

Séminaire de Théorie des Nombres .

- Besançon -

Année 1974 - 1975

SUR LE 3-RANG DES CORPS CUBIQUES NON GALOISIENS.

Georges GRAS  
Faculté des Sciences. Mathématiques.  
25030 BESANCON CEDEX

# SUR LE 3-RANG DES CORPS CUBIQUES NON GALOISIENS .

par Georges GRAS

----

Il est établi une formule donnant le 3-rang du groupe des classes des corps cubiques non galoisiens ; cette formule est une conséquence immédiate des résultats généraux obtenus dans [5] ; elle permet, d'une part, de démontrer ou de retrouver certains résultats sur le 3-rang et, d'autre part, de le calculer numériquement grâce à la technique mise au point dans [5]. La démonstration de la conjecture de Callahan [2] résulte aussi de la formule trouvée.

## 1. Notations et rappels.

a. Généralités. - Soit  $L$  un corps cubique non galoisien (il possède deux autres conjugués  $L'$  et  $L''$ ). Soient  $K$  la clôture galoisienne de  $L$  et  $k$  le corps quadratique contenu dans  $K$ . On peut engendrer  $\text{Gal}(K/\mathbb{Q}) \simeq S_3$  par  $\sigma$  et  $\tau$  vérifiant les conditions  $\sigma^3 = \tau^2 = 1$ ,  $\sigma\tau = \tau\sigma^2$ ,  $\text{Gal}(K/L) = \{1, \tau\}$  et  $\text{Gal}(K/k) = \{1, \sigma, \sigma^2\}$ .

On sait que  $p$  est totalement ramifié dans  $L/\mathbb{Q}$  si et seulement s'il est totalement ramifié dans  $K/k$  [9]. Nous noterons  $p_1, \dots, p_\omega$  (resp.  $q_1, \dots, q_{\bar{\omega}}$ ) les nombres premiers totalement ramifiés dans  $L$  et décomposés (resp. non décomposés) dans  $k$  ;  $\mathfrak{p}_i, \mathfrak{p}_i^\tau, \mathfrak{q}_j$  (resp.  $\mathfrak{P}_i, \mathfrak{P}_i^\tau, \mathfrak{Q}_j$ ),  $1 \leq i \leq \omega$ ,  $1 \leq j \leq \bar{\omega}$ , désignent les idéaux premiers de  $k$  (resp.  $K$ ) au dessus des  $p_i$  et  $q_j$ . Le nombre  $t$  d'idéaux premiers totalement ramifiés dans  $K/k$  est donc  $t = 2\omega + \bar{\omega}$ .

b. Classes et unités. - Si  $M$  est un sous-corps de  $K$ ,  $A_M, E_M, \mathfrak{S}(M), \text{Cl}_M(a), \rho(M)$ , désignant respectivement l'anneau des entiers, le groupe des unités, le 3-groupe des classes, la classe de l'idéal  $a$  et le 3-rang de  $M$ . Soit  $N : \mathfrak{S}(K) \rightarrow \mathfrak{S}(k)$  l'homomorphisme défini par  $N(\text{Cl}_K(a)) = \text{Cl}_k(N_{K/k} a)$ . Comme dans [6] (§ 2, Prop. 1) nous identifierons  $\mathfrak{S}(L)$  à  $\mathfrak{S}(K)^{1+\tau}$ . Nous noterons  $\mathfrak{S}_1(K) = \{h \in \mathfrak{S}(K), h^{(\sigma-1)^i} = 1\}$ .

Comme 2 est inversible modulo 3, on peut écrire

$$\mathfrak{S}(K) = \mathfrak{S}(K) \frac{1+\tau}{2} \oplus \mathfrak{S}(K) \frac{1-\tau}{2}, \text{ alors } \mathfrak{S}(K) \frac{1+\tau}{2} = \mathfrak{S}(L) = \{h \in \mathfrak{S}(K), h^\tau = h\}$$

et  $\mathfrak{S}(K)^{\frac{1-\tau}{2}} = \{h \in \mathfrak{S}(K), h^\tau = h^{-1}\}$ . Pour calculer  $\rho(L)$ , nous utiliserons le fait que  $\mathfrak{S}_2(K)^{1+\tau}$  est un sous-groupe d'exposant 3 de  $\mathfrak{S}(L)$  dont le rang est  $\rho(L)$  ([6], Prop. 3).

