Journal de Théorie des Nombres
de Bordeaux **13** (2001), 469–482

Groupe des unités pour des extensions diédrales complexes de degré 10 sur Q

par Omar KIHEL

Résumé. Le but de cet article est de montrer qu'un ensemble quelconque de quatre racines des polynômes quintiques $p(x)$ exhibés par H. Darmon forme sous certaines conditions un système fondamental d'unités de la fermeture normale du corps $\mathbf{Q}(\theta)$ où $p(\theta) = 0$.

Abstract. The purpose of this paper is to show that any set of four roots of the quintic polynomials exhibited by H. Darmon forms under certain conditions a fundamental system of units for the corresponding dihedral fields.

1. Introduction

L'étude des propriétés arithmétiques des corps de nombres est souvent liée à la connaissance du groupe des unités de ces corps. Il est donc normal de chercher à exhiber un système fondamental d'unités pour certain corps de nombres ; toutefois, la détermination d'un tel système n'est pas toujours facile. On se contente parfois d'un système indépendant. D. Shanks a étudié dans [15] les corps cubiques simples où les unités apparaissent de manière évidente en fonction d'une variable qui paramétrise ces corps. R. Schoof et L. Washington ont étudié dans [16] une famille de polynômes quintiques trouvés par Emma Lehmer et ont montré qu'un ensemble quelconque de quatre racines forme un système fondamental d'unités pour les corps cycliques correspondants. À partir d'une observation faite par J. Conway (proposition 2.1), H. Darmon dans un travail non publié [6] a exhibé une famille de polynômes de degré 5 dont les corps de décomposition sont des extensions diédrales de degré 10 sur le corps de fonctions $\mathbf{Q}(S,T)$ tels que lorsqu'on spécialise en $S=-2$ ou bien en $S=-4$ avec T entier positif, les racines de ces polynômes sont des unités dans les extensions diédrales correspondantes. Dans la première section de ce travail, on reconstruit la famille de polynômes trouvés par H. Darmon. On montre dans la section 3 qu'en spécialisant en $S=-2$, les extensions diédrales sont non ramifiées

Manuscrit reçu le 4 juillet 1997.

sur leurs sous-corps quadratiques respectifs et en ajustant la méthode de R. Schoof et L. Washington [16], on montre que pour $T > 385000$, quatre racines quelconques des polynômes de Darmon forment un système fondamental d'unités pour ces extensions diédrales. Pour les petites valeurs de T, on montre que l'indice ne peut prendre que les valeurs $1, 5, 11$ ou 16. On exhibe ensuite un système fondamental d'unités pour les sous-corps quintiques. Dans la dernière section, on spécialise en $S = -4$ avec T entier positif ; de la même manière qu'à la section 3, on montre que pour $T > 141590$, quatre racines quelconques des polynômes de Darmon forment un système fondamental d'unités pour les corps diédraux correspendants, et on exhibe également un système fondamental d'unités pour les sous-corps quintiques.

2. Polynômes de degré 5 et extensions diédrales

Passons à l'étude des polynômes de Darmon.

Proposition 2.1. *Soit $\{x_i\}_{i\in\mathbb{N}}$ une suite quelconque satisfaisant la récurrence*

$$x_{i-1}x_{i+1} = x_i + 1. \tag{1}$$

Alors x_i est périodique, de période 5.

Cette affirmation se vérifie par un calcul direct.
Soit

$$p(x) = \prod_{1=1}^{5}(x - \omega_i),$$

un polynôme de degré 5 dont les racines $\omega_1, \dots, \omega_5$ satisfont la récurrence (1), les indices étant lus modulo 5. Posons

$$S = \omega_1 + \omega_2 + \omega_3 + \omega_4 + \omega_5$$

et

$$T = \omega_1\,\omega_2 + \omega_2\,\omega_3 + \omega_3\,\omega_4 + \omega_4\,\omega_5 + \omega_5\,\omega_1.$$

Le polynôme $p(x)$ s'exprime en fonction de S et T. Si h est une expression en fonction des ω_i, notons par $[h]$ la somme des cinq expressions obtenues à partir de h en permutant cycliquement les indices des ω_i. Par exemple, $T = [\omega_1\,\omega_2]$, et $S = [\omega_1]$. Avec cette notation, on a

$$S^2 = [\omega_1^2] + 2\,[\omega_1\,\omega_2] + 2\,[\omega_1\,\omega_3] = [\omega_1^2] + 2\,T + 2\,S + 10,$$

ce qui entraîne

$$[\omega_1^2] = S^2 - 2\,T - 2\,S - 10.$$

Soient $\sigma_1, \ldots, \sigma_5$ les fonctions symétriques élémentaires de Newton. H. Darmon a montré que l'on a alors

$$\begin{aligned}
\sigma_1 &= S,\\
\sigma_2 &= [\omega_1\,\omega_2] + [\omega_1\,\omega_3] = T + S + 5,\\
\sigma_3 &= [\omega_1\,\omega_2\,\omega_3] + [\omega_1\,\omega_2\,\omega_4] = [\omega_2^2 + \omega_2] + [\omega_1\,\omega_3 + \omega_1]\\
&= (S^2 - 2\,T - 2\,S - 10) + 3\,S + 5 = S^2 + S - 2\,T - 5,\\
\sigma_4 &= [\omega_1\,\omega_2\,\omega_3\,\omega_4] = [(\omega_2 + 1)\,(\omega_3 + 1)] = T + 2\,S + 5,\\
\sigma_5 &= \omega_1\,\omega_2\,\omega_3\,\omega_4\,\omega_5 = (\omega_2 + 1)\,(\omega_3 + 1)\,\omega_5 = (\omega_2 + 1)\,(\omega_4 + \omega_5 + 1)\\
&\qquad = S + 3.
\end{aligned}$$

Donc les racines du polynôme

$$p(x) = x^5 - S\,x^4 + (T+S+5)\,x^3 - (S^2+S-2\,T-5)\,x^2 + (T+2\,S+5)\,x - (S+3)$$

de Darmon [6] satisfont la récurrence (1), quelles que soient les valeurs de S et T. Ici S et T sont des polynômes invariants par l'action de Galois. De plus, $p(x)$ est le polynôme le plus général de cette sorte, dépendant des deux paramètres S et T. Soit G le groupe de Galois du polynôme $p(x)$. Comme le polynôme $p(x)$ est de degré 5, alors l'ordre de G est un multiple de 5. Montrons que $G \subseteq D_5$, le groupe diédral d'ordre 10.
Commençons par un lemme.

