1$. Soit T un ensemble fini non vide de places finies de K, tel que $T \cap S_0 = \emptyset$ et $\mathrm{N}\mathfrak{p}_v \equiv 1 \bmod p$ pour tout $v \in T_{\mathrm{mod}}$.

Alors il existe une extension cyclique de degré p de K, T-totalement ramifiée et S-décomposée, si et seulement si il existe des $\sigma_{1,v} \in \delta^S_{1,v}$, $v \in T$, avec $\sigma_{1,v}$ d'ordre p si $\delta^S_{1,v} \simeq U_v/U_v^p$, tels que :

$$\prod_{v\in T} \sigma_{1,v} = 1.$$

On retiendra que la méthode utilisée permet facilement de dénombrer l'ensemble des solutions relatives à T donné.

Si $v \in T_{\mathrm{mod}}$, $\delta^S_{1,v}$ est un groupe cyclique (d'ordre 1 ou p) engendré par le Frobenius, et comme U_v/U_v^p est cyclique d'ordre p, la condition "$\sigma_{1,v}$ d'ordre p si $\delta^S_{1,v} \simeq U_v/U_v^p$" s'écrit :

$$\sigma_{1,v} = \left(\frac{K_1\left(\sqrt[p]{Y^S}\,\right)/K_1}{v_1}\right)^{a_v},\quad a_v \in (\mathbb{Z}/p\mathbb{Z})^\times,$$

où v_1 est une place arbitraire de K_1 au-dessus de v.

Si $T_p = \emptyset$, la condition nécessaire et suffisante du théorème s'écrit :

$$\text{Il existe des } a_v \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ tels que} \quad \prod_{v\in T}\left(\frac{K_1\left(\sqrt[p]{Y^S}\,\right)/K_1}{v_1}\right)^{a_v} = 1$$

(on retrouve le cas modéré étudié dans [GM]).

En fait les conditions précédentes et le produit ne portent que sur les $v \in T$ dont le Frobenius est non trivial.

2.3.5 Remarque. Pour $T \neq \emptyset$, le cas $H_T^S[p] = H^S[p]$ (i.e. $B/C = 1$) qui rend le problème trivialement impossible, est ici équivalent à $i_{T,1}(Y_T^S) = \bigoplus_{v \in T} U_v/U_v^p$ (cf. (2.3.2)), donc finalement à :

$$\mathrm{Gal}(Q_{1(S)}/Q_{1(S)}{}^T) \simeq \bigoplus_{v \in T} U_v/U_v^p \simeq \bigoplus_{v \in T} \delta_{1,v}^S,$$

où $Q_{1(S)}{}^T$ désigne la sous-extension T-décomposée maximale de $Q_{1(S)}$; dans ce cas, l'existence des $\sigma_{1,v} \neq 1$ est trivialement impossible.

2.3.6 Corollaire (cas d'une seule place). *Si $T = \{v\}$, où v est une place modérée (cf.* [Cor]*), le problème a une solution si et seulement si $\left(\frac{Q_1(S)/K_1}{v_1}\right) = 1$ (i.e. la place v est totalement décomposée dans $Q_{1(S)}/K$, ou encore $i_v(Y^S \cap K_{\{v\}}^\times) \subset U_v^p$).*

Si v est une place sauvage, le problème a une solution si et seulement si $\delta_{1,v}^S$ n'est pas isomorphe à $U_v/U_v^p \simeq U_v^{(1)}/U_v^{(1)p}$ (ou encore si l'application canonique $i_v : Y^S \cap K_{\{v\}}^\times \to U_v/U_v^p$ n'est pas surjective).

