ACTA ARITHMETICA
LXXII.4 (1995)

Structure galoisienne et corps de classes de rayon de conducteur 2

par

E. J. Gómez Ayala (Bilbao)

Si F est un corps de nombres, on note $\mathfrak{O}_F$ son anneau d'entiers. Soit K un corps quadratique imaginaire, H_K le corps de classes de Hilbert de K, $\mathfrak{p}$ un idéal premier de $\mathfrak{O}_K$ et $K(\mathfrak{p})$ le corps de classes de rayon de K de conducteur $\mathfrak{p}$. L'extension $(K(\mathfrak{p})/H_K)$ peut être considérée comme un analogue elliptique de l'extension cyclotomique $(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ pour un nombre premier p. Mais contrairement au cas cyclotomique, c'est un problème non résolu de savoir s'il existe ou non une base normale de $\mathfrak{O}_{K(\mathfrak{p})}$ sur $\mathfrak{O}_{H_K}$.

Soit $K = \mathbb{Q}(\sqrt{-d})$ avec $d = 11$, 19, 43, 67 ou 163 et soit $K(2)$ le corps de classes de rayon de K de conducteur 2. Le corps $K(2)$ est une extension cubique et modérément ramifiée de K. Le but de cet article est de montrer l'existence d'une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$ et de faire sa construction explicite. Plus précisément, on va démontrer le théorème suivant :

Théorème. *Les racines du polynôme* $X^3 - X^2 + X + 1$ (*resp.* $X^3 - X^2 + X - 163$, $X^3 - X^2 + X - 447$, $X^3 - X^2 + X + 663$, $X^3 - X^2 + X - 15$) *constituent une base normale de* $\mathfrak{O}_{K(2)}$ *sur* $\mathfrak{O}_K$ *pour* $K = \mathbb{Q}(\sqrt{-11})$ (*resp.* $K = \mathbb{Q}(\sqrt{-19})$, $K = \mathbb{Q}(\sqrt{-43})$, $K = \mathbb{Q}(\sqrt{-67})$, $K = \mathbb{Q}(\sqrt{-163})$).

Je remercie R. Schertz ([10]), qui m'a proposé d'examiner ces extensions du point de vue de la structure galoisienne. La démonstration du théorème (§2 et §3) repose sur un critère générale d'existence de base normale d'entiers dans les extensions de Kummer de degré premier qui a été démontré dans [3]. Le point de vue de Schertz, plus dans l'esprit explicite du *Jugendtraum* de Kronecker, est exposé dans le §4.

1. Préliminaires.

Les deux lemmes suivants sont faciles à démontrer.

Lemme 1.1. *Soit* $k \subseteq L \subseteq M$ *une tour d'extensions finies de corps de nombres telles que* (M/k) *et* (L/k) *sont galoisiennes. Si* a *engendre une base normale de* $\mathfrak{O}_M$ *sur* $\mathfrak{O}_k$, *alors* $\mathrm{Tr}_{M/L}(a)$ *engendre une base normale de* $\mathfrak{O}_L$ *sur* $\mathfrak{O}_k$.

Voir [8], Chap. IX, §3, Theorem 3.4. ∎

LEMME 1.2. *Soit L une extension galoisienne finie d'un corps de nombres k, F une extension finie de k et $E = FL$. On suppose que $L \cap F = k$ et que les discriminants $D_{L/k}$ et $D_{F/k}$ sont premiers entre eux. Si a engendre une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_k$, alors a engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.*

C'est une conséquence du fait que $\mathfrak{O}_{FL} = \mathfrak{O}_F\mathfrak{O}_L$ sous les hypothèses du lemme ([6], Chap. III, §3, Proposition 17). ∎

Soit maintenant $K = \mathbb{Q}(\sqrt{-d})$ avec $d = 11$, 19, 43, 67 ou 163, L une extension cubique de K, $F = K(\omega)$ (avec $\omega = \exp(2\pi i/3)$) et $E = FL$ le composé de F et L.

