Ann. Sci. Math. Québec **25** (2001), no. 2, 153–177.

SUR LA DIVISIBILITÉ EXACTE PAR 3 DU NOMBRE DE CLASSES DE CERTAINS CORPS CUBIQUES PURS

M. C. ISMAILI ET R. EL MESAOUDI

RÉSUMÉ. Soit $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ un corps cubique pur, où n est un entier naturel divisible par un premier $p \equiv 1 \pmod 3$. Lorsque n s'écrit sous certaines formes, nous donnons des conditions nécessaires et suffisantes sur n, moyennant la notion de reste cubique modulo p, pour que le nombre de classes de Γ soit exactement divisible par 3.

ABSTRACT. Let $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ be a pure cubic field, where n is a natural integer divisible by a prime $p \equiv 1 \pmod 3$. When n has certain forms, we give necessary and sufficient conditions on n, using the notion of cubic residue mod p, to have the class number of Γ exactly divisible by 3.

1. Introduction. Soit $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ un corps cubique pur, où n est un entier naturel sans facteur cubique, $k = \mathbf{Q}(\sqrt[3]{n}, j)$ sa clôture normale, $j = \exp(2i\pi/3)$, E_k le groupe des unités de k, u l'indice du sous-groupe de E_k, engendré par les unités des corps intermédiaires de $k/\mathbf{Q}$, dans E_k, h_Γ le nombre de classes de Γ et $\mathcal{H}(k)$ le 3-groupe des classes d'idéaux de k. Plusieurs travaux ([B-C2], [B-W-Z], [Ho], [Is]) ont été consacrés à l'étude du 3-groupe des classes des corps cubiques purs et de leur normalisé, ainsi qu'au calcul de l'indice u. Ismaili a établi dans [Is] que le 3-groupe $\mathcal{H}(k)$ du normalisé k de Γ est de type $(3,3)$ (c'est-à-dire isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$) si, et seulement si, 3 divise exactement h_Γ et $u = 3$. Il a aussi donné toutes les formes possibles de l'entier n lorsque $\mathcal{H}(k)$ est de type $(3,3)$ en distinguant trois situations différentes pour le corps k (types I, II, III). Les corps k de type III sont caractérisés par le fait que le corps de genres relatif $(k/k_0)^*$ de k sur k_0, où $k_0 = \mathbf{Q}(j)$, coïncide avec le 3-corps de classes de Hilbert de k, et dans chacune des formes de n rencontrées dans ce type, l'entier n est divisible par un premier $p \equiv 1 \pmod 3$. À noter que la théorie du genre assure le fait que $3|h_\Gamma$ lorsque l'entier n est divisible par un premier $p \equiv 1 \pmod 3$.

Le présent travail consiste à donner, pour chaque forme de l'entier n rencontrée dans l'étude des corps k de type III, des conditions nécessaires et suffisantes sur n, moyennant la notion de reste cubique modulo le nombre premier $p \equiv 1 \pmod 3$ divisant n, pour que le nombre de classes de $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ soit exactement divisible par 3. Cette étude nous a permis d'établir un critère de divisibilité exacte par 3 et de

Reçu le 12 octobre 2000 et, sous forme définitive, le 6 août 2001.

divisibilité par 9 du nombre de classes de plusieurs familles de corps cubiques purs pour lesquels nous montrons que l'indice $u = 3$, lequel indice est difficile à calculer en général. Nos résultats confirment ceux de Barrucand et Cohn, qui ont montré dans [B-C1] que l'indice $u = 3$ pour les entiers $n = 14, 38, 42$.

Nous résumons tous ces résultats dans le théorème et le corollaire suivants, où pour $c \in \mathbb{Z}$, le symbole $(c/p)_3 = 1$ signifie que c est reste cubique modulo p, c'est-à-dire la congruence $X^3 \equiv c \pmod p$ est résoluble dans $\mathbb{Z}$, $3||h_\Gamma$ signifie que h_Γ est exactement divisible par 3 (c'est-à-dire que $3 \mid h_\Gamma$ et $3^2 \nmid h_\Gamma$), $\mathcal{O}_{k_0}$ est l'anneau des entiers de $k_0 = \mathbf{Q}(j)$, et $\lambda = 1 - j$. À noter que dans chaque cas, la partie réciproque de l'équivalence caractérisant la divisibilité exacte de h_Γ par 3 a été établie par Ismaili dans [Is].

Théorème. *Soit $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ un corps cubique pur, où n est un entier naturel sans facteur cubique. Soit $p, q, q_1,$ et q_2 des nombres premiers tels que $p \equiv -q \equiv -q_1 \equiv -q_2 \equiv 1 \pmod 3$.*

(1) Si $n = 3^e p^{e_1}$, où $p \equiv 1 \pmod 9$ et $e, e_1 \in \{1, 2\}$, alors

$$\left(\frac{3}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(2) Si $n = p^e q^{e_1}$, où $p \equiv -q \equiv 1 \pmod 9$ et $e, e_1 \in \{1, 2\}$, alors

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(3) Soit $n = p^e q_1^{e_1} q_2^{e_2}$, avec p ou $-q_1$ ou $-q_2 \equiv 4$ ou $7 \pmod 9$, $n \equiv \pm 1 \pmod 9$, et $e, e_1, e_2 \in \{1, 2\}$.

(i) *Si $p \equiv 1 \pmod 9$, on a*

$$\left(\frac{q^{e_1} q^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(ii) *Soit $p \not\equiv 1 \pmod 9$; on pose $p = \pi_1 \pi_2$, $\pi_3 = -q_1$ et $\pi_4 = -q_2$, où les π_i sont des premiers de k_0 congrus à $1 \pmod{3\mathcal{O}_{k_0}}$.*

(a) Si $\pi_3 \not\equiv 1 \pmod{\lambda^3}$ et $r = 1$ ou 2 est choisi tel que $\pi_1 \pi_3^r \equiv 1 \pmod{\lambda^3}$, on a:

$$\left(\frac{q_1^{e_1+r} q_2^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(b) Si $\pi_3 \equiv 1 \pmod{\lambda^3}$, et $r = 1$ ou 2 est choisi tel que $\pi_1 \pi_4^r \equiv 1 \pmod{\lambda^3}$, on a:

$$\left(\frac{q_1^{e_1} q_2^{e_2+r}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(4) Soit $n = 3^e p^{e_1} q^{e_2}$, où p ou $-q \equiv 4$ ou $7 \pmod 9$, $n \not\equiv \pm 1 \pmod 9$, $e \in \{0, 1, 2\}$ et $e_1, e_2 \in \{1, 2\}$.

(i) *Si $p \equiv 1 \pmod 9$, on a*

$$\left(\frac{3^e q^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(ii) *Soit* $p \not\equiv 1 \pmod 9$.

(a) Si $e = 0$,

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(b) Si $e \neq 0$, $\pi = -q \not\equiv 1 \pmod{\lambda^3}$, *et* $r = 1$ *ou* 2 *est choisi tel que* $\pi_1\pi^r \equiv 1 \pmod{\lambda^3}$, *alors*

$$\left(\frac{q^{e_2+r}3^e}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(c) Si $e \neq 0$ *et* $\pi = -q \equiv 1 \pmod{\lambda^3}$, *alors*

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Corollaire. *Supposons que les hypothèses sont les mêmes que celles du théorème précédent et soit* c *l'entier naturel correspondant à chaque cas tel que*

$$\left(\frac{c}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Alors nous avons :

$$\left(\frac{c}{p}\right)_3 \neq 1 \Rightarrow u = 3\ ;$$
$$\left(\frac{c}{p}\right)_3 = 1 \Leftrightarrow 9|h_\Gamma.$$

Nous adopterons les notations suivantes :
$\Gamma = \mathbf{Q}(\sqrt[3]{n})$: un corps cubique pur, $n \in \mathbb{N}$, où n est sans facteur cubique ;
$k = \mathbf{Q}(j, \sqrt[3]{n})$: la clôture normale de Γ, où $j = \exp(2i\pi/3)$;
$k_0 = \mathbf{Q}(j) = \{x + yj | x, y \in \mathbf{Q}\}$: le 3e corps cyclotomique ;
$\mathcal{O}_{k_0} = \{x + yj | x, y \in \mathbb{Z}\}$: l'anneau des entiers de k_0 ;
$E_{k_0} = \{\pm 1, \pm j, \pm j^2\}$: le groupe des unités de k_0 ;
$\mathrm{Gal}(k/k_0) = \langle\sigma\rangle$, $\sigma^3 = \mathrm{id}$, $\sigma(\sqrt[3]{n}) = j\sqrt[3]{n}$ et $\sigma(j) = j$;
$\mathrm{Gal}(k/\Gamma) = \langle\tau\rangle$, $\tau^2 = \mathrm{id}$, $\tau(j) = j^2$ et $\tau(\sqrt[3]{n}) = \sqrt[3]{n}$;
F : un corps de nombres ;
$\mathcal{A}$: un idéal fractionnaire de F ;
$\mathcal{O}_F$: l'anneau des entiers de F ;
E_F : le groupe des unités de F ;
$\mathcal{H}(F)$: le 3-groupe des classes d'idéaux de F ;
h_F : le nombre de classes de F ;
$[\mathcal{A}]$: la classe de $\mathcal{A}$ dans le groupe des classes d'idéaux de F.

Dans tout ce qui suit, la lettre p désignera un nombre premier congru à $1 \pmod 3$ et les lettres q ou q_i où $i \in \{1, 2\}$ désigneront un nombre premier congru à $-1 \pmod 3$.

2. Rappels sur les corps cubiques purs. Un corps cubique pur Γ est défini comme suit :

$$\Gamma = \mathbf{Q}(\sqrt[3]{d}), d \neq s^3, d \in \mathbf{Q}, s \in \mathbf{Q}.$$

Il est facile de vérifier que tout corps cubique pur s'écrit sous la forme $\mathbf{Q}(\sqrt[3]{ab^2})$, où $a, b \in \mathbb{N}$ et ab^2 est sans facteur cubique. Lorsque $a^2 - b^2 \not\equiv 0 \pmod 9$, on dit que le corps cubique pur $\Gamma = \mathbf{Q}(\sqrt[3]{ab^2})$ est de première espèce. Il est dit de deuxième espèce si $a^2 - b^2 \equiv 0 \pmod 9$.

Proposition 1. *Soit* $\Gamma = \mathbf{Q}(\sqrt[3]{ab^2})$ *un corps cubique pur,* $\mathcal{O}_\Gamma$ *l'anneau des entiers de* Γ*, et* p *un nombre premier.*

(1) *Si* $a^2 - b^2 \not\equiv 0 \pmod 9$*, alors* $3\mathcal{O}_\Gamma = \mathcal{P}^3$*, où* $\mathcal{P}$ *est un idéal premier de* Γ.
(2) *Si* $a^2 - b^2 \equiv 0 \pmod 9$*, alors* $3\mathcal{O}_\Gamma = \mathcal{P}^2\mathcal{P}_1$*, où* $\mathcal{P}$ *et* $\mathcal{P}_1$ *sont deux idéaux premiers de* Γ.
(3) *Si* $p|ab$ *et* $p \neq 3$*, alors* $p\mathcal{O}_\Gamma = \mathcal{P}^3$*, où* $\mathcal{P}$ *est un idéal premier de* Γ.
(4) *Si* $p \not| ab$ *et* $p \neq 3$*, alors* p *est non ramifié dans* Γ.

Pour la preuve, voir [De] ou [Is].

L'extension k/k_0 étant cyclique de degré 3, on peut donc introduire la filtration des sous-groupes de $\mathcal{H}(k)$ définis par (voir [Gr])

$$\mathcal{H}_i(k) = Ker(\sigma - 1)^i = \{[\mathcal{A}] \in \mathcal{H}(k) | [\mathcal{A}]^{(\sigma-1)^i} = 1\}.$$

$\mathcal{H}_1(k)$ s'appelle le *groupe des classes ambiguës.*

Proposition 2. $\mathcal{H}_i(k) \subset \mathcal{H}_{i+1}(k)$ *et* $\mathcal{H}_i(k) = \mathcal{H}_{i+1}(k)$ *si, et seulement si,* $\mathcal{H}_i(k) = \mathcal{H}(k), i \geq 0$.

Pour la preuve, voir la proposition 4.1 de [Gr].

Remarque 1. $\mathcal{H}_1(k) = \{[\mathcal{A}] \in \mathcal{H}(k) | [\mathcal{A}]^{\sigma-1} = 1\}$ est le sous-groupe formé des classes ambiguës ; de plus, $|\mathcal{H}_1(k)| = 3^{t-1}/[E_{k_0} : E_{k_0} \cap \mathcal{N}_{k/k_0}(k^*)]$, où t est le nombre des idéaux premiers de k_0 qui se ramifient dans k.

Comme les extensions de k ou de k_0 que nous étudierons sont toutes de Kummer, nous rappelons alors dans la proposition qui suit, les lois de décomposition des idéaux premiers dans de telles extensions. Nous désignerons par L un corps de nombres contenant les racines l-ièmes de l'unité, l étant un nombre premier, et θ un élément de K tel que $\theta \neq \mu^l$ pour tout $\mu \in K$; alors $L(\sqrt[l]{\theta})$ est une extension cyclique de degré l sur L. On note par ζ une racine primitive l-ième de l'unité.

Proposition 3.

(1) *Supposons que l'idéal premier* $\mathcal{P}$ *de* L *divise le nombre* θ *exactement à la puissance* $\mathcal{P}^a$*. Alors, si* $a = 0$ *et* $\mathcal{P}$ *ne divise pas* l*,* $\mathcal{P}$ *se décompose complètement (resp. reste inerte) dans* $L(\sqrt[l]{\theta})$ *lorsque la congruence* $\theta \equiv \xi^l \pmod{\mathcal{P}}$ *est résoluble (resp. n'est pas résoluble) pour un entier* ξ *dans* L *(resp. pour tout entier* ξ *dans* L*). Mais si* a *n'est pas divisible par* l*,* $\mathcal{P}$ *est totalement ramifié dans* $L(\sqrt[l]{\theta})$.

(2) *Soit $\mathcal{B}$ un facteur premier de $1-\zeta$, qui divise $1-\zeta$ exactement à la a-ième puissance, où $(1-\zeta)=\mathcal{B}^a\mathcal{I}_1$. Supposons que $\mathcal{B}$ ne divise pas θ. Alors $\mathcal{B}$ se décompose complètement dans $L(\sqrt[l]{\theta})$ si la congruence*

$$\theta \equiv \xi^l \pmod{\mathcal{B}^{al+1}} \tag{1}$$

est résoluble pour un nombre dans L. L'idéal $\mathcal{B}$ reste inerte dans $L(\sqrt[l]{\theta})$ si la congruence

$$\theta \equiv \xi^l \pmod{\mathcal{B}^{al}} \tag{2}$$

est résoluble sans que (1) *le soit. L'idéal $\mathcal{B}$ est totalement ramifié dans $L(\sqrt[l]{\theta})$ si la congruence* (2) *n'est pas résoluble.*

Pour le preuve, voir [He].

Proposition 4. *Soit k une extension cubique cyclique de $k_0=\mathbf{Q}(j)$. Posons $q^*=0$ ou 1 selon que j n'est pas ou est norme d'un élément de $k-\{0\}$ et notons par t le nombre de premiers ramifiés dans k/k_0.*

(1) *Soit $k=k_0(\sqrt[3]{x})$ où $x=\lambda^{e_\lambda}j^{e_j}\pi_1^{e_1}\cdots\pi_g^{e_g}$ où les π_i sont des éléments premiers de k_0 tels que $\pi_i\equiv 1 \pmod{3\mathcal{O}_{k_0}}$, e_λ, $e_j\in\{0,1,2\}$ et $e_i\in\{1,2\}$ $\forall i\in\{1,...,g\}$. Alors $q^*=1 \Leftrightarrow \pi_i\equiv 1 \pmod{\lambda^3}$, $\forall i\in\{1,...,g\}$; si l'un des $\pi_i\equiv 4$ ou $7 \pmod{\lambda^3}$, alors $q^*=0$.*

(2) *Le rang de $\mathcal{H}_1(k)$ est $rg(\mathcal{H}_1(k))=t-2+q^*$.*

Pour le preuve, voir [Ge].

