Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 20 (1974)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

Autor: Archinard, Gabriel

Kapitel: Chapitre 3. — Les nombres cubiques cycliques POUR LESQUELS Z [] EST L'ANNEAU DES ENTIERS DE Q ()

DOI: https://doi.org/10.5169/seals-46902

Ces formes s'écrivent respectivement:

$$I(\psi) = \frac{a_1 - a_2}{3}(X^3 - 3X^2Y + Y^3) + a_1XY(X-Y)$$

et

$$I(\psi) = (a_1 - a_2)(X^3 - 3X^2Y + Y^3) + 3a_1XY(X-Y).$$

On voit que $I(\psi)$ est pair, pour tous X et Y entiers rationnels si et seulement si $a_1 - a_2$ est pair. C.q.f.d.

Exemple 2.1 Soit K le corps engendré par $\alpha = 5j - j^2$. On a $\alpha\alpha' = 31$ et $\alpha - 1 = 6j$, donc α est canonique unitaire et $K = Q(\theta)$, où θ est zéro du polynôme $X^3 - X^2 - 10X + 8$. Les 3 zéros de ce polynôme forment une base canonique de K et $\Delta_K = 31^2$.

La condition du théorème 2.2 étant satisfaite, 2 est diviseur commun des indices de K.

Remarque 2.2 Si 2 est diviseur commun des indices de K, O_K n'est pas monogène; mais on verra, au chapitre 4, qu'il existe des corps K où 2 n'est pas diviseur commun des indices et où O_K n'est pas monogène.

Chapitre 3. — Les nombres cubiques cycliques θ pour lesquels $Z[\theta]$ est l'anneau des entiers de $Q(\theta)$

Soit θ un nombre cubique cyclique construit avec (β, S) (cf. théorème 1.1). On cherche des conditions pour que l'anneau des entiers de $Q(\theta)$ soit $Z[\theta]$.

Lemme 3.1 Soit θ un nombre cubique cyclique, construit avec (β, S), tel que $Z[\theta]$ soit l'anneau des entiers de $Q(\theta)$. Alors $\beta = \frac{b+d}{c}j + \frac{b}{c}j^2$, où d est égal à 1 ou à 3 et où b et c sont des entiers rationnels premiers entre eux.

Démonstration Soit $\beta = b_1 j + b_2 j^2$. b_1 et b_2 sont des nombres rationnels. $1, \theta, \theta^2$ étant une base d'entiers de $Q(\theta)$, on a

$$\frac{\Delta(1, \theta, \sigma\theta)}{\Delta(1, \theta, \theta^2)} \in Z.$$

D'après les formules (1.5) et (1.6), cette condition s'écrit

$$-\frac{27}{(\beta-\beta')^2} \in Z\,.$$

Mais $(\beta-\beta')^2 = (j-j^2)^2(b_1-b_2)^2 = -3(b_1-b_2)^2$. La condition s'écrit donc $\dfrac{9}{(b_1-b_2)^2} \in Z$, soit $\dfrac{3}{b_1-b_2} \in Z$.

Soit $b_1 - b_2 = \dfrac{d}{c}$, avec c et d entiers rationnels premiers entre eux et $d > 0$; la condition $\dfrac{3}{b_1-b_2} \in Z$ devient $\dfrac{3c}{d} \in Z$, ce qui implique, c et d étant premiers entre eux et d étant positif, $d = 1$ ou $d = 3$.

Par ailleurs, $\theta \in O_K$ donc $\Delta(1, \theta, \sigma\theta) \in Z$; soit, d'après (1.6) $\beta\beta' \in Z$. Mais $\beta = \left(b_2 + \dfrac{d}{c}\right) j + b_2 j^2$; donc $\beta\beta' = b_2^2 + b_2 \dfrac{d}{c} + \left(\dfrac{d}{c}\right)^2$. La condition $\beta\beta' \in Z$ implique, c étant entier, $b_2^2 c^2 + b_2 dc + d^2 \in Z$.

Mais $d \in Z$, donc cette condition s'écrit $b_2^2 c^2 + b_2 dc \in Z$, soit $b_2 c(b_2 c + d) \in Z$. De là on tire $b_2 c \in Z$, soit $b_2 = \dfrac{b}{c}$ avec $b \in Z$.