Lemme 2.1. *Soient* $\mathbf{F}$ *un corps et* $P(x)$ *un polynôme irréductible à coefficients dans* $\mathbf{F}$ *de degré* p *sur* $\mathbf{Q}$ *où* p *est premier. Si toutes les racines de* $P(x)$ *s'expriment d'une manière rationnelle en fonction de* 2 *racines seulement, alors le groupe de Galois de* $P(x)$ *est un sous-groupe résoluble du groupe symétrique* S_p.

Les 5 racines $\omega_1, \ldots, \omega_5$ du polynôme $p(x)$ s'expriment en fonction de ω_1 et ω_2 (récurrence (1)). Alors le groupe de Galois de $p(x)$ est un sous-groupe résoluble du groupe S_5. On sait qu'un sous-groupe résoluble de S_5 est de cardinalité au plus égale à 20. Soit J l'unique sous-groupe (à conjugaison près) résoluble de S_5 contenant 20 éléments. Alors J est engendré par α et β, où

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},$$

et

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

Supposons que le groupe de Galois G est égal à J tout entier. Appliquant l'élément β à la relation $\omega_3\,\omega_5 = \omega_4 + 1$, nous avons alors $\omega_4\,\omega_5 = \omega_1 + 1$. Puisque $\omega_2\,\omega_5 = \omega_1 + 1$, nous obtenons alors que $\omega_2 = \omega_4$. Ce qui donne une contradiction. Ainsi G est un sous-groupe de D_5.

On montre par spécialisation que le groupe G est en fait D_5 tout entier. Il suffit de spécialiser par exemple en $S=-2$ et $T=1$ pour trouver que le groupe de Galois du polynôme $p(x)$ obtenu est le goupe diédral D_5 tout entier. Le corps de décomposition $\tilde{\mathbf{L}}$ de $p(x)$ est donc une extension diédrale de degré dix sur le corps des fonctions $\mathbf{Q}(S,T)$. Le groupe de Galois G est donc engendré par σ et ρ où

$$\begin{cases} \sigma(\omega_1)=\omega_2, & \sigma(\omega_2)=\omega_3, \quad \sigma(\omega_3)=\omega_4, \quad \sigma(\omega_4)=\omega_5, \quad \sigma(\omega_5)=\omega_1, \\ \rho(\omega_1)=\omega_1, & \rho(\omega_2)=\omega_5, \quad \rho(\omega_3)=\omega_4, \quad \rho(\omega_4)=\omega_3, \quad \rho(\omega_5)=\omega_2. \end{cases}$$

Appelons $\tilde{\mathbf{K}}$ le sous-corps de $\tilde{\mathbf{L}}$ fixé par le sous-groupe distingué H de D_5 d'ordre 5, et $\tilde{\mathbf{K}}_i$ $(i=1,\dots,5)$, les cinq sous-corps de $\tilde{\mathbf{L}}$ de degré 5 sur $\mathbf{Q}(S,T)$. Le corps quadratique $\tilde{\mathbf{K}}$ est engendré par l'élément

$$D=([\omega_1^2\omega_2]-[\omega_2^2\omega_1]).$$

Un calcul fait sur ordinateur nous donne que

$$D^2=\Delta(T,S)=-4T^3-(-S^2+48S+140)T^2-(-28S^3-48S^2+370S+800)T$$
$$-(4S^5+4S^4-104S^3-160S^2+700S+1375).$$

Un autre calcul nous permet d'ailleurs de constater que le discriminant de $p(x)$ est égal à

$$(S+3)^2\,\Delta(T,S)^2.$$

3. Groupe des unités quand $S=-2$

En prenant $S=-2$, le polynôme $p(x)$ dont nous noterons les racines θ_1 (la racine réelle), θ_2, θ_3, θ_4, θ_5, devient

$$p(x)=x^5+2\,x^4+(T+3)\,x^3+(2T+3)\,x^2+(T+1)\,x-1$$

et le discriminant de $p(x)$ est $\Delta(T)^2:=\Delta(T,-2)^2$, i.e.

$$\Delta(T)=-4\,T^3-40\,T^2-92\,T-103.$$

Remarque 3.1. Pour la suite de ce travail, on suppose que T est un entier strictement positif et le corps $\tilde{\mathbf{L}}$ devient simplement une extension algébrique diédrale $\mathbf{L}$ de degré 10 sur $\mathbf{Q}$ dont le sous-corps quadratique imaginaire est désormais dénoté $\mathbf{K}$, le sous-corps quintique réel est $\mathbf{K}_1$ et les sous-corps quintiques complexes sont $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$, $\mathbf{K}_5$. De plus, on suppose que $\Delta(T)$ est libre de carrés. Il existe en fait une infinité de T pour lesquels $\Delta(T)$ est libre de carrés.

Théorème 3.1. *Les racines de $p(x)$ engendrent un groupe d'unités de $\mathbf{L}$ de rang 4.*

Preuve. (i) Montrons que pour tout $i = 1, \dots, 5$, les unités θ_i et $\theta_i + 1$ sont indépendantes. Il suffit de le démontrer pour θ_1 et $\theta_1 + 1$.

Soit

$$\theta_1^a(\theta_1 + 1)^b = 1. \tag{2}$$

avec a et b dans $\mathbf{Z}$. Alors $a = 0$ si et seulement si $b = 0$.

