Annales de l'institut Fourier

Bernard Oriat

Relations entre les 2-groupes de classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$

Annales de l'institut Fourier, tome 27, nº 2 (1977), p. 37-59
<http://www.numdam.org/item?id=AIF_1977__27_2_37_0>

Ann. Inst. Fourier, Grenoble
27, 2 (1977), 37-59.

RELATIONS ENTRE LES 2-GROUPES DES CLASSES D'IDÉAUX DES EXTENSIONS QUADRATIQUES $k(\sqrt{d})$ ET $k(\sqrt{-d})$

par Bernard ORIAT

D'une façon générale nous désignerons par $\mathscr{H}_{\mathrm{L}}$ le 2-groupe des classes au sens restreint du corps de nombres L. Soit a un entier sans facteur carré positif. P. Damey et J. J. Payan ont montré dans [2] que la différence des 4-rangs : $\dim_4 \mathscr{H}_{\mathrm{Q}(\sqrt{-a})} - \dim_4 \mathscr{H}_{\mathrm{Q}(\sqrt{a})}$ ne peut prendre que l'une ou l'autre des valeurs 1 ou 0. L. Bouvier a montré dans [1] que pour $m = 4$ et 8 les différences des m-rangs : $\dim_m \mathscr{H}_{\mathrm{Q}(\sqrt{2}, \sqrt{-a})} - \dim_m \mathscr{H}_{\mathrm{Q}(\sqrt{2}, \sqrt{a})}$ sont comprises entre 0 et 4.

Nous généralisons ci-après ces propriétés. Pour énoncer le résultat obtenu, fixons quelques notations. On désignera par :

k un corps de nombres ne contenant pas $\sqrt{-1}$,

d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-d}$ n'appartiennent à k,

$\mathrm{K} = k(\sqrt{d})$, $\overline{\mathrm{K}} = k(\sqrt{-d})$,

j (resp $\bar{j}$) l'application de $\mathscr{H}_k$ dans $\mathscr{H}_{\mathrm{K}}$ (resp. $\mathscr{H}_{\overline{\mathrm{K}}}$) déduite de l'injection canonique du groupe des idéaux de k dans le groupe des idéaux de K (resp. $\overline{\mathrm{K}}$).

Posons $\mathscr{D} = \mathscr{H}_{\mathrm{K}}/j(\mathscr{H}_k)$ et $\overline{\mathscr{D}} = \mathscr{H}_{\overline{\mathrm{K}}}/\bar{j}(\mathscr{H}_k)$.

Nous démontrons que pour toute puissance de 2, notée m, supérieure ou égale à 4, et telle que le sous-corps réel maximal du $m^{\text{ème}}$ corps cyclotomique $\mathbf{Q}_0^{(m)}$ soit inclus dans k, la différence des m-rangs de $\mathscr{D}$ et $\overline{\mathscr{D}}$ est majorée par la somme de trois constantes positives ou nulles :

$$\dim_m \mathscr{D} - \dim_m \overline{\mathscr{D}} \leqslant n_1 + n_2 + n_3.$$

Si $E_{\overline{K}}$ et E_k sont les groupes d'unités de $\overline{K}$ et k, n_1 a pour valeur $n_1 = \dim_{\mathbf{Z}}(E_{\overline{K}}) - \dim_{\mathbf{Z}}(E_k)$. On trouvera les définitions de n_2 et n_3 au début du paragraphe 3. Précisons simplement pour l'instant que lorsque k est 2-principal, c'est-à-dire lorsque $\mathscr{H}_k = 1$, alors n_3 est nul et $\mathscr{D}$ (resp. $\overline{\mathscr{D}}$) coïncide avec $\mathscr{H}_K$ (resp. $\mathscr{H}_{\overline{K}}$). Si de plus k est totalement réel, alors n_2 est nul également. C'est ce qui se passe lorsque $k = \mathbf{Q}$ ou $\mathbf{Q}(\sqrt{2})$ et on retrouve alors les résultats cités ci-dessus.

Pour démontrer leur propriété, Damey et Payan ont utilisé une construction et un dénombrement des extensions non ramifiées cycliques de degré 4 d'un corps quadratique.

D'autre part, G. Gras a donné, de cette même propriété, une démonstration employant la loi de réciprocité quadratique; [3]. L. Bouvier avait utilisé des techniques analogues à celles de Damey-Payan.

La méthode que nous employons diffère de celles-ci. Elle emprunte pour l'essentiel au « Spiegelungssatz » de Leopoldt [4]. Toutefois, celui-ci pose une hypothèse : « l ne divise pas $|G|$ » qui assure la semi-simplicité des $\mathbf{F}_l[G]$-modules considérés et qui n'est pas vérifiée ici.

Le groupe $\mathscr{D}/\mathscr{D}^m$ est considéré à l'aide de l'isomorphisme de réciprocité, comme le groupe de Galois d'une extension non ramifiée de K notée N_m. Si l'on pose $L = K(\sqrt{-1})$, $G = \mathrm{Gal}(L/k)$ et $M_m = N_m(\sqrt{-1})$, alors M_m/L est une extension de Kummer et on désigne par W_m son radical. Le m-rang de $\mathscr{D}$ est alors représenté par le 2-rang de $W_m/W_{m/2}$. L'application θ_m dérive d'une application déjà employée par Leopoldt. Elle joue un rôle essentiel : en effet elle applique un groupe isomorphe à $W_m/W_{m/2}$ dans un groupe dont le 2-rang est égal au m-rang de $\overline{\mathscr{D}}$. La différence : $\dim_m \mathscr{D} - \dim_m \overline{\mathscr{D}}$ est donc majorée par $\dim_2 \operatorname{Ker} \theta_m$. Cette valeur est bornée au moyen d'un homomorphisme injectif ψ_m par $\dim_2 B^{**}/\pm B^{*2}$. Les définitions de ces ensembles : B^{**} et B^{*} sont données au paragraphe 2.

Dans le paragraphe 3, on majore cette dernière valeur par $n_1 + n_2 + n_3$. Ce calcul est élémentaire.

Le paragraphe 4 est consacré à l'énoncé d'inégalités qui bornent la différence $\dim_m \mathscr{H}_k - \dim_m \mathscr{H}_{k'}/j'(\mathscr{H}_k)$; k' désignant le corps $k(\sqrt{-1})$ et j' l'application canonique de $\mathscr{H}_k$ dans $\mathscr{H}_{k'}$.

Le paragraphe 5 contient quelques illustrations numériques.

Ces résultats n'auraient pas été mis en évidence sans les conseils et les encouragements de G. Gras. Je le prie de trouver ici l'expression de mes remerciements.

1. Définitions et rappels.

On désignera par k un corps de nombres et d un élément de k. Nous supposerons qu'aucune des racines carrées $\sqrt{d}$, $\sqrt{-d}$, $\sqrt{-1}$ n'appartient à k. On notera m_0 la plus grande puissance de 2 telle que le sous-corps réel maximal $\mathbf{Q}_0^{(m_0)}$ du $m_0^{\text{ème}}$ corps cyclotomique soit inclus dans k et on désignera par ξ une racine primitive $m_0^{\text{ème}}$ de l'unité.

Nous poserons $\mathrm{K} = k(\sqrt{d})$, $\overline{\mathrm{K}} = k(\sqrt{-d})$, $k' = k(\sqrt{-1})$ et $\mathrm{L} = k(\sqrt{d}, \sqrt{-d})$. Le groupe de Galois de L/k est un groupe de Klein que l'on désignera par G. L'élément de G qui laisse invariant K (resp. $\overline{\mathrm{K}}$) sera noté σ (resp. $\bar{\sigma}$). Le groupe G est donc égal à $\{1, \sigma, \bar{\sigma}, \sigma\bar{\sigma}\}$. On a aussi $\xi^\sigma = \xi^{\bar{\sigma}} = \xi^{-1}$ et $k' = k(\xi)$.

Nous désignerons par ρ (resp. $\bar{\rho}$) la restriction de $\bar{\sigma}$ (resp. σ) à K (resp. $\overline{\mathrm{K}}$). On a donc $\mathrm{Gal}(\mathrm{K}/k) = \{1, \rho\}$ et $\mathrm{Gal}(\overline{\mathrm{K}}/k) = \{1, \bar{\rho}\}$.

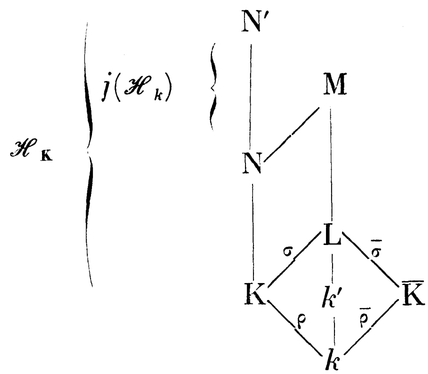
Nous désignerons par $\mathscr{H}_{\mathrm{K}}$, $\mathscr{H}_{\overline{\mathrm{K}}}$, $\mathscr{H}_k$ les 2-groupes des classes d'idéaux au sens restreint de K, $\overline{\mathrm{K}}$ et k. Soient j et $\bar{j}$ les applications de $\mathscr{H}_k$ dans $\mathscr{H}_{\mathrm{K}}$ et $\mathscr{H}_{\overline{\mathrm{K}}}$ déduites des injections du groupe des idéaux de k dans les groupes d'idéaux de K et $\overline{\mathrm{K}}$.