On a ainsi obtenu $\beta = \dfrac{b+d}{c} j + \dfrac{b}{c} j^2$. C.q.f.d.

Le théorème suivant donne des précisions supplémentaires sur β.

Théorème 3.1 Soit θ un nombre cubique cyclique tel que l'anneau des entiers de $K = Q(\theta)$ soit $Z[\theta]$ et soit (β, S) l'image de (θ, σ). Alors β satisfait l'une des conditions suivantes:

$$(3.1)\quad \begin{cases} \beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2\,, \text{ avec } b \in Z\,,\ b \equiv 1 \pmod 3\,, \\[2ex] c \in Z \quad \text{et} \quad \left(\dfrac{b^2+b+1}{3c^3}\right)^2 = \Delta_K \end{cases}$$

$$(3.2)\quad \begin{cases} \beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2\,, \text{ avec } b \in Z, b \not\equiv 0 \pmod 3\,, \\[2ex] c \in Z,\ c \not\equiv 0 \pmod 3 \text{ et } \left(\dfrac{b^2+3b+9}{c^3}\right)^2 = \Delta_K \end{cases}$$

$$(3.3)\quad \begin{cases} \beta = \dfrac{3}{c}(b+1)j + \dfrac{3}{c}bj^2\,, \text{ avec } b \in Z\,,\ b \not\equiv 1 \,(\mathrm{mod}\ 3) \\[2ex] c \in Z,\ c \not\equiv 0 \,(\mathrm{mod}\ 3) \text{ et } 81\left(\dfrac{b^2+b+1}{c^3}\right)^2 = \Delta_K\,. \end{cases}$$

Démonstration On obtient ces 3 conditions pour β en prenant successivement, dans la forme de β donnée par le lemme 3.1, $d = 1$, $d = 3$ et $b \not\equiv 0$ (mod 3) et $d = 3$ et $b \equiv 0$ (mod 3).

a) $d = 1$

Alors, $\beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2$. L'hypothèse $Z[\theta] = O_K$ entraîne $\Delta(\theta) = \Delta_K$, donc, d'après (1.9), $-\dfrac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \Delta_K$, soit encore $-\dfrac{1}{27}\dfrac{1}{c^6}(b^2+b+1)^2(-3) = \left(\dfrac{b^2+b+1}{3c^3}\right)^2 = \Delta_K$.

Cette condition entraîne $b^2 + b + 1 \equiv 0$ (mod 3), soit $b \equiv 1$ (mod 3).

b) $d = 3$ et $b \not\equiv 0$ (mod 3)

c et d étant premiers entre eux, on a $c \not\equiv 0$ (mod 3).

On a donc $\beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2$, et l'égalité $\Delta(\theta) = \Delta_K$ s'écrit

$$\left(\frac{b^2+3b+9}{c^3}\right)^2 = \Delta_K\,.$$

c) $d = 3$ et $b \equiv 0$ (mod 3)

Comme en b), on voit que $c \not\equiv 0$ (mod 3).

En posant $b = 3\,b_0$, il vient $\beta = \dfrac{3}{c}(b_0+1)j + \dfrac{3}{c} b_0 j^2$.

La condition $\Delta(\theta) = \Delta_K$ s'écrit $81\left(\dfrac{b_0^2+b_0+1}{c^3}\right)^2 = \Delta_K\,.$

Cette condition ne peut être satisfaite que si $b_0^2 + b_0 + 1 \not\equiv 0$ (mod 3), c'est-à-dire si $b_0 \not\equiv 1$ (mod 3). En écrivant b au lieu de b_0, on a les conditions (3.3). C.q.f.d.

Ces conditions (3.1), (3.2) et (3.3) sont deux à deux exclusives.

β étant un nombre satisfaisant l'une de ces conditions et θ étant construit avec (β, S), il se peut, même si S est entier, que θ ne soit pas entier.

Dans les 3 lemmes qui suivent, on donne des conditions pour que θ soit entier, lorsque β satisfait des conditions proches de (3.1), (3.2) ou (3.3).

