J. Math. Soc. Japan
Vol. 30, No. 2, 1978

Sur le nombre de classes de certaines extensions métacycliques sur Q ou sur un corps quadratique imaginaire

par Franz HALTER-KOCH et Nicole MOSER

(Reçu le 25 oct., 1975)
(Revisé le 22 juil., 1977)

Soit K/k_0 une extension galoisienne d'un corps de nombres. On se propose d'étudier le nombre de classes de K, lorsque K/k_0 vérifie les deux conditions suivantes:

——le corps de base k_0 est soit le corps des rationnels, soit un corps quadratique imaginaire.
——le groupe $\mathrm{Gal}(K/k_0)$ est le produit semi-direct d'un sous-groupe distingué d'ordre p premier impair par un sous-groupe isomorphe à $\boldsymbol{Z}/m\boldsymbol{Z}$.

Dans la première partie, nous rappelons brièvement comment obtenir une relation entre régulateurs et nombres de classes de K et de certains de ses sous-corps, d'après les travaux d'E. Artin ([1]) et de R. Brauer ([2]). Puis un assez long calcul nous permet d'évaluer le quotient des régulateurs qui figure dans la relation ci-dessus. Cela nous permet d'écrire une formule où n'apparaissent que des nombres de classes, une puissance de p, et un indice de groupes d'unités, a. Signalons que A. Scholz ([6]) fut le premier à démontrer une formule de ce genre, lorsque $p=3$ et $m=2$; et dans [4], on trouve le résultat pour le cas $2p$. Enfin, le dernier paragraphe est consacré à l'étude de l'indice a: c'est une puissance de p, dont nous donnons un majorant.

Relation entre régulateurs et nombres de classes.

Précisons d'abord quelques notations. Pour tout corps de nombres A, désignons par:

D_A le discriminant absolu,
h_A le nombre de classes,
R_A le régulateur,
s_A le nombre de plongements réels,

$2t_\Lambda$ le nombre de plongements complexes,
U_Λ le groupe des unités de Λ,
V_Λ le sous-groupe de torsion de U_Λ,
et E_Λ le quotient U_Λ/V_Λ.

Supposons d'abord simplement que le corps K soit une extension galoisienne finie d'un corps de nombres k_0, de groupe de Galois G. La formule analytique du nombre de classes donne une relation bien connue entre h_K, la fonction ζ_K, R_K et D_K. Les calculs sur les fonctions "zêta" se ramènent à des calculs sur les fonctions L d'Artin. Grâce à certains entiers, liés aux caractères de G, introduits par E. Artin dans [1], on traite de la même manière les calculs sur les discriminants. On utilise alors le théorème suivant, dû à R. Brauer [2]:

THÉORÈME 1. *Soit G un qroupe fini. Pour tout sous-groupe H de G, on note χ_H^* le caractère de G induit par le caractère trivial χ_H de H. Soit Φ un caractère sur G, à valeurs rationnelles. Alors*

$$\Phi=\sum_{\substack{H \text{ sous-groupe}\\ \text{cyclique de } G}} c_H\chi_H^*$$

où $c_H=\dfrac{\operatorname{Card} H}{\operatorname{Card} G}\times\sum_{\substack{H' \text{ sous-groupe}\\ \text{cyclique de } G \text{ contenant } H}}\mu([H':H])\Phi(z')$, *où μ désigne la fonction de Möbius, et z' un générateur de H'.*

Plaçons-nous maintenant dans le cas où K/k_0 est une extension galoisienne de degré pm, telle que:

——p soit un nombre premier impair,
——m divise $p-1$,
——$G=\mathrm{Gal}(K/k_0)$ soit engendré par deux générateurs σ et τ, liés par les relations

$$\sigma^p=\tau^m=1$$

$$\tau\sigma\tau^{-1}=\sigma^r,$$

où r est une racine primitive m-ième de l'unité modulo p.

On note H le sous-groupe engendré par σ, g_i le sous-groupe engendré par $\sigma^i\tau\sigma^{-i}$, k le sous-corps fixe par H, L_i celui qui est invariant par g_i, et l'on pose $L=L_p$. Grâce au théorème 1, on obtient les relations:

$$\zeta_{k_0}(s)^m\zeta_K(s)=\zeta_L(s)^m\zeta_k(s) \tag{1}$$

et

$$|D_{k_0}|^m|D_K|=|D_L|^m|D_k|. \tag{2}$$

A partir de ces relations, on démontre facilement la proposition suivante:

PROPOSITION 2. *Soit K/k_0 une extension galoisienne non abélienne de degré pm, précisée ci-dessus. Alors*

$$h_K=\frac{h_k h_L^m}{h_{k_0}^m}\times\frac{R_k R_L^m}{R_K R_{k_0}^m}.$$

Calcul du quotient des régulateurs, lorsque G est non abélien d'ordre pm, et que k_0 est soit un corps quadratique imaginaire, soit $\boldsymbol{Q}$.

L'hypothèse sur k_0 que l'on vient d'introduire facilite beaucoup les calculs, car alors $R_{k_0}=1$, le $\boldsymbol{Z}$-rang de E_{k_0} est nul, et l'intersection de deux $\boldsymbol{Z}$-modules E_{L_i} est réduite à 1. Pour poursuivre, il faut distinguer maintenant le cas "K réel" du cas "K imaginaire".

