

FAMILLES D'UNITES DANS LES EXTENSIONS CYCLIQUES
REELLES DE DEGRE 6 DE \mathbb{Q}

Familles d'unités dans les extensions
cycliques réelles de degré 6 de \mathbb{Q}

par Marie-Nicole GRAS

1. Introduction.

Il est bien connu qu'il existe une famille d'extensions cubiques cycliques de \mathbb{Q} particulièrement simple, formée des corps $\mathbb{Q}(w_3)$, où w_3 est racine de

$$(1.1) \quad Q_3 = X^3 - tX^2 - (t+3)X - 1, \quad t \in \mathbb{Z}.$$

Les racines de Q_3 sont w_3 , $\frac{-w_3 - 1}{w_3}$ et $\frac{-1}{1+w_3}$, le discriminant de Q_3 est $(t^2 + 3t + 9)^2$, et dans [G(MN)1], nous avons montré que :

$$(1.2) \quad \text{Si } t^2 + 3t + 9 \text{ est sans facteur carré en dehors des puissances de } 3, \text{ et si } t \neq -6, 3, \text{ alors } w_3 \text{ est un générateur du module des unités de } \mathbb{Q}(w_3).$$

Les unités ainsi définies sont "petites" (un conjugué de w_3 est voisin de 1), et il en résulte que les corps correspondants peuvent fournir des exemples de grands nombres de classes ; ces nombres de classes ont été calculés par D. Shanks [S], lorsque $t^2 + 3t + 9$ est égal à p ou $9p$, p premier.

Dans [G(MN)5], nous avons donné l'analogue de (1.1) pour les extensions cycliques réelles de degré 4 ; ce sont les corps $\mathbb{Q}(w_4)$, où w_4 est racine de

$$(1.3) \quad Q_4 = X^4 - tX^3 - 6X^2 + tX + 1, \quad t \in \mathbb{Z} - \{0, \pm 3\}.$$

Les racines de Q_4 sont w_4 , $\frac{w_4 - 1}{w_4 + 1}$, $-\frac{1}{w_4}$ et $-\frac{w_4 + 1}{w_4 - 1}$, le discriminant de Q_4 est $4(t^2 + 16)^2$ et on a :

(1.4) Si $t^2 + 16$ est sans facteur carré en dehors des puissances de 2, et si $t \neq 0$, alors w_4 est un générateur du module des unités relatives de $\mathbb{Q}(w_4)$.

Nous étudions les corps cycliques réels de degré 6 de \mathbb{Q} engendrés par un élément θ dont un conjugué est une fonction homographique de θ (ce conjugué est $\frac{\theta-1}{\theta+1}$). A partir de θ , qui n'est pas une unité relative, nous construisons une unité relative w , w racine du polynôme :

$$(1.5) \quad Q = (X - 1)^6 - (t^2 + 108)(X^2 + X)^2, \quad t \in \mathbb{Z} - \{0, \pm 6, \pm 26\},$$

et nous montrons en particulier que

(1.6) Si $t^2 + 108$ est sans facteur carré en dehors des puissances de 2 et 3, et si $t \neq 0, \pm 10, \pm 54$, alors w est un générateur du module des unités relatives de $\mathbb{Q}(w) = \mathbb{Q}(\theta)$.

Ces résultats ont été annoncés dans [G(MN)3].

Nous donnons ici le détail des démonstrations.

2. Unités relatives.

a) Notations et rappels.

Nous commençons par rappeler, sans démonstration, les propriétés classiques des extensions cycliques réelles de degré 6 de \mathbb{Q} (cf. [L], [M], [EMT]).

Soit K une extension cyclique réelle de degré 6 de \mathbb{Q} , soit σ un générateur de son groupe de Galois G , et soient k_2 et k_3 les sous-corps quadratique et cubique de K . Soit f le conducteur de K ; alors $f = \text{ppcm}(f_2, f_3)$, où f_2 et f_3 sont les conducteurs respectifs de k_2 et k_3 , et le discriminant de K est égal à $f^2 f_3^2 f_2$.

Puisque K/\mathbb{Q} est cyclique, alors $K = K_\chi$, où χ est le caractère rationnel de $\mathbb{Q}^{(f)}$ défini par $\chi = \chi^1 + \chi^{1^{-1}}$, χ^1 étant le caractère d'ordre 6, défini à inversion près, de $\text{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q}) \simeq (\mathbb{Z}/f\mathbb{Z})^*$ dont le noyau est $\text{Gal}(\mathbb{Q}^{(f)}/K)$ (cf. [L]).

Soit E le groupe des unités de K ; alors $|E|$, groupe des valeurs absolues de E , est un \mathbf{Z} -module libre de rang 5 que l'on munit canoniquement d'une structure de $\mathbf{Z}[G]$ -module en posant $|v|^\sigma = |v^\sigma|$ pour tout $v \in E$.

Il résulte de [L] que E se détermine à partir des groupes d'unités suivants :

- (i) le groupe E_2 des unités de k_2 ,
- (ii) le groupe E_3 des unités de k_3 ,
- (iii) le groupe E_χ des unités χ -relatives de K , c'est-à-dire

$$E_\chi = \left\{ u \in E , u^{1+\sigma^3} = \pm 1 \text{ et } u^{1+\sigma^2+\sigma^4} = \pm 1 \right\} .$$

Soit E' le sous- G -module de E engendré par E_2 , E_3 et E_χ ; alors $|E'| = |E_2| \oplus |E_3| \oplus |E_\chi|$ et l'indice $Q_K = (|E| : |E'|)$ est fini (il est égal à 1 , 3 , 4 ou 12 [EMT]) ce qui décrit E en fonction de E_2 , E_3 (supposés connus) et E_χ .

On vérifie que $u \in E_\chi$ si et seulement si $u^{1-\sigma+\sigma^2} = \pm 1$ et que si $u \in E_\chi$, nécessairement $u^{1+\sigma^3} = 1$; on a donc $E_\chi = \left\{ \pm 1 \right\} \oplus E_*$, où E_* est l'ensemble des éléments de E de norme relative 1 sur k_2 et k_3 , c'est-à-dire

$$(2.1) \quad E_* = \left\{ u \in E , u^{1-\sigma+\sigma^2} = 1 \right\} ,$$

et on peut identifier $|E_\chi|$ à E_* .

On sait que E_* est un module libre de rang 1 sur $\mathbf{Z}[G]/(1-\sigma+\sigma^2) \simeq \mathbf{Z}[\exp(2i\pi/6)]$; donc il existe une unité relative ϵ génératrice , et tout élément u de E_* s'écrit de manière unique

$$(2.2) \quad u = \epsilon^{\lambda + \mu\sigma} , \quad \lambda , \mu \in \mathbf{Z} ,$$

et si $\langle u \rangle$ désigne le sous-module de E_* engendré par u , $u \neq 1$, alors on a (en remarquant que l'isomorphisme ci-dessus envoie σ sur une racine d'ordre 6 de l'unité) :

$$(2.3) \quad (E_* : \langle u \rangle) = \lambda^2 + \lambda\mu + \mu^2 .$$

b) Majoration de l'indice des sous-modules de E_* .

Soit $u \in E_*$, $u \neq 1$. En utilisant le résultat général démontré dans $[G]$, nous obtenons un majorant de l'indice $(E_* : \langle u \rangle)$ qui est du même ordre de grandeur que celui établi dans $[M]$, mais qui utilise le régulateur de u .