Pour que θ soit entier, il faut et il suffit que les coefficients du polynôme (1.4) soient entiers, soit que $S \in Z$ et que les 2 conditions suivantes soient satisfaites:

$$\frac{1}{3}(S^2 - \beta\beta') \in Z \tag{3.4}$$

$$\frac{1}{27}(S^3 - 3S\beta\beta' + \beta\beta'(\beta+\beta')) \in Z \tag{3.5}$$

Lemme 3.2 Soit $S \in Z$ et β satisfaisant

$$(3.1)' \quad \begin{cases} \beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z, \\ c \in Z \text{ et } \dfrac{b^2+b+1}{3c^3} \in Z. \end{cases}$$

Alors, si θ est construit avec (β, S), une condition nécessaire et suffisante pour que θ soit entier est $S \equiv 0 \pmod 3$ et $b \equiv 4 \pmod 9$.

Démonstration :

$$\beta\beta' = \frac{b^2+b+1}{c^2} = 3c \cdot \frac{b^2+b+1}{3c^3}$$

est un entier congru à 0 (mod 3), puisque $\dfrac{b^2+b+1}{3c^3} \in Z$.

La condition (3.4) est donc équivalente à $S \equiv 0 \pmod 3$, et en tenant compte de ceci, la condition (3.5) est équivalente à $-\dfrac{1}{27}\beta\beta'(\beta+\beta') \in Z$.

Le calcul donne $-\dfrac{1}{27}\beta\beta'(\beta+\beta') = \dfrac{b^2+b+1}{27c^3}(2b+1)$.

Mais $\dfrac{b^2+b+1}{3c^3} \in Z$ entraîne $b^2+b+1 \equiv 0 \pmod 3$, ce qui est équivalent à $b \equiv 1 \pmod 3$ et à $b^2+b+1 \equiv 3 \pmod 9$. Ceci entraîne $c \not\equiv 0 \pmod 3$.

La condition $\dfrac{b^2+b+1}{3c^3} \cdot \dfrac{2b+1}{9} \in Z$ est donc équivalente à $2b+1 \equiv 0 \pmod 9$, soit à $b \equiv 4$ (mod. 9). C.q.f.d.

Remarque 3.1 La condition $b \equiv 4 \pmod 9$ est équivalente à la condition $\dfrac{b^2+b+1}{3c^3} \equiv 7 \pmod 9$ si $c \equiv 1 \pmod 3$ et à la condition $\dfrac{b^2+b+1}{3c^3} \equiv -7 \pmod 9$ si $c \equiv -1 \pmod 3$.

Lemme 3.3 Soit $S \in Z$ et β satisfaisant

$$(3.2)' \quad \begin{cases} \beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z, \ b \not\equiv 0 \pmod 3, \\ c \in Z \quad \text{et} \quad \dfrac{b^2+3b+9}{c^3} \in Z. \end{cases}$$

Alors, si θ est construit avec (β, S), une condition nécessaire et suffisante pour que θ soit entier est $S \equiv -b\,c \pmod 3$.

Démonstration $b \not\equiv 0 \pmod 3$ entraîne $b^2 + 3b + 9 \equiv 1 \pmod 3$. Donc $\dfrac{b^2+3b+9}{c^3} \in Z$ entraîne $c \not\equiv 0 \pmod 3$. Il en résulte $\beta\beta' = \dfrac{b^2+3b+9}{c^2} \equiv 1 \pmod 3$; la condition (3.4) est équivalente à $S \not\equiv 0 \pmod 3$. D'autre part, $\beta\beta'(\beta+\beta') = -\dfrac{b^2+3b+9}{c^3}(2b+3)$ est entier rationnel et la condition (3.5) entraîne la condition plus faible $S^3 \equiv -\beta\beta'(\beta+\beta') \pmod 3$. D'où, en tenant compte de $S^3 \equiv S \pmod 3$ et de $2b+3 \equiv -b \pmod 3$, $S \equiv -\dfrac{b^2+3b+9}{c^3} b \pmod 3$.

Mais $\dfrac{b^2+3b+9}{c^3} \equiv c \pmod 3$ puisque $\dfrac{b^2+3b+9}{c^2} \equiv 1 \pmod 3$ et $c \not\equiv 0 \pmod 3$. Il vient $S \equiv -b\,c \pmod 3$. Réciproquement, on vérifie que si $S \equiv -b\,c \pmod 3$, la condition (3.5) est satisfaite. C.q.f.d.

