MATHEMATICA, 58 (81), N° 1–2, 2016, pp. 14–23

SUR LE 3-RANG DU GROUPE DE CLASSES DE CERTAINS CORPS QUADRATIQUES RÉELS

ABDELMALEK AZIZI, MOHAMED TALBI, and MOHAMMED TALBI

Abstract. We determine a family of real quadratic fields whose 3-rank of class groups is greater than or equal to 2.

MSC 2010. Primary 11R16, 11R29; secondary 11S15.

Key words. Extension cubique, groupe de classes, ramification et théorie des extensions.

1. INTRODUCTION

Plusieurs mathématiciens ce sont intéressé au 3-rang du groupe de classes d'un corps quadratiques. Ainsi, dans [12, 13], on trouve des exemples de corps quadratiques imaginaires dont le 3-rang du groupe de classes est supérieur à 3, dans [1, 2, 3, 4, 5] les auteurs ont donné des exemples de familles infinies de corps quadratiques imaginaires dont le 3-rang du groupe de classes est supérieur à 3, dans [11], J. Quer a trouvé trois corps quadratiques imaginaires dont le 3-rang du groupe de classes est égal à 6, chacun d'entre eux est associé, par un théorème de Scholz, à un corps quadratique réel de discriminant divisible par 3 dont le 3-rang du groupe de classes est supérieur ou égal à 2, aussi Y. Kishi et M. Miyake ont contribué au sujet dans [8] par une paramétrisation des extensions quadratiques dont le 3-rang du groupe de classes est supérieur ou égal à 1, de même Kishi a caractérisé, dans [7], les extensions quadratiques imaginaires dont le 3-rang du groupe de classes est supérieur ou égal à 2.

De notre part, nous donnons, une caractérisation du 3-rang du groupe de classes d'une famille infinie de corps quadratiques réels dont le discriminant n'est pas divisible par 3, plus précisément, pour $\mathrm{k} = \mathbb{Q}(\sqrt{d_m})$ où $d_m = m^4 + 2m^3 - 5m^2 - 6m - 23$ est un entier positif sans facteur carré dépendant d'un entier positif m, nous donnons une condition nécessaire et suffisante pour que la famille des corps quadratiques soit de 3-rang supérieur ou égal à 2.

Dans tout ce papier nous adoptons, sauf mention contraire, les notations suivantes:

- Pour m un entier, on note
  - $p_m = m^2 + 3m + 3$,
  - $q_m = 2m^3 + 9m^2 + 9m + 27$,
  - $Q(X) = X^3 - 3p_mX - q_m$,
  - $d_m = m^4 + 2m^3 - 5m^2 - 6m - 23$ de sorte qu'il soit un entier positif sans facteur carré,
  - $\mathrm{k} = \mathbb{Q}(\sqrt{d_m})$.

- Pour d un entier positif sans facteur carré et $F=\mathbb{Q}(\sqrt{d})$, on note par $\widetilde{F}$ le dual de F (i.e., $\widetilde{F}=\mathbb{Q}(\sqrt{-3d})$ si $3\nmid d$ et $\widetilde{F}=\mathbb{Q}\left(\sqrt{-\frac{d}{3}}\right)$ sinon).

2. RAMIFICATION DANS CERTAINES EXTENSIONS

LEMME 2.1. *Soient d un entier sans facteur carré, $F=\mathbb{Q}(\sqrt{d})$ et α un entier algébrique de F, tel que $N_{F/\mathbb{Q}}(\alpha)=c^3$ où $c\in\mathbb{Z}$. Alors, le polynôme*

$$f(X)=X^3-3cX-tr_{F/\mathbb{Q}}(\alpha)$$

est irréductible si et seulement si α n'est pas un cube dans F.

Preuve. Voir [6]. □

PROPOSITION 2.2. *Soient q un nombre premier, $g(X)=X^3-aX-b$, où a et b deux entiers rationnels, un polynôme irréductible sur $\mathbb{Q}$ avec $v_q(a)<2$ ou $v_q(b)<3$. Soit θ une racine de $g(X)$ et $K=\mathbb{Q}(\theta)$, alors*

(1) *si $q\neq 3$, donc q est totalement ramifié dans $K/\mathbb{Q}$ si et seulement si $1\leq v_q(b)\leq v_q(a)$;*
(2) *3 est totalement ramifié dans $K/\mathbb{Q}$ si et seulement si l'une des conditions suivantes est vérifiée:*
   - $1\leq v_3(b)\leq v_3(a)$.
   - $3\mid a$, $a\not\equiv 3 \bmod 9$, $3\nmid b$, $b^2\not\equiv a+1 \bmod 9$.
   - $a\equiv 3 \bmod 9$, $3\nmid b$, $b^2\not\equiv a+1 \bmod 27$.

Preuve. Voir [8]. □

REMARQUE 2.3. Avec les notations de la proposition 2.2, soit p un nombre premier, $\mathcal{P}$ un diviseur premier de p dans $\mathbb{Q}(\sqrt{4a^3-27b^2})$, alors, $\mathcal{P}$ se ramifie dans le corps de décomposition de $g(X)$ si et seulement si p se ramifie totalement dans K.