Nous poserons $\mathscr{D} = \mathscr{H}_{\mathrm{K}}/j(\mathscr{H}_k)$ et $\overline{\mathscr{D}} = \mathscr{H}_{\overline{\mathrm{K}}}/\bar{j}(\mathscr{H}_k)$.

Nous désignerons par N′ la 2-extension abélienne, non ramifiée, maximale de K. (On entend par extension non ramifiée une extension dans laquelle aucun idéal ne se ramifie).

Rappelons que les deux groupes $\mathrm{Gal}(N'/K)$ et $\mathscr{H}_K$ se correspondent dans l'isomorphisme de réciprocité. Cet isomorphisme est un isomorphisme de $\mathrm{Gal}(K/k)$-modules. (La structure de $\mathrm{Gal}(K/k)$-module de $\mathrm{Gal}(N'/K)$ est définie par $y^\rho = r^{-1}yr$, r étant un prolongement de ρ à N' et y un élément de $\mathrm{Gal}(N'/K)$). Composant cet isomorphisme avec la correspondance classique de Galois, on en déduit une bijection canonique entre les sous-$\mathrm{Gal}(K/k)$-modules de $\mathscr{H}_K$ et les sous-corps de N', contenant K et galoisiens sur k. Désignons par N le sous-corps de N' qui correspond ainsi à $j(\mathscr{H}_k)$. Le groupe de Galois : $\mathrm{gal}(N/K)$ est isomorphe à $\mathscr{D}$ et la structure de $\mathrm{Gal}(K/k)$-module de $\mathrm{Gal}(N/K)$ est donc déterminée par $y^\rho = y^{-1}$, pour tout y de $\mathrm{Gal}(N/K)$.

Posons encore $M = NL$. Suivant que L soit inclus dans N ou non, on aura $M = N$ ou $[M : N] = 2$. Le dessin suivant résume les notations introduites :



Dans toute la suite on désignera par m une puissance de 2. Si H est un $\mathbf{F}_2$-espace vectoriel, on notera $\dim_2 H$ sa dimension. Si H est un 2-groupe abélien, on notera $\dim_m H$ son m-rang, c'est-à-dire : $\dim_m H = \dim_2 H^{m/2}/H^m$. Si l'on décompose H en produit direct de groupes cycliques, $\dim_m H$ est le nombre de composantes de H d'ordre supérieur ou égal à m. On notera $H^{(m)}$ l'ensemble des éléments de H dont la puissance m^{eme} est égale à 1. On a :

$$\dim_2 H^{(m)}/H^{(m/2)} = \dim_m H.$$

Désormais, on désigne par m une puissance de 2 inférieure à m_0. Soit N_m le corps intermédiaire entre N et K, maximal tel que N_m/K soit d'exposant divisant m. Nous avons donc :

$$\mathrm{Gal}\,(N_m/K) \cong \mathscr{D}/\mathscr{D}^m.$$

Posons $M_m = N_m L$.

L'extension M_m/L est une extension de Kummer dont le radical sera désigné par W_m. On a donc $W_m = \{w;\, w \in M_m, w^m \in L^*\}$, et pour tout m compris entre 4 et m_0 :

$$\dim_m \mathscr{D} = \dim_2 \mathrm{Gal}\,(N_m/N_{m/2}) = \dim_2 \mathrm{Gal}\,(M_m/M_{m/2}) = \dim_2 W_m/W_{m/2}.$$

Nous avons de plus besoin d'une structure de G-module sur les groupes W_m/L^*. Si τ est un élément de G, on note t un prolongement de τ à M_m. Si w appartient à W_m, l'élément $w^t L^*$ de W_m/L^* ne dépend pas du choix de t mais seulement de τ. En posant $(wL^*)^\tau = w^t L^*$, on définit sur W_m/L^* une structure de G-module. D'autre part, munissons $\mathrm{Gal}\,(M_m/L)$ de la structure de G-module ainsi définie : Pour tout y de $\mathrm{Gal}\,(M_m/L)$, $y^\tau = t^{-1}yt$.

Nous aurons alors $y^{\bar\sigma} = y^{-1}$ et $y^\sigma = y$.

Désignons par $\mathrm{Gal}\,(M_m/L)^\wedge$ le dual de $\mathrm{Gal}\,(M_m/L)$ c'est-à-dire le groupe des homomorphismes de $\mathrm{Gal}\,(M_m/L)$ dans L^*. Rappelons que la théorie de Kummer donne un isomorphisme canonique de W_m/L^* sur $\mathrm{Gal}\,(M_m/L)^\wedge$ ainsi défini : si wL^* appartient à W_m/L^*, il lui correspond $\alpha(wL^*)$ qui est l'homomorphisme de $\mathrm{Gal}\,(M_m/L)$ dans L^* défini par : $\alpha(wL^*)(y) = w^{y-1}$.

Écrivons cette égalité avec y^τ : nous aurons donc :

$$\alpha(wL^*)(y^\tau) = w^{t^{-1}yt-1}.$$

Écrivons-la également avec $(wL^*)^\tau$ et y.

Comme τ est d'ordre 2, on aura :

$$\alpha((wL^*)^\tau)(y) = (w^{t^{-1}})^{y-1}; \qquad \text{d'où :} \qquad \alpha((wL^*)^\tau)(y)^\tau = w^{t^{-1}y\,t-1}.$$

Nous en déduisons : $\alpha((wL^*)^\tau)(y)^\tau = \alpha(wL^*)(y^\tau)$. Cette quantité est une racine m_0^{eme} de 1 et nous avons vu que $\zeta^\sigma = \zeta^{\bar\sigma} = \zeta^{-1}$. Faisons $\tau = \sigma$ dans la relation précédente. Nous obtenons : $\alpha((wL^*)^\sigma) = \alpha(wL^*)^{-1}$ d'où $(wL^*)^\sigma = (wL^*)^{-1}$. D'autre part, en remplaçant τ par $\bar\sigma$, dans la même relation, on obtient $(wL^*)^{\bar\sigma} = wL^*$.

Remarque. — Nous venons de redémontrer ce que Leopoldt appelle plus généralement « Spiegelungsrelation » [4].

Résumons les résultats obtenus dans la

PROPOSITION 1. — *Soit* m *une puissance de* 2 *inférieure à* m_0 *et soit* N_m *le corps intermédiaire entre* N *et* K *maximal tel que* N_m *soit d'exposant divisant* m. *Soit* $M_m = N_m L$ *et soit* W_m *le radical de* M_m.

(i) *La structure de* G-*module de* W_m/L^* *est déterminée par les relations :* $(wL^*)^\sigma = (wL^*)^{-1}$ *et* $(wL^*)^{\bar\sigma} = wL^*$.

(ii) *Si de plus* m *est supérieur ou égal à* 4,

$$\dim_m \mathscr{D} = \dim_2 W_m/W_{m/2}.$$

2. Applications θ_m et ψ_m.

PROPOSITION 2*a*. — *L'extension* N/K *est décomposée sur* k *et l'extension* M/L *est décomposée sur* $\overline{K}$.

Démonstration. — Rappelons d'abord que l'extension N/K est dite décomposée sur k lorsque Gal (N/k) est produit semi-direct de l'un de ses sous-groupes par Gal (N/K). Il revient au même de dire qu'il existe un sous-corps X de N tel que : $N = KX$ et $K \cap X = k$.

Soit r un prolongement de ρ à N' et soient $\langle r \rangle$ et $\langle r^2 \rangle$ les sous-groupes de Gal (N'/k) engendrés par r et r^2. Ce dernier sous-groupe est inclus dans le centre de Gal (N'/k). Si N_0 est le sous-corps de N laissé invariant par $\langle r^2 \rangle$, l'extension N_0/k est donc galoisienne. De plus on a :

$$\mathrm{Gal}\,(N'/N_0) = \langle r^2 \rangle = \mathrm{Gal}\,(N'/K) \cap \langle r \rangle,$$

et

$$\mathrm{Gal}\,(N'/k) = \mathrm{Gal}\,(N'/K)\,\langle r \rangle.$$

L'extension N_0/K est donc décomposée sur k.