Lemme 3.4 Soit $S \in Z$ et β satisfaisant

$$(3.3)' \quad \begin{cases} \beta = \dfrac{3}{c}(b+1) j + \dfrac{3}{c} b j^2, \text{ avec } b \in Z, \ c \in Z \\ \text{et } \dfrac{b^2+b+1}{c^3} \in Z \end{cases}$$

Alors, si θ est construit avec (β, S) ,une condition nécessaire et suffisante pour que θ soit entier est $S \equiv 0 \pmod 3$.

Démonstration $\beta\beta' = \dfrac{9}{c^2}(b^2+b+1)$ est un entier congru à 0 (mod 9), la condition (3.4) est donc équivalente à $S \equiv 0 \pmod 3$. La condition (3.5) est alors aussi satisfaite. En effet $S \equiv 0 \pmod 3$ entraîne $S^3 \equiv 0 \pmod{27}$ et $3\,S\,\beta\,\beta' \equiv 0 \pmod{27}$. Donc la condition (3.5) est équivalente à $\dfrac{1}{27}\beta\beta'(\beta+\beta') \in Z$.

Cette dernière condition est vérifiée, car $\beta\beta'(\beta+\beta') = -27\,\dfrac{b^2+b+1}{c^3}(2b+1)$ est un entier congru à 0 (mod 27), puisque $\dfrac{b^2+b+1}{c^3} \in Z$. C.q.f.d.

Les résultats précédents permettent de démontrer le théorème principal de ce travail:

Théorème 3.2 Soit $(\beta, S) \in E \times Z$ et soit θ construit avec (β, S). Alors $Z[\theta]$ est l'anneau des entiers de $Q(\theta)$ si et seulement si (β, S) satisfait l'une des conditions suivantes:

$$(3.6)\quad \begin{cases} \beta = \dfrac{b+1}{c}j + \dfrac{b}{c}j^2, \text{ avec } b \in Z,\ b \equiv 4 \pmod 9,\ c \in Z \\[2ex] \text{et } \dfrac{b^2+b+1}{3c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\[2ex] S \equiv 0 \pmod 3 \end{cases}$$

$$(3.7)\quad \begin{cases} \beta = \dfrac{b+3}{c}j + \dfrac{b}{c}j^2, \text{ avec } b \in Z,\ b \not\equiv 0 \pmod 3,\ c \in Z \\[2ex] \text{et } \dfrac{b^2+3b+9}{c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\[2ex] S \equiv -bc \pmod 3 \end{cases}$$

$$(3.8)\quad \begin{cases} \beta = \dfrac{3}{c}(b+1)j + \dfrac{3}{c}bj^2, \text{ avec } b \in Z,\ b \not\equiv 1 \pmod 3,\ c \in Z \\[2ex] \text{et } \dfrac{b^2+b+1}{c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\[2ex] S \equiv 0 \pmod 3 \end{cases}$$

Ces conditions sont deux à deux exclusives et entraînent $\beta\beta'^2 \notin E^3$.

Démonstration Ces conditions sont nécessaires d'après le théorème 3.1 et les lemmes 3.2, 3.3 et 3.4.

D'après ces mêmes lemmes, θ est entier. Il reste donc, pour montrer que ces conditions sont suffisantes, à montrer que dans chacun de ces cas, $\Delta(\theta)$ est le discriminant de $Q(\theta)$.