THÉORÈME 2.4. *Soient d un entier positif sans facteur carré, $F=\mathbb{Q}(\sqrt{d})$, $\widetilde{F}$ le dual de F, $\alpha=\frac{e+f\sqrt{d}}{2}$ un entier algébrique de F, p un nombre premier et $\mathcal{P}_p$ un diviseur premier de p dans $\widetilde{F}$ tels que α n'est pas un cube dans F et $N_{F/\mathbb{Q}}(\alpha)=c^3$, où $c\in\mathbb{Z}$ et soit L le corps de décomposition de $P_\alpha(X)=X^3-3cX-e$, alors:*

(1) *Si $p\neq 3$, alors $\mathcal{P}_p$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si on a l'une des assertions:*
   - *$v_p(pgcd\ (e,c))=0$ avec $[p\nmid d$ et $p\neq 2]$ ou $[p=2$ et $d\equiv 1 \bmod 4]$,*
   - *$v_p(pgcd\ (e,c))\leq 1$ avec $[p|d$ et $p\neq 2]$ ou $[p=2$ et $d\equiv 2,3 \bmod 4]$.*
(2) *Si $p=3$, alors on a:*
   - *si $3|d$, $\mathcal{P}_3$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_3(pgcd\ (e,c))\leq 1$, $v_3(e)\neq 2$ et $v_3(f)\geq 1$;*

- *si* $3 \nmid d$ *,* $\mathcal{P}_3$ *ne se ramifie pas dans* $L/\widetilde{F}$ *si et seulement si* $v_3(e) = 2$ *et* $e^2 - 3d - 4 \equiv f \equiv 0 \bmod 9$.

Preuve. Pour q un nombre premier, on peut toujours supposer que $v_q(3c) < 2$ ou $v_q(e) < 3$, car sinon on applique la proposition 2.2 à $\frac{1}{q^3}P_\alpha(qX)$.

(1) Soit p un nombre premier impair distinct de 3, tel que $p \nmid d$, d'après la proposition 2.2, $\mathcal{P}_p$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_p(pgcd\ (e,c)) = 0$ ou $1 \leq v_p(c) < v_p(e)$. D'autre part, les conditions $1 \leq v_p(c) < v_p(e)$ et ($v_p(c) < 2$ ou $v_p(e) < 3$) entraînent que $1 \leq v_p(c) \leq 1$ d'où $v_p(c) = 1$, donc de l'équation diophantienne $e^2 = df^2 + 4c^3$, on déduit que $2v_p(e) \leq 3$, donc $v_p(e) \leq 1$, ce qui élimine la condition $1 \leq v_p(c) < v_p(e)$. Par suite, $\mathcal{P}_p$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $v_p(pgcd\ (e,c)) = 0$.

Si $p = 2$ et $d \equiv 1 \bmod 4$, alors la proposition 2.2 entraîne que $\mathcal{P}_2$ ne se ramifie pas dans L si et seulement si $v_2(pgcd\ (e,c)) = 0$ ou $1 \leq v_2(c) < v_2(e)$. On suppose que $1 \leq v_2(c) < v_2(e)$. Comme $v_2(c) < 2$ ou $v_2(e) < 3$ alors $v_2(e) = v_2(f) \geq 2$ et $v_2(c) = 1$, puisque $d \equiv 1 \bmod 4$, et $e^2 = df^2 + 4c^3$, on déduit que $\frac{e}{4}$ et $\frac{f}{4}$ ont même parité, et par suite $v_2(e^2 - df^2) \geq 6$, ce qui contredit le fait que $v_2(e^2 - df^2) = v_2(4c^3) = 5$. Par conséquent $\mathcal{P}_2$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_p(pgcd\ (e,c)) = 0$.

On suppose que $p|d$ (p impair différent de 3), comme d est sans facteur carré on déduit facilement que:

Si $v_p(c) = 1$, alors $v_p(e^2) \geq 3$, donc $v_p(e) \geq 2$, et par suite $\mathcal{P}_p$ ne se ramifie pas dans $L/\widetilde{F}$.

Si $v_p(c) \geq 2$, alors $v_p(e) \geq 3$, car sinon en comparant les p-valuations dans l'équation $e^2 = df^2 + 4c^3$, on obtient $4 = 5$, ce qui contredit la condition ($v_p(3c) < 2$ ou $v_p(e) < 3$) donc $v_p(c) < 2$. En vertu de la proposition 2.2, $\mathcal{P}_p$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_p(pgcd\ (e,c)) \leq 1$.

On suppose que $p = 2$ et $d \equiv 2$ ou $3 \bmod 4$. Alors, si $v_2(c) = 1$, comme $e^2 = df^2 + 4c^3$ et $d \equiv 2$ ou $3 \bmod 4$, alors $v_2(e) \geq 2$, d'où $\mathcal{P}_2$ ne se ramifie pas dans $L/\widetilde{F}$.