Les différentes formes de l'entier n données dans notre théorème principal sont tirées du résultat suivant dû à Ismaili (voir [Is]), et qui constitue le point de départ de notre travail. Dans ce théorème on suppose que le 3-groupe des classes du normalisé k de $\Gamma=\mathbf{Q}(\sqrt[3]{n})$, est de type $(3,3)$.

Théorème 1. *Soit p,q,q_1 et q_2 des premiers tels que $p\equiv -q\equiv -q_1\equiv -q_2\equiv 1 \pmod 3$. Soit k_1 le 3-corps de classes de Hilbert du normalisé $k=\mathbf{Q}(j,\sqrt[3]{n})$ de $\Gamma=\mathbf{Q}(\sqrt[3]{n})$, et soit $(k/k_0)^*$ le corps des genres relatif de k/k_0. Alors $k_1=(k/k_0)^*$ si, et seulement si, $3||h_\Gamma$, où h_Γ est le nombre de classes de $\Gamma=\mathbf{Q}(\sqrt[3]{n})$, et n s'écrit sous l'une des formes suivantes :*

(i) *$n=3^ep^{e_1}$ avec $p\equiv 1 \pmod 9$ et $e,e_1\in\{1,2\}$.*

(ii) *$n=q^ep^{e_1}$ avec $-q\equiv p\equiv 1 \pmod 9$ et $e,e_1\in\{1,2\}$.*

(iii) *$n=p^eq_1^{e_1}q_2^{e_2}$ avec p ou $-q_1$ ou $-q_2\equiv 4$ ou $7 \pmod 9$, $n\equiv\pm1 \pmod 9$ et $e,e_1,e_2\in\{1,2\}$.*

(iv) *$n=3^ep^{e_1}q^{e_2}$ avec p ou $-q\equiv 4$ ou $7 \pmod 9$, $e=0,1$ ou 2, $e_2,e_1\in\{1,2\}$ et $n\not\equiv\pm1 \pmod 9$.*

Pour plus de détails et pour la démonstration voir [Is].

3. Le symbole de reste normique. Soit K/k une extension abélienne de corps de nombres de conducteur f. Pour chaque idéal premier $\mathcal{P}$ (fini ou infini) de k, on désigne par $f_\mathcal{P}$ la plus grande puissance de $\mathcal{P}$ qui divise f. Soit $\beta\in k^*$ et $\mathcal{P}$ un idéal premier fini ou infini de k ; subordonné à β, on détermine un nombre auxiliaire β_0 par les conditions

$\beta_0 \equiv \beta \pmod{f_{\mathcal{P}}}$ et $\beta_0 \equiv 1 \pmod{\dfrac{f}{f_{\mathcal{P}}}}$. Alors si $(\beta_0) = \mathcal{P}^b I$ avec I premier à $\mathcal{P}$ ($b = 0$ si $\mathcal{P}$ est infini), on pose

$$\left(\frac{\beta, K}{\mathcal{P}}\right) = \left(\frac{K/k}{I}\right),$$

l'application d'Artin dans K/k appliquée à I.

Si k est un corps de nombres contenant les racines m-ièmes de l'unité, où m est un entier naturel, on définit pour deux nombres $\alpha, \beta \in k^*$ et un idéal premier $\mathcal{P}$ de k le symbole de reste normique par :

$$\left(\frac{\beta, \alpha}{\mathcal{P}}\right)_m = \frac{\left(\frac{\beta, k(\sqrt[m]{\alpha})}{\mathcal{P}}\right) \sqrt[m]{\alpha}}{\sqrt[m]{\alpha}}.$$

Si de plus $\mathcal{P}$ ne se ramifie pas dans $k(\sqrt[m]{\alpha})$, on pose

$$\left(\frac{\alpha}{\mathcal{P}}\right)_m = \frac{\left(\frac{k(\sqrt[m]{\alpha})}{\mathcal{P}}\right) \sqrt[m]{\alpha}}{\sqrt[m]{\alpha}}.$$

Remarque 2. $\big((\beta, \alpha)/\mathcal{P}\big)_m$ et $\big(\alpha/\mathcal{P}\big)_m$ sont des racines m-ièmes de l'unité.

Dans la suite nous allons donner les principales propriétés du symbole de reste normique dont une preuve se trouve dans [Ha].

Propriétés.

(1) $\left(\dfrac{\beta_1\beta_2, \alpha}{\mathcal{P}}\right)_m = \left(\dfrac{\beta_1, \alpha}{\mathcal{P}}\right)_m \left(\dfrac{\beta_2, \alpha}{\mathcal{P}}\right)_m$;

(2) $\left(\dfrac{\beta, \alpha_1\alpha_2}{\mathcal{P}}\right)_m = \left(\dfrac{\beta, \alpha_1}{\mathcal{P}}\right)_m \left(\dfrac{\beta, \alpha_2}{\mathcal{P}}\right)_m$;

(3) $\left(\dfrac{\beta, \alpha}{\mathcal{P}}\right)_m = \left(\dfrac{\alpha, \beta}{\mathcal{P}}\right)_m^{-1}$;

(4) $\left(\dfrac{\beta, \alpha}{\mathcal{P}}\right)_m = \left(\dfrac{\alpha}{\mathcal{P}}\right)_m^{-b}$
si $\mathcal{P}$ ne divise pas le conducteur $f(\sqrt[m]{\alpha})$ de $k(\sqrt[m]{\alpha})$ et apparaît dans (β) à l'exposant b. (Si $\mathcal{P}$ est infini, alors $b = 0$ et on considère le membre de droite égal à 1) ;

(5) $\left(\dfrac{\beta, \alpha}{\mathcal{P}}\right)_m = 1$ si, et seulement si, β est reste normique de $k(\sqrt[m]{\alpha})$ modulo $f(\sqrt[m]{\alpha})$;

(6) $\left(\dfrac{\tau\beta, \tau\alpha}{\tau\mathcal{P}}\right)_m = \tau \left(\dfrac{\beta, \alpha}{\mathcal{P}}\right)_m$ pour tout automorphisme τ de k ;

(7) $\displaystyle\prod_{\mathcal{P}} \left(\frac{\beta, \alpha}{\mathcal{P}}\right)_m = 1$ où le produit est pris sur les idéaux premier finis et infinis ;

(8) Si k' est une extension de degré fini de $k, \alpha \in k^*$ et $\beta' \in k'$, alors

$$\prod_{\mathcal{P}'|\mathcal{P}} \left(\frac{\beta', \alpha}{\mathcal{P}'}\right)_m = \left(\frac{\mathcal{N}_{k'/k}(\beta'), \alpha}{\mathcal{P}}\right)_m \;;$$

(9) Si $\alpha, \beta \in k^*$ et les conducteurs $f(\sqrt[m]{\alpha})$ et $f(\sqrt[m]{\beta})$ respectivement de $k(\sqrt[m]{\alpha})$ et $k(\sqrt[m]{\beta})$ sont premiers entre eux, alors on a la loi de réciprocité classique :

$$\left(\frac{\beta}{(\alpha)}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m .$$

Soit $c \in \mathbb{Z}$. Le symbole $\big(c/p\big)_3 = 1$ signifie que c est *reste cubique* modulo p. Comme l'anneau des entiers $\mathcal{O}_{k_0}$ est principal, $h_{k_0} = 1$, nous écrirons $\big((\alpha,\beta)/(\pi)\big)_3 = \big((\alpha,\beta)/\pi\big)_3$ et $\big(\alpha/(\pi)\big)_3 = \big(\alpha/\pi\big)_3$ lorsque $\alpha, \beta \in k_0^*$ et π est un entier premier de $\mathcal{O}_{k_0}$.

Remarque 3. Si β est norme de $k(\sqrt[m]{\alpha})$, alors $\big((\beta,\alpha)/\mathcal{P}\big)_m = 1$ pour tout idéal premier $\mathcal{P}$ de k (d'après la propriété 5).

Ce sont les symboles de restes normiques cubiques (avec $m = 3$) que nous utiliserons dans la suite.

4. Cas où $n = 3^e p^{e_1}$, avec $p \equiv 1 \pmod 9$. Comme $\mathbf{Q}(\sqrt[3]{ab^2}) = \mathbf{Q}(\sqrt[3]{a^2b})$ pour tout $a, b \in \mathbb{N}$, nous pouvons choisir, sans perte de généralité, $e_1 = 1$ et $e \in \{1, 2\}$ dans toute la suite. Notons qu'un corps cubique pur $\Gamma = \mathbf{Q}(\sqrt[3]{ab^2}) = \mathbf{Q}(\sqrt[3]{n})$ est de première espèce $\Leftrightarrow a^2 - b^2 \not\equiv 0 \pmod 9 \Leftrightarrow n \not\equiv \pm 1 \pmod 9$. Comme $p \equiv 1 \pmod 3$, alors $p = \pi_1\pi_2$ où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1^\tau = \pi_2$ et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$; d'après la proposition 1, p est totalement ramifié dans Γ ; par la suite π_1 et π_2 se ramifient dans k. D'une part, on a $3\mathcal{O}_{k_0} = \lambda^2\mathcal{O}_{k_0}$ où $\lambda = 1 - j$ est un élément premier de k_0 ; d'autre part, $3^e p^{e_1} \not\equiv \pm 1 \pmod 9$ car $e \neq 0$, c'est-à-dire 3 est totalement ramifié dans Γ (proposition 1) ; donc λ se ramifie dans k/k_0. Ainsi le nombre des idéaux premiers ramifiés dans k/k_0 est $t = 3$.

Si P_1, P_2, et I désignent respectivement les idéaux premiers au-dessus de π_1, π_2 et λ, on aura $I^3 = \lambda\mathcal{O}_k$, $P_i^3 = \pi_i\mathcal{O}_k$ $(i = 1, 2)$, $P_1^\tau = P_2, P_2^\tau = P_1$ et $I^\sigma = I^\tau = I$ car $\pi_1^\tau = \pi_2$ et $3\mathcal{O}_k = I^6$.

Proposition 5. *Soit p un premier tel que $p \equiv 1 \pmod 3$. Alors nous avons :*

(1) *$p = \pi_1\pi_2$ dans k_0, où π_1 et π_2 sont deux premiers distincts de $\mathcal{O}_{k_0}$, π_1 étant le conjugué de π_2 et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$.*

(2) $\left(\dfrac{c}{\pi_1}\right)_3 = \left(\dfrac{c}{\pi_2}\right)_3^2$ *pour tout $c \in \mathbb{Z}$ tel que p ne divise pas c.*

(3) $\left(\dfrac{c}{\pi_1}\right)_3 = \left(\dfrac{c}{\pi_2}\right)_3 = 1$ *si, et seulement si, c est reste cubique modulo p.*

(4) $\left(\dfrac{\pi_1}{\pi_2}\right)_3 = \left(\dfrac{\pi_2}{\pi_1}\right)_3 = 1.$

Preuve. (1) Découle du fait que p est un nombre premier $\equiv 1 \pmod 3$.

(2) $\left(\dfrac{c}{\pi_1}\right)_3 = \left(\dfrac{\pi_1, c}{\pi_1}\right)_3^{-1} = \left(\dfrac{c, \pi_1}{\pi_1}\right)_3 = \left(\dfrac{c, \pi_2^\tau}{\pi_2^\tau}\right)_3 = \tau\left(\dfrac{c, \pi_2}{\pi_2}\right)_3 = \left(\dfrac{c, \pi_2}{\pi_2}\right)_3^2 = \left(\dfrac{\pi_2, c}{\pi_2}\right)_3^{-2} = \left(\dfrac{c}{\pi_2}\right)_3^2$, car π_1 et π_2 sont non ramifiés dans $k_0(\sqrt[3]{c})$ (proposition 3) et on applique les propriétés (3), (4) et (6) de la section 3.

(3) Soit $\omega \in \mathcal{O}_{k_0}$ et π un élément premier de $\mathcal{O}_{k_0}$ ne divisant pas ω. Alors $X^3 \equiv \omega \pmod{\pi}$ est résoluble dans $\mathcal{O}_{k_0}$ si, et seulement si, $\omega^m \equiv 1 \pmod{\pi}$, où $m = (\mathcal{N}(\pi) - 1)/3$ (voir [I-R], chapitre 9).

Si $(c/\pi_1)_3 = (c/\pi_2)_3 = 1$, alors π_1 et π_2 se décomposent complètement dans $k_0(\sqrt[3]{c})$; donc les équations $c \equiv X^3 \pmod{\pi_1}$ et $c \equiv X^3 \pmod{\pi_2}$ sont résolubles dans $\mathcal{O}_{k_0}$; par la suite $c^{(p-1)/3} \equiv 1 \pmod{\pi_1}$ et $c^{(p-1)/3} \equiv 1 \pmod{\pi_2}$; alors $c^{(p-1)3} \equiv 1 \pmod{p}$; d'où d'après le critère d'Euler, on a c est reste cubique modulo p. Si c est reste cubique modulo p, alors $c^{(p-1)/3} \equiv 1 \pmod{p}$, donc $c^{(p-1)/3} \equiv 1 \pmod{\pi_1}$ et $c^{(p-1)/3} \equiv 1 \pmod{\pi_2}$; par la suite les équations $c \equiv X^3 \pmod{\pi_1}$ et $c \equiv X^3 \pmod{\pi_2}$ sont résolubles dans k_0 (voir [I-R]), c'est-à-dire $(c/\pi_1)_3 = (c/\pi_2)_3 = 1$.

(4) On a que π_1 se décompose complètement dans $k_0(\sqrt[3]{\pi_2})$ (voir [Is] page 52), c'est-à-dire $X^3 \equiv \pi_2 \pmod{\pi_1}$ admet des solutions dans $\mathcal{O}_{k_0}$ (proposition 3) ; donc $(\pi_1/\pi_2)_3 = (\pi_1/\pi_2)_3 = 1$. $\square$

Proposition 6. *Si* $(3/p)_3 \neq 1$, *alors* $\mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$.

Preuve. D'après la formule des classes ambiguës on a

$$\frac{3^{t-1} h_{k_0}}{[E_{k_0} : \ E_{k_0} \cap \mathcal{N} k^*]} = |\mathcal{H}_1(k)|,$$

où t est le nombre des premiers de k_0 qui se ramifient dans k ; on a $t = 3$ et $h_{k_0} = 1$ car $\mathcal{O}_{k_0}$ est principal. Comme $p \equiv 1 \pmod 9$, alors $p = \pi_1 \pi_2$ où π_1 et π_2 deux des éléments premiers de k_0 tels que $\pi_1^\tau = \pi_2$ et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{\lambda^3}$; puisque $3 = -j^2 \lambda^2$, alors $k = k_0(\sqrt[3]{x})$ où $x = \lambda^2 j^2 \pi_1 \pi_2$ et d'après la proposition 4, on a que j est une norme dans k/k_0 ; par la suite $|\mathcal{H}_1(k)| = 3^2$. Puisque $P_1^\sigma = P_1$ et $P_2^\sigma = P_2$, alors $\langle [P_1], [P_2] \rangle \subset \mathcal{H}_1(k)$.