a) cas où (β, S) satisfait (3.6).
$c\beta = (b+1)j + b j^2$ est sans facteur rationnel. Mais
$(c\beta)(c\beta)' = b^2 + b + 1 = 3|c|^3 \dfrac{b^2+b+1}{3|c|^3}$, avec $\dfrac{b^2+b+1}{3|c|^3}$ entier positif distinct de 1 et sans facteurs carrés.
Donc, d'après le lemme 1.3, $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), $\dfrac{b^2+b+1}{3|c|^3}$ est produit de nombres premiers distinct congrus à 1 (mod 3) et $c\beta = (j - j^2)\gamma^3\alpha$, avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \dfrac{b^2+b+1.}{3|c|^3}$
On a de plus $\dfrac{\beta^2\beta'}{\alpha^2\alpha'} = -\left(\dfrac{j-j^2}{c}\right)^3 \gamma^6\gamma'^3 \in E^3$; donc $\beta\beta'^2 \notin E^3$, d'après le théorème 1.2, α engendre $Q(\theta)$.
La formule (1.5) donne $\Delta(\theta) = -\dfrac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \left(\dfrac{b^2+b+1}{3c^3}\right)^2$ $= (\alpha\alpha')^2$; il s'ensuit que $\Delta(\theta) = (\alpha\alpha')^2$ est le discriminant de $Q(\theta)$, d'après le collaire 1.4.

b) Cas où (β, S) satisfait (3.7).
$c\beta = (b+3)j + bj^2$ n'a pas de facteur rationnel, puisque $b \not\equiv 0$ (mod 3). $(c\beta)(c\beta)' = |c^3| \dfrac{b^2+3b+9}{|c|^3}$ avec $\dfrac{b^2+3b+9}{|c|^3} \not\equiv 0 \pmod 3$, différent de 1 et sans facteur carré.
Donc le lemme 1.3 montre que $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), que $\dfrac{b^2+3b+9}{|c|^3}$ est produit de nombres premiers distincts congrus à 1 (mod 3) et que $c\beta = \gamma^3\alpha$ avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \dfrac{b^2+3b+9}{|c|^3}$. Donc $\beta\beta'^2 \notin E^3$.

Le théorème 1.2 montre que α engendre $Q(\theta)$. La formule (1.5) donne

$$\Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \left(\frac{b^2+3b+9}{c^3}\right)^2 = (\alpha\alpha')^2;$$ il s'ensuit que $\Delta(\theta) = (\alpha\alpha')^2$ est le discriminant de $Q(\theta)$, d'après le corollaire 1.4.

c) Cas où (β, S) satisfait (3.8)

$\frac{c}{3}\beta = (b+1)j + bj^2$ n'a pas de facteur rationnel.

$\left(\frac{c}{3}\beta\right)\left(\frac{c}{3}\beta\right)' = |c|^3 \frac{b^2+b+1}{|c|^3}$, avec $\frac{b^2+b+1}{|c|^3} \not\equiv 0 \pmod 3$, différent de 1 et sans facteur carré.

Le lemme 1.3 montre que $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), que $\frac{b^2+b+1}{|c|^3}$ est produit de nombres premiers distincts et congrus à 1 (mod 3) et que $\frac{c}{3}\beta = \gamma^3\alpha$ avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \frac{b^2+b+1}{|c|^3}$. Donc $\beta\beta'^2 \notin E^3$ et α engendre $Q(\theta)$ (théorème 1.2). Or $\frac{c}{3}\beta = (b+1)j + bj^2 \not\equiv \pm 1 \pmod 3$ et $\gamma^3 \equiv \pm 1 \pmod 3$, puisque γ est produit d'entiers canoniques, donc congrus à une unité (mod 3). L'égalité $\frac{c}{3}\beta = \gamma^3\alpha$ montre alors que $\alpha \not\equiv \pm 1 \pmod 3$, c'est-à-dire que α est un entier canonique non unitaire.

Il s'ensuit, d'après le corollaire 1.4, que le discriminant de $Q(\theta)$ est $81(\alpha\alpha')^2$.

Et on a ainsi $\Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = 81\left(\frac{b^2+b+1}{c^3}\right)^2 = 81(\alpha\alpha')^2$. C.q.f.d.

Comme sous-produits de la démonstration de ce théorème, on obtient les corollaires suivants:

Corollaire 3.1 Si β satisfait la condition (3.6), $Q(\theta)$ est modérément ramifié, de discriminant $\left(\frac{b^2+b+1}{3c^3}\right)^2$; si β satisfait (3.7), $Q(\theta)$ est modérément ramifié, de discriminant $\left(\frac{b^2+3b+9}{c^3}\right)^2$; et si β satisfait (3.8), $Q(\theta)$ est sauvagement ramifié, de discriminant $81\left(\frac{b^2+b+1}{c^3}\right)^2$.