Soit $a \neq 0$; appliquons σ, puis σ^4 à (2) ; après avoir multiplié, nous avons alors

$$\begin{aligned}
&(3) \qquad & 1 &= \theta_5^a(\theta_5+1)^b\theta_1^a(\theta_1+1)^b\theta_2^a(\theta_2+1)^b. \\
&(4) \qquad & &= (\theta_5^a\theta_4^b\theta_1^b)(\theta_1^a\theta_5^b\theta_2^b)(\theta_2^a\theta_1^b\theta_3^b). \\
&(5) \qquad & &= (\theta_5\theta_1\theta_2)^a\theta_1^b = (\theta_1(\theta_1+1))^a\theta_1^b.
\end{aligned}$$

D'où

$$\theta_1^{a+b}(\theta_1 + 1)^a = 1. \tag{6}$$

Elevons chaque membre de (2) (resp. (6)) à la puissance a (resp. b). Nous obtenons alors

$$\theta_1^{a^2}(\theta_1 + 1)^{ab} = 1 = \theta_1^{ab+b^2}(\theta_1 + 1)^{ab}.$$

D'où

$$\theta_1^{a^2-ab-b^2} = 1 \ ;$$

comme θ_1 n'est pas racine de l'unité, ceci implique que $a^2 - ab - b^2 = 0$, i.e. $a = b = 0$, d'où une contradiction.

(ii) Montrons maintenant que quatre racines quelconques de $p(x)$ sont des unités indépendantes. Le groupe de Galois agit sur ces unités en les permutant ; il est donc suffisant de montrer que θ_2, θ_3, θ_4 et θ_5 sont indépendantes. Supposons qu'il existe quatre entiers a, b, c, d tels que

$$\theta_2^a\,\theta_3^b\,\theta_4^c\,\theta_5^d = 1. \tag{7}$$

En appliquant la conjugaison complexe ρ à la relation (7), on obtient

$$\theta_5^a\,\theta_4^b\,\theta_3^c\,\theta_2^d = 1. \tag{8}$$

Les relations (7) et (8) nous donnent

$$(\theta_2\,\theta_5)^{a+d}\,(\theta_3\,\theta_4)^{b+c} = 1. \tag{9}$$

Vérifions que $\theta_2\,\theta_5$ et $\theta_3\,\theta_4$ sont deux unités indépendantes. Remarquons que $\theta_3\,\theta_4 = \theta_1^{-1}\,\theta_2^{-1}\,\theta_5^{-1}$; d'après (i), θ_1 et $\theta_2\,\theta_5 = \theta_1 + 1$ sont des unités indépendantes. Il s'ensuit que $\theta_2\,\theta_5$ et $\theta_3\,\theta_4$ sont deux unités indépendantes. On déduit alors de (9) que

$$\left\{ \begin{array}{rcl} a+d &=& 0, \\ b+c &=& 0. \end{array} \right. \tag{10}$$

En appliquant σ à la relation (7) et en utilisant le fait que $\theta_1\,\theta_2\,\theta_3\,\theta_4\,\theta_5 = 1$, on déduit que

$$\theta_2^{-d}\,\theta_3^{a-d}\,\theta_4^{b-d}\,\theta_5^{c-d} = 1. \tag{11}$$

En refaisant le même raisonnement pour l'équation (11), on obtient le système suivant

$$\begin{cases} c - 2\,d & = & 0, \\ a + b - 2\,d & = & 0. \end{cases} \tag{12}$$

Les systèmes (10) et (11) nous donnent $a = b = c = d = 0$. $\square$

Lemme 3.1. *Le discriminant* $D_{\mathbf{K}_i/\mathbf{Q}} = \Delta^2(T)$ *pour tout* $i \in \{1, \dots, 5\}$.

Preuve. Les cinq corps $\mathbf{K}_1, \dots, \mathbf{K}_5$ étant conjugués l'un de l'autre par des éléments de H, alors $D_{\mathbf{K}_1/\mathbf{Q}} = D_{\mathbf{K}_2/\mathbf{Q}} = D_{\mathbf{K}_3/\mathbf{Q}} = D_{\mathbf{K}_4/\mathbf{Q}} = D_{\mathbf{K}_5/\mathbf{Q}}$. De plus $D_{\mathbf{K}_i/\mathbf{Q}}$ divise le discriminant de $p(x)$ qui est égal à $\Delta^2(T)$, de sorte que $\Delta^2(T) = disc(p(x)) = a_i^2\, disc(\mathbf{K}_i)$ pour $a_i \in \mathbf{Z}$. Tout premier divisant $\Delta(T)$ se ramifie dans $\mathbf{L}$ et donc dans $\mathbf{K}_i$ et $\mathbf{K}_j$ (car $\mathbf{K}_i\mathbf{K}_j = \mathbf{L}$) pour $i \neq j$; donc tout premier divisant $\Delta(T)$ divise $D_{\mathbf{K}_i/\mathbf{Q}}$ et par suite $D_{\mathbf{K}_i/Q} = \Delta^2(T)$ pour tout $i \in \{1, \dots, 5\}$, car $\Delta(T)$ est libre de carrés. $\square$

Théorème 3.2. *L'extension* $\mathbf{L}/\mathbf{K}$ *est non ramifiée.*

Preuve. Supposons le contraire. Soit $\mathcal{P}$ un premier de $\mathbf{K}$ qui se ramifie dans $\mathbf{L}$, et soit p le premier de $\mathbf{Q}$ au-dessous de $\mathcal{P}$, c'est-à dire $p = \mathcal{P} \cap \mathbf{Z}$. Alors p se ramifie dans $\mathbf{L}$ et donc dans tous les sous-corps $\mathbf{K}_i$ vu que $\mathbf{L} = \mathbf{K}_i\,\mathbf{K}_j$ pour $i \neq j$. Donc p divise $\Delta(T)$, et par suite se ramifie dans $\mathbf{K}$; alors p se ramifie complètement dans $\mathbf{L}$:

$$p\mathcal{O}_{\mathbf{L}} = \mathcal{P}'^{10}.$$

Si on note par $T(\mathcal{P}')$ le groupe d'inertie de $\mathcal{P}'$ et par $G_i(\mathcal{P}')$ son i-ème groupe de ramification, on obtient alors $T(\mathcal{P}') = G_0(\mathcal{P}') = G$. Les diviseurs premiers de 10 ne se ramifient pas dans $\mathbf{L}$; en effet, 2 et 5 ne divisent pas $\Delta(T)$, donc ne se ramifient dans aucun sous-corps de $\mathbf{L}$. Comme 2 et 5 ne se ramifient pas dans $\mathbf{L}$, et que $e = 10$, alors $p \neq 2$, $p \neq 5$, $e_0 = 10$, de sorte que $G_0(\mathcal{P}')/G_1(\mathcal{P}')$ est cyclique d'ordre $e_0 = 10$, ce qui donne une contradiction car $G = G_0(\mathcal{P}')$ est diédral d'ordre 10. $\square$

Pour $T > 0$, le nombre de plongements réels de $\mathbf{L}$ est égal à 0 ; donc le groupe des unités de $\mathbf{L}$ sur $\mathbf{Q}$ est de rang 4.