Montrons maintenant que N_0 contient N. D'après la théorie du corps des classes, il existe un idéal $\mathfrak{P}$ de N', non ramifié dans N'/k, tel que r soit égal à l'automorphisme de Frobenius $(\mathfrak{P}, N'/k)$. Soit $\mathfrak{p}$ l'idéal premier de K en dessous de $\mathfrak{P}$. Si f est le degré résiduel de $\mathfrak{p}$ dans K/k, nous aurons $r^f = (\mathfrak{P}, N'/K)$; d'où $f = 2$. D'autre part, N'/K est abélienne, le symbole $(\mathfrak{P}, N'/K)$ ne dépend plus que de $\mathfrak{p}$ et nous pouvons écrire $r^2 = (\mathfrak{p}, N'/K)$. Puisque $f = 2$, $\mathfrak{p}$ est l'étendu d'un idéal premier de k. Dans l'isomorphisme de réciprocité liant Gal (N'/K) et $\mathscr{H}_K$, r^2 est donc l'image d'une classe d'idéaux appartenant à $j(\mathscr{H}_k)$. Le corps N_0 contient donc N et puisque N_0/K est décomposée sur k, il en sera de même de N/K.

Il reste à voir que cette propriété de décomposition se transmet à M/L. Si $N \cap L = K$, les groupes de Galois Gal $(M/\overline{K})$ et Gal (N/k) sont isomorphes par restriction des automorphismes de M à N. Dans cet isomorphisme, Gal (N/K) correspond à Gal (M/L) et l'extension M/L sera décomposée sur $\overline{K}$. Supposons maintenant que L soit contenu dans N. Nous avons alors $M = N$. Désignons désormais par r un prolongement d'ordre 2 de ρ à N et par s un prolongement de $\overline{\sigma}$ à N. L'automorphisme r prolonge donc $\overline{\sigma}$ ou $\sigma\overline{\sigma}$, et r ou rs est un prolongement de $\overline{\sigma}$ à M. Calculons $(rs)^2$. Comme $rsr = r^{-1}sr = s^{-1}$, on en déduit $(rs)^2 = 1$. Le groupe Gal $(M/\overline{K})$ est donc produit semi-direct de Gal (M/L) par l'un ou l'autre des sous-groupes $\{1, r\}$ ou $\{1, rs\}$. L'extension M/L est donc décomposée sur $\overline{K}$.

Remarque. — La première assertion de cette proposition pouvait être remplacée par l'énoncé plus général suivant : " Si K/k est une extension cyclique de degré quelconque ; si $\mathscr{H}_K$ et $\mathscr{H}_k$ sont les groupes des classes de K et k ; si j est l'application canonique de $\mathscr{H}_k$ dans $\mathscr{H}_K$; si N est le sous-corps du corps des classes de Hilbert N' de K, correspondant à $j(\mathscr{H}_k)$, c'est-à-dire invariant par l'image de $j(\mathscr{H}_k)$ dans l'isomorphisme de réciprocité : Gal $(N'/K) \cong \mathscr{H}_K$, alors l'extension N/K est décomposée sur k ". La démonstration est semblable à celle donnée plus haut.

DÉFINITION DE W'_m. — *Nous désignerons désormais par* $\overline{s}$ *un prolongement de* $\overline{\sigma}$ *à* M, *d'ordre* 2. *Pour toute puissance de* 2 *notée* m *et inférieure à* m_0, *nous noterons* W'_m *l'ensemble des éléments de* W_m *invariants par* $\overline{s}$.

Proposition 2b. — *L'injection canonique de* W'_m *dans* W_m *induit un isomorphisme de* $W'_m/\overline{K}^*$ *sur* W_m/L^*. *De plus, quel que soit* $\mathfrak{w}$ *de* W'_m, $\mathfrak{w}^{m(\sigma+1)}$ *appartient à* k^m.

Démonstration. — Considérons l'application de W'_m dans W_m/L^* qui associe à tout $\mathfrak{w}'$ de W'_m, $\mathfrak{w}'L^*$. Si $\mathfrak{w}$ est un élément de W_m, alors compte tenu de la proposition 1 (i), $\mathfrak{w}^{\bar{s}-1}$ appartient à L. Comme $\bar{s}$ est d'ordre 2, on en déduit : $(\mathfrak{w}^{\bar{s}-1})^{\bar{\sigma}+1} = 1$, et il existe α dans L tel que $\mathfrak{w}^{\bar{s}-1} = \alpha^{\bar{\sigma}-1}$. Posons alors $\mathfrak{w}' = \mathfrak{w}\alpha^{-1}$. On a $\mathfrak{w}L^* = \mathfrak{w}'L^*$ et $\mathfrak{w}'$ appartient à W'_m. L'application considérée est donc surjective. On en déduit l'isomorphisme annoncé.

Soit maintenant $\mathfrak{w}$ un élément de W'_m. Il est nécessaire de distinguer deux cas :

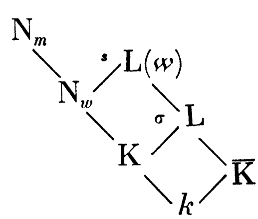
Premier cas : Il existe un sous-corps N_w de N_m tel que $L(\mathfrak{w}) = N_w L$ et $N_w \cap L = K$. Désignons alors par s un prolongement de σ à $L(\mathfrak{w})$ qui invarie N_w. Désignons encore par $\bar{s}$ la restriction de $\bar{s}$ à $L(\mathfrak{w})$. On a :

$$L(\mathfrak{w}) = N_w\overline{K} \qquad \text{et} \qquad N_w \cap \overline{K} = k.$$

On en déduit $s^2 = \bar{s}^2 = 1$ et $s\bar{s} = \bar{s}s$.

En vertu de la proposition 1, $\mathfrak{w}^{s+1}$ appartient à L. De plus $\mathfrak{w}^{s+1}$ est invariant par σ et $\bar{\sigma}$. Donc il appartient à k.

On en déduit que $\mathfrak{w}^{m(\sigma+1)}$ appartient à k^m.



Deuxième cas : Il n'existe pas de sous-corps N_w de N_m tel que $L(\mathfrak{w}) = LN_w$ et $L \cap N_w = K$. Dans ce cas, on aura donc : $L \subset N$, $N = M$ et $N_m = M_m$. Désignons encore par $\bar{s}$ la restriction de $\bar{s}$ à $L(\mathfrak{w})$ et par s un prolongement de σ à $L(\mathfrak{w})$. Comme $\bar{s}$ est un prolongement de ρ, nous avons $s^\rho = \bar{s}s\bar{s} = s^{-1}$. On posera $\zeta_m = \zeta^{m_0/m}$. Soit m' l'exposant de $L(\varpi)/K$. Si les exposants de $\mathrm{Gal}\,(L(\varpi)/K)$ et $\mathrm{Gal}\,(L(\varpi)/L)$ étaient égaux et puisque $\mathrm{Gal}\,(L(\varpi)/L)$ est cyclique, alors $\mathrm{Gal}\,(L(\varpi)/L)$ serait facteur direct de $\mathrm{Gal}\,(L(\varpi)/K)$ et $L(\varpi)/L$ se décomposerait sur K. Ces deux exposants sont donc différents et cela prouve que $L(\varpi)/K$ est cyclique de degré m'. De plus s engendre le groupe de Galois de cette extension. Si $m' = 2$, ϖ appartient à $\overline{K}$ et on obtient tout de suite le résultat. Supposons maintenant $m' \geqslant 4$ et montrons que ϖ^{1+s} appartient à $\zeta_{m'}^{-1}K$.

$$\begin{tikzcd}[column sep=small]
 & N_m = M_m \arrow[d, dash] & \\
 & L(\varpi) \arrow[d, dash] & \\
 & L \arrow[dl, dash, "\sigma"'] \arrow[dr, dash, "\bar{\sigma}"] & \\
K \arrow[dr, dash, "\rho"] & & \overline{K} \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

L'extension $L(\varpi)/L$ est une extension de Kummer de degré $m'/2$ dont le groupe de Galois est engendré par s^2.

On aura donc : $\varpi^{s^2} = \zeta_{m'/2}\varpi$ et $\varpi^{(1+s)s} = \zeta_{m'/2}\varpi^{1+s}$. Or 1 et $\zeta_{m'}^{-1}$ forment une base de L/K. Il suffit de décomposer ϖ^{1+s} sur cette base pour constater que ϖ^{1+s} appartient à $\zeta_{m'}^{-1}K$. De plus, on a $\varpi^{1+s} = \varpi^{1+\bar{s}s}$. On en déduit que ϖ^{1+s} est invariant par $\bar{s}s$. Cela prouve que ϖ^{1+s} appartient à k'. Comme $\zeta_{m'}^{-1}K \cap k' = \zeta_{m'}^{-1}k$, on en déduit que $\varpi^{(1+s)m'}$ appartient à $k^{m'}$. Puisqu'enfin, $L(\varpi)$ est inclus dans $M_m = N_m$, m' divise m et $\varpi^{m(1+\sigma)}$ appartient à k^m.

Désignons par A_k, A_L et $A_{\overline{K}}$ les anneaux d'entiers de k, L et $\overline{K}$.