Montrons que $\langle [P_1], [P_2] \rangle$ est d'ordre 9. Pour cela, il suffit de montrer que $[P_1^{a_1} P_2^{a_2}] = 1$ pour $a_1, a_2 \in \{0, 1, 2\}$ si, et seulement si, $a_1 = a_2 = 0$ (car $[P_1^3] = [P_2^3] = 1$). On a $[P_1^{a_1} P_2^{a_2}] = 1 \Rightarrow \exists\ \beta \in \mathcal{O}_k$ tel que $P_1^{a_1} P_2^{a_2} = \beta \mathcal{O}_k \Rightarrow \mathcal{N}_{k/k_0}(P_1^{a_1} P_2^{a_2}) = \mathcal{N}_{k/k_0}(\beta \mathcal{O}_k) \Rightarrow \pi_1^{a_1} \pi_2^{a_2} \mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\beta) \mathcal{O}_{k_0} \Rightarrow \exists\, \varepsilon \in E_{k_0}$ tel que $\pi_1^{a_1} \pi_2^{a_2} = \varepsilon \mathcal{N}_{k/k_0}(\beta)$ $\Rightarrow \exists\ \alpha \in \mathcal{O}_k$ tel que $\pi_1^{a_1} \pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha)$ (car $E_{k_0} \subset \mathcal{N}_{k/k_0}(k^*)$), d'où

$$\left(\frac{\pi_1^{a_1} \pi_2^{a_2}, 3^e \pi_1 \pi_2}{\mathcal{P}} \right)_3 = 1$$

pour tout idéal premier $\mathcal{P}$ de k_0 (remarque 3). Calculons ce symbole pour $\mathcal{P} = \pi_1 \mathcal{O}_{k_0}$ et $\mathcal{P} = \pi_2 \mathcal{O}_{k_0}$. D'une part,

$$\begin{aligned} A := \left(\frac{\pi_1^{a_1} \pi_2^{a_2}, 3^e \pi_1 \pi_2}{\pi_1 \mathcal{O}_{k_0}} \right)_3 &= \left(\frac{\pi_1^{a_1}, 3^e \pi_1 \pi_2}{\pi_1 \mathcal{O}_{k_0}} \right)_3 \left(\frac{\pi_2^{a_2}, 3^e \pi_1 \pi_2}{\pi_1 \mathcal{O}_{k_0}} \right)_3 \\ &= \left(\frac{\pi_1^{a_1}, 3^e}{\pi_1} \right)_3 \left(\frac{\pi_1^{a_1}, \pi_1}{\pi_1} \right)_3 \left(\frac{\pi_1^{a_1}, \pi_2}{\pi_1} \right)_3 \left(\frac{\pi_2^{a_2}, \pi_1}{\pi_1} \right)_3 \left(\frac{\pi_2^{a_2}, 3^e \pi_2}{\pi_1} \right)_3 \end{aligned}$$

D'autre part on a :

- $\left(\frac{\pi_1^{a_1}, \pi_1}{\pi_1} \right)_3 = \left(\frac{\pi_1, \pi_1}{\pi_1} \right)_3^{a_1} = 1$ par la propriété (1) de la section 3 et le fait que π_1 est norme dans $k_0(\sqrt[3]{\pi_1})/k_0$.

- $\left(\dfrac{\pi_1^{a_1}, \pi_2}{\pi_1}\right)_3 = \left(\dfrac{\pi_1, \pi_2}{\pi_1}\right)_3^{a_1} = \left(\dfrac{\pi_2}{\pi_1}\right)_3^{-a_1} = 1$ d'après les propriétés (1), (4), et la proposition 5.
- $\left(\dfrac{\pi_2^{a_2}, \pi_1}{\pi_1}\right)_3 = \left(\dfrac{\pi_2, \pi_1}{\pi_1}\right)_3^{a_2} = \left(\dfrac{\pi_2}{\pi_1}\right)_3^{a_2} = 1$ d'après les propriétés (1), (4) et la proposition 5.
- $\left(\dfrac{\pi_2^{a_2}, 3^e\pi_2}{\pi_1}\right)_3 = \left(\dfrac{\pi_2, 3^e\pi_2}{\pi_1}\right)_3^{a_2} = \left(\dfrac{3^e\pi_2}{\pi_1}\right)_3^{0} = 1$ par la proposition 3 et la propriété (4).
- $\left(\dfrac{\pi_1^{a_1}, 3^e}{\pi_1}\right)_3 = \left(\dfrac{\pi_1, 3^e}{\pi_1}\right)_3^{a_1} = \left(\dfrac{3^e}{\pi_1}\right)_3^{-a_1}$ grâce aux propriétés (1) et (4).

On obtient alors $A = (3^e/\pi_1)_3^{-a_1}$. Comme π_1 et π_2 jouent des rôles symétriques, alors $B := ((\pi_1^{a_1}\pi_2^{a_2}, 3^e\pi_1\pi_2)/\pi_2\mathcal{O}_{k_0})_3 = (3^e/\pi_2)_3^{-a_2}$, et puisque $((\pi_1^{a_1}\pi_2^{a_2}, 3^e\pi_1\pi_2)/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0, alors $A = B = 1$, c'est-à-dire $(3^e/\pi_1)_3^{a_1} = (3^e/\pi_2)_3^{a_2} = 1$. D'autre part, on a $(3/p)_3 \neq 1$ par hypothèse ; donc $(3^e/p)_3 \neq 1$ car $e \in \{1,2\}$. D'après la proposition 5, on a $(3^e/\pi_1)_3 = (3^e/\pi_2)_3^2 \neq 1$; d'où $a_1 = a_2 = 0$, car $(3^e/\pi_1)_3$ est une racine 3-ième de l'unité. Par la suite $\langle [P_1], [P_2] \rangle$ est d'ordre 9 ; or $|\mathcal{H}_1(k)| = 9$; d'où $\mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$. $\square$

Comme nous avons affaire à la relation qui lie les deux nombres de classes h_k et h_Γ, nous énonçons la proposition suivante où les notations sont comme suit : Γ un corps cubique pur, Γ' et Γ'' désignent les deux corps cubiques autres que Γ contenus dans le normalisé k de Γ, et on note par E_0 le sous-groupe de E_k défini par $E_0 = E_\Gamma E_{\Gamma'} E_{\Gamma''} E_{k_0}$.

Proposition 7.

(1) *Si on désigne par u l'indice $u = [E_k : E_0]$, alors il y a deux possibilités. Ou bien $u = 1$, $E_k = E_0$, ou bien $u = 3$, $E_0 \neq E_k$.*

(2) *De plus, $h_k = h_\Gamma^2 u/3$.*

Pour le preuve, voir [B-C1].

Théorème 2. *Soit $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ un corps cubique pur tel que $n = 3^e p^{e_1}$ où p est un premier $\equiv 1 \pmod 9$ et $e, e_1 \in \{1,2\}$. Alors*

$$\left(\frac{3}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Preuve. L'implication $3||h_\Gamma \Rightarrow (3/p)_3 \neq 1$ a été établie par Ismaili dans [Is] en montrant que $(3/p)_3 = 1 \Rightarrow 9|h_\Gamma$. Supposons que $(3/p)_3 \neq 1$. Soit $[\mathcal{A}] \in \mathcal{H}_2(k)$. Alors $[\mathcal{A}^{\sigma-1}] \in \mathcal{H}_1(k)$ car $\mathcal{H}_2(k)^{\sigma-1} \subset \mathcal{H}_1(k)$; comme $\mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$ (proposition 6) on a $[\mathcal{A}^{\sigma-1}] = [P_1^{a_1}P_2^{a_2}]$ où $a_1, a_2 \in \{0,1,2\}$; d'où $\exists\ \beta \in k^*$ tel que $\mathcal{A}^{\sigma-1} = \beta P_1^{a_1}P_2^{a_2}$; par la suite $\mathcal{N}_{k/k_0}(P_1^{a_1}P_2^{a_2}) = \mathcal{N}_{k/k_0}(\beta\mathcal{A}^{\sigma-1})$, c'est-à-dire $\pi_1^{a_1}\pi_2^{a_2}\mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\beta)\mathcal{O}_{k_0}$ (car on a $1 = \mathcal{N}_{k/k_0}(\mathcal{A}^{\sigma-1})$) ; d'où $\pi_1^{a_1}\pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha)$ (car $E_{k_0} \subset \mathcal{N}_{k/k_0}(k^*)$). D'après la démonstration de la proposition 6, on a $a_1 = a_2 = 0$; d'où $[\mathcal{A}^{\sigma-1}] = 1$, c'est-à-dire $[\mathcal{A}] \in \mathcal{H}_1(k) = \{[\mathcal{B}] \in \mathcal{H}(k) | [\mathcal{B}]^\sigma = [\mathcal{B}]\}$; donc $\mathcal{H}_2(k) \subset \mathcal{H}_1(k)$; ainsi $\mathcal{H}_1(k) = \mathcal{H}_2(k)$, (car $\mathcal{H}_1(k) \subset \mathcal{H}_2(k)$) ; par la suite $\mathcal{H}_1(k) = \mathcal{H}(k)$ (proposition 2) ; d'où $9||h_k = h_\Gamma^2 \frac{u}{3}$, c'est-à-dire $3||h_\Gamma$ et $u = 3$. $\square$

Une conséquence du théorème précédent est le résultat suivant qui nous permet d'identifier toute une famille de corps cubiques purs pour lesquels l'indice $u = 3$.

Corollaire 1. *Sous les hypothèses du théorème* 2*, on a :*

(1) $(3/p)_3 \neq 1 \Rightarrow u = 3$.
(2) $(3/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

Preuve. (1) D'après le théorème 2, $(3/p)_3 \neq 1 \Rightarrow 9||h_k$ et comme $h_k = h_\Gamma^2 \dfrac{u}{3}$, et $3||h_\Gamma$, on a $u = 3$.

(2) En effet, on sait que (voir [Is]) $(3/p)_3 = 1 \Rightarrow 9|h_\Gamma$ et comme $(3/p)_3 \neq 1 \Leftrightarrow 3||h_\Gamma$, on a le résultat. □

Exemples. Rappelons d'abord que si $A \in \mathbb{Z}$ et p est un nombre premier tel que $p \equiv 1 \pmod 3$ et $p \not| A$, alors d'après le critère d'Euler on a que, $A \equiv X^3 \pmod p$ est résoluble $\Leftrightarrow A^{(p-1)/3} \equiv 1 \pmod p$.

(1) Pour $n = 3{\cdot}19 = 57$ ou $n = 3^2{\cdot}19 = 171$, on a que 19 est un nombre premier $\equiv 1 \pmod 9$; notons que $19 = (-5-3j)(-2+3j) = \pi_1\pi_2$. Par la suite on aura $\pi_1 \equiv \pi_2 \equiv 1 \pmod{\lambda^3}$; d'autre part on a que $-\pi_1$ et $-\pi_2$ sont deux premiers primaires de k_0, c'est-à-dire $-\pi_1 \equiv -\pi_2 \equiv 2 \pmod{3\mathcal{O}_{k_0}}$; donc $(3/\pi_1)_3 = (3/\pi_2)_3^2 = j^2$ (voir [I-R], chapitre 9) ; ainsi $(3/19)_3 \neq 1$; par la suite nous pouvons affirmer, grâce au théorème 2, que $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{3\cdot 19}) = \mathbf{Q}(\sqrt[3]{57})$ et $\Gamma = \mathbf{Q}(\sqrt[3]{3^2\cdot 19}) = \mathbf{Q}(\sqrt[3]{171})$.

(2) 37 est un nombre premier $\equiv 1 \pmod 9$; de plus $37 = (7+3j)(4-3j) = \pi_1'\pi_2'$, où $\pi_1' \equiv \pi_2' \equiv 1 \pmod{\lambda^3}$; comme $-\pi_1'$ et $-\pi_2'$ sont deux premiers primaires dans $\mathcal{O}_{k_0}$, alors $(3/\pi_1')_3 = (3/\pi_2')_3^2 = j^2$ (voir [I-R], chapitre 9) ; par conséquent, $(3/17)_3 \neq 1$, (proposition 5) ; d'où $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{3\cdot 37}) = \mathbf{Q}(\sqrt[3]{111})$ et $\Gamma = \mathbf{Q}(\sqrt[3]{3^2\cdot 37}) = \mathbf{Q}(\sqrt[3]{333})$.

(3) Pour tous les nombres premiers $p \in \{109, 127, 163, 181, 199\}$ et $e \in \{1, 2\}$, on vérifie que $p \equiv 1 \pmod 9$ et $(3/p)_3 \neq 1$, par la suite $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{3^e p})$ où $e \in \{1, 2\}$.

5. Cas où $n = q^e p^{e_1}$**, avec** $p \equiv -q \equiv 1 \pmod 9$**.** Ici $e, e_1 \in \{1, 2\}$. Comme $n \equiv \pm 1 \pmod 9$, alors Γ est de deuxième espèce ; donc 3 n'est pas totalement ramifié dans Γ (proposition 1) ; par la suite $\lambda = 1 - j$ est non ramifié dans k/k_0. Puisque $p \equiv -q \equiv 1 \pmod 3$, alors q est inerte dans k_0 et $p = \pi_1\pi_2$ où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$ et $\pi_1 = \pi_2^\tau$; par la suite les premiers qui se ramifient dans k/k_0 sont π_1, π_2 et q. Comme $p \equiv -q \equiv 1 \pmod 9$, alors $-q = \pi_3$ est un nombre premier de k_0 tel que $\pi_3 \equiv \pi_1 \equiv \pi_2 \equiv 1 \pmod{\lambda^3}$; donc si on pose $x = \pi_3^e \pi_1^{e_1} \pi_2^{e_1}$ on a que $k = k_0(\sqrt[3]{x})$.

Théorème 3. *Soit* $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ *un corps cubique pur tel que* $n = q^e p^{e_1}$ *où* p *et* q *sont des premiers vérifiant* $p \equiv -q \equiv 1 \pmod 9$ *et* $e, e_1 \in \{1, 2\}$. *Alors*

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Preuve. On a $\pi_i \equiv 1 \pmod{\lambda^3}$ pour tout $1 \leq i \leq 3$; alors j est une norme dans k/k_0 (proposition 4). Donc $[E_{k_0} : E_{k_0} \cap \mathcal{N}k^*] = 1$; par la suite $|\mathcal{H}_1(k)| = 3^2$ car le nombre des premiers qui se ramifient dans k/k_0 est 3. On montre d'une manière analogue à celle du théorème 2 que $(q/p)_3 \neq 1 \Rightarrow 3||h_\Gamma$; il suffit de remplacer 3 par q dans la proposition 6 et le théorème 2. Inversement si $3||h_\Gamma$, alors d'après Ismaili [Is] on a $(q/p)_3 \neq 1$. $\square$

Corollaire 2. *Sous les hypothèses du théorème* 3*, on a :*

(1) $(q/p)_3 \neq 1 \Rightarrow u = 3$.
(2) $(q/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

La démonstration est la même que celle du corollaire 1.

Exemples. (1) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 17^e})$, où $e \in \{1, 2\}$; 19 et 17 sont deux nombres premiers congrus respectivement à 1 et $-1 \pmod 9$. On a $17 \equiv -2 \pmod{19}$ et $(2/19)_3 \neq 1$, (car $2^6 \not\equiv 1 \pmod{19}$) ; alors $(17/19)_3 \neq 1$. D'où $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 17}) = \mathbf{Q}(\sqrt[3]{323})$ et $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 17^2}) = \mathbf{Q}(\sqrt[3]{5491})$.

(2) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{37 \cdot 17^e})$, où $e \in \{1, 2\}$; 37 est un premier $\equiv 1 \pmod 9$; comme $(17/37)_3 \neq 1$, alors $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{17 \cdot 37}) = \mathbf{Q}(\sqrt[3]{629})$ et $\Gamma = \mathbf{Q}(\sqrt[3]{17^2 \cdot 37}) = \mathbf{Q}(\sqrt[3]{10693})$.

(3) On a que 71 est un premier congru à $-1 \pmod 9$, et $71 \equiv 14 \pmod{19}$. Comme $(14/19)_3 \neq 1$ (car $14^6 \not\equiv 1 \pmod{19}$, alors $(71/19)_3 \neq 1$; d'où d'après le théorème 3, $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{71 \cdot 19}) = \mathbf{Q}(\sqrt[3]{1349})$ et $\Gamma = \mathbf{Q}(\sqrt[3]{19^2 \cdot 71}) = \mathbf{Q}(\sqrt[3]{25631})$.

Comme les tables de [B-W-Z] donnant le nombre de classes de $\mathbf{Q}(\sqrt[3]{n})$ arrêtent en $n = 998$, nous vérifions le théorème 3 seulement pour $\mathbf{Q}(\sqrt[3]{19 \cdot 17}) = \mathbf{Q}(\sqrt[3]{323})$ et $\mathbf{Q}(\sqrt[3]{17 \cdot 37}) = \mathbf{Q}(\sqrt[3]{629})$ dont le nombre de classes est 3.