Posons  $(E_k : E_k \cap NK^*) = 3^a$  et  $(E_k \cap NK^* : NE_K) = 3^\delta$  ( $A + \delta = 0$  si  $k$  est imaginaire et  $k \neq \mathbb{Q}(j)$ ,  $a + \delta = 0$  ou 1 sinon). Soit  $\mathfrak{S}_1^\circ(K)$  le groupe engendré par les classes des idéaux "ambiges" dans  $K/k$ ; on sait que  $(\mathfrak{S}_1(K) : \mathfrak{S}_1^\circ(K)) = 3^\delta$  ([5], p. 28). Dans le cas  $\delta = 1$ , il existe une classe  $h_0$  de la forme  $h_0 = Cl_K(\mathfrak{A}_0^{1+\tau})$  dont l'image dans  $\mathfrak{S}_1(K) / \mathfrak{S}_1^\circ(K)$  est génératrice ([6], p. 3); soit  $\mathfrak{S}_0 = \langle h_0 \rangle$  le groupe engendré par  $h_0$  (si  $\delta = 0$ , on pose  $\mathfrak{S}_0 = (1)$ ). Comme  $\mathfrak{S}_0 \subset \mathfrak{S}_2(K)^{1+\tau}$ ,  $h_0$  est d'ordre  $3^\delta$ , ce qui fait que  $\mathfrak{S}_0$  est facteur direct dans  $\mathfrak{S}_1(K)$ .

Posons  $\mathfrak{S}_1^+ = \mathfrak{S}_1^\circ(K)^{1+\tau}$ ,  $\mathfrak{S}_1^- = \mathfrak{S}_1^\circ(K)^{1-\tau}$  (on a  $\mathfrak{S}_1(K) = \mathfrak{S}_1^+ \oplus \mathfrak{S}_1^- \oplus \mathfrak{S}_0$ ),  $\mathfrak{S} = \mathfrak{S}_1^+ \oplus \mathfrak{S}_0$  ( $\mathfrak{S} = \mathfrak{S}_1(K)^{1+\tau}$ ),  $\tilde{\mathfrak{S}} = \{h \in \mathfrak{S}(K), h^{\sigma-1} \in \mathfrak{S}\}$  ([5], th. 4.2),  $\tilde{\mathfrak{S}}^- = \{h \in \tilde{\mathfrak{S}}, h^\tau = h^{-1}\} = \tilde{\mathfrak{S}}^{1-\tau}$ . Comme  $\mathfrak{S} \subset \mathfrak{S}_2(K)^{1+\tau}$ ,  $\mathfrak{S}^3 = (1)$ .

Soit enfin  $\mathfrak{S}_R(k) \subset \mathfrak{S}(k)$  le sous-groupe engendré par les classes des idéaux  $\mathfrak{p}_1, \dots, \mathfrak{p}_\omega$ . On pose  $\dim(\mathfrak{S}_R(k) / \mathfrak{S}_R(k) \cap \mathfrak{S}(k)^3) = \alpha$ ; on a alors  $\dim(\mathfrak{S}(k) / \mathfrak{S}_R(k) \mathfrak{S}(k)^3) = \rho(k) - \alpha$ . En outre on a  $\alpha \leq \omega$ .

## 2. Résultat fondamental.

Lemme 1. - On a la suite exacte  $1 \rightarrow \tilde{\mathfrak{S}}^- \rightarrow \tilde{\mathfrak{S}} \rightarrow \mathfrak{S} \rightarrow 1$ .

Soit  $h \in \tilde{\mathfrak{S}}$ , on vérifie que  $h^{1+\tau} \in \mathfrak{S}$ :  $h^\sigma = hh + h_0^x$ ,  $h_+ \in \mathfrak{S}_1^+$ ,  $x \pmod 3$ ;  
 $h^{\sigma^2} = hh_+^2 h_0^{2x}$ ; d'où  $h^{\sigma(1+\tau)} = h^{\sigma+\tau\sigma^2} = hh_+ h_0^x h_+^\tau h_+^2 h_0^{2x} = h^{1+\tau}$ ,  
 d'où  $h^{1+\tau} \in \mathfrak{S}_1(K)$  soit  $h^{1+\tau} \in \mathfrak{S}_1(K)^{1+\tau} = \mathfrak{S}$ . Il y a surjectivité car  
 $\mathfrak{S} \subset \tilde{\mathfrak{S}}$  et  $\mathfrak{S} = \mathfrak{S}^{1+\tau} \subset \tilde{\mathfrak{S}}^{1+\tau}$ .

Lemme 2. - On a la suite exacte  $1 \rightarrow \tilde{\mathfrak{S}}^- \rightarrow \mathfrak{S}_2(K)^{1+\tau} \rightarrow \mathfrak{S}_2(K)^{1+\tau} \rightarrow 1$ .

