

Séminaire de Théorie des Nombres .

- Besançon -

Année 1975-76

LIEN ENTRE LE GROUPE DES UNITES ET LA MONOGENEITE  
DES CORPS CUBIQUES CYCLIQUES

Marie-Nicole GRAS  
Faculté des Sciences. Mathématiques  
25030 BESANCON CEDEX

# LIEN ENTRE LE GROUPE DES UNITES ET LA MONOGENEITE DES CORPS CUBIQUES CYCLIQUES .

par M.N. GRAS

---

Introduction . Cet exposé est la suite de l'existence de  $\mathbb{Z}$ -bases d'entiers de la forme  $1, \vartheta, \vartheta^2$  dans les corps cubiques cycliques ([2]). Nous démontrons de nouvelles conditions nécessaires pour qu'un corps cubique cyclique admette une telle base et nous donnons des résultats numériques pour les corps de conducteur inférieur à 4000 .

1 Rappels .

Soit  $K$  une extension cubique cyclique de  $\mathbb{Q}$ ; soit  $G = \{1, \sigma, \sigma^2\}$  le groupe de Galois de  $K$  sur  $\mathbb{Q}$ ; soit  $A$  l'anneau des entiers de  $K$ . Soit  $m$  le conducteur de  $K$ ; le discriminant de  $K/\mathbb{Q}$  est égal à  $m^2$ . Le conducteur  $m$  de  $K$  s'écrit de manière unique sous la forme  $m = \frac{a^2 + 27b^2}{4}$ ,  $b > 0$ , le signe de  $a$  étant déterminé par une congruence sur  $a$  (cf. [1]).

Soit  $\zeta$  une racine primitive  $m^{\text{ième}}$  de l'unité et soit  $\theta = \text{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta)$ ; les éléments  $1, \theta$  et  $\theta^\sigma$  constituent une base d'entiers de  $K$ ; on dit que l'anneau des entiers de  $K$  est monogène [5] s'il existe une  $\mathbb{Z}$ -base de  $A$  de la forme  $1, \vartheta, \vartheta^2$ . Soit  $\Delta(\vartheta)$  le discriminant du polynôme irréductible de l'entier  $\vartheta$  sur  $\mathbb{Q}$ ; les éléments  $1, \vartheta, \vartheta^2$  constituent une base d'entiers de  $K$  si et seulement si  $\Delta(\vartheta) = m^2$ .

Soit  $E$  le groupe des unités de norme 1 de  $K$  considéré comme  $G$ -module . Soit  $\varepsilon$  un générateur de  $E$  . Toute unité  $\psi$  de  $E$  s'écrit de manière unique  $\psi = \varepsilon^{x+y\sigma}$  ,  $x, y \in \mathbb{Z}$  . Dans [2] , nous avons démontré le théorème suivant :

Théorème : L'anneau des entiers de  $K$  est monogène si et seulement si  $K$  possède une unité  $\psi$  de norme 1 vérifiant les deux conditions :

$$(i) \quad \text{Tr}_{K/\mathbb{Q}} (\psi + \psi^{-1}) + 3 = 0 ,$$

$$(ii) \quad \text{Tr}_{K/\mathbb{Q}} \frac{\psi^2 - \psi^{-1}}{m} = \gamma^3 , \gamma \in \mathbb{Z} .$$

II Position du problème .

Dans [2] , nous avons établi trois conditions nécessaires et suffisantes de monogénéité de  $A$  ; elles permettent d'obtenir de nombreux exemples de corps  $K$  possédant une telle base , mais il n'est pas toujours possible , étant donné un corps cubique cyclique , de voir simplement s'il admet ou non une  $\mathbb{Z}$ -base d'entiers  $1, \eta, \eta^2$  . D'où la nécessité d'établir des conditions nécessaires pour que  $A$  soit monogène . Plusieurs conditions ont été énoncées dans [2] . Une autre condition portant sur  $a$  et  $b$  ( si  $a \equiv 0 \pmod{7}$  , il est nécessaire que  $b \not\equiv \pm 3 \pmod{7}$  ; si  $b \equiv 0 \pmod{7}$  , il est nécessaire que  $a \not\equiv \pm 3 \pmod{7}$ ) m'a été signalée par James G. Huard ( Pennsylvanie ) .

Dans ce travail , nous étudions des conditions nécessaires qui se rapportent au groupe des unités de  $K$  , lorsqu'un générateur  $\varepsilon$  du groupe des unités de  $K$  est connu ( cf. [1] ) . Ces conditions sont obtenues en exploitant le théorème précédent .

