J. Math. Soc. Japan
Vol. 26, No. 4, 1974

Sur les l-classes d'idéaux des extensions non galoisiennes de $\boldsymbol{Q}$ de degré premier impair l a clôture galoisienne diédrale de degré $2l$

Par Georges GRAS

(Reçu le 31 mai, 1973)
(Revisé le 3 oct, 1973)

Introduction.

Dans [3], S. Kobayashi donne une intéressante construction du groupe de Galois de l'extension abélienne non ramifiée maximale d'exposant 3 du corps $\boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{m})$, pour certains $m \in \boldsymbol{Z}$. La valeur du 3-rang du groupe des classes de $\boldsymbol{Q}(\sqrt[3]{m})$ est alors une conséquence de l'étude de ce groupe de Galois.

Les résultats de Kobayashi suggèrent l'existence de relations entre les l-rangs des groupes des classes d'une extension de degré l de $\boldsymbol{Q}$ non galoisienne et de sa clôture galoisienne, lorsque celle-ci est diédrale de degré $2l$. C'est ce que nous essayons de préciser dans cette note.

Je tiens à remercier ici S. Kobayashi qui m'a communiqué ses résultats avant leur parution et le Professeur S. Iyanaga auquel je dois cet échange.

§ 1. Généralités.

Soit $L/\boldsymbol{Q}$ une extension de degré l de $\boldsymbol{Q}$ (l premier impair) non galoisienne, ayant une clôture galoisienne K diédrale de degré $2l$ sur $\boldsymbol{Q}$. On notera σ et τ des générateurs de $G = \mathrm{Gal}(K/\boldsymbol{Q})$ vérifiant les relations :

$$\sigma^l = \tau^2 = 1 \qquad \text{et} \qquad \sigma\tau = \tau\sigma^{-1}.$$

Soient $H = \langle\sigma\rangle$ et $T = \langle\tau\rangle$ les sous-groupes de G engendrés par σ et τ. On note k le sous-corps de K fixe par H (c'est une extension quadratique de $\boldsymbol{Q}$) ; on peut supposer que L est fixe par T (les l conjugués L_i de L (i défini modulo l) sont fixes par les sous-groupes $\{1, \sigma^i\tau\sigma^{-i}\}$) ; enfin la restriction de τ à k définit l'élément d'ordre 2 de $\mathrm{Gal}(k/\boldsymbol{Q})$.

On note A_L, A_k et A_K les anneaux d'entiers de L, k et K, $\mathfrak{I}(L)$, $\mathfrak{I}(k)$ et $\mathfrak{I}(K)$ les groupes des idéaux fractionnaires de L, k et K, $\mathcal{H}(L)$, $\mathcal{H}(k)$ et $\mathcal{H}(K)$ les l-groupes des classes des corps L, k et K. On note j l'homomorphisme canonique $\mathcal{H}(k) \to \mathcal{H}(K)$ et ν l'expression $1+\sigma+\cdots+\sigma^{l-1}$.

L'extension K/k étant cyclique de degré l, on peut lui appliquer les méthodes que nous avons développées dans [2] et qui concernent $\mathcal{H}(K)$ (notamment en introduisant la filtration des sous-groupes de $\mathcal{H}(K)$ définis par $\mathcal{H}_i(K)=\mathrm{Ker}\,(\sigma-1)^i$).

§ 2. Étude de $\mathcal{H}(L)$.

Comme l'homomorphisme canonique $\mathcal{H}(L)\to\mathcal{H}(K)$ est injectif, nous convenons d'identifier $\mathcal{H}(L)$ à son image dans $\mathcal{H}(K)$. On peut donc considérer $\mathcal{H}(L)$ comme sous-groupe de $\mathcal{H}(K)$.

PROPOSITION 1. *On a* $\mathcal{H}(L)=\mathcal{H}(K)^T$ (sous-groupe de $\mathcal{H}(K)$ formé par les classes invariantes par τ) *et les groupes* $\mathcal{H}(L_i)$ *sont isomorphes entre eux.*

DÉMONSTRATION. Les éléments de $\mathcal{H}(L)$ sont fixes par T. Soit $h\in\mathcal{H}(K)$ une classe fixe par τ; $h=Cl_K(\mathfrak{A})$ et $Cl_K(\mathfrak{A}^\tau)=Cl_K(\mathfrak{A})$, soit $Cl_K(\mathfrak{A}^{1+\tau})=Cl_K(\mathfrak{A}^2)$, or $Cl_K(\mathfrak{A}^{1+\tau})$ est la classe dans K de l'étendu de l'idéal $N_{K/L}(\mathfrak{A})$, d'où $Cl_K(\mathfrak{A})\in\mathcal{H}(L)$ car 2 est premier à l. La seconde assertion est immédiate.

Par analogie avec le cas cyclique, on peut définir la filtration:

$$\mathcal{H}_i(L)=\mathcal{H}_i(K)^T=\{h\in\mathcal{H}_i(K),\ h^\tau=h\}\ ;$$

les $\mathcal{H}_i(L)$ sont des T-modules mais non des H-modules; ils constituent une suite croissante de sous-groupes de $\mathcal{H}(L)$ et $\mathcal{H}_i(L)=\mathcal{H}(L)$ pour i assez grand. On appellera $\mathcal{H}_1(L)$ le groupe des "l-classes ambiges" de L (définition différente de celle de [1]).

On se propose d'abord de donner un encadrement pour la valeur de l'ordre de $\mathcal{H}_1(L)$ (noté $|\mathcal{H}_1(L)|$), encadrement qui conduit, dans certains cas, à une expression simple pour $|\mathcal{H}_1(L)|$, et ensuite d'étudier $\mathcal{H}_2(L)$.

REMARQUE 1. Soit $\bar{t}$ (resp. t) le nombre d'idéaux premiers totalement ramifiés dans $L/\boldsymbol{Q}$ (resp. K/k). Alors $t-\bar{t}$ représente le nombre de nombres premiers ramifiés dans K/k et décomposés dans $k/\boldsymbol{Q}$ (en effet, d'après [4] p. 32, un nombre premier est totalement ramifié dans $L/\boldsymbol{Q}$ si et seulement si il est totalement ramifié dans K/k).