Lemme 3.2. *Si* $\varepsilon \in \mathcal{O}^*_{L/Q}$, *alors* $N_{\mathbf{L}/\mathbf{K}}(\varepsilon) = \pm 1$.

Preuve. Le corps quadratique imaginaire $\mathbf{K}$ est différent de $\mathbf{Q}(\sqrt{-1})$ et de $\mathbf{Q}(\sqrt{-3})$ et donc $\mathcal{O}^*_{\mathbf{K}/\mathbf{Q}} = \{\pm 1\}$. $\square$

Il existe un H-homomorphisme α de $\mathcal{O}_{\mathbf{L}}^*$ dans l'anneau de groupe $\mathbb{R}[H]$ donné par

$$\alpha : \quad \varepsilon \quad \longmapsto \quad 2 \sum_{\tau \in H} \log |\tau(\varepsilon)| \cdot \tau.$$

Le noyau de α est l'ensemble des racines de l'unité dans $\mathbf{L}$, i.e. $\{+1, -1\}$. De plus $\alpha(\mathcal{O}_{\mathbf{L}}^*)$ est contenu dans l'idéal d'augmentation

$$V = \{ \sum_{\tau \in H} \alpha_\tau \, \tau : \sum_{\tau \in H} \alpha_\tau = 0\, , \; \alpha_\tau \in \mathbb{R} \}.$$

V est un hyperplan dans $\mathbb{R}^5$, il est donc de dimension réelle égale à 4. Enfin,

$$\alpha(\mathcal{O}_{\mathbf{L}}^*) \cong \mathcal{O}_{\mathbf{L}}^* / \{\pm 1\},$$

qui est un réseau dont le $\mathbf{Z}-$rang est 4 dans V.

Lemme 3.3. $\mathcal{O}_{\mathbf{L}/\mathbf{Q}}^*$ *est un* $\mathbf{Z}[H]-$*module.*

Lemme 3.4. *Il existe un isomorphisme d'anneaux entre* $\mathbf{Z}[\zeta_5]$ *et* $\mathbf{Z}[H]/(N)$ *qui à* σ *associe* ζ_5*, où* $N = 1+\sigma+\sigma^2+\sigma^3+\sigma^4 \in \mathbf{Z}[H]$ *représente la* H*-norme et où* ζ_5 *est une racine primitive cinquième de l'unité.*

Pour un espace vectoriel réel V et $\Lambda \subset V$, un réseau de rang maximal dans V, on note $\text{dét}(\Lambda)$ le volume de V/Λ.

Théorème 3.3. *Soit* V *un espace vectoriel réel de dimension 4 muni d'un produit scalaire. Soit* $\Lambda \subset V$ *un réseau dont le* $\mathbf{Z}-$*rang est 4 et* H *un groupe d'ordre 5 qui agit isométriquement sur* V*. Supposons que* $N = \sum_{\tau \in H} \tau$ *annule* V*. Alors, il existe un vecteur* x*, qui engendre* Λ *comme* H*-module, satisfaisant*

$$\|x\| \leq 2^{\frac{1}{2}} 5^{-\frac{1}{8}} \, d\acute{e}t(\Lambda)^{\frac{1}{4}}.$$

Preuve. Voir le théorème 2.2 de [16]. □

Corollaire 3.1. *Il existe* $\varepsilon \in \mathcal{O}_{\mathbf{L}}^*$ *une unité qui engendre* $\mathcal{O}_{\mathbf{L}}^*/\{\pm 1\}$ *comme* H*-module telle que*

$$\left(\sum_{\tau \in H} \log^2 |\tau(\varepsilon)| \right)^{\frac{1}{2}} \leq 2^{-\frac{1}{2}} R_{\mathbf{L}}{}^{\frac{1}{4}},$$

où $R_{\mathbf{L}}$ *est le régulateur du corps* $\mathbf{L}$.

Preuve. On vient de voir que $\mathcal{O}_{\mathbf{L}}^*/\{+1, -1\}$ est isomorphe à un réseau $\Lambda \subset V$ dont le $\mathbf{Z}$ -rang est 4. On munit l'espace vectoriel V qui est annulé par la H-norme du produit scalaire suivant : pour $x = \sum_{\tau \in H} x_\tau \, \tau$ et $y = \sum_{\tau \in H} y_\tau \, \tau$,

$$< x, y >= \sum_{\tau \in H} x_\tau \, y_\tau.$$

Ici H agit isométriquement sur V. D'après le théorème 3.3, il existe $\varepsilon \in \mathcal{O}_{\mathbf{L}}^*$ tel que $\|\varepsilon\| \leq 2^{\frac{1}{2}}5^{-\frac{1}{8}}\mathrm{dét}(\Lambda)^{\frac{1}{4}}$. On vérifie que $\mathrm{dét}(\Lambda) = \sqrt{5}R_{\mathbf{L}}$ car $r+s=5$, où $r=0$ est le nombre de plongements réels et $s=5$ le nombre de paires de plongements complexes de $\mathbf{L}$. Alors

$$\|\varepsilon\| = 2\Big(\sum_{\tau\in H}\log^2|\tau(\varepsilon)|\Big)^{\frac{1}{2}} \leq 2^{-\frac{1}{2}}R_{\mathbf{L}}{}^{\frac{1}{4}}.$$

$\square$

Remarque 3.2. Soit ε l'unité de $\mathbf{L}$ du corollaire 3.1. Alors ou bien $\mathbf{Q}(\varepsilon) = \mathbf{K}_i$ pour un certain i ou bien $\mathbf{Q}(\varepsilon) = \mathbf{L}$.

