BULLETIN DE LA S. M. F.

GEORGES GRAS

Extensions abéliennes non ramifiées de degré premier d'un corps quadratique

Bulletin de la S. M. F., tome 100 (1972), p. 177-193

<http://www.numdam.org/item?id=BSMF_1972__100__177_0>

Bull. Soc. math. France,
100, 1972, p. 177-193.

EXTENSIONS ABÉLIENNES NON RAMIFIÉES DE DEGRÉ PREMIER D'UN CORPS QUADRATIQUE

PAR

GEORGES GRAS

[Grenoble]

RÉSUMÉ. — Soient p un nombre premier impair, et k un corps quadratique. Une méthode de construction des extensions abéliennes non ramifiées de degré p de k est obtenue grâce à une description de ces extensions au moyen de sous-groupes convenables du groupe multiplicatif d'un corps abélien, $\tilde{k}$, de degré absolu $p-1$, canoniquement associé à k et p. Ces groupes sont explicites dès que sont connus le groupe des classes et le groupe des unités de $\tilde{k}$ (ce qui est, numériquement, le plus difficile). Un polynôme, universel pour le degré p (calculé ici pour $p = 3$ et $p = 5$) définit alors l'extension cherchée.

L'étude des groupes précédents conduit enfin à un énoncé du « Spiegelungsatz » de LEOPOLDT, pour le cas quadratique, aboutissant (pour $p = 3$) à une illustration numérique détaillée. D'autres exemples ($p = 5$) ainsi que des tables numériques sont joints.

Introduction. — Nous nous proposons de donner, pour les extensions quadratiques des rationnels, une démonstration directe du « Spiegelungsatz » de LEOPOLDT [4] qui relie, pour tout nombre premier p impair, le p-rang du groupe des classes d'idéaux d'un corps quadratique k au p-rang d'un certain groupe de classes d'idéaux d'une extension cyclique de degré $p-1$ des rationnels notée $\tilde{k}$.

Cette démonstration donne en même temps les moyens techniques permettant de rechercher systématiquement les extensions non ramifiées de degré premier impair d'un corps quadratique, donnant ainsi une solution naturelle au problème posé par HASSE et résolu notamment pour le corps $\mathbf{Q}(\sqrt{-47})$ ([2] et [3]); en particulier, nous donnons une méthode de construction d'un polynôme irréductible de degré p sur $\mathbf{Q}$ dont le corps de décomposition est l'extension cherchée du corps quadratique. La recherche d'exemples numériques est basée sur une investigation relativement simple dans le corps $\tilde{k}$ associé à k et p par le « Spiegelungsatz ».

Lorsque $p = 3$, le « Spiegelungsatz » montre que les 3-rangs du groupe des classes des corps quadratiques $\mathbf{Q}(\sqrt{m})$ et $\mathbf{Q}(\sqrt{-3m})$ sont égaux ou diffèrent d'une unité. Nous montrons que l'on peut déterminer la valeur exacte du 3-rang du groupe des classes de $\mathbf{Q}(\sqrt{-3m})$ au moyen de calculs et algorithmes faisant intervenir le corps $\mathbf{Q}(\sqrt{m})$ et uniquement ce corps : voir notamment la partie 4 consacrée à une illustration numérique en ce qui concerne le cas $p = 3$ et pour des 3-rangs inférieurs ou égaux à 2; SHANKS a tout récemment donné des exemples de corps quadratiques imaginaires pour lesquels le 3-rang est égal à 3 ([8], [9]). Nous avons, pour l'un d'entre eux, fait l'étude numérique en se plaçant du point de vue du « Spiegelungsatz ».

1. Caractérisation des extensions abéliennes non ramifiées de degré p premier impair d'un corps quadratique k

Dans toute la suite, nous notons, pour un corps K, K' le composé de K avec le corps $\mathbf{Q}'$ engendré sur $\mathbf{Q}$ par les racines p-ièmes de l'unité, et nous supposons le corps quadratique k non contenu dans $\mathbf{Q}'$.

Si N/k est une extension abélienne de degré p de k, alors N'/k' (qui est abélienne) est non ramifiée si, et seulement si, N/k est non ramifiée; lorsque ceci a lieu, on vérifie facilement que $N/\mathbf{Q}$ et $N'/\mathbf{Q}'$ sont galoisiennes et que leurs groupes de Galois sont isomorphes au groupe diédral d'ordre $2p$. Convenons de dire qu'une extension abélienne N' de k' est décomposée sur k si N'/k est abélienne et s'il existe une extension N/k (nécessairement abélienne) telle que $N' = Nk'$: il résulte de cette définition que l'ensemble $\mathcal{N}$ des extensions N abéliennes non ramifiées de degré p de k est en correspondance bijective (et canonique) avec l'ensemble $\mathcal{N}'$ des extensions N' abéliennes non ramifiées de degré p de k' qui sont décomposées sur k.

Notations. — Si N est une extension de $\mathbf{Q}$ à groupe de Galois diédral d'ordre $2p$, les groupes de Galois des extensions N'/N, k'/k et $\mathbf{Q}'/\mathbf{Q}$ sont isomorphes par restriction; nous les identifions et les notons par la lettre G. Nous identifions de même les groupes de Galois de $N'/\mathbf{Q}'$ et $N/\mathbf{Q}$, puis les groupes de Galois de $k'/\mathbf{Q}'$ et $k/\mathbf{Q}$. Désignons par s_i, i défini modulo p, $i \not\equiv 0$ modulo p, l'élément de G qui élève toute racine de l'unité à la puissance i, et par τ l'élément d'ordre 2 du groupe de Galois de $k'/\mathbf{Q}'$. Soit enfin $T = \{1, s_{-1}\tau\}$ considéré comme sous-groupe du groupe de Galois de $k'/\mathbf{Q}$.

Le théorème suivant va nous donner une caractérisation effective des ensembles $\mathcal{N}$ et $\mathcal{N}'$.

THÉORÈME 1. — *Soit k une extension quadratique de $\mathbf{Q}$ non contenue dans le corps $\mathbf{Q}'$ des racines p-ièmes de l'unité, et soit $\tilde{k}$ le sous-corps de k'*

fixe par le sous-groupe T; notons $\tilde{\Omega}$ *l'image, par l'homomorphisme canonique* $\tilde{\varkappa} : \tilde{k}^* \to \tilde{k}^*/\tilde{k}^{*p}$, *du sous-groupe (et sous-G-module) formé des éléments* α *tels que* $\alpha^{s_i} \in \alpha^i \tilde{k}^{*p}$, *pour tout* i, $i \not\equiv 0$ *modulo* p.