Si $v_2(c) \geq 2$ alors $v_2(e) \leq 2$, et par suite $\mathcal{P}_2$ ne se ramifie pas dans $L/\widetilde{F}$. Donc, d'après la proposition 2.2, $\mathcal{P}_2$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_2(pgcd\ (e,c)) \leq 1$.

(2) Si $p = 3$, on distingue deux cas, suivant que 3 divise d ou non:

(I) Cas où $3|d$: si $v_3(c) = 0$, alors $3 \nmid e$, et par suite

$$c \equiv 4c^3 \equiv e^2 - df^2 \equiv 1 \bmod 3,$$

donc $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $e^2 - (3c+1) \equiv 0 \bmod 27$, d'autre part, de l'équation $e^2 = df^2 + 4c^3$ et $c \equiv 1 \bmod 3$, on déduit que

$$e^2 - (3c+1) = df^2 + 3c(c^2-1) + c^3 - 1 \equiv df^2 \bmod 27.$$

Comme d est sans facteur carré, alors $v_3(d) = 1$, et on a

$$v_3(df^2) \geq 3 \Leftrightarrow 2v_3(f) + 1 \geq 3 \Leftrightarrow v_3(f) \geq 1.$$

Par conséquent, $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $v_3(f) \geq 1$. Si $v_3(c) = 1$, alors $v_3(f) = 1$ et $v_3(e) \geq 2$.

Si $v_3(e) = 2$ alors, d'après la proposition 2.2, $\mathcal{P}_3$ se ramifie dans $L/\widetilde{F}$.

Si $v_3(e) \geq 3$, on applique la proposition 2.2 à $hP_\alpha(X) = P_\alpha(h^{-1}(X))$ où $h(z) = \frac{z}{27}$, on déduit que, $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$.

Si $v_3(c) \geq 2$ alors $v_3(e) \geq 3$, ce qui contredit l'hypothèse $v_3(e) < 3$. Donc, $\mathcal{P}_3$ ne se ramifie pas dans $L/\widetilde{F}$ si et seulement si $v_3(pgcd\ (e, c)) \leq 1$, $v_3(e) \neq 2$ et $v_3(f) \geq 1$.

(II) Cas où $3 \nmid d$: si $v_3(c) = 0$ et $v_3(e) = 0$, alors

$$c \equiv 1 \bmod 3 \Rightarrow e^2 - (3c + 1) \equiv df^2 \bmod 27.$$

Puisque $v_3(d) = 0$, on conclut d'après la proposition 2.2 que $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $v_3(f) \geq 2$.

Aussi, on a

$$c \equiv 2 \bmod 3 \Rightarrow d \equiv 2 \bmod 3 \Rightarrow e^2 - 3d - 4 \equiv e^2 - (3c + 1) \bmod 27,$$

ce qui montre l'équivalence dans ce cas.

Si $v_3(c) = 0$ et $v_3(e) \geq 1$, alors $\mathcal{P}_3$ se ramifie dans $L/\widetilde{F}$ si et seulement si $v_3(e) = 1$.

Si $v_3(c) = 1$ et $v_3(e) = 0$. On obtient facilement, en utilisant $e^2 = df^2 + 4c^3$ et la proposition 2.2, que $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $e^2 \equiv 1 \bmod 9$. Comme $d \equiv 1 \bmod 3$, on déduit que $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $v_3(e^2 - 3d - 4) \geq 2$.

Si $v_3(c) = 1$ et $v_3(e) = 1$, $\mathcal{P}_3$ est ramifié dans $L/\widetilde{F}$.
Si $v_3(c) \geq 2$ et $v_3(e) = 0$, alors $\mathcal{P}_3$ est non ramifié dans $L/\widetilde{F}$ si et seulement si $v_3(e^2 - 3d - 4) \geq 2$.

Si $v_3(c) \geq 2$ et $v_3(e) \geq 1$, alors, d'après la proposition 2.2, $L/\widetilde{F}$ est ramifié pour les diviseurs de 3.

Donc, $L/\widetilde{F}$ est non ramifiée pour les diviseurs de 3 si et seulement si

$$e^2 - 3d - 4 \equiv f \equiv 0 \bmod 9 \text{ et } v_3(e) = 2.$$

□

Lemme 2.5. *Soient m un entier positif tel que $m \equiv 1 \bmod 7$, $p_m = m^2 + 3m + 3$ et $q_m = 2m^3 + 9m^2 + 9m + 27$. On suppose que $\dfrac{4p_m^3 - q_m^2}{27}$ est sans facteur carré, alors, $Q(X) = X^3 - 3p_mX - q_m$ est irréductible sur $\mathbb{Q}$.*

Preuve. On a $d_m = (m^2 + m - 3)^2 - 32$, il est clair que $3 \nmid d_m$ et que $d_m \equiv 1 \bmod 4$, aussi, on a $27d_m = 4p_m^3 - q_m^2$, ce qui est équivalent à dire que $27d_m + q_m^2 = 4p_m^3$, c'est à dire que $q_m^2 - 3^2(-3d_m) = 4p_m^3$, donc

$$N_{\widetilde{\mathrm{k}}/\mathbb{Q}}(\alpha) = p_m^3 \text{ où } \alpha = \frac{q_m + 3\sqrt{-3d_m}}{2}.$$

