Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Georges Gras

Étude du ℓ-groupe des classes des extensions cycliques de degré ℓ

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 2 (1971-1972), exp. n° 20, p. 1-12

<http://www.numdam.org/item?id=SDPP_1971-1972__13_2_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 20, 12 p.

17 avril 1972

ÉTUDE DU ℓ-GROUPE DES CLASSES DES EXTENSIONS CYCLIQUES DE DEGRÉ ℓ

par Georges GRAS

Introduction. - Soit K/k une extension cyclique de corps de nombres de degré premier ℓ. On sait, depuis TAKAGI (1920), calculer le nombre a des ℓ-classes de K (au sens ordinaire) invariantes par $\mathrm{Gal}(K/k)$ par la formule (pour ℓ impair) :

$$a = \frac{h(k)\,\ell^{t-1}}{(E_k : E_k \cap NK^*)}$$

où $h(k)$ est le nombre de ℓ-classes (au sens ordinaire) de k, t est le nombre d'idéaux premiers ramifiés dans K/k, et E_k est le groupe des unités de k.

CHEVALLEY ([2], 1933) a généralisé l'expression de a au cas cyclique de degré quelconque, grâce à un théorème de Herbrand sur les unités. La formule ci-dessus est valable pour $\ell = 2$ à condition de remplacer la notion de classe au sens ordinaire par la notion de classe au sens restreint, et de remplacer E_k par le groupe F_k^+ des unités de k totalement positives.

Un résultat de LEOPOLDT ([7], 1953) montre que lorsque $k = \mathbb{Q}$, le ℓ-rang R_1 du groupe des classes de K vérifie les inégalités

$$t - 1 \leq R_1 \leq (\ell - 1)(t - 1) ;$$

sachant que le ℓ-rang du groupe des classes invariantes est ici $t - 1$, on peut se demander s'il existe des classes d'ordre ℓ non invariantes et, plus généralement, si la structure du ℓ-groupe des classes peut se déterminer effectivement. Ce sont les problèmes que nous allons traiter ici.

I. Résultats généraux.

Soit K/k une extension cyclique de degré premier ℓ ; soient H le groupe de Galois de K/k, et σ un générateur de H. On désigne par A_K l'anneau des entiers de K, par E_K le groupe des unités de K, par $\mathcal{J}(K)$ (resp. $\mathcal{J}_0(K)$) le groupe des idéaux fractionnaires (resp. principaux au sens restreint) de K, et enfin par $\mathcal{H}(K)$ le ℓ-groupe des classes au sens restreint de K. Les quantités A_k, E_k, $\mathcal{J}(k)$, $\mathcal{J}_0(k)$ et $\mathcal{H}(k)$ se définissent de façon analogue.

Si $\mathcal{J}$ est un sous-groupe quelconque de $\mathcal{J}(K)$, on pose $\mathcal{J}_0 = \mathcal{J} \cap \mathcal{J}_0(K)$. On note N l'application norme de $\mathcal{J}(K)$ dans $\mathcal{J}(k)$, et on note encore N l'application de $\mathcal{H}(K)$ dans $\mathcal{H}(k)$ qui s'en déduit par passage aux classes. On pose

$$\nu = 1 + \sigma + \ldots + \sigma^{\ell-1} .$$

On note j l'homomorphisme extension des idéaux de $\mathcal{J}(k)$ dans $\mathcal{J}(K)$ ainsi que l'application de $\mathcal{H}(k)$ dans $\mathcal{H}(K)$ qui s'en déduit : on rappelle que l'action de

$j \circ N$ est identique à celle de ν .

1. Propriétés élémentaires de $\mathcal{H}(K)$.

(a) Groupe des classes invariantes. - Soit $\mathcal{H}_1$ le sous-groupe de $\mathcal{H}(K)$ formé des classes invariantes par H . On rappelle les résultats suivants.

THÉORÈME I.1. - Soit t le nombre d'idéaux ramifiés dans K/k et soit E_k^+ le sous-groupe de E_k formé des unités totalement positives de k . Alors

$$|\mathcal{H}_1| = \frac{|\mathcal{H}(k)|\ \ell^{t-1}}{(E_k^+ : E_k^+ \cap NK^*)} .$$

COROLLAIRE I.1. - Lorsque $k = \mathbb{Q}$, $|\mathcal{H}_1| = \ell^{t-1}$.

COROLLAIRE I.2. - Lorsque $E_k^+ \subset N(E_K^+)$, E_K^+ désignant le groupe des unités totalement positives de K , on peut engendrer $\mathcal{H}_1$ par des classes d'idéaux invariants, donc d'idéaux premiers ramifiés dans K/k , et d'idéaux de k étendus à K .

Ce corollaire résulte de la suite exacte :

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

$\mathcal{H}_1^0$ désignant le sous-groupe de $\mathcal{H}_1$ formé des classes des idéaux de K invariants par σ .

(b) Filtration associée à $\mathcal{H}(K)$. - Le groupe $\mathcal{H}(K)$ est un ℓ-groupe fini muni d'une structure de H-module. On pose :

$$\mathcal{H}_i = \{h \in \mathcal{H}(K) ,\ h^{(\sigma-1)^i} = 1\} ,$$

$$\mathcal{H}^{(n)} = \{h \in \mathcal{H}(K) ,\ h^{\ell^n} = 1\} .$$

PROPOSITION I.1. - On a

(i) $\mathcal{H}_i \subset \mathcal{H}_{i+1}$ et $\mathcal{H}_i = \mathcal{H}_{i+1}$ si, et seulement si, $\mathcal{H}_i = \mathcal{H}(K)$;

(ii) les ordres des groupes $\mathcal{H}_{i+1}/\mathcal{H}_i$ décroissent vers 1 ;

(iii) lorsque $\mathcal{H}(K)^\nu = \{1\}$, on a, pour tout $n \geq 0$, la relation $\mathcal{H}^{(n)} = \mathcal{H}_{n(\ell-1)}$.