Lemme 2*a*. — *Si* m *est une puissance de* 2 *comprise entre* 2 *et* m_0 *et si* ϖ *appartient à* W'_m, *alors* ϖ^m *appartient à* $\overline{K}$ *et l'idéal engendré par* ϖ^m *est de la forme* $\varpi^m A_{\overline{K}} = \mathfrak{C}^{m/2}\mathfrak{A}^m$; $\mathfrak{C}$ *étant un idéal de* k *et* $\mathfrak{A}$ *un idéal de* $\overline{K}$.

Démonstration. — Supposons donc que w appartienne à W'_m. L'extension $L(w)/L$ est non ramifiée d'exposant divisant m et l'idéal $w^m A_L$ est donc la puissance m^{eme} d'un idéal de L. Écrivons cet idéal sous la forme $\mathfrak{B}\mathfrak{D}$, $\mathfrak{B}$ étant un idéal de L ramifié dans $L/\overline{K}$ et $\mathfrak{D}$ un idéal de L non ramifié dans $L/\overline{K}$. On a donc $w^m A_L = \mathfrak{B}^m \mathfrak{D}^m$. Comme w^m appartient à $\overline{K}$, nous aurons $\mathfrak{D}^{\bar{\sigma}} = \mathfrak{D}$ et $\mathfrak{D}$ est l'étendu d'un idéal de $\overline{K}$. Quant à $\mathfrak{B}$, on peut le décomposer en produit d'idéaux premiers (ramifiés sur $\overline{K}$) de la façon suivante :

$$\mathfrak{B} = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_3^{a_3+\sigma a'_3} \ldots,$$

avec :

$\mathfrak{p}_1$ idéal de L complètement ramifié dans L/k;

$\mathfrak{p}_2$ idéal de L ramifié dans $L/\overline{K}$ et inerte dans L/K;

$\mathfrak{p}_3$ idéal de L ramifié dans $L/\overline{K}$ et décomposé dans L/K.

D'après la proposition 2*b*, $w^{m(1+\sigma)}$ appartient à k^m et d'autre part $\mathfrak{D}^{\sigma+1}$ est l'étendu d'un idéal de k. Donc,

$$\mathfrak{B}^{\sigma+1} = \mathfrak{p}_1^{2a_1} \ldots \mathfrak{p}_2^{2a_2} \ldots \mathfrak{p}_3^{(a_3+a'_3)(1+\sigma)} \ldots$$

est aussi l'étendu d'un idéal de k. On aura donc $a_1 \equiv 0 \ (2)$ et $a_3 + a'_3 \equiv 0 \ (2)$. On en déduit que $\mathfrak{p}_1^{a_1}$ est l'étendu d'un idéal de $\overline{K}$. Si a_3 est pair, $\mathfrak{p}_3^{a_3}$ est l'étendu d'un idéal de $\overline{K}$ et il en est de même de $\mathfrak{p}_3^{\sigma a'_3}$. Si maintenant a_3 est impair, on peut écrire :

$$\mathfrak{p}_3^{a_3+\sigma a'_3} = \mathfrak{p}_3^{a_3-1+\sigma(a'_3-1)} \mathfrak{p}_3^{1+\sigma} \qquad \text{et} \qquad \mathfrak{p}_3^{2(1+\sigma)}$$

est l'étendu d'un idéal de k. Finalement $\mathfrak{p}_3^{(a_3+\sigma a'_3)m}$ sera l'étendu d'un idéal de $\overline{K}$ de la forme $\mathfrak{C}^{m/2}\mathfrak{A}^m$, $\mathfrak{C}$ étant un idéal de k et $\mathfrak{A}$ un idéal de $\overline{K}$. Quant à $\mathfrak{p}_2$, il est tel que $\mathfrak{p}_2^2$ soit l'étendu d'un idéal de k. Donc $\mathfrak{p}_2^m$ est l'étendu d'un idéal de la forme $\mathfrak{C}^{m/2}$, $\mathfrak{C}$ étant un idéal de k. Nous avons donc montré que $w^m A_L = \mathfrak{C}^{m/2}\mathfrak{A}^m A_L$, avec $\mathfrak{C}$ idéal de k et $\mathfrak{A}$ idéal de $\overline{K}$. Comme w^m appartient à $\overline{K}$, on en déduit : $w^m A_K = \mathfrak{C}^{m/2}\mathfrak{A}^m$.

Proposition 2*c*. — *Soit m une puissance de 2 comprise entre 2 et m_0. Si w appartient à W'_m, soit* $\mathrm{Cl}(\mathfrak{A})$ *la* *classe de l'idéal* $\mathfrak{A}$ *de* $\overline{\mathrm{K}}$ *défini par le lemme* 2*a*. *Alors* $\mathrm{Cl}(\mathfrak{A})^m$ *appartient à* $\bar{j}(\mathscr{H}_k)$.

Démontrons tout d'abord le lemme suivant :

LEMME 2*b*. — *Soit* x *un élément de* $\overline{\mathrm{K}}$, *tel que* $x^{\sigma+1}$ *soit un élément totalement positif de* k. *Alors il existe* c *dans* k *tel que* xc *soit un élément totalement positif de* $\overline{\mathrm{K}}$.

En effet, on peut écrire les plongements réels de $\overline{\mathrm{K}}$ dans $\mathbf{C}$ sous la forme $p_1, \ldots, p_s, \sigma p_1, \ldots, \sigma p_s$ et les restrictions de $p_1, \ldots, p_s$ à k seront des plongements distincts de k dans $\mathbf{C}$.

Soit c un élément de k tel que c^{p_i} ait le même signe que x^{p_i}, pour tout i de 1 à s. Nous aurons donc $(xc)^{p_i} > 0$ et $(xc)^{\sigma p_i} > 0$. Ceci montre que xc est un élément totalement positif de $\overline{\mathrm{K}}$.

Démontrons la proposition 2*c*. Soit w un élément de W'_m. En vertu de la proposition 1 (ii), du lemme 2*b* et puisque m est supérieur à 2, il existe c dans k tel que $w^m c^{-1}$ soit totalement positif.

Nous en déduisons : $\mathrm{Cl}(w^m \mathrm{A}_{\overline{\mathrm{K}}}) = \mathrm{Cl}(c\mathrm{A}_{\overline{\mathrm{K}}})$. (Il n'est question ici que de classes au sens restreint). D'où $\mathrm{Cl}(w^m \mathrm{A}_{\overline{\mathrm{K}}})$ appartient à $\bar{j}(\mathscr{H}_k)$. Comme $w^m \mathrm{A}_{\overline{\mathrm{K}}} = \mathfrak{C}^{m/2}\mathfrak{A}^m$, avec $\mathfrak{A}$ idéal de k, on en déduit que $\mathrm{Cl}(\mathfrak{A})^m$ appartient à $\bar{j}(\mathscr{H}_k)$. En d'autres termes, $\mathrm{Cl}(\mathfrak{A})\bar{j}(\mathscr{H}_k)$ appartient à $\overline{\mathscr{D}}^{(m)}$. On en déduit la définition de θ_m.

DÉFINITION DE θ_m. — *Soit* m *une puissance de* 2 *comprise entre* 4 *et* m_0. *Soit* w *appartenant à* W'_m *et soit* $\mathrm{Cl}(\mathfrak{A})$ *la classe de l'idéal* $\mathfrak{A}$ *de* $\overline{\mathrm{K}}$ *défini par le lemme* 2*a*. *Nous noterons* θ_m *l'homomorphisme de* $\mathrm{W}'_m/\mathrm{W}'_{m/2}$ *dans* $\overline{\mathscr{D}}^{(m)}/\overline{\mathscr{D}}^{(m/2)}$ *qui associe à* $w\mathrm{W}'_{m/2}$ *la classe de* $\mathrm{Cl}(\mathfrak{A})\bar{j}(\mathscr{H}_k)$ *modulo* $\overline{\mathscr{D}}^{(m/2)}$.

DEFINITION DE B^{**} ET B^*. — *Nous désignerons par* B^{**} *l'ensemble des éléments* u *de* $\overline{\mathrm{K}}$ *tels que l'idéal engendré par* u *soit de la forme* $\mathfrak{C}^2 b^2 \mathrm{A}_{\overline{\mathrm{K}}}$ *avec* $\mathfrak{C}$ *idéal de* k, b *élément totalement positif de* $\overline{\mathrm{K}}$, *et tels que* $u^{\sigma+1}$ *appartienne à* k^4.

En abrégé :

$$B^{**} = \{u;\, u \in \overline{K},\ uA_{\overline{K}} = \mathfrak{C}^2 b^2 A_{\overline{K}},\ \mathfrak{C} \text{ idéal de } k,\ b \in \overline{K}^+,\ u^{\sigma+1} \in k^4\}.$$

Nous noterons B^*, *l'ensemble des éléments de* $\overline{K}$, *dont la norme dans* $\overline{K}/k$ *est un carré de* k. *En abrégé :*

$$B^* = \{u;\ u \in \overline{K},\ u^{\sigma+1} \in k^2\}.$$

On déduit immédiatement du lemme 2*b*, que B^{*2} est inclus dans B^{**}.