Considérons la suite exacte suivante ([2] p. 28):

$$1\longrightarrow\mathcal{H}_1^0(K)\longrightarrow\mathcal{H}_1(K)\longrightarrow E_k\cap NK^*/NE_K\longrightarrow 1\,,$$

où E_k et E_K sont les groupes des unités de k et K, $\mathcal{H}_1^0(K)$ est le sous-groupe de $\mathcal{H}_1(K)$ engendré par les classes des idéaux de K invariants par H; posons:

$$(E_k\cap NK^*:\ NE_K)=l^\delta\,;$$

comme k est un corps quadratique et que l est impair, δ est égal à 0 ou à 1. Nous distinguerons les deux cas suivants:

$$\text{Cas A: } \delta=0,$$

$$\text{Cas B: } \delta=1.$$

DÉFINITION. On pose $l^a=(E_k\colon E_k\cap NK^*)$ et $l^b=(E_k\colon NE_K)$; on a alors $b=a+\delta$.

DÉFINITION DU GROUPE $\mathfrak{J}$. Dans le cas A, on définit le groupe $\mathfrak{J}=\langle\mathfrak{P}_1,\cdots,\mathfrak{P}_t\rangle$, sous-groupe de $\mathfrak{J}(K)$ engendré par les t idéaux premiers de K ramifiés dans K/k. Dans le cas B, l'ordre du quotient $\mathcal{H}_1(K)/\mathcal{H}_1^0(K)$ étant égal à l, il existe un idéal $\mathfrak{A}_0$ de K tel que $Cl_K(\mathfrak{A}_0)\in\mathcal{H}_1(K)\setminus\mathcal{H}_1^0(K)$. On a alors $Cl_K(\mathfrak{A}_0^g)=Cl_K(\mathfrak{A}_0)$ et on peut même supposer $\mathfrak{A}_0$ premier ([2] p. 43). On définit alors le groupe $\mathfrak{J}=\langle\mathfrak{P}_1,\cdots,\mathfrak{P}_t,\mathfrak{A}_0^{1+\tau}\rangle$. Dans tous les cas $\mathfrak{J}$ est un sous T-module de $\mathfrak{J}(K)$ et on a en outre la propriété suivante:

LEMME 1. *Le T-module $\mathfrak{J}$ vérifie:* $\mathfrak{J}\cap\mathfrak{J}(K)^{\tau-1}=\mathfrak{J}^{\tau-1}$.

Soit $\mathfrak{A}\in\mathfrak{J}\cap\mathfrak{J}(K)^{\tau-1}$; alors $\mathfrak{A}=\mathfrak{B}^{\tau-1}$, $\mathfrak{B}\in\mathfrak{J}(K)$, et on peut supposer que $\mathfrak{B}$ ne contient pas de diviseurs premiers invariants par τ. Soit $\mathfrak{P}$ un idéal premier figurant dans $\mathfrak{B}$; si $\mathfrak{P}$ est l'un des $\mathfrak{P}_i$ alors $\mathfrak{P}\in\mathfrak{J}$. Si $\mathfrak{P}$ n'était ni $\mathfrak{A}_0$, ni $\mathfrak{A}_0^\tau$, ni l'un des $\mathfrak{P}_i$, alors $\mathfrak{A}$ contiendrait le facteur $\mathfrak{P}^{\tau-1}$ (avec $\mathfrak{P}^\tau\neq\mathfrak{P}$) ce qui est absurde car $\mathfrak{A}\in\mathfrak{J}$. Le seul cas qui reste à étudier est $\mathfrak{P}=\mathfrak{A}_0$ ou $\mathfrak{A}_0^\tau$; écrivons $\mathfrak{B}=\mathfrak{A}_0^{x+y\tau}\mathfrak{A}'$, $x,y\in\boldsymbol{Z}$, $\mathfrak{A}'$ premier à $\mathfrak{A}_0^{1+\tau}$, donc d'après ce qui précède $\mathfrak{A}'\in\mathfrak{J}$; $\mathfrak{B}^{\tau-1}=\mathfrak{A}_0^{(x+y\tau)(\tau-1)}\mathfrak{A}'^{\tau-1}\in\mathfrak{J}$, donc $\mathfrak{A}_0^{(x+y\tau)(\tau-1)}\in\mathfrak{J}$ et il existe $z\in\boldsymbol{Z}$ tel que $\mathfrak{A}_0^{(x+y\tau)(\tau-1)}=\mathfrak{A}_0^{z(1+\tau)}$; or ceci entraine $x=y$ et $z=0$, donc $\mathfrak{B}=\mathfrak{A}_0^{(1+\tau)x}\mathfrak{A}'\in\mathfrak{J}$.

PROPOSITION 2. *On a les suites exactes de T-modules:*

$$1\longrightarrow\operatorname{Ker}\theta\longrightarrow\mathfrak{J}/\mathfrak{J}^l\xrightarrow{\theta}\mathcal{H}_1(K)/j(\mathcal{H}(k))\longrightarrow 1,\tag{1}$$

$$1\longrightarrow\operatorname{Ker}\mu\longrightarrow\mathfrak{J}^{1+\tau}/\mathfrak{J}^{l(1+\tau)}\xrightarrow{\mu}\mathcal{H}_1(L)\longrightarrow 1,\tag{2}$$

$$1\longrightarrow\operatorname{Ker}\mu\longrightarrow\operatorname{Ker}\theta,\tag{3}$$

$$1\longrightarrow(\mathfrak{J}^{1-\tau}/\mathfrak{J}^{l(1-\tau)})\cap\operatorname{Ker}\theta\longrightarrow\operatorname{Ker}\theta\xrightarrow{1+\tau}\operatorname{Ker}\mu.\tag{4}$$