La démonstration est élémentaire.

On en déduit alors le résultat suivant :

PROPOSITION I.2. - Soit R_q le ℓ^q-rang de $\mathcal{H}(K)$ (i. e. la dimension sur F_ℓ de $\mathcal{H}^{\ell^{q-1}}(K)/\mathcal{H}^{\ell^q}(K)$) ; alors R_q est égal à la dimension sur F_ℓ de $\mathcal{H}^{(q)}/\mathcal{H}^{(q-1)}$.

Si $\mathcal{H}^\nu(K) = \{1\}$, alors on a la relation

$$\ell^{R_q} = \prod_{i=(q-1)(\ell-1)}^{q(\ell-1)-1} |\mathcal{H}_{i+1}/\mathcal{H}_i| .$$

2. Démonstration d'un théorème.

THÉORÈME I.2. - *Soit* $\mathcal{H}$ *un sous-H-module de* $\mathcal{H}(K)$, *et soit* $\widetilde{\mathcal{H}}$ *l'ensemble formé des* $h \in \mathcal{H}(K)$ *tels que* $h^{\sigma-1} \in \mathcal{H}$;

(i) $\widetilde{\mathcal{H}}$ *est un sous-H-module de* $\mathcal{H}(K)$ *qui contient* $\mathcal{H}$ *et* $\mathcal{H}_1$;

(ii) *pour tout sous-H-module* $\mathcal{J}$ *de* $\mathcal{J}(K)$ *dont l'image dans* $\mathcal{H}(K)$ *est égale à* $\mathcal{H}$ *et qui est tel que* $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$, *on a la suite exacte de* $F_\ell[H]$*-modules* :

$$1 \to N\mathcal{J}_0/(N\mathcal{J} \cap \mathcal{J}_0(k))^\ell \to N\mathcal{J} \cap N\mathcal{J}_0(K)/(N\mathcal{J} \cap \mathcal{J}_0(k))^\ell \xrightarrow{\Phi} \widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1 \to 1 ,$$

où $\mathcal{J}_0 = \mathcal{J} \cap \mathcal{J}_0(K)$.

Remarque. - L'existence de tels H-modules $\mathcal{J}$, vérifiant $\mathcal{J} \cap \mathcal{J}(K)^{\sigma-1} = \mathcal{J}^{\sigma-1}$, est assurée, et ceci quel que soit $\mathcal{H}$.

Démonstration. - L'assertion (i) est évidente. Etudions la partie (ii).

(a) *Définition d'un homomorphisme* φ *de* $N\mathcal{J} \cap N\mathcal{J}_0(K)$ *dans* $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. - Soit $a \in N\mathcal{J} \cap N\mathcal{J}_0(K)$; il existe $\mathfrak{A}_0 \in \mathcal{J}$ et $\alpha \in K_+^*$ tels que $a = N\mathfrak{A}_0 = N(\alpha A_K)$; l'idéal $\mathfrak{A}_0 \alpha^{-1} A_K$, étant de norme A_K, il existe $\mathfrak{A} \in \mathcal{J}(K)$ tel que :

(i) $\mathfrak{A}_0 = \alpha A_K \mathfrak{A}^{\sigma-1}$.

On note $\varphi(a)$ l'image de la classe de $\mathfrak{A}$ dans $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. Montrons que $\varphi(a)$ ne dépend pas des choix effectués. Si $a = N\mathfrak{A}'_0 = N(\alpha' A_K)$, $\mathfrak{A}'_0 \in \mathcal{J}$, $\alpha' \in K_+^*$, alors il existe $b \in \mathcal{J}$ et $c \in \mathcal{J}(K)$ tels que :

(ii) $\mathfrak{A}'_0 = \mathfrak{A}_0 b^{\sigma-1}$,

(iii) $\alpha' A_K = \alpha A_K c^{\sigma-1}$;

au couple $(\mathfrak{A}'_0, \alpha')$ est associé un idéal $\mathfrak{A}'$ tel que

(iv) $\mathfrak{A}'_0 = \alpha' A_K \mathfrak{A}'^{\sigma-1}$.

Les relations ci-dessus conduisent à la relation

$$\mathfrak{A}^{\sigma-1} \mathfrak{A}'^{1-\sigma} b^{\sigma-1} = \alpha' \alpha^{-1} A_K ,$$

qui montre que la classe de l'idéal $\mathfrak{A}\mathfrak{A}'^{-1} b$ est dans $\mathcal{H}_1$; comme $b \in \mathcal{J}$, $\mathfrak{A}$ et $\mathfrak{A}'$ ont la même image dans $\widetilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1$. On a bien un homomorphisme, et on vérifie qu'il est surjectif.

(b) *Définition de* $\bar{\varphi}$. - On vérifie que le noyau de φ contient $(N\mathcal{J} \cap \mathcal{J}_0(k))^\ell$; d'où l'homomorphisme $\bar{\varphi}$ par passage au quotient.