1) *K réel.*

Nécessairement, $k_0=\boldsymbol{Q}$. Les $\boldsymbol{Z}$-modules E_K, E_L, E_k ont respectivement pour rang $pm-1$, $p-1$ et $m-1$. Posons

$$a=(E_K:\ E_L E_{L\sigma}\cdots E_{L\sigma^{m-1}}E_k);$$

cet indice a est à priori fini ou infini. Soit φ le plongement usuel de E_K dans l'espace logarithmique $\boldsymbol{R}^{s_K+t_K}$; l'image de $E_L E_{L\sigma}\cdots E_{L\sigma^{m-1}}E_k$ est un sous-réseau de $\varphi(E_K)$, et d'après le théorème sur les diviseurs élémentaires, le rapport des volumes des parallélépipèdes fondamentaux vaut a. Donc le rapport des régulateurs vaut aussi a. Notons R^* celui de $E_L E_{L\sigma}\cdots E_{L\sigma^{m-1}}E_k$.

$$R^*=aR_K. \tag{3}$$

Soit $\{\varepsilon_1,\cdots,\varepsilon_{p-1}\}$(resp. $\{\eta_1,\cdots,\eta_{m-1}\}$) un système d'unités fondamentales de L (resp. k). Le régulateur R^* est la valeur absolue d'un des mineurs d'ordre $pm-1$ de la matrice:

$$\begin{pmatrix}
ln|\varepsilon_1| & \cdots & ln|\varepsilon_1^{\sigma^{p-1}}| & ln|\varepsilon_1^{\tau}| & \cdots & ln|\varepsilon_1^{\sigma^{p-1}\tau}| & \cdots & ln|\varepsilon_1^{\tau^{m-1}}| & \cdots & ln|\varepsilon_1^{\sigma^{p-1}\tau^{m-1}}| \\
\vdots & & & & & & & & & \\
ln|\varepsilon_{p-1}| & \cdots & ln|\varepsilon_{p-1}^{\tau}| & \cdots & ln|\varepsilon_{p-1}^{\sigma^{p-1}\tau}| & \cdots & & & & ln|\varepsilon_{p-1}^{\sigma^{p-1}\tau^{m-1}}| \\
ln|\varepsilon_1^{\sigma}| & \cdots & ln|\varepsilon_1^{\tau\sigma}| & \cdots & ln|\varepsilon_1^{\sigma^{p-1}\tau\sigma}| & \cdots & & & & ln|\varepsilon_1^{\sigma^{p-1}\tau^{m-1}\sigma}| \\
\vdots & & \vdots & & & & & & & \\
ln|\varepsilon_{p-1}^{\sigma^{m-1}}| & \cdots & ln|\varepsilon_{p-1}^{\tau\sigma^{m-1}}| & \cdots & & & & & & ln|\varepsilon_{p-1}^{\sigma^{p-1}\tau^{m-1}\sigma^{m-1}}| \\
ln|\eta_1| & & \vdots & & & & & & & \vdots \\
\vdots & & & & & & & & & \\
ln|\eta_{m-1}| & \cdots & ln|\eta_{m-1}^{\tau}| & \cdots & & & & & & ln|\eta_{m-1}^{\sigma^{p-1}\tau^{m-1}}|
\end{pmatrix}$$

(les exposants des unités sont lus de droite à gauche).

Les η_i sont fixes par σ, et les ε_i par τ. Posons

$$E_i=\begin{pmatrix} ln|\varepsilon_1^{\sigma^i}| \\ \vdots \\ ln|\varepsilon_{p-1}^{\sigma^i}| \end{pmatrix},\ 0\leqq i\leqq p-1,\quad\text{et}\quad F_j=\begin{pmatrix} ln|\eta_1^{\tau^j}| \\ \vdots \\ ln|\eta_{m-1}^{\tau^j}| \end{pmatrix},\ 0\leqq j\leqq m-1.$$

La matrice s'écrit:

$$\begin{pmatrix} E_0 & \cdots E_{p-1} & E_0 & \cdots E_{p-1} & \cdots E_0 & \cdots E_{p-1} \\ E_1 & \cdots E_0 & E_r & \cdots E_{r+p-1} & \cdots E_{rm-1} & \cdots E_{rm-1+p-1} \\ \vdots & & & & & \\ E_{m-1} & \cdots E_{m-1+p-1} & E_{(m-1)r} & \cdots E_{(m-1)r+p-1} & \cdots E_{(m-1)rm-1} & \cdots E_{(m-1)rm-1+p-1} \\ F_0 & \cdots F_0 & F_1 & \cdots F_1 & \cdots F_{m-1} & \cdots F_{m-1} \end{pmatrix}.$$