DÉFINITION DE ψ_m. — *Soit* m *une puissance de* 2 *comprise entre* 4 *et* m_0. *Supposons que* $\varpi W'_{m/2}$ *appartienne à* $\operatorname{Ker} \theta_m$. *Conservons les notations du lemme* 2*a*, *c'est-à-dire :* $\varpi^m A_{\overline{K}} = \mathfrak{C}^{m/2}\mathfrak{A}^m$. *Nous avons donc :* $\mathrm{Cl}(\mathfrak{A})^{m/2}$ *appartient à* $\bar{j}(\mathscr{H}_k)$ *et il existe un idéal* $\mathfrak{C}_0$ *de* k *et un élément* b *totalement positif de* $\overline{K}$ *tels que*

$$\mathfrak{A}^{m/2} = \mathfrak{C}_0 b A_{\overline{K}}; \qquad \text{d'où} \qquad \varpi^m A_{\overline{K}} = \mathfrak{C}^{m/2}\mathfrak{C}_0^2 b^2 A_{\overline{K}}.$$

D'autre part, en vertu de la proposition 1 (ii), $\varpi^{m(\sigma+1)}$ appartient à k^4. Nous avons donc vérifié que ϖ^m appartient à B^{**}.

Supposons maintenant que ϖ appartienne à $W'_{m/2}$; alors $\varpi^{(m/2)(\sigma+1)}$ appartient à k^2, $\varpi^{m/2}$ appartient à B^* et ϖ^m appartient à B^{*2}. Il s'en suit que l'on peut définir un homomorphisme ψ_m de $\operatorname{Ker} \theta_m$ dans $B^{**}/\pm B^{*2}$ en associant à l'élément $\varpi W'_{m/2}$ de $\ker \theta_m$, la classe de ϖ^m modulo $\pm B^{*2}$.

PROPOSITION 2*d*. — *L'homomorphisme* ψ_m *défini ci-dessus est injectif.*

Démonstration. — Supposons que $\varpi W'_{m/2}$ appartienne à $\operatorname{Ker} \theta_m$. Cela signifie que ϖ^m appartient à $\pm B^{*2}$. On en déduit d'abord que ϖ^m appartient à L^2 et que $L(\varpi)/L$ est d'exposant divisant $m/2$. Nous aurons $\varpi^{m/2} = u$ ou $\sqrt{-1}\,u$ avec u dans B^*. On en déduit aussi que $\varpi^{(m/2)(\sigma+1)}$ appartient à k^2. Ceci montre que $L(\varpi^{m/4})/L$ est décomposée sur K, c'est-à-dire que $L(\varpi^{m/4})/K$ est d'exposant 2.

(En vertu du critère de décomposition classique des extensions biquadratiques). L'extension $L(w)/K$ est donc d'exposant divisant $m/2$ et w appartient à $M_{m/2}$, donc à $W_{m/2}$.

Remarque. — On peut définir une application de $W'_m/W'_{m/2}$ dans $W'_{m/2}/W'_{m/4}$ en associant à $wW'_{m/2}$, $w^2W'_{m/4}$. Il s'agit d'un homomorphisme injectif. De plus si $wW'_{m/2}$ appartient à $\operatorname{Ker}\theta_m$, alors $w^2W'_{m/4}$ appartient à $\operatorname{Ker}\theta_{m/2}$. Pour toute puissance de 2 comprise entre 8 et m_0, il existe donc un homomorphisme injectif β_m de $\operatorname{Ker}\theta_m$ dans $\operatorname{Ker}\theta_{m/2}$. On a d'ailleurs $\psi_m = \psi_{m/2} \circ \beta_m$.

Le corollaire suivant se déduit des propositions précédentes :

COROLLAIRE. — *Pour toute puissance de* 2 *notée* m *et comprise entre* 4 *et* m_0, *on a :*

$$\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}} \leqslant \dim_2 B^{**}/\pm B^{*2}.$$

En effet, $\dim_m \mathcal{D}$ est égal à $\dim_2 W'_m/W'_{m/2}$ en vertu des propositions 1 et 2*b*. D'autre part, $\dim_m \overline{\mathcal{D}} = \dim_2 \overline{\mathcal{D}}^{(m)}/\overline{\mathcal{D}}^{(m/2)}$. En factorisant l'homomorphisme θ_m, on obtient l'inégalité :

$$\dim_2 W'_m/W'_{m/2} - \dim_2 \overline{\mathcal{D}}^{(m)}/\overline{\mathcal{D}}^{(m/2)} \leqslant \dim_2 \operatorname{Ker}\theta_m,$$

c'est-à-dire :

$$\dim_m \mathcal{D} - \dim_m \overline{\mathcal{D}} \leqslant \dim_2 \operatorname{Ker}\theta_m.$$

Enfin, on déduit de la proposition 2*d* l'inégalité :

$$\dim_2 \operatorname{Ker}\theta_m \leqslant \dim_2 B^{**}/\pm B^{*2}.$$

3. Majoration de $B^{**}/\pm B^{*2}$.

Notations. — On désignera par $E_{\overline{K}}$ (resp. E_k) le groupe des unités de $\overline{K}$ (resp. k). Les dimensions sur $\mathbf{Z}$ des groupes quotients de ces groupes par leurs sous-groupes de torsion seront notés $\dim_{\mathbf{Z}}(E_{\overline{K}})$ et $\dim_{\mathbf{Z}}(E_k)$. L'ensemble des éléments totalement positifs de $\overline{K}$ (resp. k) sera noté $\overline{K}^+$ (resp. k^+). On posera également $E^+ = E_{\overline{K}} \cap \overline{K}^+$ et $E_k^+ = E_k \cap k^+$. Dans ce paragraphe, on notera N au lieu de $N_{\overline{K}/k}$, la norme dans l'extension $\overline{K}/k$.

On désignera par E^{**} (resp. E^*) l'ensemble des unités ε de $\overline{K}$ telles que $N(\varepsilon)$ appartienne à k^4 (resp. k^2). En abrégé :

$$\begin{aligned} E^{**} &= E_{\overline{K}} \cap B^{**} = \{\varepsilon;\ \varepsilon \in E_{\overline{K}},\ \varepsilon^{\sigma+1} \in k^4\} \\ E^* &= E_{\overline{K}} \cap B^* \ \ = \{\varepsilon;\ \varepsilon \in E_{\overline{K}},\ \varepsilon^{\sigma+1} \in k^2\}. \end{aligned}$$

On notera F (resp. F') l'ensemble des éléments de $\overline{K}$ engendrant un idéal qui est l'étendu d'un idéal de k (resp. d'un idéal strictement principal de k). En abrégé :

$$\begin{aligned} F \ &= \{u;\ u \in \overline{K},\ uA_{\overline{K}} = \mathfrak{C}A_{\overline{K}},\ \ \mathfrak{C} \text{ idéal de } k\} \\ F' &= \{u;\ u \in \overline{K},\ uA_{\overline{K}} = \mathfrak{C}A_{\overline{K}},\ \ \mathfrak{C} \text{ idéal strict. principal de } k\}. \end{aligned}$$

On a donc $F' = k^+E_{\overline{K}}$. On posera aussi :

$$F^+ = \overline{K}^+ \cap F \qquad \text{et} \qquad F'^+ = \overline{K}^+ \cap F'.$$

On notera C (resp. C') l'ensemble des éléments de k engendrant le carré d'un idéal de k (resp. le carré d'un idéal principal au sens ordinaire de k). En abrégé :

$$\begin{aligned} C \ &= \{u;\ u \in k,\ uA_k = \mathfrak{C}^2,\ \ \mathfrak{C} \text{ idéal de } k\} \\ C' &= \{u;\ u \in k,\ uA_k = \mathfrak{C}^2,\ \ \mathfrak{C} \text{ idéal principal ordinaire de } k\}. \end{aligned}$$

On a donc $C' = k^2E_k$.

Nous noterons P_k le sous-groupe de $\mathscr{H}_k$ engendré par les classes d'idéaux principaux (au sens ordinaire) de k. Enfin nous définirons les constantes n_1, n_2, n_3 en posant :

$$\begin{aligned} n_1 &= \dim_{\mathbf{Z}} E_{\overline{K}} - \dim_{\mathbf{Z}} E_k \\ n_2 &= \dim_2\, (E_k^+ \cap N\overline{K})/E_k^2NE_{\overline{K}}^{\pm} \\ n_3 &= \dim_2\, \mathscr{H}_k^{(2)}/\mathrm{Ker}\,\overline{j}\,P_k. \end{aligned}$$

PROPOSITION 3*a*. — *Il existe une suite exacte :*

$$1 \to B^{*2}E^{**}/\pm B^{*2} \to B^{**}/\pm B^{*2} \xrightarrow{f} C \cap N\overline{K}^+/k^2NF^+.$$

Démonstration. — Définissons tout d'abord l'application f. Si u appartient à B^{**}, il engendre un idéal de la forme : $uA_{\overline{K}} = \mathfrak{C}^2b^2A_{\overline{K}}$ avec $\mathfrak{C}$ idéal de k et b dans $\overline{K}^+$. De plus, on a $u^{\sigma+1} = \wp^4$ avec $\wp$ dans k. D'où :

$$\wp^2A_k = \mathfrak{C}^2b^{\sigma+1}A_k.$$

Nous définissons $f(u)$ comme étant la classe de $\wp^2 b^{-(\sigma+1)}$ modulo $k^2\mathrm{NF}^+$.