6. Cas où $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$ avec $p \equiv 1 \pmod 9$ et $-q_1$ ou $-q_2 \equiv 4$ ou $7 \pmod 9$. Ici $e_1, e_2 \in \{1, 2\}$ et sans perte de généralité on peut supposer que $e = 1$ (car $\mathbf{Q}(\sqrt[3]{ab^2}) = \mathbf{Q}(\sqrt[3]{a^2 b})$). Comme $p \equiv 1 \pmod 3$, alors $p = \pi_1 \pi_2$, où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$ et $\pi_1^\tau = \pi_2$. On a $3\mathcal{O}_{k_0} = \lambda^2 \mathcal{O}_{k_0}$ où $\lambda = 1 - j$. Puisque $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$, alors les premiers de k_0 qui se ramifient dans k sont $\pi_1 \mathcal{O}_k = P_1^3$, $\pi_2 \mathcal{O}_k = P_2^3$, $q_1 \mathcal{O}_k = \mathcal{Q}_1^3$ et $q_2 \mathcal{O}_k = \mathcal{Q}_2^3$ car $q_1 \equiv q_2 \equiv -1 \pmod 3$, où P_1, P_2, Q_1, Q_2 désignent des idéaux premiers de k.

Proposition 8. $(q_1^{e_1} q_2^{e_2}/p)_3 \neq 1 \Rightarrow \mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$.

Preuve. On a $k = k_0(\sqrt[3]{x})$, où $x = \pi_1 \pi_2 \pi_3^{e_1} \pi_4^{e_2}$ avec $\pi_3 = -q_1$ et $\pi_4 = -q_2$. Comme $-q_1$ ou $-q_2 \equiv 4$ ou $7 \pmod 9$, alors j n'est pas une norme dans k/k_0 (proposition 4) ; donc $[E_{k_0} : E_{k_0} \cap \mathcal{N}k^*] = 3$. Par la formule des classes ambiguës, on a $|\mathcal{H}_1(k)| = 3^2$, car le nombre des idéaux premiers qui se ramifient dans k/k_0 est $t = 4$. Comme $P_1^\sigma = P_1$ et $P_2^\sigma = P_2$, alors $\langle [P_1], [P_2] \rangle \subset \mathcal{H}_1(k)$. Montrons que $\langle [P_1], [P_2] \rangle$ est d'ordre 9. Pour cela, il suffit de montrer que $[P_1^{a_1} P_2^{a_2}] = 1$ pour $a_1, a_2 \in \{0, 1, 2\}$ si, et seulement si, $a_1 = a_2 = 0$, (car $[P_1^3] = [P_2^3] = 1$).

On a : $[P_1^{a_1} P_2^{a_2}] = 1 \Rightarrow \exists\ \alpha \in \mathcal{O}_k$ tel que $P_1^{a_1} P_2^{a_2} = \alpha \mathcal{O}_k \Rightarrow \mathcal{N}_{k/k_0}(P_1^{a_1} P_2^{a_2}) = \mathcal{N}_{k/k_0}(\alpha \mathcal{O}_k) \Rightarrow \pi_1^{a_1} \pi_2^{a_2} \mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\alpha) \mathcal{O}_{k_0} \Rightarrow \exists\ \varepsilon \in E_{k_0}$ tel que $\varepsilon \pi_1^{a_1} \pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha) \Rightarrow ((\varepsilon \pi_1^{a_1} \pi_2^{a_2}, \pi_1 \pi_2 q_1^{e_1} q_2^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0. En particulier, pour $\mathcal{P} = \pi_1\mathcal{O}_{k_0}$ et $\mathcal{P} = \pi_2\mathcal{O}_{k_0}$, on a d'une part que

$$A := \left(\frac{\varepsilon\pi_1^{a_1}\pi_2^{a_2}, \pi_1\pi_2 q_1^{e_1}q_2^{e_2}}{\pi_1\mathcal{O}_{k_0}}\right)_3$$
$$= \left(\frac{\varepsilon, \pi_1}{\pi_1}\right)_3\left(\frac{\varepsilon, \pi_2 q_1^{e_1}q_2^{e_2}}{\pi_1}\right)_3\left(\frac{\pi_1^{a_1}, \pi_1\pi_2}{\pi_1}\right)_3\left(\frac{\pi_1^{a_1}, q_1^{e_1}q_2^{e_2}}{\pi_1}\right)_3\left(\frac{\pi_2^{a_2}, \pi_1}{\pi_1}\right)_3\left(\frac{\pi_2^{a_2}, \pi_2 q_1^{e_1}q_2^{e_2}}{\pi_1}\right)_3$$

D'autre part on a :

• $((\varepsilon, \pi_1)/\pi_1)_3 = 1$; en effet, si $\varepsilon = \pm 1$, alors ε est norme dans $k_0(\sqrt[3]{\pi_1})/k_0$; si $\varepsilon = j$ ou j^2, alors π_1 se décompose complètement dans $k_0(\sqrt[3]{\varepsilon})$, puisque $p \equiv 1 \pmod 9$; par la suite $(k_0(\sqrt[3]{\varepsilon})/\pi_1) = 1$, d'où $((\varepsilon, \pi_1)/\pi_1)_3 = (\varepsilon/\pi_1)_3 = 1$.

• $((\varepsilon, \pi_2 q_1^{e_1}q_2^{e_2})/\pi_1)_3 = 1$ et $((\pi_2^{a_2}, \pi_1 q_1^{e_1}q_2^{e_2})/\pi_1)_3 = 1$ d'après la propriété (4).

• $((\pi_2^{a_2}, \pi_1)/\pi_1)_3 = ((\pi_1, \pi_2^{a_2})/\pi_1)_3^{-1} = (\pi_2/\pi_1)_3^{a_2} = 1$ d'après les propriétés (3), (4) et la proposition 5.

• $((\pi_1^{a_1}, \pi_1\pi_2)/\pi_1)_3 = ((\pi_1^{a_1}, \pi_1)/\pi_1)_3(\pi_2/\pi_1)_3^{-a_1} = 1$ car $(\pi_2/\pi_1)_3 = 1$ et π_1 est une norme dans $k_0(\sqrt[3]{\pi_1})/k_0$ (il suffit de remarquer que

$$\mathcal{N}_{k/k_0}(\sqrt[3]{\pi_1}) = (\sqrt[3]{\pi_1})(j\sqrt[3]{\pi_1})(j^2\sqrt[3]{\pi_1}) = \pi_1).$$

D'où

$$A = \left(\frac{\pi_1^{a_1}, q_1^{e_1}q_2^{e_2}}{\pi_1}\right)_3 = \left(\frac{q_1^{e_1}q_2^{e_2}}{\pi_1}\right)_3^{-a_1}.$$

En changeant les rôles de π_1 et π_2 on obtient :

$$B := \left(\frac{\varepsilon\pi_1^{a_1}\pi_2^{a_2}, \pi_1\pi_2 q_1^{e_1}q_2^{e_2}}{\pi_2\mathcal{O}_{k_0}}\right)_3 = \left(\frac{q_1^{e_1}q_2^{e_2}}{\pi_2}\right)_3^{-a_2}.$$

Puisque $(q_1^{e_1}q_2^{e_2}/p)_3 \neq 1$, alors d'après la proposition 5, $(q_1^{e_1}q_2^{e_2}/\pi_1)_3 = (q_1^{e_1}q_2^{e_2}/\pi_2)_3^2 \neq 1$. Par la suite $A = B = 1$ entraîne que $a_1 = a_2 = 0$; d'où $\langle[P_1], [P_2]\rangle$ est d'ordre 9. $\square$

Théorème 4. *Soit p, q_1, q_2 des premiers tels que $p \equiv -q_1 \equiv -q_2 \equiv 1 \pmod 3$ et soit h_Γ le nombre de classes du corps cubique pur $\Gamma = \mathbf{Q}(\sqrt[3]{n})$, où $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$. Si $p \equiv 1 \pmod 9$ et $-q_1$ ou $-q_2 \equiv 4$ ou $7 \pmod 9$, alors*

$$(q_1^{e_1}q_2^{e_2}/p)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Preuve. L'implication $3||h_\Gamma \Rightarrow (q_1^{e_1}q_2^{e_2}/p)_3 \neq 1$ a été établie par Ismaili dans [Is]. Comme $h_k = h_\Gamma^2 \dfrac{u}{3}$ (proposition 7), alors

$$(3||h_\Gamma \text{ et } u = 3) \Leftrightarrow 9||h_k.$$

Il suffit donc de montrer que $\mathcal{H}_1(k) = \mathcal{H}_2(k)$ car ceci imliquera que $\mathcal{H}(k) = \mathcal{H}_1(k)$ (proposition 2), c'est-à-dire $9||h_k$. Or $[\mathcal{A}] \in \mathcal{H}_2(k) \Rightarrow [\mathcal{A}]^{\sigma-1} \in \mathcal{H}_1(k) = \langle[P_1], [P_2]\rangle$ $\Rightarrow \exists\, a_1, a_2 \in \{0, 1, 2\}$ tels que $[\mathcal{A}^{\sigma-1}] = [P_1^{a_1}P_2^{a_2}] \Rightarrow \exists\, \alpha \in k^*$ tel que $P_1^{a_1}P_2^{a_2} = \alpha\mathcal{A}^{\sigma-1} \Rightarrow \pi_1^{a_1}\pi_2^{a_2}\mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\alpha)\mathcal{O}_{k_0}$ (car $\mathcal{N}_{k/k_0}(\mathcal{A}^{\sigma-1}) = 1$) $\Rightarrow \exists\, \varepsilon \in E_{k_0}$ tel que $\varepsilon\pi_1^{a_1}\pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha) \Rightarrow a_1 = a_2 = 0$ (ceci d'après la démonstration de la proposition précédente) $\Rightarrow [\mathcal{A}] \in \mathcal{H}_1(k) \Rightarrow \mathcal{H}_2(k) \subset \mathcal{H}_1(k) \Rightarrow \mathcal{H}_1(k) = \mathcal{H}_2(k)$. D'où $\mathcal{H}_1(k) = \mathcal{H}(k)$, c'est-à-dire $9||h_k$. $\square$

Corollaire 3. *Sous les hypothèses du théorème* 4*, on a :*

(1) $(q_1^{e_1}q_2^{e_2}/p)_3 \neq 1 \Rightarrow u = 3$.
(2) $(q_1^{e_1}q_2^{e_2}/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

La preuve est similaire à celle des corollaires précédents.

Exemples. (1) Prenons $p = 19, q_1 = 2, q_2 = 5$; on a $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 2 \cdot 5}) = \mathbf{Q}(\sqrt[3]{190})$. Puisque $(2 \cdot 5/19)_3 \neq 1$ (car $10^6 \not\equiv 1 \pmod{19}$) ; d'après le théorème 4, $3||h_\Gamma$ et $u = 3$.

(2) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 2^2 \cdot 5^2}) = \mathbf{Q}(\sqrt[3]{1900})$; on a $(2^2 \cdot 5^2/19)_3 = (100/19)_3$. Comme $100 \equiv 5 \pmod{19}$ et $(5/19)_3 \neq 1$, car $5^{(19-1)/3} = 5^6 \not\equiv 1 \pmod{19}$, alors $(100/19)_3 \neq 1$. D'où $3||h_\Gamma$ et $u = 3$.

(3) Si on considère $p = 37, q_1 = 5, q_2 = 7$, on a $n = 37 \cdot 5 \cdot 7 = 1295 \equiv -1 \pmod 9$. Puisque $35 \equiv -2 \pmod{37}$ et $(2/37)_3 \neq 1$ (car $2^{12} \not\equiv 1 \pmod{37}$), alors $(35/37)_3 \neq 1$; par la suite $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{1295})$.

7. Cas où $n = 3^e p^{e_1} q^{e_2} \not\equiv \pm 1 \pmod 9$ **avec** $p \equiv 1 \pmod 9$ **et** $-q \equiv 4$ **ou** $7 \pmod 9$**.** Ici $e \in \{0, 1, 2\}$, $e_2 \in \{1, 2\}$ et sans perte de généralité on suppose que $e_1 = 1$ (car $\mathbf{Q}(\sqrt[3]{a^2 b}) = \mathbf{Q}(\sqrt[3]{ab^2})$, pour tout $a, b \in \mathbb{N}$). Comme $p \equiv 1 \pmod 9$, alors $p = \pi_1\pi_2$ où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1^\tau = \pi_2$ et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$ et $3\mathcal{O}_{k_0} = \lambda^2\mathcal{O}_{k_0}$. Or $n \not\equiv \pm 1 \pmod 9$. Alors les premiers de k_0 qui se ramifient dans k sont $\pi_1\mathcal{O}_k = P_1^3$, $\pi_2\mathcal{O}_k = P_2^3$, $q\mathcal{O}_k = \mathcal{Q}^3$ et $\lambda\mathcal{O}_k = I^3$, $\forall e \in \{0, 1, 2\}$, où P_1, P_2, I et $\mathcal{Q}$ désignent des idéaux premiers de k.

Théorème 5. *Soit* p *et* q *des premiers tels que* $p \equiv -q \equiv 1 \pmod 3$ *et* h_Γ *le nombre de classes du corps cubique pur* $\Gamma = \mathbf{Q}(\sqrt[3]{n})$*, où* $n = 3^e p^{e_1} q^{e_2} \not\equiv \pm 1 \pmod 9$*,* $e \in \{0, 1, 2\}$ *et* $e_1, e_2 \in \{1, 2\}$*. Si* $p \equiv 1 \pmod 9$ *et* $-q \equiv 4$ *ou* $7 \pmod 9$*, alors*

$$\left(\frac{3^e q^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Preuve. L'implication $3||h_\Gamma \Rightarrow (3^e q^{e_2}/p)_3 \neq 1$ a été établie par Ismaili dans [Is]. Supposons que $(3^e q^{e_2}/p)_3 \neq 1$. Dans le cas où $e \neq 0$ la démonstration est analogue à celle du théorème 4 en remplaçant q par 3. Si $e = 0$ on démontre que

$$(q/p)_3 \neq 1 \Rightarrow \mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle = \mathcal{H}(k) \text{ et } |\mathcal{H}_1(k)| = 9,$$

de la même manière que dans la preuve de la proposition 8. □

Corollaire 4. *Sous les hypothèses du théorème* 5*, on a :*

(1) $(3^e q^{e_2}/p)_3 \neq 1 \Rightarrow u = 3$.
(2) $(3^e q^{e_2}/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

La preuve est similaire à celle des corollaires précédents.

Exemples. (1) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{3 \cdot 5 \cdot 19}) = \mathbf{Q}(\sqrt[3]{285})$. On a $3 \cdot 5 = 15 \equiv -4 \pmod{19}$ et $\left(\frac{4}{19}\right)_3 \neq 1$, car $4^6 \not\equiv 1 \pmod{19}$; par la suite $\left(\frac{15}{19}\right)_3 \neq 1$. D'où $3||h_\Gamma$ et $u = 3$.

(2) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{3^2 \cdot 5^2 \cdot 37}) = \mathbf{Q}(\sqrt[3]{8325})$. On a $3^2 \cdot 5^2 = 225 \equiv 3 \pmod{37}$ et $3^{(37-1)/3} = 3^{12} \not\equiv 1 \pmod{37}$; donc $(3^2 \cdot 5^2/37)_3 \neq 1$; d'où $3||h_\Gamma$ et $u = 3$.

(3) Si on considère $p = 19$, $q = 5$ et $e = 0$, on aura $pq = 19 \cdot 5 \not\equiv \pm 1 \pmod 9$, et $(5/19)_3 \neq 1$, (car $5^{(19-1)/3} = 5^6 \not\equiv 1 \pmod{19}$). Alors $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{19 \cdot 5}) = \mathbf{Q}(\sqrt[3]{95})$.

8. Cas où $n = p^{e_1} q^{e_2} \not\equiv \pm 1 \pmod 9$ **avec** $p \equiv 4$ **ou** $7 \pmod 9$**.** Ici $e_2 \in \{1, 2\}$ et nous pouvons supposer que $e_1 = 1$, car $\mathbf{Q}(\sqrt[3]{a^2 b}) = \mathbf{Q}(\sqrt[3]{ab^2})$. Pour traiter ce cas, nous aurons besoin de la proposition suivante due à Gerth [Ge].