DÉMONSTRATION. (i) Définition de θ: Notons $q(\mathfrak{A})$, $\mathfrak{A}\in\mathfrak{J}$, un élément de $\mathfrak{J}/\mathfrak{J}^l$; si $q(\mathfrak{A})\in\mathfrak{J}/\mathfrak{J}^l$, alors $\theta(q(\mathfrak{A}))$ est l'image de $Cl_K(\mathfrak{A})$ dans $\mathcal{H}_1(K)/j(\mathcal{H}(k))$. Vérifions que la classe d'un élément de $\mathfrak{J}^l$ est contenue dans $j(\mathcal{H}(k))$: pour un $\mathfrak{P}_i$, c'est évident; soit $\mathfrak{A}_0^{1+\tau}\in\mathfrak{J}$ (cas B), on sait que $\mathfrak{A}_0^g=\mathfrak{A}_0\alpha A_K$, $\alpha\in K^*$, d'où $\mathfrak{A}^\nu=\mathfrak{A}_0^l\beta A_K$, $\beta\in K^*$, par conséquent $Cl_K(\mathfrak{A}_0)^l\in j(\mathcal{H}(k))$ et, à fortiori, $Cl_K(\mathfrak{A}_0^l)^{1+\tau}=1\in j(\mathcal{H}(k))$. Montrons la surjectivité: Dans le cas A, elle est évidente; dans le cas B, il faut montrer que $Cl_K(\mathfrak{A}_0^{1+\tau})$ permet de retrouver $Cl_K(\mathfrak{A}_0)$: on a $\mathfrak{A}_0^{g-1}=\alpha A_K$, $\alpha\in K^*$; $N_{K/k}(\alpha)$ est donc une unité $\varepsilon\in E_k$ et on peut toujours supposer $N_{k/Q}(\varepsilon)=1$. On aura $\mathfrak{A}_0^{(\sigma-1)\tau}=\alpha^\tau A_K$ soit $\mathfrak{A}_0^{(\sigma-1)\tau+\sigma-1}=\alpha\alpha^\tau A_K$, avec $N_{K/k}(\alpha\alpha^\tau)=N_{K/Q}(\alpha)=N_{k/Q}(\varepsilon)=1$; donc $\alpha\alpha^\tau=\gamma^{\sigma-1}$, $\gamma\in K^*$ (théorème 90 de Hilbert) et $\mathfrak{A}_0^{(\sigma-1)\tau+\sigma-1}=\gamma^{\sigma-1}A_K$. On peut écrire $(\sigma-1)\tau=\sigma\tau-\tau=\tau(\sigma^{l-1}-1)$ soit $\gamma^{\sigma-1}A_K=(\mathfrak{A}_0^{\tau(\sigma^{l-2}+\cdots+\sigma+1)+1})^{\sigma-1}$; l'idéal $\mathfrak{M}=\gamma^{-1}A_K\mathfrak{A}_0^{\tau(\sigma^{l-2}+\cdots+\sigma+1)+1}$ est invariant

par H, il est donc de la forme $\mathfrak{M}=\mathfrak{M}_0\mathfrak{a}A_K$, $\mathfrak{M}_0$ produit d'idéaux ramifiés dans K/k, $\mathfrak{a}\in\mathfrak{J}(k)$. On a alors $\tau(\sigma^{l-2}+\cdots+\sigma+1)=(1+\sigma^{-1}+\cdots+\sigma^{-(l-2)})\tau$ et $\mathfrak{M}=\mathfrak{A}_0^{(1+\sigma^{-1}+\cdots+\sigma^{-(l-2)})\tau+1}\gamma^{-1}A_K=\mathfrak{A}_0^{(l-1)\tau+1}\beta A_K$, $\beta\in K^*$ (compte tenu de la relation $\mathfrak{A}_0^{\sigma}=\mathfrak{A}_0\alpha A_K$); on peut écrire $\mathfrak{A}_0^{1-\tau}=\mathfrak{M}_0(\mathfrak{b}\beta)A_K$, $\mathfrak{b}\in\mathfrak{J}(k)$, car on a déjà vu que $\mathfrak{A}_0^l$ est équivalent à l'étendu d'un idéal de k. Par conséquent, dans $\mathcal{H}_1(K)/j(\mathcal{H}(k))$, les images de $Cl_K(\mathfrak{A}_0^{1-\tau})$ et $Cl_K(\mathfrak{A}_0^{1+\tau})$ sont atteintes, donc celle de $Cl_K(\mathfrak{A}_0)$ aussi (d'où (1)).

(ii) Définition de μ: Soit $\bar{q}(\mathfrak{A}^{1+\tau})$, $\mathfrak{A}\in\mathfrak{J}$, un élément de $\mathfrak{J}^{1+\tau}/\mathfrak{J}^{l(1+\tau)}$; alors $\mu(\bar{q}(\mathfrak{A}^{1+\tau}))$ est la classe $Cl_K(\mathfrak{A}^{1+\tau})$; c'est bien un élément de $\mathcal{H}_1(L)$. Les classes des éléments de $\mathfrak{J}^{l(1+\tau)}$ sont égales à 1: en effet, si $\mathfrak{A}\in\mathfrak{J}$, $Cl_K(\mathfrak{A}^l)\in j(\mathcal{H}(k))$, donc on aura $Cl_K(\mathfrak{A}^{l(1+\tau)})\in j(\mathcal{H}(k))^{1+\tau}=\{1\}$. On vérifie que la surjectivité provient de la surjectivité de θ et du fait que $\mathcal{H}(K)^{\tau}=\mathcal{H}(K)^{1+\tau}$.

(iii) L'application considérée est la restriction à $\operatorname{Ker}\mu$ de l'application canonique $\mathfrak{J}^{1+\tau}/\mathfrak{J}^{l(1+\tau)}\to\mathfrak{J}/\mathfrak{J}^l$; si $\bar{q}(\mathfrak{A}^{1+\tau})\in\operatorname{Ker}\mu$, $\mathfrak{A}\in\mathfrak{J}$, $q(\mathfrak{A}^{1+\tau})\in\mathfrak{J}/\mathfrak{J}^l$ et $Cl_K(\mathfrak{A}^{1+\tau})=1$, donc $q(\mathfrak{A}^{1+\tau})\in\operatorname{Ker}\theta$. Si $q(\mathfrak{A}^{1+\tau})=1$ alors $\mathfrak{A}^{1+\tau}\in\mathfrak{J}^l$; on vérifie facilement que $\mathfrak{A}^{1+\tau}\in\mathfrak{J}^{l(1+\tau)}$ d'où l'injectivité.