Théorème 3.4. *Si $\mathbf{Q}(\varepsilon) = \mathbf{K}_i$ pour un i, alors $R_{\mathbf{L}} \geq \frac{1}{2^4 5^2}\log^4(\frac{\Delta^2(T)}{M})$ pour un $M \leq 2^{20}$.*

Preuve. Soient $\varepsilon_1, \dots, \varepsilon_5$ les conjugués de ε ; on ordonne les ε_i de telle sorte que $|\varepsilon_1| \leq \ldots \leq |\varepsilon_5|$. Alors

$$\begin{aligned}|\Delta^2(T)| = D_{\mathbf{K}_i/\mathbf{Q}} &\leq \prod_{1\leq i<j\leq 5}|\varepsilon_i-\varepsilon_j|^2\\ &= \Big(\prod_{1\leq i<j\leq 5}|1-\frac{\varepsilon_i}{\varepsilon_j}|^2\Big)\Big(\prod_{j=1}^{5}|\varepsilon_j|^{2(j-1)}\Big) \leq M\prod_{j=1}^{5}|\varepsilon_j|^{2(j-3)}.\end{aligned}$$

Dans cette dernière inégalité on utilise le fait que $\prod_{j=1}^{5}|\varepsilon_j|^2 = 1$ et

$$M = \sup_{0<|x_1|\leq\ldots\leq|x_5|}\Big(\prod_{1\leq i<j\leq 5}|1-\frac{x_i}{x_j}|^2\Big).$$

Par conséquent, $\log(|\frac{\Delta^2(T)}{M}|) \leq \sum_{j=1}^{5}2(j-3)\log|\varepsilon_j|$. En utilisant l'inégalité de Cauchy-Schwarz on obtient

$$\log\Big(\frac{|\Delta^2(T)|}{M}\Big) \leq 2\sqrt{10}\Big(\sum_{j=1}^{5}\log^2|\varepsilon_j|\Big)^{\frac{1}{2}}.$$

D'après le corollaire 3.1, on aura

$$R_{\mathbf{L}} \geq \frac{1}{2^4 5^2}\log^4\left(\frac{\Delta^2(T)}{M}\right).$$

$\square$

Théorème 3.5. *Si $\mathbf{Q}(\varepsilon) = \mathbf{L}$, alors $R_{\mathbf{L}} \geq \frac{5^2}{2^{10}}\log^4|\frac{\Delta(T)}{M}|$ pour un $M \leq 2^{10}$.*

Preuve. Rappelons que $\mathbf{K}_1$ est le sous-corps réel de degré 5 de $\mathbf{L}$. Alors $\mathbf{K}_1(\varepsilon) = \mathbf{L}$. On sait que

$$D_{\mathbf{L}/\mathbf{Q}} = N_{\mathbf{K}/\mathbf{Q}}(D_{\mathbf{L}/\mathbf{K}})D^5_{\mathbf{K}/\mathbf{Q}} = \Delta(T)^5 = N_{\mathbf{K}_1/\mathbf{Q}}(D_{\mathbf{L}/\mathbf{K}_1})D^2_{\mathbf{K}_1/\mathbf{Q}} ;$$

donc $N_{\mathbf{K}_1/\mathbf{Q}}(D_{\mathbf{L}/\mathbf{K}_1}) = \Delta(T)$. Sans perte de généralité, on peut supposer que $\log^2|\varepsilon| \geq \log^2|\sigma^i(\varepsilon)|$ pour tout $i \in \{1,2,3,4\}$. De plus $|\mathrm{Disc}(\varepsilon, \rho(\varepsilon))| = |\varepsilon - \rho(\varepsilon)|^2$ et donc $|N_{\mathbf{K}_1/\mathbf{Q}}(D_{\mathbf{L}/\mathbf{K}_1})| = |\Delta(T)| \leq |N_{\mathbf{K}_1/\mathbf{Q}}(\varepsilon - \rho(\varepsilon))|^2$. Alors

$$|\Delta(T)| \leq |\varepsilon - \rho(\varepsilon)|^2|\sigma(\varepsilon) - \rho\sigma^4(\varepsilon)|^2|\sigma^2(\varepsilon) - \rho\sigma^3(\varepsilon)|^2|\sigma^3(\varepsilon) - \rho\sigma^2(\varepsilon)|^2 \times |\sigma^4(\varepsilon) - \rho\sigma(\varepsilon)|^2.$$

Il y a quatre cas à discuter. Discutons ici juste le cas où

$$|\rho\sigma(\epsilon)| = |\sigma(\epsilon)| \geq |\sigma^4(\epsilon)| = |\rho\sigma^4(\epsilon)|,$$

et

$$|\rho\sigma^2(\epsilon)| = |\sigma^2(\epsilon)| \geq |\sigma^3(\epsilon)| = |\rho\sigma^3(\epsilon)|.$$

Les autres cas se traitent de la même manière. Alors

$$\begin{aligned} |\Delta(T)| &\leq M|\varepsilon|^2|\sigma(\varepsilon)|^4|\sigma^2(\varepsilon)|^4 \\ &= M|\sigma(\varepsilon)|^2|\sigma^2(\varepsilon)|^2|\sigma^3(\varepsilon)|^{-2}|\sigma^4(\varepsilon)|^{-2}, \end{aligned}$$

où

$$M = \sup_{\varepsilon \in \mathcal{O}^*_{\mathbf{L}}} \left|1 - \frac{\rho(\varepsilon)}{\varepsilon}\right|^2 \left|1 - \frac{\rho\sigma^4(\varepsilon)}{\sigma(\varepsilon)}\right|^2 \left|1 - \frac{\rho\sigma^3(\varepsilon)}{\sigma^2(\varepsilon)}\right|^2 \left|1 - \frac{\sigma^3(\varepsilon)}{\rho\sigma^2(\varepsilon)}\right|^2 \times \left|1 - \frac{\sigma^4(\varepsilon)}{\rho\sigma(\varepsilon)}\right|^2.$$

Ainsi dans tous les cas, nous avons

$$\begin{aligned} \log\left(\frac{|\Delta(T)|}{M}\right) &\leq 2\left(|\log|\sigma(\varepsilon)|| + \left|\log|\sigma^2(\varepsilon)|\right| + \left|\log|\sigma^3(\varepsilon)|\right| + \left|\log|\sigma^4(\varepsilon)|\right|\right) \\ &\leq 2^2\Big(\sum_{\substack{\tau\in H\\ \tau\neq 1}} \log^2|\tau(\varepsilon)|\Big)^{\frac{1}{2}} \leq 2^2\sqrt{\frac{4}{5}}\Big(\sum_{\tau\in H}\log^2|\tau(\varepsilon)|\Big)^{\frac{1}{2}} \\ &\leq \frac{2^3}{\sqrt{5}}\frac{{R_{\mathbf{L}}}^{\frac{1}{4}}}{\sqrt{2}} \leq \frac{2^3}{\sqrt{10}}{R_{\mathbf{L}}}^{\frac{1}{4}}. \end{aligned}$$