Montrons qu'il s'agit bien d'une application. Rappelons d'abord que $k^+ \cap \mathrm{N}\overline{\mathrm{K}} = \mathrm{N}\overline{\mathrm{K}}^+$. Ceci prouve que $\wp^2 b^{-(\sigma+1)}$ appartient à $\mathrm{C} \cap \mathrm{N}\overline{\mathrm{K}}^+$. Montrons que $f(u)$ ne dépend pas du choix de $\mathfrak{C}$ et b.

Si $u\mathrm{A}_{\overline{\mathrm{K}}}$ s'écrit de deux façons :

$$u\mathrm{A}_{\overline{\mathrm{K}}} = \mathfrak{C}^2 b^2 \mathrm{A}_{\overline{\mathrm{K}}} = \mathfrak{C}'^2 b'^2 \mathrm{A}_{\overline{\mathrm{K}}}$$

nous aurons alors :

$$bb'^{-1}\mathrm{A}_{\overline{\mathrm{K}}} = \mathfrak{C}'\mathfrak{C}^{-1}\mathrm{A}_{\overline{\mathrm{K}}} \qquad \text{et} \qquad bb'^{-1}$$

appartient à F^+. D'où

$$\wp^2 b^{-(\sigma+1)}[\wp^2 b'^{-(\sigma+1)}]^{-1} = (bb'^{-1})^{-(\sigma+1)}$$

appartient à NF^+ et $f(u)$ ne dépend pas du choix de $\mathfrak{G}$ et b.

Supposons maintenant que u appartienne à $\pm\, \mathrm{B}^{*2}$.

Nous pouvons alors (Lemme 2b) écrire un élément de B^* sous la forme cb avec c dans k et b dans $\overline{\mathrm{K}}^+$. La quantité u est donc de la forme $u = \pm\, c^2 b^2$ et on a :

$$u\mathrm{A}_{\overline{\mathrm{K}}} = c^2 b^2 \mathrm{A}_{\overline{\mathrm{K}}}.$$

Définissons $\wp$: On a

$$u^{\sigma+1} = c^4 b^{2(\sigma+1)} \qquad \text{d'où} \qquad \wp^4 = c^4 b^{2(\sigma+1)}$$

et

$$\wp^2 = \pm\, c^2 b^{\sigma+1}.$$

Mais $c^2 b^{\sigma+1}$ est un carré dans k et -1 ne peut être un carré dans k. On a donc $\wp^2 = c^2 b^{\sigma+1}$ et $f(u)$ est la classe modulo $k^2\mathrm{NF}^+$ de $\wp^2 b^{-(\sigma+1)} = c^2$. Donc $f(u)$ est égal à $k^2\mathrm{NF}^+$. Nous avons bien défini un homomorphisme f.

Montrons que $\operatorname{Ker} f$ est inclus dans $\mathrm{B}^{*2}\mathrm{E}^{**}/\pm\mathrm{B}^{*2}$. Conservons les notations introduites au début de cette démonstration. Supposons que $u(\pm\, \mathrm{B}^{*2})$ appartienne à $\operatorname{Ker} f$. Il existe donc z dans F^+ et c dans k tels que $\wp^2 b^{-(\sigma+1)} = z^{\sigma+1} c^2$

Nous aurons

$$\mathfrak{G}^2 = \wp^2 b^{-(\sigma+1)}\mathrm{A}_k = z^{\sigma+1} c^2 \mathrm{A}_k.$$

D'où :

$$u A_{\overline{K}} = \mathfrak{G}^2 b^2 A_{\overline{K}} = z^{\sigma+1} c^2 b^2 A_{\overline{K}}.$$

Mais z appartient à F. Cela prouve que $z^{\sigma+1} A_{\overline{K}} = z^2 A_{\overline{K}}$ et nous aurons :

$$u A_{\overline{K}} = (zcb)^2 A_{\overline{K}} \qquad \text{et} \qquad u = (zcb)^2 \varepsilon$$

avec ε dans $E_{\overline{K}}$. Or $(zcb)^{\sigma+1} = \rho^2$ et zcb appartient à B^*. Donc ε appartient à E^{**} et u appartient à $B^{*2}E^{**}$.

L'inclusion inverse ne présente pas de difficulté. Si ε appartient à E^{**}, alors on a $\varepsilon A_{\overline{K}} = A_{\overline{K}}$ et on peut choisir pour calculer $f(\varepsilon)$: $\mathfrak{G} = A_k$, $b = 1$. Il s'en suit que si $\varepsilon^{\sigma+1} = \rho^4$, $f(\varepsilon)$ est égal à $k^2 NF^+$.

PROPOSITION 3*b*.

$$\mathrm{Dim}_2\, B^{*2}E^{**}/\pm B^{*2} = \dim_2 E^{**}/\pm E^{*2} \leqslant n_1.$$

Démonstration. — La première égalité est immédiate. En effet :

$$B^{*2}E^{**}/\pm B^{*2} \cong E^{**}/\pm B^{*2} \cap E^{**} = E^{**}/\pm E^{*2}.$$

Comme $\sqrt{-1}$ n'appartient pas à $\overline{K}$, le 2-sous-groupe de torsion de E^{**} est ± 1. D'autre part $E^4_{\overline{K}}$ est inclus dans E^{**} et cela prouve que $\dim_{\mathbf{Z}} E^{**}$ est égal à $\dim_{\mathbf{Z}} E_{\overline{K}}$. Nous aurons donc :

$$\dim_2 E^{**}/\pm E^{**2} = \dim_{\mathbf{Z}} E_{\overline{K}}.$$

Le groupe des unités de k, E_k est inclus dans E^*. Considérons l'homomorphisme de E_k^2 dans E^{*2}/E^{**2} qui associe à α^2 (α appartenant à E_k), $\alpha^2 E^{**2}$. Il a pour noyau E_k^4. Cela montre que :

$$\dim_2 E_k^2/E_k^4 \leqslant \dim_2 E^{*2}/E^{**2}.$$

Comme $\sqrt{-1}$ n'appartient pas à E_k, le 2-sous-groupe de torsion de E_k^2 est réduit à 1 et $\dim_2 E_k^2/E_k^4 = \dim_{\mathbf{Z}} E_k$.

Enfin $\pm E^{*2}/\pm E^{**2} \cong E^{*2}/E^{**2}$ et on aura :

$$\begin{aligned} \dim_2 E^{**}/\pm E^{*2} &= \dim_2 E^{**}/\pm E^{**2} - \dim_2 \pm E^{*2}/\pm E^{**2} \\ &\leqslant \dim_{\mathbf{Z}} E_{\overline{K}} - \dim_{\mathbf{Z}} E_k = n_1. \end{aligned}$$

PROPOSITION 3c. — $\mathrm{Dim}_2\, C \cap N\overline{K}^+/k^2NF^+ \leqslant n_2 + n_3$.

La démonstration de cette inégalité repose sur l'existence d'un isomorphisme :

$$C' \cap N\overline{K}^+/k^2NF'^+ \cong E_k^+ \cap N\overline{K}/E_k^2NE_{\overline{K}}^+,$$

et de deux suites exactes :

$$1 \to C' \cap N\overline{K}^+ \to C \cap N\overline{K}^+ \to \mathscr{H}_k^{(2)}/P_k,$$
$$k^2NF^+/k^2NF'^+ \to \mathrm{Ker}\,\overline{j}/P_k \cap \mathrm{Ker}\,\overline{j} \to 1.$$

Considérons l'inclusion $E_k^+ \cap N\overline{K} \subset C' \cap N\overline{K}^+$ et l'application naturelle f: $E_k^+ \cap N\overline{K} \to C' \cap N\overline{K}^+/k^2NF'^+$. Soit ε un élément de $E_k^+ \cap N\overline{K}$ tel que ε appartienne à $k^2NF'^+$. Nous aurons donc : $\varepsilon = u^{\sigma+1}c^2$, avec c dans k et u dans F'^+. Cet élément s'écrit donc $u = c_0\alpha$ avec c_0 dans k^+ et α dans $E_{\overline{K}}$. Comme u est totalement positif, α l'est aussi. On a donc $\varepsilon = \alpha^{\sigma+1}(c_0c)^2$ et c_0c appartient à E_k. Finalement ε appartient à $E_k^2NE_{\overline{K}}^+$. Réciproquement, l'inclusion $E_k^2NE_{\overline{K}}^+ \subset k^2NF'^+$ ne pose pas de problème. Nous avons donc montré que le noyau de f est $E_k^2NE_{\overline{K}}^+$.