(c) *Noyau de* $\bar{\varphi}$. - Si $a \in N\mathcal{J}_0$, $a = N(\alpha A_K)$ avec $\alpha A_K \in \mathcal{J}$; on a alors

$$\alpha A_K = \alpha A_K (A_K)^{\sigma-1} \quad \text{et} \quad \varphi(a) = 1 .$$

Réciproquement, soient $\mathfrak{A}_0 \in \mathcal{J}$ et $\alpha \in K_+^*$ tels que $\mathfrak{A}_0 = \alpha A_K \mathfrak{A}^{\sigma-1}$, la classe de $\mathfrak{A}$ étant dans $\mathcal{H}\mathcal{H}_1$; il existe $\beta \in K_+^*$, $\mathfrak{A}_1 \in \mathcal{J}$ et $\mathfrak{A}'_1 \in \mathcal{J}$ avec $cl(\mathfrak{A}'_1) \in \mathcal{H}_1$ tels que $\mathfrak{A} = \mathfrak{A}_1 \mathfrak{A}'_1 \beta A_K$; alors

$$\mathfrak{A}^{\sigma-1} = \mathfrak{A}_1^{\sigma-1}\,\mathfrak{A}_1'^{\sigma-1}\,\beta^{\sigma-1}\,A_K\ ,$$

soit $\mathfrak{A}^{\sigma-1} = \mathfrak{A}_1^{\sigma-1}\,\beta^{\sigma-1}\,\gamma A_K$ en écrivant $\mathfrak{A}_1'^{\sigma-1}$ sous la forme γA_K (on a alors $\gamma \in K_+^*$ et $N\gamma \in E_k^+$). On a donc

$$\alpha A_K = \mathfrak{A}_0\,\mathfrak{A}_1^{\sigma-1}\,\beta^{\sigma-1}\,\gamma A_K\ ,$$

d'où

$$\gamma^{-1}\,\alpha\beta^{1-\sigma}\,A_K = \mathfrak{A}_0\,\mathfrak{A}_1^{\sigma-1}\ ;$$

comme $\mathfrak{A}_0$ et $\mathfrak{A}_1$ sont dans $\mathfrak{J}$, on a

$$\mathfrak{A}_0\,\mathfrak{A}_1^{\sigma-1} = \gamma^{-1}\,\alpha\beta^{1-\sigma}\,A_K \in \mathfrak{J}_0\ ,$$

d'où

$$N(\gamma^{-1}\,\alpha\beta^{1-\sigma}\,A_K) = N(\alpha A_K) = a\ ,$$

et a est bien un élément de $N\mathfrak{J}_0$.

3. Enoncé des résultats.

Nous avons en vue une formule explicite donnant la valeur de $|\mathcal{H}/\mathcal{H}|$ généralisant ainsi l'expression de $|\mathcal{H}_1|$ (théorème I.1) (laquelle correspond à $\mathcal{H} = \{1\}$). Pour cela, nous allons chercher à remplacer les groupes d'idéaux qui interviennent dans la suite exacte du théorème précédent par des groupes de nombres convenables.

(a) Préliminaires.

DEFINITION I.1. - Posons $I_0 = N\mathfrak{J} \cap \mathfrak{J}_0(k)$, et considérons la suite exacte

$$1 \to E_k^+ \to k_+^* \xrightarrow{\psi} \mathfrak{J}_0(k) \to 1\ ,$$

où k_+^* désigne le sous-groupe de k^* formé des éléments totalement positifs ; on pose $\Lambda = \psi^{-1}(I_0)$.

PROPOSITION I.3. - On a

$$|\mathcal{K}/\mathcal{H}| = \frac{|\mathcal{H}(k)|}{|N\mathcal{H}|}\ \frac{|(\Lambda \cap NK^*)/\Lambda^\ell|}{|\Lambda/\Lambda^\ell|}\ \ell^{t-1}\ .$$

La démonstration se ramène essentiellement à la démonstration de l'exactitude des suites ci-dessous

$$1 \to N\mathfrak{J}_0/I_0^\ell \to (I_0 \cap N\mathfrak{J}_0(K))/I_0^\ell \to \mathcal{K}/\mathcal{H}\mathcal{H}_1 \to 1$$

(qui n'est autre que celle du théorème I.2),

$$1 \to (E_k^+ \cap NK^*)/E_k^{+\ell} \to (\Lambda \cap NK^*)/\Lambda^\ell \to (\Lambda \cap NK^*)/\Lambda^\ell(E_k^+ \cap NK^*) \to 1\ ,$$

$$1 \to (\Lambda \cap NK^*)/\Lambda^\ell \to \Lambda/\Lambda^\ell \to \Lambda/(\Lambda \cap NK^*) \to 1\ ,$$

$$1 \to (E_k^+ \cap NK^*)/E_k^{+\ell} \to E_k^+/E_k^{+\ell} \to E_k^+/(E_k^+ \cap NK^*) \to 1\ ,$$

$$1 \to N\mathfrak{J}_0 \to N\mathfrak{J} \to \mathcal{H}/\mathcal{H}^{\sigma-1} \to 1\ ,$$

$$1 \to \mathcal{H}_1 \cap \mathcal{H} \to \mathcal{H} \xrightarrow{\sigma-1} \mathcal{H}^{\sigma-1} \to 1\ ,$$

$$1 \to E_k^+/E_k^{+\ell} \to \Lambda/\Lambda^\ell \to I_0/I_0^\ell \to 1 ,$$

et des isomorphismes suivants :

$$(\Lambda \cap N\mathfrak{K}^*)/\Lambda^\ell(E_k^+ \cap N\mathfrak{K}^*) \simeq (I_0 \cap N\mathfrak{J}_0(K))/I_0^\ell ,$$

$$N\mathfrak{J}/I_0 \simeq N\mathfrak{K} .$$

(b) Evaluation du terme $|(\Lambda \cap N\mathfrak{K}^*)/\Lambda^\ell|/|\Lambda/\Lambda^\ell|$. - Introduisons maintenant le symbole de Hilbert. Soit ζ une racine primitive ℓ-ième de l'unité, et soient K' et k' les corps obtenus en adjoignant à K et k le nombre ζ . L'extension K'/k' est une extension de Kummer, et il existe $\alpha \in k'$ tel que $K' = k'(\sqrt[\ell]{\alpha})$.