Les ensembles $\mathfrak{M}$ *et* $\mathfrak{M}'$ *sont en correspondance bijective (et canonique) avec l'ensemble des sous-*$\mathbf{F}_p$*-espaces vectoriels de dimension* 1 *de* $\tilde{\Omega}$ *engendrés par un élément* $\tilde{\varkappa}(\alpha)$ *tel que :*

(i) *l'idéal principal engendré par* α *dans* $\tilde{k}$ *est la puissance p-ième d'un idéal fractionnaire de* $\tilde{k}$ *premier à p;*

(ii) *pour tout idéal* $\tilde{\mathfrak{p}}$ *au-dessus de p dans* $\tilde{k}$, *il existe* $\xi \in \tilde{k}$ *tel que* $\xi^p - \alpha$ *soit de* $\tilde{\mathfrak{p}}$*-valuation supérieure ou égale à* $e + 1$, e *désignant l'indice de ramification absolu de p dans* $\tilde{k}$.

La démonstration de ce théorème résulte des remarques suivantes :

(*a*) Un critère de décomposition donné dans [7] et [5] montre qu'une extension N' diédrale de degré $2p$ de $\mathbf{Q}'$ et contenant k' est décomposée sur k si, et seulement si, elle est de la forme $N' = k'(\alpha^{1/p})$, $\alpha \in \tilde{k}^*$, α non puissance p-ième dans $\tilde{k}$ et α vérifiant les conditions de conjugaison $\alpha^{s_i} \in \alpha^i \tilde{k}^{*p}$, pour tout i, $i \not\equiv 0$ modulo p [c'est-à-dire que $\tilde{\varkappa}(\alpha)$ doit être un élément de $\tilde{\Omega}$].

(*b*) La théorie de la ramification dans les extensions de Kummer nous donne les conditions supplémentaires suivantes portant sur α : d'une part, le fait que l'idéal engendré par α dans k' est la puissance p-ième d'un idéal de k' et, d'autre part, le fait que pour tout idéal $\mathfrak{p}'$, au-dessus de p dans k', α soit congru à une puissance p-ième selon un module convenable.

(*c*) Une étude approfondie de l'extension $k'/\tilde{k}$ nous permet (en suivant ce qui est fait dans [6] pour le cas $p = 3$) de ramener les conditions exprimées au point (*b*) aux conditions (i) et (ii) du théorème (*cf.* [1], p. 16-21).

Remarque. — Les résultats de la théorie du corps de classes appliqués à l'ensemble $\mathfrak{M}$ et ceux donnés par le théorème 1 vont nous conduire à un énoncé du « Spiegelungsatz » sous une forme destinée avant tout à permettre l'illustration très complète du paragraphe 4.

2. Démonstration élémentaire du « Spiegelungsatz »

Définitions. — Soit $\tilde{\mathcal{C}}'$ (resp. $\tilde{\mathcal{C}}$) le sous-groupe de $\tilde{\Omega}$ formé des éléments $\tilde{\varkappa}(\alpha)$ vérifiant la propriété (i) [resp. les propriétés (i) et (ii) du théorème 1)].

On désigne par $\tilde{\mathcal{A}}_p$ (resp. $\mathcal{A}_p$) le groupe des classes de $\tilde{k}$ (resp. k) dont la puissance p-ième est la classe unité, et par $\tilde{\mathcal{A}}'_p$ le sous-groupe de $\tilde{\mathcal{A}}_p$ formé des éléments $\tilde{h}$ vérifiant la relation $\tilde{h}^{s^i} = \tilde{h}$ pour tout i, $i \not\equiv 0$

modulo p; on désigne par $\tilde{r}$, r, $\tilde{r}'$ les rangs respectifs des groupes $\tilde{\mathcal{A}}_p$, $\mathcal{A}_p$, $\tilde{\mathcal{A}}'_p$; on note $\tilde{\mathcal{E}}$ le sous-groupe de $\tilde{\mathcal{C}}'$ formé des éléments représentables par une unité de $\tilde{k}$. A l'élément $\tilde{\varkappa}(\alpha)$ de $\tilde{\mathcal{C}}'$, associons la classe de l'idéal $\mathfrak{N}$ dont la puissance p-ième est l'idéal (α) : on vérifie que l'on définit ainsi un homomorphisme φ de $\tilde{\mathcal{C}}'$ dans $\tilde{\mathcal{A}}'_p$. Le « Spiegelungsatz » est alors contenu dans le théorème suivant :

THÉORÈME 2. — *Les $\mathbf{F}_p$-espaces vectoriels $\mathcal{A}_p$, $\tilde{\mathcal{A}}'_p$, $\tilde{\mathcal{E}}$, $\tilde{\mathcal{C}}'$, $\tilde{\mathcal{C}}$ ont les propriétés suivantes :*

(i) *$\tilde{\mathcal{C}}$ est isomorphe à $\mathcal{A}_p$;*

(ii) *la suite $1 \to \tilde{\mathcal{E}} \to \tilde{\mathcal{C}}' \xrightarrow{\varphi} \tilde{\mathcal{A}}'_p \to 1$ est exacte;*

(iii) *$\tilde{\mathcal{E}}$ est de dimension 1 (resp. 0) lorsque $\tilde{k}$ est réel (resp. imaginaire);*

(iv) *$\tilde{\mathcal{C}}$ est un sous-espace de $\tilde{\mathcal{C}}'$ de codimension inférieure ou égale à 1.*

COROLLAIRE. — *On a la relation $\tilde{r}' = r - \dim \tilde{\mathcal{E}} + \operatorname{codim} \tilde{\mathcal{C}}$.*

La démonstration des trois premières propriétés est relativement immédiate : la première résultant de la théorie du corps de classes appliquée à k et de la correspondance décrite dans le théorème 1; la seconde résultant essentiellement des définitions, et la troisième d'une propriété générale de $\mathbf{Z}[G]$-module du groupe des unités d'une extension cyclique réelle de degré premier à p, compte tenu des relations de conjugaison caractérisant $\tilde{\Omega}$. La propriété (iv), plus délicate, résulte d'une étude locale des propriétés des nombres α tels que $\tilde{\varkappa}(\alpha) \in \tilde{\Omega}$ (pour plus de détails concernant la démonstration du théorème 2 se reporter à [1]).

A partir d'un corps k, on sait construire explicitement les extensions diédrales sur $\mathbf{Q}'$ contenant k' et décomposées sur k : le paragraphe suivant a pour objet la construction explicite (au moyen d'un polynôme irréductible « universel » pour le degré p) de l'extension N de k qui correspond à N'.

3. Construction des extensions diédrales de degré $2p$ (resp. des extensions diédrales de degré $2p$ non ramifiées sur leur sous-corps quadratique)

Soit α un élément de $\tilde{k}$ dont l'image par $\tilde{\varkappa}$ appartienne à $\tilde{\Omega}$; alors si θ est une racine du polynôme $X^p - \alpha$, on sait que l'extension $k'(\theta)$ est diédrale sur $\mathbf{Q}'$ et décomposée sur k; on note N l'extension diédrale de $\mathbf{Q}$ correspondante.

