COMPOSITIO MATHEMATICA

GEORGES GRAS

Plongements kummériens dans les $\mathbb{Z}_p$-extensions

Compositio Mathematica, tome 55, n° 3 (1985), p. 383-396
<http://www.numdam.org/item?id=CM_1985__55_3_383_0>

Compositio Mathematica 55 (1985) 383–396.

PLONGEMENTS KUMMERIENS DANS LES $\mathbb{Z}_p$-EXTENSIONS

Georges Gras

Introduction

Soit $\tilde{k}$ le composé des $\mathbb{Z}_p$-extensions d'un corps de nombres k contenant le groupe μ_{p^e} des racines p^e-ièmes de l'unité; on peut alors engendrer la sous-extension maximale $\tilde{N}$ de $\tilde{k}$, d'exposant p^e, de façon kummérienne (i.e. en écrivant $\tilde{N} = k(\sqrt[p^e]{\tilde{R}})$, où $\tilde{R}$ est un sous-groupe convenable de $k^\times$ contenant $k^{\times p^e}$). La détermination explicite de $\tilde{R}$ est un problème qui a été abordé dans des cas particuliers par plusieurs auteurs:

(i) par F. Bertrandias et J.-J. Payan [1], d'un point de vue théorique, dans l'optique de vérifier la conjecture de Leopoldt par le calcul de la $\mathbb{F}_p$-dimension de $\tilde{R}/k^{\times p}$;

(ii) par J.E. Carroll [3], par J.E. Carroll et H. Kisilevsky [4], dans le cadre de la p-ramification abélienne;

(iii) par J.E. Carroll [2], K. Kramer et A. Candiotti [8], R. Greenberg [7], dans le but d'étudier des liens remarquables qui existent entre le K_2 du corps k et les problèmes de plongements kummériens dans les $\mathbb{Z}_p$-extensions (notamment en ce qui concerne (lorsque $e = 1$) la comparaison des groupes $\tilde{R}/k^{\times p}$ et $\{a \in k^\times, \{a, \exp(2i\pi/p)\} = 1$ dans $K_2 k\}/k^{\times p}$, dont les $\mathbb{F}_p$-dimensions sont égales sous la conjecture de Leopoldt, d'après un résultat de J. Tate [10]).

Nous donnons dans cet article la méthode qui permet de trouver $\tilde{R}$ en toute généralité, dès que les classes et les unités du corps k sont connues; de façon précise, le calcul effectif de $\tilde{R}$ que nous obtenons provient du fait que nous avons donné dans [5] une solution de type corps de classes au problème du plongement dans les $\mathbb{Z}_p$-extensions (en déterminant le groupe d'Artin de toute extension de la forme $N \cap \tilde{k}$, N étant une p-extension abélienne p-ramifiée de k).

Après l'étude du cas général, Théorème 1.1, nous illustrons complètement le cas quadratique imaginaire, pour $p^e = 2$, ceci pour deux raisons:

(i) c'est le premier cas non trivial qui peut permettre une étude approfondie des problèmes de 2-ramification et de K_2;

(ii) les calculs explicites peuvent être conduits à leur terme, et illustrés numériquement par de nombreux exemples (cf. §II, 6).

I Cas general

Soit k un corps de nombres contenant le groupe μ_{p^e} des racines p^e-ièmes de l'unité (p premier, $e \geqslant 1$).

On appelle S l'ensemble des idéaux premiers de k au-dessus de p, $\hat{k}$ la p-extension abélienne p-ramifiée maximale de k (i.e. non ramifiée en dehors de S) et $\tilde{k} \subset \hat{k}$ le composé des $\mathbb{Z}_p$-extensions de k; on note G le groupe Gal $(\hat{k}/k)$ et $\tilde{G}$ le groupe Gal $(\tilde{k}/k)$.

On définit alors N (resp. $\tilde{N}$) comme la sous-extension maximale de $\hat{k}$ (resp. $\tilde{k}$) d'exposant p^e; on a donc $\tilde{N} = N \cap \tilde{k}$. Il y a deux façons de caractériser N et $\tilde{N}$:

(i) par le corps de classes, en trouvant A (resp. $\tilde{A}$), le groupe d'Artin de N (resp. $\tilde{N}$);

(ii) par la théorie de Kummer, en trouvant R (resp. $\tilde{R}$), le radical de N (resp. $\tilde{N}$).

1) Groupe d'Artin de $\tilde{N}$.

Soit P le groupe des idéaux principaux de k engendrés par un élément $u \in k^\times$ congru à 1 modulo $\prod_{\mathfrak{p} \in S} \mathfrak{p}$; soit I le groupe des idéaux fractionnaires de k dont une p-puissance est dans P. Alors le groupe d'Artin de N est

$$A = I^{p^e} P_{\mathfrak{f}},$$

où $\mathfrak{f}$ est le conducteur de N (ou un multiple) et $P_{\mathfrak{f}}$ le rayon modulo $\mathfrak{f}$. La détermination du groupe d'Artin de $\tilde{N}$ résulte alors du corollaire au théorème 2.1 de [5] utilisant la fonction Log définie sur G et à valeurs dans C/Λ, où $C = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}$ (produit des complétés de k en $\mathfrak{p} \in S$), où Λ est le sous-$\mathbb{Q}_p$-espace vectoriel de C engendré par les logarithmes p-adiques des unités de k; rappelons ce résultat:

PROPOSITION 1.1: *Le groupe d'Artin* $\tilde{\mathrm{A}}$ *de la sous-extension maximale* $\tilde{\mathrm{N}}$ *d'exposant* $\mathrm{p^e}$ *du composé des* $\mathbb{Z}_\mathrm{p}$*-extensions de* k *est égal à* $\{\mathfrak{a} \in \mathrm{I}, \mathrm{Log}\,\mathfrak{a} \in \mathrm{p^e}\overline{\mathrm{Log\ I}}\}$, *où* $\overline{\mathrm{Log\ I}} = \mathrm{Log\ G}$ *est l'adhérence de* Log I *dans* C/Λ (*on rappelle que si* $\mathfrak{a} \in \mathrm{I}$, Log $\mathfrak{a}$ *est l'image dans* C/Λ *de* $1/\mathrm{n} \log \mathrm{a}$, *pour n'importe quel* $\mathrm{n} \in \mathbb{N}^*$ *tel que* $\mathfrak{a}^{\mathrm{n}} = (\mathrm{a}) \in \mathrm{P}$, log *désignant le logarithme* p*-adique usuel*; *ceci définit* Log *pour* $(\frac{\hat{\mathrm{k}}/\mathrm{k}}{\mathfrak{a}}) \in \mathrm{G}$ *car* Log *est triviale sur le groupe d'Artin de* $\hat{\mathrm{k}}/\mathrm{k}$; *enfin* Log *se prolonge à* G).