Soit $a \in k^*$; a est une norme dans l'extension K/k si, et seulement si, le symbole de Hilbert $(\alpha , a)_\wp = 1$ pour toute place $\wp$ de k' en vertu du théorème des normes de Hasse et des propriétés du symbole de Hilbert ; les lois de réciprocité globales entraînent alors la formule du produit :

$$\prod_\wp (\alpha , \beta)_\wp = 1 , \quad \alpha , \beta \in k' \qquad (\text{cf } [10], \text{ p. } 228\text{-}229).$$

Dans le cas particulier où $a \in k$, on peut démontrer le résultat suivant.

PROPOSITION 1.4. - Soit K/k une extension cyclique de degré ℓ ; soient $K' = K(\zeta)$ et $k' = k(\zeta)$; si $\alpha \in k'$ est tel que $K' = k'(\sqrt[\ell]{\alpha})$ et si $a \in k$, on a

$$(\alpha , a)_\wp = (\alpha , a)_{\wp'} ,$$

pour tout idéal $\wp'$ conjugué de $\wp$ dans k'/k .

Remarque. - Le symbole $(\alpha , a)_\wp$ peut donc se noter par abus $(\alpha , a)_p$ avec $p = \wp \cap A_k$.

La détermination de $(\Lambda \cap N\mathfrak{K}^*)/\Lambda^\ell$ est ramenée à un calcul explicite de symboles.

PROPOSITION I.5. - Soit q l'homomorphisme canonique $\Lambda \to \Lambda/\Lambda^\ell$, et soit $q(a_1)$, ... , $q(a_n)$ une F_ℓ-base de Λ/Λ^ℓ ; le nombre $|\Lambda/\Lambda^\ell|/|(\Lambda \cap N\mathfrak{K}^*)/\Lambda^\ell|$ est égal à ℓ^r , où r est le rang du système linéaire homogène défini sur F_ℓ par les t équations :

$$\prod_{i=1}^n (\alpha , a_i)_p^{x_i} = 1 ,$$

pour tout idéal p ramifié dans K/k .

En outre, on a les relations :

$$0 \leqslant r \leqslant t - 1 \quad \text{pour} \quad t \geqslant 1 , \text{ et } \quad r = 0 \quad \text{si} \quad t = 0 .$$

On peut alors rassembler les résultats obtenus dans le théorème suivant.

THÉORÈME I.3. - Soit $\mathfrak{K}$ un sous-H-module de $\mathfrak{K}(K)$; soit $\mathfrak{J}$ un sous-H-module de $\mathfrak{J}(K)$ dont l'image dans $\mathfrak{K}(K)$ est égale à $\mathfrak{K}$ et tel que $\mathfrak{J} \cap \mathfrak{J}(K)^{\sigma-1} = \mathfrak{J}^{\sigma-1}$; soit $\Lambda = \psi^{-1}(N\mathfrak{J} \cap \mathfrak{J}_0(k))$ le groupe de nombres associé à $\mathfrak{J}$, et soit $q(a_1),\ldots,q(a_n)$, $a_i \in \Lambda$, une base de Λ/Λ^ℓ ; alors

$$|\mathcal{K}/\mathcal{H}| = \frac{|\mathcal{H}(k)|}{|N\mathcal{K}|}\, \ell^{t-1-r} ,$$

où $t \geqslant 0$ est le nombre d'idéaux ramifiés dans K/k, et où $r \leqslant t-1$ est le rang du système linéaire sur F_ℓ :

$$\prod_{i=1}^{n} (\alpha , a_i)_{\mathfrak{p}}^{x_i} = 1 , \text{ pour tout } \mathfrak{p} \text{ ramifié dans } K/k .$$

II. Conséquences des résultats obtenus.

1. Cas du corps des rationnels.

Si $k = \mathbb{Q}$, l'expression de $|\mathcal{K}/\mathcal{H}|$ est alors $|\mathcal{K}/\mathcal{H}| = \ell^{t-1-r}$.

Considérons alors $\mathcal{H} = \mathcal{H}_1$; comme $E_{\mathbb{Q}}^{+} = \{1\}$, il résulte du corollaire I.2 que $\mathcal{H}_1$ est engendré par les classes des idéaux premiers ramifiés dans $K/\mathbb{Q}$; si $p_1 , \dots , p_t$ sont ces nombres premiers, on peut prendre (relativement à $\mathcal{H} = \mathcal{H}_1$) le groupe, engendré par $p_1 , \dots , p_t$, $\Lambda = \langle p_1 , \dots , p_t \rangle$; l'existence de classes d'ordre ℓ, non invariantes par H, est équivalente à la relation $|\mathcal{K}_1/\mathcal{H}_1| > 1$, soit $t - 1 > r$. (cf. résultats numériques pour $\ell = 3$ dans [3].)

2. Exemple de structure de $\mathcal{H}(K)$.

Le résultat suivant se démontre sans difficultés.

PROPOSITION II.1. - Soit n le plus grand entier tel que $\mathcal{H}_n = \mathcal{H}(K)$; on pose $n = a(\ell - 1) + b$, $a \geqslant 0$, $0 \leqslant b < \ell - 1$. On suppose que les quotients $\mathcal{H}_{i+1}/\mathcal{H}_i$ sont d'ordre ℓ pour $0 \leqslant i < n$. Alors :

(i) si $\mathcal{H}_{(K)}^{\nu} = \{1\}$, $\mathcal{H}(K)$ est isomorphe à $(\mathbb{Z}/\ell^{a+1}\mathbb{Z})^{b} (\mathbb{Z}/\ell^{a}\mathbb{Z})^{\ell-1-b}$;

(ii) si $\mathcal{H}_{(K)}^{\nu} \neq \{1\}$, $\mathcal{H}(K)$ est isomorphe à l'un des trois groupes suivants :

$(\mathbb{Z}/\ell\mathbb{Z})^{\ell}$; $(\mathbb{Z}/\ell^2\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})^{\lambda}$ avec $\lambda \leqslant \ell - 1$; $(\mathbb{Z}/\ell^{a+1}\mathbb{Z})^{b} \times (\mathbb{Z}/\ell^{a}\mathbb{Z})^{\ell-1-b}$.