(2.4) Définition : On appelle régulateur de $u \in E_*$,

$$R_*(u) = (\text{Log } |u|)^2 + (\text{Log } |u^\sigma|)^2 - (\text{Log } |u|)(\text{Log } |u^\sigma|) .$$

(2.5) Théorème : Si $f \geq 28$, pour toute unité u de E_* , $u \neq 1$, on a

$$(E_* : \langle u \rangle) \leq M_* = \frac{16}{3} \frac{R_*(u)}{\left(\text{Log } \frac{f-20}{4}\right)^2} .$$

(2.6) Lemme : Pour toute unité u de E_* , $u \neq 1$, on a

$$\text{Max}_{i=0, \dots, 5} (\sigma^i(u^2)) \geq \frac{f-20}{4} .$$

Démonstration du lemme : on considère la norme de la résolvante de Lagrange (où $j^3 = 1$, $j \neq 1$) :

$$\begin{aligned} \Phi(u) = & (u - ju^\sigma + j^2 u^{\sigma^2} - u^{\sigma^3} + ju^{\sigma^4} - j^2 u^{\sigma^5}) (u - j^2 u^\sigma + ju^{\sigma^2} \\ & - u^{\sigma^3} + j^2 u^{\sigma^4} - ju^{\sigma^5}) , \end{aligned}$$

c'est-à-dire

$$\begin{aligned} (2.7) \quad \Phi(u) = & (u - u^{\sigma^3})^2 + (u^{\sigma^2} - u^{\sigma^5})^2 + (u^{\sigma^4} - u^\sigma)^2 \\ & - (u - u^{\sigma^3})(u^{\sigma^2} - u^{\sigma^5}) - (u^{\sigma^2} - u^{\sigma^5})(u^{\sigma^4} - u^\sigma) - (u^{\sigma^4} - u^\sigma)(u^{\sigma^2} - u^{\sigma^5}) . \end{aligned}$$

(i) On a $\Phi(u) \neq 0$ si $u \in E_*$, $u \neq 1$. En effet , supposons que

$\Phi(u) = 0$; alors $u - u^{\sigma^3} = u^{\sigma^2} - u^{\sigma^5} = u^{\sigma^4} - u^\sigma = \alpha$, et $\alpha \in k_2$. Puis - que $u^{1+\sigma^3} = 1$, on a $u^2 = \alpha u + 1$, $\alpha \in k_2$, et donc u est de degré sur \mathbb{Q}

inférieur ou égal à 4 , ce qui est impossible, puisque toute unité relative non triviale est un élément primitif de K .

(ii) D'après [G] page 114 , pour tout $u \in E_*$, $u \neq 1$, $\Phi(u)$ est un entier rationnel divisible par f , et si on applique le résultat général page 118 , on obtient $\text{Max}_{i=0, \dots, 5} (\sigma^i(u^2)) \geq \frac{f}{16}$; on va améliorer cette minoration .

(iii) Supposons que $|u|$ soit le plus grand des $|u^{\sigma^i}|$; puisque $u \in E_*$, on a $|u^{\sigma}| |u^{\sigma^5}| = |u|$, et donc $|u^{\sigma}| > 1$. On pose $a = |u|$ et $x = |u^{\sigma}|$; alors $1 < x < a$. Puisque $|u^{\sigma^2}| = |u^{\sigma}| / |u| = x/a$ et que $|u^{\sigma^3}| = 1/a$, $|u^{\sigma^4}| = 1/x$ et $|u^{\sigma^5}| = a/x$, on obtient , en exprimant que f est inférieur ou égal à la somme des valeurs absolues de l'expression (2.7) :

$$f \leq g(x) = \left(1 + \frac{1}{a} + \frac{1}{a^2}\right) \left(x^2 + \frac{a^2}{x^2}\right) + \left(a + 1 + \frac{1}{a} + \frac{1}{a^2}\right) \left(x + \frac{a}{x}\right) + a^2 + a + 6 + \frac{1}{a} + \frac{1}{a^2} .$$

Or $g'(x) = \left(1 + \frac{1}{a} + \frac{1}{a^2}\right) \left(2x - 2\frac{a^2}{x^3}\right) + \left(a + 1 + \frac{1}{a} + \frac{1}{a^2}\right) \left(1 - \frac{a}{x^2}\right)$, et donc $g'(x)$ est du signe de $x^2 - a$. On en déduit que $g(x)$ atteint son maximum en

$$g(1) = g(a) = 3a^2 + 4a + 10 + \frac{4}{a} + \frac{3}{a^2} .$$

$$\text{Or } 4a^2 + 20 - g(1) = \frac{1}{a^2} (a^4 - 4a^3 + 10a^2 - 4a - 3)$$

$$= \frac{1}{a^2} [(a-1)^4 + 4(a-1)(a+1)] \geq 0 \text{ puisque } a \geq 1 ; \text{ donc } a^2 \geq \frac{f-20}{4} , \text{ ce}$$

qui achève la démonstration du lemme .

Démonstration du théorème : On applique le théorème II 1 de [G] page 106 . On considère la fonction norme de la résolvante de Lagrange Φ de degré $d_\Phi = 2$; on obtient , d'après (2.6) , pour tout $u \in E_*$, $u \neq 1$,

$$\text{Max}_{i=0, \dots, 5} (\sigma^i(u^2)) \geq \frac{f-20}{4} > 1 \text{ si } f \geq 28 ;$$

on a donc $(E_* : \langle u \rangle) \leq M_* = \frac{\mathfrak{M}(\langle u \rangle)}{m} \left(\frac{1}{4} \text{Log} \frac{f-20}{4} \right)^{-2}$, où $\frac{\mathfrak{M}(\langle u \rangle)}{m}$ est une constante géométrique explicite, qui se calcule en considérant le plongement logarithmique du groupe des unités de K :

On pose, pour tout $i = 0, \dots, 5$, $y_i = \sigma^i(\text{Log } |u|) = \text{Log } |\sigma^i(u)|$; alors puisque $u \in E_*$, on a

$$(2.8) \quad \begin{cases} y_0 + y_3 = 0 \\ y_1 + y_4 = 0 \\ y_2 + y_5 = 0 \\ y_0 + y_2 + y_4 = 0 \\ y_1 + y_3 + y_5 = 0 \end{cases}$$

relations équivalentes à

$$(2.9) \quad \begin{cases} y_2 = -y_0 + y_1 \\ y_3 = -y_0 \\ y_4 = -y_1 \\ y_5 = y_0 - y_1 \end{cases}$$

Alors, d'après le corollaire II 2, page 111, de [G], on a

$$\frac{\mathfrak{M}(\langle u \rangle)}{m} = \frac{1}{\gamma^2} \frac{\mathfrak{R}(\langle u \rangle)}{\int_V dy_0 dy_1}, \text{ où } \gamma^2 = \frac{6^2}{3} = 12, \text{ où } V \text{ est le domaine de}$$

\mathbb{R}^2 délimité par les droites dont les équations, déduites de (2.9), sont : $|y_0| = 1$, $|y_1| = 1$, $|y_0 - y_1| = 1$ (l'aire de V est égale à 3), et où $\mathfrak{R}(\langle u \rangle) = \Phi(\text{Log } |u|)$, Φ ayant été défini en (2.7) ; on vérifie que $\mathfrak{R}(\langle u \rangle) = 12 R_*(u)$, où $R_*(u)$ est défini en (2.4).

$$\text{On a donc } M_* = \frac{1}{12} \frac{12 R_*(u)}{3} \left(\frac{1}{4} \text{Log} \frac{f-20}{4} \right)^{-2} = \frac{16}{3} \frac{R_*(u)}{\left(\text{Log} \frac{f-20}{4} \right)^2},$$

d'où le théorème (2.5).

(2.10) Remarque : D'après [G] page 112, si on utilise la fonction discriminant Δ de degré $d_\Delta = 6 \times 5 = 30$, on déduit

$$M_* = 1200 \frac{R_*(u)}{\left(\text{Log} \frac{3^9 7^7}{2^{16}} f^2 f_3^2 f_2 \right)^2};$$

cette majoration doit être utilisée si $f = 13, 21$ et donne un résultat meilleur que celle obtenue avec ϕ si $f = 28$ et $f = 37$.

(2.11) Remarque : Dans le cas des extensions cycliques réelles de degré 3 et 4 de \mathbb{Q} (dont on désignera toujours par σ un générateur du groupe de Galois), de conducteurs respectifs f_3 et f_4 , on obtient avec les mêmes notations qu'en (2.1), (2.4) et (2.5) :

(i) cas du degré 3 ([G], p. 119)

$$E_* = \{ u \in E, u^{1+\sigma+\sigma^2} = 1 \}$$

$$R_*(u) = (\text{Log } |u|)^2 + (\text{Log } |u^\sigma|)^2 + (\text{Log } |u|)(\text{Log } |u^\sigma|)$$

$$M_* = 4 \frac{R_*(u)}{\left(\text{Log } \frac{f_3 - 3}{3} \right)^2}$$

(ii) cas du degré 4 ([G(MN)5], p. 11)

$$E_* = \{ |u|, u \in E, u^{1+\sigma^2} = \pm 1 \}$$

$$R_*(u) = (\text{Log } |u|)^2 + (\text{Log } |u^\sigma|)^2$$

$$M_* = 4 \frac{R_*(u)}{\left(\text{Log } \frac{f_4 - 6}{2} \right)^2}.$$

3. Une famille d'extensions cycliques réelles de degré 6 de \mathbb{Q} .

Soit $\Omega = \mathbb{C} - \left\{ -2, -1, -\frac{1}{2}, 0, 1, j, j^2 \right\}$; on vérifie que l'application σ définie par :

$$(3.1) \quad \sigma(\theta) = \frac{\theta - 1}{\theta + 2}, \quad \text{pour tout } \theta \in \Omega,$$

est une bijection d'ordre 6 de Ω sur Ω , et que l'on a $\sigma^2(\theta) = \frac{-1}{\theta + 1}$,

$\sigma^3(\theta) = -\frac{\theta+2}{2\theta+1}$, $\sigma^4(\theta) = -\frac{\theta+1}{\theta}$, $\sigma^5(\theta) = -\frac{2\theta+1}{\theta-1}$ et $\sigma^6(\theta) = \theta$ pour tout $\theta \in \Omega$.