Corollaire 3.2 Si β satisfait l'une des conditions (3.6), (3.7), (3.8), $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3).

Remarque 3.2 Si β satisfait la condition (3.7) (respectivement (3.8)) et si $|c| = 1$, β est entier canonique et satisfait aussi la condition (2.3) (respectivement (2.4)) du théorème 2.1.

C'est le seul cas où l'on peut choisir la trace S de manière que, θ étant construit avec (β, S), $1, \theta, \theta^2$ et $\theta, \sigma\theta, \sigma^2\theta$ (respectivement $1, \theta, \sigma\theta$) forment des bases d'entiers de $Q(\theta)$.

Définition 3.1 On dit dans ce cas que l'anneau des entiers de $Q(\theta)$ est trivialement monogène.

En abandonnant la référence à (β, S), on peut énoncer:

Théorème 3.3 Soit K/Q une extension cubique cyclique de discriminant $\Delta_K = m^2$. Alors, si O_K est monogène, l'équation diophantienne suivante est soluble:

$$X^2 + 3X + 9 = mY^3 \tag{3.9}$$

Démonstration On garde les notations du théorème 3.2. O_K étant monogène, il existe $\theta \in O_K$, construit avec un couple (β, S) qui satisfait l'une des conditions (3.6), (3.7) ou (3.8).

Si (3.6) est satisfaite, $b^2 + b + 1 = m\,3\,|c|^3$, donc l'équation (3.9) admet la solution $(3b, 3|c|)$.

Si (3.7) est satisfaite, $b^2 + 3b + 9 = m|c|^3$, donc (3.9) admet la solution $(b, |c|)$,

Si (3.8) est satisfaite, $9(b^2+b+1) = m|c|^3$, donc (3.9) admet la solution $(3b, |c|)$.

Ce théorème admet le réciproque suivant:

Théorème 3.4 Soit $m \neq 1$ un produit de nombres premiers distincts et congrus à 1 (mod 3).

Alors:

a) si l'équation diophantienne

(3.10) $$X^2 + 3X + 9 = mY^3$$

est soluble avec $X \not\equiv 0 \pmod 3$ ou avec $X \equiv 12 \pmod{27}$, il existe une extension K/Q modérément ramifiée, de discriminant m^2 et dont l'anneau des entiers est monogène.

b) si l'équation diophantienne

(3.11) $$X^2 + X + 1 = mY^3$$

est soluble, il existe une extension K/Q sauvagement ramifiée, de discriminant $81\, m^2$ et dont l'anneau des entiers est monogène.

Démonstration

a) Si (b, c) est une solution de (3.10) avec $b \not\equiv 0 \pmod 3$ le nombre $\beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2$ satisfait la condition (3.7) du théorème 3.2. Ce théorème montre que le nombre θ construit avec $(\beta, -bc)$ engendre un corps K tel que $O_K = Z\,[\theta]$ et $\Delta_K = m^2$.

Si (b, c) est une solution de (3.10) avec $b \equiv 12 \pmod{27}$, alors $b_0 = \dfrac{b}{3}$ est un entier congru à $4 \pmod 9$ et $c_0 = \dfrac{c}{3}$ est entier. Le nombre $\dfrac{b_0+1}{c_0} j + \dfrac{b_0}{c_0} j^2$ satisfait la condition (3.6) du théorème 3.2; ce qui montre que le nombre θ construit avec $(\beta, 0)$ engendre un corps K tel que $O_K = Z\,[\theta]$ et $\Delta_K = m^2$.

b) Soit (b, c) une solution de (3.11). Il faut $b \not\equiv 1 \pmod 3$ et $c \not\equiv 0 \pmod 3$. Le nombre $\beta = 3\dfrac{b+1}{c} j + 3\dfrac{b}{c} j^2$ satisfait la condition (3.8) du théorème 3.2; ce qui montre que le nombre θ construit avec $(\beta, 0)$ engendre un corps K tel que $O_K = Z\,[\theta]$ et $\Delta_K = 81\, m^2$. C.q.f.d.

Remarque 3.3 Si (X, Y) est solution de l'équation diophantienne (3.10), la condition $X \equiv 12 \pmod{27}$ est équivalente à la condition $m \equiv 7 \pmod 9$.