Calculons le noyau: Soit  $h \in \mathfrak{S}_2(K)$ ,  $h^\tau = h^{-1}$ ; on a  $h^\sigma = hh_- h_+ h_0^x$ ,  
 $h_- \in \mathfrak{S}_1^-$ ,  $h_+ \in \mathfrak{S}_1^+$ ,  $x \pmod 3$ ;  $h^{\sigma^2} = hh_-^2 h_+^2 h_0^{2x}$  et  
 $h^{\tau(\sigma-1)} = h^{(\sigma^2-1)\tau} = h^{1-\sigma^2} = h_-^{-2} h_+^{-2} h_0^{-2x}$ ; d'un autre côté,  
 $h^{\tau(\sigma-1)} = h_-^\tau h_+^\tau h_0^{x\tau} = h_-^{-1} h_+^x$ , d'où, en comparant:  $h_- = 1$  soit  
 $h^{\sigma-1} = h_+ h_0^x \in \mathfrak{S}$ , d'où  $h \in \tilde{\mathfrak{S}}$  soit  $h \in \tilde{\mathfrak{S}}^-$ .

Lemme 3. - On a  $N\mathfrak{S} = (1)$  et  $N\mathfrak{S}_1(K) = \mathfrak{S}_R(k)\mathfrak{S}(k)^3$ .

Soit  $h \in \mathfrak{S}$  ;  $h$  est de la forme  $Cl_K(\mathfrak{A}^{1+\tau})$  d'où  
 $Nh = Cl_K(N\mathfrak{A}^{1+\tau}) = Cl_K(\mathfrak{a}^{1+\tau}) = 1$  (avec  $\mathfrak{a} = N\mathfrak{A}$ ).

Soit  $N\mathfrak{S}_1(K) = N(\mathfrak{S} \oplus \mathfrak{S}_1^-) = N\mathfrak{S}_1^-$  ; or  $\mathfrak{S}_1^- = \mathfrak{S}_1^{\circ(1-\tau)}$  est engendré par les  $Cl_K(\mathfrak{A}^{1-\tau})$ ,  $\mathfrak{A}$  idéal ambige, donc par les classes des idéaux  $\mathfrak{P}_i^{1-\tau}$  et des idéaux  $\mathfrak{a}^{1-\tau} A_K$  ( $\mathfrak{a}$  idéal de  $k$ ), d'où finalement  $N\mathfrak{S}_1^-$  est engendré par les classes des idéaux  $\mathfrak{p}_i$  et  $\mathfrak{a}^3$  (compte tenu du fait que  $\mathfrak{p}_i^{1+\tau}$  et  $\mathfrak{a}^{1+\tau}$  sont principaux), d'où  $N\mathfrak{S}_1^- = \mathfrak{S}_R(k)\mathfrak{S}(k)^3$ .

On peut maintenant calculer  $\rho(L)$  : on a  $3^{\rho(L)} = |\mathfrak{S}_2(K)^{1+\tau}| = |\mathfrak{S}_2(K)/\overline{\mathfrak{S}}|$  (lemme 2) =  $|\mathfrak{S}_2(K)/|\mathfrak{S}/\mathfrak{S}|$  (lemme 1) =  $|\mathfrak{S}_1(K)| \cdot |\mathfrak{S}_2(K)/\mathfrak{S}_1(K)| / |\mathfrak{S}/\mathfrak{S}|$  ; en appliquant les résultats de [5] (th. 4.3) on aura :

$$\begin{aligned} |\mathfrak{S}_2(K)/\mathfrak{S}_1(K)| &= 3^{t-1-r} |\mathfrak{S}(k)| / |N\mathfrak{S}_1(K)| = |\mathfrak{S}(k)/\mathfrak{S}_R(k)\mathfrak{S}(k)^3| 3^{t-1-r} \\ \text{(lemme 3)} &= 3^{\rho(k)-\alpha+t-1-r}, \text{ puis } |\mathfrak{S}/\mathfrak{S}| = |\mathfrak{S}(k)| / |N\mathfrak{S}| \cdot 3^{t-1-r'} = \\ &3^{t-1-r'} |\mathfrak{S}(k)| \text{ (lemme 3) et enfin } |\mathfrak{S}_1(K)| = |\mathfrak{S}(k)| 3^{t-1-a} \text{ ([5], th. 4.1).} \end{aligned}$$

Les nombres  $r$  et  $r'$  sont relatifs aux groupes  $\mathfrak{S}_1(K)$  et  $\mathfrak{S}$  (cf. [5], th. 4.3 et a) p. 36). On obtient alors :

Théorème. - On a  $\rho(L) = \rho(k) - \alpha + t - 1 - a - (r-r')$ .

