SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

G. GRAS

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

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 85-103

<http://www.numdam.org/item?id=STNG_1971-1972__1__85_0>

ETUDE DU ℓ-GROUPE DES CLASSES DES EXTENSIONS CYCLIQUES DE DEGRE ℓ .

par G. GRAS le 26.4.72

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 $Gal(K/k)$ par la formule (pour ℓ impair) :

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

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 ([1], 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 E_k^+ les unités de k totalement positives.

Un résultat facile de Leopoldt ([6], 1953) montre que lorsque $k = \mathbb{Q}$, le ℓ-rang R_1 du groupe des classes de K vérifie les inégalités

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

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 - RESULTATS GENERAUX.

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. $\mathcal{J}_o(K)$) 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 , $\mathcal{J}(k)$, $\mathcal{J}_o(k)$ et $\mathcal{H}(k)$ se définissent de façon analogue.

Si $\mathcal{J}$ est un sous-groupe quelconque de $\mathcal{J}(K)$ on pose $\mathcal{J}_o = \mathcal{J} \cap \mathcal{J}_o(K)$. 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 :

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*

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

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 :

$$1 \to \mathcal{H}_1^o \to \mathcal{H}_1 \to E_k^+ \cap NK^*/NE_K^+ \to 1 \ ,$$

$\mathcal{H}_1^o$ désignant le sous-groupe de $\mathcal{H}_1$ formé des classes les 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 $\mathbb{F}_\ell$ de $\mathcal{H}^{\ell^{q-1}}(K)/\mathcal{H}^{\ell^q}(K)$) ; alors R_q est égal à la dimension sur $\mathbb{F}_\ell$ 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 $\mathfrak{H}$ un sous-H-module de $\mathfrak{H}(K)$ et soit $\tilde{\mathfrak{H}}$ l'ensemble formé des $h \in \mathfrak{H}(K)$ tels que $h^{\sigma-1} \in \mathfrak{H}$;

(i) $\tilde{\mathfrak{H}}$ est un sous-H-module de $\mathfrak{H}(K)$ qui contient $\mathfrak{H}$ et $\mathfrak{H}_1$.

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

$$1 \to N\mathcal{J}_o/(N\mathcal{J} \cap \mathcal{J}_o(k))^\ell \to N\mathcal{J} \cap N\mathcal{J}_o(K)/(N\mathcal{J} \cap \mathcal{J}_o(k))^\ell \xrightarrow{\bar{\varphi}} \tilde{\mathfrak{H}}/\mathfrak{H}\mathfrak{H}_1 \to 1 \ ,$$

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

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 $\mathfrak{H}$.

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

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

$$\text{(i)} \quad \mathfrak{U}_o = \alpha A_K \mathfrak{U}^{\sigma-1} \ .$$

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

$$\text{(ii)} \quad \mathfrak{U}'_o = \mathfrak{U}_o b^{\sigma-1} \ ,$$

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

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

$$\text{(iv)} \quad \mathfrak{U}'_o = \alpha' A_K \mathfrak{U}'^{\sigma-1} \ .$$

Les relations ci-dessus conduisent à la relation

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

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

b) Définition de $\bar{\varphi}$.

La relation $\nu = (\sigma-1)^{\ell-1} - \ell A(\sigma)$ montre que l'on a l'inclusion $\tilde{\mathfrak{H}}^{\ell} \subset \mathfrak{H}\mathfrak{H}_1$. Il en résulte que le noyau de φ contient $(N\mathcal{J}\cap\mathcal{J}_o(k))^{\ell}$; d'où l'homomorphisme $\bar{\varphi}$ par passage au quotient.

c) Noyau de $\bar{\varphi}$.

Si $\mathfrak{a} \in N\mathcal{J}_o$, $\mathfrak{a} = N(\alpha A_K)$ avec $\alpha A_K \in \mathcal{J}$; on a alors $\alpha A_K = \alpha A_K (A_K)^{\sigma-1}$ et $\varphi(\mathfrak{a}) = 1$.