Supprimons la p-ième colonne pour obtenir R^*. Sur chaque autre colonne d'indice multiple de p, ajoutons les $p-1$ colonnes précédentes, en remarquant que $E_0+E_1+\cdots+E_{p-1}=0$. En regroupant les 0, il vient

$$R^*=\left|\det\begin{pmatrix} E_0 & \cdots E_{p-2} & \cdots E_0 & \cdots E_{p-2} \cdots & 0 \cdots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \quad \vdots \\ E_{m-1} & \cdots E_{m-1+p-2} & \cdots E_{(m-1)rm-1} & \cdots E_{(m-1)rm-1+p-2} & 0 \cdots 0 \\ F_0 & \cdots F_0 & \cdots F_{m-1} & \cdots F_{m-1} \cdots & pF_1 \cdots pF_{m-1} \end{pmatrix}\right|.$$

En effectuant le produit par blocs, on obtient:

$$R^*=p^{m-1}R_k\Delta_1 \tag{4}$$

$$\text{avec } \Delta_1=\left|\det\begin{pmatrix} E_0 & \cdots E_{p-2} & \cdots E_0 & \cdots E_{p-2} \\ E_{m-1} & \cdots E_{m-1+p-2} & \cdots E_{(m-1)rm-1} & \cdots E_{(m-1)rm-1+p-2} \end{pmatrix}\right|.$$

Le déterminant Δ_1 ne dépend plus que du corps L. On le calcule en effectuant des réductions successives, grâce au lemme suivant qui se démontre facilement:

LEMME 3. *Soient n un entier, $c_1, \cdots, c_n$ n colonnes de $n-1$ réels telles que*

$$c_1+c_2+\cdots+c_n=(0).$$

Alors $\det(c_1-c_2, c_2-c_3, \cdots, c_{n-1}-c_n)=n\det(c_1, \cdots, c_{n-1})$.

Pour préciser la méthode utilisée, donnons la première réduction: Δ_1 est composé de m blocs, ayant tous la même première ligne; conservons le premier bloc, et à chacun des autres, retranchons colonne à colonne le précédent. Comme la première colonne de chaque bloc détermine celui-ci, nous l'écrirons seule. On obtient:

$$\Delta_1=R_L\Delta_2 \tag{5}$$

$$\text{avec } \Delta_2=\left|\det\begin{pmatrix} E_r-E_1 & E_{r2}-E_r & \cdots E_{rm-1}-E_{rm-2} \\ E_{2r}-E_2 & E_{2r2}-E_{2r} & \cdots E_{2rm-1}-E_{2rm-2} \\ \vdots & \vdots & \\ E_{(m-1)r}-E_{m-1} & E_{(m-1)r2}-E_{(m-1)r} & \cdots E_{(m-1)rm-1}-E_{(m-1)rm-2} \end{pmatrix}\right|.$$

Effectuons le changement de variable

$$A_\lambda^{i,l}=E_{\lambda+lr^{i-1}(r-1)}-E_\lambda,$$

avec $1\leqq i\leqq m-1$ et $1\leqq l\leqq m-1$.

Le déterminant Δ_2 s'écrit en fonction des $A_\lambda^{i,l}$:

$$\Delta_2=\left|\det\begin{pmatrix} A_1^{1,1} & A_r^{2,1} & \cdots & A_{r^{m-2}}^{m-1,1} \\ A_2^{1,2} & A_{2r}^{2,2} & \cdots & A_{2r^{m-2}}^{m-1,2} \\ \vdots & \vdots & & \vdots \\ A_{m-1}^{1,m-1} & A_{(m-1)r}^{2,m-1} & \cdots & A_{(m-1)r^{m-2}}^{m-1,m-1} \end{pmatrix}\right|.$$

C'est une forme analogue à celle de Δ_1. On obtient ainsi

$$\Delta_i=p^{i-1}\Delta_{i+1}R_L \tag{6}$$

$$1\leqq i\leqq m$$

$$\Delta_{m+1}=1.$$

En regroupant les formules (3), (4), (5) et (6), on trouve l'égalité

$$R^*=R_kR_L^m\,p^{(m-1)+1+2+\cdots+m-1}.$$

D'où

$$h_K=a\frac{h_kh_L^m}{p^{\frac{(m-1)(m+2)}{2}}}. \tag{7}$$

2) *K imaginaire, $k_0=\boldsymbol{Q}$.*

Dans ce cas, m est pair ; posons $m=2n$, et $q=\dfrac{p-1}{2}$. Les rangs des $\boldsymbol{Z}$-modules E_K, E_L et E_k valent respectivement $pn-1$, q et $n-1$; l'indice $a=(E_K\colon E_LE_{L\sigma}\cdots E_{L\sigma^{m-1}}E_k)$ peut donc être fini. Notons R^* le régulateur de $E_LE_{L\sigma}\cdots E_{L\sigma^{m-1}}E_k$; comme dans le cas réel,

$$R^*=aR_K. \tag{8}$$

Désignons par $\{\varepsilon_1,\cdots,\varepsilon_q\}$ (resp. $\{\eta_1,\cdots,\eta_{n-1}\}$) un système d'unités fondamentales de L (resp. k). Comme L admet un plongement réel, supposons $\varepsilon_1,\cdots,\varepsilon_q$ réels. D'autre part, la restriction de la conjugaison complexe à K est τ^n ; on vérifie que les isomorphismes $\sigma^i\tau^j$, pour $0\leqq i\leqq p-1$, et $0\leqq j\leqq n-1$, constituent un système exact de représentants modulo la conjugaison complexe. Le régulateur R^* est donc la valeur absolue d'un des mineurs d'ordre $pn-1$ de la matrice