COROLLAIRE: *L'application* Log *induit la suite exacte suivante*:

$$1 \to \tilde{A}/I^{p^e}P_{\mathfrak{f}} \to I/I^{p^e}P_{\mathfrak{f}} \xrightarrow{\mathrm{Log}} \overline{\mathrm{Log}\ I}/p^e\,\overline{\mathrm{Log}\ I} \to 0.$$

En effet, si α: $I \to G$ désigne l'application d'Artin, l'adhérence de $\alpha(A) = \alpha(I^{p^e}P_{\mathfrak{f}})$ dans G est égale à Gal $(\hat{k}/N)$ qui, par définition de N,

est égal à G^{p^e}; donc l'application Log applique bien $I^{p^e}P_{\mathfrak{f}}$ dans p^e Log $G = p^e \overline{\text{Log } I}$.

D'où la recherche pratique de $\tilde{A}$:

(i) on détermine $\overline{\text{Log } I}$ (ce qui suppose la connaissance numérique du p-groupe des classes Cl et du groupe des unités de k);

(ii) on détermine le conducteur $\mathfrak{f}$ de N (ou un multiple);

(iii) dans le groupe fini $I/I^{p^e}P_{\mathfrak{f}}$, on recherche les éléments dont le logarithme est dans $p^e\,\overline{\text{Log } I}$.

EXEMPLE: Soit $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-586})$ et $p^e = 3$; on a $Cl = Cl_1 \oplus Cl_2$ où Cl_1 et Cl_2 sont les 3-groupes des classes de $k_1 = \mathbb{Q}(\sqrt{-586})$ et de $k_2 = \mathbb{Q}(\sqrt{1758})$. Notons σ et τ les générateurs respectifs de Gal (k/k_1) et de Gal (k/k_2), et pour un nombre premier q notons $\mathfrak{l}_q$ un idéal premier de k au-dessus de q. On a alors $Cl = \langle cl\,\mathfrak{l}_5^2, cl\,\mathfrak{l}_{43}^{1+\tau}\rangle \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (l'idéal $\mathfrak{l}_5$ est inerte dans k/k_1, et la classe de l'idéal $\mathfrak{l}_5^2$, dans k_1, engendre Cl_1 qui est d'ordre 9; le nombre premier 43 est totalement décomposé dans k, la classe d'un idéal premier au-dessus de 43, dans k_2, engendre Cl_2 qui est d'ordre 3; d'où la description de Cl). On a $\mathfrak{l}_5^{18} = (1891621 + 20088\sqrt{-586})$, $\mathfrak{l}_{43}^{3(1+\tau)} = (407 + 7\sqrt{1758})$. On a ici $C = \mathbb{Q}_3 \oplus \sqrt{-586}\,\mathbb{Q}_3 \oplus \sqrt{-3}\,\mathbb{Q}_3 \oplus \sqrt{1758}\,\mathbb{Q}_3$ *et* $\Lambda = \sqrt{1758}\,\mathbb{Q}_3$ (L'unité fondamentale de k provient de celle de k_2, et son logarithme 3-adique définit un élément non nul de trace nulle qui se trouve dans le sous-espace $\mathbb{Q}_3 \oplus \sqrt{1758}\,\mathbb{Q}_3$); d'où $C/\Lambda \simeq \mathbb{Q}_3 \oplus \sqrt{-586}\,\mathbb{Q}_3 \oplus \sqrt{-3}\,\mathbb{Q}_3$. On a donc, en notant $U = \{u \in C,\ u \equiv 1 \bmod \sqrt{-3}\}$, $\overline{\text{Log } I} = (\langle \frac{1}{18} \log(1891621 + 20088\sqrt{-586}), \frac{1}{3}\log(407 + 7\sqrt{1758})\rangle + \log U + \Lambda)/\Lambda$; on vérifie facilement que $\log U = 3\mathbb{Z}_3 \oplus 3\sqrt{-586}\,\mathbb{Z}_3 \oplus 3\sqrt{-3}\,\mathbb{Z}_3 \oplus \sqrt{1758}\,\mathbb{Z}_3$, que $\frac{1}{18}\log(1891621 + 20088\sqrt{-586}) \in \log U$, et que $\frac{1}{3}\log(407 + 7\sqrt{1758}) \equiv -\frac{2}{3}\sqrt{1758}$ modulo $\log U$. Il en résulte alors $\overline{\text{Log } I} \simeq 3\mathbb{Z}_3 \oplus 3\sqrt{-586}\,\mathbb{Z}_3 \oplus 3\sqrt{-3}\,\mathbb{Z}_3$.

REMARQUE: Le corollaire au théorème 2.1 de [5] montre qu'ici, $\tilde{k}$ est linéairement disjoint du 3-corps de classes absolu de Hilbert de k (car $\overline{\text{Log } I} = \text{Log } U$), et on en déduit aussi que l'ordre de Gal $(\hat{k}/\tilde{k})$ est égal à 27.

On vérifie ensuite que $I/I^3\,P_{\mathfrak{f}}$ peut être représenté par le groupe d'idéaux $\langle \mathfrak{l}_5^2, \mathfrak{l}_{43}^{1+\tau}, (2), (3 - \sqrt{-586}), (1 + 3\sqrt{-3})\rangle$ ou encore $\langle \mathfrak{l}_5, \mathfrak{l}_{43}^{1+\tau}, \mathfrak{l}_2, \mathfrak{l}_5\mathfrak{l}_7^{1+\sigma}\mathfrak{l}_{17}, \mathfrak{l}_7^{1+\sigma\tau}\rangle = \langle \mathfrak{l}_2, \mathfrak{l}_5, \mathfrak{l}_{43}^{1+\tau}, \mathfrak{l}_7^{1+\sigma\tau}, \mathfrak{l}_7^{1+\sigma}\mathfrak{l}_{17}\rangle$. Le calcul des logarithmes 3-adiques de ces idéaux montre alors que le sous-groupe de $I/I^3\,P_{\mathfrak{f}}$ formé des éléments dont le logarithme est dans 3 $\overline{\text{Log } I}$ peut être représenté par le groupe $\langle \mathfrak{l}_2\mathfrak{l}_5, \mathfrak{l}_2^{-1}\mathfrak{l}_{43}^{1+\tau}\rangle$.

2) Radical de N.

Soit

$$R = \left\{ a \in k^\times,\ k\left(\sqrt[p^e]{a}\right) \subset N \right\}$$

le radical de N. Soit $k^{\times}(S)$ le groupe des S-unités de k. Soit $I(S)$ le sous-groupe du groupe des idéaux fractionnaires de k engendré par les éléments de S; soient Cl le p-groupe des classes de k, $Cl(S)$ le sous-groupe engendré par les classes des éléments de $I(S)$, et Cl^S le quotient $Cl/Cl(S)$; on note ${}_{p^e}Cl^S$ le sous-groupe de Cl^S formé des éléments annulés par p^e.

Il est bien connu que $a \in R$ si et seulement si l'idéal (a) de k est de la forme $(a) = \mathfrak{m}\mathfrak{a}^{p^e}$, où $\mathfrak{a}$ est un idéal quelconque de k et $\mathfrak{m} \in I(S)$. L'application qui à $a \in R$ associe l'image de la classe de $\mathfrak{a}$ dans Cl^S induit la suite exacte

$$1 \to k^{\times}(S)/k^{\times}(S)^{p^e} \to R/k^{\times p^e} \to {}_{p^e}Cl^S \to 1,$$

qui permet de trouver R dès que le groupe des classes de k et celui des unités sont connus.