Proposition 9. *Soit* $k = k_0(\sqrt[3]{x}) \neq k_0$*, où* $x = \lambda^{e_\lambda} j^{e_j} \pi_1^{e_1} \cdots \pi_f^{e_f} \pi_{f+1}^{e_{f+1}} \cdots \pi_g^{e_g}$, $\lambda = 1 - j$ *et où* π_i *est un élément premier de* k_0 *tel que* $\pi_i \equiv 1 \pmod{\lambda^3}$ *pour* $1 \leq i \leq f$ *et* $\equiv 4$ *ou* $7 \pmod{\lambda^3}$ *pour* $f+1 \leq i \leq g$*,* e_λ *et* $e_j \in \{0, 1, 2\}$ *et* $e_i \in \{1, 2\}$ *pour* $1 \leq i \leq g$*.*

(1) *Si* $x \equiv 1 \pmod{\lambda^3}$*, on a*

$$(k/k_0)^* = k(\sqrt[3]{\pi_1}, \ldots, \sqrt[3]{\pi_f}, \sqrt[3]{\pi_{f+1}\pi_{f+2}{}^{r_{f+2}}}, \ldots, \sqrt[3]{\pi_{f+1}\pi_g^{r_g}}) \tag{3}$$

où $r_i = 1$ *ou* 2 *est choisi tel que* $\pi_{f+1}\pi_i^{r_i} \equiv 1 \pmod{\lambda^3}$ *pour* $f+2 \leq i \leq g$*.*

(2) *Si* $x \equiv 1 \pmod{\lambda^3}$*, on a une égalité similaire pour* $(k/k_0)^*$ *si on élimine une des racines cubiques de la partie droite de l'égalité* (3)*.*

Comme $p \equiv 1 \pmod 3$, alors $p = \pi_1 \pi_2$ où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1^\tau = \pi_2$ et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$, puisque $n = pq^{e_2} \not\equiv \pm 1 \pmod 9$, alors les premiers de k_0 qui se ramifient dans k sont $\pi_1 \mathcal{O}_k = P_1^3$, $\pi_2 \mathcal{O}_k = P_2^3$, $q\mathcal{O}_k = \mathcal{Q}^3$ et $\lambda \mathcal{O}_k = I^3$, où $\lambda = 1 - j$, P_1, P_2, $\mathcal{Q}$, et I sont des idéaux premiers de k.

Proposition 10. $(q/p)_3 \neq 1 \Rightarrow \mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$.

Preuve. Comme $p \equiv 4$ ou $7 \pmod 9$, alors j n'est pas une norme dans k/k_0 (proposition 4) ; donc $[E_{k_0} : E_{k_0} \cap \mathcal{N}_{k/k_0}(k^*)] = 3$; par la suite $|\mathcal{H}_1(k)| = 9$ car $t = 4$ et $h_{k_0} = 1$. On a $\langle [P_1], [P_2] \rangle \subset \mathcal{H}_1(k)$ car $P_i^\sigma = P_i$ $(i = 1, 2)$. Montrons dans la suite que $\langle [P_1], [P_2] \rangle$ est d'ordre 9, pour cela il suffit de montrer que $[P_1^{a_1} P_2^{a_2}] = 1$ pour $a_1, a_2 \in \{0, 1, 2\}$ si, et seulement si, $a_1 = a_2 = 0$.

D'après la proposition 9, on a $(k/k_0)^* = k(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2})$. Si $[P_1^{a_1} P_2^{a_2}] = 1$, alors $\exists\, \alpha \in \mathcal{O}_k$ tel que $P_1^{a_1} P_2^{a_2} = \alpha \mathcal{O}_k$; par la suite $\pi_1^{a_1} \pi_2^{a_2} \mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\alpha) \mathcal{O}_{k_0}$; donc $\exists\, \varepsilon \in E_{k_0}$ tel que $\varepsilon \pi_1^{a_1} \pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha)$; d'où $((\varepsilon \pi_1^{a_1} \pi_2^{a_2}, \pi_1 \pi_2 q^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0. Calculons ce symbole pour $\mathcal{P} = \pi_1 \mathcal{O}_{k_0}$ et $\pi_2 \mathcal{O}_{k_0}$, on a (grâce à la propriété (8)) :

$$A := \left(\frac{\varepsilon \pi_1^{a_1} \pi_2^{a_2}, \pi_1 \pi_2 q^{e_2}}{\pi_1} \right)_3 = \left(\frac{\alpha, \pi_1 \pi_2 q^{e_2}}{P_1} \right)_3 = \left(\frac{\alpha, \pi_1}{P_1} \right)_3 \left(\frac{\alpha, \pi_2}{P_1} \right)_3 \left(\frac{\alpha, q^{e_2}}{P_1} \right)_3 .$$

D'après la formule produit (propriété (7)) on a

$$\prod_{\mathcal{P}} \left(\frac{\alpha, \pi_1}{\mathcal{P}} \right)_3 = 1.$$

Si $\mathcal{P}$ est infini, alors $((\alpha, \pi_1)/\mathcal{P})_3 = 1$ (d'après la propriété 4). Si $\mathcal{P} = P_2$, alors $((\alpha, \pi_1)/P_2)_3 = (\pi_1/P_2)_3^{a_2} = 1$ car $(\pi_1/\pi_2)_3 = 1$ et $k(\sqrt[3]{\pi_1})/k$ est non ramifiée.

Si $\mathcal{P}$ est fini et différent de P_1 et P_2, alors $((\alpha, \pi_1)/\mathcal{P})_3 = (\pi_1/\mathcal{P})_3^0 = 1$ (d'après la propriété (4)) car $k(\sqrt[3]{\pi_1}) \subset (k/k_0)^*$ qui est non ramifiée sur k ; d'où $((\alpha, \pi_1)/P_1)_3 = 1$, et comme $((\alpha, \pi_2)/P_1)_3 = (\pi_2/P_1)_3^{-a_2} = 1$ (car $(\pi_2/\pi_1)_3 = 1$), alors

$$A = \left(\frac{\alpha, q^{e_2}}{P_1}\right)_3 = \left(\frac{q^{e_2}}{P_1}\right)_3^{-a_1}.$$

On reprend les mêmes calculs en intervertissant les rôles de π_1 et π_2. On obtient alors :

$$B := \left(\frac{\varepsilon\pi_1^{a_1}\pi_2^{a_2}, \pi_1\pi_2 q^{e_2}}{\pi_2}\right)_3 = \left(\frac{q^{e_2}}{P_2}\right)_3^{-a_2}.$$

Comme $(q/p)_3 \neq 1$, alors $(q/\pi_1)_3$ et $(q/\pi_2)_3$ sont différents de 1, c'est-à-dire P_1 et P_2 restent inertes dans $k(\sqrt[3]{q^{e_2}})$; par la suite $(q^{e_2}/P_1)_3$ et $(q^{e_2}/P_2)_3$ sont différents de 1 (car $e_2 \in \{1, 2\}$). D'où $a_1 = a_2 = 0$, car $A = B = 1$. Puisque $[P_1]^3 = [P_2]^3 = 1$, alors $\langle [P_1], [P_2] \rangle$ est d'ordre 9. Ainsi $\mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$. $\square$

Théorème 6. *Soit p et q deux nombres premiers tels que $p \equiv 4$ ou $7 \pmod 9$, $q \equiv -1 \pmod 3$ et h_Γ le nombre de classes du corps cubique pur $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ où $n = p^{e_1}q^{e_2} \not\equiv \pm 1 \pmod 9$, $e_1, e_2 \in \{1, 2\}$. Alors on a :*

$$(q/p)_3 \neq 1 \Leftrightarrow 3 || h_\Gamma.$$

Preuve. Dans ce cas on a, $(k/k_0)^* = k(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2})$ (proposition 9). Soit $[\mathcal{A}] \in \mathcal{H}_2(k)$. Donc $[\mathcal{A}^{\sigma-1}] \in \mathcal{H}_1(k) = \langle [P_1], [P_2] \rangle$. Alors il existe $a_1, a_2 \in \{0, 1, 2\}$ tels que $[\mathcal{A}^{\sigma-1}] = [P_1^{a_1}P_2^{a_2}]$, c'est-à-dire $\exists\ \alpha \in k^*$ tel que $P_1^{a_1}P_2^{a_2} = \alpha\mathcal{A}^{\sigma-1}$. D'où $\exists\ \varepsilon \in E_{k_0}$ tel que $\varepsilon\pi_1^{a_1}\pi_2^{a_2} = \mathcal{N}_{k/k_0}(\alpha)$ car $\mathcal{N}_{k/k_0}(\mathcal{A}^{\sigma-1}) = 1$. Par la suite, $((\varepsilon\pi_1^{a_1}\pi_2^{a_2}, \pi_1\pi_2 q^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0. D'après les propriétés (1) et (8) on a :

$$\begin{aligned} A &:= \left(\frac{\varepsilon\pi_1^{a_1}\pi_2^{a_2}, \pi_1\pi_2 q^{e_2}}{\pi_1}\right)_3 = \left(\frac{\alpha, \pi_1\pi_2 q^{e_2}}{P_1}\right)_3 \\ &= \left(\frac{\alpha, \pi_1}{P_1}\right)_3 \left(\frac{\alpha, \pi_2}{P_1}\right)_3 \left(\frac{\alpha, q^{e_2}}{P_1}\right)_3 = 1. \end{aligned}$$

Puisque $k(\sqrt[3]{\pi_2})/k$ est non ramifiée et $(\pi_2/\pi_1)_3 = 1$, alors $((\alpha, \pi_2)/P_1)_3 = (\pi_2/\pi_1)_3^{-a_1} = 1$. On a $((\alpha, \pi_1)/P_1)_3 = 1$; en effet, soit

$$\mathcal{A} := \prod_{i=1}^{g} \mathcal{P}_i^{a_i^0 + a_i^1\sigma + a_i^2\sigma^2}$$

la décomposition de $\mathcal{A}$ en idéaux premiers de k, alors

$$\mathcal{A}^{\sigma-1} = \prod_{i=1}^{g} \mathcal{P}_i^{(a_i^2 - a_i^0) + (a_i^0 - a_i^1)\sigma + (a_i^1 - a_i^2)\sigma^2}.$$

Comme $P_i^\sigma = P_i$ $(i = 1, 2)$, on peut supposer que P_1 et P_2 ne divisent pas $\mathcal{A}$. D'après la formule du produit, on a

$$\prod_{\mathcal{P}} \left(\frac{\alpha, \pi_1}{\mathcal{P}}\right)_3 = 1 \tag{4}$$

- Si $\mathcal{P}$ est infini, alors $((\alpha, \pi_1)/\mathcal{P})_3 = 1$ (la propriété (4) s'applique car $\mathcal{P}$ est non ramifié dans $k(\sqrt[3]{\pi_1})$ puisque k est totalement imaginaire).
- Si $\mathcal{P} = P_2$, alors $((\alpha, \pi_1)/P_2)_3 = (\pi_1/P_2)_3^{-a_2} = 1$ car $k(\sqrt[3]{\pi_1})$ est non ramifiée sur k et $(\pi_1/\pi_2)_3 = 1$.
- Si $\mathcal{P}$ est différent de P_1 et P_2 et ne divise pas $\mathcal{A}^{\sigma-1}$, alors $((\alpha, \pi_1)/\mathcal{P})_3 = (\pi_1/\mathcal{P})_3^0 = 1$ car $\alpha\mathcal{O}_k = P_1^{a_1} P_2^{a_2} \mathcal{A}^{1-\sigma}$. Par la suite l'égalité (4) se réduit à

$$\left(\frac{\alpha, \pi_1}{P_1}\right)_3 \prod_{i=1}^{g} \left(\frac{\alpha, \pi_1}{\mathcal{P}_i}\right)_3 \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^\sigma}\right)_3 \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^{\sigma^2}}\right)_3 = 1 \tag{5}$$

D'autre part, en utilisant le fait que $k(\sqrt[3]{\pi_1})/k$ est non ramifiée et la propriété (4), on obtient $((\alpha, \pi_1)/\mathcal{P}_i)_3 = (\pi_1/\mathcal{P}_i)_3^{(a_i^2 - a_i^0)}$ car $\alpha\mathcal{O}_k = P_1^{a_1} P_2^{a_2} \mathcal{A}^{1-\sigma}$. Comme les racines 3-ièmes de l'unité sont fixées par σ, alors d'après la propriété (6) on a

$$\left(\frac{\alpha, \pi_1}{\mathcal{P}_i^\sigma}\right)_3 = \sigma^2 \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^\sigma}\right)_3 = \left(\frac{\alpha^{\sigma^2}, \pi_1}{\mathcal{P}_i}\right)_3 = \left(\frac{\pi_1}{\mathcal{P}_i}\right)_3^{(a_i^0 - a_i^1)}$$

et

$$\left(\frac{\alpha, \pi_1}{\mathcal{P}_i^{\sigma^2}}\right)_3 = \sigma \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^\sigma}\right)_3 = \left(\frac{\alpha^\sigma, \pi_1}{\mathcal{P}_i}\right)_3 = \left(\frac{\pi_1}{\mathcal{P}_i}\right)_3^{(a_i^1 - a_i^2)}$$

car $\mathcal{A}^{1-\sigma} = \displaystyle\prod_{i=1}^{g} \mathcal{P}_i^{(a_i^0 - a_i^2) + (a_i^1 - a_i^0)\sigma + (a_i^2 - a_i^1)\sigma^2}$, $\alpha^\sigma \mathcal{O}_k = P_1^{a_1} P_2^{a_2} \mathcal{A}^{\sigma(1-\sigma)}$ et $\alpha^{\sigma^2} \mathcal{O}_k = P_1^{a_1} P_2^{a_2} \mathcal{A}^{\sigma^2(1-\sigma)}$. Ainsi,

$$\left(\frac{\alpha, \pi_1}{\mathcal{P}_i}\right)_3 \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^\sigma}\right)_3 \left(\frac{\alpha, \pi_1}{\mathcal{P}_i^{\sigma^2}}\right)_3 = \left(\frac{\pi_1}{\mathcal{P}_i}\right)_3^{(a_i^2 - a_i^0) + (a_i^1 - a_i^2) + (a_i^0 - a_i^1)} = 1.$$

D'où $((\alpha, \pi_1)/P_1)_3 = 1$ (ceci par l'égalité (5)). Par la suite $((\alpha, q^{e_2})/P_1)_3 = 1$ car $A = 1$ et puisque $(k/k_0)^* = k(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2})$, alors $k(\sqrt[3]{q^{e_2}})/k$ est non ramifiée. Ainsi $A = (q^{e_2}/P_1)_3^{a_1}$ (propriété (4)). D'une manière analogue on obtient :

$$B := \left(\frac{\varepsilon \pi_1^{a_1} \pi_2^{a_2}, \pi_1 \pi_2 q^{e_2}}{\pi_2}\right)_3 = \left(\frac{\alpha, \pi_1 \pi_2 q^{e_2}}{P_2}\right)_3 = \left(\frac{q^{e_2}}{P_2}\right)_3^{-a_2}.$$

Comme $(q/p)_3 \neq 1$, alors π_1 et π_2 sont inertes dans $k_0(\sqrt[3]{q^e})$. D'où P_1 et P_2 sont inertes dans $k(\sqrt[3]{q^e})$, c'est-à-dire $(q^{e_2}/P_1)_3$ et $(q^{e_2}/P_2)_3$ sont différents de 1 (proposition 3). Or $A = B = 1$ et $e_1, e_2 \in \{1, 2\}$; alors $a_1 = a_2 = 0$; donc $[\mathcal{A}]^{\sigma-1} = 1$. Par la suite, $\mathcal{H}_2(k) \subset \mathcal{H}_1(k)$; d'où $\mathcal{H}(k) = \mathcal{H}_1(k)$. Comme $|\mathcal{H}_1(k)| = 9$, alors $9||h_k$. Par la suite, $3||h_\Gamma$ et $u = 3$ (proposition 7).

Si $3||h_\Gamma$, alors d'après [Is], on a $(q/p)_3 \neq 1$. $\square$

Corollaire 5. *Sous les hypothèses du théorème* 6*, on a :*

(1) $(q/p)_3 \neq 1 \Rightarrow u = 3$.
(2) $(q/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

La démonstration est la même que celle du corollaire 1.