Montrons maintenant que f est surjective. Soit u appartenant à $C' \cap N\overline{K}^+$. Nous avons donc $u = \varphi^{\sigma+1}$ avec φ dans $\overline{K}^+$ et $u = \varepsilon c^2$ avec ε dans E_k^+ et c dans k. On en déduit que $uk^2NF'^+ = \varepsilon k^2NF'^+$ et comme $\varepsilon = (\varphi c^{-1})^{\sigma+1}$, ε appartient donc à $E_k^+ \cap N\overline{K}$. L'image de ε par f est $uk^2NF'^+$. L'isomorphisme est démontré.

Soit maintenant u appartenant à $C \cap N\overline{K}^+$. Il existe un idéal $\mathfrak{C}$ de k tel que $uA_k = \mathfrak{C}^2$. Comme u est totalement positif, la classe de $\mathfrak{C}$ appartient à $\mathscr{H}_k^{(2)}$ et en associant à u la classe de $\mathrm{Cl}(\mathfrak{C})$ modulo P_k, nous obtenons un homomorphisme de $C \cap N\overline{K}^+$ dans $\mathscr{H}_k^{(2)}/P_k$ qui a pour noyau $C' \cap N\overline{K}^+$. Ceci démontre que la première suite est exacte.

Soit u un élément de k^2NF^+. Il s'écrit $u = \varphi^{\sigma+1}c^2$ avec φ dans F^+ et c dans k. On a donc $\varphi A_{\overline{K}} = \mathfrak{C}A_{\overline{K}}$. La classe de $\mathfrak{C}$ appartient à $\mathrm{Ker}\,\overline{j}$. Cette classe est définie modulo $P_k \cap \mathrm{Ker}\,\overline{j}$. En effet si on écrit $u = \varphi'^{\sigma+1}c'^2$ avec φ' dans F^+ et c' dans k, on aura alors :

$$\varphi' A_{\overline{K}} = \mathfrak{C}' A_{\overline{K}} \qquad \text{et} \qquad \varphi^{\sigma+1}A_k = \mathfrak{C}^2, \qquad \varphi'^{\sigma+1}A_k = \mathfrak{C}'^2$$

d'où :

$$\mathfrak{C}\mathfrak{C}'^{-1} = cc'^{-1}A_k \qquad \text{et} \qquad \mathrm{Cl}(\mathfrak{C}\mathfrak{C}'^{-1})$$

appartient à P_k. Nous avons donc défini une application de k^2NF^+ dans $\mathrm{Ker}\, \bar{j}/P_k \cap \mathrm{Ker}\, \bar{j}$. C'est un homomorphisme surjectif et $k^2NF'^+$ est inclus dans son noyau. En factorisant, on obtient la dernière suite exacte.

Nous en déduisons :

$$\begin{aligned}\dim_2 C \cap N\overline{K}^+/k^2NF^+ &\leqslant \dim_2 C \cap N\overline{K}^+/C' \cap N\overline{K}^+ \\ &\quad + \dim_2 C' \cap N\overline{K}^+/k^2NF'^+ - \dim_2 k^2NF^+/k^2NF'^+ \\ &\leqslant \dim_2 \mathscr{H}_k^{(2)}/P_k + n_2 - \dim_2 \mathrm{Ker}\, \bar{j}P_k/P_k = n_2 + n_3.\end{aligned}$$

On déduit alors des propositions $3a$, b et c l'inégalité : $\dim_2 B^{**}/\pm B^{*2} \leqslant n_1 + n_2 + n_3$. Compte-tenu du corollaire énoncé à la fin du paragraphe 2, nous avons démontré :

Théorème. — *Soient n_1, n_2, n_3 les trois constantes définies par :*

$$\begin{aligned} n_1 &= \dim_{\mathbf{Z}} E_{\overline{K}} - \dim_{\mathbf{Z}} E_k, \\ n_2 &= \dim_2 (E_k^+ \cap N\overline{K})/E_k^2 NE_{\overline{K}}^{\pm}, \\ n_3 &= \dim_2 \mathscr{H}_k^{(2)}/\mathrm{Ker}\, \bar{j}P_k. \end{aligned}$$

Pour toute puissance de 2, notée m, supérieure à 4 et telle que $\mathbf{Q}_0^{(m)}$ soit inclus dans le corps de base k, les différences des m-rangs des groupes $\mathscr{D} = \mathscr{H}_K/j(\mathscr{H}_k)$ et *$\overline{\mathscr{D}} = \mathscr{H}_{\overline{K}}/\bar{j}(\mathscr{H}_k)$ sont majorées par :*

$$\dim_m \mathscr{D} - \dim_m \overline{\mathscr{D}} \leqslant n_1 + n_2 + n_3.$$

4. Deux autres inégalités.

Nous désignerons encore par k un corps de nombres ne contenant pas $\sqrt{-1}$ et par m_0 le plus grand entier tel que $\mathbf{Q}_0^{(m_0)}$ soit inclus dans k. On posera $k' = k(\sqrt{-1})$ et on notera N au lieu de $N_{k'/k}$ la norme dans l'extension k'/k. On désignera par $\mathscr{H}_k$ et $\mathscr{H}_{k'}$ les 2-groupes des classes au sens restreint de k et k' et par j' l'application de $\mathscr{H}_k$ dans $\mathscr{H}_{k'}$ déduite de l'injection canonique du groupe des idéaux de k dans le groupe des idéaux de k'. On notera P_k le sous-groupe de $\mathcal{H}_k$ engendré par les classes d'idéaux principaux au sens ordinaire. On appellera $E_{k'}$ et E_k les groupes d'unités de k' et k. La notation $\dim_{\mathbf{Z}}$ conserve le même sens.

Posons

$$\begin{aligned} n'_1 &= \dim_{\mathbf{Z}} E_{k'} - \dim_{\mathbf{Z}} E_k, \\ n'_2 &= \dim_2 E_k^+ \cap Nk'/E_k^2 NE_{k'}, \\ n'_3 &= \dim_2 \mathcal{H}_k^{(2)}/\operatorname{Ker} j' P_k. \end{aligned}$$

En utilisant des méthodes analogues à celles qui sont développées dans les paragraphes précédents, on obtient :

Proposition 4*a*. — *Pour toute puissance de* 2, *notée* m *et comprise entre* 4 *et* m_0, *on a* :

$$\dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k) \leqslant n'_1 + n'_2 + n'_3 + 1.$$

Si l'on pose

$$n''_1 = \dim_{\mathbf{Z}} E_k \qquad \text{et} \qquad n''_2 = \dim_2 \mathcal{H}_k^{(2)}/P_k,$$

on obtient :

Proposition 4*b*. — *Pour toute puissance de* 2, *notée* m *et comprise entre* 4 *et* m_0, *on a :*

$$\dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k) - \dim_m \mathcal{H}_k \leqslant n''_1 + n''_2.$$

5. Cas particuliers.

Revenons au théorème énoncé au paragraphe 3. Si le corps de base k est 2-principal, la constante n_3 est nulle. Si de plus, on suppose que k est 2-principal au sens restreint et totalement réel, alors $E_k^+ = E_k^2$ et $n_2 = 0$. Il s'en suit :

Proposition 5. — *Supposons que le corps de base* k *soit* 2-*principal (au sens restreint) et totalement réel. Pour toute puissance de* 2, *notée* m, *supérieure à* 4 *et telle que* k *contienne* $\mathbf{Q}_0^{(m)}$, *les différences des* m-*rangs des groupes* $\mathcal{H}_K$ *et* $\mathcal{H}_{\overline{K}}$ *sont majorées par :*

$$\dim_m \mathcal{H}_K - \dim_m \mathcal{H}_{\overline{K}} \leqslant \dim_{\mathbf{Z}} E_{\overline{K}} - \dim_{\mathbf{Z}} E_k.$$

1) *Résultat de Damey-Payan* [2]. Posons $k = \mathbf{Q}$.

Désignons par a un entier sans facteur carré positif. Pour $d = a$, on a :

$$n_1 = \dim_{\mathbf{Z}} \mathrm{E}_{\mathbf{Q}(\sqrt{-a})} - \dim_{\mathbf{Z}} \mathrm{E}_{\mathbf{Q}} = 0$$

et pour $d = -a$, on a :

$$n_1 = \dim_{\mathbf{Z}} \mathrm{E}_{\mathbf{Q}(\sqrt{a})} - \dim_{\mathbf{Z}} \mathrm{E}_{\mathbf{Q}} = 1.$$

On en déduit :

$$0 \leqslant \dim_4 \mathscr{H}_{\mathbf{Q}(\sqrt{-a})} - \dim_4 \mathscr{H}_{\mathbf{Q}(\sqrt{a})} \leqslant 1.$$

En affinant certains détails de la démonstration générale on peut montrer de plus :

Si la norme de l'unité fondamentale de $\mathbf{Q}(\sqrt{a})$ est égale à -1 et si $a \not\equiv 1\ (8)$, alors la différence des 4-rangs des groupes des classes de $\mathbf{Q}(\sqrt{a})$ et $\mathbf{Q}(\sqrt{-a})$ est nulle.