EXEMPLE: Poursuivons l'illustration du cas $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-586})$; on a donc ici $R = \langle j, \sqrt{-3}, \epsilon_0, a_1, a_2 \rangle k^{\times 3}$, où $j = (-1 + \sqrt{-3})/2$, $\epsilon_0 = 587 + 14\sqrt{1758}$ est l'unité fondamentale de k, a_1 et a_2 sont les générateurs des idéaux $\mathfrak{l}_5^{18}$ et $\mathfrak{l}_{43}^{3(1+\tau)}$.

3) Symbole de reste de puissance p^e-ième.

Rappelons brièvement la définition de ce symbole: Soit $a \in k^{\times}$ et soit $\mathfrak{b}$ un idéal de k étranger à (a) et S; le symbole $\left(\frac{a}{\mathfrak{b}}\right)$ est l'unique élément de μ_{p^e} défini, via l'action du symbole d'Artin, par:

$$\left(\frac{k\left(\sqrt[p^e]{a}\right)/k}{\mathfrak{b}}\right)\sqrt[p^e]{a} = \left(\frac{a}{\mathfrak{b}}\right)\sqrt[p^e]{a};$$

il est bien connu aussi que si $\mathfrak{b} = \mathfrak{l}$ est un idéal premier, alors $\left(\frac{a}{\mathfrak{l}}\right)$ est caractérisé par la congruence

$$\left(\frac{a}{\mathfrak{l}}\right) \equiv a^{(q-1)/p^e} \text{ modulo } \mathfrak{l},$$

où q est le cardinal du corps résiduel de k en $\mathfrak{l}$.

Nous avons maintenant tous les éléments pour déterminer le radical de $\tilde{N}$.

4) Radical de $\tilde{N}$.

Soit $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_t\}$ un ensemble fini d'idéaux de k étrangers à S tel que

$$\langle \mathfrak{b}_1, \ldots, \mathfrak{b}_t \rangle I^{p^e} P_{\mathfrak{f}} = \tilde{A};$$

considérons l'application φ suivante:

$$\varphi\colon R/k^{\times p^e} \to \mu_{p^e}^t$$

déduite de l'application qui à $a \in R$ (a choisi étranger à $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$, ce qui est toujours possible modulo $k^{\times p^e}$, puisque $(a) = \mathfrak{m}\mathfrak{a}^{p^e}$, $\mathfrak{m} \in I(S)$) associe la famille $((\frac{a}{\mathfrak{b}_t}))_{i=1,\ldots,t}$. Soit $a \in R$, a étranger à $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$; alors $a \in \tilde{R}$ si et seulement si $k(\sqrt[p^e]{a}) \subset \tilde{N}$, donc si et seulement si $\sqrt[p^e]{a}$ est fixe par Gal $(N/\tilde{N})$, soit $\sqrt[p^e]{a}$ fixe par tout élément de la forme $(\frac{N/k}{\mathfrak{b}})$, $\mathfrak{b} \in \tilde{A}$; mais comme $\tilde{A} = \langle \mathfrak{b}_1, \ldots, \mathfrak{b}_t \rangle A$, où A est le groupe d'Artin de N, on en déduit que $a \in \tilde{R}$ si et seulement si $\sqrt[p^e]{a}$ est fixe par tout élément $(\frac{N/k}{\mathfrak{b}_t})$, $i = 1, \ldots, t$, donc si et seulement si $(\frac{a}{\mathfrak{b}_t}) = 1$, pour tout $i = 1, \ldots, t$; autrement dit, $\tilde{R}/k^{\times p^e}$ est le noyau de φ.

Résumons ce qui précède dans l'énoncé suivant:

THÉORÈME 1.1: *Soit* k *un corps de nombres contenant les racines* p^e*-ièmes de l'unité. Soit* R *le radical de l'extension kummérienne maximale* p*-ramifiée de* k, *d'exposant* p^e, *et soit* $\mathfrak{f}$ *le conducteur de cette extension. Soit* I *le groupe des idéaux de* k *étrangers à* p, *soit* $P_{\mathfrak{f}} \subset I$ *le rayon modulo* $\mathfrak{f}$, *et soient* $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ *des idéaux de* I *tels que* $\langle \mathfrak{b}_1, \ldots, \mathfrak{b}_t \rangle I^{p^e} P_{\mathfrak{f}} = \{\mathfrak{a} \in I, \operatorname{Log} \mathfrak{a} \in p^e \overline{\operatorname{Log} I}\}$. *Alors l'application de* R *dans* $\mu_{p^e}^t$ *qui à* $a \in R$ *associe* $((\frac{a}{\mathfrak{b}_i}))_{i=1,\ldots,t}$ *a pour noyau le radical* $\tilde{R}$ *de la sous-extension maximale d'exposant* p^e *du composé des* $\mathbb{Z}_p$*-extensions de* k.

EXEMPLE: Terminons l'illustration du cas $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-586})$; il ne reste plus qu'à calculer le tableau des symboles de la forme $(\frac{a}{\mathfrak{b}})$, $a \in \{j, \sqrt{-3}, \epsilon_0, a_1, a_2\}$ et $\mathfrak{b} \in \{\mathfrak{l}_2\mathfrak{l}_5, \mathfrak{l}_2^{-1}\mathfrak{l}_{43}^{1+\tau}\}$:

	$\mathfrak{l}_2\mathfrak{l}_5$	$\mathfrak{l}_2^{-1}\mathfrak{l}_{43}^{1+\tau}$
j	1	1
$\sqrt{-3}$	1	1
ϵ_0	j	1
a_1	1	j
a_2	j	1

Le calcul des symboles ci-dessus s'effectue à partir des congruences suivantes (où $\sqrt{-3} = 2j + 1$):

$$\sqrt{-586} \equiv 3(\mathfrak{l}_5), \sqrt{-3}\sqrt{-586} \equiv 34(\mathfrak{l}_{43}^{1+\tau}),$$

$$j \equiv -7(\mathfrak{l}_{43}), \; j \equiv 6(\mathfrak{l}_{43}^{\tau}).$$

On obtient donc

$$\tilde{R} = \langle j, \sqrt{-3}, \epsilon_0^{-1} a_2 \rangle$$

$$= \langle \frac{-1+\sqrt{-3}}{2}, \sqrt{-3}, 66625 + 1589\sqrt{1758} \rangle.$$

II Cas des corps quadratiques imaginaires (et $p = 2$)

Soit $k = \mathbb{Q}(\sqrt{-m})$, $m > 0$ sans facteur carré; on suppose ici $p = 2$, $e = 1$. Les problèmes locaux à résoudre vont dépendre essentiellement de $C = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}$ qui prend les huit valeurs habituelles: $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{-3})$, $\mathbb{Q}_2(\sqrt{-5})$, $\mathbb{Q}_2(\sqrt{-6})$, $\mathbb{Q}_2 \times \mathbb{Q}_2$, $\mathbb{Q}_2(\sqrt{-10})$, $\mathbb{Q}_2(\sqrt{-14})$. Nous définissons aussi l'invariant $\rho = 0$ ou 1, en posant $\rho = 1$ si et seulement si tout diviseur premier impair de m est congru à ± 1 modulo 8.