PROPOSITION 1.3. *Soit $a \in \mathfrak{O}_L$. Alors a engendre une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_K$ si et seulement si a engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.*

On a un diagramme de corps et extensions de corps :

$$\begin{array}{ccccc} \mathbb{Q}(\omega) & \xrightarrow{2} & F & \xrightarrow{3} & E \\ {\scriptstyle 2}\uparrow & & {\scriptstyle 2}\uparrow & & {\scriptstyle 2}\uparrow \\ \mathbb{Q} & \xrightarrow{2} & K & \xrightarrow{3} & L \end{array}$$

Supposons que a engendre une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_K$; ceci implique que l'extension (L/K) est modérément ramifiée et par conséquent les discriminants $D_{L/K}$ et $D_{F/K}$ sont premiers entre eux. Puisque $L \cap F = K$, l'élément a engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$, d'après le lemme 1.2.

Réciproquement, soit $\mathrm{Gal}(E/F) = \{1, \sigma, \sigma^2\}$ et supposons que a engendre une base normale $\{a, a^\sigma, a^{\sigma^2}\}$ de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. On a $K \cap \mathbb{Q}(\omega) = \mathbb{Q}$ et les discriminants $D_{K/\mathbb{Q}}$ et $D_{\mathbb{Q}(\omega)/\mathbb{Q}}$ sont premiers entre eux car l'idéal $3\mathbb{Z}$ ne se ramifie pas dans l'extension $(K/\mathbb{Q})$. Soit $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{1, \tau\}$ (avec $\omega^\tau = \omega^2$); puisque ω engendre une base normale $\{\omega, \omega^\tau\}$ de $\mathbb{Z}[\omega]$ sur $\mathbb{Z}$, ω engendre aussi une base normale de $\mathfrak{O}_F$ sur $\mathfrak{O}_K$, d'après le lemme 1.2. Soit ϱ le seul élément de $\mathrm{Gal}(E/K)$ tel que $\omega^\varrho = \omega^\tau$ et ϱ est l'identité sur L, de sorte que $\mathrm{Gal}(E/K) = \{1, \sigma, \sigma^2, \varrho, \sigma\varrho, \sigma^2\varrho\}$. On sait que les produits $\{a\omega, a^\sigma\omega, a^{\sigma^2}\omega, a\omega^\tau, a^\sigma\omega^\tau, a^{\sigma^2}\omega^\tau\}$ constituent une base de $\mathfrak{O}_E$ comme $\mathfrak{O}_K$-module, mais en fait cette base est une base normale, car ces éléments sont les conjugués du produit $a\omega$ sous l'action de $\mathrm{Gal}(E/K)$ compte tenu du fait que $a^\varrho = a$, puisque $a \in \mathfrak{O}_L$. On en déduit que $a\omega$ engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_K$. D'après le lemme 1.1, $\mathrm{Tr}_{E/L}(a\omega)$ engendre une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_K$. Mais $\mathrm{Tr}_{E/L}(a\omega) = -a$ et par conséquent a engendre une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_K$. ∎

On sait que $\mathfrak{O}_K$ est un anneau principal. Soit $K(2)$ le corps de classes de rayon de K de conducteur 2; puisque 2 est inerte dans K, on sait que $K(2)$ est une extension cubique de K ([7], Chap. VIII, §1, Theorem 7). Le

seul idéal premier de K qui se ramifie dans l'extension $(K(2)/K)$ est $2\mathfrak{O}_K$. Par conséquent, l'extension $(K(2)/K)$ est modérément ramifiée.