Corollaire 1 (Conjecture de Callahan [2]). - Si  $t = 0$ , alors  $\rho(L) = \rho(k) - 1$ .  
 En effet, si  $t = 0$ ,  $K/k$  est non ramifiée, d'où  $\alpha = a = r = r' = 0$ .  
 (Ceci démontre la conjecture de Callahan lorsque  $k$  est réel ou imaginaire).

Corollaire 2. - Si  $t = 1$ , alors  $\rho(L) = \rho(k)$ .

D'après [5] (th. 4.3) on a  $r, r', a \leq t-1$ , d'où  $a = r = r' = 0$ , et  $t=1$  implique  $\bar{w} = 1$ ,  $w = 0$ , d'où  $\alpha = 0$ .

Corollaire 3. - On a  $\rho(L) \leq \rho(k) - \alpha + t - 1 - a$ .

En effet, on a toujours  $r' \leq r$  (on a  $\mathfrak{S} \subset \mathfrak{S}_1(K)$  et les groupes de nombres  $\Lambda'$  et  $\Lambda$  associés à  $\mathfrak{S}$  et  $\mathfrak{S}_1(K)$  pourront toujours être pris tels que  $\Lambda' \subset \Lambda$  ; cf. [5], chap. IV, § B, 2).

Remarque. On obtient des minoration de  $\rho(L)$  en majorant  $r-r'$  convenablement.

Corollaire 4. - (cf. [6] et Kobayashi [7]). - Si  $\mathfrak{S}(k) = (1)$ , alors  $\rho(K) = 2(t-1) - r - a$ .

En effet, on a ([5], prop. 4.1) :  $\mathfrak{S}_2(K) = \{h \in \mathfrak{S}(K), h^3 = 1\}$ , d'où  $\rho(K)$ .

3. Etude de  $r$  et  $r'$ . - D'après [5] (pp. 36-37) on doit considérer des groupes d'idéaux  $\mathfrak{J}$  et  $\mathfrak{J}'$  représentant  $\mathfrak{S}_1(K)$  et  $\mathfrak{S}$  ; on prendra donc  $\mathfrak{J} = \langle \mathfrak{P}_1, \mathfrak{P}_1^\tau ; \mathfrak{Q}_j ; \mathfrak{A}_\omega^{1+\tau}, \dots ; \alpha_\ell A_K \rangle$  et  $\mathfrak{J}' = \langle \mathfrak{P}_1^{1+\tau} ; \mathfrak{Q}_j ; \mathfrak{A}_\omega^{1+\tau} \rangle$  où les classes des idéaux  $\alpha_\ell$  de  $k$  engendrent  $\mathfrak{S}(k)$ ,  $\ell = 1, \dots, \rho(k)$ . La condition donnée dans [5] (th. 4.2 (ii)) est satisfaite pour  $\mathfrak{J}$  et  $\mathfrak{J}'$ .

Les groupes  $\Lambda$  et  $\Lambda'$  qui s'en déduisent sont de la forme suivante :

$\Lambda = \langle \epsilon, a_\omega, p_i, q_j, \alpha_n \rangle$  et  $\Lambda' = \langle \epsilon, a_\omega, p_i, q_j \rangle$ , où  $\epsilon$  est l'unité fondamentale de  $k$  si  $k$  est réel ou  $\epsilon = j$  si  $k = \mathbb{Q}(j)$  (sinon  $\epsilon$  ne figure pas dans  $\Lambda$  et  $\Lambda'$ ),  $a_\omega$  est (éventuellement) la norme absolue de  $\mathfrak{A}_\omega$ , les  $\alpha_n$  sont des nombres de  $k$  ( $n \leq \rho(k) + \omega$ ) engendrant le groupe  $\langle p_i, \alpha_\ell^3 \rangle \cap \mathfrak{J}_\omega(k)$  (où  $\mathfrak{J}_\omega(k)$  est le groupe des idéaux principaux de  $k$ ).

Remarque. Dans le cas des corps purs (i. e.  $k = \mathbb{Q}(j)$ ) alors  $K = k(\sqrt[3]{n})$ ,  $n \in \mathbb{Z}$ , ce qui fait que la décomposition en idéaux premiers de  $\sqrt[3]{n} A_K$  donne une relation non triviale entre les  $\mathfrak{P}_i, \mathfrak{P}_i^\tau$  et  $\mathfrak{Q}_j$  où tous les  $\mathfrak{P}_i$  figurent à un exposant non congru à 0 mod 3 ; on a alors :  $\Lambda = \langle j, a_\omega, p_i, q_j, \pi_i \rangle$  et  $\Lambda' = \langle j, a_\omega, p_i, q_j \rangle$  où  $\pi_i$  est un générateur de  $p_i$ .