Soit $s = s_g$ un générateur de G ($g \in \mathbf{Z}$ est une racine primitive modulo p que l'on suppose choisie de telle manière que $g^{p-1} - 1$ ne soit pas divisible

par p^2). On pose $\omega = \Sigma_i\, g^{p-1-i}\, s^{i-1}$, $1 \leqq i \leqq p-1$, c'est un élément de $\mathbf{Z}[G]$.

LEMME 1. — *Le $\mathbf{F}_p[G]$-module $\tilde{\Omega}$ est l'image par $\tilde{\varkappa}$ de $\tilde{k}^{*\omega}$.*

Si $\alpha = u^\omega$, $u \in \tilde{k}^*$, on a alors $\alpha^{s-g} = u^{\omega(s-g)} = u^{s^{p-1}-g^{p-1}}$, soit $\alpha^{s-g} \in \tilde{k}^{*p}$, ce qui montre que $\tilde{\varkappa}(\alpha) \in \tilde{\Omega}$. Inversement, si $\tilde{\varkappa}(\alpha) \in \tilde{\Omega}$, $\alpha^s = \alpha^g v^p$, $v \in \tilde{k}$; on est alors conduit à la relation $\alpha^{s^{p-1}} = \alpha = \alpha^{g^{p-1}} v^{p\omega}$, soit, en posant $1 - g^{p-1} = \Lambda p$, $\alpha^{p\Lambda} = v^{p\omega}$, et puisque 1 est la seule racine p-ième de l'unité contenue dans $\tilde{k}$, $\alpha^\Lambda = v^\omega$, ce qui s'écrit $\tilde{\varkappa}(\alpha)^\Lambda = \tilde{\varkappa}(v)^\omega$, et le lemme en résulte, car p ne divise pas Λ.

LEMME 2. — *Le nombre $x = \mathrm{Tr}_{N'/N}(\theta)$ est primitif dans l'extension N/k.*

La vérification en est immédiate (*cf.* [1], p. 30).

On peut toujours supposer $\alpha = u^\omega$ entier, et alors x est racine d'un polynôme irréductible de degré p à coefficients entiers dont la connaissance équivaut à celle des nombres $A_\lambda = \mathrm{Tr}_{N/k}\, x^\lambda$, $1 \leqq \lambda \leqq p$, d'après les relations de Newton.

LEMME 3. — *Chaque nombre A_λ est une combinaison $\mathbf{Z}$-linéaire de la forme $\Sigma_\Gamma c_\Gamma \mathrm{Tr}_{\tilde{k}/\mathbf{Q}} u^\Gamma$, où les Γ sont des éléments de $\mathbf{Z}[G]$; les éléments Γ et les entiers rationnels c_Γ ne dépendent pas de u.*

On vérifie que, pour tout i, $i \not\equiv 0$ modulo p, il existe $u_i \in \tilde{k}$ tel que $\theta^{s_i} = \theta^i u_i$. Soit alors σ un générateur du groupe de Galois de N'/k'; on a successivement :

$A_\lambda = \Sigma_k x^{\lambda\sigma^k} = \Sigma_k (\Sigma_i\, \theta^{s_i\sigma^k})^\lambda = \Sigma_k (\Sigma_i\, \zeta^{ki}\, \theta^{s_i})^\lambda = \Sigma_k \Sigma_{(t)} \zeta^{k\Sigma t_j} \theta^{S(t)} = p\, \Sigma'_{(t)} \theta^{S(t)}$,

avec les conventions suivantes :

(*a*) les indices i, j et k varient respectivement de 1 à $p-1$, de 1 à λ et de 1 à p, et $S(t)$ désigne la sommation $\Sigma_j\, s^{s^{t_j}}$;

(*b*) le multi-indice $(t) = (t_1, t_2, \ldots, t_\lambda)$ parcourt $\{1, 2, \ldots, p-1\}^\lambda$;

(*c*) la sommation Σ' est étendue aux λ-uples $(t_1, \ldots, t_\lambda)$ tel que $\Sigma\, t_j \equiv 0 \bmod p$.

Soit P le sous-ensemble de $\{1, 2, \ldots, p-1\}^\lambda$ formé des λ-uples $(t_1, \ldots, t_\lambda)$ tels que $\Sigma\, t_j \equiv 0 \bmod p$; le groupe G opère sur P si l'on définit $(t_1, \ldots, t_\lambda)^{s_i} = (t'_1, \ldots, t'_\lambda)$, où t'_k est le plus petit résidu positif modulo p du nombre it_k. En désignant par $\mathfrak{T}$ une trajectoire, on peut écrire :

$$A_\lambda = p\, \Sigma_{\mathfrak{T}}\, \Sigma_{(t)\in\mathfrak{T}}\, \theta^{S(t)}$$

et, après avoir vérifié que chaque trajectoire comporte $p-1$ éléments, on obtient

$$A_\lambda = p\, \Sigma_{\mathfrak{T}}\, \mathrm{Tr}_{N'/N}\, \theta^{S(t)}$$

où $(t_1, \ldots, t_\lambda)$ désigne un élément quelconque de $\mathfrak{T}$. En écrivant que $\theta^{s_{t_j}} = \theta^{t_j} u_{t_j}$, $u_{t_j} \in \tilde{k}$, et compte tenu du fait que $\theta^p = u^\omega$, on obtient

$$(\theta^{S(t)})^p = \alpha^{S(t)} = u^{\omega S(t)},$$

or $\omega\, s_{t_j}$ est de la forme $\omega\, t_j + \mu_j\, p$, $\mu_j \in \mathbf{Z}$, ce qui fait que $\omega\, S(t)$ se met sous la forme $\omega \Sigma\, t_j + \mu\, p$, $\mu \in \mathbf{Z}$; on peut noter cette quantité $p\, \Gamma_{\mathfrak{T}}$: elle ne dépend ni de u ni de l'élément $(t_1, \ldots, t_\lambda)$ choisi dans $\mathfrak{T}$. On démontre ainsi que A_λ est de la forme

$$p\, \Sigma_{\mathfrak{T}}\, \mathrm{Tr}_{N'/N}\left(u^{\Gamma_{\mathfrak{T}}}\right) = p\, \Sigma_{\mathfrak{T}}\, \mathrm{Tr}_{\tilde{k}/\mathbf{Q}}\left(u^{\Gamma_{\mathfrak{T}}}\right).$$

Il est clair que cette démonstration donne en même temps l'algorithme très simple permettant de trouver les quantités $\Gamma_{\mathfrak{T}}$; en particulier, pour $p = 3$ et $\omega = 2 + s$, $s = s_2$, on obtient le polynôme

$$X^3 - 3\, u^{1+s}\, X - u^{1+s}\, \mathrm{Tr}\,(u);$$

pour $p = 5$, et $\omega = s^3 + 2\, s^2 - s + 3$, $s = s_2$, on obtient le polynôme

$$X^5 - \frac{5}{2}\,\mathrm{Tr}\,(u^{1+s^2})\, X^3 - 5\,\mathrm{Tr}\,(u^{1+s+s^3})\, X^2$$
$$- 5\left(\mathrm{Tr}\,(u^{2+s^2+s^3}) - \frac{1}{2}\,\mathrm{Tr}\,(u^{2+2s^2}) + n\right) X$$
$$- n\left(\mathrm{Tr}\,(u^{s^2-2s+2}) + 20\,\mathrm{Tr}\,(u^{s^2-s+1}) + 30\,\mathrm{Tr}\,(u) - \frac{25}{2}\,\mathrm{Tr}\,(u^{-1})\,\mathrm{Tr}\,(u^{1+s^2})\right),$$

où $n = N_{\tilde{k}/\mathbf{Q}}(u)$, et où Tr désigne la trace $\mathrm{Tr}_{\tilde{k}/\mathbf{Q}}$.