1) Cas particuliers immédiats.

Il s'agit des corps k pour lesquels le groupe Gal $(\hat{k}/\tilde{k})$ est trivial; nous avons caractérisé une telle situation dans [5], corollaire au théorème 5.2; ce résultat s'énonce ici de la façon suivante:

THÉORÈME 2.1: *Si* k *est l'un des corps* $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-l})$ *ou* $\mathbb{Q}(\sqrt{-2l})$, *l premier*, $l \equiv 3, 5 \bmod 8$, *alors l'extension biquadratique de k contenue dans le composé des* $\mathbb{Z}_2$*-extensions de* k *est* $\mathrm{k}(\sqrt{1+\sqrt{-1}}, \sqrt{\sqrt{-1}})$ *pour* $\mathrm{k} = \mathbb{Q}(\sqrt{-1})$, $\mathrm{k}(\sqrt{\sqrt{-2}}, \sqrt{-1})$ *pour* $\mathrm{k} = \mathbb{Q}(\sqrt{-2})$, $\mathrm{k}(\sqrt{2}, \sqrt{-1})$ *dans les deux autres cas.*

Ce résultat est élémentaire, mais le problème devient bien plus difficile dès que Gal $(\hat{k}/\tilde{k})$ est non trivial (cf. Exemple du §1); nous allons reprendre et préciser les étapes générales évoquées dans le §1, afin d'aboutir à une méthode de calcul systématique de $\tilde{R}$, pour tout corps quadratique imaginaire. Les résultats seront donnés de façon immédiatement utilisable par le lecteur, pour tout calcul numérique; les justifications élémentaires seront omises.

2) Calcul du radical de N.

On suppose ici k distinct de $\mathbb{Q}(\sqrt{-1})$ et de $\mathbb{Q}(\sqrt{-2})$. On peut donc poser $m = l_1 \dots l_n$ ou $2l_1 \dots l_n$, $l_1, \dots, l_n$ nombres premiers impairs dis-

tincts, $n \geqslant 1$; on note $\mathfrak{l}_i$ l'idéal premier au-dessus de l_i, $i = 1, \ldots, n$, et on note $\mathfrak{p}$ un idéal premier de k au-dessus de 2.
On a les résultats classiques suivants:

LEMME 1: *Une $\mathbb{F}_2$-base de ${}_2\mathrm{Cl}$ est donnée par les ensembles de classes suivants*:

$\{cl\mathfrak{l}_1, \ldots, cl\mathfrak{l}_n\}$, *si* $-m \equiv -2 \bmod 4$,

$\{cl\mathfrak{l}_1, \ldots, cl\mathfrak{l}_{n-1}, cl\mathfrak{p}\}$, *si* $-m \equiv -1 \bmod 4$,

$\{cl\mathfrak{l}_1, \ldots, cl\mathfrak{l}_{n-1}\}$, *si* $-m \equiv -3 \bmod 4$.

LEMME 2: *Supposons* 2 *non inerte dans* k. *Alors il existe* $\mathrm{a} \in \mathrm{k}^\times$ *tel que* $(\mathrm{a}) = \mathfrak{p}\mathfrak{a}^2$ *dans* k, *si et seulement si* $\rho = 1$. *Si c'est le cas, et si l'on écrit* $-\mathrm{m} = \mathrm{x}^2 - 2\mathrm{y}^2$ *dans* $\mathbb{Z}$, *alors* $(\mathrm{x} + \sqrt{-\mathrm{m}}) = \mathfrak{p}\mathfrak{a}_0^2$ *dans* k, *pour un choix convenable du signe de* x *lorsque* 2 *est décomposé.*

LEMME 3: *Si* 2 *est décomposé dans* k *et si* $\rho = 0$, *alors la classe de* $\mathfrak{p}$ *est d'ordre pair.*

Ces lemmes préliminaires nous permettent de déterminer R à partir de la suite exacte (cf. §I, 2)

$$1 \to k^\times(S)/k^\times(S)^2 \to R/k^{\times 2} \to {}_2Cl^S \to 1,$$

où l'on rappelle que $k^\times(S)$ est le groupe des S-unités de k et Cl^S le 2-groupe des classes en dehors de S; le résultat est le suivant:

PROPOSITION 2.1: *Le radical de* N *est* $\mathrm{R} = \langle 2, -1, l_1, \ldots, l_{n-1}\rangle \mathrm{k}^{\times 2}$ *si* $\rho = 0$, $\mathrm{R} = \langle 2, -1, l_1, \ldots, l_{n-1}, \mathrm{x} + \sqrt{-\mathrm{m}}\rangle \mathrm{k}^{\times 2}$ *si* $\rho = 1$ (*où* x *est donné par une solution dans* $\mathbb{Z}$ *de l'équation* $-\mathrm{m} = \mathrm{x}^2 - 2\mathrm{y}^2$).

REMARQUE: On a toujours $k(\sqrt{2}) \subset \tilde{k}$; on pourra donc "ignorer" 2 dans le calcul de $\tilde{R}$. Ces générateurs de R sont indépendants modulo $k^{\times 2}$.

3) Calcul du conducteur de N.

C'est le plus petit commun multiple des conducteurs des sous-extensions quadratiques de N/k; il suffit donc de calculer les conducteurs des extensions $K = k(\sqrt{-1})$, $k(\sqrt{2})$, $k(\sqrt{\pm l})$, l premier impair, $\pm l \equiv 1 \bmod 4$, et enfin $k(\sqrt{x + \sqrt{-m}})$ lorsque $\rho = 1$ (en supposant toujours $k \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$).

Il suffit de déterminer une uniformisante de K et de calculer la différente relative dans K/k (puis le discriminant relatif) par la méthode

habituelle des groupes de ramification (cf. [9], chap. IV, §§1, 2, propositions 4 et 5); ici, le conducteur de K/k est égal à son discriminant; on obtient:

PROPOSITION 2.2: *Le conducteur* $\mathfrak{f}$ *de* N *a la valeur suivante*:

$$\begin{aligned}
&\text{(i) } \textit{cas } \rho = 0; \quad \mathfrak{f} = (2) \textit{ pour } -m \equiv -2 \bmod 4,\\
&\qquad\qquad\quad \mathfrak{f} = (4) \textit{ pour } -m \equiv -1 \bmod 4,\\
&\qquad\qquad\quad \mathfrak{f} = (8) \textit{ pour } -m \equiv -3 \bmod 4,\\
&\text{(ii) } \textit{cas } \rho = 1; \quad \mathfrak{f} = 4\mathfrak{p} \textit{ pour } -m \equiv -1, -2 \bmod 4,\\
&\qquad\qquad\quad \mathfrak{f} = (8) \textit{ pour } -m \equiv -3 \bmod 4.
\end{aligned}$$

4) Détermination du groupe d'Artin de $\tilde{N}$.