On pose $t = 2 \sum_{i=1}^6 \sigma^i(\theta) + 6$, et on vérifie que les quantités $\sigma^i(\theta)$,

$1 \leq i \leq 6$, sont les six racines distinctes du polynome

$$(3.2) \quad P = X^6 - \frac{t-6}{2}X^5 - 5\frac{t+6}{4}X^4 - 20X^3 + 5\frac{t-6}{4}X^2 + \frac{t+6}{2}X + 1.$$

On suppose que $t \in \mathbb{Z}$; alors $K_t = \mathbb{Q}(\theta)$ est une extension cyclique de \mathbb{Q} de degré diviseur de 6, et elle est réelle (voir (3.4)).

(3.3) Proposition: Si $t \in \mathbb{Z}$, $t \neq 0$, $t \neq \pm 6$, $t \neq \pm 26$, alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration: D'après ce qui précède, on est dans l'un des cas suivants:

(i) P est irréductible dans $\mathbb{Q}[X]$.

(ii) $P = P_1 \sigma(P_1)$, avec $P_1 = (X - \theta)(X - \theta^{\sigma^2})(X - \theta^{\sigma^4}) \in \mathbb{Q}[X]$.

Ce cas a lieu si et seulement si $[K_t : \mathbb{Q}] = 3$. On vérifie que l'on a

$$(3.4) \quad P = \left(X^3 - \frac{t-6}{4}X^2 - \frac{t+6}{4}X - 1 \right)^2 - \frac{t^2+108}{16}(X^2+X)^2,$$

et on en déduit que $\mathbb{Q}(\sqrt{t^2+108}) \subset K_t$ et donc que $[K_t : \mathbb{Q}] = 3$ si et seulement si t^2+108 est un carré dans \mathbb{Z} . Il est alors élémentaire de vérifier que les seules solutions dans \mathbb{Z} de l'équation $t^2+108 = y^2$ sont $t = \pm 6$, $y = \pm 12$ et $t = \pm 26$, $y = \pm 28$.

(iii) $P = P_2 \sigma(P_2) \sigma^2(P_2)$, avec $P_2 = (X - \theta)(X - \theta^{\sigma^3}) \in \mathbb{Q}[X]$.

Ce cas a lieu si et seulement si $[K_t : \mathbb{Q}] = 2$. Soit

$$(3.5) \quad \varphi = \theta^{-1-\sigma^3} = -\frac{2\theta+1}{\theta(\theta+2)};$$

on vérifie que φ est racine de

$$(3.6) \quad A = X^3 - \frac{t-6}{4} X^2 - \frac{t+6}{4} X - 1 ,$$

et donc $[K_t : \mathbb{Q}] = 2$ si et seulement si A a toutes ses racines rationnelles, ce qui est vérifié si et seulement si $\underline{t = 0}$, et ces racines sont $1, -\frac{1}{2}$ et -2 ; on a alors

$$P = (X^2 - 2X - 2) (X^2 + X - \frac{1}{2}) (X^2 + 4X + 1) .$$

$$(iv) P = \prod_{i=0}^5 (X - \theta^{\sigma^i}) , \quad \theta \in \mathbb{Q} .$$

Ce cas a lieu si et seulement si $\theta \in \mathbb{Q}$ et on vérifie que si $\theta \in \{-1, -2, -4, -\frac{1}{2}, -\frac{1}{4}\}$, alors $t \notin \mathbb{Z}$.

(3.7) Remarque: si on change t en $-t$, θ est changé en θ^{-1} ; on peut donc supposer $t \geq 0$.

(3.8) Définition: Soit $t \in \mathbb{N}$, $t \neq 0, 6, 26$. On considère la famille des extensions cycliques réelles de degré 6, $K_t = \mathbb{Q}(\theta)$, où θ est racine du polynôme P défini en (3.2).

(3.9) Proposition: Soit $K_t = \mathbb{Q}(\theta)$ défini en (3.8).

(i) le sous-corps quadratique de K_t est $k_2 = \mathbb{Q}(\sqrt{t^2 + 108})$;

(ii) le conducteur f_2 de k_2 se détermine de la manière suivante : soient p_1, \dots, p_r les nombres premiers impairs qui divisent $t^2 + 108$ à une puissance non congrue à zéro modulo 2; alors :

si $t \not\equiv 0 \pmod{2}$ ou si $t \equiv \pm 6 \pmod{16}$, on a $f_2 = p_1 \dots p_r$,

si $t \equiv 0 \pmod{2}$ et si $t \not\equiv \pm 6 \pmod{16}$, on a $f_2 = 4 p_1 \dots p_r$.

Démonstration: (i) a été démontré en (3.4).

(ii) On étudie $t^2 + 108$ modulo 64 :

si $t \equiv 1 \pmod{2}$, alors $t^2 + 108 \equiv 1 \pmod{4}$;

si $t \equiv 0 \pmod{4}$, alors $t^2 + 108 \equiv 3 \times 4 \pmod{16}$;

si $t \equiv 2 \pmod{4}$, on pose $t = 4n + 6$, alors

$$t^2 + 108 = 16(n^2 + 3n + 9) ;$$

si $n \equiv 0, 1 \pmod{4}$, alors $t \equiv 6, 10 \pmod{16}$, et on a $n^2 + 3n + 9 \equiv 1 \pmod{4}$,

si $n \equiv 2, 3 \pmod{4}$, alors $t = 14, 2 \pmod{16}$, et on a $n^2 + 3n + 9 \equiv 3 \pmod{4}$, d'où le résultat.

(3.10) Proposition : Soit $K_t = \mathbb{Q}(\theta)$ défini en (3-8) .

(i) le sous-corps cubique de K_t est $k_3 = \mathbb{Q}(\varphi)$, où $\varphi = \theta^{-1} - \sigma^3$ et
 $\text{Irr}(\varphi, \mathbb{Q}) = X^3 - \frac{t-6}{4} X^2 - \frac{t+6}{4} X - 1$;

(ii) le conducteur f_3 de k_3 se détermine de la manière suivante :
 soient q_1, \dots, q_s les nombres premiers autres que 2 et 3 qui divisent
 $t^2 + 108$ à une puissance non congrue à zéro modulo 3 ; alors

si $t \not\equiv 0 \pmod{3}$ ou si $t \equiv 0 \pmod{27}$, on a $f_3 = q_1 \dots q_s$,

si $t \equiv 0 \pmod{3}$ et si $t \not\equiv 0 \pmod{27}$, on a $f_3 = 9q_1 \dots q_s$.

Démonstration : (i) a été démontré en (3.5) et (3.6) .

(ii) Le discriminant de $\text{Irr}(\varphi, \mathbb{Q})$ est égal à

$$\left[\left(\frac{t-6}{4} \right)^2 + 3 \frac{t-6}{4} + 9 \right]^2 = \left(\frac{t^2 + 108}{16} \right)^2 . \text{ On écrit}$$

$$t^2 + 108 = 4^a 3^b q_1^{\alpha_1} \dots q_s^{\alpha_s} , \quad \alpha_i = 1 \text{ ou } 2 , \quad i = 1, \dots, s , \quad a = 0 , 1 \text{ ou } 2 , \quad b = 0 , 2 \text{ ou } 3 , \quad q_i \equiv 1 \pmod{3} , \quad q_i \equiv 1 \pmod{3} .$$

La démonstration du résultat est la même que celle qui a été faite pour le cas $t = 4n + 6$ dans [G(MN)4] , pages 5 à 7 .

(3.11) Proposition : Soit $K_t = \mathbb{Q}(\theta)$ défini en (3.8) .

Le conducteur f de K_t se détermine de la manière suivante :

soit m le produit des nombres premiers autres que 2 et 3 qui divisent
 $t^2 + 108$ à une puissance non congrue à zéro modulo 6 ; alors

$$f = 4^k 3^l m , \text{ où}$$

$k = 0$ si $t \equiv 1 \pmod{2}$ ou $t \equiv \pm 6 \pmod{16}$, $k = 1$ sinon ,

$l = 0$ si $t \equiv 1 \pmod{3}$, $l = 1$ si $t \equiv 0 \pmod{27}$, $l = 2$ sinon .