$$\begin{pmatrix} 2ln|\varepsilon_1| & \cdots & 2ln|\varepsilon_1^{\sigma^{p-1}}| & 2ln|\varepsilon_1^{\tau}| & \cdots & 2ln|\varepsilon_1^{\sigma^{p-1}\tau}| & \cdots & 2ln|\varepsilon_1^{\tau^{n-1}}| & \cdots & 2ln|\varepsilon_1^{\sigma^{p-1}\tau^{n-1}}| \\ \vdots & & \vdots & \vdots & & \vdots & & & & \vdots \\ 2ln|\varepsilon_q^{\sigma^{m-1}}| & \cdots & 2ln|\varepsilon_q^{\tau\sigma^{m-1}}| & \cdots & 2ln|\varepsilon_q^{\sigma^{p-1}\tau\sigma^{m-1}}| & \cdots & & 2ln|\varepsilon_q^{\sigma^{p-1}\tau^{n-1}\sigma^{m-1}}| & & \\ 2ln|\eta_1| & \cdots & 2ln|\eta_1^{\tau}| & \cdots & 2ln|\eta_1^{\sigma^{p-1}\tau}| & \cdots & & 2ln|\eta_1^{\sigma^{p-1}\tau^{n-1}}| & & \\ \vdots & & \vdots & & \vdots & & & \vdots & & \\ 2ln|\eta_{n-1}| & \cdots & 2ln|\eta_{n-1}^{\tau}| & & \cdots & & & 2ln|\eta_{n-1}^{\sigma^{p-1}\tau^{n-1}}| & & \end{pmatrix}.$$

Les η_i sont fixes par σ, et les ε_i par τ. Notons E_i la matrice-colonne

$\begin{pmatrix} ln|\varepsilon_1^{\sigma^i}| \\ ln|\varepsilon_2^{\sigma^i}| \\ \cdots \\ ln|\varepsilon_q^{\sigma^i}| \end{pmatrix}$ et F_i la matrice-colonne $\begin{pmatrix} 2ln|\eta_1^{\tau^i}| \\ 2ln|\eta_2^{\tau^i}| \\ \vdots \\ 2ln|\eta_{n-1}^{\tau^i}| \end{pmatrix}$. Comme $r^n \equiv -1$ modulo p, $\tau^n\sigma^i=\sigma^{-i}\tau^n$, et $E_i^{\tau^n}=E_i=E_{p-i}$. Avec ces notations,

$$R_k=|\det(F_0, F_1, \cdots, F_{n-2})|,$$

$$R_L=|\det(E_0, 2E_1, \cdots, 2E_{q-1})|=|\det(2E_1, 2E_2, \cdots, 2E_q)|,$$

et la matrice s'écrit:

$$\begin{pmatrix} 2E_0 & 2E_1 & \cdots & 2E_{p-1} & 2E_0 & \cdots & 2E_0 & \cdots & 2E_{p-1} \\ 2E_1 & 2E_2 & & 2E_0 & 2E_r & \cdots & 2E_{rn-1} & \cdots & 2E_{rn-1+p-1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 2E_{m-1} & 2E_m & \cdots & 2E_{m-1+p-1} & 2E_{(m-1)r} & \cdots & 2E_{(m-1)r^{n-1}} & \cdots & 2E_{(m-1)r^{n-1}+p-1} \\ F_0 & F_0 & \cdots & F_0 & F_1 & \cdots & F_{n-1} & \cdots & F_{n-1} \end{pmatrix}.$$

Supprimons la première colonne; sur chaque autre colonne d'indice congru à 1 modulo p, ajoutons les $p-1$ colonnes suivantes, en remarquant que $E_0+E_1+\cdots+E_{p-1}=0$. En regroupant les zéros, on obtient:

$$R^*=\left|\det\begin{pmatrix} 2E_1 & \cdots & 2E_{p-1} & 2E_1 & \cdots & 2E_{p-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 2E_m & \cdots & 2E_{m-1+p-1} & 2E_{(m-1)r+1} & \cdots & 2E_{(m-1)r^{n-1}+p-1} & 0 & \cdots & 0 \\ F_0 & \cdots & F_0 & F_1 & \cdots & F_{n-1} & pF_1 & \cdots & pF_{n-1} \end{pmatrix}\right|.$$

Donc

$$R^*=p^{n-1}R_k\Delta_1 \tag{9}$$

avec

$$\Delta_1=\left|\det\begin{pmatrix} 2E_1 & 2E_{p-1} & 2E_1 & \cdots & 2E_{p-1} & \cdots & 2E_{p-1} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 2E_m & \cdots & 2E_{m-1+p-1} & 2E_{(m-1)r+1} & \cdots & 2E_{(m-1)r+p-1} & \cdots & 2E_{(m-1)r^{n-1}+p-1} \end{pmatrix}\right|.$$