α n'est pas cube dans $\widetilde{\mathrm{k}}$, car sinon, il existe $\beta = \frac{k+l\sqrt{-3d_m}}{2} \in O_{\widetilde{\mathrm{k}}}$, l'anneau des entiers de $\widetilde{\mathrm{k}}$ $(k, l \in \mathbb{Z})$, tel que $\alpha = \beta^3$, ainsi

$$\begin{cases} \alpha = \beta^3 \\ \\ N_{\widetilde{\mathrm{k}}/\mathbb{Q}}(\alpha) = (N_{\widetilde{\mathrm{k}}/\mathbb{Q}}(\beta))^3 \end{cases} \Leftrightarrow \begin{cases} 4q_m &= k(k^2 - 9l^2d_m) \quad (1) \\ 4 &= l(k^2 - l^2d_m) \quad (2) \\ 8p_m^3 &= (k^2 + 3l^2d_m)^3 \quad (3). \end{cases}$$

De (2), on déduit que $l \mid 4$ et par conséquent $l \in \{\pm 1,\ \pm 2,\ \pm 4\}$.

Si $l = 1$ alors, $4 = k^2 - d_m$, c'est à dire $4 + d_m = k^2$. D'autre part,

$$(3) \Rightarrow (2p_m)^3 = (k^2 + 3d_m)^3 = (4 + d_m + 3d_m)^3 = (4 + 4d_m)^3 = (4(1 + d_m))^3,$$

d'où $p_m = 2(1 + d_m)$, ce qui contredit le fait que p_m est impair.

Si $l = 2$, alors $(2) \Rightarrow 2 = k^2 - 4d_m$, donc $k^2 = 2 + 4d_m$. Aussi, de (3) on tire que $(2p_m)^3 = (2 + 4d_m + 12d_m)^3 = (2 + 16d_m)^3$, donc $p_m = 1 + 8d_m$. Or la condition $m \equiv 1 \bmod 7$, entraîne que $d_m \equiv 4 \bmod 7$ et $p_m \equiv 0 \bmod 7$, ce qui est impossible.

Si $l = 4$ alors, $(2) \Rightarrow 1 = k^2 - 16d_m \Rightarrow k^2 = 1 + 16d_m$. D'autre part

$$(3) \Rightarrow (2p_m)^3 = (1 + 16d_m + 48d_m)^3 = (1 + 64d_m)^3,$$

d'où $2p_m = 1 + 64d_m$ ce qui est impossible.

Par un calcul analogue, on trouve que si $l = -1$, alors $p_m = 2(d_m - 1)$, si $l = -2$, donc $p_m = 8d_m - 1$, si $l = -4$, on a $2p_m = 64d_m - 1$ et tous ces cas ne peuvent pas se produire. Donc en vertu du lemme 2.1, $Q(X) = X^3 - 3p_mX - q_m$ est irréductible sur $\mathbb{Q}$. □

THÉORÈME 2.6. *Soit d un entier positif sans facteur carré. Alors, toute extension cubique non ramifiée de $\mathbb{Q}(\sqrt{d})$ est donnée par le polynôme $f(X) = X^3 - dwX - d^2u$ avec $u,\ w \in \mathbb{Z}$, tels que pgcd $(u, w) = 1$, $4w^3 - 27du^2$ est un carré dans $\mathbb{Z}$ et pgcd $(3,\ w) = 1$.*

Preuve. Voir [7]. □

THÉORÈME 2.7. *Soient $f(X) = X^n + AX + B \in \mathbb{Z}[X]$, de discriminant D, q un nombre premier qui ne divise pas n et $K = \mathbb{Q}(\theta)$, où θ est une racine de $f(X)$. Alors, la décomposition de q en produits d'idéaux premiers dans K est donnée par:*

1. *Si $v_q(B) > v_q(A)$ et $q \nmid a$, alors $q = \mathcal{Q}\mathcal{A}^{(n-1)/a}$, et $\mathcal{A}$ est q-analogue à $X^a - A_q$ où $a = pgcd\ (n-1, v_q(A))$ et $A_q = A/q^{v_q(A)}$ (la décomposition de $\mathcal{A}$ dans K est similaire à celle de $X^a - A_q$ modulo q).*
2. *Si $v_q(B) \leq v_q(A)$ et $v_q(A) > 0$, alors $q = \mathcal{A}^{n/b}$, et $\mathcal{A}$ est q-analogue à $X^b - B_q$ où $b = pgcd\ (n, v_q(B))$.*
3. *Si $q \nmid AB$ et $q \mid D$, alors la décomposition de $f(X)$ en produit de facteurs irréductibles (modulo q) est*

$$f(X) \equiv (X - u)^2 P_1(X) \dots P_s(X) (\mathrm{mod} q) \text{ et } q = \mathcal{Q}_1 \dots \mathcal{Q}_s \mathcal{A},$$