Démonstration : le nombre $t^2 + 108$ s'écrit de manière unique en isolant les puissances de 2 et 3 ,

$$t^2 + 108 = 4^a 3^b x_1 x_2^2 x_3^3 x_4^4 x_5^5 y_6 ,$$

$a = 0 , 1 \text{ ou } 2$, $b = 0 , 2 \text{ ou } 3$, $x_1 , x_2 , x_3 , x_4 , x_5$ sans facteurs carrés et étrangers deux à deux .

Alors , d'après les propositions (3.10) et (3.11) , on a
 $f_2 = 4^k 3^{\iota'} x_1 x_3 x_5$, $f_3 = 9^{\iota''} x_1 x_2 x_4 x_5$, $k, \iota', \iota'' = 0$ ou 1 ,
et donc puisque $f = \text{ppcm}(f_2, f_3)$, $f = 4^k 3^{\iota} x_1 x_2 x_3 x_4 x_5 = 4^k 3^{\iota} m$,
où $\iota = \max(\iota', 2\iota'')$.

On a donc

$$(3.12) \quad t^2 + 108 = 4^a 3^b m \gamma , \quad \gamma \text{ premier à } 2 \text{ et } 3 ,$$

et puisque $f = 4^k 3^{\iota} m$, $k \leq a$, $\iota \leq b$, on a

$$(3.13) \quad t^2 + 108 = f \gamma c .$$

Le tableau (3.14) qui suit donne pour les 16 cas numérotés $i \bullet j$,
les valeurs de $t^2 + 108$, f et c , ce qui démontre et précise la proposi -
tion (3.11) .

(3.14) Conducteur f de K_t .

$t^2 + 108$	$t \equiv \pm 1 \pmod{3}$	$t \equiv \pm 3 \pmod{9}$	$t \equiv \pm 9 \pmod{27}$	$t \equiv 0 \pmod{27}$
f c				
$t \equiv 1 \pmod{2}$	$1 \bullet 1$ $m \gamma$ $m \quad 1$	$1 \bullet 2$ $9m \gamma$ $9m \quad 1$	$1 \bullet 3$ $27m \gamma$ $9m \quad 3$	$1 \bullet 4$ $27m \gamma$ $3m \quad 9$
$t \equiv 0 \pmod{4}$	$2 \bullet 1$ $4m \gamma$ $4m \quad 1$	$2 \bullet 2$ $36m \gamma$ $36m \quad 1$	$2 \bullet 3$ $108m \gamma$ $36m \quad 3$	$2 \bullet 4$ $108m \gamma$ $12m \quad 9$
$t \equiv \pm 2 \pmod{16}$	$3 \bullet 1$ $16m \gamma$ $4m \quad 4$	$3 \bullet 2$ $144m \gamma$ $36m \quad 4$	$3 \bullet 3$ $432m \gamma$ $36m \quad 12$	$3 \bullet 4$ $432m \gamma$ $12m \quad 36$
$t \equiv \pm 6 \pmod{16}$	$4 \bullet 1$ $16m \gamma$ $m \quad 16$	$4 \bullet 2$ $144m \gamma$ $9m \quad 16$	$4 \bullet 3$ $432m \gamma$ $9m \quad 48$	$4 \bullet 4$ $432m \gamma$ $3m \quad 144$

(3.15) Remarque : Pour tout $t \in \mathbb{N}$, $t \neq 0, 6, 26$, on obtient un corps $K_t = \mathbb{Q}(\theta)$ défini en (3.8). Un même corps peut être obtenu pour plusieurs valeurs de t , mais ce nombre de fois est fini. En effet, si f_1, f_2 et f_3 sont donnés, d'après la démonstration de la proposition (3.11), seuls les produits $x_1 x_5$ et $x_2 x_4$ interviennent dans les calculs des conducteurs, ce qui fait un nombre fini de combinaisons possibles pour les puissances des nombres premiers qui divisent x_1, x_5, x_2 et x_4 , à une puissance 6-ième près, mais d'après le théorème de Thue, l'équation $t^2 + 108 = dy^6$ admet un nombre fini de solutions.

4. Le groupe E_* pour les corps K_t .

a) Introduction.

Dans le cas des corps cycliques de degré 3 ou 4, les éléments w_3 et w_4 définis respectivement en (1.1) et (1.3) appartiennent à E_* .

Dans le cas des corps cycliques de degré 6, l'élément θ défini en (3.1) n'appartient pas à E_* . En effet, d'une part θ n'est un entier de K_t que si $t \equiv 2 \pmod{4}$ et d'autre part, pour tout t , on a bien $\theta^{1+\sigma^2+\sigma^4} = 1$ mais $\theta^{1+\sigma^3} \neq 1$.

On considère l'élément $w = \theta^{1-\sigma^3}$ (cf. [M], p. 29) : alors il est évident que $w \in E_*$ si w est un entier de K_t , ce qui résulte de :

(4.1) Proposition : L'élément $w = \theta^{1-\sigma^3}$ est racine du polynôme $Q = (X - 1)^6 - (t^2 + 108)(X^2 + X)^2$.

Démonstration : On a $w = -\frac{\theta(2\theta+1)}{\theta+2}$, d'où l'on déduit

$$w - 1 = -2 \frac{\theta^2 + \theta + 1}{\theta + 2}$$

$$\text{et } w^2 + w = 2 \frac{\theta(\theta-1)(\theta+1)(2\theta+1)(\theta+2)}{(\theta+2)^3}$$

Or il résulte de (3.2) que

$$t = 2 \frac{2\theta^6 + 6\theta^5 - 15\theta^4 - 40\theta^3 - 15\theta^2 + 6\theta + 2}{\theta(\theta-1)(\theta+1)(2\theta+1)(\theta+2)}$$

$$= \frac{4(\theta^2 + \theta + 1)^3 - 54(\theta^2 + \theta)}{(\theta^2 + \theta)(\theta^2 + \theta - 2)(2\theta + 1)},$$

d'où l'on déduit

$$t^2 + 108 = \frac{16(\theta^2 + \theta + 1)^6}{[\theta(\theta-1)(\theta+1)(2\theta+1)(\theta+2)]^2},$$

et donc $(w-1)^6 = (t^2 + 108)(w^2 + w)^2$, c.q.f.d. .

b) Définition et propriétés de l'unité w de E_* .

(4.2) Définition : Pour tout $t \in \mathbb{N}$, $t \neq 0, 6, 26$, soit

$$w = \theta^{1-\sigma^3} = -\frac{\theta(2\theta+1)}{\theta+2},$$

où θ est défini en (3.8) ; on a alors

$$\text{Irr}(w, \mathbb{Q}) = (X-1)^6 - (t^2 + 108)(X^2 + X)^2.$$

(4.3) Proposition : Soit $w \in K_t$ définie en (4.2). Il existe $v \in E_*$ telle que $w = v^{1+\sigma}$ si et seulement si t est de la forme $t = s(s^2 + 9)$, $s \in \mathbb{Z}$.

(4.4) Lemme : Soit K un corps cyclique réel de degré 6, soit $u \in E_*$, soient $q = \text{Tr}_{K/\mathbb{Q}}(u)$ et $r = \text{Tr}_{K/\mathbb{Q}}(uu^\sigma)$. Alors :

(i) $\text{Irr}(u, \mathbb{Q}) = X^6 - qX^5 + (q+r+3)X^4 - (q^2 - 2r - 4)X^3 + (q+r+3)X^2 - qX + 1$;

(ii) une condition nécessaire et suffisante pour qu'il existe $v \in E_*$ telle que $u = v^{1+\sigma}$ est que l'équation diophantienne

$$x^3 - 3(q+3)x - 6q - r - 12 = 0$$

admette une solution $x \in \mathbb{Z}$, et alors $x = \text{Tr}_{K/\mathbb{Q}}(v)$.

Démonstration du lemme :

(i) Un élément u de E_* , $u \neq 1$, est nécessairement un élément primitif de K , et on calcule les fonctions symétriques de u et ses conjugués en tenant compte de la relation (2.1).