2.3.7 Corollaire. *Soit t un ensemble fini non vide de places de K vérifiant $\mathrm{N}\mathfrak{p}_v \equiv 1$ (p) pour tout $v \in t_{\mathrm{mod}}$, et disjoint de S_0. Alors il existe une infinité de places modérées v' pour lesquelles il existe une extension cyclique de degré p de K, t ou $t \cup \{v'\}$-totalement ramifiée, S-décomposée.*

Démonstration. Dans $Q_{1(S)}/K_1$, pour un choix arbitraire de $\sigma_{1,v} \in \delta_{1,v}$, $v \in t$, $\sigma_{1,v}$ d'ordre p si $\delta_{1,v}^S \simeq U_v/U_v^p$, posons $\prod_{v \in t} \sigma_{1,v} = \tau$; si $\tau \neq 1$, par le théorème de Čebotarev on peut trouver v' telle que $\left(\frac{Q_1(S)/K}{v_1'}\right) = \tau$, et $T = t \cup \{v'\}$ répond au critère du théorème (2.4.2). $\square$

Ce résultat est intéressant en pratique uniquement s'il n'y a pas de solution avec t.

Plus généralement, on voit que dès que T contient des places (modérées) dont les Frobenius engendrent $\mathrm{Gal}(Q_{1(S)}/K_1)$, il existe une extension cyclique de degré p, T-ramifiée (non nécessairement totalement), S-décomposée.

Pour d'autres corollaires se reporter à [G1] qui traite également du cas des extensions cycliques de degré p^e.

3. Ramifications minimales

Ainsi que le suggèrent un certain nombre de travaux de Martinet (comme [M2]), on peut poser la définition suivante :

3.1 Définition. Soit K un corps de nombres, soit S un ensemble fini fixé de places non complexes de K et soit p premier.

On dit que $T \subset \mathcal{P}\ell_0$ ($T \neq \emptyset$, $T \cap S_0 = \emptyset$, $\mathrm{N}\mathfrak{p}_v \equiv 1$ (p) pour tout $v \in T_{\mathrm{mod}}$) est un ensemble de ramification minimal de K (relativement à S et p) s'il existe au moins une extension cyclique de degré p de K, T-totalement ramifiée, S-décomposée, telle que pour tout $t \subset T$, $t \neq T$, $t \neq \emptyset$, ceci n'ait pas lieu pour t.

Il est clair que si T (minimal) contient des places sauvages, les extensions T-totalement ramifiées solutions peuvent avoir des conducteurs (donc des discriminants relatifs) distincts au niveau du facteur sauvage ; la notion d'extension (cyclique de degré p) à discriminant relatif minimal (en un sens qu'il conviendrait de préciser) est plus fine mais peut se gérer à partir de la précédente, plus intrinsèque.

On observe que si $|T| = 1$, la condition de minimalité renvoie au corollaire (2.3.6) ; dès que $|T| \geq 2$, si T contient une place v pour laquelle $\delta^S_{1,v}$ n'est pas isomorphe à U_v/U_v^p, T n'est pas minimal (en effet, il existe une extension $\{v\}$-totalement ramifiée S-décomposée, puisque l'on peut prendre $\sigma_{1,v} = 1$ d'après (2.3.6)).

On suppose donc implicitement que les T considérés ont au moins 2 éléments et sont tels que $\delta^S_{1,v} \simeq U_v/U_v^p$ pour tout $v \in T$; si $v \in T_{\mathrm{mod}}$ ceci signifie que le Frobenius de v dans $Q_{1(S)}/K_1$ est d'ordre p et si $v \in T_p$ la condition, plus contraignante, signifie $i_{v,1}(Y^S_T) = U_v^{(1)}/U_v^{(1)\,p}$.

On obtient alors sans peine :

3.2 Théorème. *Soit $T \subset \mathcal{P}\ell_0$ un ensemble fini de places finies de K ($|T| \geq 2$, $T \cap S_0 = \emptyset$, $\mathrm{N}\mathfrak{p}_v \equiv 1$ (p) pour tout $v \in T_{\mathrm{mod}}$) tel que $\delta^S_{1,v} \simeq U_v/U_v^p$ pour tout $v \in T$. On suppose $T_{\mathrm{mod}} \neq \emptyset$.*

Alors T est un ensemble de ramification minimal si et seulement si le $\mathbb{F}_p$-espace des familles $(\sigma_{1,v})_{v\in T}$, $\sigma_{1,v} \in \delta^S_{1,v}$, telles que $\prod_{v\in T} \sigma_{1,v} = 1$, est de dimension 1 et est engendré par une famille $(\tau_{1,v})_{v\in T}$, $\tau_{1,v} \in \delta^S_{1,v}$, telle que $\tau_{1,v} \neq 1$ pour tout $v \in T$.