On peut donc appliquer cette proposition dans les trois cas suivants :

(i) $|\mathcal{H}(k)| = 1$, $|E_k^{+}/(E_k^{+} \cap NK^{*})| = \ell^{t-2}$ $(t \geqslant 2)$;

(ii) $|\mathcal{H}(k)| = \ell$, $|E_k^{+}/(E_k^{+} \cap NK^{*})| = \ell^{t-1}$ $(t \geqslant 1)$;

(iii) $|\mathcal{H}(k)| = \ell^2$ et $t = 0$.

Si $k = \mathbb{Q}$, et si ℓ est impair, il ne subsiste que le cas (i) avec $t = 2$.

Remarque. - Le cas (iii) a été cité par KISILEVSKY ([6]) sous des hypothèses très particulières.

3. Comparaison des 4-rangs de $\mathbb{Q}(\sqrt{m})$ et de $\mathbb{Q}(\sqrt{-m})$ [3].

Soit m un entier sans facteurs carrés. Posons $K = \mathbb{Q}(\sqrt{m})$ et $K' = \mathbb{Q}(\sqrt{-m})$, et réservons la notation $'$ pour toute quantité qui concerne le corps K'.

Soient $p_1 , \dots , p_{t^*}$ les nombres premiers impairs ramifiés dans $K/\mathbb{Q}$ (ils se

ramifient aussi dans $K'/\mathbb{Q}$). Si 2 ne divise pas m , il est nécessairement ramifié dans K ou dans K' (et dans l'un des deux seulement), sinon il est ramifié dans les deux corps.

On aura $|\mathcal{H}_1| = 2^{t-1}$ et $|\mathcal{H}'_1| = 2^{t'-1}$, les groupes $\mathcal{H}_1$ et $\mathcal{H}'_1$ étant engendrés par les classes des idéaux premiers ramifiés. Les groupes Λ et Λ' associés seront donc

$$\Lambda = \langle p_1 , \cdots , p_{t^*} \rangle , \quad \Lambda' = \langle p_1 , \cdots , p_{t^*} , 2 \rangle \text{ ou vice-versa}$$

lorsque m est impair,

$$\Lambda = \Lambda' = \langle p_1 , \cdots , p_{t^*} , 2 \rangle \text{ lorsque 2 divise m .}$$

On forme alors les matrices A et A' des systèmes linéaires associés au groupe Λ et Λ' ; la proposition I.2 ramène la comparaison des 4-rangs R_2 et R'_2 de K et K' à la comparaison des rangs r et r' de A et A' : en effet, on a la relation $R_2 - R'_2 = t - t' + r' - r$.

Une étude directe des matrices A et A' conduit au résultat suivant (obtenu dans [3] par d'autres méthodes).

PROPOSITION II.2. - Soit m un entier sans facteurs carrés, avec $m \equiv 1 \bmod 4$ si 2 ne divise pas m et $m/2 \equiv 1 \bmod 4$ sinon. Les 4-rangs R_2 et R'_2 de $\mathbb{Q}(\sqrt{m})$ et $\mathbb{Q}(\sqrt{-m})$ différent d'une unité au plus. De façon plus précise :

$$R_2 \leqslant R'_2 \leqslant R_2 + 1 \qquad \text{pour } m > 0 ,$$

$$R_2 - 1 \leqslant R'_2 \leqslant R_2 \qquad \text{pour } m < 0 .$$

III. Méthodes effectives. Résultats numériques.

1. Construction des extensions cycliques de degré ℓ de $\mathbb{Q}$.

La théorie de Galois permet de caractériser les extensions cycliques de degré ℓ d'un corps k dans le cadre de la théorie de Kummer appliquée au corps $k' = k(\zeta)$. Soit $G = \mathrm{Gal}(k'/k)$; si s est un générateur de G , on pose $\zeta^s = \zeta^\chi$, où χ est un entier défini modulo ℓ ; on note $\mathfrak{X}^*$ l'ensemble des éléments $\bar{\alpha}$ de $k'^*/k'^{*\ell}$ qui vérifient $\alpha^s = \bar{\alpha}^\chi$; $\mathfrak{X}^*$ est un sous-$\mathbb{F}_\ell$-espace de $k'^*/k'^{*\ell}$.

Associons à K/k (cyclique de degré ℓ) un nombre $\alpha \in k'^*$ tel que

$$K' = K(\zeta) = k'(\sqrt[\ell]{\alpha}) ;$$

K/k est déterminée par l'image de α dans l'espace projectif $\mathbb{P}(k'^*/k'^{*\ell})$. On est alors conduit au résultat suivant.

PROPOSITION III.1. - L'application qui associe à K/k un point de $\mathbb{P}(k'^*/k'^{*\ell})$ est une bijection de l'ensemble des extensions cycliques de degré ℓ de k sur $\mathbb{P}(\mathfrak{X}^*)$.

Supposons maintenant $k = \underset{\sim}{Q}$, posons $\underset{\sim}{Q}' = \underset{\sim}{Q}(\zeta_0)$ et $\mathfrak{P}_0 = (1 - \zeta_0)$ idéal premier au-dessus de ℓ dans $\underset{\sim}{Q}'$.. Etant donné $K/\underset{\sim}{Q}$ cyclique de degré ℓ et $\alpha \in \underset{\sim}{Q}'$ choisi congru à 1 modulo $\mathfrak{P}_0$ et définissant $K' = \underset{\sim}{Q}'(\sqrt[\ell]{\alpha})$, on note $p_1, \dots, p_t$ les nombres premiers ramifiés dans $K/\underset{\sim}{Q}$ et, pour tout i, $1 \leqslant i \leqslant t$, on fait choix d'un idéal premier $\mathfrak{P}_i$ de $\underset{\sim}{Q}'$ au-dessus de p_i. On construit un t-uple $(v_1, \dots, v_t) \in \underset{\sim}{F}_\ell^t$ de la manière suivante :

$$v_i \equiv v_{\mathfrak{P}_i}(\alpha) \quad \text{modulo } \ell \quad \text{si} \quad \mathfrak{P}_i \neq \mathfrak{P}_0 ,$$

$$v_i \equiv \frac{\alpha - 1}{1 - \zeta_0} \quad \text{modulo } \mathfrak{P}_0 \quad \text{si} \quad \mathfrak{P}_i = \mathfrak{P}_0 .$$