N'importe quel u de $\tilde{k}$ tel que u^ω ne soit pas une puissance p-ième conduit, au moyen du polynôme précédent, à une extension diédrale de degré $2\,p$ [et à une extension diédrale non ramifiée sur le corps k si $\alpha = u^\omega$ est tel que $\tilde{\varkappa}(\alpha) \in \tilde{\mathcal{C}}$]; le critère suivant permet de reconnaître très simplement si la condition $u^\omega \notin \tilde{k}^{*p}$ est réalisée ou non.

Critère. — *Soit $u \in \tilde{k}^*$; une condition nécessaire et suffisante pour que le polynôme, obtenu à partir d'une racine du polynôme $X^p - \alpha$, $\alpha = u^\omega$, ait pour corps de décomposition une extension diédrale de degré $2\,p$, est qu'il n'admette pas de racines rationnelles.*

Il faut donc montrer que si u^ω est de la forme β^p, $\beta \in \tilde{k}$, le polynôme obtenu à partir de u a une racine rationnelle :

On se place dans la k'-algèbre $\overline{N}' = k'[X]/(X^p - \beta^p)$ notée $k'[\overline{X}]$. Définissons par analogie $\overline{X}^\sigma = \zeta\, \overline{X}$; alors $\{1, \sigma, \ldots, \sigma^{p-1}\}$ est un groupe de k'-automorphismes de $\overline{N}'$. De même, si on définit $\overline{X}^{s_i} = \overline{X}^i\, u_i$, $i = 1, \ldots, p-1$, on vérifie que l'on obtient un groupe de k-automor-

phismes de $\overline{N}'$ (bien entendu la restriction à k' de s_i coïncide avec le k-automorphisme de k' désigné par la même notation). Soit $\overline{N}$ le sous-anneau de $\overline{N}'$ fixe par le groupe des s_i, $i = 1, \ldots, p-1$; $\overline{N}$ est une k-algèbre. On a l'isomorphisme de k'-algèbres

$$k'[X]/(X^p - \beta^p) \simeq \Pi_{k=1}^{k=p} k'[X]/(X - \zeta^k \beta) \simeq (k')^p$$

(en effet, k' est de caractéristique nulle); dans cet isomorphisme, en désignant par $\bar{\gamma} = (\gamma_1, \ldots, \gamma_p)$ un élément de $\overline{N}'$, le conjugué $\bar{\gamma}^{s_i}$ est de la forme $(\gamma_1^{s_i}, \ldots, \gamma_p^{s_i})$ et par conséquent la k-algèbre $\overline{N}$ est isomorphe au produit de p copies de k.

Définissons $\bar{x} = \Sigma_i \overline{X}^{s_i} \in \overline{N}$, $1 \leq i \leq p-1$; alors en désignant par q_l la projection canonique de $\overline{N}$ sur le l-ième facteur, on obtient

$$q_l(\bar{x}) = \Sigma_{i=1}^{p-1} \zeta^{li} \beta^i u_i = \mathrm{Tr}_{k'/k}(\zeta^l \beta);$$

par conséquent, puisque $\bar{x}$ est racine du polynôme de $\mathbf{Q}[X]$, $X^p + a_{p-1} X^{p-1} + \ldots + a_1 X + a_0$, $q_0(\bar{x})$ est un rationnel racine de ce polynôme et les quantités $q_l(\bar{x})$, $l = 1, \ldots, p-1$, sont des racines conjuguées dans k (ou des racines multiples rationnelles).

4. Étude détaillée du cas $p = 3$ pour $r \leq 2$

Si $k = \mathbf{Q}(\sqrt{m})$, $m \in \mathbf{Z}$ sans facteurs carrés, on vérifie que $\tilde{k} = \mathbf{Q}(\sqrt{\tilde{m}})$ avec $\tilde{m} = -(m/3)$ ou $-3m$ selon que 3 divise m ou non. Le groupe $\tilde{\mathcal{C}}'_3$ est alors identique au groupe $\tilde{\mathcal{C}}_3$ et, si $\alpha \in \tilde{k}^*$, alors $\tilde{\varkappa}(\alpha) \in \tilde{\Omega}$ si, et seulement si, $N_{\tilde{k}/\mathbf{Q}}(\alpha)$ est le cube d'un rationnel.

Il y a, lorsque r est égal à 1 ou 2, 9 types d'exemples possibles : les calculs explicités ci-après montrent que ces 9 cas se rencontrent effectivement.

Cas		k	m	$\tilde{m}$	$\tilde{r}$	h	$\tilde{h}$
(i)	$\tilde{\mathcal{C}} = \tilde{\mathcal{E}}$	Imaginaire	— 23	69	0	3	1
(ii)	$\tilde{\varkappa}(\tilde{\varepsilon}) \in \tilde{\mathcal{C}}$	»	— 237	79	1	12	3
(iii)	$\tilde{\varkappa}(\tilde{\varepsilon}) \notin \tilde{\mathcal{C}}$	»	— 687	229	1	12	3
(iv)	$\tilde{\varkappa}(\tilde{\varepsilon}) \in \tilde{\mathcal{C}}$	»	— 4027	12081	1	9	3
(v)	$\varkappa(\tilde{\varepsilon}) \in \tilde{\mathcal{C}}$	»	—298483	895449	2	81	27
(vi)	$\tilde{\varkappa}(\tilde{\varepsilon}) \notin \tilde{\mathcal{C}}$	»	— 34603	103809	2	27	9
(vii)	$\tilde{\mathcal{C}}' = \tilde{\mathcal{C}}$	Réel	79	— 237	1	3	12
(viii)	$\tilde{\mathcal{C}}' \neq \tilde{\mathcal{C}}$	»	12081	— 4027	2	3	9
(ix)	$\tilde{\mathcal{C}}' = \tilde{\mathcal{C}}$	»	103809	— 34603	2	9	27

Le tableau ci-avant décrit le cas considéré et regroupe les différentes données numériques utiles : $\tilde{r}$ désigne le 3-rang du groupe $\tilde{\mathcal{C}}_3$, h et $\tilde{h}$ sont les nombres de classes respectifs de k et $\tilde{k}$, et $\tilde{\varepsilon}$ est, lorsque $\tilde{k}$ est réel, l'unité fondamentale de $\tilde{k}$.