D'où $R_{\mathbf{L}} \geq \frac{5^2}{2^{10}}\log|\frac{\Delta(T)}{M}|^4$ pour un $M \leq 2^{10}$. $\square$

Lemme 3.5. *Les racines θ_i de $p(x)$ dans le corps des complexes vérifient :*
(a) $\log|\theta_1| = -\log(T+3) + \delta_1$,
(b) $\log|\theta_2| = \log|\theta_5| = \frac{1}{2}\log\left(\frac{T+4}{T+3}\right) + \delta_2$,
(c) $\log|\theta_3| = \log|\theta_4| = \frac{1}{2}\log\left(\frac{(T+3)^2}{T+4}\right) + \delta_3$,
avec $|\delta_1| < 0.08$, $|\delta_2| < 10^{-2}$, $|\delta_3| < \frac{9}{2}\ 10^{-2}$.

Preuve. (a) On vérifie sur ordinateur que pour $T > 4$,

$$p((T+3)^{-1}) > 0 > p(1.08\,(T+3)^{-1}).$$

Alors la racine réelle θ_1 de $p(x)$ vérifie

$$(T+3)^{-1} < \theta_1 < 1.08(T+3)^{-1}.$$

Donc $\theta_1 = (1+\delta_1')(T+3)^{-1}$ avec $|\delta_1'| < 0.08$. Par conséquent, $\log|\theta_1| = -\log((T+3)+\delta_1$, où $|\delta_1| \leq |\delta_1'| < 0.08$.

(b) On utilise la récurrence $\theta_2\theta_5 = \theta_1 + 1$, θ_2 et θ_5 étant des complexes conjugués. On obtient que

$$|\theta_2|^2 = |\theta_5|^2 = \theta_2\theta_5 = \theta_1 + 1,$$

ce qui entraîne

$$2\log|\theta_2| = 2\log|\theta_5| = \log|\theta_1 + 1|.$$

Donc

$$\log|\theta_2| = \log|\theta_5| = \frac{1}{2}\log((1+\delta_1)(T+3)^{-1}+1).$$

Ainsi

$$\log|\theta_2| = \log|\theta_5| = \frac{1}{2}\log\left(\frac{T+4}{T+3}\right) + \delta_2,$$

où $\delta_2 \leq \frac{1}{2}\frac{\delta_1}{T+4} < 10^{-2}$ car $T > 0$.

(c) On utilise le fait que $\theta_1\theta_2\theta_3\theta_4\theta_5 = 1$. □

Théorème 3.6. *Pour* $T > 388000$, *les racines de* $p(x)$ *engendrent un groupe d'unités* $\mathcal{U}$ *tel que* $i_{\mathbf{L}} = [\mathcal{O}_{\mathbf{L}}^* : \{+1,-1\}\mathcal{U}] = 1$. *Pour* $T > 86$, $i_{\mathbf{L}} = 1$, 5 *ou* 16.

Preuve. La preuve se fait en trois étapes.
1. Soit $R = R(\theta_2, \theta_3, \theta_4, \theta_5)$, alors $[\mathcal{O}_{\mathbf{L}}^* : \mathcal{U}] = \frac{R}{R_{\mathbf{L}}}$. Les plongements σ de $\mathbf{L}$ dans $\mathbb{C}$ étant tous complexes, alors $R = |\text{dét}(2\log|\sigma^i\theta_j|)_{1\leq i,j\leq 4}|$. Donc $R = 2^4|\text{dét}(\log|\theta_{i+j}|)_{1\leq i,j\leq 4}|$. Or (voir [18], p. 226)

$$R = \frac{2^4}{|H|}\prod_{\chi\neq 1}|\sum_{\tau\in H}\chi(\tau)\log|\tau(\theta_1)||.$$

Par conséquent,

$$R = \frac{2^4}{5}\prod_{\substack{\zeta^5=1\\ \zeta\neq 1}}|\log|\theta_1| + \zeta\log|\theta_2| + \zeta^2\log|\theta_3| + \zeta^3\log|\theta_4| + \zeta^4\log|\theta_5||.$$

En utilisant le lemme 2.5 on obtient

$$R = \frac{2^4}{5}\prod_{\substack{\zeta^5=1\\ \zeta\neq 1}}\left|-\log(T+3) + \frac{\zeta+\zeta^4}{2}\log\left(\frac{T+4}{T+3}\right) + \frac{\zeta^2+\zeta^3}{2}\log\left(\frac{(T+3)^2}{T+4}\right) + D_\zeta\right|$$

où $|D_\zeta| < 0.2$. On vérifie facilement que l'expression de droite prend sa plus grande valeur lorsque $D_\zeta = -0.2$. En utilisant les théorèmes 3.4 et 3.5, on vérifie que $[\mathcal{O}_{\mathbf{L}}^* : \mathcal{U}] = \frac{R}{R_{\mathbf{L}}} < 5$ pour $T > 388000$. Donc $i_{\mathbf{L}} < 5$.
2. $\mathcal{U}$ et $\mathcal{O}_{\mathbf{L}}^*/\{\pm 1\}$ sont tous deux des $\mathbf{Z}[\zeta_5]$-modules. D'après le corollaire 3.1, on peut trouver $\varepsilon \in \mathcal{O}_{\mathbf{L}}^*$ qui engendre $\mathcal{O}_{\mathbf{L}}^*/\{\pm 1\}$ comme $\mathbf{Z}[\zeta_5]$-module. Soit θ une racine de $p(x)$ fixée, $\theta \in \mathcal{O}_{\mathbf{L}}^*$, alors il existe $\alpha \in \mathbf{Z}[\zeta_5]$ tel que $\theta = \pm\alpha\varepsilon$. Le groupe des unités engendré par les racines de $p(x)$ vérifie $\mathcal{U} \cong \mathbf{Z}[\zeta_5]\theta$. Par conséquent

$$\mathcal{O}_{\mathbf{L}}^*/\{\pm 1\}\mathcal{U} \cong \mathbf{Z}[\zeta_5]/\alpha\mathbf{Z}[\zeta_5]$$

comme $\mathbf{Z}[\zeta_5]$-modules. Donc

$$i_{\mathbf{L}} = [\mathcal{O}_{\mathbf{L}}^* : \{+1, -1\}\mathcal{U}] = |\mathrm{Norm}_{\mathbf{Z}[\zeta_5]/\mathbf{Z}}(\alpha)|.$$