De nouveau, le déterminant Δ_1 ne dépend que de L; c'est la juxtaposition de n blocs de largeur $p-1$, de hauteur $m\times q$. A chaque bloc (à partir du deuxième), retranchons le premier bloc, colonne par colonne. Dans le premier bloc, retranchons à la colonne commençant par E_{q+i} $(1\leqq i\leqq q)$ celle commençant par E_{q+1-i}. Comme $E_{q+i}=E_{q+1-i}$, on obtient:

$$\Delta_1=R_L\Delta_2 \tag{10}$$

avec

$$\Delta_2=$$
$$\left|\det\begin{pmatrix} 2E_{q+2}-2E_{q+1} & \cdots 2E_0-2E_2 & 2E_{r+1}-2E_2 & \cdots 2E_{rn-1+p-1}-2E_0 \\ \vdots & & & \\ 2E_{q+m}-2E_{q+m-1} & \cdots 2E_{m-2}-2E_m & 2E_{(m-1)r+1}-2E_m & \cdots 2E_{(m-1)rn-1+p-1}-2E_{m-2} \end{pmatrix}\right|.$$

Pour les réductions suivantes, nous utiliserons les lemmes ci-dessous:

LEMME 4. *Soient* $E_0, E_1, \cdots, E_q$, $q+1$ *colonnes de* q *réels tels que* $E_0+2E_1+\cdots+2E_q=0$. *Posons* $p=2q+1$. *Alors*

$$|\det[2E_0-2E_1, 2E_1-2E_2, \cdots, 2E_{q-1}-2E_q]|=p|\det[E_0, 2E_1, \cdots, 2E_{q-1}]|$$
$$=|\det[2E_{q-1}-2E_{q-2}, 2E_{q-2}-2E_{q-3}, \cdots, 2E_1-2E_0, 2E_0-2E_q]|.$$

LEMME 5. *Soient* p *un entier impair,* $A_0, A_1, \cdots, A_{p-1}$, p *colonnes de* $q=\dfrac{p-1}{2}$ *réels tels que* $A_0=0$ *et* $A_i=A_{p-i}$, *pour* $1\leqq i\leqq p-1$. *Alors*

$$|\det(A_1-A_0, A_2-A_1, \cdots, A_q-A_{q-1})|=|\det(A_1, A_2, \cdots, A_q)|.$$

LEMME 6. *Soient* p *un entier impair,* $B_0, B_1, \cdots, B_{p-1}$, p *colonnes de* $q=\dfrac{p-1}{2}$ *réels tels que* $B_0+B_1+\cdots+B_{p-1}=0$ *et que* $B_i=B_{p-i}$. *Alors*

$$|\det(B_1-B_0, B_2-B_1, \cdots, B_q-B_{q-1})|=p|\det(B_1, B_2, \cdots, B_q)|.$$

La première ligne du premier bloc de Δ_2 s'écrit à l'aide de différences $2E_l-2E_j$, avec $2\leqq j\leqq q+1$, et $l+j=p+2$. Donc

$$2E_l-2E_j=2E_{p+2-j}-2E_j=2E_{j-2}-2E_j.$$

On vérifie que toutes les différences du type $2E_{j-2}-2E_j$ pour $0\leqq j\leqq p-1$, figurent, au signe près, dans l'ensemble $\{2E_{j-2}-2E_j,\ 2\leqq j\leqq q+1\}$. Comme 2 est inversible modulo p, on peut annuler la première ligne de tous les blocs de Δ_2, à partir du deuxième, en retranchant des sommes de $(2E_{j-2}-2E_j)$. En utilisant le lemme 4, il vient

$$\Delta_2=pR_L\Delta_3. \tag{11}$$

Les lemmes 5 et 6 permettent de poursuivre les réductions, et l'on arrive à l'égalité

$$R^*=R_kR_L^mp^{n-1+\alpha},$$

où α est la somme des entiers impairs inférieurs à m. D'où

$$h_K=a\frac{h_kh_L^m}{p^{\frac{m^2+2m-4}{4}}}. \tag{12}$$

3) *K imaginaire et* k_0 *quadratique imaginaire.*

Dans ce dernier cas, les $\boldsymbol{Z}$-rangs de E_K, E_L et E_k sont respectivement de

$pm-1$, $p-1$ et $m-1$. Posons $a=(E_K : E_L E_{L\sigma} \cdots E_{L\sigma^{m-1}} E_k)$. On a encore, si R^* désigne le régulateur de $E_L E_{L\sigma} \cdots E_{L\sigma^{m-1}} E_k$,

$$R^* = aR_K .$$

Comme la restriction à k_0 de la conjugaison complexe correspond au $\boldsymbol{Q}$-isomorphisme non trivial de k_0, pour écrire R^*, il suffit de considérer les plongements de K de la forme $\sigma^i\tau^j$, $0 \leqq i \leqq p-1$ et $0 \leqq j \leqq m-1$. En posant

$$E_i = \begin{pmatrix} 2ln|\varepsilon_1^{\sigma^i}| \\ \vdots \\ 2ln|\varepsilon_{p-1}^{\sigma^i}| \end{pmatrix} \quad \text{et} \quad F_j = \begin{pmatrix} 2ln|\eta_1^{\tau^j}| \\ \vdots \\ 2ln|\eta_{m-1}^{\tau^j}| \end{pmatrix}$$