On rappelle que le groupe d'Artin $\tilde{A}$ de $\tilde{N}$ est défini par la suite exacte (cf. §I, 1)

$$1 \to \tilde{A}/I^2P_{\mathfrak{f}} \to I/I^2P_{\mathfrak{f}} \overset{\text{Log}}{\to} \overline{\text{Log } I}/2\,\overline{\text{Log } I} \to 0;$$

dans le cas quadratique imaginaire, la fonction Log s'identifie au logarithme 2-adique usuel, log, étendu à $\dot{I}$, car $\Lambda = 0$. Comme en pratique Cl est décrit sous la forme

$$I = \langle \mathfrak{c}_1, \ldots, \mathfrak{c}_r \rangle P,\ \mathfrak{c}_1, \ldots, \mathfrak{c}_r \in \dot{I},$$

on considère la suite exacte

$$1 \to I^2P/I^2P_{\mathfrak{f}} \to I/I^2P_{\mathfrak{f}} \to I/I^2P \simeq Cl/Cl^2 \to 1,$$

où $I^2P/I^2P_{\mathfrak{f}} \simeq P/P_{\mathfrak{f}}(P \cap I^2)$; ainsi, si l'on écrit $P = \langle (u_1), \ldots, (u_s) \rangle P_{\mathfrak{f}}(P \cap I^2)$, alors

$$I = \langle \mathfrak{c}_1, \ldots, \mathfrak{c}_r, (u_1), \ldots, (u_s) \rangle I^2P_{\mathfrak{f}}.$$

Nous allons déterminer $P/P_{\mathfrak{f}}(P \cap I^2)$; pour cela, soient

$$k_S^\times = \left\{ u \in k^\times,\ u \equiv 1 \bmod \prod_{\mathfrak{p} \in S} \mathfrak{p} \right\} \text{ et } k_{\mathfrak{f}}^\times = \{ u \in k^\times,\ u \equiv 1 \bmod \mathfrak{f} \},$$

et soit

$$\Omega = \left\{ u \in k_S^\times,\ (u) \in P_{\mathfrak{f}}(P \cap I^2) \right\};$$

alors on a $P/P_{\mathfrak{f}}(P \cap I^2) \simeq k_S^\times/\Omega$.

LEMME 4: *Le groupe* Ω *a l'expression suivante*:

$$\Omega = \langle -1, l_1, \ldots, l_{n'} \rangle k_{\mathfrak{f}}^{\times} k_S^{\times 2}, \text{ si } -m \equiv -2, -3 \bmod 4,$$

$$\Omega = \langle -1, l_1, \ldots, l_{n'}, 2+\sqrt{-m} \rangle k_{\mathfrak{f}}^{\times} k_S^{\times 2}, \text{ si } -m \equiv -5 \bmod 8,$$

$$\Omega = \langle -1, l_1, \ldots, l_{n'}, \sqrt{-m} \rangle k_{\mathfrak{f}}^{\times} k_S^{\times 2}, \text{ si } -m \equiv -1 \bmod 8 \text{ et } \rho = 0,$$

$$\text{ou } -m \equiv -1 \bmod 16 \text{ et } \rho = 1,$$

$$\Omega = \langle -1, l_1, \ldots, l_{n'}, 3\sqrt{-m} \rangle k_{\mathfrak{f}}^{\times} k_S^{\times 2}, \text{ si } -m \equiv -9 \bmod 16$$

et $\rho = 1$, *l'entier* n' *étant égal à* n *si* $-m \equiv -2 \bmod 4$, $n-1$ *sinon*.

Soit $u \in k_S^{\times}$ tel que $(u) = (u_{\mathfrak{f}})\mathfrak{a}^2$, $u_{\mathfrak{f}} \in k_{\mathfrak{f}}^{\times}$, $\mathfrak{a} \in I$:

(i) cas $-m \equiv -2, -3 \bmod 4$. Comme ${}_2Cl = \langle cl\mathfrak{l}_1, \ldots, cl\mathfrak{l}_{n'} \rangle$, on peut écrire $\mathfrak{a} = (v)\prod_{i=1}^{n'} \mathfrak{l}_i^{x_i}$, $x_i \in \mathbb{Z}$, $v \in k_S^{\times}$, d'où $u = \pm u_{\mathfrak{f}} v^2 \prod_{i=1}^{n'} l_i^{x_i}$; d'où Ω dans ce cas.

(ii) cas $-m \equiv -1 \bmod 4$. Dans ce cas ${}_2Cl = \langle cl\mathfrak{l}_1, \ldots, cl\mathfrak{l}_{n'}, cl\mathfrak{p} \rangle$, et on peut écrire $\mathfrak{a} = (a)\mathfrak{p}^{x_0}\prod_{i=1}^{n'} \mathfrak{l}_i^{x_i}$, $x_0, x_i \in \mathbb{Z}$, $a \in k^{\times}$. Soit $\mathfrak{b} \in I$ tel que $\mathfrak{p}\mathfrak{b} = (b)$, $b \in k^{\times}$; on a alors $\mathfrak{b}^2 = (b^2/2) = (v)$, $v \in k_S^{\times}$.

Si $-m \equiv -5 \bmod 8$, la démonstration de la proposition 2.1 de [6] montre que l'on a $v \equiv 2 \pm \sqrt{-m}$ modulo 4, donc modulo $\mathfrak{f}$ d'après la proposition 2.2; il vient alors $\mathfrak{a}^2 = (a^2 b^{2x_0} v^{-x_0} \prod_{i=1}^{n'} l_i^{x_i})$, soit $u = \pm u_{\mathfrak{f}}(ab^{x_0})^2 v^{-x_0} \prod_{i=1}^{n'} l_i^{x_i}$. On a $2 \pm \sqrt{-m} = vu'_{\mathfrak{f}}$, $u'_{\mathfrak{f}} \in k_{\mathfrak{f}}^{\times}$, donc $(2+\sqrt{-m})(2-\sqrt{-m}) \in k_{\mathfrak{f}}^{\times} k_S^{\times 2}$ puisque $N_{k/\mathbb{Q}} v = N\mathfrak{b}^2$ est un carré dans $\mathbb{Q}^{\times}$; on peut donc remplacer v par $2+\sqrt{-m}$ modulo $k_{\mathfrak{f}}^{\times} k_S^{\times 2}$. D'où le lemme dans ce cas.

Si $-m \equiv -1 \bmod 8$, la démonstration du lemme 1 du théorème 2.3 de [6] montre que l'on a $v \equiv \sqrt{-m} + 4(m-1)/8 \bmod 4\mathfrak{p}$. Si $\rho = 0$, $(\sqrt{-m}) \in I^2 P_{\mathfrak{f}}$, car $\mathfrak{f} = (4)$ dans ce cas; si $\rho = 1$ et $-m \equiv -1 \bmod 16$, on a aussi $(\sqrt{-m}) \in I^2 P_{\mathfrak{f}}$; enfin si $\rho = 1$ et $-m \equiv -9 \bmod 16$, on a $v \equiv \sqrt{-m} + 4 \equiv -3\sqrt{-m} \bmod \mathfrak{f}$, et $(3\sqrt{-m}) \in I^2 P_{\mathfrak{f}}$. D'où le lemme dans ce cas, de façon analogue.

Il reste à trouver un système de représentants de $k_S^{\times}/\Omega$.