avec $N(\mathcal{Q}_i) = q^{\deg(P_i)}, N(\mathcal{A}) = q^2$ *où*

$$\mathcal{A} = \begin{cases} \mathcal{Q}\mathcal{Q}' & avec \quad N(\mathcal{Q}) = N(\mathcal{Q}') = q \quad si \quad 2 \mid v_q(D) \ et \ \left(\frac{D_q}{q}\right) = (-1)^{n-s} \\ \mathcal{Q} & avec \quad N(\mathcal{Q}) = q^2 \quad si \quad 2 \mid v_q(D) \ et \left(\frac{D_q}{q}\right) = (-1)^{n-s+1} \\ \mathcal{Q}^2 & avec \quad N(\mathcal{Q}) = q \quad si \quad 2 \nmid v_q(D) \end{cases}$$

(4) *Si* $q \nmid ABD$, *alors* q *est* q*-analogue à* $f(X)$.

Preuve. Voir [9]. □

LEMME 2.8. *Soit* m *un entier positif,* $p_m = m^2 + 3m + 3$ *et* $q_m = 2m^3 + 9m^2 + 9m + 27$, *alors on a*

$$pgcd\ (p_m, q_m) = \begin{cases} 1 \ si \ m \not\equiv 0 \bmod 3 \ et \ m \not\equiv 3 \bmod 7, \\ 7 \ si \ m \not\equiv 0 \bmod 3 \ et \ m \equiv 3 \bmod 7, \\ 3 \ si \ m \equiv 0 \bmod 3 \ et \ m \not\equiv 3 \bmod 7, \\ 21 \ si \ m \equiv 0 \bmod 3 \ et \ m \equiv 3 \bmod 7. \end{cases}$$

De plus, $v_7(d_m) \geq 1 \Leftrightarrow m \equiv 3 \bmod 7$. *Plus précisément dans le cas où* $m \equiv 3 \bmod 7$ *on a:*

(1) $v_7(d_m) = 2 \Leftrightarrow m \not\equiv 24 \bmod 7^2$
(2) $v_7(d_m) = 3$ *si* $m \equiv 24 \mod 7^2$.

Preuve. Voir [10]. □

LEMME 2.9. *Soit* p *un nombre premier impair distinct de* 3.

(1) *Si* $p|p_m$, *donc* $Q(X)$ *admet une racine dans* $\mathbb{F}_p \Leftrightarrow {q_m}^{\frac{p-1}{3}} \equiv 1 \bmod p$.
(2) *Si* $p \nmid p_m$ *et* $(\frac{d_m}{p}) = 1$, *alors:*
- *si* $p \equiv 1 \bmod 6$, *donc* $Q(X)$ *admet une racine dans* $\mathbb{F}_p$ *si et seulement si* $\left(\frac{q_m + 3\sqrt{-3d_m}}{2}\right)^{\frac{p-1}{3}} \equiv 1 \bmod p$,
- *si* $p \equiv 5 \bmod 6$, *donc* $Q(X)$ *admet une racine dans* $\mathbb{F}_p$ *si et seulement si* $a \equiv 1 \bmod p$ *et* $b|p$ *où* a *et* b *sont tels que* $\left(\frac{q_m + 3\sqrt{-3d_m}}{2}\right)^{\frac{p^2-1}{3}} = a + b\sqrt{-3d_m}$.

Preuve. On a $Q(X) = X^3 - 3p_mX - q_m$.
(1) Si $p|p_m$, alors $Q(X) \equiv X^3 - q_m (\mathrm{mod} p)$, donc

$$Q(X) \text{ admet une racine dans } \mathbb{F}_p \Leftrightarrow q_m \text{ est un cube dans } \mathbb{F}_p$$
$$\Leftrightarrow \left(\frac{q_m}{p}\right)_3 = 1 \Leftrightarrow q_m^{\frac{p-1}{3}} \equiv 1 \bmod p.$$

(2) Si $p \nmid p_m$. On sait que le corps fini à p^2 éléments contient les racines cubiques de l'unité. En appliquant la méthode de Cardan, on déduit que les racines de $Q(X)$ dans $\mathbb{F}_{p^2}$ sont de la forme $\zeta + \zeta'$ où $\zeta^3 = \frac{q_m + 3\sqrt{-3d_m}}{2}$ et $\zeta'^3 = \frac{q_m - 3\sqrt{-3d_m}}{2}$. Donc $Q(X)$ admet au moins une racine modulo p si et seulement

si $X^3 - \frac{q_m+3\sqrt{-3d_m}}{2}$ et $X^3 - \frac{q_m-3\sqrt{-3d_m}}{2}$ admettent des racines dans $\mathbb{F}_{p^2}$ si et seulement si $\frac{q_m+3\sqrt{-3d_m}}{2}$ et $\frac{q_m-3\sqrt{-3d_m}}{2}$ sont des cubes dans $\mathbb{F}_{p^2}$ si et seulement si $\left(\frac{q_m\pm3\sqrt{-3d_m}}{2}\right)^{\frac{p^2-1}{3}} = 1$ dans $\mathbb{F}_{p^2}$. Comme $N_{\widetilde{F}/\mathbb{Q}}\left(\frac{q_m+3\sqrt{-3d_m}}{2}\right) = p_m^3$, alors $(\frac{q_m\pm3\sqrt{-3d_m}}{2})^{\frac{p^2-1}{3}} = 1$ dans $\mathbb{F}_{p^2}$ est équivalent à $(\frac{q_m+3\sqrt{-3d_m}}{2})^{\frac{p^2-1}{3}} = 1$ dans $\mathbb{F}_{p^2}$.