Principe de la méthode : soit  $p$  un nombre premier impair tel que le polynome irréductible de  $\varepsilon$  sur  $\mathbb{Q}$  admette trois racines modulo  $p$  , non né -

cessairement distinctes . Soit  $\ell \not\equiv 1 \pmod{p}$  ; il existe des entiers  $\alpha, \beta, \gamma$  modulo  $p$  tels que

$$\varepsilon \equiv \alpha \pmod{\ell} , \quad \varepsilon^\sigma \equiv \beta \pmod{\ell} , \quad \varepsilon^{\sigma^2} \equiv \gamma \pmod{\ell} .$$

Toute unité  $\psi$  de norme 1 de  $K$  s'écrit de manière unique  $\psi = \varepsilon^{x+y\sigma}$  ;

$$\text{alors } \text{Tr}_{K/\mathbb{Q}}(\psi) \equiv \alpha^x \beta^y + \beta^x \gamma^y + \gamma^x \alpha^y \pmod{p}$$

$$\text{et } \text{Tr}_{K/\mathbb{Q}}(\psi^{-1}) \equiv \alpha^{-x} \beta^{-y} + \beta^{-x} \gamma^{-y} + \gamma^{-x} \alpha^{-y} \pmod{p}$$

On cherche s'il existe un nombre premier  $p$  tel que les égalités du théorème soient mises en défaut modulo  $p$  pour toute unité  $\psi$  (donc en fait pour tout  $x, y$ ) .

### III Deux propositions préliminaires .

Proposition 1 : Soit  $K$  un corps cubique cyclique ; soit  $\psi$  une unité de norme 1 de  $K$  . pour tout entier  $n \geq 2$  ,

$$\text{Tr}_{K/\mathbb{Q}}(\psi^n + \psi^{-n}) + 3 \neq 0 .$$

Démonstration : Il suffit de démontrer la proposition pour  $n = p$  , nombre premier . Posons  $T = \text{Tr}_{K/\mathbb{Q}}(\psi)$  et  $S = \text{Tr}_{K/\mathbb{Q}}(\psi^{-1})$  .

$$\text{Si } p = 2 , \text{Tr}_{K/\mathbb{Q}}(\psi^2 + \psi^{-2}) + 3 > 3 .$$

Si  $p$  est un nombre premier impair , on remarque que

$$\text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) + 3 = \psi^p + \psi^{p\sigma} + \psi^{p\sigma^2} + \psi^{-p} + \psi^{-p\sigma} + \psi^{-p\sigma^2} + 3 =$$

$$(\psi^{p+1})(\psi^{p\sigma+1})(\psi^{p\sigma^2+1}) + 1 = (\psi+1)(\psi^\sigma+1)(\psi^{\sigma^2+1}) f(\psi, \psi^\sigma, \psi^{\sigma^2}) + 1 =$$

$(T+S+2) P(T, S) + 1$  ( $f$  est un polynome symétrique à coefficients entiers et est donc de la forme  $P(T, S)$ ) .

L'égalité  $\text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) + 3 = 0$  est donc équivalente à

$$(T+S+2)P(T,S) = -1 ;$$

donc si  $T+S+2 \neq -1$ , cette égalité est impossible .

1<sup>er</sup> cas particulier :  $T+S+1 = 0$

Puisque  $p$  est un nombre premier, on a  $\psi^p + \psi^{p\sigma} + \psi^{p\sigma^2} \equiv (\psi + \psi^\sigma + \psi^{\sigma^2})^p$

mod  $p$  ; donc  $\text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) \equiv T^p + S^p \equiv T+S \pmod{p}$  . Donc si

$T+S+1 = 0$ , on obtient  $\text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) + 3 \equiv 2 \pmod{p}$ , donc différent

de zéro puisque  $p \neq 2$  .

2<sup>e</sup> cas particulier :  $T+S+3 = 0$  ( cas où l'unité  $\psi$  vérifie la relation pour  $n = 1$  ) .

Alors  $\psi + \psi^\sigma + \psi^{\sigma^2} + \psi^{-1} + \psi^{-\sigma} + \psi^{-\sigma^2} + 3 = (\psi + \psi^{-\sigma} + 1)(\psi^{-1} + \psi^\sigma + 1) = 0$ , et

$$\psi^p + \psi^{p\sigma} + \psi^{p\sigma^2} + \psi^{-p} + \psi^{-p\sigma} + \psi^{-p\sigma^2} + 3 = (\psi^p + \psi^{-p\sigma} + 1)(\psi^{-p} + \psi^{p\sigma} + 1) .$$

Supposons que  $\psi + \psi^{-\sigma} + 1 = 0$  ( le raisonnement est analogue si  $\psi^{-1} + \psi^\sigma + 1 = 0$  )

$$\text{Alors } \text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) + 3 = [\psi^{p+1} - (\psi+1)^p] [\psi^{-p+1} - (\psi+1)^{-p}] .$$

Cette quantité est invariante par conjugaison ; comme  $\psi$  est une unité de norme 1, l'un des nombres  $\psi$ ,  $\psi^\sigma$  ou  $\psi^{\sigma^2}$  est positif . Supposons que ce

soit  $\psi^\tau$ ,  $\tau \in \{1, \sigma, \sigma^2\}$  ; alors  $\psi^{\tau p} + 1 - (\psi^\tau + 1)^p < 0$  et

$\psi^{-\tau p} + 1 - (1 + \psi^\tau)^{-p} > 0$  ; donc  $\text{Tr}_{K/\mathbb{Q}}(\psi^p + \psi^{-p}) + 3 < 0$  ; cette quantité

est donc différente de zéro .