Exemples. (1) Prenons $p = 7$ et $q = 2$ on a $(2/7)_3 \neq 1$ (car $2^{(7-1)/3} = 2^2 \not\equiv 1 \pmod 9$). Alors pour $\Gamma = \mathbf{Q}(\sqrt[3]{7 \cdot 2}) = \mathbf{Q}(\sqrt[3]{14})$ on a $3||h_\Gamma$ et $u = 3$.

(2) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{7 \cdot 11}) = \mathbf{Q}(\sqrt[3]{77})$. On a $7 \cdot 11 \not\equiv \pm 1 \pmod 9$, et $(11/7)_3 \neq 1$ (car $11^{(7-1)/3} = 11^2 \not\equiv 1 \pmod 7$). D'où $3||h_\Gamma$ et $u = 3$.

(3) On considère $p = 13 \equiv 4 \pmod 9$ et $q = 11 \equiv -1 \pmod 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{13 \cdot 11^2}) = \mathbf{Q}(\sqrt[3]{1573})$. On a $13 \cdot 11^2 \not\equiv \pm 1 \pmod 9$ et $(11/13)_3 \neq 1$ (car $11 \equiv -2 \pmod{13}$ et $2^{(13-1)/2} = 2^6 \not\equiv 1 \pmod{13}$). Par la suite $3||h_\Gamma$ et $u = 3$.

9. Cas où $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$ avec $p \equiv 4$ ou $7 \pmod 9$. Ici $e_1, e_2 \in \{1, 2\}$ et sans perte de généralité on peut supposer que $e = 1$. Comme $p \equiv 1 \pmod 3$, alors $p = \pi_1\pi_2$ où π_1 et π_2 sont des premiers de k tels que $\pi_1 = \pi_2^\tau$ et $\pi_1 \equiv \pi_2 \equiv 1 \pmod{3\mathcal{O}_{k_0}}$, puisque $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$, alors les premiers qui se ramifient dans k/k_0 sont $\pi_1\mathcal{O}_k = P_1^3$, $\pi_2\mathcal{O}_k = P_2^3$, $\pi_3\mathcal{O}_k = \mathcal{Q}_1^3$ et $\pi_4\mathcal{O}_k = \mathcal{Q}_2^3$ où $\pi_i = -q_i$ $(i = 3, 4)$. Si on pose $x = \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2}$ on aura $k = k_0(\sqrt[3]{x})$ où $x \equiv 1 \pmod{\lambda^3}$, car $n \equiv \pm 1 \pmod 9$ et $k = k_0(\sqrt[3]{n}) = k_0(\sqrt[3]{-n})$.

Premier cas : $\pi_3 \not\equiv 1 \pmod{\lambda^3}$. On pose $x_1 = \pi_1\pi_2^2$ et $x_2 = \pi_1\pi_3^r$, où $r = 1$ ou 2 est choisi tel que $x_2 \equiv 1 \pmod{\lambda^3}$, on a $x_1 = \pi_1\pi_2^2 \equiv \pi_1^3 \equiv 1 \pmod{\lambda^3}$ et $(k/k_0)^* = k(\sqrt[3]{x_1}, \sqrt[3]{x_2})$ (d'après la proposition 9).

Lemme 1. *Pour toute unité $\varepsilon \in E_{k_0}$, $((\varepsilon, \pi_1)/\pi_1)_3 = ((\varepsilon, \pi_2)/(\pi_2))_3$.*

Preuve. Si $\varepsilon = \pm 1$ on a $((\pm 1, \pi_1)/\pi_1)_3 = ((\pm 1, \pi_2)/\pi_2)_3 = 1$ car 1 et -1 sont normes dans $k_0(\sqrt[3]{\pi_1})/k_0$ et $k_0(\sqrt[3]{\pi_2})/k_0$. Si $\varepsilon = j$ ou j^2, d'après la propriété (6) on a $((\varepsilon, \pi_1)/\pi_1)_3 = ((\tau\varepsilon^2, \tau\pi_2)/\tau\pi_2)_3 = \tau((\varepsilon^2, \pi_2)/\pi_2)_3 = ((\varepsilon^2, \pi_2)/\pi_2)_3^2 = ((\varepsilon, \pi_2)/(\pi_2))_3$. $\square$

Lemme 2. *Nous avons $[\mathcal{Q}_1] = [\mathcal{Q}_2] = 1 \Rightarrow (q_1^{e_1+r} q_2^{e_2}/p)_3 = 1$.*

Preuve. Comme $[\mathcal{Q}_1] = 1$, $\exists\ \varepsilon \in E_{k_0}$, $\exists\ \alpha \in k^*$ tels que $\varepsilon\pi_3 = \mathcal{N}_{k/k_0}(\alpha)$. Cela entraîne que $((\varepsilon\pi_3, \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2})/\pi_1)_3 = ((\varepsilon\pi_3, \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2})/\pi_2)_3 = 1$, de sorte que

$$\left(\frac{\varepsilon, \pi_1}{\pi_1}\right)_3 \left(\frac{\pi_3, \pi_1}{\pi_1}\right)_3 = \left(\frac{\varepsilon, \pi_2}{(\pi_2)}\right)_3 \left(\frac{\pi_3, \pi_2}{\pi_2}\right)_3$$

(d'après les propriétés (1), (2) et (4)). Donc $((\pi_3, \pi_1)/\pi_1)_3 = ((\pi_3, \pi_2)/\pi_2)_3 = \tau((\pi_3, \pi_1)/\pi_1)_3$ (d'après le lemme 1 et la propriété 6). D'où $((\pi_3, \pi_1)/\pi_1)_3 = 1$ car $\pi_3^\tau = \pi_3$ et l'unique racine cubique de 1 fixée par τ est 1. D'une manière analogue, on montre que $[\mathcal{Q}_2] = 1 \Rightarrow ((\pi_4, \pi_1)/\pi_1)_3 = 1$; il suffit de remplacer π_3 par π_4. Ainsi, $((\pi_3^{e_1+r}\pi_4^{e_2}, \pi_1)/\pi_1)_3 = 1$; d'où $(q_1^{e_1+r} q_2^{e_2}/\pi_1)_3 = (q_1^{e_1+r} q_2^{e_2}/\pi_2)_3 = 1$, c'est-à-dire $(q_1^{e_1+r} q_2^{e_2}/p)_3 = 1$ (proposition 5). $\square$

Proposition 11. *Nous avons* $(q_1^{e_1+r}q_2^{e_2}/p)_3 \neq 1 \Rightarrow \mathcal{H}_1(k) = \langle [P_1], [\mathcal{Q}_1], [\mathcal{Q}_2] \rangle$.

Preuve. On a $\pi_3 \not\equiv 1 \pmod{\lambda^3}$. Alors d'après la proposition 4, j n'est pas norme dans k/k_0 ; donc $|\mathcal{H}_1(k)| = 3^2$ (d'après la formule des classes ambiguës). Puisque $P_i^\sigma = P_i$ et $\mathcal{Q}_j^\sigma = \mathcal{Q}_j$ $(i, j \in \{1,2\})$, alors $H = \langle [P_1], [\mathcal{Q}_1], [\mathcal{Q}_2] \rangle \subset \mathcal{H}_1(k)$. Nous montrons que H est d'ordre 9. On a $[P_1] \neq 1$, car sinon $\exists \alpha \in k^*$ tel que $P_1 = \alpha\mathcal{O}_k$, d'où $\pi_1\mathcal{O}_{k_0} = \mathcal{N}_{k/k_0}(\alpha)\mathcal{O}_{k_0}$; par la suite, $\exists \varepsilon \in E_{k_0}$ tel que $\varepsilon\pi_1 = \mathcal{N}_{k/k_0}(\alpha)$. D'où $((\varepsilon\pi_1, x)/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0, en particulier pour $\mathcal{P} = \pi_1\mathcal{O}_{k_0}, \pi_2\mathcal{O}_{k_0}$, et $\pi_3\mathcal{O}_{k_0}$. Si on calcule ce symbole en utilisant ses propriétés on obtient :

$$\begin{aligned}
A &:= \left(\frac{\varepsilon\pi_1, \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2}}{\pi_1}\right)_3 = \left(\frac{\varepsilon, \pi_1}{\pi_1}\right)_3 \left(\frac{\pi_1, \pi_3^{e_1}\pi_4^{e_2}}{\pi_1}\right)_3 = 1.\\
B &:= \left(\frac{\varepsilon\pi_1, \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2}}{\pi_2}\right)_3 = \left(\frac{\varepsilon, \pi_2}{\pi_2}\right)_3 = 1.\\
C &:= \left(\frac{\varepsilon\pi_1, \pi_1\pi_2\pi_3^{e_1}\pi_4^{e_2}}{\pi_3}\right)_3 = \left(\frac{\varepsilon, \pi_3^{e_1}}{\pi_3}\right)_3 \left(\frac{\pi_1, \pi_3^{e_1}}{\pi_3}\right)_3 = 1.
\end{aligned}$$

Puisque $B = ((\varepsilon, \pi_2)/\pi_2)_3 = 1$, alors $\varepsilon = \pm 1$, car sinon $\varepsilon \in \{\pm j, \pm j^2\}$; alors

$$B = \left(\frac{\varepsilon}{\pi_2}\right)_3 = \frac{\left(\frac{k_0(\sqrt[3]{\varepsilon})}{\pi_2}\right)\sqrt[3]{\varepsilon}}{\sqrt[3]{\varepsilon}} = \varepsilon^{(p-1)/3} \neq 1,$$

car $p \not\equiv 1 \pmod 9$, ce qui est absurde. Ainsi $((\pi_1, \pi_3^{e_1}\pi_4^{e_2})/\pi_1)_3 = 1$ et $((\pi_1, \pi_3^{e_1})/\pi_3)_3 = 1$. D'autre part, on a par la formule produit

$$\left(\frac{\pi_1, \pi_3}{\pi_1}\right)_3 \left(\frac{\pi_1, \pi_3}{\pi_3}\right)_3 \left(\frac{\pi_1, \pi_3}{\lambda}\right)_3 = 1.$$

Comme $\pi_1\pi_3^r \equiv 1 \pmod{\lambda^3}$, alors λ est non ramifié dans $k_0(\sqrt[3]{\pi_1\pi_3^r})$ (proposition 3) ; donc $((\pi_1, \pi_3^r)/\lambda)_3 = ((\pi_1, \pi_1\pi_3^r)/\lambda)_3 = (\pi_1\pi_3^r/\lambda)_3^0 = 1$; par la suite $((\pi_1, \pi_3)/\lambda)_3 = 1$, car $r \in \{1,2\}$, d'où $((\pi_1, \pi_3)/\pi_3)_3^2 = ((\pi_1, \pi_3)/\pi_1)_3 = ((\pi_1, \pi_4)/\pi_1)_3 = 1$, car $e_2 \in \{1,2\}$ et $A = B = 1$. Ainsi $((\pi_1, \pi_3^{e_1+r}\pi_4^{e_2})/\pi_1)_3 = 1$, par la suite $(q_1^{e_1+r}q_2^{e_2}/p)_3 = 1$ ce qui est absurde. D'où $[P_1] \neq 1$.

On suppose que $[\mathcal{Q}_1] \neq 1$; sinon on prend $[\mathcal{Q}_2] \neq 1$ (d'après le lemme 2) ; on a $[P_1^a\mathcal{Q}_1] \neq 1$ pour $a \in \{1,2\}$, sinon $\exists\ \alpha \in \mathcal{O}_k$ tel que $P_1^a\mathcal{Q}_1 = \alpha\mathcal{O}_k$ et comme $k((\pi_3^{e_1+r}\pi_4^{e_2})^{1/3})/k$ est non ramifiée car $k(\pi_3^{e_1+r}\pi_4^{e_2})^{1/3} = k\left(\sqrt[3]{x_1x_2}\right)$, alors $((\alpha, \pi_3^{e_1+r}\pi_4^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier de k et différent de P_1 et P_2. Par la suite d'après la formule produit on a

$$\left(\frac{\alpha, \pi_3^{e_1+r}\pi_4^{e_2}}{P_1}\right)_3 \left(\frac{\alpha, \pi_3^{e_1+r}\pi_4^{e_2}}{\mathcal{Q}_1}\right)_3 = 1.$$

On a

$$\tau\left(\frac{(\alpha, \pi_3^{e_1+r}\pi_4^{e_2})}{\mathcal{Q}_1}\right)_3 = \left(\frac{(\alpha^\tau, \pi_3^{e_1+r}\pi_4^{e_2})}{\mathcal{Q}_1}\right)_3 = \left(\frac{\pi_3^{e_1+r}\pi_4^{e_2}}{\mathcal{Q}_1}\right)_3^{-1} = \left(\frac{(\alpha, \pi_3^{e_1+r}\pi_4^{e_2})}{\mathcal{Q}_1}\right)_3.$$

D'où $((\alpha,\pi_3^{e_1+r}\pi_4^{e_2})/\mathcal{Q}_1)_3=1$, car 1 est l'unique racine 3-ième de l'unité fixée par τ. Ainsi $((\alpha,\pi_3^{e_1+r}\pi_4^{e_2})/P_1)_3=(\pi_3^{e_1+r}\pi_4^{e_2}/P_1)_3^{-a}=1$; par la suite $(\pi_3^{e_1+r}\pi_4^{e_2}/P_1)_3=1$, c'est-à-dire P_1 se décompose complètement dans $k(\pi_3^{e_1+r}\pi_4^{e_2})^{1/3}$, ce qui est absurde car $(\pi_3^{e_1+r}\pi_4^{e_2}/p)_3\neq 1$. Donc $(\pi_3^{e_1+r}\pi_4^{e_2}/\pi_1)_3\neq 1$, c'est-à-dire π_1 est inerte dans $k(\pi_3^{e_1+r}\pi_4^{e_2})^{1/3}$ ce qui implique que P_1 est inerte dans $k(\pi_3^{e_1+r}\pi_4^{e_2})^{1/3}$. D'où $[P_1^a\mathcal{Q}_1]\neq 1$ $\forall a\in\{1,2\}$. Par la suite $\langle[P_1]\rangle\cap\langle[\mathcal{Q}_1]\rangle=\{1\}$ et comme $[P_1^3]=[\mathcal{Q}_1^3]=1$, alors $\langle[P_1],[\mathcal{Q}_1]\rangle$ est d'ordre 9. Ainsi $\mathcal{H}_1(k)=\langle[P_1],[\mathcal{Q}_1]\rangle$. Si $[\mathcal{Q}_1]=1$ alors d'après le lemme 2 $[\mathcal{Q}_2]\neq 1$, et on montre de la même façon que $\mathcal{H}_1(k)=\langle[P_1],[\mathcal{Q}_2]\rangle$ (il suffit de remplacer $\mathcal{Q}_1$ par $\mathcal{Q}_2$). $\square$

Proposition 12. $(q_1^{e_1+r}q_2^{e_2}/p)_3\neq 1\Rightarrow 9||h_k$.