Si U (resp. $U_{\mathfrak{f}}$) désigne l'adhérence dans C de $k_S^{\times}$ (resp. $k_{\mathfrak{f}}^{\times}$), on a

$$k_S^{\times}/\Omega \simeq U/V, \text{ où } V = \langle -1, l_1, \ldots, l_{n'}, v_0 \rangle U_{\mathfrak{f}} U^2,$$

v_0 étant, selon le cas, l'un des nombres 1, $2+\sqrt{-m}$, $\sqrt{-m}$ ou $3\sqrt{-m}$ du lemme 4. On considère alors la suite exacte suivante induite par l'application log (où tor désigne la 2-torsion):

$$1 \to \operatorname{tor} U/\operatorname{tor} V \to U/V \to \log U/\log V \to 0;$$

Tableau A

$-m$ mod 16	ρ	$\mathfrak{f}$	$\log U$	$\log V$	$u_i \bmod V$	$\log u_i \bmod(\log V)$
$-1, -9$	0	(4)	$(4)\oplus(2+2\sqrt{-m})$	$(4)\oplus(4\sqrt{-m})$	$2+\sqrt{-m}$	$2+2\sqrt{-m}$
-1	1	$4\mathfrak{p}$	$(4)\oplus(2+2\sqrt{-m})$	$(8)\oplus(4+4\sqrt{-m})$	$2+\sqrt{-m}, 2-\sqrt{-m}$	$2+2\sqrt{-m}, 2-2\sqrt{-m}$
-9	1	$4\mathfrak{p}$	$(4)\oplus(2+2\sqrt{-m})$	$(8)\oplus(4+4\sqrt{-m})$	$2+\sqrt{-m}, 2-\sqrt{-m}$	$2-2\sqrt{-m}, 2+2\sqrt{-m}$
-2	0	(2)	$(4)\oplus(2+\sqrt{-m})$	$(4)\oplus(2\sqrt{-m})$	$1+\sqrt{-m}$	$2+\sqrt{-m}$
-2	1	$4\mathfrak{p}$	$(4)\oplus(2+\sqrt{-m})$	$(8)\oplus(4+2\sqrt{-m})$	$1+\sqrt{-m}, 1-\sqrt{-m}$	$2-\sqrt{-m}, 2+\sqrt{-m}$
$-3, -11$	0	(8)	$(2)\oplus(2\sqrt{-m})$	$(4)\oplus(4\sqrt{-m})$	$\sqrt{-m}, 2+\sqrt{-m}$	$2, 2\sqrt{-m}$
$-5, -13$	0	(4)	$(2)\oplus(2\sqrt{-m})$	$(4)\oplus(2\sqrt{-m})$	$\sqrt{-m}$	2
-6	0	(2)	$(4)\oplus(\sqrt{-m})$	$(4)\oplus(2\sqrt{-m})$	$1+\sqrt{-m}$	$\sqrt{-m}$
$-7, -15$	0	(8)	$(4)\oplus(2+2\sqrt{-m})$	$(4)\oplus(4\sqrt{-m})$	$\sqrt{-m}, 2+\sqrt{-m}$	$0, 2+2\sqrt{-m}$
-7	1	(8)	$(4)\oplus(2+2\sqrt{-m})$	$(8)\oplus(4+4\sqrt{-m})$	$\sqrt{-m}, 2+\sqrt{-m}, 2-\sqrt{-m}$	$4, -2+2\sqrt{-m}, -2-2\sqrt{-m}$
-15	1	(8)	$(4)\oplus(2+2\sqrt{-m})$	$(8)\oplus(4+4\sqrt{-m})$	$\sqrt{-m}, 2+\sqrt{-m}, 2-\sqrt{-m}$	$0, 2+2\sqrt{-m}, 2-2\sqrt{-m}$
-10	0	(2)	$(4)\oplus(2+\sqrt{-m})$	$(4)\oplus(2\sqrt{-m})$	$1+\sqrt{-m}$	$2+\sqrt{-m}$
-14	0	(2)	$(4)\oplus(\sqrt{-m})$	$(4)\oplus(2\sqrt{-m})$	$1+\sqrt{-m}$	$\sqrt{-m}$
-14	1	$4\mathfrak{p}$	$(4)\oplus(\sqrt{-m})$	$(8)\oplus(2\sqrt{-m})$	$1+\sqrt{-m}, 3+\sqrt{-m}$	$\sqrt{-m}, 4+\sqrt{-m}$

l'expression de $\log U$ est donnée par le tableau I de [6], et on peut de même déterminer $\log U_{\mathfrak{f}}$ facilement, puis

$$\log V = \langle \log l_1, \ldots, \log l_{n'}, \log v_0 \rangle + \log U_{\mathfrak{f}} + 2 \log U.$$

Ensuite, pour trouver des représentants $u_1, \ldots, u_s$ tels que

$$U = \langle u_1, \ldots, u_s \rangle V,$$

on utilise la suite exacte précédente compte tenu du fait que tor $U/\text{tor } V$ est trivial sauf si 2 est décomposé dans $k/\mathbb{Q}$, auquel cas ce groupe est d'ordre 2; les résultats correspondants constituent le tableau A ci-dessus (dans ce tableau, les groupes de logarithmes, $\log U$, $\log V$, sont caractérisés par une $\mathbb{Z}_2$-base à deux éléments).

5) Calcul des symboles

Ayant déterminé $\tilde{A}$ comme noyau de l'application $\langle \mathfrak{c}_1, \ldots, \mathfrak{c}_r, (u_1), \ldots, (u_s) \rangle I^2 P_{\mathfrak{f}} / I^2 P_{\mathfrak{f}} \to \overline{\log I}/2\,\overline{\log I}$, et écrit

$$\tilde{A} = \langle \mathfrak{b}_1, \ldots, \mathfrak{b}_t \rangle I^2 P_{\mathfrak{f}},$$

il reste à calculer les symboles suivants: $(\frac{-1}{\mathfrak{b}})$, $(\frac{l}{\mathfrak{b}})$, pour $l \in \{l_1, \ldots, l_{n-1}\}$, $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_t\}$, si $\rho = 0$, $(\frac{-1}{\mathfrak{b}})$, $(\frac{l}{\mathfrak{b}})$, $(\frac{x+\sqrt{-m}}{\mathfrak{b}})$, pour $l \in \{l_1, \ldots, l_{n-1}\}$, $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_t\}$, si $\rho = 1$.

REMARQUE: Si a est un nombre rationnel impair étranger à $\mathfrak{b} \in I$, alors $(\frac{a}{\mathfrak{b}}) = (\frac{a}{N\mathfrak{b}})$, où $N\mathfrak{b}$ désigne la norme absolue de $\mathfrak{b}$ et $(\div)$ le symbole de Jacobi usuel; d'où les règles que nous rappelons:

(i) On a $(\frac{-1}{\mathfrak{b}}) = (-1)^{(N\mathfrak{b}-1)/2}$;

(ii) par réciprocité quadratique, on a $(\frac{l}{\mathfrak{b}}) = (-1)^{(l-1)(N\mathfrak{b}-1)/4}(\frac{N\mathfrak{b}}{l})$;

(iii) le calcul de $(\frac{x+\sqrt{-m}}{\mathfrak{b}})$ s'effectue de façon analogue après avoir trouvé $\beta \in \mathbb{Z}$ tel que $\sqrt{-m} \equiv \beta \bmod \mathfrak{b}$: on est ramené à calculer $(\frac{x+\beta}{\mathfrak{b}}) = (\frac{x+\beta}{Nb})$.