On connait un critère explicite pour l'existence d'une base normale d'entiers dans une extension de Kummer cubique ([3], Proposition 2.13) :

PROPOSITION 1.4. *Soit E/F une extension de Kummer cubique. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ si et seulement s'il existe $\alpha \in \mathfrak{O}_E$ tel que $\alpha^3 \in \mathfrak{O}_F$, $E = F(\alpha)$, $\alpha \equiv 1 \bmod (1-\omega)$, $\alpha^3\mathfrak{O}_F = \mathfrak{a}\mathfrak{b}^2$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux premiers entre eux et sans facteurs carrés, et $\mathfrak{b}$ est un idéal principal avec un générateur x tel que $x \equiv 1 \bmod 3$. Dans ce cas, $a = (1/3)(1 + \alpha + (\alpha^2/x))$ engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.* ∎

Soit dorénavant $F = K(\omega)$ et $E = K(2)F$ le composé de $K(2)$ et F. D'après les propositions 1.3 et 1.4, il est donc naturel d'étudier d'abord s'il existe ou non une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$, et la réponse à cette question étant positive, comme l'on montre dans le §2, d'essayer ultérieurement d'en tirer une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_K$, ce qui est fait dans le §3.

2. Étude de l'extension de Kummer (E/F)**.** On va montrer qu'il existe une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.

PROPOSITION 2.1. *Soit $K = \mathbb{Q}(\sqrt{-d})$ avec $d = 11,\ 19,\ 43,\ 67$ ou 163, $F = K(\sqrt{-3})$ et $E = K(2)F$ le composé de $K(2)$ et F. Alors il existe une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.*

Examinons les propriétés de l'extension (E/F). On a un diagramme de corps et extensions de corps :

$$\begin{array}{ccccc} \mathbb{Q}(\omega) & \xrightarrow{2} & F & \xrightarrow{3} & E \\ {\scriptstyle 2}\uparrow & & {\scriptstyle 2}\uparrow & & {\scriptstyle 2}\uparrow \\ \mathbb{Q} & \xrightarrow{2} & K & \xrightarrow{3} & K(2) \end{array}$$

Les seuls idéaux premiers de F qui peuvent se ramifier dans l'extension (E/F) sont les idéaux premiers de F qui sont au-dessus de $2\mathfrak{O}_K$. Puisque l'extension $(F/\mathbb{Q})$ n'est pas cyclique, $2\mathfrak{O}_F$ n'est pas un idéal premier de $\mathfrak{O}_F$; il n'est pas non plus ramifié sur $\mathbb{Q}$, car l'idéal $2\mathbb{Z}$ ne se ramifie pas dans $(\mathbb{Q}(\omega)/\mathbb{Q})$ ni dans $(K/\mathbb{Q})$. On a donc $2\mathfrak{O}_F = \mathfrak{p}\mathfrak{q}$ avec $\mathfrak{p}$ et $\mathfrak{q}$ des idéaux premiers distincts de $\mathfrak{O}_F$ et tels que $\mathfrak{q} = \mathfrak{p}^\tau$, où τ est le seul élément non trivial de $\mathrm{Gal}(F/K)$. On sait que $\mathfrak{O}_F$ est principal ([2], Case I); on peut déterminer facilement des générateurs pour ces idéaux premiers de la forme $(1/2)(a\sqrt{-3} + b\sqrt{-d})$ avec $a, b \in \mathbb{Z}$ en résolvant l'équation $3a^2 - db^2 = \pm 8$. On pose $\pi = (1/2)(\sqrt{-3} + \sqrt{-11})$ (resp. $\pi = (1/2)(3\sqrt{-3} + \sqrt{-19})$, $\pi = (1/2)(19\sqrt{-3} + 5\sqrt{-43})$, $\pi = (1/2)(5\sqrt{-3} + \sqrt{-67})$, $\pi = (1/2)(-715\sqrt{-3} + 97\sqrt{-163})$) pour $d = 11$ (resp. pour $d = 19$, $d = 43$, $d = 67$, $d = 163$), $\mathfrak{p} = \pi\mathfrak{O}_F$ et $\mathfrak{q} = \pi^\tau\mathfrak{O}_F$; on remarque que $\pi\pi^\tau = -2$ pour $d = 11$ et $\pi\pi^\tau = 2$ pour les autres valeurs de d.