Si $(\frac{d_m}{p}) = 1$, alors $\sqrt{d_m} \in \mathbb{F}_p$, et par conséquent

$$\sqrt{-3d_m} \in \mathbb{F}_p \Leftrightarrow \sqrt{-3} \in \mathbb{F}_p \Leftrightarrow \left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \bmod 6.$$

Donc, si $p \equiv 1 \bmod 6$, alors $\sqrt{-3d_m} \in \mathbb{F}_p$ et $\frac{q_m+3\sqrt{-3d_m}}{2} \in \mathbb{F}_p$. On déduit que $(\frac{q_m+3\sqrt{-3d_m}}{2})^{\frac{p^2-1}{3}} = 1$ dans $\mathbb{F}_{p^2}$ si et seulement si $(\frac{q_m+3\sqrt{-3d_m}}{2})^{\frac{p^2-1}{3}} = 1$ dans $\mathbb{F}_p$ si et seulement si $((\frac{q_m+3\sqrt{-3d_m}}{2})^{\frac{p-1}{3}})^{p+1} = 1$ dans $\mathbb{F}_p$. Puisque $p \equiv 1 \bmod 6$, alors

$$\left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p-1}{3}} \not\equiv -1 \bmod p \Rightarrow \left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p-1}{3}} \equiv 1 \bmod p,$$

ainsi

$$\left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p^2-1}{3}} = 1 \text{ dans } \mathbb{F}_{p^2} \Leftrightarrow \left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p-1}{3}} = 1 \text{ dans } \mathbb{F}_p.$$

Si $p \equiv 5 \bmod 6$, alors $\sqrt{-3d_m} \notin \mathbb{F}_p$. Soient a et b tels que $a + b\sqrt{-3d_m} = \left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p^2-1}{3}}$, alors

$$\left(\frac{q_m+3\sqrt{-3d_m}}{2}\right)^{\frac{p^2-1}{3}} = 1 \text{ dans } \mathbb{F}_{p^2} \Leftrightarrow a \equiv 1 \bmod p \text{ et } b \equiv 0 \bmod p.$$

□

PROPOSITION 2.10. *Soient $m \equiv 1 \bmod 7$ et K_1 le corps de décomposition de $Q(X) = X^3 - 3p_mX - q_m$, alors K_1/k est une extension non ramifiée et 7 est inerte dans $K_m = \mathbb{Q}(\theta)$, où θ est une racine de $Q(X)$.*

Preuve. En faisant appel au théorème 2.4 dans le cas où $d = -3d_m$.
Soit p un nombre premier différent de 3 et de 7, alors le lemme 2.8 entraîne que $v_p(pgcd\ (p_m, q_m)) = 0$ et comme $v_p(-3d_m) \geq v_p(pgcd\ (p_m, q_m))$, on déduit que les idéaux premiers au dessus de p ne se ramifient pas dans K_1.

Si $p = 7$, on a:

- Si $m \not\equiv 0 \bmod 3$ et $m \equiv 3 \bmod 7$, alors $v_7(pgcd\ (p_m, q_m)) = 1$. Or $v_7(-3d_m) = v_7(d_m)$, comme $v_7(d_m) \geq 1 \Leftrightarrow m \equiv 3 \bmod 7$ (lemme 2.8), alors $v_7(pgcd\ (p_m, q_m)) \leq v_p(-3d_m)$. Donc les idéaux premiers au dessus de 7 ne se ramifient pas dans K_1.

- Si $m \equiv 0 \bmod 3$ et $m \equiv 3 \bmod 7$, alors d'après le lemme 2.8
$$v_7(pgcd\ (p_m, q_m)) = 1, \text{ or } v_7(-3d_m) = v_7(d_m) \geq 1$$
car $m \equiv 3 \bmod 7$, d'où $v_7(pgcd\ (p_m, q_m)) \leq v_p(-3d_m)$. Donc les idéaux premiers au dessus de 7 ne se ramifient pas dans K_1.
- Si $[m \not\equiv 0 \bmod 3$ et $m \not\equiv 3 \bmod 7]$ ou $[m \equiv 0 \bmod 3$ et $m \not\equiv 3 \bmod 7]$, on a $v_7(pgcd\ (p_m, q_m)) = 0 \leq v_p(-3d_m)$, par conséquent, tout idéal premier diviseur de 7 ne se ramifie pas dans K_1.