Alors si q est la plus grande puissance d'un premier qui divise $i_{\mathbf{L}}$ (i.e. $\mathrm{Norm}_{\mathbf{Z}[\zeta_5]/\mathbf{Z}}(\alpha)$) alors $q \equiv 0$ ou $1 \pmod 5$. Puisque pour $T > 388000$, $i_{\mathbf{L}} < 5$, alors $i_{\mathbf{L}} = 1$. On vérifie que pour $T > 86$, $i_{\mathbf{L}} < 25$; donc les seules valeurs possibles de $i_{\mathbf{L}}$ sont 1, 5, 11 et 16.
3. Montrons maintenant que $i_{\mathbf{L}} \neq 11$. Supposons le contraire. D'après le lemme 3.4, $\mathbf{Z}[\zeta_5] \cong \mathbf{Z}[H]/(N)$ en tant que $H-$modules. On sait que $\mathbf{Z}[\zeta_5]$ est un module sur H et aussi sur le groupe diédral $D_5 =< \sigma,\ \rho : \sigma^5 = id,\ \rho^2 = id$ et $\rho\sigma = \sigma^{-1}\rho >$. On sait que σ agit sur $\mathbf{Z}[\zeta_5]$ comme multiplication par ζ_5.

Déterminons l'action de ρ sur $\mathbf{Z}[\zeta_5]$. Posons alors

$$\rho(1) = u.$$

On obtient que

$$\rho\sigma(1) = \sigma^4\rho(1) = \zeta_5^4\rho(1) = \zeta_5^{-1}\rho(1),$$

et par suite

$$\rho(\zeta_5) = \rho(\sigma(1)) = \zeta_5^{-1}u.$$

En continuant le même processus, on aura

$$\rho(\zeta_5^i) = \zeta_5^{-i}u.$$

Ainsi

$$\rho(x) = \overline{x}\,u \qquad \forall x \in \mathbf{Z}[\zeta_5].$$

Or on sait que $\rho^2 = id$, de sorte que

$$1 = \rho^2(1) = \rho(u) = \overline{u}\,u.$$

Par conséquent u est une unité dans $\mathbf{Z}[\zeta_5]$.

Nous avons

$$i_{\mathbf{L}} = [\mathcal{O}_{\mathbf{L}}^* : \{+1, -1\}\mathcal{U}] = \mathrm{Norm}_{\mathbf{Z}[\zeta_5]/\mathbf{Z}}(\alpha) = 11,$$

donc

$$i_{\mathbf{L}} = \mathrm{Norm}_{\mathbf{Z}[\zeta_5]}(I) = 11,$$

où I est l'idéal principal de $\mathbf{Z}[\zeta_5]$ engendré par α. De plus ρ opère aussi sur l'idéal I et on a

$$\rho(I) = I.$$

Comme u est une unité dans $\mathbf{Z}[\zeta_5]$, on a aussi

$$\rho(I) = \overline{I}\, u = \overline{I}.$$

Ainsi $\overline{I} = I$. On sait que 11 se décompose complètement dans $\mathbf{Z}[\zeta_5]$ et on a

$$11 = \mathcal{P}_1\, \mathcal{P}_2\, \mathcal{P}_3\, \mathcal{P}_4,$$

où $\overline{\mathcal{P}_1} = \mathcal{P}_2$ et $\overline{\mathcal{P}_3} = \mathcal{P}_4$. Alors $\mathcal{P}_i = I$ pour un certain $i \in \{1, 2, 3, 4\}$ ce qui est en contradiction avec $\overline{I} = I$. □

Corollaire 3.2. $\{\theta_i,\, \theta_i + 1\}$ *est un système fondamental d'unités de* $\mathbf{K}_i$, *pour tout* $i \in \{1, \dots , 5\}$.

Preuve. Comme les $\mathbf{K}_i$ sont conjugués l'un de l'autre par des éléments de H (le sous-groupe d'ordre 5 de D_5), il suffit de faire la preuve pour $\mathbf{K}_1$ (le sous-corps réel de degré 5 de $\mathbf{L}$). Rappelons que $\mathbf{K}_1$ a quatre plongements complexes et un plongement réel ; donc son groupe des unités est de rang 2. Comme $\theta_2\, \theta_5 = \theta_1 + 1$ (voir (i) de la preuve du théorème 2.1), alors θ_1 et $\theta_1 + 1$ sont indépendantes. Montrons maintenant qu'elles engendrent le groupe des unités de $\mathbf{K}_1$. Soit u une unité dans $\mathbf{K}_1$, alors u est une unité dans $\mathbf{L}$, et par suite $u = \pm\theta_1^{a_1}\, \theta_2^{a_2}\, \theta_3^{a_3}\, \theta_4^{a_4}$. Soit ρ la conjugaison complexe ; donc $u = \rho(u) = \pm\theta_1^{a_1}\, \theta_5^{a_2}\, \theta_4^{a_3}\, \theta_3^{a_4}$. On déduit alors que $a_3 = a_4$ et $a_2 = 0$, et ainsi $u = \pm\theta_1^{a_1}\, (\theta_3\, \theta_4)^{a_3}$. Comme par ailleurs $\theta_3\, \theta_4 = (\theta_1\, \theta_2\, \theta_5)^{-1} = (\theta_1\, (\theta_1 + 1))^{-1}$, le résultat découle immédiatement. □

Remarque 3.3. On a vérifié sur ordinateur avec PARI que pour les valeurs de T comprises entre 1 et 100, $\{\theta_1,\, \theta_1 + 1\}$ est un système fondamental d'unités de $\mathbf{K}_1$.