Proposition 2 : Si  $m \neq 9$ , alors pour toute unité  $\psi$  de norme 1 de  $K$ , on a

$$\text{Tr}_{K/\mathbb{Q}}(\psi^{1-\sigma} + \psi^{\sigma-1}) + 3 \neq 0 .$$

Démonstration :  $\text{Tr}_{K/\mathbb{Q}}(\psi^{1-\sigma} + \psi^{\sigma-1}) + 3 = (\psi + \psi^\sigma + \psi^{\sigma^2})(\psi^{-1} + \psi^{-\sigma} + \psi^{-\sigma^2}) = TS$

qui est nul si et seulement si  $T$  ou  $S$  est nul .

Soit  $K$  un corps cubique cyclique de conducteur  $m$  possédant une unité  $\psi$  telle que  $\text{Tr}_{K/\mathbb{Q}}(\psi) = 0$ . Alors  $T = 0$  et

$$S = \frac{T^2 - m\gamma}{3} = -\frac{m\gamma}{3}, \quad \gamma \in \mathbb{Z} \quad (\text{l'égalité } S = \frac{T^2 - m\gamma}{3} \text{ est démontrée}$$

dans [3] et rappelée dans [2]) ; d'où  $\text{Irr}(\psi, \mathbb{Q}) = X^3 - \frac{m\gamma}{3}X - 1$ .

Le discriminant de  $\text{Irr}(\psi, \mathbb{Q})$  est égal à  $-4\left(-\frac{m\gamma}{3}\right)^3 - 27 = \frac{4m^3\gamma^3}{27} - 27$  ;

il doit être égal à  $(\beta m)^2$ ,  $\beta$  entier ; donc  $\frac{4m^3\gamma^3}{27} - 27 = \beta^2 m^2$ .

Si  $m = 9m'$ , on obtient  $4 \cdot 27 m'^3 \gamma^3 - 27 = 81 \beta^2 m'^2$ , soit  $m'^2(4m'\gamma^3 - 3\beta^2) = 1$  ; donc  $m' = 1$  et  $m = 9$ . Grâce à [4] (th.5 p.247), on vérifie que la seule solution est donnée par ( $\varepsilon$  désignant un générateur

de  $K = \mathbb{Q} \left( \sqrt[9]{\phantom{x}} \right)$  :  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon) = 0$ ,  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1}) = -3$ ,  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{1-\sigma}) = 3$  et

$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{\sigma-1}) = -6$  (si  $m = 9$ ,  $K = \mathbb{Q} \left( \sqrt[9]{\phantom{x}} \right)$  admet une base  $1, \vartheta, \vartheta^2$ ).

Si  $m \neq 0 (9)$ , alors  $\gamma = 3\gamma'$  et  $4m^3\gamma'^3 - 27 = 3\beta^2 m^2$ , soit  $m^2(4m\gamma'^3 - 3\beta^2) = 27$  ; donc  $m^2 \mid 27$  ( $m = 1$  ou  $3$ ) ce qui est impossible.

Remarque 1. On a  $\psi \in E^{\sigma-1}$  si et seulement si  $\psi = \varepsilon^{x+y\sigma}$ , avec  $x+y \equiv 0 \pmod{3}$ .

#### IV Principaux résultats.

Proposition 3 : Soit  $\varepsilon$  un générateur du groupe des unités de norme 1 de  $K$ , soient  $t = \text{Tr}_{K/\mathbb{Q}}(\varepsilon)$  et  $s = \text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1})$ .

Alors si l'une au moins des conditions suivantes est vérifiée, l'anneau des entiers de  $K$  n'est pas monogène.

1.  $(t+1, s+1) \neq 1$  ;

2.  $(t, s) \neq 1$  et  $\neq 3$  ;
3.  $(t-1, s-1) \neq 1$  et  $\neq 5$  ;
4.  $(t-2, s-2) \neq 1$  et  $\neq 7$  ;
5.  $(t-3, s-3) \neq 1$  et  $\neq 3$  .

Démonstration : Les cinq cas énoncés ci-dessus correspondent à la situation suivante : il existe un nombre premier  $p$  tel que , en choisissant convenablement  $\mathcal{Y}/p$  , on ait :

$$\varepsilon \equiv 1 \pmod{\mathcal{Y}} , \quad \varepsilon^\sigma \equiv \alpha \pmod{\mathcal{Y}} , \quad \varepsilon^{\sigma^2} \equiv \alpha^{-1} \pmod{\mathcal{Y}}$$

où  $\alpha$  désigne respectivement une racine primitive 2<sup>ème</sup> , 3<sup>ème</sup> , 4<sup>ème</sup> , 6<sup>ème</sup> et 1<sup>ère</sup> de l'unité modulo  $p$  . Alors pour tout  $\psi = \varepsilon^{x+y\sigma}$  ,

$$R = \text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv (\alpha^x + \alpha^{-y} + 1)(\alpha^{-x} + \alpha^y + 1) \pmod{p} .$$

Il suffit

alors d'étudier les valeurs de cette expression pour les cinq cas cités .