(ii) Il existe $v \in E_*$ telle que $u = v^{1+\sigma}$ si et seulement s'il existe $v \in E_*$ telle que $u^{1+\sigma} = v^{3\sigma}$, et d'après [G], pp. 120-122, ceci a lieu si et seulement si

$$B = \prod_{i=1}^6 \left(X - (u^{\sigma^{i-1}} u^{\sigma^i})^{1/3} \right) \in \mathbb{Z}[X] .$$

Pour tout i modulo 6, on pose $v_i = (u^{\sigma^{i-1}} u^{\sigma^i})^{1/3}$, et il résulte de (i) que $B \in \mathbb{Z}[X]$ si et seulement si

$$x = v_0 + v_1 + v_2 + v_3 + v_4 + v_5 \in \mathbb{Z}$$

$$\text{et } y = v_0 v_1 + v_1 v_2 + v_2 v_3 + v_3 v_4 + v_4 v_5 + v_5 v_0 \in \mathbb{Z} .$$

Mais $v_i v_{i+1} = u^{\sigma^i}$, et donc $y = q$. Il en résulte que $B \in \mathbb{Z}[X]$ si et seulement si $x \in \mathbb{Z}$.

On considère les nombres complexes :

$$\begin{aligned} z_1 &= (v_0 + v_2 + v_4) + (v_1 + v_3 + v_5) , \\ z_2 &= j(v_0 + v_2 + v_4) + j^2(v_1 + v_3 + v_5) , \\ z_3 &= j^2(v_0 + v_2 + v_4) + j(v_1 + v_3 + v_5) . \end{aligned}$$

$$\text{Alors } z_1 + z_2 + z_3 = 0 ,$$

$$z_1 z_2 + z_2 z_3 + z_3 z_1 = -3(v_0 + v_2 + v_4)(v_1 + v_3 + v_5) = -3(q+3) ,$$

$$\begin{aligned} \text{et } z_1 z_2 z_3 &= (v_0 + v_2 + v_4)^3 + (v_1 + v_3 + v_5)^3 \\ &= v_0^3 + v_1^3 + v_2^3 + v_3^3 + v_4^3 + v_5^3 + 6v_0 v_1 + 6v_1 v_2 + 6v_2 v_3 + 6v_3 v_4 + 6v_4 v_5 \\ &+ 6v_5 v_0 + 12 = 6q + r + 12 . \end{aligned}$$

Donc $x = v_0 + v_1 + v_2 + v_3 + v_4 + v_5$ est l'unique racine réelle de l'équation $x^3 - 3(q+3)x - 6q - r - 12 = 0$, ce qui achève la démonstration du lemme .

Démonstration de la proposition : On déduit du lemme (4.4) (i) et de l'expression (4.2) de $\text{Irr}(w, \mathbb{Q})$ que $q = 6$ et $r = -t^2 - 102$.

Donc d'après le lemme (4.4) (ii), il existe $v \in E_*$ telle que $w = v^{1+\sigma}$ si et seulement s'il existe $x \in \mathbb{Z}$ tel que

$$(4.5) \quad x^3 - 27x + 54 + t^2 = 0 ,$$

équation qui s'écrit

$$t^2 = -(x-3)^2(6+x).$$

Nécessairement, on a donc $-6-x=s^2$, $s \in \mathbb{Z}$, et alors $t^2 = s^2(s^2+9)^2$; on choisit $s \geq 0$ et alors $t = s(s^2+9)$.

Les solutions de (4.5) sont donc

$$x = -6 - s^2, \quad t = s(s^2 + 9).$$

(4.6) Proposition : Soit $w \in K_t$ définie en (4.2) et soit $R_*(w)$ le régulateur de w défini en (2.4); lorsque $t \rightarrow +\infty$, on a

$$R_*(w) \sim (\text{Log } t)^2.$$

Démonstration : D'après (3.4), on a $P = P_1 \sigma(P_1)$, où

$$P_1 = X^3 - \left(\frac{t-6}{4} + \frac{\sqrt{t^2+108}}{4}\right)X^2 - \left(\frac{t+6}{4} + \frac{\sqrt{t^2+108}}{4}\right)X - 1,$$

polynôme de la forme $X^3 - \alpha X^2 - (\alpha+3)X - 1$, $\alpha \in \mathbb{R}$, et les racines de ce polynôme, lorsque $\alpha \rightarrow +\infty$, sont équivalentes à α , -1 et $-\frac{1}{\alpha}$.

On choisit pour θ la plus grande racine de P_1 ; alors $\theta \sim$

$$\frac{t-6}{4} + \frac{\sqrt{t^2+108}}{4} \sim \frac{t}{2} \text{ lorsque } t \rightarrow \infty, \text{ et donc } w = -\frac{\theta(2\theta+1)}{\theta+2} \sim -t,$$

$$w^\sigma = -\frac{(\theta-1)\theta}{(\theta+1)(\theta+2)} \sim -1, \text{ et alors}$$

$$R_*(w) = (\text{Log } |w|)^2 + (\text{Log } |w^\sigma|)^2 - (\text{Log } |w|)(\text{Log } |w^\sigma|) \sim (\text{Log } t)^2.$$

(4.7) Remarque : Dans le cas des extensions cycliques de degré 3 et 4 définies en (1.1) et (1.3), on a aussi $R_*(w_3) \sim (\text{Log } t)^2$ et $R_*(w_4) \sim (\text{Log } t)^2$, les quantités $R_*(w_3)$ et $R_*(w_4)$ ayant été définies en (2.11).

(4.8) Théorème : Soit $w \in K_t$ ($w \in E_*$) définie en (4.2). Soit f le conducteur de K_t déterminé en (3.14). Si $t \geq 26$ et si $f \geq 28$, alors on a

$$(E_* : \langle w \rangle) \leq M_t = \frac{16}{3} \left(\frac{\text{Log } (t+6)}{\text{Log } \frac{f-20}{4}} \right)^2.$$

Démonstration : ce théorème est une conséquence immédiate du théorème (2.5) et des deux lemmes suivants :

(4.9) Lemme : On a $R_*(w) \leq \left(\max_{i=0, \dots, 5} \text{Log } |w^{\sigma^i}| \right)^2$.

Démonstration : supposons que $|w^{\sigma}|$ soit la plus grande des quantités $|w^{\sigma^i}|$; puisque $w \in E_*$, on a $|w| |w^{\sigma^2}| = |w^{\sigma}|$, et donc $|w| > 1$ et $|w^{\sigma^2}| > 1$; alors

$$\begin{aligned} R_*(w) &= (\text{Log } |w^{\sigma}|)^2 + (\text{Log } |w|)(\text{Log } |w| - \text{Log } |w^{\sigma}|) \\ &= (\text{Log } |w^{\sigma}|)^2 - \text{Log } |w| \text{Log } |w^{\sigma^2}| < (\text{Log } |w^{\sigma}|)^2 \end{aligned}$$

puisque $\text{Log } |w| > 0$ et $\text{Log } |w^{\sigma^2}| > 0$.

(4.10) Lemme : Si $t \geq 26$, la plus grande racine en valeur absolue w de $Q =$

$(X-1)^6 - (t^2 + 108)(X^2 + X)^2$ vérifie

$$\sqrt{t^2 + 108} + 3 < w < t + 6.$$

Démonstration : On a $Q = Q_1 Q_2$, où

$$Q_1 = X^3 - (3 + \sqrt{t^2 + 108})X^2 + (3 - \sqrt{t^2 + 108})X - 1 \quad \text{et}$$

$$Q_2 = X^3 - (3 - \sqrt{t^2 + 108})X^2 + (3 + \sqrt{t^2 + 108})X - 1.$$

On montre d'abord que si $t \geq 9$, les racines u, u' et u'' de Q_1 vérifient

$$-1 < u < -\frac{1}{2} < u' < 0 < 3 + \sqrt{t^2 + 108} < u''$$

et les racines v, v' et v'' de Q_2 vérifient

$$-\sqrt{t^2 + 108} + 3 < v < -2 < 0 < v'' < 1.$$

Donc la plus grande racine en valeur absolue de Q est u'' et elle vérifie

$$u'' > \sqrt{t^2 + 108} + 3.$$

Il reste à montrer que si $t \geq 26$, alors $u'' < t + 6$, et pour cela, il suffit de montrer que $Q(t+6) > 0$. On a

$$Q(t+6) = (t+5)^2 - (t^2 + 108)(t+6)^2(t+7)^2, \quad \text{et on vérifie que si } t \geq 26, \text{ alors } t^2 + 108 \leq (t+2)^2; \text{ donc}$$

$$Q(t+6) \geq (t+5)^6 - (t+2)^2(t+6)^2(t+7)^2, \quad \text{et on a } Q(t+6) > 0 \text{ car } (t+5)^3 - (t+2)(t+6)(t+7) = 7t + 41 > 0.$$

(4.11) Remarque : En ce qui concerne les corps $\mathbb{Q}(w_3)$ et $\mathbb{Q}(w_4)$ définis respectivement en (1.1) et (1.3) , on déduit de [G(MN)1] , p. 36 , qu'avec des notations analogues à celles du théorème (4.8) on a :

(i) cas du degré 3 : si $t \geq 1$, alors

$$(E_* : \langle w_3 \rangle) \leq M_t = 4 \left(\frac{\text{Log}(t+3)}{f_3 - 3} \right)^2 \cdot \frac{1}{\text{Log} \frac{3}{3}}$$

(ii) cas du degré 4 : si $t \geq 5$, alors

$$(E_* : \langle w_4 \rangle) \leq M_t = 4 \left(\frac{\text{Log}(t+4)}{f_4 - 6} \right)^2 \cdot \frac{1}{\text{Log} \frac{4}{2}}$$

c) Générateur de E_* lorsque $t \in T$.