(iv) A $q(\mathfrak{A})\in\operatorname{Ker}\theta$ on associe $\bar{q}(\mathfrak{A}^{1+\tau})$; comme $Cl_K(\mathfrak{A})\in j(\mathcal{H}(k))$, $Cl_K(\mathfrak{A}^{1+\tau})=1$ donc $\bar{q}(\mathfrak{A}^{1+\tau})\in\operatorname{Ker}\mu$. Si $\bar{q}(\mathfrak{A}^{1+\tau})=1$, $\mathfrak{A}^{1+\tau}\in\mathfrak{J}^{l(1+\tau)}$ soit $\mathfrak{A}^{1+\tau}=\mathfrak{B}^{l(1+\tau)}$, $\mathfrak{B}\in\mathfrak{J}$; $(\mathfrak{A}/\mathfrak{B}^l)^{1+\tau}=A_K$, donc il existe $\mathfrak{A}_1\in\mathfrak{J}(K)$ tel que $\mathfrak{A}/\mathfrak{B}^l=\mathfrak{A}_1^{1-\tau}$ et $q(\mathfrak{A})=q(\mathfrak{A}_1^{1-\tau})$ dans $\mathfrak{J}/\mathfrak{J}^l$; comme $\mathfrak{A}_1^{1-\tau}\in\mathfrak{J}$ on peut supposer que $\mathfrak{A}_1\in\mathfrak{J}$ (Lemme 1) donc $q(\mathfrak{A})$ appartient à l'image de $\mathfrak{J}^{1-\tau}$ dans $\mathfrak{J}/\mathfrak{J}^l$ que l'on peut identifier à $\mathfrak{J}^{1-\tau}/(\mathfrak{J}^l\cap\mathfrak{J}^{1-\tau})=\mathfrak{J}^{1-\tau}/\mathfrak{J}^{l(1-\tau)}$. D'où la dernière suite exacte.

COROLLAIRE 1. *On a* $|\operatorname{Ker}\theta|=l^{b+1}/|\operatorname{Ker}j|$.

En effet, $|\mathfrak{J}/\mathfrak{J}^l|=l^{t+\delta}$ et, d'après (1),

$$|\operatorname{Ker}\theta|=\frac{l^{t+\delta}|j(\mathcal{H}(k))|}{|\mathcal{H}_1(K)|}=\frac{l^{t+\delta}|\mathcal{H}(k)|\,l^a}{|\mathcal{H}(k)|\,l^{t-1}|\operatorname{Ker}j|}\quad\text{soit}\quad|\operatorname{Ker}\theta|=\frac{l^{\delta+a+1}}{|\operatorname{Ker}j|}.$$

Or on a $b=a+\delta$, donc $|\operatorname{Ker}\theta|=l^{b+1}/|\operatorname{Ker}j|$.

REMARQUE 2. Comme k est un corps quadratique, on a $b\leqq 1$, d'où $|\operatorname{Ker}\theta|\leqq l^2$.

REMARQUE 3. Dans le cas B, $\mathfrak{J}^{1-\tau}$ est engendré par les $\mathfrak{P}_i^{1-\tau}$ (car $\mathfrak{A}_0^{(1+\tau)(1-\tau)}=(1)$) donc, dans tous les cas, on aura $\mathfrak{J}^{1-\tau}=\mathfrak{J}_0^{1-\tau}$ où $\mathfrak{J}_0$ est le sous-groupe de $\mathfrak{J}$ engendré par les idéaux premiers ramifiés dans K/k et décomposés dans $k/\boldsymbol{Q}$ (il y en a $2(t-\bar{t})$); $\mathfrak{J}_0^{1-\tau}/\mathfrak{J}_0^{l(1-\tau)}$ est donc d'ordre $l^{t-\bar{t}}$.

THÉORÈME 1. *On a les inégalités:*

$$|\operatorname{Ker}j|\,l^{\bar{t}-a-1}\leqq|\mathcal{H}_1(L)|\leqq|\operatorname{Ker}j|\,l^{\bar{t}-a-1}|\operatorname{Ker}\theta\cap\mathfrak{J}_0^{1-\tau}/\mathfrak{J}_0^{l(1-\tau)}|.$$

DÉMONSTRATION. C'est une conséquence immédiate des suites exactes (1), (2), (3), (4), du corollaire 1, des remarques 1 et 3 et du fait que $|\mathfrak{J}^{1+\tau}/\mathfrak{J}^{l(1+\tau)}|=l^{\delta+\bar{t}}$:

D'après (2), $|\mathcal{H}_1(L)| = \frac{l^{\delta+\bar{t}}}{|\mathrm{Ker}\,\mu|}$; (3) permet une minoration et (4) une majoration de $|\mathcal{H}_1(L)|$:

$$|\mathcal{H}_1(L)| \geqq \frac{l^{\delta+\bar{t}}}{|\mathrm{Ker}\,\theta|} = \frac{l^{\delta+\bar{t}}|\mathrm{Ker}\,j|}{l^{b+1}} = l^{\delta+\bar{t}-b-1}|\mathrm{Ker}\,j| = l^{\bar{t}-a-1}|\mathrm{Ker}\,j| ;$$

$$|\mathcal{H}_1(L)| \leqq \frac{l^{\delta+\bar{t}}}{|\mathrm{Ker}\,\theta|}|\mathrm{Ker}\,\theta \cap \mathfrak{I}^{1-\tau}/\mathfrak{I}^{l(1-\tau)}| = l^{\bar{t}-a-1}|\mathrm{Ker}\,j|\,|\mathrm{Ker}\,\theta \cap \mathfrak{I}^{1-\tau}/\mathfrak{I}^{l(1-\tau)}| .$$

COROLLAIRE 2. *On a les inégalités:*

$$|\mathrm{Ker}\,j|\,l^{\bar{t}-a-1} \leqq |\mathcal{H}_1(L)| \leqq l^{\bar{t}-a+1} .$$

COROLLAIRE 3. *Si* $|\mathrm{Ker}\,j| = l^2$ *on si* $t = \bar{t}$ *alors* $|\mathcal{H}_1(L)| = |\mathrm{Ker}\,j|\,l^{\bar{t}-a-1}$.