En fait $E = F(2)$, le corps de classes de rayon de F de conducteur 2. En effet, $K(2) \subseteq F(2)$ par la théorie du corps de classes et par conséquent $E \subseteq F(2)$. Puisque $\mathfrak{O}_F$ est principal, le groupe de Galois de $F(2)$ sur F est isomorphe à $(\mathfrak{O}_F/2\mathfrak{O}_F)^*/\operatorname{Im}(\mathfrak{O}_F^*)$. Le groupe $(\mathfrak{O}_F/2\mathfrak{O}_F)^*$ est un groupe à $\Phi(2) = \Phi(\mathfrak{p}\mathfrak{q}) = \Phi(\mathfrak{p})\Phi(\mathfrak{q}) = 9$ éléments et l'image du groupe engendré par $-\omega$ dans $(\mathfrak{O}_F/2\mathfrak{O}_F)^*$ est à trois éléments. On en déduit que $[F(2) : F] \leq 3$ et par conséquent $E = F(2)$.

Le corps E est une extension galoisienne cubique de F dans laquelle les seuls idéaux premiers de F qui se ramifient sont $\mathfrak{p}$ et $\mathfrak{q}$. De plus, E est la seule extension galoisienne cubique de F qui possède cette propriété. En effet, soit E' une extension galoisienne cubique de F dans laquelle les seuls idéaux premiers de F qui se ramifient sont $\mathfrak{p}$ et $\mathfrak{q}$; par la théorie du corps de classes, il existe $i \geq 1$ et $j \geq 1$ tels que $E' \subseteq F(\mathfrak{p}^i\mathfrak{q}^j)$. Mais le groupe de Galois de $F(\mathfrak{p}^i\mathfrak{q}^j)$ sur F est isomorphe à $(\mathfrak{O}_F/\mathfrak{p}^i\mathfrak{q}^j)^*/\operatorname{Im}(\mathfrak{O}_F^*)$, un groupe abélien à $\Phi(\mathfrak{p}^i\mathfrak{q}^j) = \Phi(\mathfrak{p}^i)\Phi(\mathfrak{q}^j) = 4^{i+j-2}9$ éléments; puisque l'image du groupe engendré par $-\omega$ dans ce groupe est d'ordre 3 ou 6, il n'existe qu'un seul corps L tel que $F \subseteq L \subseteq F(\mathfrak{p}^i\mathfrak{q}^j)$ et $[L : F] = 3$; puisque $F \subseteq E = F(2) \subseteq F(\mathfrak{p}^i\mathfrak{q}^j)$ et $[E : F] = 3$, on a donc $L = E' = E$.

On va montrer qu'il existe $t \in \mathfrak{O}_F^*$ tel que $2\pi t \equiv 1 \bmod (1-\omega)^3$; ce fait impliquera, d'après le critère de ramification de Hecke pour les extensions de Kummer de degré premier ([4], Chap. V, §39, Theorems 118 et 119) que $F((2\pi t)^{1/3})$ est une extension galoisienne cubique de F dans laquelle les seuls idéaux premiers de F qui se ramifient sont $\mathfrak{p}$ et $\mathfrak{q}$ et par conséquent que $E = F((2\pi t)^{1/3})$.