R^* est identique au R^* calculé pour le cas réel. On obtient donc

$$h_K = a \frac{h_k h_L^m}{h_{k_0}^m p^{\frac{(m-1)(m+2)}{2}}} . \tag{13}$$

Rassemblons les résultats (7), (12) et (13) dans l'énoncé suivant :

THÉORÈME 7. *Soit K/k_0 une extension "diédrale" de degré pm de k_0, corps quadratique imaginaire ou corps des rationnels. Alors*

$$h_K = a \frac{h_k h_L^m}{h_{k_0}^m} \times \frac{1}{p^b} ,$$

où $a=(E_K : E_L E_{L\sigma} \cdots E_{L\sigma^{m-1}} E_k)$, et où b est un entier qui vaut $\frac{(m-1)(m+2)}{2}$ si K est réel ou k_0 quadratique imaginaire, et $\frac{m^2+2m-4}{4}$ lorsque K est une extension imaginaire de $\boldsymbol{Q}$.

Evaluation de l'indice a.

Dans ce paragraphe, nous conservons les hypothèses du Théorème 7. En plus des notations définies dans la première partie, désignons par

H_Λ le groupe des idéaux principaux (fractionnaires) du corps de nombres algébriques Λ,

$$U_{K/k} = \{\varepsilon \in U_K \mid N_{K/k}\varepsilon = 1\}$$

et

$$E_{K/k} = U_{K/k} \cdot V_K / V_K .$$

Il est clair que $V_K = V_k$, et que si v est un entier valant 1 lorsque k contient les racines p-ièmes de l'unité, et 0 sinon, le groupe $U_{K/k} \cap V_k$ possède p^v éléments.

Supposons $k_0 \neq \boldsymbol{Q}(\sqrt{-3})$, ou $k_0 = \boldsymbol{Q}(\sqrt{-3})$ er $p \neq 3$. Alors comme $E_{L\sigma^\nu}$ se plonge naturellement dans $E_{K/k'}$ et l'on définit

$$a_0=\left(E_{K/k}:\prod_{\nu=0}^{m-1}E_{L\sigma^\nu}\right).$$

L'indice a peut alors s'écrire :

$$a=a_0\cdot(E_K:E_{K/k}\cdot E_k).$$

Il suffit d'appliquer les résultats de M. Rosen ([**5**]) pour obtenir la structure de $E_{K/k}$. Soient ζ une racine primitive p-ième de l'unité, R l'anneau $\boldsymbol{Z}[\zeta]$, et R_0 le sous-anneau de R fixe par l'isomorphisme ψ défini par $(\zeta\mapsto\zeta^r)$. Alors $A=\boldsymbol{Z}[G]/(1+\sigma+\cdots+\sigma^{p-1})$ est isomorphe à l'algèbre à produit croisé $R[\langle\tau\rangle]$; $E_{K/k}$ est un A-module sans torsion, donc il existe un isomorphisme de A-modules :

$$E_{K/k}\cong\bigoplus_{i=1}^{s}(1-\zeta)^{\varepsilon_i}\mathfrak{a}_iR\,,$$

où s est un entier qui vaut m si K est réel ou $k_0\neq\boldsymbol{Q}$, et $m/2$ si K est imaginaire et $k_0=\boldsymbol{Q}$; les $\mathfrak{a}_i$ sont des idéaux de R_0, et les ε_i sont des entiers vérifiant $0\leqq\varepsilon_i<m$. Dans cet isomorphisme, l'action de σ correspond à la multiplication par ζ, et l'action de τ à celle de ψ. On obtient ainsi l'isomorphisme :

$$E_L\cong\bigoplus_{i=1}^{s}\mathfrak{P}^{\tilde{\varepsilon}_i}\mathfrak{a}_i\,,$$

où $\mathfrak{P}=(1-\zeta)R\cap R_0$, et où $\tilde{\varepsilon}_i=\begin{cases}0 \text{ si } \varepsilon_i=0\\ 1 \text{ si } \varepsilon_i>0\end{cases}$. De plus,

$$E_{K/k}/\prod_{\nu=0}^{m-1}E_{L\sigma^\nu}\cong\bigoplus_{i=1}^{s}(1-\zeta)^{\tilde{\varepsilon}_i}R/\mathfrak{P}^{\tilde{\varepsilon}_i}R\,;$$

c'est un p-groupe abélien élémentaire, d'ordre $p^{\sum_{i=1}^{s}\delta_i}$, où

$\delta_i=\begin{cases}0 & \text{si } \varepsilon_i=0\\ m-\varepsilon_i & \text{si } \varepsilon_i>0\end{cases}$. Ceci implique

$$a_0=\prod_{i=1}^{s}p^{\delta_i}\leqq p^{s(m-1)}.$$

Pour obtenir l'interprétation des nombres δ_i (resp. ε_i) en termes de groupes d'unités, désignons par r_j le nombre d'indices $i\in\{1,\cdots,s\}$ pour lesquels $1\leqq\varepsilon_i\leqq j$; on vérifie que p^{r_j} est l'ordre du p-groupe abélien élémentaire $E_L^{(1-\sigma)^j}\cap E_{K/k}^p/E_L^{p(1-\sigma)^j}$, et que, si $j>1$, on a :

$$p^{r_j-r_{j-1}}=(E_L^{(1-\sigma)^j}\cap E_{K/k}^p:E_L^{(1-\sigma)^j}\cap E_{K/k}^{p(1-\sigma)}).$$