(4.12) Définition : On appelle T l'ensemble des $t \in \mathbb{N}$, $t \neq 0$, tels que $t^2 + 108$ soit sans facteurs carrés , en dehors des puissances de 2 et 3 .

(4.13) Proposition : L'ensemble T est infini .

Démonstration : Elle est analogue à celle de [N] p. 389 .

(4.14) Remarque : Les définitions analogues concernant les corps $\mathbb{Q}(w_3)$ et $\mathbb{Q}(w_4)$ sont :

(i) Cas du degré 3 : On appelle T_3 l'ensemble des $t \in \mathbb{Z}$, $t \geq -1$, tels que $t^2 + 3t + 9$ soit sans facteurs carrés , en dehors des puissances de 3 .

(ii) Cas du degré 4 : On appelle T_4 l'ensemble des $t \in \mathbb{N}$, $t \neq 0$, tels que $t^2 + 16$ soit sans facteurs carrés en dehors des puissances de 2 .

(4.15) Proposition : Soit $t \in T$ et soit $K_t = \mathbb{Q}(w)$, w définie en (4.2) . Soit f le conducteur de K_t ; alors $f = (t^2 + 108) / c$, où c est un entier qui divise 144 .

Démonstration : La proposition résulte immédiatement de (3.13) et

(3.14) en remarquant que $t \in T$ équivaut à $\gamma = 1$.

(4.16) Proposition : Les notations sont celles du théorème (2.5) appliqué à $\langle w \rangle$. Lorsque $t \in T$ et $t \rightarrow +\infty$, alors $M_* \rightarrow 4/3$.

Démonstration : D'après la proposition (4.6) , on a $R_*(w) \sim (\text{Log } t)^2$ lorsque $t \rightarrow +\infty$. Par ailleurs , si $t \in T$, d'après la proposition (4.15) , on a $f = (t^2 + 108)/c$, $1 \leq c \leq 144$, et donc $\text{Log}((f - 20)/4) \sim \text{Log } t^2$,

et donc $M_* = \frac{16}{3} R_*(u) / \left(\text{Log} \frac{f - 20}{4} \right)^2 \rightarrow \frac{4}{3}$ lorsque $t \in T$ et $t \rightarrow +\infty$.

(4.17) Remarque : Avec les notations (2.11) et (4.14) , pour les corps cycliques de degré 3 et 4 , on a $M_* \rightarrow 1$ lorsque $t \in T_3$ ou $t \in T_4$ et $t \rightarrow +\infty$. Le résultat obtenu pour les corps cycliques de degré 6 n'est pas le même, mais pour la famille de corps qui sera définie au d) , on aura $M_* \rightarrow 1$.

(4.18) Théorème : Pour tout $t \in T$, défini en (4.12) , soit $K_t = \mathbb{Q}(w)$ le corps réel cyclique de degré 6 défini par

$$\text{Irr}(w, \mathbb{Q}) = (X - 1)^6 - (t^2 + 108)(X^2 + X)^2$$
 ,
 et soit E_* le module des unités relatives de K_t . Alors si $t \neq 10, 54$, l'unité w est un générateur de E_* .

Démonstration : Pour les corps réels cycliques de degré 6 ainsi définis , on connaît une unité relative . On applique l'algorithme de dévisage des unités (cf. [G] , p. 112) . On cherche s'il existe $\lambda, \mu \in \mathbb{Z}$ et $\epsilon \in E_*$ tels que $w = \epsilon^{\lambda + \mu\sigma}$ pour tout λ, μ tels que

$$\rho = (E_* : \langle w \rangle) = \lambda^2 + \lambda\mu + \mu^2 \leq M_t$$

(cf. théorème (4.8)) . Les seules valeurs possibles de ρ sont $\rho = 3$, $\rho = 4$ et $\rho \geq 7$ ($\rho = 7, 9, 13 \dots$) .

(i) On a $\rho = 3$ si et seulement si $t = s(s^2 + 9)$, $s \in \mathbb{N}$ (d'après la proposition (4.3)) . Alors

$$t^2 + 108 = (s^2 + 3)^2 (s^2 + 12) .$$

D'après (4.15) et (3.12) , on a $t^2 + 108 = 4^a 3^b m$, $a = 0, 1$ ou 2 , $b = 0, 2$ ou 3 , m sans facteurs carrés ; donc nécessairement , $s^2 + 3 \in \{1, 2, 4, 3, 6, 12\}$, ce qui fait un nombre fini de valeurs de s à essayer ; on trouve les deux seules solutions :

$$s = 1, t = 10, t^2 + 108 = 16 \times 13, f = 13$$

$$s = 3, t = 54, t^2 + 108 = 16 \times 27 \times 7, f = 21.$$

Donc si $t \in T$, $t \neq 10, 54$, alors $(E_* : \langle w \rangle) \neq 3$.

(ii) On a $\rho = 4$ si et seulement si il existe $u \in E_*$ telle que $w = u^2$, ce qui est impossible puisque w n'est pas totalement positive (cf. enca-drements du lemme (4.10)).

(iii) Montrons qu'il existe un ensemble fini T_0 , tel que si $t \in T_0$, alors le théorème (4.8) entraîne que $(E_* : \langle w \rangle) < 7$.

D'après ce théorème, si $t \geq 26$ et $f \geq 28$, alors

$$(E_* : \langle w \rangle) \leq M_t = \frac{16}{3} \left(\text{Log}(t+6) / \text{Log} \frac{f-20}{4} \right)^2.$$

Puisque d'après (4.15), $f = (t^2 + 108)/c$, on a

$$M_t = \frac{16}{3} \left(\text{Log}(t+6) / \text{Log} \frac{t^2 + 108 - 20c}{4c} \right)^2.$$

On a donc $M_t < 7$ si et seulement si

$$h(t) = \text{Log} \frac{t^2 + 108 - 20c}{4c} - \frac{4}{\sqrt{21}} \text{Log}(t+6) > 0.$$

$$\text{Or } h'(t) = \frac{2t}{t^2 + 108 - 20c} - \frac{4}{\sqrt{21}} \frac{1}{t+6} > \frac{2t}{t^2 + 88} - \frac{1}{t+6},$$

puisque $c \geq 1$ et $\sqrt{21} > 4$. Donc si $t \geq 9$, $h'(t) > 0$, donc $h(t)$ est croissante ; or $h(t) \rightarrow +\infty$ lorsque $t \rightarrow +\infty$; donc il existe t_0 tel que si $t \geq t_0$, alors $h(t) > 0$, ce qui entraîne $M_t < 7$.

Donc si $f \geq 28$, pour tout $c \geq 1$, il existe $t(c) = \max(t_0, 26)$ tel que si $t \geq t(c)$, alors $(E_* : \langle w \rangle) < 7$. Puisque c divise 144, on en déduit les $t(c)$ possibles :

c	1	3	4	9	12	16	36	48	144
t(c)	26	26	26	30	38	48	93	117	295

En utilisant les congruences modulo 16 et 27 que doit vérifier t selon les valeurs de c , (cf. tableau (3.14)), on obtient que $(E_* : \langle w \rangle) < 7$ si $t \in T - T_0$, où

$$T_0 = [1, 5] \cup [7, 22] \cup \{24, 25, 27, 38, 42, 54, 90\}.$$

(iv) Dans le tableau qui suit, pour chaque valeur de $t \in T_0$, on calcule $t^2 + 108$, et on donne pour le corps K_t correspondant, le n° du cas du tableau (3.14), la valeur de c , le conducteur f de K_t , une valeur approchée de M_* calculée directement (pour $f = 13, 21, 28$ et 37 , M_* est calculée avec le discriminant (2.10)), et la valeur de $(E_* : \langle w \rangle)$ qui est obtenue après avoir testé, lorsque $M_* \geq 7$ s'il existe $u \in E_*$ telle que $w = u^{\lambda + \mu\sigma}$, pour tout $\lambda, \mu \in \mathbb{N}$ tels que $\lambda^2 + \lambda\mu + \mu^2 \leq M_*$. On déduit de ce tableau le théorème (4.18).