4. Groupe des unités quand $S = -4$

Prenons $S = -4$;le polynôme de Darmon dont les racines seront encore dénotées θ_1, θ_2, θ_3, θ_4, θ_5, devient

$$p(x) = x^5 + 4x^4 + (T + 1)x^3 + (2T - 7)x^2 + (T - 3)x + 1,$$

et

$$\Delta(T) = -4\,T^3 + 68\,T^2 - 344T + 401.$$

On garde dans cette section les mêmes notations qu'à la section précedente. On suppose T entier supérieur à 2 ; le corps quadratique $\mathbf{K}$ est alors imaginaire et les racines de $p(x)$ sont des unités dans $\mathbf{L}$. On suppose toujours que $\Delta(T)$ est libre de carrés. De la même manière qu'à la section 3, on montre que pour $T > 141590$ quatre racines de $p(x)$ prises au hasard sont des unités indépendantes et forment un système fondamental d'unités de L. Les théorèmes 3.1, 3.2, 3.3, 3.4 et 3.5 et les lemmes 3.1, 3.2, 3.3 et 3.4 restent vrais et les preuves sont exactement les mêmes. Le lemme 3.5 devient

Lemme 4.1. *Les racines θ_i de $p(x)$ dans $\mathbb{C}$ vérifient :*
(a) $\log|\theta_1| = -\log(T-5) + \delta_1$,
(b) $\log|\theta_2| = \log(\theta_5) = \frac{1}{2}\log(\frac{(T-6)}{T-5}) + \delta_2$,
(c) $\log|\theta_3| = \log(\theta_4) = \frac{1}{2}\log(\frac{(T-5)^2}{T-6}) + \delta_3$,
avec $|\delta_1| < 5\,10^{-3}$, $|\delta_2| < 5/8\ 10^{-3}$, $|\delta_3| < 25/8\,10^{-3}$.

Preuve. (a) On vérifie que pour $T > 14$,

$$P(-1.025(T-5)^{-1}) < 0 < P(-(T-5)^{-1}).$$

Alors la racine réelle θ_1 de $p(x)$ vérifie : $-1.02(T+3)^{-1} < \theta_1 < 1(T+3)^{-1}$, d'où le résultat. Pour (b) et (c) on fait exactement comme dans le lemme 3.5. □

Théorème 4.1. *Pour $T > 141590$, les racines de $p(x)$ engendrent un groupe d'unités $\mathcal{U}$ tel que $i_{\mathbf{L}} = [\mathcal{O}_L^* : \{+1,-1\}\mathcal{U}] = 1$. Pour $T > 50$, $i = 1, 5, 11$ ou 16.*

Preuve. Elle est identique à celle du théorème 3.6. □

Corollaire 4.1. *$\{\theta_i,\ \theta_i + 1\}$ est un système fondamental d'unités de K_i, pour $i \in \{1, \ldots, 5\}$.*

Preuve. Voir la preuve du corollaire 3.2. □

Remerciements. Je tiens à exprimer ma gratitude envers mon directeur de thèse C. Levesque pour ses conseils judicieux et les encouragements qu'il m'a prodigués le long de ce travail. Je tiens aussi à remercier vivement H. Darmon pour m'avoir permis d'utiliser [6], pour les discussions fructueuses que j'ai eues avec lui, et pour le temps énorme qu'il m'a consacré. Je remercie aussi C. Greither pour les discussions que j'ai eues avec lui.

Bibliographie

[1] W. E. H. Berwick, *Algebraic number fields with two independent units.* Proc. London Math. Soc **34** (1932), 360–378.
[2] K. K. Billevič, *Sur les unités d'un corps algébrique de degré 3 ou 4.* Mat. Sbornik N. S. **40** (1956) (en russe).
[3] A. Brumer, *On the group of units of an absolutely cyclic number field of prime degree.* J. Math. Soc. Japan **21** (1969), 357–358.
[4] T. W. Cusick, *Lower bounds for regulators.* Lecture Notes in Math. **1068**, 63–73, Springer, Berlin, 1984.

[5] H. DARMON, *Une famille de polynômes liée à* $X_0(5)$. Notes non publiées, 1993.
[6] H. DARMON, *Note on a polynomial of Emma Lehmer*. Math. Comp. **56** (1991), 795–800.
[7] M. EDWARDS, *Galois Theory*. Graduate Texts in Mathematics **101**, Springer-Verlag, New York, 1984.
[8] M.-N. GRAS, *Special units in real cyclic sextic fields*. Math. Comp. **48** (1987), 179–182.
[9] M. ISHIDA, *Fundamental units of certain algebraic number fields*. Abh. Math. Semi.Univ. Hamburg **39** (1973), 245–250.
[10] K. IWASAWA, *A note on the group of units of an algebraic number field*. J. Math. Pures Appl. **35** (1956), 189–192.
[11] O. LECACHEUX, *Unités d'une famille de corps liés à la courbe* $X_1(25)$. Ann. Inst. Fourier **40** (1990), 237–254.
[12] E. LEHMER, *Connections between Gaussian periods and cyclic units*. Math. Comp. **50** (1988), 535–541.
[13] S. MAKI, *The determination of units in real cyclic sextic fields*. Lecture Notes in Math. **797**, Springer, Berlin, 1980.
[14] D. SHANKS, *The simplest cubic fields*. Math. Comp. **28** (1974), 1137–1152.
[15] R. SCHOOF, L. C. WASHINGTON, *Quintic polynomials and real cyclotomic fields with large class number*. Math. Comp. **50** (1988), 541–555.
[16] H.-J. STENDER, *Lösbare Gleichungen* $ax^n - by^n = c$ *und Grundeinheiten für einige algebraische Zahlkörper vom Grade* $n = 3, 4, 6$. J. Reine Angew. Math. 290 (1977), 24–62.
[17] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1982.
[18] E. WEISS, *First Course in algebra and number theory*. Academic Press, New York-London, 1971.
[19] C. L. Zhao, *The fundamental units in absolutely cyclic number fields of degree five*. Sci. Sinica Ser. A **27** (1984), 27–40.

Omar KIHEL
Department of Mathematics and Computer Sci.
University of Lethbridge
4401 University Drive
Lethbridge, Alberta,
Canada, T1K 3M4
E-mail : kihel@cs.uleth.ca