Avant d'utiliser cette remarque pour préciser r_1, démontrons le résultat suivant :

LEMME 8. *Soient $\varepsilon\in U_{K/k}$, $\gamma\in K^*$ et $\omega\in k^*$ tels que $\varepsilon^{1-\sigma}=\gamma^p\omega$; alors on peut trouver un entier d premier à p, et un entier u tels que $N_{K/k}(\gamma)^u=\omega^d$.*

DÉMONSTRATION: Appliquons $(1-\sigma)^{p-2}$ à $\varepsilon^{1-\sigma}=\gamma^p\omega$; comme $(1-\sigma)^{p-1}=p\lambda+\sum_{\nu=0}^{p-1}\sigma^\nu$, où $\lambda\in\boldsymbol{Z}[\langle\sigma\rangle]$ est un élément inversible de $\boldsymbol{Z}_p[\langle\sigma\rangle]$, (cf. [3], p. 30),

$$\varepsilon^{p\lambda}=\gamma^{p(1-\sigma)^{p-2}};$$

choisissons $\lambda'\in\boldsymbol{Z}[\langle\sigma\rangle]$ et $d\in\boldsymbol{Z}$ de sorte que $(p, d)=1$ et que $\lambda\lambda'=d$, extrayons les racines p-ièmes, et appliquons $\lambda'(1-\sigma)$; on obtient ainsi:

$$\varepsilon^{d(1-\sigma)}=\gamma^{\lambda'(1-\sigma)^{p-1}}=\gamma^{dp}\cdot N_{K/k}(\gamma^{\lambda'}).$$

Comme $\lambda'\in\boldsymbol{Z}[\langle\sigma\rangle]$, il existe un entier u tel que

$$N_{K/k}(\gamma^{\lambda'})=N_{K/k}(\gamma^u) \quad \text{et} \quad N_{K/k}(\gamma)^u=\omega^d. \qquad \text{C. Q. F. D.}$$

Considérons maintenant les groupes d'idéaux $H_{K,0}=\{(\alpha)\in H_K\,|\,(\alpha)^\sigma=(\alpha)\}$, et $H_{L,0}=H_L\cap H_{K,0}$. Si $(\alpha)\in H_{L,0}$, alors $(\alpha^p)=(N_{L/k_0}(\alpha))\in H_{k_0}$, donc il existe $\varepsilon\in U_L$ et $\mu\in k_0^*$ tels que $\alpha^p=\mu\varepsilon$. Posons $\Phi(\alpha)=\varepsilon^{1-\sigma}$; nous obtenons le résultat suivant:

PROPOSITION 9. *Φ induit un épimorphisme*

$$\tilde{\Phi}: H_{L,0}/H_{k_0}\longrightarrow E_L^{1-\sigma}\cap E_{K/k}^p/E_L^{p(1-\sigma)}.$$

Si $L=k_0(\sqrt[p]{\beta})$, avec $\beta\in k_0$, le noyau de $\tilde{\Phi}$ est un groupe d'ordre p, engendré par $(\sqrt[p]{\beta})\cdot H_{k_0}$. Sinon, $L^p\cap k_0=k_0^p$, et $\tilde{\Phi}$ est un isomorphisme.

DÉMONSTRATION: On vérifie sans problème que Φ induit un homomorphisme $\tilde{\Phi}: H_{L,0}/H_{k_0}\to E_L^{1-\sigma}\cap E_{K/k}^p/E_L^{p(1-\sigma)}$. Pour déterminer le noyau de $\tilde{\Phi}$, choisissons $(\alpha)\in H_{L,0}$ tel que $\alpha^p=\mu\varepsilon$ et $\varepsilon^{1-\sigma}=\gamma_0^{p(1-\sigma)}\omega$, avec $\mu\in k_0^*$, $\varepsilon\in U_L$, $\gamma_0\in U_L$, $\omega\in V_k$. Comme $N_{K/k}(\omega)=1$, ω est une racine p-ième de l'unité; mais $\alpha^{p(1-\sigma)}=\varepsilon^{1-\sigma}=\gamma_0^{p(1-\sigma)}\omega$, donc $\omega=1$ et $(\alpha\gamma_0^{-1})^p\in k\cap L=k_0$. Si $L^p\cap k_0=k_0^p$, $\alpha\gamma_0^{-1}\in k_0$, et $(\alpha)\in H_{k_0}$; si $L=k_0(\sqrt[p]{\beta})$, il est clair que $(\sqrt[p]{\beta})H_{k_0}$ engendre le noyau de $\tilde{\Phi}$.

Reste à démontrer la surjectivité: choisissons $\varepsilon\in U_L$ et $\gamma\in U_{K/k}$ tels que $\varepsilon^{1-\sigma}=\gamma^p\omega$; alors il existe $\delta\in K^*$ tel que $\delta^{1-\sigma}=\gamma$, et d'après lemme 8, $\omega=1$. Il suffit de poser $\mu=N_{K/L}(\varepsilon\delta^{-p})^{(p-1)/m}$ et $\alpha=\varepsilon\cdot N_{K/L}(\delta)^{-(p-1)/m}$ pour obtenir le résultat cherché: $\alpha^p=\mu\varepsilon$, avec $\mu\in k_0$ et $\alpha\in L$. C. Q. F. D.