Remarques.

(*a*) Nous avons volontairement omis de rechercher, au moyen des algorithmes de Châtelet, la valeur de r, car celle-ci se déduit systématiquement de l'étude numérique faite (et qui concerne uniquement le corps $\tilde{k}$) compte tenu des relations suivantes (corollaire au théorème 2) :

(i) Si k est imaginaire, alors

$$\dim \tilde{\mathcal{C}} = r \qquad \text{et} \qquad \dim \tilde{\mathcal{C}}' = \tilde{r} + 1;$$

(ii) si k est réel, alors

$$\dim \tilde{\mathcal{C}} = r \qquad \text{et} \qquad \dim \tilde{\mathcal{C}}' = \tilde{r}.$$

Autrement dit, on est ramené à l'évaluation de la codimension de $\tilde{\mathcal{C}}$ dans $\tilde{\mathcal{C}}'$.

(*b*) Certains calculs non triviaux ne peuvent être justifiés ici : ce sont notamment :

(i) la recherche de l'unité fondamentale d'un corps quadratique réel basée sur le développement en fraction continue de $\sqrt{\tilde{m}}$;

(ii) la recherche d'un représentant des classes d'idéaux d'ordre 3 qui utilise les algorithmes de A. CHATELET.

Ces calculs nécessitent l'emploi d'un ordinateur.

1° *Étude du cas* (i) : $(\dim \tilde{\mathcal{C}}' = 1$ *et* $r = 0$ *ou* $1)$.

On vérifie que $\tilde{\varepsilon} = (25 + 3\sqrt{69})/2$ est congrue à -1 modulo $3\sqrt{69}$; un polynôme définissant l'extension non ramifiée de degré 3 de k sera $X^3 - 3X - 25$, ou encore, avec $Y = 3/(X - 1)$, le polynôme $Y^3 - Y - 1$ de discriminant 23 (ici on a $\mathbf{r} = \mathbf{1}$).

2° *Étude du cas* (ii) : $(\dim \tilde{\mathcal{C}}' = 2$ *et* $r = 1$ *ou* $2)$.

L'unité fondamentale de $\tilde{k}$ est $\tilde{\varepsilon} = 80 + 9\sqrt{79}$, congrue à -1 modulo 9. Le nombre $\alpha = 21 + 2\sqrt{79}$ est de norme 5^3; on vérifie que α est le cube d'un idéal non principal. Comme α ne vérifie pas les congruences, la codimension est égale à 1, et $\mathbf{r} = \mathbf{1}$ (un polynôme est alors $X^3 + X^2 - 6$, de discriminant 12.79).

3° *Étude du cas* (iii) : $(\dim \tilde{\mathcal{C}}' = 2$ *et* $r = 1$ *ou* $2)$.

L'unité fondamentale de $\tilde{k}$ est $\tilde{\varepsilon} = (15 + \sqrt{229})/2$ non congrue à un cube. Le nombre $\alpha = (27 + \sqrt{229})/2$ est de norme 5^3 et vérifie $\alpha \equiv \sqrt{229}/2 \equiv (\sqrt{229}/2)^3 \bmod 9$. On vérifie que les idéaux au-dessus de 5 ne sont pas principaux, et ainsi α définit l'extension non ramifiée de k par le polynôme $X^3 - 15X - 27$ (de discriminant $3^3.687$) (on a encore $\mathbf{r} = \mathbf{1}$, mais les rôles de $\tilde{\varepsilon}$ et α sont échangés).

4° *Étude du cas* (iv) : $(\dim \tilde{\mathcal{C}}' = 2$ *et* $r = 1$ *ou* $2)$.

On a $\tilde{\varepsilon} = 49813142553178097815 + 453202710584702148\sqrt{12081}$ qui est congrue à -1 modulo 9; le nombre $\alpha = (8903 + 81\sqrt{12081})/2$ est de norme -8. On vérifie que les idéaux premiers au-dessus de 2 ne sont pas principaux; on a alors $\alpha \equiv 1$ modulo 9. Le corps k possède 4 extensions non ramifiées qui sont définies par exemple par les nombres $\tilde{\varepsilon}$, α, $\tilde{\varepsilon}\alpha$, $\tilde{\varepsilon}\alpha^2$. Celle relative à α est définie par le polynôme $X^3 + 6X + 8903$ ou encore par le polynôme $X^3 + X^2 + X + 330$.

On démontre ainsi que $\mathbf{r} = \mathbf{2}$.

5° *Étude du cas* (v) : $(\dim \tilde{\mathcal{C}}' = 3$ *et* $r = 2$ *ou* $3)$.

On a $\tilde{\varepsilon} = 712726108162445683586086855255 + 75318600196040417716\,9254276\sqrt{\tilde{m}}$, et on vérifie que $\tilde{\varkappa}(\tilde{\varepsilon}) \in \tilde{\mathcal{C}}$; le nombre $\alpha = 975590550\,1954 + 10309726803\sqrt{\tilde{m}}$ est le cube d'un idéal non principal de norme 5 (la norme de α est -5^3) et $\tilde{\varkappa}(\alpha) \in \tilde{\mathcal{C}}$. Il est plus rapide ici d'étudier le corps k : on obtient les nombres $\alpha_1 = (1/2)(545 + \sqrt{m})$ de norme 53^3, $\alpha_2 = (1/2)(5251 + \sqrt{m})$ de norme 191^3, $\alpha_3 = (1/2)(5503 + \sqrt{m})$ de norme 197^3, $\alpha_4 = 666 + 7\sqrt{m}$ de norme $(13 \times 19)^3$. On vérifie que $\varkappa(\alpha_1)$ et $\varkappa(\alpha_2)$ forment une base de $\mathcal{C} = \mathcal{C}'$ et que, par conséquent, $\mathbf{r} = \mathbf{2}$.

Si l'on désire démontrer que $r = 2$ en n'utilisant que des données numériques dans $\tilde{k}$, il faut trouver un nombre β dont la norme soit un cube et qui ne vérifie pas les congruences requises (on aura ainsi $\operatorname{codim} \tilde{\mathcal{C}} = 1$).

6° *Étude du cas* (vi) : $(\dim \tilde{\mathcal{C}}' = 3$ *et* $r = 2$ *ou* $3)$.

On a ici $\tilde{\varepsilon} = 3149462358295 + 9775048444\sqrt{\tilde{m}}$; les nombres

$$\alpha = 322 + \sqrt{\tilde{m}} \qquad \text{et} \qquad \beta = (1/2)(21587 + 67\sqrt{\tilde{m}})$$

sont de normes respectives -5^3 et -8; aucun des nombres $\tilde{\varepsilon}$, α, β ne vérifie les congruences requises et la codimension est égale à 1 (soit $\mathbf{r} = \mathbf{2}$). On vérifie que $\tilde{\varkappa}(\alpha\beta)$ et $\tilde{\varkappa}(\beta\tilde{\varepsilon})$ forment une base de $\tilde{\mathcal{C}}$.