Traitons à titre d'exemple les cas 1 et 2 . Les cas 3, 4 et 5 se démontrent de manière analogue .

$$1. \quad \text{On a } \alpha = -1 \text{ et } R \equiv [(-1)^x + (-1)^y + 1]^2 \pmod{p} .$$

Si  $x \equiv 0$  et  $y \equiv 1 \pmod{2}$  ou  $x \equiv y \equiv 1 \pmod{2}$  , alors  $R \equiv 1 \pmod{p}$

Si  $x \equiv 0$  et  $y \equiv 0 \pmod{2}$  , alors  $R \equiv 9 \pmod{p}$  ; si  $p \neq 3$  , la congruence  $R \equiv 0 \pmod{p}$  est impossible ; si  $p = 3$  ,  $x$  et  $y$  sont pairs et d'après la proposition 1,  $R \neq 0$  .

2. On a  $\alpha^3 \equiv 1 \pmod{p}$  ,  $\alpha \neq 1 \pmod{p}$  ( donc nécessairement  $p = 3$  ou  $p \equiv 1 \pmod{3}$  ) . On vérifie que si  $(x, y) \neq (1, 2)$  ou  $(2, 1) \pmod{3}$  ,  $R \equiv 3$  ou  $9 \pmod{p}$  ; donc si  $p \neq 3$  ,  $R \neq 0 \pmod{p}$  .

Si  $x \equiv 1 \pmod{3}$  et  $y \equiv 2 \pmod{3}$  , alors  $R \equiv 0 \pmod{p}$  . Mais alors  $x+y \equiv 0 \pmod{3}$  et si  $m \neq 9$  , on sait d'après la proposition 2 que  $R \neq 0$  .

Si  $m = 9$  ,  $t = 0$  ,  $s = -3$  et le corps cubique cyclique de conducteur 9 admet une base  $1, \vartheta, \vartheta^2$  .

Remarque 2.

Le cas 1 est valable pour  $p = 2$  ; on retrouve ainsi que si  $t$  et  $s$  sont impairs, l'anneau des entiers de  $K$  n'est pas monogène .

Remarque 3. Dans les cas 2 ( resp. 3 et 4 ) les diviseurs premiers  $p$  du p.g.c.d. vérifient nécessairement  $p \equiv 1 \pmod{3}$  ( resp.  $p \equiv 1 \pmod{4}$  et  $p \equiv 1 \pmod{3}$  ou  $p = 3$  ) .

Proposition 4. Soit  $p$  un nombre premier ,  $p \neq 2, 3$  tel que le polynome irréductible de  $\xi$  sur  $\mathbb{Q}$  admette trois racines  $\alpha, \beta, \gamma$  modulo  $p$  ; soit  $g$  une racine primitive modulo  $p$  . Soient  $u, v, w$  les entiers uniques modulo  $p-1$  tels que :

$$\alpha \equiv g^u \pmod{p}, \quad \beta \equiv g^v \pmod{p} \quad \text{et} \quad \gamma \equiv g^w \pmod{p} .$$

Pour tout triplet d'entiers modulo  $p-1$  :  $(U, V, W)$  tels que  $U+V+W \equiv 0 \pmod{p-1}$  et  $g^U + g^V + g^W + g^{-U} + g^{-V} + g^{-W} + 3 \equiv 0 \pmod{p}$ , on résoud le système en  $(x, y)$  :

$$\begin{cases} ux + vy = U \\ vx + wy = V \end{cases}$$

Soit  $\mathcal{J}$  l'ensemble de tous les couples  $(x, y)$  ainsi déterminés .

Pour tout  $\psi = \xi^{x+ys}$ , l'égalité  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 = 0$  est impossible si  $(x, y) \notin \mathcal{J}$ .

Démonstration : Les entiers  $u, v, w$  sont connus numériquement puisque  $t$  et  $s$  le sont ; comme  $\xi$  est une unité de norme 1 ,  $u+v+w \equiv 0 \pmod{p-1}$  . On cherche s'il existe des entiers  $x$  et  $y$  modulo  $p-1$  tels que :

$$(1) \quad g^{ux+vy} + g^{vx+wy} + g^{wx+uy} + g^{-ux-vy} + g^{-vx-wy} + g^{-wx-uy} + 3 \equiv 0 \pmod{p} .$$

On pose alors  $U = ux+vy$  ,  $V = vx+wy$  et  $W = wx+uy$  ( on a donc  $U+V+W \equiv 0 \pmod{p-1}$  ) . On est donc amené à résoudre l'équation en  $U, V, W \in [0, p-2]$  ,  $U+V+W \equiv 0 \pmod{p-1}$  :

$$(2) \quad g^U + g^V + g^W + g^{-U} + g^{-V} + g^{-W} + 3 \equiv 0 \pmod{p} .$$

Or l'égalité  $U+V+W \equiv 0 \pmod{p-1}$  entraîne



$$g^U + g^V + g^W + g^{-U} + g^{-V} + g^{-W} + 3 = (g^U + g^{-V} + 1)(g^V + g^{-U} + 1).$$

On en déduit que :