Réciproquement, soient $\mathfrak{A}_o \in \mathcal{J}$ et $\alpha \in K_+^*$ tels que $\mathfrak{A}_o = \alpha A_K \mathfrak{A}^{\sigma-1}$, la classe de $\mathfrak{A}$ étant dans $\mathfrak{H}\mathfrak{H}_1$; il existe $\beta \in K_+^*$, $\mathfrak{A}_1 \in \mathcal{J}$ et $\mathfrak{A}'_1 \in \mathcal{J}$ avec $cl(\mathfrak{A}'_1) \in \mathfrak{H}_1$ 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 $\alpha A_K = \mathfrak{A}_o\mathfrak{A}_1^{\sigma-1}\beta^{\sigma-1}\gamma A_K$, d'où $\gamma^{-1}\alpha\beta^{1-\sigma}A_K = \mathfrak{A}_o\mathfrak{A}_1^{\sigma-1}$; comme $\mathfrak{A}_o$ et $\mathfrak{A}_1$ sont dans $\mathcal{J}$, on a $\mathfrak{A}_o\mathfrak{A}_1^{\sigma-1} = \gamma^{-1}\alpha\beta^{1-\sigma}A_K \in \mathcal{J}_o$, d'où $N(\gamma^{-1}\alpha\beta^{1-\sigma}A_K) = N(\alpha A_K) = \mathfrak{a}$ et $\mathfrak{a}$ est bien un élément de $N\mathcal{J}_o$.

3. Enoncé des résultats.

Nous avons en vue une formule explicite donnant la valeur de :

$$|\tilde{\mathfrak{H}}/\mathfrak{H}|$$

généralisant ainsi l'expression de $|\mathfrak{H}_1|$ (théorème I.1) (laquelle correspond à $\mathfrak{H} = \{1\}$). 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.

Définition I.1.

Posons $I_o = N\mathcal{J} \cap \mathcal{J}_o(k)$ et considérons la suite exacte :

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

où k_+^* désigne le sous-groupe de k^* formé des éléments totalement positifs ; on pose :

$$\Lambda = \psi^{-1}(I_o) .$$

Proposition I.3.

On a :

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

La démonstration se ramène essentiellement à la démonstration de l'exactitude des suites de $\mathbb{F}_\ell$-espaces vectoriels suivantes :

$$1 \to N\mathcal{J}_o/I_o^\ell \to I_o \cap N\mathcal{J}_o(K)/I_o^\ell \to \tilde{\mathcal{H}}/\mathcal{H}\mathcal{H}_1 \to 1$$

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

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

$$1 \to \Lambda \cap NK^*/\Lambda^\ell \to \mathcal{N}/\Lambda^\ell \to \mathcal{N}/\Lambda \cap NK^* \to 1 ,$$

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

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

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

$$1 \to E_k^+/E_k^{+\ell} \to \mathcal{N}/\Lambda^\ell \to I_o/I_o^\ell \to 1 ,$$

et des isomorphismes suivants :

$$\Lambda \cap NK^*/\Lambda^\ell(E_k^+ \cap NK^*) \simeq I_o \cap N\mathcal{J}_o(K)/I_o^\ell ,$$

$$N\mathcal{J}/I_o \simeq N\mathcal{H} .$$

b) Evaluation du terme $\dfrac{|\Lambda \cap NK^*/\Lambda^\ell|}{|\mathcal{N}/\Lambda^\ell|}$.

Introduisons maintenant le symbole de Hilbert. Soit ζ une racine primitive $\ell^{\text{ème}}$ 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 c'est une norme dans l'extension K'/k' , donc 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 :

$$\prod_{\wp} (\alpha,\beta)_{\wp} = 1 \ , \quad \alpha \ , \ \beta \in k' \quad \text{(cf [9], pp. 228-229).}$$

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

Proposition I.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 premier $\wp'$ *conjugué de* $\wp$ *dans* k'/k .

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

La détermination de $\Lambda \cap NK^*/\Lambda^{\ell}$ est ramenée à un calcul explicite de symboles :

Proposition I.5.

Soit q *l'homomorphisme canonique* $\Lambda \to \Lambda/\Lambda^{\ell}$ *et soit* $q(a_1),\ldots,q(a_n)$ *une* $\mathbb{F}_{\ell}$*-base de* Λ/Λ^{ℓ} ; *le nombre* $\dfrac{|\Lambda/\Lambda^{\ell}|}{|\Lambda \cap NK^*/\Lambda^{\ell}|}$ *est égal à* ℓ^r *où* r *est le rang du système linéaire homogène défini sur* $\mathbb{F}_{\ell}$ *par les* t *équations :*

$$\prod_{i=1}^{n} (\alpha,a_i)_{\mathfrak{p}}^{x_i} = 1 \ , \ \text{pour tout idéal } \mathfrak{p}$$

ramifié dans K/k .

En outre, on a les relations :

$0 \le r \le t-1$ pour $t \ge 1$ et $r = 0$ si $t = 0$.

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

Théorème I.3.