Si un symbole $(\frac{a}{\mathfrak{b}})$ ne peut se calculer parce que a n'est pas étranger à $\mathfrak{b}$, on peut modifier a modulo $k^{\times 2}$ pour le rendre étranger à $\mathfrak{b}$.

Les éléments universels $u_1, \ldots, u_s$ du tableau A peuvent être modifiés modulo $\mathfrak{f}$, notamment pour faire en sorte que les symboles $(\frac{a}{\mathfrak{b}})$ soient tous définis sans avoir à modifier les éléments a.

6) Conclusion et exemples.

L'ensemble des résultats obtenus peut s'énoncer globalement de la façon suivante:

THÉORÈME 2.2: *Soit* $k = \mathbb{Q}(\sqrt{-m})$, *où* m *est de la forme* $l_1 \dots l_n$ *ou* $2l_1 \dots l_n$, $n \geqslant 1$, $l_1, \dots, l_n$ *premiers impairs distincts. Soient* $c, \dots, c_r$ *des idéaux impairs représentant le 2-groupe des classes* I/P *de* k, *et soient* $(u_1), \dots, (u_s)$ *des idéaux principaux impairs représentant* $P/P_f(P \cap I^2)$. *Soient alors* $\mathfrak{b}_1, \dots, \mathfrak{b}_t$ *des idéaux impairs tels que* $\langle \mathfrak{b}_1, \dots, \mathfrak{b}_t \rangle = \{\mathfrak{b} \in \langle c_1, \dots, c_r, (u_1), \dots, (u_s) \rangle, \log \mathfrak{b} \in 2\overline{\log I}\}$. *Enfin soit* $R' = \langle -1, l_1, \dots, l_{n-1} \rangle$ *si* $\rho = 0$, $R' = \langle -1, l_1, \dots, l_{n-1}, x + \sqrt{-m} \rangle$ (*où*-$m = x^2 - 2y^2$ *dans* $\mathbb{Z}$) *si* $\rho = 1$.

Alors, un élément a_0, *tel que* $k(\sqrt{2}, \sqrt{a_0})$ *soit la sous-extension bi-quadratique sur* k *contenue dans le composé des* $\mathbb{Z}_2$*-extensions de* k, *est donné par l'unique élément non trivial* a_0 *de* R' *qui vérifie* $(\frac{a_0}{\mathfrak{b}_i}) = 1$, *pour tout* $i = 1, \dots, t$.

NOTE: Pour l'utilisation pratique de ce théorème, rappelons que $\rho = 0$ ou 1 est égal à 1 si et seulement si $l_i \equiv \pm 1 \bmod 8$ pour tout $i = 1, \dots, n$, que les éléments $u_1, \dots, u_s$ sont donnés, une fois pour toutes, dans le tableau A, ainsi que leurs logarithmes.

EXEMPLE 1: Soit $k = \mathbb{Q}(\sqrt{-1155}) = \mathbb{Q}(\sqrt{-3.5.7.11})$, dont le groupe des classes est $\langle cl\mathfrak{l}_3, cl\mathfrak{l}_5, cl\mathfrak{l}_7 \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3$. On a immédiatement $\overline{\log I} = \langle \frac{1}{2}\log 3, \frac{1}{2}\log 5, \frac{1}{2}\log 7 \rangle + \log U = \log U = (2) \oplus (2\sqrt{-m})$ dans $C = \mathbb{Q}_2(\sqrt{-3})$; d'où $2\overline{\log I} = (4) \oplus (4\sqrt{-m})$. Le tableau A indique qu'il faut considérer le groupe d'idéaux $\langle \mathfrak{l}_3, \mathfrak{l}_5, \mathfrak{l}_7, (\sqrt{-m}), (2 + \sqrt{-m}) \rangle = \langle \mathfrak{l}_3, \mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3\mathfrak{l}_5\mathfrak{l}_7\mathfrak{l}_{11}, \mathfrak{l}_{19}\mathfrak{l}_{61} \rangle = \langle \mathfrak{l}_3, \mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_{11}, \mathfrak{l}_{19}\mathfrak{l}_{61} \rangle$; on calcule les logarithmes de ces idéaux modulo $(4) \oplus (4\sqrt{-m})$:

$$\begin{aligned} \text{on } a \quad & \log \mathfrak{l}_3 \equiv 2 \bmod (4) \oplus (4\sqrt{-m}) \\ & \log \mathfrak{l}_5 \equiv 2 \bmod (4) \oplus (4\sqrt{-m}) \\ & \log \mathfrak{l}_7 \equiv 0 \bmod (4) \oplus (4\sqrt{-m}) \\ & \log \mathfrak{l}_{11} \equiv 2 \bmod (4) \oplus (4\sqrt{-m}) \\ & \log(\mathfrak{l}_{19}\mathfrak{l}_{61}) \equiv 2\sqrt{-m} \bmod (4) \oplus (4\sqrt{-m}) \end{aligned}$$

ce qui fait que l'on trouve $\mathfrak{b}_1 = \mathfrak{l}_3\mathfrak{l}_5$, $\mathfrak{b}_2 = \mathfrak{l}_7$, $\mathfrak{b}_3 = \mathfrak{l}_3\mathfrak{l}_{11}$. Ici, $R' = \langle -1, 3, 5, 7 \rangle$, d'où le tableau des symboles $(\frac{a}{\mathfrak{b}})$:

	$\mathfrak{l}_3\mathfrak{l}_5$	$\mathfrak{l}_7$	$\mathfrak{l}_3\mathfrak{l}_{11}$
−1	−1	−1	1
3	1	−1	−1
5	−1	−1	−1
7	−1	−1	−1

D'où $a_0 = 35$ et $\tilde{N} = k(\sqrt{2}, \sqrt{35})$.