- si  $p \equiv 1 \pmod{3}$ , l'équation (2) admet les deux solutions

$$\left(\frac{p-1}{3}, \frac{p-1}{3}, \frac{p-1}{3}\right), \left(2\frac{p-1}{3}, 2\frac{p-1}{3}, 2\frac{p-1}{3}\right) \text{ et } \frac{p-4}{3} \text{ autres}$$

solutions où tous les  $U, V, W$  sont distincts deux à deux et appartiennent à

$$\{0, 1, \dots, p-2\} - \left\{\frac{p-1}{3}, \frac{p-1}{2}, 2\frac{p-1}{3}\right\}.$$

- si  $p \equiv 2 \pmod{3}$ , l'équation (2) admet  $\frac{p-2}{3} \cdot 3!$  solutions où

tous les  $U, V, W$  sont distincts deux à deux et appartiennent à  $\{0, 1, \dots, p-2\}$

$$- \left\{\frac{p-1}{2}\right\}.$$

Pour chaque valeur de  $(U, V, W)$  ainsi trouvée, on résout le système

$$\begin{cases} ux + vy = U \\ vx + wy = V \end{cases}$$

Toutes les solutions de (1) sont bien les éléments de  $\mathcal{J}$ .

Remarque 4. Le cas  $p = 3$  est entièrement traité à l'aide de la proposition 3, cas 1.

Remarque 5. En théorie,  $\mathcal{Y}$  étant déterminé par la congruence  $\varepsilon \equiv \alpha \pmod{p}$ , ( $\alpha$  étant choisi arbitrairement dans l'ensemble des trois racines modulo  $p$  de  $\text{Irr}(\varepsilon, \mathbb{Q})$ ), on sait que  $\varepsilon^\sigma$  est congru à l'un des nombres  $\beta, \gamma$  et un seul.

En pratique, nous n'avons pas fait la distinction, ce qui oblige à réunir les deux possibilités et, à priori, affaiblit les conditions nécessaires.

En fait, cela revient à remplacer  $\mathcal{J}$  par  $\mathcal{J}' = \{(x, y) \text{ et } (y, x), (x, y) \in \mathcal{J}\}$ .

L'incidence pratique est donc négligeable (par exemple, les propriétés  $x$  et  $y$  pairs,  $x+y \equiv 0 \pmod{3}$  sont des propriétés invariantes par échange de  $x$  et  $y$ ).

Proposition 5 . Soit  $\varepsilon$  un générateur du groupe des unités de norme 1 de  $K$  ;  
soit  $\psi = \varepsilon^{x+y\sigma}$  .

a) S'il existe un nombre premier  $p$  tel que quels que soient  $x$  et  $y$  modulo  $p-1$  , la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  est impossible,  $A$  n'est pas monogène .

b) S'il existe un nombre premier  $p$  tel que la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  ne soit possible que pour  $x$  et  $y$  pairs ( ou multiples d'un même entier ) ,  $A$  n'est pas monogène .

c) Pour tout nombre premier  $p_i$  tel que  $\text{Irr}(\varepsilon, \mathbb{Q})$  admette trois racines modulo  $p_i$  , soit  $\mathcal{J}_i$  l'ensemble des solutions à la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p_i}$  . S'il existe une famille finie de nombres  $p_i$  tels que l'intersection des familles  $\mathcal{J}_i$  ainsi obtenues soit vide ,  $A$  n'est pas monogène .

d) Supposons que pour un nombre premier  $p$  , la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  admette des solutions . Ces solutions sont obtenues pour certaines familles de  $(U, V, W)$  . Pour chacune de ces familles, si  $g^{2U} + g^U + 1 \not\equiv 0 \pmod{p}$  , pour que la condition (ii) du théorème du I soit vérifiée , il est nécessaire que  $g^{2U} + g^U \equiv mc^3 \pmod{p}$  .

Démonstration :

a) et c) sont évidents ( a) est d'ailleurs un cas particulier de c) ) .

b) est évident en appliquant la proposition 1 .

d) Soit  $T = \text{Tr}_{K/\mathbb{Q}}(\psi)$  ; comme  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  ,  
on a  $\text{Tr}_{K/\mathbb{Q}}(\psi^{-1}) \equiv -T - 3 \pmod{p}$  et  $\psi^3 - T\psi^2 - (T+3)\psi - 1 \equiv 0 \pmod{p}$  ;

il en résulte que  $\psi^3 - 3\psi - 1 \equiv T(\psi^2 + \psi)$  modulo  $p$  , ce qui entraîne  $(\psi^2 + \psi)^2(T^2 + 3T + 9) \equiv (\psi^2 + \psi + 1)^3$  . Or  $\text{Tr}_{K/\mathbb{Q}}(\psi^2 - \psi^{-1}) \equiv T^2 + 3T + 9$   
et  $\psi \equiv g^U(\varepsilon)$  . Pour que la condition (ii) du théorème du I soit vérifiée,

il est donc nécessaire que :

$$(g^{2U} + g^U)^2 \equiv m \gamma^3 \pmod{p} \equiv (g^{2U} + g^U + 1)^3 \pmod{p} \quad (p)$$

c'est-à-dire si  $g^{2U} + g^U + 1 \not\equiv 0 \pmod{p}$  ,  $g^{2U} + g^U \equiv m c^3 \pmod{p}$  .