Si $p = 3$, on a:
$$v_3(pgcd\ (p_m, q_m)) = \begin{cases} 0 \text{ si } m \not\equiv 0 \bmod 3 \\ 1 \text{ si } m \equiv 0 \bmod 3, \end{cases}$$
donc $v_3(pgcd\ (p_m, q_m)) \leq 1$. D'autre part, $v_3(3) = 1 \geq 1$ et $v_3(q_m) \neq 2$ car sinon 9 divise q_m, par suite $9|2m^3$ (définition de q_m), donc $9|m^3$, d'où $3|m$. Ainsi $v_3(q_m) \geq 3$ car $q_m = 3^3(2k'^3 + 3k'^2 + k' + 1)$, donc $v_3(q_m) \neq 2$. D'après le théorème 2.4, on déduit que tout diviseur de 3 ne se ramifie pas dans K_1. Donc K_1/k est non ramifiée.

Comme $m \equiv 1 \bmod 7$ et d_m est sans facteur carré, alors 7 divise p_m. En vertu du lemme 2.9, $Q(X)$ admet une racine dans $\mathbb{F}_7$ si et seulement si $q_m^2 \equiv 1 \bmod 7$ si et seulement si $q_m \equiv \pm 1 \bmod 7$. Puisque $m \equiv 1 \bmod 7$, on déduit que $q_m \equiv 5 \bmod 7$, et par suite q_m n'est pas un cube dans $\mathbb{F}_7$. Donc $Q(X)$ est irréductible modulo 7. Or d'après [10] $O_{K_m} = \mathbb{Z}[\rho_m]$, où ρ_m est la plus grande racine du polynôme $P_m(x) = x^3 - mx^2 - (m+1)x - 1$ et $[O_{K_m} : \mathbb{Z}[\theta]] = 27$, où O_{K_m} est l'anneau des entiers de K_m. Comme 7 ne divise pas 27 et $Q(X)$ est irréductible modulo 7, alors 7 est inerte dans O_{K_m}. □

3. CARACTÉRISATION DU 3-RANG DU GROUPE DE CLASSES DE $\mathbf{K = \mathbb{Q}(\sqrt{D_M})}$

DÉFINITION 3.1. Soient M un corps de nombres, Cl_M son groupe de classes et p un nombre premier. Le *p-rang du groupe des classes de M* est la dimension de $Cl_M/p\ Cl_M$ sur $\mathbb{F}_p$.

THÉORÈME 3.2. *Soit m un entier positif tels que $m \equiv 1 \bmod 7$ et $d_m = m^4 + 2m^3 - 5m^2 - 6m - 23$ un entier positif sans facteur carré. Alors, le rang du 3-groupe de classes de* k $= \mathbb{Q}(\sqrt{d_m})$ *est supérieur ou égal à 2 si et seulement s'il existe $(u,\ w) \in \mathbb{Z}^2$ vérifiant:*

- *$pgcd\ (3, w) = pgcd\ (u, w) = 1$,*
- *$4w^3 - 27d_m u^2$ est un carré dans $\mathbb{Z}$,*
- *$P(X) = X^3 - d_m wX - d_m^2 u$ est irréductible sur $\mathbb{Q}$,*
- *$\left[7|u \text{ et } \left(\frac{w}{7}\right) = 1\right]$ ou $[7|w$ et $u \equiv \pm 4 \bmod 7]$ ou $[7 \nmid uw$ et $P(X)$ est réductible modulo 7 et $P(X) \not\equiv (X-a)^3 \bmod 7]$.*

Preuve. On suppose que le 3-rang du groupe de classes de k est supérieur ou égal à 2, alors il existe une autre extension non ramifiée, K_2, de k, posons $K = K_1K_2$, alors K est normal sur $\mathbb{Q}$ de degré 18, et $Gal(K/\text{k})$ est bicubique bicyclique. On considère la décomposition de 7 dans K. Soit T et Z les

groupes respectivement d'inertie et de décomposition d'un ideal $\mathcal{B}$ divisant 7 dans $G = Gal(K/\mathbb{Q})$, f et g les ordres respectivement de Z/T et G/Z, alors $fg = 18$. Comme $m \equiv 1 \bmod 7$, on déduit que $d_m^3 \equiv 1 \bmod 7$ c'est à dire $(\frac{d_m}{7}) = 1$, par suite 7 se décompose complètement dans k et K/k est non ramifiée. D'autre part 7 ne se décompose pas complètement dans K_1. Alors, $f = 3$ ou 9, et puisque Z/T est cyclique alors $f = 3$ et $g = 6$, donc 7 se décompose complètement en six premier dans K. Par conséquent, il existe K' sous-corps de K sur k où 7 se décompose en trois premier dans une extension cubique de K'. En vertu du théorème 2.6, il existe $(u,\ w) \in \mathbb{Z}^2$ tel que $P(X) = X^3 - d_m wX - d_m^2 u$ est irréductible, $pgcd\ (3, w) = 1$, $pgcd\ (u, w) = 1$, $4w^3 - 27d_m u^2$ est un carré dans $\mathbb{Z}$ et K'/k est non ramifie où K' est le corps de décomposition de $P(X)$ sur $\mathbb{Q}$. Or comme 7 se décompose complètement dans K', alors d'après le théorème 2.7 on déduit que:

Si $7 \nmid w$, alors $7 \mid u$ et $(\frac{wd_m}{7}) = 1 \Leftrightarrow 7 \mid u$ et $(\frac{w}{7}) = 1$.