En effet, soit $k = \mathbb{Q}(\sqrt{3d})$ le sous-corps quadratique réel de F. D'après les tables numériques réalisées Bordeaux, $u = 23+4\sqrt{33}$ (resp. $u = 151+20\sqrt{57}$, $u = 16855 + 1484\sqrt{129}$, $u = 515095 + 36332\sqrt{201}$, $u = 7592629975 + 343350596\sqrt{489}$) est l'unité fondamentale de k pour $d = 11$ (resp. pour $d = 19$, $d = 43$, $d = 67$, $d = 163$). Un théorème de Kubota ([5], §3, Satz 2) affirme que si $v^2 = -u$, alors v est une unité fondamentale de F; on obtient ainsi que $v = 2\sqrt{-3}+\sqrt{-11}$ (resp. $v = 5\sqrt{-3}-2\sqrt{-19}$, $v = -53\sqrt{-3}-14\sqrt{-43}$, $v = 293\sqrt{-3} + 62\sqrt{-67}$, $v = 35573\sqrt{-3} + 4826\sqrt{-163}$) est une unité fondamentale de F pour $d = 11$ (resp. pour $d = 19$, $d = 43$, $d = 67$, $d = 163$). Si l'on pose $t = v$ pour d égal à 11, 43, 67 et 163, et $t = v^3$ pour d égal à 19, on vérifie aisément que $2\pi t \equiv 1 \bmod (1-\omega)^3$. De cette congruence on déduit immédiatement que si $x = -\pi t$, alors x est un générateur de $\mathfrak{p}$ tel que $x \equiv 1 \bmod 3$. On remarque que $2pt$ et x sont des nombres réels. Soit α la seul racine cubique réelle de $2\pi t$; alors la proposition 1.4 assure que $a = (1/3)(1 + \alpha + (\alpha^2/x))$ engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. ∎

3. Descente à K. On démontre maintenant le théorème annoncé dans l'introduction.

THÉORÈME. *Les racines du polynôme* X^3-X^2+X+1 (*resp.* $X^3-X^2+X-163$, $X^3-X^2+X-447$, $X^3-X^2+X+663$, X^3-X^2+X-15) *constituent une base normale de* $\mathfrak{O}_{K(2)}$ *sur* $\mathfrak{O}_K$ *pour* $K=\mathbb{Q}(\sqrt{-11})$ (*resp.* $K=\mathbb{Q}(\sqrt{-19})$, $K=\mathbb{Q}(\sqrt{-43})$, $K=\mathbb{Q}(\sqrt{-67})$, $K=\mathbb{Q}(\sqrt{-163})$).

Soit $a=(1/3)(1+\alpha+(\alpha^2/x))$ l'élément de $\mathfrak{O}_E$ qui a été calculé dans la démonstration de la proposition 2.1, c'est-à-dire, α est la seule racine cubique réelle de $2\pi t$ et $x=-\pi t$; on sait que a engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. On veut démontrer que a engendre une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$; d'après la proposition 1.3, il suffit de montrer que $a\in K(2)$.

Pour calculer le polynôme irréductible $P(X)$ de a sur K, il suffit de considérer les conjugués de a sous l'action de $\mathrm{Gal}(K(2)/K)$. Posons $\beta=\alpha^2/x$; alors

$$a=(1/3)(1+\alpha+\beta),\quad b=(1/3)(1+\omega\alpha+\omega^2\beta),\quad c=(1/3)(1+\omega^2\alpha+\omega\beta)$$

sont les racines de $P(X)$ et

$$P(X)=X^3-(a+b+c)X^2+(ab+ac+bc)X-abc.$$

On a

$$a+b+c=1,\qquad ab+ac+bc=(1/3)(1-\alpha\beta),$$
$$abc=(1/27)(1-3\alpha\beta+\alpha^3+\beta^3).$$

On a $\alpha\beta=-2$ et abc égal à -1 (resp. 163, 447, -663, 15) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$). On a donc

$$P(X)=X^3-X^2+X-\lambda,$$

avec $\lambda=-1$ (resp. $\lambda=163$, $\lambda=447$, $\lambda=-663$, $\lambda=15$) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$). Le discriminant Δ de $P(X)$ est égal à $2^2(-11)$ (resp. $2^2 97^2(-19)$, $2^2 3^2 59^2(-43)$, $2^2 3^2 67^2(-67)$, $2^2 3^2(-163)$) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$). Ce fait implique que les racines de $P(X)$ engendrent un corps L de degré 6 sur $\mathbb{Q}$ tel que $\mathrm{Gal}(L/\mathbb{Q})$ est isomorphe au groupe diédrale D_3 et K est la seule extension quadratique de $\mathbb{Q}$ contenue dans L. On a $L\subseteq E$, l'extension E/K est cyclique de degré six et $[L:K]=3$; on a donc $L=K(2)$. Par conséquent, $a\in K(2)$ et a engendre une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$. ∎