### Résultats numériques .

Ils concernent les corps cubiques cycliques de conducteur  $m < 4000$  . Dans [2] , nous avons obtenu les résultats suivants : il y a 630 corps cubiques cycliques de conducteur  $m < 4000$  . Parmi eux , nous en avons trouvé 76 dont l'anneau des entiers est monogène . Les conditions nécessaires que nous avons établi dans [2] permettaient de conclure que 446 corps n'étaient pas monogènes . Il restait 108 corps pour lesquels nous n'avions pas pu conclure .

Parmi ces 108 corps , il y en a six dont nous n'avions pas calculé un générateur  $\varepsilon$  du groupe des unités dans [1] . L'utilisation de l'ordinateur du C I R C E ( dont l'accès nous a été grandement facilité par M<sup>r</sup> Fiolet que nous remercions ) muni de la quadruple précision pour les nombres réels nous a permis de déterminer le polynome irréductible de ces unités . Dans la Table 1 , nous donnons les valeurs de  $t = \text{Tr}_{K/\mathbb{Q}}(\varepsilon)$  et  $s = \text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1})$  pour ces six corps . Les valeurs de  $t$  et  $s$  pour les autres corps se trouvent dans [1] .

Pour les 108 corps qui restaient à étudier , nous avons testé les conditions des propositions 3 et 5 pour tous les nombres premiers  $p < 1000$  tels que  $\text{Irr}(\varepsilon, \mathbb{Q})$  admette trois racines . Nous avons rassemblé tous les résultats dans la Table 2 . Nous avons étudié les conditions suivantes ( entre parenthèses , nous indiquons la manière dont nous représentons cette condition dans la table ) :

- calcul des différents P.G.C.D. de la proposition 3 .
- recherche d'un nombre premier  $p$  tel que la congruence

$\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  soit impossible (pas de solutions) .

- recherche d'un nombre premier  $p$  tel que la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$  n'ait lieu que si  $\psi \in E^2$  (solutions paires) .

- lorsqu'il y a des solutions et lorsque  $p \equiv 1 \pmod{3}$  , étude des congruences modulo  $p$  que doit vérifier  $m$  d'après le d) de la proposition 5 (congruences) .

- en résolvant tous les systèmes modulo 3 , recherche des nombres premiers  $p \equiv 1 \pmod{3}$  tels que la congruence  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \equiv 0 \pmod{p}$

n'ait lieu que si  $\psi \in E^{1-\sigma}$  ( $x + y \equiv 0 \pmod{3}$ ) .

En étudiant toutes ces conditions pour les nombres premiers  $p < 1000$  , nous avons trouvé qu'il ne reste que 8 corps cubiques cycliques pour lesquels nous ne savons pas conclure .

Ils ont pour conducteur :

$m = 823, 1693, 2377, 2467, 2503, 43 \cdot 61$  ( $a = 85$  ,  $b = 11$ ) , 2707 et 3169.

Il est bien évident que si on poursuivait les essais pour des nombres premiers  $p$  plus grands , on pourrait trouver que certains de ces corps ne sont pas monogènes . Nous pensons d'ailleurs ( cf. conjecture 3 ) qu'ils ne sont pas monogènes .

## VI Lien entre la monogénéité de $K$ et une conjecture sur les unités de $K$ .

Les nombreux exemples numériques obtenus dans [1] permettent d'énoncer la conjecture suivante :

Conjecture 1 : Soit  $K$  un corps cubique cyclique ; soit  $\psi$  une unité de norme 1 de  $K$  ; si  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 \neq 0$  , alors pour tout  $x, y \in \mathbb{Z}$  tels que  $x^2 - xy + y^2 \neq 1$  , on a  $\text{Tr}_{K/\mathbb{Q}}(\psi^{x+y\sigma} + \psi^{-x-y\sigma}) + 3 \neq 0$  .

Cette conjecture entraîne la conjecture moins forte suivante :

Conjecture 2 : Soit  $K$  un corps cubique cyclique ; si une unité  $\psi$  de norme 1 de  $K$  vérifie  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 = 0$  , alors l'unité génératrice  $\varepsilon$  du groupe des unités de norme 1 de  $K$  vérifie la même relation .

Remarque 5. Nous connaissons quelques exemples de corps cubiques cycliques dont un générateur  $\varepsilon$  de  $E$  vérifie  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon + \varepsilon^{-1}) + 3 = 0$  et pour lesquels il existe une autre unité  $\psi$  telle que  $\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 = 0$  ; par exemple :

$m = 7$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon) = -1$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1}) = -2$
	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{2-\sigma}) = 5$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{\sigma-2}) = -8$
$m = 9$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon) = 0$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1}) = -3$
	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{1-\sigma}) = 3$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{\sigma-1}) = -6$
$m = 13$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon) = 1$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1}) = -4$
	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{3-\sigma}) = 66$	$\text{Tr}_{K/\mathbb{Q}}(\varepsilon^{\sigma-3}) = -69$

Remarque 6. Les propositions 1 et 2 sont une approche de la conjecture 1 .