EXEMPLE 2: Soit $k = \mathbb{Q}(\sqrt{-161}) = \mathbb{Q}(\sqrt{-7.23})$; on vérifie que $Cl = \langle cl\mathfrak{l}_3, cl\mathfrak{l}_7 \rangle \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $cl\mathfrak{l}_3$ étant d'ordre 8 et $cl\mathfrak{l}_7$ d'ordre 2. On vérifie que $\log \mathfrak{l}_3 = \frac{1}{8} \log(80 + \sqrt{-161})$ et $\log \mathfrak{l}_7 = \frac{1}{2} \log 7$ sont dans $\log U = (4) \oplus (2 + 2\sqrt{-161})$, d'où $2 \overline{\log \mathfrak{l}} = (8) \oplus (4 + 4\sqrt{-161})$. On est dans le cas $-m \equiv -1 \bmod 16$ et $\rho = 1$ du tableau A; on a donc à considérer le groupe d'idéaux $\langle \mathfrak{l}_3, \mathfrak{l}_7, (2 + \sqrt{-161}), (2 - \sqrt{-161}) \rangle = \langle \mathfrak{l}_3, \mathfrak{l}_7, \mathfrak{l}_3\mathfrak{l}_5\mathfrak{l}_{11}, \bar{\mathfrak{l}}_3\bar{\mathfrak{l}}_5\bar{\mathfrak{l}}_{11} \rangle$.

$$\begin{aligned} \text{On } a \quad & \log \mathfrak{l}_3 \equiv 2 - 2\sqrt{-161} \bmod (8) \oplus (4 + 4\sqrt{-161}) \\ & \log \mathfrak{l}_7 \equiv 4 \bmod (8) \oplus (4 + 4\sqrt{-161}) \\ & \log(\mathfrak{l}_3\mathfrak{l}_5\mathfrak{l}_{11}) \equiv 2 + 2\sqrt{-161} \bmod (8) \oplus (4 + 4\sqrt{-161}) \\ & \log(\bar{\mathfrak{l}}_3\bar{\mathfrak{l}}_5\bar{\mathfrak{l}}_{11}) \equiv 2 - 2\sqrt{-161} \bmod (8) \oplus (4 + 4\sqrt{-161}) \end{aligned}$$

ce qui donne $\mathfrak{b}_1 = \mathfrak{l}_7\mathfrak{l}_5\mathfrak{l}_{11}$ et $\mathfrak{b}_2 = \mathfrak{l}_3\bar{\mathfrak{l}}_3\bar{\mathfrak{l}}_5\bar{\mathfrak{l}}_{11}$. On a ici $R' = \langle -1, 7, 1 + \sqrt{-161} \rangle$; d'où le tableau des symboles $(\frac{a}{\mathfrak{b}})$:

	$\mathfrak{l}_7\mathfrak{l}_5\mathfrak{l}_{11}$	$\mathfrak{l}_3\bar{\mathfrak{l}}_3\mathfrak{l}_5\bar{\mathfrak{l}}_{11}$
-1	1	-1
7	-1	1
$1+\sqrt{-161}$	-1	1

D'où $a_0 = 7(1 + \sqrt{-161})$ et $\tilde{N} = k(\sqrt{2}, \sqrt{7 + 7\sqrt{-161}})$.

EXEMPLE 3: Soit $k = \mathbb{Q}(\sqrt{-l})$, l premier, $-l \equiv -7 \bmod 8$. On a $Cl = (1)$, et $2 \overline{\log \mathfrak{l}} = 2 \log U = (8) \oplus (4 + 4\sqrt{-l})$; comme $\rho = 1$, le tableau A conduit à considérer le groupe d'idéaux $\langle \mathfrak{l} = (\sqrt{-l}), (2 + \sqrt{-l}), (2 - \sqrt{-l}) \rangle$, et on obtient facilement $\mathfrak{b}_1 = \mathfrak{l}(4 + l)$ si $-l \equiv -7 \bmod 16$, $\mathfrak{b}_1 = \mathfrak{l}$ si $-l \equiv -15 \bmod 16$. On a $R' = \langle -1, x + \sqrt{-l} \rangle$ (où $-l = x^2 - 2y^2$, x impair, y pair):

(i) cas $-l \equiv -7 \bmod 16$. On a $(\frac{-1}{\mathfrak{l}(4+l)}) = (\frac{-1}{l}) = -1$.

On a $(\frac{x + \sqrt{-l}}{\mathfrak{l}}) = (\frac{x}{l})$. On a (si le symbole est défini)

$$\left(\frac{x + \sqrt{-l}}{(4 + l)}\right) = \left(\frac{x + \sqrt{-l}}{(2 + \sqrt{-l})}\right)\left(\frac{x + \sqrt{-l}}{(2 - \sqrt{-l})}\right)$$

$$= \left(\frac{x - 2}{(2 + \sqrt{-l})}\right)\left(\frac{x + 2}{(2 - \sqrt{-l})}\right) = \left(\frac{x^2 - 4}{4 + l}\right)$$

$$= \left(\frac{2y^2 - l - 4}{4 + l}\right) = \left(\frac{2y^2}{4 + l}\right) = \left(\frac{2}{4 + l}\right) = (-1)^{((4+l)^2-1)/8} = -1.$$

D'où $(\frac{x+\sqrt{-l}}{l(4+l)}) = -(\frac{x}{l})$ dans ce cas.

Si $x+\sqrt{-l}$ et $2\pm\sqrt{-l}$ ne sont pas étrangers, on vérifie qu'il suffit de modifier $2\pm\sqrt{-l}$ modulo 8 et les calculs sont identiques.

(ii) cas $-l \equiv -15 \mod 16$. On a $(\frac{-1}{l}) = (\frac{-1}{l}) = -1$ et on a $(\frac{x+\sqrt{-l}}{l}) = (\frac{x}{l})$.

En conclusion, si $k = \mathbb{Q}(\sqrt{-l})$, l premier, $l \equiv 7 \mod 8$, on a

$$a_0 = \left(\frac{-x}{l}\right)(x+\sqrt{-l}), \text{ si } -l \equiv -7 \mod 16,$$

$$a_0 = \left(\frac{x}{l}\right)(x+\sqrt{-l}), \text{ si } -l \equiv -15 \mod 16.$$

Bibliographie

[1] F. Bertrandias et J.-J. Payan: Γ-extensions et invariants cyclotomiques. *Ann. Sci. Ec. Norm. Sup.* 5 (1972) 517–543.

[2] J.E. Carroll: *On the 2-primary part of* K_2O *and on* $\mathbb{Z}_2$*-extensions for imaginary quadratic fields,* Ph. D. Harvard (1973).

[3] J.E. Carroll: On determining the quadratic subfields of $\mathbb{Z}_2$-extensions of complex quadratic fields. *Comp. Math.* 30 3 (1975) 259–271.

[4] J.E. Carroll and H. Kisilevsky: Initial layers of $\mathbb{Z}_\ell$-extensions of complex quadratic fields. *Comp. Math.* 32 2 (1976) 157–168.

[5] G. Gras: Logarithme p-adique et groupes de Galois. *Journal de Crelle* 343 (1983) 64–80.

[6] G. Gras: Sur les $\mathbb{Z}_2$-extensions d'un corps quadratique imaginaire. *Ann. Inst. Fourier* 33 4 (1983) 1–18.

[7] R. Greenberg: A note on K_2 and the theory of $\mathbb{Z}_p$-extensions. *Amer. J. Math.* 100 6 (1978) 1235–1245.

[8] K. Kramer and A. Candiotti: On K_2 and $\mathbb{Z}_\ell$-extensions of number fields. *Amer. J. Math.* 100 1 (1978) 177–196.

[9] J.-P. Serre: *Corps locaux*. Hermann (1962).

[10] J. Tate: Relations between K_2 and Galois cohomology. *Invent. Math.* 36 (1976) 257–274.

(Oblatum 19-VIII 1983)

Georges Gras
Université de Franche-Comté-Besançon
Faculté des Sciences, Mathématiques
E.R.A. au C.N.R.S. N°070654
F-25030 BESANÇON Cedex
France