7° *Étude du cas* (vii) : (dim $\tilde{\mathcal{C}}' = 1$ *et* $r = 0$ *ou* 1).

Le nombre $\alpha = 8 + 3\sqrt{-237}$ est de norme 13^3, et α est le cube d'un idéal non principal et vérifie $\alpha \equiv -1$ modulo $3\sqrt{-237}$; ainsi la codimension est nulle et $\mathbf{r = 1}$. Un polynôme définissant l'unique extension non ramifiée de k est $X^3 + X^2 - 4X - 2$.

8° *Étude du cas* (viii) : (dim $\tilde{\mathcal{C}}' = 2$ *et* $r = 1$ *ou* 2).

Considérons les nombres :

$$\alpha_1 = \frac{69 + \sqrt{-4027}}{2} \quad \text{de norme } 13^3;$$

$$\alpha_2 = \frac{125 + \sqrt{-4027}}{2} \quad \text{de norme } 17^3;$$

$$\alpha_3 = \frac{153 + \sqrt{-4027}}{2} \quad \text{de norme } 19^3;$$

$$\alpha_4 = 91 + 2\sqrt{-4027} \quad \text{de norme } 29^3;$$

on vérifie alors que $\tilde{\varkappa}(\alpha_1)$ et $\tilde{\varkappa}(\alpha_3)$ forment une base de $\tilde{\mathcal{C}}'$ et que $\tilde{\varkappa}(\alpha_1)$ n'est pas dans $\tilde{\mathcal{C}}$. Par conséquent, $\tilde{\mathcal{C}}$ est engendré par $\tilde{\varkappa}(\alpha_3)$ et dim $\tilde{\mathcal{C}} = 1$, d'où $\mathbf{r = 1}$. L'unique extension non ramifiée de degré 3 de k est alors définie par le polynôme $X^3 - 57X - 153$ (de discriminant 27.4027).

9° *Étude du cas* (ix) : (dim $\tilde{\mathcal{C}}' = 2$ *et* $r = 1$ *ou* 2).

Considérons les nombres :

$$\alpha_1 = \frac{491 + \sqrt{-34603}}{2} \quad \text{de norme } 41^3;$$

$$\alpha_2 = \frac{617 + \sqrt{-34603}}{2} \quad \text{de norme } 47^3;$$

$$\alpha_3 = \frac{207 + \sqrt{-34603}}{2} \quad \text{de norme } 61^3;$$

$$\alpha_4 = 389 + 4\sqrt{-34603} \quad \text{de norme } 89^3;$$

$$\alpha_1 \equiv \frac{5 + \sqrt{-34603}}{2} \equiv \left(\frac{5 - \sqrt{-34603}}{2}\right)^3 \bmod 9;$$

$$\alpha_2 \equiv \alpha_1 \bmod 9;$$

$$\alpha_3 \equiv -2\sqrt{-34603} \equiv (2\sqrt{-34603})^3 \bmod 9;$$

$$\alpha_4 \equiv 2 + 4\sqrt{-34603} \equiv (2 - 4\sqrt{-34603})^3 \bmod 9,$$

Par conséquent, $\mathbf{r = \dim \tilde{\mathcal{C}} = 2}$; on aura facilement dans ce cas les 4 extensions non ramifiées de degré 3 de k. Prenons $\tilde{\varkappa}(\alpha_1)$ et $\tilde{\varkappa}(\alpha_2)$ comme base de $\tilde{\mathcal{C}}$: le nombre $\alpha_1 \alpha_2^s \alpha_3$ est le cube de $288 + \sqrt{-34603}$ tandis

que $\alpha_1\,\alpha_2\,\alpha_4$ est le cube de $370 + \sqrt{-34603}$; par suite,

$$\tilde{\chi}(\alpha_3) = \tilde{\chi}(\alpha_1)^2\,\tilde{\chi}(\alpha_2) \qquad \text{et} \qquad \tilde{\chi}(\alpha_4) = \tilde{\chi}(\alpha_1)^2\,\tilde{\chi}(\alpha_2)^2.$$

Avec α_1, on obtient le polynôme $X^3 - 123\,X - 491$; avec α_2, on obtient $X^3 - 141\,X - 617$; avec α_3, on obtient $X^3 - 183\,X - 207$, et enfin $X^3 - 267\,X - 778$ avec α_4.

Le discriminant de $X^3 - 123\,X - 491$ est égal à 27.34603,
» $X^3 - 141\,X - 617$ » » 27.34603,
» $X^3 - 183\,X - 207$ » » $27.5^2.34603$,
» $X^3 - 267\,X - 778$ » » $27.2^6.34603$.

SHANKS ([8] et [9]) a récemment trouvé des corps quadratiques imaginaires ayant un 3-rang égal à 3. Il s'agit notamment des nombres m suivants : -63199139, -138603587, -80059613, -390949805, -795990917, -566717033, -315524687.

Étude du cas $m = -63199139$.

On a $\tilde{m} = 189597417$; d'après SHANKS, on a $h = 27 \times 116$, $\tilde{h} = 18$, $r = 3$ et $\tilde{r} = 2$.

Dans le corps $\tilde{k}$, nous trouvons les nombres suivants :

$$\alpha = 47940482125686330958748469733691145398478214648304429948865827173678051261370839191988380 20 + 3481658646016985875162924243000341970452525403849114161232272479072084789313717895281 33\sqrt{\tilde{m}}$$

qui est de norme 17^3,

$$\beta = \frac{1}{2}(12668293941264965627701795034481316687537534002515107085756570381053294714145667751746646135313293 + 9200298615115006175392300143196127938542531112888439030172321889475360142412932346983791337 27\sqrt{\tilde{m}}).$$

qui est de norme 4^3, et l'unité fondamentale

$$\tilde{\varepsilon} = 98196737988131155361495412178603192682063829336643518580683976573580491993034807620757801993721418477148986746484563007257784443611021587382961220830495102436507592046934590192992953367044261853778981770920859265902409872167116162987964964395546718369078068719376069900778216982833231948727115497087385936262384187385863832291689023510336163145860952440485555892339980 47 + 71314994482264371079388075786338715674635221971$$

$$06763672033894589955892411069846394251261512316859889709837134349691921729983705200930372590982495376370576266304346434433470358328668584390558998490548447990265479902127089824028014865382281799543227679883866107597767459111557880839953010967601699469577185189329346277881930009651052460024081099517174358587592799703432\sqrt{\tilde{m}}.$$

Ces trois nombres vérifient les congruences requises et permettent d'obtenir les 13 extensions non ramifiées de degré 3 de K.

5. Illustration du cas $p = 5$ et k imaginaire

Les calculs sont encore bien plus complexes, car $\tilde{k}$ est de degré 4 sur $\mathbf{Q}$, et la recherche d'une unité dans $\tilde{k}$ est très difficile.

(*a*) *Étude de* $k = \mathbf{Q}(\sqrt{-79})$.