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

$$|\tilde{H}/H| = \frac{|H(k)|}{|NH|}\, \ell^{t-1-r} ,$$

où $t \geq 0$ *est le nombre d'idéaux ramifiés dans* K/k , *et où* $r \leq t-1$ *est le rang du système linéaire sur* $\mathbb{F}_\ell$:

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

II - CONSEQUENCES DES RESULTATS OBTENUS.

1. Cas du corps des rationnels.

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

Considérons alors $H = H_1$; comme $E_{\mathbb{Q}}^{+} = \{1\}$ il résulte du corollaire I.2 que H_1 est engendré par les classes des idéaux premiers ramifiés dans $K/\mathbb{Q}$; si $p_1,\ldots,p_t$ sont ces nombres premiers, on peut prendre (relativement à $H = H_1$) le groupe engendré par $p_1,\ldots,p_t$:

$$\Lambda = \langle p_1,\ldots,p_t \rangle ;$$

l'existence de classes d'ordre ℓ , non invariantes par H , est équivalente à la relation $|\tilde{H}_1/H_1| > 1$ soit $t-1 > r$. Nous avions déjà précisé que ce fait était réalisé dans de nombreux cas (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 $n = a(\ell-1) + b$, $a \geq 0$, $0 \leq b < \ell-1$. On suppose que les quotients $\mathcal{H}_{i+1}/\mathcal{H}_i$ sont d'ordre ℓ pour $0 \leq i < n$. 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 $\lambda \leq \ell-1$; $(\mathbb{Z}/\ell^{a+1}\mathbb{Z})^b\times(\mathbb{Z}/\ell^a\mathbb{Z})^{\ell-1-b}$.

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

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

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

(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 Kisilewsky ([5]) sous des hypothèses très particulières.

3. Comparaison des 4-rangs de $\mathbb{Q}(\sqrt{m})$ et de $\mathbb{Q}(\sqrt{-m})$ ([2]) .

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 $p_1,\ldots,p_{t^*}$ 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 :

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

lorsque m est impair,

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

On forme alors les matrices A et A' des systèmes linéaires associés au groupes 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 [2] 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* $\frac{m}{2} \equiv 1 \bmod 4$ *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 :*

$$R_2 \leq R'_2 \leq R_2 + 1 \quad \text{si } 2 \nmid m \ (m \equiv 1 \bmod 4) \ ,$$
$$\text{ou si } 2 \mid m \ , \ m > 0 \ ;$$

$$R_2 - 1 \leq R'_2 \leq R_2 \quad \text{si } 2 \mid m \ , \ m < 0 \ .$$

III - METHODES EFFECTIVES - RESULTATS NUMERIQUES.

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'en-

semble des éléments $\bar{\alpha}$ de $k'^*/k'^{*\ell}$ qui vérifient $\bar{\alpha}^s = \bar{\alpha}^\chi$; $\mathfrak{X}^*$ 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 associé 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 $k = \mathbb{Q}$, posons $\mathbb{Q}' = \mathbb{Q}(\zeta_o)$ et $\wp_o = (1-\zeta_o)$ idéal premier au-dessus de ℓ dans $\mathbb{Q}'$. Etant donné $K/\mathbb{Q}$ cyclique de degré ℓ et $\alpha \in \mathbb{Q}'$, choisi congru à 1 modulo $\wp_o$ et définissant $K' = \mathbb{Q}'(\sqrt[\ell]{\alpha})$, on note $p_1,\ldots,p_t$ les nombres premiers ramifiés dans $K/\mathbb{Q}$ et pour tout i , $1 \le i \le t$, on fait choix d'un idéal premier $\wp_i$ de $\mathbb{Q}'$ au-dessus de p_i . On construit un t-uple $(v_1,\ldots,v_t) \in \mathbb{F}_\ell^t$ de la manière suivante :

$$v_i \equiv v_{\wp_i}(\alpha) \quad \text{modulo } \ell \quad \text{si} \quad \wp_i \neq \wp_o$$

$$v_i \equiv \frac{\alpha-1}{1-\zeta_o} \quad \text{modulo } \wp_o \quad \text{si} \quad \wp_i = \wp_o \ .$$

Soit $\mathbb{V}$ le quotient de $\{(v_1,\ldots,v_t\} \in \mathbb{F}_\ell^t$, $v_i \neq 0$ pour tout i , $1 \le i \le t\}$ par la relation d'équivalence définissant l'espace projectif $\mathbb{P}(\mathbb{F}_\ell^t)$; on est alors conduit à énoncer :

Proposition III.2.