t	$t^2 + 108$	cas	c	f	M_*	$(E_* : \langle w \rangle)$
1	109	1 • 1	1	109	2,89	1
2	16.7	3 • 1	4	28	16,92	1
3	9.13	1 • 2	1	117	2,83	1
4	4.31	2 • 1	1	124	2,79	1
5	133	1 • 1	1	133	2,74	1
7	157	1 • 1	1	157	2,63	1
8	4.43	2 • 1	1	172	2,58	1
9	27.7	1 • 3	3	63	6,31	1
10	16.13	4 • 1	16	13	24,83	3
11	229	1 • 1	1	229	2,46	1
12	4.9.7	2 • 2	1	252	2,42	1
13	277	1 • 1	1	277	2,39	1
14	16.19	3 • 1	4	76	6,41	1
15	9.37	1 • 2	1	333	2,33	1
16	4.91	2 • 1	1	364	2,30	1
17	397	1 • 1	1	397	2,28	1
18	16.27	3 • 3	12	36	25,25	1
19	469	1 • 1	1	469	2,23	1
20	4.127	2 • 1	1	508	2,22	1
21	9.61	1 • 2	1	549	2,20	1
22	16.37	4 • 1	16	37	25,73	1
24	4.9.19	2 • 2	1	684	2,16	1
25	733	1 • 1	1	733	2,14	1
27	27.31	1 • 4	9	93	7,11	1
38	16.97	4 • 1	16	97	8,42	1
42	16.9.13	4 • 2	16	117	7,57	1
54	16.27.7	4 • 4	144	21	56,14	3
90	16.27.19	4 • 3	48	171	8,21	1

(4.19) Remarque : En ce qui concerne les corps $\mathbb{Q}(w_3)$ et $\mathbb{Q}(w_4)$ définis respectivement en (1.1) et (1.3) , alors

(i) cas du degré 3 :

si $t \in T_3$ et si $t \neq 3$, alors w_3 est un générateur de E_* .

(ii) cas du degré 4 :

si $t \in T_4$, alors w_4 est un générateur de E_* .

(4.20) Cas particulier : Si $t \equiv 2 \pmod{4}$, on pose $t = 4n + 6$, et alors $t^2 + 108 = 16(n^2 + 3n + 9)$. Alors on a les propriétés suivantes :

(i) Le polynôme P défini en (3.2) appartient à $\mathbb{Z}[X]$ et θ est une unité de K .

(ii) D'après (3.10) , si $\varphi = \theta^{-1} - \sigma^3$, alors $\text{Irr}(\varphi, \mathbb{Q}) = X^3 - nX^2 - (n+3)X - 1$; le corps k_3 fait partie des corps (1.1) et puisque $t \in T$, $n^2 + 3n + 9$ est sans facteurs carrés en dehors des puissances de 3 , et donc si $t \neq 18$ ($n \neq 3$) , alors φ est un générateur de E_3 . Dans ce cas , un générateur de E_* et un générateur de E_3 sont connus .

(4.21) Remarque : Le conducteur f_3 de k_3 s'écrit de manière unique $f_3 = (a_3^2 + 27b_3^2)/4$, a_3 et b_3 de même parité , $a_3 \equiv 1 \pmod{3}$, $b_3 > 0$, et si $t \in T$, les différents cas du tableau (3.14) correspondent à des valeurs précises de a_3 et b_3 . En particulier :

les cas $3 \bullet 1$ et $4 \bullet 1$ correspondent à $b_3 = 1$,

le cas $2 \bullet 1$ correspond à $b_3 = 2$,

le cas $1 \bullet 1$ correspond à $b_3 = 4$.

Si $b_3 = 1$, on obtient des corps cubiques cycliques (1.1) , donc une unité " petite " , mais si $b_3 = 2$ ou $b_3 = 4$, on obtient des corps cubiques cycliques où en général les unités sont " grandes " (cf. tables de $[G(MN)2]$) . Cependant dans les trois cas , il existe une unité relative du corps de degré 6 qui est " petite " .

d) Générateur de E_* lorsque $t = s(s^2 + 9)$, $s \in S$.

(4.22) Définition : On appelle S l'ensemble des $s \in \mathbb{N}$, $s \neq 0, 2$ tels que $s^2 + 3$ et $s^2 + 12$ soient sans facteurs carrés, en dehors des puissances de 2 .

(4.23) Proposition : L'ensemble S est infini .

Démonstration : Pour tout $s \in \mathbf{N}$, $s^2 + 3 \equiv 1 \pmod{3}$ ou $s^2 + 3 \equiv 3 \pmod{9}$; il en est de même pour $s^2 + 12$ et donc 3^2 ne divise pas $s^2 + 3$ et $s^2 + 9$. Les diviseurs premiers de $s^2 + 3$ et $s^2 + 12$ sont congrus à 1 modulo 6 . Le raisonnement est alors classique (cf. [N] p. 389) : on a besoin d'évaluer

$$2 \sum_{n=1}^{\infty} \frac{1}{(6n+1)^2} \leq \sum_{n=1}^{\infty} \left(\frac{1}{(6n-1)^2} + \frac{1}{(6n+1)^2} \right) = \frac{\pi^2}{6} - \frac{1}{4} \frac{\pi^2}{6} - \frac{1}{9} \frac{\pi^2}{8} - 1$$

$$= \frac{\pi^2}{9} - 1 < 0.1 , \text{ et ce nombre est suffisamment petit pour qu'il existe une infinité de } s \in \mathbf{N} \text{ tels que } s^2 + 3 \text{ et } s^2 + 12 \text{ soient sans facteurs carrés .}$$

(4.24) Définition des corps L_s : Pour tout $s \in S$, soit $t = s(s^2 + 9)$; puisque $s \neq 0, 2$, on a $t \notin \{0, 6, 26\}$. On considère le corps cyclique réel de degré 6 $L_s = K_t = \mathbf{Q}(w)$, où w est définie en (4.2) .

(4.25) Proposition : On a $L_s = \mathbf{Q}(v)$, où

$$\text{Irr}(v, \mathbf{Q}) = (X-1)^6 + (s^2 + 12)(X^5 - X^4 - s^2 X^3 - X^2 + X) .$$

Démonstration : Puisque $t = s(s^2 + 9)$, d'après la proposition (4.3), il existe $v \in E_*$ telle que $w = v^{1+\sigma}$ et on a $\text{Tr}_{L_s/\mathbf{Q}}(v) = -6 - s^2$ et $\text{Tr}_{L_s/\mathbf{Q}}(v^{1+\sigma}) = 6$. On applique alors le lemme (4.4) (ii) .

(4.26) Proposition : Soit $s \in S$ et soit $L_s = \mathbf{Q}(v)$ définie en (4.24) et (4.25). Soit f le conducteur de L_s ; alors $f = (s^2 + 3)(s^2 + 12)/e$, où e est un entier qui divise 48 .

Démonstration : Puisque $t = s(s^2 + 9)$, on a

$$t^2 + 108 = (s^2 + 3)^2 (s^2 + 12) ;$$

on applique la proposition (3.11) et on écrit

$$(s^2 + 3)^2 (s^2 + 12) = 4^a 3^b m \gamma ,$$

$a = 0, 1$ ou 2 , $b = 0, 2$ ou 3 , m et γ premiers à 2 et 3 . Puisque $s^2 + 3$ et $s^2 + 12$ sont sans facteurs carrés en dehors de 2 et 3 , m divise $(s^2 + 3)(s^2 + 12)$ et γ divise $(s^2 + 3)$. On pose $e = (s^2 + 3)(s^2 + 12)/f$ (f est de la forme $4^k 3^l m$), et on vérifie que :

si $s \equiv \pm 1 \pmod{3}$, alors $b = 0$ et $t \equiv \pm 1 \pmod{3}$; les corps L_S appartiennent aux familles $2 \bullet 1$, $3 \bullet 1$ ou $4 \bullet 1$ de (3.14) et $e = 1, 4$ ou 16 ;
 si $s \equiv 0 \pmod{3}$, alors $b = 3$ et $t \equiv 0 \pmod{27}$; les corps L_S appartiennent aux familles $2 \bullet 4$, $3 \bullet 4$ ou $4 \bullet 4$ de (3.14) et $e = 3, 12$ ou 48 .

(4.27) Proposition : Les notations sont celles du théorème (2.5) appliqué à $\langle v \rangle$; lorsque $s \in S$ et que $s \rightarrow +\infty$, alors $M_* \rightarrow 1$.