Preuve. Comme $(q_1^{e_1+r}q_2^{e_2}/p)_3\neq 1$, alors $(\pi_3/\pi_1)_3\neq 1$ ou $(\pi_4/\pi_1)_3\neq 1$, car si $(\pi_3/\pi_1)_3=(\pi_4/\pi_1)_3=1$, on aurait $(\pi_3^{e_1+r}\pi_4^{e_2}/\pi_1)_3=1$, c'est-à-dire $(q_1^{e_1+r}q_2^{e_2}/p)_3=1$ (proposition 5). Supposons que $(\pi_3/\pi_1)_3=((\pi_3,\pi_1)/\pi_1)_3\neq 1$; d'après la démonstration de la proposition 11 on a $\mathcal{H}_1(k)=\langle[P_1],[\mathcal{Q}_1]\rangle$. Soit $[\mathcal{A}]\in\mathcal{H}_2(k)$, alors $[\mathcal{A}^{\sigma-1}]\in\mathcal{H}_1(k)$, d'où $[\mathcal{A}^{\sigma-1}]=1$ car sinon :

- $[\mathcal{A}^{\sigma-1}]=[P_1]\Rightarrow\exists\ \alpha\in k^*$ tel que $P_1=\alpha\mathcal{A}^{\sigma-1}\Rightarrow\exists\ \varepsilon\in E_{k_0}$ tel que $\varepsilon\pi_1=\mathcal{N}_{k/k_0}(\alpha)\Rightarrow(q_1^{e_1+r}q_2^{e_2}/p)_3=1$ (d'après la démonstration de la proposition 11), ce qui est absurde. Même conclusion si $[\mathcal{A}^{\sigma-1}]=[P_1^2]$.
- $[\mathcal{A}^{\sigma-1}]=[\mathcal{Q}_1]\Rightarrow\exists\ \beta\in k^*$ tel que $\mathcal{Q}_1=\beta\mathcal{A}^{\sigma-1}\Rightarrow\exists\ \varepsilon'\in E_{k_0}$ tel que $\varepsilon'\pi_3=\mathcal{N}_{k/k_0}(\beta)\Rightarrow((\pi_1,\pi_3)/\pi_1)_3=1$ (d'après la démonstration du lemme 2) $\Rightarrow(\pi_3/\pi_1)_3=1$, contradiction. Même conclusion si $[\mathcal{A}^{\sigma-1}]=[\mathcal{Q}_1^2]$.
- $[P_1^a\mathcal{Q}_1]=[\mathcal{A}^{\sigma-1}]$ pour $a\in\{1,2\}\Rightarrow\exists\ \gamma\in k^*$ tel que $P_1^a\mathcal{Q}_1=\gamma\mathcal{A}^{\sigma-1}\Rightarrow\gamma\mathcal{O}_k=P_1^a\mathcal{Q}_1\mathcal{A}^{1-\sigma}$. On pose $y=\pi_3^{e_1+r}\pi_4^{e_2}$ et soit

$$\mathcal{A}=\prod_{i=1}^{g}\mathcal{P}_i^{a_i^0+a_i^1\sigma+a_i^2\sigma^2},$$

la décomposition de $\mathcal{A}$ en idéaux premiers de k. Comme $k\left(\sqrt[3]{y}\right)$ est non ramifiée sur k (car $k\left(\sqrt[3]{y}\right)\subset(k/k_0)^*$ qui est non ramifiée sur k) et $P_i^\sigma=P_i$, $\mathcal{Q}_j^\sigma=\mathcal{Q}_j$ $\forall i,j\in\{1,2\}$, on montre de la même manière que dans le théorème 6 que

$$\left(\frac{\gamma,y}{\mathcal{P}_i}\right)_3\left(\frac{\gamma,y}{\mathcal{P}_i^\sigma}\right)_3\left(\frac{\gamma,y}{\mathcal{P}_i^{\sigma^2}}\right)_3=1$$

(il suffit de remplacer α par γ et π_1 par $\pi_3^{e_1+r}\pi_4^{e_2}$). Si on applique la formule produit sur γ et α dans k on aura :

$$\left(\frac{\gamma,y}{P_1}\right)_3\left(\frac{\gamma,y}{\mathcal{Q}_1}\right)_3=1 \tag{6}$$

car $((\gamma,y)/\mathcal{P})_3\ =(y/\mathcal{P})_3^0=1$ pour tout idéal premier $\mathcal{P}$ de k ne divisant pas γ. On a $\tau((\gamma,y)/\mathcal{Q}_1)_3=((\gamma,y)/\mathcal{Q}_1)_3=((\gamma^\tau,y)/\mathcal{Q}_1)_3=(\pi_3^{e_1+r}\pi_4^{e_2}/\mathcal{Q}_1)_3^{-1}=((\gamma,y)/\mathcal{Q}_1)_3$ (car $k(\sqrt[3]{y})/k$ est non ramifiée). Donc $((\gamma,y)/\mathcal{Q}_1)_3=1$ car l'unique racine 3-ième de l'unité fixée par τ est 1. Enfin $((\gamma,\pi_3^{e_1+r}\pi_4)/P_1)_3=(\pi_3^{e_1+r}\pi_4/P_1)_3^{-a}=1$, (d'après la relation (6) et la propriété (4)), et puisque $a\in\{1,2\}$, alors $(\pi_3^{e_1+r}\pi_4/P_1)_3=1$; par la suite $(\pi_3^{e_1+r}\pi_4/\pi_1)_3 = 1$, c'est-à-dire π_1 se décompose complètement dans $k\left(\sqrt[3]{y}\right)$, contradiction avec le fait que $(q_1^{e_1+r}q_2^{e_2}/p)_3 \neq 1$. On conclut que $[\mathcal{A}^{\sigma-1}] \notin \langle [P_1], [\mathcal{Q}_1]\rangle - \{1\}$; par la suite $[\mathcal{A}^{\sigma-1}] = 1$, c'est-à-dire $[\mathcal{A}] \in \mathcal{H}_1(k)$. D'où $\mathcal{H}_1(k) = \mathcal{H}_2(k) = \mathcal{H}(k)$. Comme $|\mathcal{H}_1(k)| = 9$, alors $9||h_k$. Si au lieu de considérer $(\pi_3/\pi_1)_3 \neq 1$ on suppose que $(\pi_4/\pi_1)_3 \neq 1$, on procède de la même manière pour montrer que $\mathcal{H}_1(k) = \mathcal{H}_2(k)$ (il suffit de remplacer $\mathcal{Q}_1$ par $\mathcal{Q}_2$). $\square$

Second cas : $\pi_3 \equiv 1 \pmod{\lambda^3}$. Dans ce cas on a $\pi_4 = -q_2 \not\equiv 1 \pmod{\lambda^3}$, et si on pose $x_1 = \pi_1\pi_2^2$ et $x_2 = \pi_1\pi_4^r$ où $r = 1$ ou 2 est choisi tel que $x_2 \equiv 1 \pmod{\lambda^3}$, alors $(k/k_0)^* = k\left(\sqrt[3]{x_1}, \sqrt[3]{x_2}\right)$ (Proposition 9).

Proposition 13. *Nous avons* $(q_2^{e_2+r}q_1^{e_1}/p)_3 \neq 1 \Rightarrow 9||h_k$.

Preuve. On reprend la démonstration de la proposition 12 en remplaçant q_1 par q_2 et $\mathcal{Q}_1$ par $\mathcal{Q}_2$. $\square$

Théorème 7. *Soit* p, q_1 *et* q_2 *des nombres premiers tels que* $p \equiv 4$ *ou* $7 \pmod 9$ *et* $-q_1 \equiv -q_2 \equiv 1 \pmod 3$ *et soit* h_Γ *le nombre de classes du corps cubique pur* $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ *où* $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$. *On a :*

(1) *Si* $\pi_3 = -q_1 \not\equiv \pmod{\lambda^3}$ *et si* $r = 1$ *ou* 2 *est choisi tel que* $\pi_1\pi_3^r \equiv 1 \pmod{\lambda^3}$*, alors*
$$(q_1^{e_1+r}q_2^{e_2}/p)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(2) *Si* $\pi_3 = -q_1 \equiv \pmod{\lambda^3}$*, alors* $\pi_4 = -q_2 \not\equiv \pmod{\lambda^3}$ *et si* $r = 1$ *ou* 2 *est choisi tel que* $\pi_1\pi_4^r \equiv 1 \pmod{\lambda^3}$*, alors*
$$(q_2^{e_2+r}q_1^{e_1}/p)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Preuve. L'implication directe découle des propositions 12 et 13, et du fait que $h_k = h_\Gamma^2 \frac{u}{3}$ et l'implication réciproque a été établie par Ismaili dans [Is]. $\square$

Corollaire 6. *Sous les hypothèses du théorème* 7*, on a :*

(1) $(q_1^{e_1+r}q_2^{e_2}/p)_3 \neq 1 \Rightarrow u = 3$ *et* $(q_1^{e_1+r}q_2^{e_2}/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.
(2) $(q_1^{e_1}q_2^{e_2+r}/p)_3 \neq 1 \Rightarrow u = 3$ *et* $(q_1^{e_1}q_2^{e_2+r}/p)_3 = 1 \Leftrightarrow 9|h_\Gamma$.

La preuve est similaire à la démonstration des corollaires précédents.

Exemples. (1) Soit $n = 13 \cdot 2^2 \cdot 5 = 260 \equiv -1 \pmod 9$. Ici 13 est un premier $\equiv 4 \pmod 9$, notons que $13 = (4+3j)(1-3j) = \pi_1\pi_2$ et $\pi_1 \equiv \pi_2 \equiv 7 \pmod{\lambda^3}$. Si $\pi_3 = -q_1 = -2$, on a $\pi_3 \equiv 7 \pmod{\lambda^3}$ et $\pi_1\pi_3^2 \equiv 1 \pmod{\lambda^3}$; dans ce cas $r = 2$. Puisque $(2^4 \cdot 5/13)_3 = (10/13)_3 \neq 1$ car $10 \equiv -3 \pmod{13}$ et $3^{(13-1)/3} = 3^4 \not\equiv 1 \pmod{13}$, alors $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{13 \cdot 2^2 \cdot 5}) = \mathbf{Q}(\sqrt[3]{260})$.

Dans les exemples suivants nous avons $7 = (1+3j)(-2-3j) = \pi_1\pi_2$, où $\pi_1 \equiv \pi_2 \equiv 4 \pmod{\lambda^3}$.

(2) Si on considère $p = 7$, $q_1 = 2$, $q_3 = 11$ et $\pi_3 = -q_1 = -2 \equiv 7 \pmod{\lambda^3}$ ($\pi_3 \not\equiv 1 \pmod{\lambda^3}$), on aura $\pi_1\pi_2 \equiv 28 \equiv 1 \pmod{\lambda^3}$ c'est-à-dire $r = 1$. Comme $2^2 \cdot 11 = 44 \equiv 2 \pmod 7$ et $(2/7)_3 \neq 1$ (car $2^{(7-1)/3} = 2^2 \not\equiv 1 \pmod 7$), alors $(2^2 \cdot 11/7)_3 \neq 1$; par la suite $3||h_\Gamma$ et $u = 3$, où $\Gamma = \mathbf{Q}(\sqrt[3]{7 \cdot 2 \cdot 11}) = \mathbf{Q}(\sqrt[3]{154})$.

(3) Soit $n = 7 \cdot 5 \cdot 17$. Si $\pi_3 = -5$ on a $\pi_3 \equiv 4 \pmod{\lambda^3}$, par la suite $\pi_1\pi_3^2 \equiv 64 \equiv 1 \pmod{\lambda^3}$; dans ce cas, $r = 2$; on a $(5^3 \cdot 17/7)_3 = (17/7)_3$; or $17 \equiv 3 \pmod 7$, et $(3/7)_3 \neq 1$ (car $3^{(7-1)/2} = 3^2 \not\equiv 1 \pmod 7$) ; alors $(17/7)_3 \neq 1$. Par la suite $3||h_\Gamma$ et $u = 3$, où $\Gamma = \mathbf{Q}(\sqrt[3]{n}) = \mathbf{Q}(\sqrt[3]{595})$.

10. Cas où $n = 3^e p^{e_1} q^{e_2}$ **avec** $p \equiv 4$ **ou** $7 \pmod 9$**.** Ici $e, e_2 \in \{1, 2\}$ et nous pouvons supposer, sans perte de généralité, que $e_1 = 1$. Puisque $p \equiv 1 \pmod 3$ alors $p = \pi_1\pi_2$ où π_1 et π_2 sont des premiers de k_0 tels que $\pi_1 = \pi_2^\tau \equiv 1 \pmod{3\mathcal{O}_{k_0}}$. Comme $n = 3^e pq^{e_2} \not\equiv \pm 1 \pmod 9$. Alors les premiers qui se ramifient dans k/k_0 sont $\pi_i\mathcal{O}_k = P_i^3$ $(i = 1, 2), q\mathcal{O}_k = Q^3$ et $\lambda\mathcal{O}_k = I^3$ où $\mathcal{Q}$ est un idéal premier de k, $3\mathcal{O}_{k_0} = \lambda^2\mathcal{O}_{k_0}$ et $\lambda = 1 - j$. On pose $-q = \pi$ et $x = 3^e\pi_1\pi_2\pi^{e_2}$, donc $k = k_0(\sqrt[3]{x})$.

Premier cas : $\pi \not\equiv 1 \pmod{\lambda^3}$. On pose $x_1 = \pi_1\pi_2^2$ et $x_2 = \pi_1\pi^r$ où $r = 1$ ou 2 est choisi tel que $x_2 \equiv 1 \pmod{\lambda^3}$, on a $x_1 \equiv 1 \pmod{\lambda^3}$ et $(k/k_0)^* = k\left(\sqrt[3]{x_1}, \sqrt[3]{x_2}\right)$ (proposition 9). On démontre d'une manière analogue à celle du théorème précédent (en remplaçant q_2 par 3) que :

$$\left(\frac{q^{e_2+r}3^e}{p}\right)_3 \neq 1 \Rightarrow 3||h_\Gamma.$$

Second cas : $\pi \equiv 1 \pmod{\lambda^3}$.

Proposition 14. $(q/p)_3 \neq 1 \Rightarrow \mathcal{H}_1(k) = \langle [P_1], [\mathcal{Q}] \rangle$.

Preuve. On a $|\mathcal{H}_1(k)| = 9$ grâce à la formule des classes ambiguës et comme $P_1^\sigma = P_1$ et $Q^\sigma = Q$, alors $\langle [P_1], [\mathcal{Q}] \rangle \subset \mathcal{H}_1(k)$. Dans la suite nous montrons que $\langle [P_1], [\mathcal{Q}] \rangle$ est d'ordre 9. Pour cela il suffit de montrer $[P_1] \neq 1$, $[\mathcal{Q}] \neq 1$ et $[P_1^a\mathcal{Q}] \neq 1$, où $a \in \{1, 2\}$, car $[P_1^3] = [\mathcal{Q}^3] = 1$.

(i) $[P_1] \neq 1$, sinon $P_1 = \alpha\mathcal{O}_k$; alors $\exists\ \varepsilon \in E_{k_0}$ tel que $\varepsilon\pi_1 = \mathcal{N}_{k/k_0}(\alpha)$; par la suite $((\varepsilon\pi_1, 3^e\pi_1\pi_2q^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0, en particulier pour $\mathcal{P} = q\mathcal{O}_{k_0}$. En utilisant les proprités (1), (2), et (3) on obtient :

$$A = \left(\frac{\varepsilon\pi_1, 3^e\pi_1\pi_2q^{e_2}}{q}\right)_3 = \left(\frac{\varepsilon, q^{e_2}}{q}\right)_3 \left(\frac{\pi_1, q^{e_2}}{q}\right)_3 = 1.$$

Comme $-q \equiv 1 \pmod{\lambda^3}$, alors λ est non ramifié dans $k_0(\sqrt[3]{q})$. Par la suite $((\varepsilon, q)/\lambda)_3 = (q/\lambda)_3^0 = 1$ (propriété (4)) et d'après la formule produit on a $((\varepsilon, q)/\lambda)_3((\varepsilon, q)/q)_3 = 1$, d'où $((\varepsilon, q)/q)_3 = 1$. Ainsi $A = (\pi_1/q)_3^{e_2} = (q/\pi_1)_3^{e_2} = 1$, car les conducteurs de $k_0(\sqrt[3]{\pi_1})$ et $k_0(\sqrt[3]{q})$ sont premiers entre eux (propriété (9)) ; par la suite $(q/p)_3 = 1$, ce qui est absurde. D'où $[P_1] \neq 1$ et $[P_1^2] \neq 1$.