On aura $\tilde{k} = \mathbf{Q}(\sqrt{79(\omega+3)})$ avec $\omega = (\sqrt{5}-1)/2$; on vérifie que

$$\tilde{\varepsilon} = \frac{87 + 95\,\omega + (8+\omega)\sqrt{79(\omega+3)}}{2}$$

est une unité de $\tilde{k}$ de norme relative à $\mathbf{Q}(\sqrt{5})$ égale à 1.

Ici $\tilde{\varepsilon}^{\omega} = \tilde{\varepsilon}^{s^3+2s^2-s+3} = \tilde{\varepsilon}^{1-2s}$ et $\tilde{\varkappa}(\tilde{\varepsilon}^{1-2s}) \in \tilde{\mathcal{E}}$. On obtient

$$\tilde{\varepsilon}^{1-2s} = \frac{468952 + 290025\,\omega + (27735 + 17160\,\omega)\sqrt{79(\omega+3)}}{2}.$$

On trouve alors le polynôme suivant :

$$X^5 - 10\,X^3 - 5.79\,X^2 + 5.9722\,X - 647879$$

qui conduit, en prenant $Y = (X+1)/5$, au polynôme

$$Y^5 - Y^4 - 3\,Y^2 + 79\,Y - 223.$$

On vérifie aisément que ce polynôme n'admet pas de racines rationnelles, ce qui prouve que $\tilde{\varepsilon}^{1-2s}$ n'est pas une puissance 5-ième (en vertu du critère du paragraphe 3) : on obtient donc le corps de classes absolu de $\mathbf{Q}(\sqrt{-79})$.

(*b*) *Étude de* $\mathbf{Q}(\sqrt{-47})$ (Hasse).

Le polynôme trouvé par Hasse est

$$\text{(H)} \quad X^5 - 2\,X^4 + 2\,X^3 - 3\,X^2 + 6\,X - 5;$$

avant lui, WEBER donnait, grâce à la théorie des fonctions modulaires, le polynôme

$$\text{(W)} \quad X^5 - X^3 - 2X^2 - 2X - 1,$$

tandis que FRICKE donnait le polynôme

$$\text{(F)} \quad X^5 - X^4 + X^3 + X^2 - 2X + 1.$$

A partir de l'unité

$$\tilde{\varepsilon} = \frac{1}{2}\left(\frac{47 - 5\sqrt{5}}{2} - \sqrt{5}\sqrt{47\frac{5 - \sqrt{5}}{2}}\right),$$

nous obtenons le polynôme $X^5 + 3X^4 + 4X^3 + X^2 + 3X - 1$ qui conduit immédiatement au polynôme de Hasse en remplaçant X par $X - 1$.

Remarque. — Dans [3], HASSE donne le lien qui existe entre les racines des trois polynômes : il existe un choix convenable des racines w, f, h des polynomes (W), (F), (H) tel que :

$$h = w^2 - w, \qquad w = -f^4 - 2f + 1.$$

Nous trouvons les relations suivantes :

$$f = -\frac{1}{11}(h^4 + h^3 + 5h^2 + h - 2),$$

$$w = \frac{1}{11}(6h^4 - 5h^3 + 8h^2 - 16h + 21),$$

qui n'ont pas été indiquées par HASSE.

LISTE DES DISCRIMINANTS INFÉRIEURS A 2300
DES CORPS QUADRATIQUES RÉELS
DONT L'UNITÉ FONDAMENTALE EST 3-PRIMAIRE

29	69	77	85	93	109	113
137	172	173	177	181	232	248
249	253	257	268	281	296	312
316	321	328	332	337	348	353
397	401	412	417	424	449	456
457	461	488	497	505	521	524
533	556	581	597	604	633	636
653	716	717	728	732	733	741
745	773	796	808	824	849	865
877	921	929	952	953	965	988
993	997	1004	1005	1009	1013	1068
1084	1117	1137	1148	1153	1157	1165

1180	1181	1205	1213	1217	1237	1240
1241	1249	1256	1261	1272	1277	1288
1292	1293	1297	1304	1308	1317	1320
1324	1333	1353	1385	1388	1397	1416
1429	1433	1436	1453	1473	1477	1497
1501	1529	1541	1544	1545	1564	1581
1585	1609	1624	1640	1641	1645	1649
1669	1672	1685	1689	1724	1745	1753
1769	1781	1793	1816	1841	1865	1884
1897	1901	1916	1921	1945	1965	1973
1976	1993	2005	2008	2013	2021	2024
2029	2037	2040	2044	2045	2060	2072
2085	2121	2129	2137	2149	2153	2161
2184	2185	2193	2201	2221	2229	2233
2252	2253	2265	2281	2284	2285	

Exemples de corps quadratiques $\tilde{k}$ imaginaires pour lesquels le 3-rang du groupe des classes est égal a 2

Le discriminant d est premier et congru à 1 modulo 4; on indique alors l'ordre du groupe des classes et, dans la première partie de la table, les nombres 3-primaires permettant de définir les extensions abéliennes non ramifiées de degré 3 de $k = \mathbf{Q}(\sqrt{-3d})$ (un seul nombre si $\dim \tilde{\mathcal{C}} = 1$, deux nombres si $\dim \tilde{\mathcal{C}} = 2$). La dernière colonne donne l'entier dont le cube est la norme de l'entier 3-primaire.

Dans la seconde partie, on indique le discriminant d et, entre parenthèses, le nombre de classes de $\mathbf{Q}(\sqrt{d})$.

Première partie

Discriminant d	Nombre de classes	Entiers 3-primaires	Normes
— 3 299	27	$1/2(45 + \sqrt{d})$	11
— 4 027	9	$1/2(153 + \sqrt{d})$	19
— 19 427	27	$1/2(171 + \sqrt{d})$	23
— 34 603	27	$1/2(491 + \sqrt{d})$, $1/2(617 + \sqrt{d})$	41, 47
— 64 067	81	$1/2(729 + \sqrt{d})$	53
— 65 203	45	$1/2(1327 + \sqrt{d})$	77
— 89 923	27	$1/2(171 + \sqrt{d})$	31
— 90 163	45	$1/2(873 + 7\sqrt{d})$	109
— 96 827	99	$1/2(27 + \sqrt{d})$	29
— 98 347	45	$74 + \sqrt{d}$	47
— 98 443	27	$1/2(599 + 5\sqrt{d})$	89