Soit $\underset{\sim}{V}$ le quotient de

$$\{(v_1, \dots, v_t) \in \underset{\sim}{F}_\ell^t , \ v_i \neq 0 \ \text{pour tout } i , \ 1 \leqslant i \leqslant t\} ,$$

par la relation d'équivalence définissant l'espace projectif $\underset{\sim}{P}(\underset{\sim}{F}_\ell^t)$; on est alors conduit à énoncer la proposition suivante.

PROPOSITION III.2. - *Etant donné un choix des idéaux $\mathfrak{P}_i$ et de la racine primitive ℓ-ième de l'unité ζ_0, la construction du t-uple $(v_1, \dots, v_t) \in \underset{\sim}{F}_\ell^t$ à partir du nombre α définit une application bijective de $\underset{\sim}{P}(\mathfrak{X}^*)$ sur l'ensemble $\underset{\sim}{V}$.*

Remarque III.1. - $\operatorname{card}(\underset{\sim}{V}) = (\ell - 1)^{t-1}$.

Les notations introduites dans ce paragraphe sont valables dans toute la suite.

2. Système linéaire associé à Λ.

Soient $p_1, \dots, p_t$ les nombres premiers ramifiés dans $K/\underset{\sim}{Q}$; si ℓ est ramifié, on posera $\ell = p_t$.

Pour simplifier, nous ferons l'hypothèse suivante :

$$\mathcal{H} \text{ contient } \mathcal{H}_1 ;$$

on peut alors supposer que le groupe $\mathcal{J}$ associé contient les idéaux premiers $p_1, \dots, p_t$ ramifiés dans $K/\underset{\sim}{Q}$. Il en résulte alors que le groupe $\mathcal{N}/\mathcal{N}^\ell$ associé à $\mathcal{J}$ possède une base de la forme :

$$q(a_1), \dots, q(a_n) \quad \text{avec} \quad a_i = p_i \quad \text{pour} \quad 1 \leqslant i \leqslant t ,$$

et a_i premier à $p_1 \dots p_t$ pour tout $i > t$.

DÉFINITION III.1. - *Soit $\mathfrak{P}$ un idéal premier dans $\underset{\sim}{Q}'$; on note $n_{\mathfrak{P}}$ le nombre de conjugués distincts de $\mathfrak{P}$ dans $\underset{\sim}{Q}'/\underset{\sim}{Q}$ et on pose, pour $a \in \underset{\sim}{Q}$,*

$$[a]_{\mathfrak{P}} = (p , a)_{\mathfrak{P}} , \quad (p) = \mathfrak{P} \cap \underset{\sim}{Z} , \quad \mathfrak{P} \neq \mathfrak{P}_0 ,$$

$$[a]_{\mathfrak{P}_0} = (\zeta_0 , a)_{\mathfrak{P}_0} \quad \text{sinon.}$$

Les calculs effectifs de [10] (Prop. 8, p. 217 et Prop. 5, p. 236) permettent alors de démontrer le résultat suivant.

PROPOSITION III.3. - Soit $p = p_i$, et soit $a \in \underset{\sim}{Q}$ premier à p_i ; alors

$$(\alpha , a)_{p_i} = [a]_{\wp_i}^{-v_i n_{\wp_i}} ,$$

où $(v_1 , \dots , v_t)$ est le t-uple défini à partir de α.

Remarque III.2. - Si $p_i \neq \ell$, on a

$$(\alpha , a)_{\wp_i} \equiv (a^{-v_i})^{(p_i-1)/\ell} \quad \text{modulo } \wp_i ,$$

Si $p_i = \ell$, on a

$$(\alpha , a)_{\ell} = \zeta_0^{v_t((a^{\ell-1}-1)/\ell)} .$$

Ces relations prenettent un calcul effectif des symboles $(\alpha , a)_{\wp}$ lorsque a est premier à $\wp$.

Posons, pour simplifier l'écriture :

$$n_i = n_{\wp_i} , \quad [a]_i = [a]_{\wp_i} \quad \text{et} \quad (\alpha , a_i)_j = (\alpha , a_i)_{\wp_j} .$$

On démontre alors, en utilisant notamment la formule du produit, le théorème suivant.

THÉORÈME III.1. - Soit Λ un groupe de nombres associé au quotient $\mathcal{K}/\mathcal{K}$. On suppose que Λ/Λ^{ℓ} possède une base de la forme $q(p_1) , \dots , q(p_t) , q(a_{t+1}) , \dots , q(a_n)$ avec a_i premier à $p_1 \dots p_t$ pour $i > t$. Le système linéaire

$$\prod_{i=1}^{n} (\alpha , a_i)_j^{x_i} = 1 , \quad 1 \leqslant j \leqslant t ,$$

s'écrit :

$$\prod_{i=1}^{n} [a_i]_j^{v_j x_i} \prod_{k=1}^{t} [a_j]_k^{-v_k x_j} = 1 , \quad 1 \leqslant j \leqslant t .$$

COROLLAIRE. - Lorsque $\mathcal{K} = \mathcal{K}_1$, le système associé à $\Lambda = \langle p_1 , \dots , p_t \rangle$ est

$$\prod_{i=1}^{t} ([p_i]_j^{v_j x_i} [p_j]_i^{-v_i x_j}) = 1 , \quad 1 \leqslant j \leqslant t .$$