Etant donné un choix des idéaux $\wp_i$ et de la racine primitive $\ell^{\text{ème}}$ de l'unité ζ_o , la construction du t-uple $(v_1,\ldots,v_t) \in \mathbb{F}_\ell^t$ à partir du nombre α définit une application bijective de $\mathbb{P}(\mathfrak{X}^*)$ sur l'ensemble $\mathbb{V}$.

Remarque III.1.

Card $(\mathbb{V}) = (\ell-1)^{t-1}$.

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 $K/\mathbb{Q}$; si ℓ est ramifié, on posera $\ell = p_t$.

Pour simplifier nous ferons l'hypothèse suivante :

$$H \text{ contient } H_1 ;$$

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

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

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

Définition III.1.

Soit $\mathfrak{P}$ un idéal premier dans $\mathbb{Q}'$; on note $n_{\mathfrak{P}}$ le nombre de conjugués distincts de $\mathfrak{P}$ dans $\mathbb{Q}'/\mathbb{Q}$ et on pose pour $a \in \mathbb{Q}$:

$$[a]_{\mathfrak{P}} = (p,a)_{\mathfrak{P}} \quad , \quad (p) = \mathfrak{P}\cap\mathbb{Z} \quad , \quad \mathfrak{P} \neq \mathfrak{P}_o \ ,$$

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

Les calculs effectifs de [9] (Prop. 8, p. 217 et Prop. 5, p. 236) permettent alors de démontrer :

Proposition III.3.

Soit $p = p_i$ et soit $a \in \mathbb{Q}$ premier à p_i ; alors

$(\alpha,a)_{p_i} = [a]_{\mathfrak{P}_i}^{-v_i n_{\mathfrak{P}_i}}$, 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 :

$$(\alpha,a)_{\mathfrak{P}_i} \equiv (a^{-v_i})^{\frac{p_i-1}{\ell}} \quad \text{modulo} \quad \mathfrak{P}_i \ ;$$

Si $p_i = \ell$, on a :

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

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

Posons, pour simplifier l'écriture :

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

Théorème III.1.

Soit Λ un groupe de nombres associé au quotient $\tilde{\mathcal{H}}/\mathcal{H}$. On suppose que Λ/Λ^ℓ possède une base de la forme $q(p_1),\ldots,q(p_t)$, $q(a_{t+1}),\ldots,q(a_n)$ avec a_i premier à $p_1\ldots p_t$ pour $i > t$. Le système linéaire $\prod_{i=1}^{n} (\alpha,a_i)_j^{x_i} = 1$, $1 \le j \le t$ s'écrit :

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

Démonstration :

On a $\prod_{i=1}^{n} (\alpha,a_i)_j^{x_i} = \prod_{\substack{i=1 \\ i\neq j}}^{n} [a_i]_j^{-v_j n_j x_i} (\alpha,a_j)_j^{x_i} = 1$; la formule du produit appliquée au couple (α,a_j) s'écrit $\prod_{\wp} (\alpha,a_j)_\wp = 1$ soit $\prod_{k=1}^{t} (\alpha,a_j)_k^{n_k} = 1$, d'où $(\alpha,a_j)_j^{n_j} = \prod_{\substack{i=1 \\ i\neq j}}^{t} (\alpha,a_j)_i^{-n_i} = \prod_{\substack{i=1 \\ i\neq j}}^{t} [a_j]_i^{+n_i^2 v_i}$.

Si $\wp_i \neq \wp_o$, p_j est totalement décomposé dans Ω'/Ω et $n_j = \ell-1$, sinon $n_j = 1$; par conséquent, on aura

$$(\alpha,a_j)_j = \prod_{\substack{i=1 \\ i\neq j}}^{t} [a_j]_i^{n_j v_i} \qquad \text{et finalement}$$

$$1 = \prod_{\substack{i=1 \\ i\neq j}}^{n} [a_i]_j^{-v_j n_j x_i} \prod_{\substack{i=1 \\ i\neq j}}^{t} [a_j]_i^{x_j n_j v_i} \quad , \text{ d'où le théorème.}$$

Corollaire.

Lorsque $\mathcal{H} = \mathcal{H}_1$ le système associé à $\Lambda = \langle p_1, \ldots, p_t \rangle$ est :

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

Remarque :

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

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

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

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

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

Proposition III.4.

Le rang r est égal à 0 si et seulement si p_i est congru à une puissance $\ell^{\text{ème}}$ 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 :

$$\begin{cases} -a_{12}v_2x_1 + a_{21}v_1x_2 = 0 \\ a_{12}v_2x_1 - a_{21}v_1x_2 = 0 \end{cases}$$

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 [3]).

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.