COROLLAIRE 4. *Dans le cas où* K/k *est non ramifiée, on obtient* $|\mathcal{H}_1(L)| = \frac{|\mathrm{Ker}\,j|}{l} = l^b$.

(cf. [2] p. 28 : $|\mathrm{Ker}\,j| = l|E_k/NE_K| = l^{b+1}$).

Par exemple, dans le cas où k est imaginaire et K/k non ramifiée (ce qui exclue $k = \boldsymbol{Q}(\sqrt{-3})$ pour $l=3$), on a $b=0$ soit $|\mathcal{H}_1(L)|=1$ (il faut remarquer que ceci n'implique pas $|\mathcal{H}(L)|=1$ car $\mathcal{H}(L)$ n'est pas un H-module).

Passons maintenant à l'étude de $\mathcal{H}_2(L)$.

LEMME 2. *On a* $\mathcal{H}_2(L)^{\sigma-1} \subset \mathcal{H}_1(K)^{1-\tau}$ *et* $\mathcal{H}_2(L)^{\sigma-1} \cap \mathcal{H}_1(L) = \{1\}$.

Soit $h^{\sigma-1} \in \mathcal{H}_2(L)^{\sigma-1}$, $h \in \mathcal{H}_2(L)$ (on a donc $h^{(\sigma-1)^2}=1$ et $h^{\tau}=h$) ; $h^{(\sigma-1)\tau} = h^{\sigma\tau-\tau} = h^{\tau(\sigma^{-1}-1)} = h^{\sigma^{-1}-1} = h^{(\sigma-1)(\sigma^{l-2}+\cdots+\sigma+1)}$ or $h^{\sigma-1} \in \mathcal{H}_1(K)$ donc $h^{(\sigma-1)(1+\sigma+\cdots+\sigma^{l-2})} = h^{(\sigma-1)(l-1)} = h^{l(\sigma-1)}h^{-(\sigma-1)}$. Si on démontre que $h^{l(\sigma-1)}=1$, on aura $h^{(\sigma-1)(\tau+1)}=1$ soit $h^{\sigma-1} \in \mathcal{H}_1(K)^{1-\tau}$. Or ceci résulte du fait que $\nu = (\sigma-1)^{l-1} - lA(\sigma)$ ($A(\sigma)$ inversible dans $\boldsymbol{Z}_l[H]$, cf. [2] p. 30), donc $h^{lA(\sigma)(\sigma-1)} = h^{(\sigma-1)^l} = 1$ car $h \in \mathcal{H}_2(L)$. Comme $\mathcal{H}_1(L) = \mathcal{H}_1(K)^T = \mathcal{H}_1(K)^{1+\tau}$ et que $\mathcal{H}_1(K)^{1+\tau} \cap \mathcal{H}_1(K)^{1-\tau} = \{1\}$, il en résulte que $\mathcal{H}_2(L)^{\sigma-1} \cap \mathcal{H}_1(L) = \{1\}$.

THÉORÈME 2. *On a* $|\mathcal{H}_2(L)/\mathcal{H}_1(L)| \leqq \frac{l^{t-\bar{t}}|\mathcal{H}(k)|}{|\mathrm{Ker}\,j|} l^{t-\bar{t}}|j(\mathcal{H}(k))|$.

DÉMONSTRATION. Le lemme 2 conduit, grace à la suite exacte de groupes

$$1 \longrightarrow \mathcal{H}_1(L) \longrightarrow \mathcal{H}_2(L) \xrightarrow{\sigma-1} \mathcal{H}_2(L)^{\sigma-1} \longrightarrow 1 ,$$

à

$$|\mathcal{H}_2(L)/\mathcal{H}_1(L)| = |\mathcal{H}_2(L)^{\sigma-1}| \leqq |\mathcal{H}_1(K)^{1-\tau}| ;$$

or

$$|\mathcal{H}_1(K)| = |\mathcal{H}_1(K)^{1+\tau}|\,|\mathcal{H}_1(K)^{1-\tau}| = |\mathcal{H}_1(L)|\,|\mathcal{H}_1(K)^{1-\tau}|$$

et, en utilisant la minoration de $|\mathcal{H}_1(L)|$ du théorème 1, on obtient

$$|\mathcal{H}_1(K)^{1-\tau}| = |\mathcal{H}_1(K)|/|\mathcal{H}_1(L)| = \frac{|\mathcal{H}(k)|\,l^{t-1-a}}{|\mathcal{H}_1(L)|} \leqq l^{t-\bar{t}}\frac{|\mathcal{H}(k)|}{|\mathrm{Ker}\,j|} .$$

PROPOSITION 3. *Pour* $l=3$ *on a* $\mathcal{H}_2(L) = \{h \in \mathcal{H}(L),\ h^3=1\}$.

DÉMONSTRATION. Soit $h\in\mathcal{H}(L)$, alors $h\in\mathcal{H}(K)^{1+\tau}$ et $h^{\nu}\in\mathcal{H}(K)^{(1+\tau)\nu}=\{1\}$; donc $h^{(\sigma-1)^{l-1}}=h^{lA(\sigma)}$ et, pour $l=3$, on a bien $h^3=1$ si et seulement si $h^{(\sigma-1)^2}=1$, donc si et seulement si $h\in\mathcal{H}_2(L)$.