Remarque. - Il suffit de poser $[a_i]_j = \zeta_0^{a_{ij}}$ pour avoir les systèmes ci-dessus, écrits en notation additive,

$$\sum_{i=1}^{n} a_{ij} v_j x_i - \sum_{k=1}^{t} a_{jk} v_k x_j = 0 , \quad 1 \leqslant j \leqslant t .$$

3. Cas particulier $\mathcal{K} = \mathcal{K}_1$.

Dans ce cas, la dimension de $\mathcal{K}_2/\mathcal{K}_1$ est égale à $t - 1 - r$, où r est le rang du système

$$\sum_{i=1}^{t} (a_{ij} v_j x_i - a_{ji} v_i x_j) = 0 , \quad 1 \leqslant j \leqslant t .$$

PROPOSITION III.4. - Le rang r est égal à 0 si, et seulement si, p_i est congru à une puissance ℓ-ème modulo p_j pour tout $i , j , i \neq j$, en remplaçant cette

condition par $p_i \equiv 1$ modulo ℓ^2 lorsque $p_t = \ell$. En outre, lorsque $r = 0$ pour K, on a $r = 0$ relativement aux $(\ell - 1)^{t-1}$ extensions ayant même discriminant que K.

Ce résultat provient, d'une part, de la forme du système et, d'autre part, des formules explicites pour le calcul des $[a_i]_j$, $i \neq j$ (cf. Remarque III.2).

PROPOSITION III.5. - Lorsque $t = 2$, l'ordre du groupe $\mathcal{H}_2$ est le même pour les $\ell - 1$ extensions $K/\mathbb{Q}$ ramifiées en p_1, p_2.

Démonstration. - Pour $t = 2$, le système correspondant à $\mathcal{H} = \mathcal{H}_1$ s'écrit :

$$\begin{cases} -a_{12} v_2 x_1 + a_{21} v_1 x_2 = 0 \\ a_{12} v_2 x_1 - a_{21} v_1 x_2 = 0 \end{cases}$$

et son rang (égal à 0 ou 1) ne dépend pas du couple (v_1, v_2).

Ce résultat devient faux, en général, pour $t > 2$ (cf. contre-exemple donné dans [4]).

4. Etude du cas $\ell = 3$.

Lorsque ℓ est égal à 3, on a la relation (proposition I.1) $\mathcal{H}^{(1)} = \mathcal{H}_2$, d'où par la proposition I.2, la proposition ci-dessous.

PROPOSITION III.6. - Le 3-rang d'une extension cubique cyclique de $\mathbb{Q}$ est donné par la formule :

$$R_1 = 2(t - 1) - r ,$$

où r est le rang du système linéaire attaché au groupe $\Lambda = \langle p_1, \ldots, p_t \rangle$ [1].

5. Algorithme.

Etant donnée une extension cyclique de degré ℓ, $K/\mathbb{Q}$, la détermination de $\mathcal{H}(K)$ est algorithmique. Outre des opérations élémentaires (décomposition d'un idéal en produit d'idéaux premiers, calcul des symboles de Hilbert, calcul du rang d'un système linéaire, ...), l'algorithme se ramène essentiellement à la résolution d'équations du type

$$N\alpha = a , \quad a \in \mathbb{Q} ,$$

ceci n'est pas trop difficile en pratique car on n'impose pas à α d'être entier (les cas $\ell = 2$ et $\ell = 3$ se traitent en général sans difficultés).

En résumé : Supposons avoir déterminé $\mathcal{H}_i$; on connait donc un sous-H-module $\mathcal{J}_i$ de $\mathcal{J}(K)$ dont l'image dans $\mathcal{H}(K)$ est $\mathcal{H}_i$ (tel que $\mathcal{J}_i \cap \mathcal{J}^{\sigma-1}(K) = \mathcal{J}_i^{\sigma-1}$) ainsi que le groupe de nombres Λ_i associé. Le système linéaire du théorème III.1 permet de trouver des éléments $a \in \Lambda_i$ qui sont normes dans $K/\mathbb{Q}$.

Ayant résolu les équations $N\alpha = a$, correspondant aux solutions indépendantes du

système, on utilise l'homomorphisme φ (défini dans le théorème I.2) qui conduit immédiatement à la détermination de $\mathcal{H}_{i+1} = \mathcal{H}_i$ par l'intermédiaire d'un groupe $\mathcal{J}_{i+1}$.

Remarque. - Cet algorithme généralise, pour $\ell = 2$, celui de [8] qui permet d'atteindre $\mathcal{H}_3$. Il est à rapprocher de celui de [9], également pour $\ell = 2$.

Exemple : Corps cubiques de discriminants $(7.673)^2$: Corps définis par le polynôme :

$$X^3 - 3.7.673\,X - 113.7.673 .$$

Si θ est une racine de ce polynôme, les nombres

$$\alpha_1 = \frac{13.7 + \theta}{3} \quad \text{et} \quad \alpha_2 = \frac{673 + 5\theta + 5\theta'}{3}$$

sont des entiers dont les polynômes irréductibles sont respectivement :

$$X^3 - 13.7\,X^2 + 170.7\,X - 7 \quad \text{et} \quad X^3 - 673\,X^2 + 166.673\,X - 3^3.673 .$$

On a

$$\alpha_1\,A_K = \mathfrak{p}_7 \quad \text{et} \quad A_K = \mathfrak{p}_{673}\cdot\mathfrak{p}_3^3 , \text{ et } \alpha_1\,A_K = \mathfrak{p}_7\,A_K^{\sigma-1} , \quad \alpha_2/3\,A_K = \mathfrak{p}_{673}(\mathfrak{p}_3^{2+\sigma})^{1-\sigma} .$$

On peut donc écrire

$$\mathcal{J}_2 = \langle \mathfrak{p}_7 , \mathfrak{p}_{673} , \mathfrak{p}_3^{2+\sigma} , \mathfrak{p}_3^{\sigma(2+\sigma)} , \mathfrak{p}_3^{\sigma^2(2+\sigma)} \rangle \quad \text{et} \quad \Lambda_2 = \langle 7 , 673 , 3^3 \rangle .$$

le rang r_2 est alors nul, et $|\mathcal{H}_3/\mathcal{H}_2| = 3$.