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 $\Lambda = \langle p_1,\ldots,p_t\rangle$.

5. Algorithme.

Etant donné 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 :

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

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 $H_{i+1} = \tilde{H}_i$ par l'intermédiaire d'un groupe $\mathcal{J}_{i+1}$.

Remarque :

Cet algorithme généralise, pour $\ell = 2$, celui de [7] qui permet d'atteindre H_3. Il est à rapprocher de celui de [8], également pour $\ell = 2$.

TABLE DES CORPS CUBIQUES AVEC UN 3-RANG MAXIMUM,
POUR $t = 2$ $(R_1 = 2)$ et $p_1, p_2 < 1000$.

3, 73	19,151	241	433	643	487	211,307	277,397
271	277	277	631	673	601	367	541
307	373	313	673	757	727	223,277	757
523	487	487	757	139,199	787	283	829
577	577	613	769	277	877	439	283,313
613	691	877	823	373	883	661	349
757	733	907	859	601	991	787	499
919	31,163	67,193	877	619	163,313	859	619
991	271	283	97,313	631	349	919	691
7,181	349	349	337	661	379	229,283	307,313
223	373	643	433	769	757	457	421
337	619	661	463	151,211	823	241,271	499
421	829	937	601	283	181,331	379	523
463	883	997	997	331	397	457	739
673	37,103	73,103	103,409	367	673	751	919
769	421	241	439	409	823	787	313,349
811	433	313	823	433	859	829	463
853	487	439	919	547	193,409	859	577
883	739	709	991	607	643	877	607
13,103	991	883	109,199	691	733	271,487	331,409
229	43,193	79, 97	373	727	199,211	571	547
421	409	157	709	877	313	661	727
499	457	283	997	157,337	397	769	877
619	613	337	127,349	373	661	823	937
853	643	349	421	379	733	919	337,499
859	61,163	409	619	439	859	967	811

.../...

349,661	691	787	661	991	661,727	739,967
709	733	439,727	673	601,811	853	751,811
877	877	733	709	823	877	967
967	937	457,673	739	607,643	673,757	757,907
367,439	397,523	829	757	823	769	991
733	613	877	541,739	937	787	811,919
739	631	977	757	613,643	997	823,919
937	907	463,547	853	811	691,757	877,967
373,457	919	643	547,619	829	823	997
577	409,523	733	571,607	907	859	907,919
613	571	487,499	661	619,643	907	919,991
769	421,499	499,523	709	751	937	967,991
787	691	577	757	631,661	709,727	997
883	829	643	787	829	751	
379,409	433,571	823	859	859	727,823	
463	631	853	577,619	919	919	
541	739	997	757	643,859	733,859	
601	751	523,547	811	883	991	

TABLE DES CORPS CUBIQUES AVEC UN 3-RANG MAXIMUM,

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			

TABLES ANALOGUES AUX PRECEDENTES POUR t = 2

/ ℓ = 5 /

5,251	41,191	211,251	991	821,881
601	571	811	331,751	941,991
11,241	61,761	241,701	401,421	
661	131,331	251,331	631	
31,191	571	751	601,761	
211	941	941	641,661	
991	191,941	271,571	701,911	

/ ℓ = 7 /

127,449	197,211	883	449,827	673,757
743	337,673	379,827	617,953	757,911

BIBLIOGRAPHIE

[1] - C. CHEVALLEY - "Sur la théorie du corps de classes dans les corps finis et les corps locaux". Journal of the Faculty of Sciences, Tokyo, Vol. II, Part. 9 (1933).

[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". J.f.d.r.u.a. Math., Band 244 (1970), 37-54.

[3] - G. GRAS - "Sur le ℓ-groupe des classes des extensions cycliques de degré premier ℓ ". Note C.R.A.S., t. 274 (1972), 1145-1148.

[4] - K. IWASAWA - "A note on the group of units of an algebraic Number field". J. Math. Pures Appl., 35 (1956), 189-192.

[5] - H. KISILEVSKY - "Some results related to Hilbert's theorem 94". J. of Number theory, 2 (1970), 199-206.

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

[7] - L. REDEI und H. REICHARDT - "Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers". J. f.d.r.u.a. Math., 170 (1933).

[8] - D. SHANKS - "Gauss's Ternary form reduction and the 2-sylow subgroup". Math. of computation, 25 (1971), 837-853.

[9] - J.P. SERRE - "Corps locaux". Act. sc. et ind., Paris, 1962.

[10] - O. TAUSSKY - "A remark concerning Hilbert's Theorem 94". J.f.d.r. u.a. Math., 239/240 (1970), 435-438.