COROLLAIRE 5. *Si $l=3$, le 3-rang $\rho(L)$ de $\mathcal{H}(L)$ vérifie les inégalités:*

$$|\mathrm{Ker}\, j|\,3^{\bar{t}-a-1}\leqq 3^{\rho(L)}\leqq|\mathcal{H}(k)|\,3^{t-a-1}|\mathrm{Ker}\,\theta\cap\mathfrak{J}_0^{1-\tau}/\mathfrak{J}_0^{3(1-\tau)}|\,.$$

COROLLAIRE 6. *Si $l=3$ et si $t=\bar{t}$, le 3-rang $\rho(L)$ de $\mathcal{H}(L)$ vérifie les inégalités:* $|\mathrm{Ker}\, j|\,3^{t-a-1}\leqq 3^{\rho(L)}\leqq|\mathcal{H}(k)|\,3^{t-a-1}$; *si en outre* $|\mathcal{H}(k)|=1$, *on obtient* $\rho(L)=t-a-1$.

THÉORÈME 3. *On suppose $l=3$, $t=\bar{t}$ et $|\mathcal{H}(k)|=1$; on a donc $\rho(L)=t-a-1$. Alors le 3-rang $\rho(K)$ du groupe $\mathcal{H}(K)$ est égal à $2(t-a-1)=2\rho(L)$.*

DÉMONSTRATION. Il suffit, pour calculer $\rho(K)$, d'appliquer la méthode décrite dans [2]. Comme $\mathcal{H}(k)=\{1\}$, le groupe $\mathfrak{J}$ que nous avons défini, représente $\mathcal{H}_1(K)$ (Dans [2], il est nécéssaire que $\mathfrak{J}$ soit un H-module et vérifie $\mathfrak{J}\cap\mathfrak{J}(K)^{\sigma-1}=\mathfrak{J}^{\sigma-1}$; on prendra donc ici $\mathfrak{J}_1=\langle\mathfrak{P}_1,\cdots,\mathfrak{P}_t,\mathfrak{A}_0^{1+\tau},\mathfrak{A}_0^{(1+\tau)\sigma},\cdots,\mathfrak{A}_0^{(1+\tau)\sigma^{l-1}}\rangle$ en convenant que $\mathfrak{A}_0=A_K$ dans le cas A). Posons $k=\boldsymbol{Q}(\sqrt{m})$, $m\in\boldsymbol{Z}$, et soit $\tilde{k}$ le corps $\boldsymbol{Q}(\sqrt{-3m})$ ($\tilde{k}=\boldsymbol{Q}$ si $k=\boldsymbol{Q}(\sqrt{-3})$).

LEMME 3. *Soit $p\neq 3$ un nombre premier ramifié dans K/k; alors p est inerte dans $\boldsymbol{Q}(\sqrt{-3})$ (i.e. $p\equiv-1 \bmod 3$) et son degré résiduel dans $\tilde{k}/\boldsymbol{Q}$ est égal à 1.*

D'après [4] (Proposition III. 3) un tel nombre premier $p\neq 3$ ne peut pas se ramifier dans $k/\boldsymbol{Q}$; donc, puisque $t=\bar{t}$, p est inerte dans $k/\boldsymbol{Q}$ et, d'après [4] (Proposition IV. 3 et Corollaire 2 à la Proposition IV. 15), on a $p\equiv\left(\frac{m}{p}\right) \bmod 3$ (symbole de Legendre), où $k=\boldsymbol{Q}(\sqrt{m})$; or $\left(\frac{m}{p}\right)=-1$ et on obtient $p\equiv-1 \bmod 3$, d'où la première partie du lemme; la seconde résulte alors du fait que $\mathfrak{p}$ est nécéssairement de degré résiduel 1 dans l'extension $k(\sqrt{-3})/k$ (cf. [2] p. 20).

On calcule maintenant $I_1=N_{K/k}\mathfrak{J}_1\cap\mathfrak{J}_0(k)$ (cf. [2] p. 36); ici I_1 sera de la forme $\langle p_1A_k,\cdots,p_tA_k,a_0A_k\rangle$, où $a_0\in\boldsymbol{Z}$ avec $a_0\boldsymbol{Z}=N_{K/\boldsymbol{Q}}\mathfrak{A}_0$. Par conséquent, le groupe de nombres Λ_1 associé sera: $\Lambda_1=\langle\varepsilon,p_1,p_2,\cdots,p_t,a_0\rangle$, où ε est une unité convenable de k ($\varepsilon=1$ si k est imaginaire et est différent de $\boldsymbol{Q}(\sqrt{-3})$, $\varepsilon=\frac{1}{2}(1+\sqrt{-3})$ si $k=\boldsymbol{Q}(\sqrt{-3})$ et ε est l'unité fondamentale de k si k est réel). Soit $\gamma\in\tilde{k}$ tel que $K(\sqrt{-3})=k(\sqrt{-3},\sqrt[3]{\gamma})$ (cf. [4], Prop. IV. 3); alors le rang du système linéaire associé à Λ_1 par l'intermédiaire du symbole de Hilbert $(\gamma,u)_{\mathfrak{p}}$, $u\in\Lambda_1$, $\mathfrak{p}$ idéal premier de k ramifié dans K/k, est une conséquence du résultat suivant:

LEMME 4. *Si u est un rationnel, on a $(\gamma,u)_{\mathfrak{p}}=1$ pour tout idéal premier $\mathfrak{p}$ de k ramifié dans K/k* (cf. [3]).

D'après les formules explicites pour le symbole de Hilbert, calculé dans

$k(\sqrt{-3})$ ([2] p. 14), on a pour $\mathfrak{p}=pA_k$ ne divisant pas 3: $(\gamma, u)_{\mathfrak{p}} \equiv c^{\frac{q-1}{3}} \bmod \mathfrak{p}$ avec $q=p^2$ puisque p est inerte dans $k/\boldsymbol{Q}$. D'après le lemme précédent γ (donc c) est congru modulo $\mathfrak{p}$ à un rationnel, et comme $\frac{p+1}{3}$ est entier, $c^{\frac{q-1}{3}}=c^{\frac{p+1}{3}(p-1)}$ est congru à 1 modulo p. Si $\mathfrak{p}$ divise 3, cela résulte alors de la formule du produit, compte tenu du fait que 3 n'est pas decomposé dans $k/\boldsymbol{Q}$. Le rang du système linéaire associé à Λ_1 est donc égal à a. D'après [2] p. 41, on obtient $|\mathcal{H}_2(K)/\mathcal{H}_1(K)|=3^{t-a-1}$, d'où le théorème.