Ecrivons maintenant que 3^3 est norme : $3^3\,\mathbb{Z} = N(3) = N(\mathfrak{p}_3^{2+\sigma})$, soit

$$3A_K = \mathfrak{p}_3^{2+\sigma}\,\mathfrak{p}_3^{(\sigma+1)(\sigma-1)} ;$$

d'où $\mathcal{J}_3 = \langle \mathfrak{p}_7 , \mathfrak{p}_{673} , \mathfrak{p}_3^{\sigma+2} , \cdots , \mathfrak{p}_3^{\sigma+1} , \cdots \rangle = \langle \mathfrak{p}_7 , \mathfrak{p}_{673} , \mathfrak{p}_3 , \cdots \rangle$ et $\Lambda_3 = \langle 7 , 673 , 3 \rangle$; 3 n'étant pas reste cubique modulo 7 , il en résulte $r_3 = 1$ et $|\mathcal{H}_4/\mathcal{H}_3| = 1$.

On en déduit que $|\mathcal{H}(K)| = 27$ et que $\mathcal{H}(K)$ est isomorphe à $(\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

On peut vérifier que le corps défini par le polynôme $X^3 - 3.7.673\,X - 76.7.673$ a aussi la propriété $|\mathcal{H}(K)| = 27$. Nous avons d'ailleurs réeemment démontré que, pour $t \neq 2$, lorsque un corps K est tel que $|\mathcal{H}_3/\mathcal{H}_2| = \ell$, alors il en est de même pour les $\ell - 1$ corps de même discriminant.

Conclusion [ajoutée à la correction des épreuves, le 1er décembre 1972]. - La méthode exposée est suffisamment générale pour permettre une étude systématique des des problèmes de ℓ-classes d'idéaux dans le cas cyclique de degré ℓ , et suffisamment explicite pour conduire à de nombreuses illustrations numériques (pour des exemples de l'un et l'autre de ces deux aspects, et aussi pour les démonstrations non mentionnées ici, se reporter à :

GRAS (Georges). - Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ . - Saint-Martin d'Hères, Université de Grenoble-I, Institut de Mathématiques pures, 1972 (Thèse Sc. math., Grenoble 1972) [multigraphiée].

pour $t = 3$ ($R_1 = 4$) et p_1 , p_2 , $p_3 < 1000$.

3	271	919	67	193	643	151	331	409	349	877	967
3	307	523	67	283	349	151	331	547	367	439	733
3	307	919	73	103	439	151	331	727	379	463	733
3	523	757	79	97	337	151	331	877	379	691	937
3	577	757	79	97	433	157	373	787	397	613	907
3	577	991	79	157	337	157	373	883	397	631	919
3	757	991	79	157	877	157	379	601	397	907	919
3	919	991	79	283	349	157	379	877	433	571	787
7	181	673	79	349	877	157	439	727	457	673	997
7	337	811	79	433	631	163	313	349	457	877	997
7	673	769	79	631	859	199	733	859	523	673	757
13	421	499	79	673	757	241	379	877	577	757	991
13	499	853	79	673	769	241	457	829	691	757	907
19	151	691	97	313	463	241	457	877	727	823	919
19	373	577	103	823	919				877	967	997
31	163	349	103	919	991	271	571	661			
31	373	883	127	619	643	271	823	919			
37	103	991	127	673	757	277	541	757			
37	433	739	139	199	661	283	313	349			
43	193	409	139	373	769	307	421	499			
43	613	643	139	631	661	307	499	523			
61	163	313	151	211	367	307	523	739			
61	241	877	151	283	691	349	661	877			

BIBLIOGRAPHIE

[1] BAUER (Helmut). - Über die kubischen Klassenkörper zyklischer kubischer Zahlkörper, Dissertation Universität Karlsruhe, 1969.

[2] CHEVALLEY (C.). - Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sc. Univ. Tokyo, t. 2, 1929-1934, p. 365-476 (Thèse Sc. math. Paris, 1934).

[3] DAMEY (P.) et PAYAN (J.-J.). - Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2 , J. für die reine und angew. math., t. 244, 1970, p. 37-54.

[4] GRAS (G.). - Sur le ℓ-groupe des classes des extensions cycliques de degré premier ℓ , C. R. Acad. Sc. Paris, t. 274, 1972, Série A, p. 1145-1148.

[5] IWASAWA (K.). - A note on the group of units of an algebraic number field, J. Math. pures et appl., 9e série, t. 35, 1956, p. 189-192.

[6] KISILEVSKY (H.). - Some results related to Hilbert's theorem 94, J. of Number Theory, t. 2, 1970, p. 199-206.

[7] LEOPOLDT (H. W.). - Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., t. 9, 1953, p. 351-362.

[8] REDEI (L.) und REICHARDT (H.). - Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlköpers, J. für die reine und angew. Math., t. 170, 1933, p. 69-74.

[9] SHANKS (D.). - Gauss's ternary form reduction and the 2-sylow subgroup, Math. of Comput., t. 25, 1971, p. 837-853.

[10] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[11] TAUSSKY (O.). - A remark concerning Hilbert's theorem 94, J. für die reine und angew. Math., t. 239/240, 1970, p. 435-438.

Georges GRAS
Université de Grenoble-I
Inst. Math. pures, Boîte postale 116
38402 SAINT MARTIN D'HERES

(Texte reçu le 6 juillet 1972)