— 99 707	117	$1/2\,(952839 + 3995\sqrt{d})$	8549
—103 567	117	$16 + \sqrt{d}$	47
—104 107	45	$288 + 5\sqrt{d}$	139
—104 659	45	$947 + 4\sqrt{d}$	137
—106 663	99	$682 + \sqrt{d}$	83
—110 059	81	$1/2\,(1811 + 9\sqrt{d})$	145
—114 043	45	$1/2\,(\ 891 + \sqrt{d})$	61
—117 043	63	$1/2\,(\ 297 + 5\sqrt{d})$	91
—117 203	63	$1/2\,(2187 + \sqrt{d})$	107
—124 363	45	$1/2\,(\ 657 + 11\sqrt{d})$	157
—124 771	99	$1/2\,(\ 279 + \sqrt{d})$	37
—130 523	117	$12834 + 509\sqrt{d}$	3239
—134 059	81	$1/2\,(\ 729 + \sqrt{d})$	55
—135 059	117	$1/2\,(1467 + \sqrt{d})$	83
—136 139	135	$1/2\,(\ 981 + \sqrt{d})$	65
—137 587	45	$569 + 8\sqrt{d}$	209
—160 403	117	$1/2\,(1577 + 9\sqrt{d})$	157
—163 411	99	$1/2\,(\ 967 + \sqrt{d})$	65
—165 523	45	$1/2\,(2263 + 7\sqrt{d})$	149
—170 267	117	$1/2\,(\ 495 + \sqrt{d})$	47
—176 899	63	$1/2\,(\ 855 + \sqrt{d})$	61
—179 483	117	$135568 + 441\sqrt{d}$	3763
—187 547	117	$1/2\,(1449 + \sqrt{d})$	83
—190 387	45	$1/2\,(1379 + 9\sqrt{d})$	163
—202 243	63	$56 + \sqrt{d}$	59
—202 387	81	$1/2\,(\ 607 + 7\sqrt{d})$	137
—218 363	153	$1/2\,(1057043 + 2565\sqrt{d})$	8611
—222 043	81	$1/2\,(3681 + \sqrt{d})$	151
—222 883	63	$1/2\,(4777 + 9\sqrt{d})$	217

Deuxième partie

—264 659 (279)	—266 491 (81)	—267 403 (63)
—272 659 (99)	—290 539 (99)	—290 803 (81)
—298 483 (81)	—324 319 (297)	—332 947 (135)
—341 851 (135)	—346 259 (225)	—349 183 (243)
—356 467 (81)	—376 483 (99)	—379 571 (243)
—384 547 (63)	—392 099 (171)	—396 523 (81)
—405 491 (189)	—426 931 (135)	—430 411 (81)
—464 467 (99)	—469 283 (243)	—486 139 (153)
—498 787 (81)	—511 627 (99)	—513 899 (189)

Deuxième partie (suite)

—519 611 (225)	—520 963 (99)	—542 323 (81)
—552 659 (351)	—553 171 (153)	—559 747 (81)
—568 187 (153)	—570 859 (135)	—587 659 (135)
—592 483 (99)	—593 987 (171)	—607 843 (117)
—612 643 (117)	—632 299 (189)	—640 267 (117)
—644 107 (99)	—664 771 (135)	—672 379 (99)
—687 923 (207)	—695 059 (171)	—757 507 (99)
—758 851 (117)	—782 707 (117)	—790 043 (171)
—803 027 (261)	—805 451 (477)	—812 443 (99)
—814 939 (189)	—872 107 (99)	—879 283 (117)
—879 299 (279)	—914 971 (135)	—931 123 (117)
—949 243 (135)	—955 139 (459)	—967 627 (189)
—991 603 (117)		

Structure de la 3-composante lorsque 81 divise le nombre de classes h et que le 3-rang est égal a 2

Cette table traite tous les corps quadratiques imaginaires considérés dans les tables précédentes. Dans les colonnes 4 et 6 figurent deux idéaux (premiers) dont les classes sont génératrices de la 3-composante [nous en avons donné une **Z**-base de la forme $(n, \theta - c)$, où n est la norme de l'idéal et $\theta = (\overline{1} + \sqrt{d})/2$].

Discriminant d	h	Structure	Générateur 1	Ordre	Générateur 2	Ordre
— 64 067	81	(3,27)	(29, θ — 4)	3	(3, θ)	27
—110 059	81	(3,27)	(67, θ — 12)	3	(5, θ)	27
—134 059	81	(9, 9)	(5, θ)	9	(13, θ — 3)	9
—202 387	81	(3,27)	(37, θ — 7)	3	(7, θ — 2)	27
—222 043	81	(3,27)	(73, θ — 6)	3	(7. θ — 2)	27
—266 491	81	(3,27)	(59, θ — 18)	3	(13, θ — 1)	27
—290 803	81	(3,27)	(43, θ — 3)	3	(23, θ — 1)	27
—298 483	81	(9,9)	(7, θ — 2)	9	(13, θ — 3)	9
—349 183	243	(3,81)	(151, θ — 34)	3	(2, θ)	81
—356 467	81	(3,27)	(71, θ — 16)	3	(29, θ)	27
—379 571	243	(3,81)	(149, θ — 4)	3	(3, θ)	81
—396 523	81	(3,27)	(47, θ — 21)	3	(13, θ — 4)	27
—430 411	81	(9,9)	(5, θ — 1)	9	(37, θ — 5)	9
—469 283	243	(3,81)	(71, θ — 6)	3	(7, θ — 2)	81
—498 787	81	(3,27)	(53, θ — 3)	3	(13, θ — 3)	27
—542 323	81	(3,27)	(109, θ — 18)	3	(7, θ — 1)	27
—559 747	81	(3,27)	(151, θ — 18)	3	(7, θ)	27

BIBLIOGRAPHIE

[1] GRAS (G.). — *Extensions abéliennes non ramifiées de degré premier d'un corps quadratique*, Thèse 3e cycle, Grenoble, 1970.

[2] HASSE (H.). — Ueber den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante-47, *Acta Arith.*, Warszawa, t. 9, 1964, p. 419-434.

[3] HASSE (H.) und LIANG (J.). — Ueber den Klassenkorper zum quadratischen Zahlkörper mit der Diskriminante-47 (Fortsetzung), *Acta Arith.*, Warszawa, t. 16, 1969, p. 89-97.

[4] LEOPOLDT (H. W.). — Zur Struktur der *l*-Klassengruppe galoisscher Zahlkörper, *J. für reine und angew. Math.*, t. 199, 1958, p. 165-174.

[5] MARTINET (J.). — Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2 *p*, *Ann. Inst. Fourier*, Grenoble, t. 19, 1969, fasc. 1, p. 1-80 (Thèse Sc. math., Grenoble, 1968).

[6] MARTINET (J.) und PAYAN (J. J.). — Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne. *J. für reine und angew. Math.*, t. 228, 1967, p. 15-37.

[7] PAYAN (J. J.). — Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base, *Ann. scient. Éc. Norm. Sup.*, 4e série, t. 1, 1968, p. 445-458.

[8] SHANKS (D.) and WEINBERGER (P.). — A quadratic field of prime discriminant requiring three generators for its class group, and related theory, *J. of number Theory* (à paraître).

[9] SHANKS (D.). — New types of quadratic fields having three invariants divisible by 3, *J. of number Theory* (à paraître).

(Texte reçu le 25 août 1971.)

Georges GRAS,
Institut de Mathématiques pures,
Boîte postale 116,
38-Saint-Martin-d'Hères.