Une condition nécessaire est donc que l'on ait :

$$\sum_{v\in T} \mathrm{rg}_p(U_v) \leq \mathrm{rg}_p(Y^S/K^{\times p}) + 1,$$

ce qui majore $|T|$ très canoniquement ; si $T_p = \emptyset$, on obtient simplement :

$$|T| \leq \mathrm{rg}_p(Y^S/K^{\times p}) + 1.$$

Toujours lorsque $T_p = \emptyset$, la condition de minimalité est équivalente au fait que les Frobenius des places de T sont non triviaux et vérifient une "unique" relation de la forme :

$$\prod_{v \in T} \left(\frac{Q_1(S)/K_1}{v} \right)^{a_v} = 1,$$

$a_v \in (\mathbb{Z}/p\mathbb{Z})^\times$ pour tout $v \in T$ ($|T| \geq 2$).

Par des considérations d'algèbre linéaire élémentaire, l'utilisation du théorème de Čebotarev permet de classer les parties T minimales.

3.3 Exemple. Soit $K = \mathbb{Q}(\sqrt{5}\,)$, $S = Pl^{\mathrm{r}}_\infty$, $p = 2$.
Le corps gouvernant est donc :

$$Q_1(S) = K(\sqrt{-1}\,, \sqrt{\varepsilon}\,), \quad \varepsilon = \frac{1+\sqrt{5}}{2}.$$

C'est une extension biquadratique de K totalement ramifiée en 2.
Considérons alors :

$$T = \{\mathfrak{l}_5,\ \mathfrak{l}_{11},\ \mathfrak{l}_{19}\},$$

où :

$$\mathfrak{l}_5 = (\sqrt{5}\,), \quad \mathfrak{l}_{11} = (4+\sqrt{5}\,), \quad \mathfrak{l}_{19} = (1-2\sqrt{5}\,) \ ;$$

on obtient facilement (en termes de symboles de restes quadratiques dans les corps résiduels) :

$$\left(\frac{-1}{\mathfrak{l}_5}\right) = 1, \quad \left(\frac{-1}{\mathfrak{l}_{11}}\right) = -1, \quad \left(\frac{-1}{\mathfrak{l}_{19}}\right) = -1,$$
$$\left(\frac{\varepsilon}{\mathfrak{l}_5}\right) = -1, \quad \left(\frac{\varepsilon}{\mathfrak{l}_{11}}\right) = 1, \quad \left(\frac{\varepsilon}{\mathfrak{l}_{19}}\right) = -1.$$

Ceci montre que :

$$\delta_{\mathfrak{l}_5} = \mathrm{Gal}(Q_1(S)/K(\sqrt{-1}\,)), \ \delta_{\mathfrak{l}_{11}} = \mathrm{Gal}(Q_1(S)/K(\sqrt{\varepsilon}\,)),$$
$$\delta_{\mathfrak{l}_{19}} = \mathrm{Gal}(Q_1(S)/K(\sqrt{-\varepsilon}\,)),$$

d'où l'on déduit que T est un ensemble minimal.
Mais on peut vérifier que $T = \{\mathfrak{l}_5,\ \mathfrak{l}_{11},\ \bar{\mathfrak{l}}_{19} = (1+2\sqrt{5}\,)\}$ n'en est plus un (en effet, $t = \{\mathfrak{l}_{11},\ \bar{\mathfrak{l}}_{19}\}$ est minimal car $\delta_{\bar{\mathfrak{l}}_{19}} = \delta_{\mathfrak{l}_{11}}$).

On voit sur ce dernier exemple à 2 éléments que le choix des conjugués des places est essentiel.