(ii) $[\mathcal{Q}] \neq 1$ sinon. Soit $\alpha \in k^*$ tel que $\mathcal{Q} = \alpha\mathcal{O}_k$. Alors $\varepsilon q = \mathcal{N}_{k/k_0}(\alpha)$ avec $\varepsilon \in E_{k_0}$, donc $((\varepsilon q, 3^e\pi_1\pi_2q^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0. En particulier pour $\mathcal{P} = \pi_1\mathcal{O}_{k_0}$ et $\mathcal{P} = \pi_2\mathcal{O}_{k_0}$ on a

$$B := \left(\frac{\varepsilon q, 3^e\pi_1\pi_2q^{e_2}}{\pi_1}\right)_3 = \left(\frac{\varepsilon, \pi_1}{\pi_1}\right)_3 \left(\frac{q, \pi_1}{\pi_1}\right)_3.$$

$$C := \left(\frac{\varepsilon q, 3^e\pi_1\pi_2q^{e_2}}{\pi_2}\right)_3 = \left(\frac{\varepsilon, \pi_2}{\pi_2}\right)_3 \left(\frac{q, \pi_2}{\pi_2}\right)_3.$$

D'après le lemme 1 et le fait que $B = C = 1$ on a : $((q, \pi_1)/\pi_1)_3 = ((q, \pi_2)/\pi_2)_3 = \tau((q, \pi_1)/\pi_1)_3$ (propriété (6)). Comme 1 est l'unique racine 3-ième de l'unité fixée par τ, alors $((q, \pi_1)/\pi_1)_3 = 1$. Donc $(q/\pi_1)_3 = 1$, c'est-à-dire $(q/p)_3 = 1$, ce qui est absurde car $(q/p)_3 \neq 1$, par la suite $[\mathcal{Q}] \neq 1$ et $[\mathcal{Q}^2] \neq 1$.

(iii) Montrons $[P_1^a \mathcal{Q}] \neq 1$ $\forall a \in \{1, 2\}$. Sinon $P_1^a \mathcal{Q} = \alpha \mathcal{O}_k$, où $\alpha \in k^*$; alors $\exists\, \varepsilon \in E_{k_0}$ tel que $\varepsilon \pi_1^a q = \mathcal{N}_{k/k_0}(\alpha)$; d'où $((\varepsilon \pi_1^a q, 3^e \pi_1 \pi_2 q^{e_2})/\mathcal{P})_3 = 1$ pour tout idéal premier $\mathcal{P}$ de k_0, en particulier pour $\mathcal{P} = q\mathcal{O}_{k_0}$. D'après les propriétés (1), (2) et (4) on a :

$$D := \left(\frac{\varepsilon \pi_1 q, 3^e \pi_1 \pi_2 q^{e_2}}{q}\right)_3 = \left(\frac{\varepsilon, q^{e_2}}{q}\right)_3 \left(\frac{\pi_1^a, q^{e_2}}{q}\right)_3 \left(\frac{q, 3^e \pi_1 \pi_2}{q}\right)_3 = 1.$$

D'après (i) on a $((\varepsilon, q^{e_2})/q)_3 = 1$ et comme $\tau((q, 3^e \pi_1 \pi_2)/q)_3 = ((q, 3^e \pi_1 \pi_2)/q)_3$, alors $D = ((\pi_1^a, q)/q)_3 = (\pi_1/q)_3^a = (q/\pi_1)_3^a = 1$. Or $(q/\pi_1)_3^a \neq 1$; d'où $[P_1^a \mathcal{Q}] \neq 1$. Puisque $[P_1^3] = [\mathcal{Q}^3] = 1$ et d'après (i), (ii), (iii) on a que $\langle [P_1], [\mathcal{Q}] \rangle$ est d'ordre 9. Ainsi, $\mathcal{H}_1(k) = \langle [P_1], [\mathcal{Q}] \rangle$. □

Théorème 8. *Soit p et q des premiers tels que $p \equiv 4$ ou $7 \pmod 9$ et $-q \equiv 1 \pmod 3$ et soit h_Γ le nombre de classes du corps cubique pur $\Gamma = \mathbf{Q}(\sqrt[3]{n})$, où $n = 3^e p^{e_1} q^{e_2}$ et $e, e_1, e_2 \in \{1, 2\}$.*

(1) *Si $\pi = -q \not\equiv 1 \pmod{\lambda^3}$ et si $r = 1$ ou 2 est tel que $\pi_1 \pi^r \equiv 1 \pmod{\lambda^3}$, alors*

$$\left(\frac{3^e q^{e_2 + r}}{p}\right)_3 \neq 1 \Leftrightarrow 3 || h_\Gamma.$$

(2) *Si $\pi = -q \equiv 1 \pmod{\lambda^3}$, alors*

$$(q/p)_3 \neq 1 \Leftrightarrow 3 || h_\Gamma.$$

Preuve. (1) La démonstration de l'implication directe est analogue à celle du théorème précédent. L'implication réciproque est déjà démontrée par Ismaili dans [Is].

(2) Supposons que $(q/p)_3 \neq 1$; alors d'après la proposition 14 on a $\mathcal{H}_1(k) = \langle [P_1], [\mathcal{Q}] \rangle$. Or $[\mathcal{A}] \in \mathcal{H}_2(k) \Rightarrow [\mathcal{A}^{\sigma - 1}] \in \mathcal{H}_1(k) \Rightarrow [\mathcal{A}^{\sigma - 1}] = [P_1^a \mathcal{Q}^b]$, où $a, b \in \{0, 1, 2\} \Rightarrow \exists\, \alpha \in k^*$ et $\varepsilon \in E_{k_0}$ tels que $\varepsilon \pi_1^a q^b = \mathcal{N}_{k/k_0}(\alpha) \Rightarrow a = b = 0$ (d'après la démonstration de la proposition 14) $\Rightarrow [\mathcal{A}] \in \mathcal{H}_1(k) \Rightarrow \mathcal{H}_2(k) = \mathcal{H}_1(k) = \mathcal{H}(k) \Rightarrow 9 || h_k \Rightarrow (3 || h_\Gamma$ et $u = 3)$. L'application réciproque a été établie par Ismaili dans [Is]. □

Corollaire 7. *Sous les hypothèses du théorème 8, on a :*

(1) $(3^e q^{e_2 + r}/p)_3 \neq 1 \Rightarrow u = 3$ *et* $(3^e q^{e_2 + r}/p)_3 = 1 \Leftrightarrow 9 | h_\Gamma$.
(2) $(q/p)_3 \neq 1 \Rightarrow u = 3$ *et* $(q/p)_3 = 1 \Leftrightarrow 9 | h_\Gamma$.

La preuve est similaire à celle des corollaires précédents.

Exemples. Rappelons que $7 = (1 + 3j)(-2 - 3j) = \pi_1 \pi_2$, où $\pi_1 \equiv \pi_2 \equiv 4 \pmod{\lambda^3}$.

(1) Si on considère $p = 7$, $q = 2$ et $\pi = -q \equiv 7 \pmod{\lambda^3}$ on aura $\pi \not\equiv 1 \pmod{\lambda^3}$ et $\pi_1 \pi \equiv 1 \pmod{\lambda^3}$, c'est-à-dire $r = 1$. Comme $2^2 \cdot 3 = 12 \equiv 5 \pmod 7$ et

$5^{(7-1)/3} = 5^2 \not\equiv 1 \pmod 7$, alors $(2^2 \cdot 3/7)_3 \neq 1$; par la suite d'après (1) du théorème 8 on a $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{3 \cdot 7 \cdot 2}) = \mathbf{Q}(\sqrt[3]{42})$.

(2) Soit $n = 3 \cdot 7 \cdot 5 = 105$; dans ce cas $p = 7$, $q = 5$ et $\pi = -5 \equiv 4 \pmod{\lambda^3}$; comme $\pi_1\pi^2 \equiv 1 \pmod{\lambda^3}$, alors $r = 2$. Puisque $(3 \cdot 5^3/7)_3 = (3/7)_3 \neq 1$, (car $3^2 \not\equiv 1 \pmod 7$), alors d'après (1) du théorème 8, $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{105})$.

(3) Soit $\Gamma = \mathbf{Q}(\sqrt[3]{3 \cdot 7 \cdot 17}) = \mathbf{Q}(\sqrt[3]{357})$. Si $\pi = -17$ on aura $\pi \equiv 1 \pmod{\lambda^3}$; comme $17 \equiv 3 \pmod 7$ et $(3/7)_3 \neq 1$, (car $3^2 \not\equiv 1 \pmod 7$), alors d'après (2) du théorème 8, $3||h_\Gamma$ et $u = 3$.

(4) Si on considère $p = 13$ et $q = 71$ on aura $p \equiv 4 \pmod 9$ et $\pi = -q \equiv 1 \pmod{\lambda^3}$. Puisque $71 \equiv 6 \pmod{13}$ et $(6/13)_3 \neq 1$, (car $6^{(13-1)/3} = 6^4 \not\equiv 1 \pmod{13}$) alors $(71/13)_3 \neq 1$. D'où, d'après (2) du théorème 8, $3||h_\Gamma$ et $u = 3$ pour $\Gamma = \mathbf{Q}(\sqrt[3]{3 \cdot 13 \cdot 71}) = \mathbf{Q}(\sqrt[3]{2769})$.

English extended abstract. Let $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ be a pure cubic field, where n is a cube-free positive integer, $k = \mathbf{Q}(\sqrt[3]{n}, j)$ is the normal closure of Γ with $j = e^{2i\pi/3}$, E_k is the unit group of k, u is the index of the units generated by the intermediate fields of $k/\mathbf{Q}$ in the unit group E_k, h_Γ is the class number of Γ and $\mathcal{H}(k)$ is the 3-class group of k. Ismaili [Is] proved that the 3-class group $\mathcal{H}(k)$ of the normal closure k of Γ is of type $(3,3)$, *i.e.*, is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if and only if 3 divides exactly h_Γ and $u = 3$. He also gave all the possible forms of the integer n when $\mathcal{H}(k)$ is of type $(3,3)$ by considering three possible types for the field k: types I, II, III. The fields k of type III are characterized by the fact that the relative genus field $(k/k_0)^*$ of k over $k_0 = \mathbf{Q}(j)$ coincides with the Hilbert 3-class field of k and by the property that the integer n is divisible by a prime $p \equiv 1 \pmod 3$.

In this paper, we concentrate on fields k of type III, and we give necessary and sufficient conditions, involving cubic residue symbols modulo the prime $p \equiv 1 \pmod 3$ dividing the integer n defining Γ, under which the class number of $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ is exactly divisible by 3. This led us to establish a criterion giving the divisibility of the class number by exactly 3 or by 9 for many families of pure cubic fields for which the unit index u is 3. In general, the unit index u is difficult to evaluate. Our results are supported by those of Barrucand and Cohn, who showed in [B-C1] that $u = 3$ when $n = 14, 38, 42$.

Our results are summarized in the following theorem and corollary. For $c \in \mathbb{Z}$, the symbol $(c/p)_3 = 1$ means that c is a cubic residue modulo p, *i.e.*, the congruence $X^3 \equiv c \pmod p$ has a solution in $\mathbb{Z}$. We write $3||h_\Gamma$ to mean h_Γ is exactly divisible by 3: $3 \mid h_\Gamma$ and $3^2 \nmid h_\Gamma$. Moreover, $\mathcal{O}_{k_0}$ is the ring of integers of $k_0 = \mathbf{Q}(j)$ and $\lambda = 1 - j$. Let us mention that the sufficient side of the equivalence characterizing the exact divisibility of h_Γ by 3 has been proved by Ismaili [Is].

Theorem. *Let $\Gamma = \mathbf{Q}(\sqrt[3]{n})$ be a pure cubic field, where n is a cube-free positive integer. Let p, q, q_1 and q_2 be prime numbers such that $p \equiv -q \equiv -q_1 \equiv -q_2 \equiv 1 \pmod 3$.*

(1) If $n = 3^e p^{e_1}$ with $p \equiv 1 \pmod 9$ and $e, e_1 \in \{1,2\}$, then

$$\left(\frac{3}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(2) If $n = p^e q^{e_1}$ *with* $p \equiv -q \equiv 1 \pmod 9$ *and* $e, e_1 \in \{1,2\}$, *then*

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(3) Let $n = p^e q_1^{e_1} q_2^{e_2} \equiv \pm 1 \pmod 9$ *with* p *or* $-q_1$ *or* $-q_2 \equiv 4$ *or* $7 \pmod 9$ *and with* $e, e_1, e_2 \in \{1,2\}$.

(i) *If* $p \equiv 1 \pmod 9$, *then*

$$\left(\frac{q^{e_1} q^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(ii) *Let* $p \not\equiv 1 \pmod 9$ *and let* $p = \pi_1\pi_2$, $\pi_3 = -q_1$ *and* $\pi_4 = -q_2$, *where the* π_i*'s are primes of* k_0 *congruent to* $1 \pmod{3\mathcal{O}_{k_0}}$.

(a) If $\pi_3 \not\equiv 1 \pmod{\lambda^3}$ *and* $r \in \{1,2\}$ *is chosen so that* $\pi_1\pi_3^r \equiv 1 \pmod{\lambda^3}$, *then*

$$\left(\frac{q_1^{e_1+r} q_2^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(b) If $\pi_3 \equiv 1 \pmod{\lambda^3}$ *and* $r \in \{1,2\}$ *is chosen so that* $\pi_1\pi_4^r \equiv 1 \pmod{\lambda^3}$, *then*

$$\left(\frac{q_1^{e_1} q_2^{e_2+r}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(4) Let $n = 3^e p^{e_1} q^{e_2} \not\equiv \pm 1 \pmod 9$ *with* p *or* $-q \equiv 4$ *or* $7 \pmod 9$ *and with* $e \in \{0,1,2\}$ *and* $e_1, e_2 \in \{1,2\}$.

(i) *If* $p \equiv 1 \pmod 9$, *then*

$$\left(\frac{3^e q^{e_2}}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(ii) *Let* $p \not\equiv 1 \pmod 9$.

(a) If $e = 0$, *then*

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(b) If $e \neq 0$, $\pi = -q \not\equiv 1 \pmod{\lambda^3}$ *and* $r \in \{1,2\}$ *is chosen so that* $\pi_1\pi^r \equiv 1 \pmod{\lambda^3}$, *then*

$$\left(\frac{q^{e_2+r} 3^e}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

(c) If $e \neq 0$ *and* $\pi = -q \equiv 1 \pmod{\lambda^3}$, *then*

$$\left(\frac{q}{p}\right)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Corollary. *Assume the same hypotheses as thoses of the last theorem. Define* c *to be the natural number appearing in each equivalence*

$$(c/p)_3 \neq 1 \Leftrightarrow 3||h_\Gamma.$$

Then

$$(c/p)_3 \neq 1 \Rightarrow u = 3.$$

Moreover

$$(c/p)_3 = 1 \Leftrightarrow 9|h_\Gamma.$$

Some numerical examples are provided for each case considered in the last theorem.

BIBLIOGRAPHIE

[B-C1] P. Barrucand and H. Cohn, *Remarks on principal factors in a relative cubic field*, J. Number Theory **3** (1971), 226–239.

[B-C2] P. Barrucand and H. Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*, J. Number Theory. **2** (1970), 7–21.

[B-W-Z] B. D. Beach, H. C. Williams and C. R. Zarnke, *Some computer results on units in quadratic and cubic fields*, Proceedings of the Twenty-Fifth Summer Meeting of the Canadian Mathematical Congress (Lakehead Univ, Thunder Bay, Ont.) (1971), 609–648.

[De] R. Dedekind, *Über die anzahl der idealklassen in reinen kubischen zahlkörpern*, J. für reine und angewandte Mathematik Bd. **121** (1900), 40–123.

[Ge] F. Gerth III, *On* 3*-class groups of cyclic cubic extensions of certain number fields*, J. Number Theory **8** (1976); no. 1, 84–98.

[Gr] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier (Grenoble) **23**; no. 3 (1973).

[Ha] H. Hasse, *Newe begründung und verallgemeinerung der theorie der normenrest Symbols*, J. für reine und angewandte Mathematik Bd. **162** (1930), 134–143.

[He] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981.

[Ho] T. Honda, *Pure cubic fields whose class numbers are multiples of three*, J. Number Theory **3** (1971), 7–12.

[I-R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1982.

[Is] M. C. Ismaili, *Sur la capitulation des* 3*-classes d'idéaux de la clôture normale d'un corps cubique pur*, Thèse de doctorat, Univ. Laval, Québec (1992).

M. C. ISMAILI ET R. EL MESAOUDI
DÉPARTEMENT DE MATHÉMATIQUES
FACULTÉ DES SCIENCES
UNIVERSITÉ MOHAMMED 1
OUJDA - MAROC