Si $7 \mid w$ alors $2u$ est un cube modulo 7 si et seulement si $2u \equiv \pm 1 \bmod 7$ si et seulement si $u \equiv \pm 4 \bmod 7$.

Si $7 \nmid uw$, alors, comme $7 \nmid d_m$ et $v_7(d_m(4w^3 - 27d_m u^2))$ est pair, donc $P(X) \equiv (X - b)^2 P_1(X) \bmod 7$ où b est un entier modulo 7 et P_1 est un polynôme ou $P(X)$ est scindé à zéros simples modulo 7 ce qui veut dire que $P(X)$ est réductible modulo 7 et $P(X) \not\equiv (X - a)^3 \bmod 7$.

Inversement, s'il existe un tel couple $(u,\ w)$ satisfaisant les conditions du théorème 3.2. Alors 7 se décompose complètement en six idéaux dans le corps de décomposition de $P(X)$ sur $\mathbb{Q}$, d'après la proposition 2.10, 7 est inerte dans K_m, ainsi 7 ne se décompose pas complètement dans le corps de décomposition de $Q(X) = X^3 - 3p_m X - q_m$ sur $\mathbb{Q}$, ce qui donne que les corps de décomposition de $P(X)$ et $Q(X)$ sont deux extensions distincts non ramifiées de k, par conséquent le 3-rang du groupe de classes de k est supérieur ou égal à 2. □

Exemples. Pour m un entier positif tels que $m \equiv 1 \bmod 7$ et $d_m = m^4 + 2m^3 - 5m^2 - 6m - 23$ est un entier positif sans facteur carré. Notons r_3 le 3-rang du groupe de classes de $\mathrm{k} = \mathbb{Q}(\sqrt{d_m})$, alors, en utilisant le théorème 3.2, si ils existent u et w deux entiers vérifiant les conditions de théorème on aura $r_3 \geq 2$.

m	d_m	u	w	r_3
22	252977	21	1381	2
29	751657	21	141943	2
36	1766209	42	13399	2
43	3568289	24	13468	2
50	6487177	14	5035	2
71	26101849	14	24007	2
78	37933249	21	146323	2
92	73153777	43	73405	2

REFERENCES

[1] Craig, M., *A type of class group for imaginary quadratic fields*, Acta Arith., **22** (1973), 449–459.

[2] Craig, M., *A construction for irregular discriminants*, Osaka J. Math., **14** (1977), 2, 356–402.

[3] Diaz y Diaz, F., *Sur le* 3*-rang des corps quadratiques*, Pub. Math. d'Orsay 78, **11**, Université de Paris-Sud, Département de Mathématique, Orsay, 1978.

[4] Diaz y Diaz, F., *On some families of imaginary quadratic fields*, Math. Comp., **32** (1978), 142, 637–650.

[5] Diaz y Diaz, F., Shanks, D. and Williams, H.C., *Quadratic fields with* 3*-rank equal to* 4, Math. Comp., **33** (1979), 146, 836–840.

[6] Kishi, Y., *A criterion for a certain type of imaginary quadratic fields to have* 3*-ranks of the ideal class groups greater than one*, Proc. Japan Acad. Ser. A Math. Sci., **74** (1998), 93–97.

[7] Kishi, Y., *A constructive approch to Spiegelung relations betwen* 3*-ranks of absolute ideal class group and congruent ones modulo* $(3)^2$ *in quadratic fields*, J. Number Theory, **83** (2000), 1–49.

[8] Kishi, Y. and Miyake, M., *Characterization of the quadratic fields whose class number are divible by three*, J. Number Theory, **80** (2000), 209–217.

[9] Llorente, P., Nart, E. and Vila, N., *Decomposition of primes in number fields defined by trinomials*, J. Théor. Nombres Bordeaux, **3** (1991), 1, 27–41.

[10] Louboutin, S., *Class number and class group problems for some non-normal totally real cubic number fields*, Manuscripta Math., **106** (2001), 411–427.

[11] Quer, J., *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de rang* 12, C. R. Math. Acad. Sci. Paris, Sér. I, **305** (1987), 6, 215–218.

[12] Shanks, D. and Weinberger, P., *A quadratic field of prime discriminant requiring three generators for its class group and related theory*, Acta Arith., **21** (1972), 71–87.

[13] Shanks, D., *New types of quadratic fields having three invariants divisible by* 3, J. Number Theory, **4** (1972), 537–556.

Received February 28, 2015
Accepted July 05, 2016

Université Mohamed Premier
Faculté des Sciences
Département de Mathématiques et Informatique
Oujda, Maroc
E-mail: abdelmalekazizi@yahoo.fr
E-mail: ksirat1971@yahoo.fr
E-mail: talbimm@yahoo.fr