La proposition 9 conduit à l'estimation suivante pour l'indice a: lorsque $k_0\neq\boldsymbol{Q}(\sqrt{-3})$, ou $k_0=\boldsymbol{Q}(\sqrt{-3})$ et $p\neq3$:

THÉORÈME 10. *$a=p^{\alpha+w}$, où $0\leqq\alpha\leqq s(m-1)$ et où*

$$w=\begin{cases} 1 & \text{si } K=k(\sqrt[p]{u}),\ \text{avec } u \text{ unité de } k,\\ 0 & \text{sinon}.\end{cases}$$

DÉMONSTRATION: Il est suffisant de vérifier que

$$(*) \qquad p^{r_1}\leqq p^{w-v}\,|H_{K,0}/H_k|;$$

en effet, dans ce cas, on a:

$$p^{r_1}\leqq p^{1+w-v}(U_k: N_{K/k}U_K),$$

grâce à l'isomorphisme $H_{K,0}/H_k \cong H^1(\langle\sigma\rangle, U_K)$, et à la relation $|H^1(\langle\sigma\rangle, U_K)| = p(U_k : N_{K/k}U_K)$ (voir [7]). D'autre part,

$$a_0 \leqq p^{r_1(m-1)+(s-r_1)(m-2)},$$

et d'après (*),

$$(E_K : E_{K/k}E_k) = (U_K : U_{K/k}U_k) = \frac{p^{s+v-1}}{(U_k : N_{K/k}U_K)} \leqq p^{s-r_1+w}.$$

Donc on obtient :

$$a = a_0(E_K : E_{K/k}E_k) \leqq p^{s(m-1)+w}.$$

Pour démontrer (*), observons d'abord que le plongement de H_L dans H_K induit un monomorphisme de $H_{L,0}/H_{k_0}$ dans $H_{K,0}/H_k$; distinguons alors quatre cas :

1) Si $v=0$, alors $w=0$, L n'est pas de la forme $k_0(\sqrt[p]{\beta})$, avec $\beta \in k_0$, donc

$$p^{r_1} = |H_{L,0}/H_{k_0}| \leqq |H_{K,0}/H_k|.$$

2) Si $v=1$ et $L=k_0(\sqrt[p]{\beta})$, avec β dans k_0, alors β ne peut être une unité de k_0 ; (sinon β serait une racine de l'unité et L/k_0 serait galoisienne, ce qui est en contradiction avec l'hypothèse). On obtient $K=k(\sqrt[p]{\beta})$, et comme p ne divise pas $[k : k_0]$, β ne peut être remplacé par une unité de k, si bien que $w=0$. La proposition 9 implique alors :

$$p^{r_1} = p^{-1}|H_{L,0}/H_{k_0}| \leqq p^{-1}|H_{K,0}/H_k|.$$

3) Si $v=1$, si L n'est pas de la forme $k_0(\sqrt[p]{\beta})$, avec β élément de k_0, et si $w=0$, alors $K=k(\sqrt[p]{u})$ et $(\sqrt[p]{u}) \notin H_k$;

$$u^r = u^i y^p \quad \text{avec} \quad y \in k,\ i \not\equiv 1 \bmod p,$$

et ainsi, $(\sqrt[p]{u})$ appartient à $H_{K,0}$ sans appartenir à $H_{L,0}H_k$; cela conduit à l'inégalité :

$$p^{r_1} = |H_{L,0}/H_{k_0}| \leqq p^{-1}|H_{K,0}/H_k|.$$

4) Si $v=w=1$, alors d'après 2), L n'est pas de la forme $k_0(\sqrt[p]{\beta})$ avec β dans k_0, et grâce à la proposition 9 on obtient

$$p^{r_1} = |H_{L,0}/H_{k_0}| \leqq |H_{K,0}/H_k|,$$

ce qui termine la démonstration. C. Q. F. D.

REMARQUE. Le théorème 10 est encore valable pour $k_0=\boldsymbol{Q}(\sqrt{-3})$ er $p=3$, mais la démonstration demande d'autres méthodes.

Bibliographie

[1] E. Artin, Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, J. Reine Angew. Math., **164** (1931), 1-11.
[2] R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpers, Math. Nachr., **4** (1951), 158-174.
[3] G. Gras, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, Ann. Inst. Fourier, **23** (1973), 1-48.
[4] N. Moser, Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbf{Q}$, Sém. th. Nb. Grenoble, 1974.
[5] M. Rosen, Representations of Twisted Group Rings, Ph. D. Thesis, Princeton, 1963.
[6] A. Scholz, Idealklassen und Einheiten in kubischen Körpern, Monat. Math. Phys., **40** (1933), 211-222.
[7] H. Yokoi, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31-44.

Franz HALTER-KOCH
Universität Essen-Gesamthochschule
Fachbereich 6
43 Essen
Unionstrasse 2
West Germany

Nicole MOSER
Institut Fourier
Laboratoire associé au C.N.R.S.
BP 116
38402 St Martin D'Heres
France