On retrouve ainsi les résultats de Kobayashi ([3]) qui a demontré ce théorème pour $k=\boldsymbol{Q}(\sqrt{-3})$ et $K=k(\sqrt[3]{m})$ avec des hypothèses sur m qui coïncident, dans ce cas, avec celles de notre énoncé.

§ 3. Exemple numérique.

On considère l'extension cubique non galoisienne $L=\boldsymbol{Q}(\sqrt[3]{2\cdot 7\cdot 13})=\boldsymbol{Q}(\sqrt[3]{182})$ dont la clôture galoisienne est $K=\boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{182})$.

Soit $k=\boldsymbol{Q}(\sqrt{-3})$; on vérifie facilement que 3 est ramifié dans K/k, que 2 est inerte dans $k/\boldsymbol{Q}$, 7 et 13 sont decomposés dans $k/\boldsymbol{Q}$ et que si ζ_3 est une racine cubique de l'unité, primitive, alors $\zeta_3 \in k$ et n'est pas norme dans K/k.

Avec les notations des paragraphes I et II, on a $t=6$ et $\bar{t}=4$. On notera $\mathfrak{p}_2=2A_k$, $\mathfrak{p}_3=\sqrt{-3}\,A_k$, $\mathfrak{p}_7=(2+\sqrt{-3})A_k$, $\mathfrak{p}_7^{\tau}=(2-\sqrt{-3})A_k$, $\mathfrak{p}_{13}=(1+2\sqrt{-3})A_k$ et $\mathfrak{p}_{13}^{\tau}=(1-2\sqrt{-3})A_k$ les idéaux premiers de k ramifiés dans K/k.

a) *Détermination de* $\mathcal{H}_1(K)$.

D'après la formule de Chevalley (cf. [2] p. 25), on a $|\mathcal{H}_1(K)|=\frac{3^{t-1}}{(E_k : E_k \cap NK^*)}=3^4$ et, d'après [2] p. 28, toute classe invariante est, ici, classe d'un idéal invariant (autrement dit $\delta=0$); par conséquent, il existe deux relations indépendantes non triviales entre les classes des six idéaux premiers de K ramifiés dans K/k: $\mathfrak{P}_2$, $\mathfrak{P}_3$, $\mathfrak{P}_7$, $\mathfrak{P}_7^{\tau}$, $\mathfrak{P}_{13}$ et $\mathfrak{P}_{13}^{\tau}$. La première est donnée par $\sqrt[3]{2\cdot 7\cdot 13}\,A_K=\mathfrak{P}_2\mathfrak{P}_7^{1+\tau}\mathfrak{P}_{13}^{1+\tau}$; la seconde s'obtient à partir d'une unité du corps (via le théorème 90 de Hilbert): On trouve que $\eta=-17+3\sqrt[3]{182}$ est une unité de K de norme relative 1. On a donc $\eta=\varphi^{\sigma-1}$ avec, par exemple, $\varphi=1+\eta+\eta\eta^{\sigma}$; on vérifie facilement que $\frac{\varphi}{3}$ est encore un entier et que sa norme relative est $N_{K/k}\left(\frac{\varphi}{3}\right)=-7\cdot 13(8+3\sqrt{-3})=-7\cdot 13(2-\sqrt{-3})(1+2\sqrt{-3})$; il en résulte que $\frac{\varphi}{3}A_K=\mathfrak{P}_7^{1+2\tau}\mathfrak{P}_{13}^{2+\tau}$. En utilisant les notations de la proposition 2, on a $\mathfrak{I}=\langle \mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_7, \mathfrak{P}_7^{\tau}, \mathfrak{P}_{13}, \mathfrak{P}_{13}^{\tau}\rangle$ et $\operatorname{Ker}\theta$ (qui est d'ordre 9) est engendré par les images de $\mathfrak{P}_2\mathfrak{P}_7^{1+\tau}\mathfrak{P}_{13}^{1+\tau}$ et de $\mathfrak{P}_7^{1+2\tau}\mathfrak{P}_{13}^{2+\tau}$ dans $\mathfrak{I}/\mathfrak{I}^3$. On peut, par exemple, prendre pour $\boldsymbol{F}_3$-base de $\mathcal{H}_1(K)$: $Cl_K(\mathfrak{P}_2)$, $Cl_K(\mathfrak{P}_3)$, $Cl_K(\mathfrak{P}_7)$ et $Cl_K(\mathfrak{P}_7^{\tau})$.

b) *Calcul de* $\rho(K)$.

On applique encore la méthode décrite dans [2]: le groupe A_1 associé à $\mathfrak{I}_1$ est de la forme $A_1=\langle\zeta_3, 2, 3, \alpha, \alpha^\tau, \beta, \beta^\tau\rangle$ avec $\alpha=2+\sqrt{-3}$, $\alpha^\tau=2-\sqrt{-3}$, $\beta=1+2\sqrt{-3}$, $\beta^\tau=1-2\sqrt{-3}$; le calcul des symboles de Hilbert $(182, u)_\mathfrak{p}$, $u\in A_1$, $\mathfrak{p}$ idéal premier de k ramifié dans K/k, conduit à la matrice (en notation additive):

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 1 & 2 & 1 & 1 & 0 & 2 & 1 \\ 2 & 1 & 1 & 0 & 2 & 2 & 1 \\ 2 & 2 & 2 & 1 & 0 & 2 & 1 \end{pmatrix}$$

chaque ligne étant formée des symboles $(182, \zeta_3)_\mathfrak{p}$, $(182, 2)_\mathfrak{p}$, $(182, 3)_\mathfrak{p}$, $(182, \alpha)_\mathfrak{p}$, $(182, \alpha^\tau)_\mathfrak{p}$, $(182, \beta)_\mathfrak{p}$ et $(182, \beta^\tau)_\mathfrak{p}$ où $\mathfrak{p}$ parcourt l'ensemble $\{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_7, \mathfrak{p}_7^\tau, \mathfrak{p}_{13}, \mathfrak{p}_{13}^\tau\}$. Le rang de cette matrice est 4; les 3 solutions indépendantes du système sont, par exemple:

$$2\alpha\alpha^\tau\beta\beta^\tau=182\in NK^*,$$

$$\alpha\alpha^{2\tau}\beta^2\beta^\tau=7\cdot 13(8+3\sqrt{-3})\in NK^*,$$

$$\beta\beta^\tau=13\in NK^*;$$

les deux premières provenant des relations entre les "classes ambiges" trouvées plus haut.