Corollaire 5 (Honda, Callahan [3]). - Si  $L$  est pur, on a  $\rho(L) = 0$  si et seulement si on a l'un des deux cas suivants :

$$\omega = 0, \bar{\omega} = 1, a = 0 \quad \text{ou bien} \quad \omega = 0, \bar{\omega} = 2, a = 1.$$

Si  $\rho(L) = 0$ , on a  $r-r' \leq \omega-1$  (si  $\omega \geq 1$ ), d'où  $\rho(L) \geq t-1-a-(\omega-1) = \omega + \bar{\omega} - a$  ; il est nécessaire d'avoir  $\omega + \bar{\omega} \leq a$  d'où  $\omega \leq 1$  et  $\rho(L) = 2\omega + \bar{\omega} - a - 1$  soit  $2\omega + \bar{\omega} = a + 1$  et  $\omega + \bar{\omega} \leq a$ , ce qui conduit à  $\omega = 1$  et  $\bar{\omega} = a-1$  soit  $a = 1$  et  $\bar{\omega} = 0$ , cas impossible car si  $\omega = 1, \bar{\omega} = 0, n = p, p \equiv 1(9)$  et  $a = 0$ .

Si  $\omega = 0$ , alors  $\bar{\omega} = a + 1$ , d'où les deux cas.

Remarque. L'expression de  $\rho(L)$  donnée par notre théorème étant "exacte", les minoration de  $\rho(L)$  proviennent des majorations de  $r-r'$  ; or les symboles de Hilbert définissant les coefficients du système ont des propriétés très particulières et vérifient certaines relations (par exemple [6], lemme 4). On doit ainsi pouvoir retrouver les minoration déjà existantes ([1], [3]).

D'autre part, comme le remarquent Gerth III [4] et Kobayashi [8], le cas  $\delta = 1$  oblige à déterminer  $\mathfrak{A}_\omega$ , ce qui est une difficulté essentielle ;

dans les autres cas, notre système linéaire permet de trouver numériquement  $\rho(L)$ , à condition d'admettre que l'on connaît parfaitement le 3-groupe des classes de  $k$ , ce qui est une hypothèse raisonnable.

Dans le cas où  $\epsilon$  est norme ( $a = 0$ ) on devra résoudre l'équation  $N_{K/k} \delta = \epsilon$  ( $\delta \in K^*$ ) ; il n'est cependant pas nécessaire de distinguer les cas  $\delta = 0$  et  $\delta = 1$ , ce qui fait que l'équation précédente, admettant une infinité de solutions, sera plus facile à résoudre (voir aussi [8] pour le cas des corps purs).

Après avoir obtenu ces résultats, nous avons appris par D. Shanks que Gerth III avait démontré indépendamment la relation citée dans notre théorème dans : Ranks of 3-Class Groups of Non-Galois Cubic Fields (à paraître dans Acta Arithmetica).

- [1] P. Barrucand et H. Cohn, A rational Genus, class Number divisibility, and Unit Theory for Pure Cubic Fields, Jour. of Number Theory, 2, pp. 7-21 (1970).
- [2] T. Callahan, The 3-class Groups of non-Galois cubic Fields (I), Mathematika, 21, pp. 72-89 (1974).
- [3] T. Callahan, The 3-class Groups of non-Galois cubic Fields (Thesis, Univ. of Toronto) (1974).
- [4] F. Gerth III, On 3-class Groups of Pure Cubic Fields (à paraître).
- [5] G. Gras, Sur les 1-classes d'idéaux dans les extensions cycliques relatives de degré premier  $l$ , Ann. Inst. Fourier, 23, 3, pp. 1-48 (1973).
- [6] G. Gras, Sur les 1-classes d'idéaux des extensions non galoisiennes de  $\mathbb{Q}$  de degré premier impair  $l$  à clôture galoisienne diédrale de degré  $2l$ , Jour. Math. Soc. Japan, 26, 4, pp. 677-685 (1974).
- [7] S. Kobayashi, On the 1-class rank in some algebraic number fields (à paraître).
- [8] S. Kobayashi, On the 3-rank of the ideal class groups of certain pure cubic fields II (à paraître).
- [9] J. Martinet et J.-J. Payan, Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne, J. f. d. r. u. a. Math., 228, pp. 15-37 (1967).