Démonstration : On a $R_*(v) = \frac{1}{3} R_*(w)$, où $w = v^{1+\sigma}$; lorsque $s \rightarrow +\infty$, $t = s(s^2 + 9) \rightarrow +\infty$ et d'après (4.6), $R_*(w) \sim (\text{Log } t)^2 \sim (\text{Log } s^3)^2$. Par ailleurs, si $s \in S$, d'après la proposition (4.26), on a $f = (s^2 + 3)(s^2 + 9)/e$, $1 \leq e \leq 48$, et donc $\text{Log } \frac{f-20}{4} \sim \text{Log } s^4$, lorsque $s \rightarrow +\infty$, et donc

$$M_* = \frac{16}{3} R_*(v) / \left(\text{Log } \frac{f-20}{4} \right)^2 \sim \frac{1}{3} (\text{Log } s^3)^2 / (\text{Log } s^4)^2,$$

et $M_* \rightarrow 1$ lorsque $s \in S$ et $s \rightarrow +\infty$.

(4.28) Remarque : Comme pour les extensions cycliques réelles de degré 3 et 4 , la majoration établie au théorème (2.5) ne peut pas être améliorée pour l'ensemble des extensions cycliques réelles de degré 6 de \mathbb{Q} .

(4.29) Théorème : Pour tout $s \in S$, défini en (4.22), soit $L_S = \mathbb{Q}(v)$ le corps réel cyclique de degré 6 défini par

$$\text{Irr}(v, \mathbb{Q}) = (X - 1)^6 + (t^2 + 12)(X^5 - X^4 - s^2 X^3 - X^2 + X),$$

et soit E_* le module des unités relatives de L_S . Pour tout $s \in S$, l'unité v est un générateur de E_* .

Démonstration : On procède de la même manière que pour démontrer le théorème (4.18).

(i) Pour toute unité v définie en (4.25) il n'existe pas d'unité $u \in E_*$ telle que $v = u^{1+\sigma}$. En effet, d'après le lemme (4.4) (ii), appliqué à

$q = -6 - s^2$ et $r = 6$, il existe $u \in E_*$ telle que $v = u^{1+\sigma}$ si et seulement s'il existe $y \in \mathbb{Z}$ tel que

$$y^3 + 3(s^2 + 3)y + 6s^2 + 18 = 0.$$

Cette équation s'écrit $y^3 + 9y + 18 = -3s^2(y+2)$; on a donc nécessairement $y \equiv 0 \pmod{3}$; alors $y^3 + 9y + 18 \equiv -9 \pmod{27}$ et l'équation donnée est trivialement impossible modulo 27.

(ii) Montrons que si $s \in S$, $s \geq 10$, alors le théorème (4.8) entraîne que $(E_* : \langle v \rangle) < 7$, ce qui est équivalent à $(E_* : \langle w \rangle) < 21$, où $w = v^{1+\sigma}$.

D'après ce théorème, si $s \geq 2$ (alors $t = s(s^2 + 9) \geq 26$), et si $f \geq 28$, on a

$$(E_* : \langle w \rangle) \leq M_s = \frac{16}{3} \left(\frac{\text{Log}(s^3 + 9s + 6)}{\text{Log} \frac{(s^2 + 3)(s^2 + 12) - 20e}{4e}} \right)^2,$$

puisque $f = (s^2 + 3)(s^2 + 12)/e$ d'après (4.26).

Or si $s \geq 3$, il est immédiat que $s^3 + 9s + 6 \leq (s+1)^3$, et si $s \geq 8$, on vérifie, en tenant compte de $e \leq 48$, que $(s^2 + 3)(s^2 + 12) - 20e \geq s^4 \geq 4e(s/4)^4$; donc si $s \geq 8$, on a

$$M_s \leq \frac{16}{3} \left(\frac{\text{Log}(s+1)^3}{\text{Log}(s/4)^4} \right)^2 = 3 \left(\frac{\text{Log}(s+1)}{\text{Log}(s/4)} \right)^2.$$

Donc si $s \geq 8$, on a $M_s < 21$ dès que $\frac{\text{Log}(s+1)}{\text{Log}(s/4)} < \sqrt{7}$, et il est élémentaire de vérifier que cette inégalité est vérifiée dès que $s \geq 10$.

(iii) Il reste à étudier les corps obtenus pour $1 \leq s \leq 9$, $s \neq 2$. Si $s = 1$, alors $t = 10$; si $s = 3$, alors $t = 54$, et $10, 54 \in T$; on a vérifié au théorème (4.18) que $(E_* : \langle w \rangle) = 3$. Pour les six valeurs restantes de s , on obtient le tableau suivant :

s	t	$t^2 + 108$	cas	e	f	M_*
4	100	$19^2 \cdot 28$	$2 \bullet 1$	1	532	4, 93
5	170	$28^2 \cdot 37$	$4 \bullet 1$	4	259	8, 56
6	270	$39^2 \cdot 48$	$3 \bullet 4$	12	156	13, 53
7	406	$52^2 \cdot 61$	$4 \bullet 1$	4	793	6, 98
8	584	$67^2 \cdot 76$	$2 \bullet 1$	1	5092	4, 25
9	810	$84^2 \cdot 93$	$4 \bullet 4$	12	651	9, 37

et on a $M_* < 21$, ce qui achève la démonstration du théorème (4.29).

(4.30) Cas particulier : Si $s \in S$ et si $s = 6r + 3$, alors le conducteur f_2 de k_2 est $f_2 = 36r^2 + 36r + 21$, et on vérifie que l'unité fondamentale ϵ_2 de E_2 est

$$\epsilon_2 = \frac{(12r^2 + 12r + 5) + (2r + 1)\sqrt{36r^2 + 36r + 21}}{2}$$

On a $t = (6r + 3)(36r^2 + 36r + 18) = 4(54r^3 + 81r^2 + 54r + 12) + 6$, et donc d'après (4.20), un générateur ϵ_3 de E_3 est tel que :

$$\text{Irr}(\epsilon_3, \mathbb{Q}) = X^3 - (54r^3 + 81r^2 + 54r + 12)X^2 - (54r^3 + 81r^2 + 54r + 15)X - 1.$$

Enfin, d'après (4.29), un générateur v de E_* est tel que :

$$\text{Irr}(v, \mathbb{Q}) = (X - 1)^6 + (36r^2 + 36r + 21)[X^5 - X^4 - (36r^2 + 36r + 9)^2 X^3 - X^2 + X].$$

Pour ces corps L_S , les cinq générateurs du groupe des unités sont connus explicitement.

BIBLIOGRAPHIE

- [EMT] V. ENNOLA, S. MÄKI et R. TURUNEN - On real cyclic sextic fields, Math. of Computation, vol. 45, n° 17, 1985, 591-611.
- [G] G. GRAS et M.-N. GRAS - Calcul du nombre de classes et des unités des extensions abéliennes réelles de \mathbb{Q} , Bull. Sci. Math., 2^{ème} série, 10, 1977, 97-129.
- [G(MN)1] M.-N. GRAS - Arithmétique des extensions cycliques de \mathbb{Q} de degré 3 et 4, Publications de l'Université de Laval, Québec, 1984, 27-53.
- [G(MN)2] M.-N. GRAS - Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbb{Q} , Journal für die reine und angew. Math., Band 277, 1975, 89-116.
- [G(MN)3] M.-N. GRAS - Special units in real cyclic sextic fields, Math. of Computation, vol. 48, n° 177, 1987.

- [G(MN)4] M.-N. GRAS - Sur les corps cubiques cycliques dont l'anneau des entiers est monogène , Annales Scientifiques de l'Université de Besançon, 3^{ème} série, fasc.6, Mathématiques, 1973, 1-26 .
- [G(MN)5] M.-N. GRAS - Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de \mathbb{Q} , Publications mathématiques de la Faculté des Sciences de Besançon , Théorie des Nombres , 1977-78 , 1-79 .
- [L] H.- W. LEOPOLDT - Über Einheitengruppe und Klassenzahl reeller abelschen Zahlkörper, Abh. Deutsche Akad. Wiss. Berlin , Math. 2, 1954 , 1-48 .
- [M] S. MÄKI - The determination of units in real cyclic sextic fields , Lecture Note in Maths. v. 797, Springer Verlag , 1980 .
- [N] M. NARKIEWICZ - Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw, 1974 .
- [S] D. SHANKS - The Simplest cubic fields , Math. of Computation, vol. 28, 1974, 1137-1152 .

Marie-Nicole GRAS
Université de Besançon et C.N.R.S.
Equipe de Mathématiques
U. A. n° 040741
Faculté des Sciences
F - 25030 BESANCON CEDEX