La conjecture 2 permettrait de résoudre presque entièrement le problème de l'existence des  $\mathbb{Z}$ -bases d'entiers de  $K$  de la forme  $1, \vartheta, \vartheta^2$ , dès que l'on connaît un générateur  $\varepsilon$  du groupe des unités de norme 1 de  $K$ . En effet, le théorème du 1 et la conjecture 2 entraîneraient que si  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon + \varepsilon^{-1}) + 3 \neq 0$  , alors il n'existerait pas d'unité  $\psi$  de  $K$  telle que

$\text{Tr}_{K/\mathbb{Q}}(\psi + \psi^{-1}) + 3 = 0$  et  $K$  n'admettrait pas de base  $1, \vartheta, \vartheta^2$  ( en

particulier , cette propriété permettrait de dire que les 8 corps cubiques cycliques pour lesquels nous n'avions pas su conclure ne sont pas monogènes ) . Il resterait à étudier le cas où  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon + \varepsilon^{-1}) + 3 = 0$  :

- si  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon^2 - \varepsilon^{-1}) = m\gamma^3$  ,  $K$  admet une base  $1, \vartheta, \vartheta^2$  ;

- si  $\text{Tr}_{K/\mathbb{Q}}(\varepsilon^2 - \varepsilon^{-1}) \neq m\gamma^3$  , une étude numérique doit être

faite dans chaque cas . Pour les conducteurs  $m < 4000$  , les conditions nécessaires établies dans [2] ont permis de conclure que  $A$  n'était pas monogène .

Ceci nous amène à énoncer la conjecture suivante ( entraînée seulement en partie par la conjecture 2 ) :

Conjecture 3 : Soit  $K$  un corps cubique cyclique . L'anneau des entiers de  $K$  est monogène si et seulement si un générateur  $\xi$  du groupe des unités de norme 1 de  $K$  vérifie les deux conditions :

$$(i) \quad \text{Tr}_{K/\mathbb{Q}}(\xi + \xi^{-1}) = -3 ;$$

$$(ii) \quad \text{Tr}_{K/\mathbb{Q}} \frac{\xi^2 - \xi^{-1}}{m} = \gamma^3 , \gamma \in \mathbb{Z}.$$

Table 1

Cette table donne les valeurs de  $t = \text{Tr}_{K/\mathbb{Q}}(\varepsilon)$  et  $s = \text{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1})$

qui n'avaient pas été calculées dans [1] . Pour chacun des six corps nous donnons les valeurs de m, a, b, t et s .

m	a	b	t	s
3067	19	21	-307269686475168	-3033081529293615
3319	37	21	90172964167691	-751696907976863620
3499	-89	15	-21444832035505	-22368345102371782
3637	115	7	-11183971977835	-21407614886472
3733	55	21	-705073276437779479	-20913796439592236804284
3967	-125	3	-43327870993071604	224368785975002831

Table 2

Dans cette table , nous donnons pour chacun des corps pour lesquels nous n'avons pas su conclure dans [2] :

- le conducteur m ,
- les entiers a et b tels que  $4m = a^2 + 27b^2$  ,
- dans la colonne " monogénéité " , nous mettons " non " si A n'est pas monogène et " ? " si nous n'avons pas su conclure ,
- dans la colonne " raison " , nous mettons une raison qui a permis de conclure ,
- dans la colonne " p " , nous mettons la valeur du nombre premier p qui a donné la contradiction .

m	a	b	monogénéité	raison	p
151	19	3	non	$(t+1, s+1)=9$	3
181	7	5	non	solutions paires	7
211	13	5	non	pas de solutions	199
337	-5	7	non	solutions paires	7
367	-35	3	non	$(t+1, s+1)=3$	3
409	31	5	non	$(t-2, s-2)=13$	13
421	19	7	non	solutions paires	7
487	25	7	non	congruences	7
571	31	7	non	congruences	7
619	-17	9	non	$(t+1, s+1)=3$	3
631	43	5	non	$(t+1, s+1)=5$	5
673	37	7	non	$(t-3, s-3)=49$	7
769	49	5	non	$(t+1, s+1)=7$	7
823	-5	11	?		
829	7	11	non	$(t, s)=7$	7
853	-35	9	non	$(t+1, s+1)=15$	3
859	13	11	non	$(t+1, s+1)=13$	13
871	-53	5	non	$(t+1, s+1)=5$	5
883	-47	7	non	solutions paires	7
907	19	11	non	pas de solutions	61
1033	-53	7	non	$(t, s)=7$	7
1039	-59	5	non	pas de solutions	41
1087	55	7	non	solutions paires	37
1123	-35	11	non	congruences	7
1153	7	13	non	$(t, s)=61$	61
1171	-11	13	non	solutions paires	13
1201	-59	7	non	congruences	7