Remarquons que si $a \equiv 1\ (8)$, alors la différence en question peut prendre l'une ou l'autre des valeurs 0 ou 1; (par exemple : $a = 17$ et $a = 3\,161$).

On en déduit qu'il existe une infinité d'entiers a sans facteur carré tels que la différence des 4-rangs des groupes des classes de $\mathbf{Q}(\sqrt{a})$ et $\mathbf{Q}(\sqrt{-a})$ prenne la valeur 0. D'autre part, il existe également une infinité d'entiers a sans facteur carré tels que la différence en question ait pour valeur 1. En effet, lorsque p est premier congru à 1 modulo 8, $\mathbf{Q}(\sqrt{p})$ est 2-principal et le 2-groupe des classes de $\mathbf{Q}(\sqrt{-p})$ est cyclique d'ordre divisible par 4.

2) *Résultat de L. Bouvier* [1]. Posons $k = \mathbf{Q}(\sqrt{2})$. Désignons encore par a un entier sans facteur carré positif. Pour $d = a$ nous aurons : $n_1 = 0$ et pour $d = -a : n_1 = 2$. On en déduit les inégalités suivantes, qui améliorent [1] :

$$0 \leqslant \dim_m \mathscr{H}_{\mathbf{Q}(\sqrt{2}, \sqrt{-a})} - \dim_m \mathscr{H}_{\mathbf{Q}(\sqrt{2}, \sqrt{a})} \leqslant 2,$$

pour $m = 4$ et 8.

Chacune des différences peut donc prendre trois valeurs. Nous nous sommes demandés si les neuf cas existent réellement. Pour cela nous avons programmé le calcul des 4-rangs et 8-rangs des groupes des classes de $\mathbf{Q}(\sqrt{2}, \sqrt{a})$ et $\mathbf{Q}(\sqrt{2}, \sqrt{-a})$

à l'aide de la méthode de Gras [3]. Nous avons mis en évidence huit cas distincts.

Le tableau suivant contient un exemple de chacun d'eux. On trouve sur la même ligne que a, les 4-rangs et les 8-rangs de $\mathbf{Q}(\sqrt{2}, \sqrt{a})$ et $\mathbf{Q}(\sqrt{2}, \sqrt{-a})$.

a	4-rangs	8-rangs	a	4-rangs	8-rangs
3	0 0	0 0	69	0 2	0 0
15	0 1	0 0	257	1 2	0 2
33	0 1	0 1	395	0 2	0 2
65	1 1	0 1	573	0 2	0 1

Pour a variant de 3 à 3 500, il n'existe pas d'exemple où la différence des 4-rangs soit nulle et la différence des 8-rangs égale à 2.

3) *Un exemple où la différence des 4-rangs de* $\mathscr{D}$ *et* $\overline{\mathscr{D}}$ *dépasse* n_1.

La propriété de Damey-Payan présente une grande analogie avec la propriété de Scholtz [6]. De même que nous généralisons ici la première en essayant de remplacer $\mathbf{Q}$ par un corps de base plus général, de même nous avons essayé de généraliser celle de Scholtz. (En fait, on peut même le faire avec le « Spiegelungssatz ». Le problème ne présente d'ailleurs aucune difficulté. La démonstration de Leopoldt se transpose immédiatement. On pourra trouver les détails dans [5]). Le résultat obtenu est le suivant :

Désignons momentanément par :

k un corps de nombres ne contenant pas $\sqrt{-3}$,

d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-3d}$ n'appartiennent à k,

$\mathrm{K} = k(\sqrt{d})$, $\overline{\mathrm{K}} = k(\sqrt{-3d})$, $k' = k(\sqrt{-3})$,

$\mathscr{H}_{\mathrm{K}}$, $\mathscr{H}_{\overline{\mathrm{K}}}$, $\mathscr{H}_{k'}$, $\mathscr{H}_k$ les 3-groupes des classes de K, $\overline{\mathrm{K}}$, k' et k,

j, $\bar{j}$, j' les applications de $\mathscr{H}_k$ dans $\mathscr{H}_{\mathrm{K}}$, $\mathscr{H}_{\overline{\mathrm{K}}}$, $\mathscr{H}_{k'}$ déduites des injections canoniques du groupe des idéaux de k dans les groupes d'idéaux de K, $\overline{\mathrm{K}}$ et k'.

Les notations $\mathrm{E}_{\overline{\mathrm{K}}}$, $\mathrm{E}_{k'}$, E_k, $\dim_{\mathbf{Z}}$ ont toujours la même signification. Nous démontrons dans [5] les inégalités :

(1) $\dim_m \mathscr{H}_{\mathrm{K}}/j(\mathscr{H}_k) - \dim_m \mathscr{H}_{\overline{\mathrm{K}}}/\bar{j}(\mathscr{H}_k) \leqslant \dim_{\mathbf{Z}} \mathrm{E}_{\overline{\mathrm{K}}} - \dim_m \mathrm{E}_k$

(2) $\dim_m \mathscr{H}_k - \dim_m \mathscr{H}_{k'}/j'(\mathscr{H}_k) \leqslant \dim_{\mathbf{Z}} \mathrm{E}_{k'} - \dim_{\mathbf{Z}} \mathrm{E}_k + 1,$

(3) $\dim_m \mathscr{H}_{k'}/j'(\mathscr{H}_k) - \dim_m \mathscr{H}_k \leqslant \dim_{\mathbf{Z}} \mathrm{E}_k,$

pour toute puissance de 3 notée m et, telle que $\mathbf{Q}_0^{(m)}$ soit inclus dans k.

Le théorème du paragraphe 3 est donc l'analogue de l'inégalité (1). Les deux autres inégalités : (2) et (3) correspondent aux propositions $4a$ et b. Il est curieux de constater, que les bornes obtenues ne sont pas les mêmes (alors que dans les propriétés de Damey-Payan et Scholtz, elles coïncidaient). C'est la raison pour laquelle nous avons cherché un exemple où la différence des 4-rangs de $\mathscr{D}$ et $\overline{\mathscr{D}}$ soit strictement supérieure à $n_1 = \dim_{\mathbf{Z}} \mathrm{E}_{\overline{\mathrm{K}}} - \dim_{\mathbf{Z}} \mathrm{E}_k$.

Posons $k = \mathbf{Q}(\sqrt{-2})$. Ce corps est principal. Nous aurons donc $n_3 = 0$, $\mathscr{D} = \mathscr{H}_{\mathrm{K}}$ et $\overline{\mathscr{D}} = \mathscr{H}_{\overline{\mathrm{K}}}$. Prenons pour d un entier sans facteur carré. La constante n_1 vaut alors 1 et n_2 vaut 0 ou 1 suivant les cas :

— Si -1 est norme d'une unité dans $\overline{\mathrm{K}}/k$, alors $n_2 = 0$.

— Si -1 est norme dans $\overline{\mathrm{K}}/k$ sans être norme d'unité, alors $n_2 = 1$.

— Si -1 n'est pas norme dans $\overline{\mathrm{K}}/k$, alors $n_2 = 0$.

Nous avons programmé le calcul de la différence

$$\dim_4 \mathscr{H}_{\mathrm{K}} - \dim_4 \mathscr{H}_{\overline{\mathrm{K}}},$$

à l'aide de la méthode de Gras [3].

Pour $d = 1\,679$ cette différence vaut 2. Signalons que ce fait ne se produit qu'une seule fois, lorsque d varie de 3 à 2 500.

BIBLIOGRAPHIE

[1] L. Bouvier, Sur le 2-groupe des classes de certains corps biquadratiques, 3e cycle, Grenoble.

[2] P. Damey et J. J. Payan, Existence et construction des extensions

galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2, *Jour. für die reine und angew. Math.*, 244 (1970).

[3] G. GRAS, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, *Ann. de l'Institut Fourier*, 23 (1973), 1-48.

[4] H. W. LEOPOLDT, Zur Struktur der l-Klassengruppe galoischer Zahlkörper, *Journ. für die reine und angew. Math.*, 199 (1958), 165-175.

[5] B. ORIAT, Spiegelungssatz, Publications Mathématiques de la Faculté des Sciences de Besançon (1975).

[6] A. SCHOLTZ, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *Jour. für die reine und angew. Math.*, 166 (1931), 201-203.

Manuscrit reçu le 13 avril 1976
Proposé par J. Martinet.

Bernard ORIAT,
Faculté des Sciences
Route de Gray
25030 Besançon Cedex.