On aura donc (cf. [2] p. 41): $|\mathcal{H}_2(K)/\mathcal{H}_1(K)|=3$ soit $|\mathcal{H}_2(K)|=3^5$; c'est-à-dire que le 3-rang de $\mathcal{H}(K)$ est égal à 5.

c) *Détermination de* $\rho(L)$, $\mathcal{H}(K)$ *et* $\mathcal{H}(L)$.

Déterminons d'abord $\mathcal{H}_2(K)$. Pour trouver un groupe $\mathfrak{I}_2$ associé à $\mathcal{H}_2(K)$, il suffit de résoudre l'équation $N_{K/k}(x)=13$, $x\in K^*$. On trouve que $x=5\cdot 13+9\sqrt[3]{182}+5(\sqrt[3]{182})^2$ a pour polynome irréductible

$$X^3-3\cdot 5\cdot 13X^2-3\cdot 5\cdot 13\cdot 61X-13\cdot 61^3;$$

on en déduit, compte tenu aussi du fait que $x\in L$, que $xA_K=\mathfrak{P}_{13}^{1+\tau}\mathfrak{P}_{61}^{(1+2\sigma)(1+\tau)}$, où $\mathfrak{P}_{61}$ est un idéal premier au-dessus de 61 (61 étant totalement décomposé dans $K/\boldsymbol{Q}$). Comme $\frac{x}{61}$ est de norme 13, on écrit $\frac{x}{61}A_K=\mathfrak{P}_{13}^{1+\tau}\mathfrak{A}^{\sigma-1}$ soit, ici, $\mathfrak{A}=\mathfrak{P}_{61}^{\sigma+\tau+\sigma\tau}$; d'où:

$$\mathfrak{I}_2=\langle\mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_7, \mathfrak{P}_7^\tau, \mathfrak{P}_{13}, \mathfrak{P}_{13}^\tau, \mathfrak{P}_{61}^{\sigma+\tau+\sigma\tau}, \cdots\rangle$$

et

$$A_2=\langle\zeta_3, 2, 3, \alpha, \alpha^\tau, \beta, \beta^\tau, 61\frac{1+9\sqrt{-3}}{2}\rangle.$$

En fait $\mathcal{H}_2(K)$ admet, par exemple, pour base :

$$\{Cl_K(\mathfrak{P}_2), Cl_K(\mathfrak{P}_3), Cl_K(\mathfrak{P}_7), Cl_K(\mathfrak{P}_7'), Cl_K(\mathfrak{P}_{61}^{\sigma+\tau+\sigma\tau})\}\ .$$

La détérmination de $\mathcal{H}_2(L)$ est immédiate : on a $\mathcal{H}_2(L)=\mathcal{H}_2(K)^{1+\tau}$, soit :

$$\mathcal{H}_2(L)=\langle Cl_K(\mathfrak{P}_2^{1+\tau}), Cl_K(\mathfrak{P}_3^{1+\tau}), Cl_K(\mathfrak{P}_7^{1+\tau}), Cl_K(\mathfrak{P}_{61}^{(\sigma+\tau+\sigma\tau)(1+\tau)})\rangle$$

$$=\langle Cl_K(\mathfrak{P}_2), Cl_K(\mathfrak{P}_3), Cl_K(\mathfrak{P}_7^{1+\tau})\rangle \text{ car } \mathfrak{P}_{61}^{(\sigma+\tau+\sigma\tau)(1+\tau)}\sim\mathfrak{P}_{13}^{1+\tau}\ .$$

Les trois classes engendrant $\mathcal{H}_2(L)$ sont indépendantes, d'où $\rho(L)=3$.

Enfin, le calcul des symboles $\left(182, 61\dfrac{1+9\sqrt{-3}}{2}\right)_\mathfrak{p}$ montre que la matrice associée à Λ_2 se déduit de la précédente en rajoutant la colonne $\begin{pmatrix}1\\0\\2\\2\\2\\2\end{pmatrix}$ ce qui fait que le rang de cette nouvelle matrice est 5, donc que $|\mathcal{H}_3(K)/\mathcal{H}_2(K)|=1$, soit $\mathcal{H}(K)=\mathcal{H}_2(K)\cong(\boldsymbol{Z}/3\boldsymbol{Z})^5$ et $\mathcal{H}(L)=\mathcal{H}_2(L)\cong(\boldsymbol{Z}/3\boldsymbol{Z})^8$.

Bibliographie

[1] A. Fröhlich, The genus field and genus group in finite number fields, Mathematika, 6 (1959), 40-4 et Mathematika, 6 (1959), 142-146.

[2] G. Gras, Sur les *l*-classes d'idéaux dans les extensions cycliques relatives de degré premier *l* (Thèse, Grenoble 1972), Ann. Inst. Fourier, 23, Fasc. 3 et 4.

[3] S. Kobayashi, On the 3-rank of the ideal class groups of certain pure cubic fields, J. Fac. Sci. Univ. Tokyo Sec. IA, 20 (1973), 209-216.

[4] J. Martinet, Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$ (Thèse, Grenoble 1968), Ann. Inst. Fourier, 19 (1969), 1-80.

Georges GRAS
Institut de Mathématiques pures
Laboratoire associé au C.N.R.S. n°188
Boîte postale n°116
38402 Saint-Martin-d'Hères
France