m	a	b	monogénéité	raison	p
1231	19	13	non	$(t,s)=13$	13
1237	-41	11	non	congruences	421
1279	43	11	non	pas de solutions	223
1297	25	13	non	solutions paires	73
1303	55	9	non	$(t+1,s+1)=9$	3
1387	-65	7	non	$(t+1,s+1)=5$	5
1429	-71	5	non	$(t+1,s+1)=5$	5
1447	-35	13	non	$(t+1,s+1)=5$	5
1453	67	7	non	congruences	77
1609	19	15	non	$(t+1,s+1)=3$	3
1651	-77	5	non	solutions paires	7
1663	73	7	non	$(t,s)=7$	7
1693	-47	13	?		
1741	49	13	non	solutions paires	13
1747	61	11	non	congruences	61
1861	37	15	non	$(t+1,s+1)=3$	3
1873	-65	11	non	$(t+1,s+1)=5$	5
1897	55	13	non	$(t+1,s+1)=5$	5
1993	13	17	non	congruences	43
2007	-15	17	non	$(t-3,s-3)=75$	5
2061	21	17	non	$(t,s)=21$	7
2083	-23	17	non	$x+y=0 (3)$	37
2131	91	3	non	$(t+1,s+1)=3$	3
2137	85	7	non	$(t,s)=103$	103
2161	-29	17	non	solutions paires	433
2221	-53	15	non	$(t+1,s+1)=9$	3
2239	91	5	non	$(t-3,s-3)=25$	5

m	a	b	monogénéité	raison	P
2293	37	17	non	pas de solutions	53
2311	-89	7	non	$(t+1, s+1)=7$	7
2371	-41	17	non	pas de solutions	197
2377	79	11	?		
2467	-11	19	?		
2473	73	13	non	$(t-2, s-2)=139$	139
2503	-47	17	?		
2521	97	5	non	pas de solutions	113
2551	49	17	non	congruences	7
2593	25	19	non	$(t+1, s+1)=5$	5
2617	91	9	non	$(t+1, s+1)=3$	3
2623	85	11	?		
2647	-29	19	non	pas de solutions	97
2677	31	19	non	congruences	19
2683	97	7	non	$(t, s)=7$	7
2707	55	17	?		
2779	-71	15	non	$(t+1, s+1)=3$	3
2817	39	19	non	$(t-2, s-2)=13$	13
2851	73	15	non	$(t+1, s+1)=5$	5
2863	-83	13	non	solutions paires	13
2887	91	11	non	$(t, s)=13$	13
2983	103	7	non	$(t+1, s+1)=7$	7
3037	49	19	non	solutions paires	7
3049	-17	21	non	$(t+1, s+1)=3$	3
3067	19	21	non	solutions paires	7
3121	-89	13	non	$(t-1, s-1)=13$	13
3141	-69	17	non	$(t-3, s-3)=363$	11

m	a	b	monogénéité	raison	p
3169	97	11	?		
3307	-59	19	non	$(t-1, s-1)=13$	13
3319	37	21	non	$(t+1, s+1)=3$	3
3357	75	17	non	pas de solutions	577
3361	-113	5	non	$(t-3, s-3)=49$	7
3433	-77	17	non	congruences	7
3469	103	11	non	solutions paires	97
3493	97	13	non	solutions paires	157
3499	-89	15	non	$(t+1, s+1)=9$	3
3511	79	17	non	$(t-3, s-3)=169$	13
3517	109	9	non	$(t+1, s+1)=3$	3
3559	67	19	non	solutions paires	61
3583	7	23	non	solutions paires	7
3613	13	23	non	solutions paires	13
3637	115	7	non	congruences	7
3643	-17	23	non	$(t-1, s-1)=17$	17
3673	-83	17	non	congruences	151
3679	-53	21	non	$(t+1, s+1)=9$	3
3691	-101	13	non	solutions paires	13
3709	-119	5	non	$(t+1, s+1)=49$	7
3727	25	23	non	solutions paires	157
3733	55	21	non	$(t+1, s+1)=3$	3
3793	103	13	non	congruences	37
3877	-35	23	non	$(t+1, s+1)=23$	23
3919	-77	19	non	$(t+1, s+1)=7$	7
3931	-89	17	non	congruences	19
3967	-125	3	non	$(t+1, s+1)=9$	3

BIBLIOGRAPHIE .

- [1] GRAS M.N.- Méthodes et Algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de  $\mathbb{Q}$ , Journal de Crelle, Band 277, pp. 89-116 ( 1975 ) .
- [2] GRAS M.N.- Sur les corps cubiques cycliques dont l'anneau des entiers est monogène , Ann. Sc. Univ. Besançon, fasc. 6 ( 1973 ) .
- [3] HASSE H.- Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Abhandlungen der Deutschen Akademie der Wissenschaften zu Berlin ( 1948 ) , n° 2 , pp. 1-95 .
- [4] MORDELL L.J. - Diophantine Equations , Academic Press , (1969).
- [5] PAYAN J.J.- Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur  $\mathbb{Q}$  ou sur un corps quadratique imaginaire , Arkiv för matematik, Vol II ( 1973 ) N° 2 , pp. 239-244 .