3.4 Remarque. On peut vérifier par la théorie de Kummer l'existence d'une extension quadratique L/K, $\{\mathfrak{l}_5,\ \mathfrak{l}_{11},\ \mathfrak{l}_{19}\}$-totalement ramifiée totalement réelle "minimale" :

Posons $\alpha = \sqrt{5}\,(4+\sqrt{5}\,)(2\sqrt{5}\,-1) = 35 + 6\sqrt{5}$; il est clair que l'on a $\alpha >> 0$ et que $L = K(\sqrt{\alpha}\,)$ est $\{\mathfrak{l}_5,\ \mathfrak{l}_{11},\ \mathfrak{l}_{19}\}$-totalement ramifiée si elle est non ramifiée en 2 ; or on a :

$$\alpha \equiv -1 + 2\sqrt{5}\, = 1 - 4\frac{1-\sqrt{5}}{2} \equiv 1 \mod 4.$$

Il reste à vérifier la non existence d'extensions quadratiques $\{\mathfrak{l}_5\}$, $\{\mathfrak{l}_{11}\}$, $\{\mathfrak{l}_{19}\}$, $\{\mathfrak{l}_5,\ \mathfrak{l}_{11}\}$, $\{\mathfrak{l}_5,\ \mathfrak{l}_{19}\}$, $\{\mathfrak{l}_{11},\ \mathfrak{l}_{19}\}$-totalement ramifiées totalement réelles ; ceci se fait à partir du radical :

$$W^{\text{pos}} = \langle \varepsilon\sqrt{5}\,,\ 4+\sqrt{5}\,,\ \varepsilon(2\sqrt{5}\,-1)\rangle K^{\times 2}.$$

Il faut alors vérifier que les 6 extensions quadratiques correspondantes sont ramifiées en 2 en utilisant les congruences de Kummer ; c'est assez fastidieux numériquement (nombres **non** congrus à un carré modulo 4) mais sans difficultés.

En conclusion on peut dire que le principe de réflexion (même pour $p = 2$) est particulièrement profond et utile dans la mesure où il "échange" ramification et décomposition, rendant ainsi plus simple le problème de départ ; en outre la forme même du critère obtenu permet d'envisager des calculs de densités dans l'esprit des résultats de Cohen (dans ce même numéro) puisque les techniques analytiques sont tout particulièrement adaptées aux calculs de densités de Frobenius.

Bibliographie

[CDO] H. Cohen, F. Diaz y Diaz, M. Olivier, *Computing ray class groups, conductors and discriminants.* Math. of Comp. **67** (1998), 773–795.

[Co1] H. Cohen, *Advanced topics in computational number theory.* G.T.M. **193**, Springer-Verlag (2000).

[Co2] H. Cohen, *A survey of computational class field theory.* J. Théorie des Nombres de Bordeaux **11** (1999), 1–13.

[Cor] G. Cornell, *The sructure of the ray class group.* In : Algebraic Number Theory, RIMS, Kokyuroku (1987).

[Fi] C. Fieker, *Computing class fields via the Artin map.* Jour. Symb. Comput. (to appear).

[G1] G. Gras, *Pratique de la théorie du corps de classes global.* En préparation.

[G2] G. Gras, *Théorèmes de réflexion.* J. Théorie des Nombres de Bordeaux **10** (1998), 399–499.

[GM] G. Gras, A. Munnier, *Extensions cycliques T-totalement ramifiées.* Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1996/97-1997/98.

[J] J.-F. Jaulent, *Théorie ℓ-adique globale du corps de classes.* J. Théorie des Nombres de Bordeaux **10** (1998), 355–397.

[M1] J. Martinet, *Méthodes géométriques dans la recherche des petits discriminants.* Séminaire de Théorie des Nombres de Paris 1983-1984, Birkhäuser, Bâle (1985), 147-179.

[M2] J. Martinet, *On some 2-class fields.* Communication privée.

[N] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie.* Invent. Math. **21** (1973), 59–116.

[Š] I.R. Šafarevič, *Extensions with given points of ramification.* Publ. Math. Inst. Hautes Etudes Sci. **18** (1964), 71–95 ; A.M.S. Transl. (2) **59** (1966), 128–149.

[St] P. Stevenhagen, *Ray class groups and governing fields.* Ph. D. Thesis, University of Amsterdam, Amsterdam (1988).

Georges Gras
Laboratoire de Mathématiques UMR 6623
Faculté des Sciences de Besançon
25030 Besançon cedex
France
E-mail : gras@math.univ-fcomte.fr