Remarque. Le corps $K(2)$ est le corps de décomposition de $P(X)$ sur $\mathbb{Q}$; on ne peut pas donc obtenir l'extension $(K(2)/K)$ comme la translation d'une extension galoisienne de $\mathbb{Q}$. Le corps $K(2)$ est une extension diédrale de $\mathbb{Q}$, de groupe de Galois D_3; J. Martinet et J.-J. Payan ont étudié ce type d'extensions dans leur article [9].

4. Construction d'un générateur avec des fonctions modulaires. Il est sans doute intéressant d'exprimer un générateur de base normale de

$\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$ comme la valeur d'une fonction elliptique ou modulaire; autrement dit, d'exprimer avec des fonctions elliptiques ou modulaires un $\xi \in \mathfrak{O}_{K(2)}$ tel que

$$\begin{aligned} \mathrm{Tr}_{K(2)/K}(\xi) &\in \mathfrak{O}_K^* = \{\pm 1\}, \\ (\xi + \omega\xi^{\sigma} + \omega^2\xi^{\sigma^2})^3\mathfrak{O}_K &= \mathfrak{p}^2\mathfrak{q}, \\ (\xi + \omega^2\xi^{\sigma} + \omega\xi^{\sigma^2})^3\mathfrak{O}_K &= \mathfrak{p}\mathfrak{q}^2, \end{aligned}$$

où $\mathrm{Gal}(K(2)/K) = \{1, \sigma, \sigma^2\}$. Un tel ξ joue pour l'extension $K(2)/K$, du point de vue de la structure galoisienne, le même rôle que joue $\zeta_p = \exp(2\pi i/p)$ pour l'extension cyclotomique $(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

Après avoir démontré le théorème principal contenu dans cet article, R. Schertz m'a montré à Augsburg les calculs qu'il avait réalisés il y a quelques années en utilisant les *Klasseninvarianten* de Weber ([11]), qu'on reproduit dans la suite.

Rappelons qu'on définit la fonction êta de Dedekind sur le demi-plan de Poincaré $\mathbb{H}$ par le produit infini

$$\eta(\tau) = q_\tau^{1/24} \prod_{m=1}^{\infty} (1 - q_\tau^m)$$

avec $q_\tau = \exp(2\pi i\tau)$; il s'agit donc d'une fonction holomorphe de $\mathbb{H}$ dans $\mathbb{C}$. On définit la fonction modulaire de Schläfli f par

$$f(\tau) = q_\tau^{1/48}\, \eta((\tau + 1)/2)/\eta(\tau)$$

([11], p. 86 et p. 114; [1], §6; il faut noter que Birch, suivant Heegner, appelle σ la fonction de Schläfli). La fonction de Schläfli est une fonction modulaire de niveau 48 définie dans un sous-groupe de $\Gamma(1)$ d'indice 72.

Soit $K = \mathbb{Q}(\sqrt{-d})$ avec $d = 11$, 19, 43, 67 ou 163. On sait que $f(\sqrt{-d})$ est réel et possitif ([1], p. 291), que $K(2) = K(f(\sqrt{-d}))$ et que $f(\sqrt{-d})$ est un entier algébrique. On connait le polynôme irréductible $Q(X)$ de $f(\sqrt{-d})$ sur K; en fait, $f(\sqrt{-d})$ engendre une extension cubique non galoisienne de $\mathbb{Q}$ et $Q(X)$ est à coefficients entiers. On a $Q(X)$ égal à ([11], p. 475) :

$$\begin{aligned} &X^3 - 2X^2 + 2X - 2 && \text{pour } d = 11, \\ &X^3 - 2X - 2 && \text{pour } d = 19, \\ &X^3 - 2X^2 - 2 && \text{pour } d = 43, \\ &X^3 - 2X^2 - 2X - 2 && \text{pour } d = 67, \\ &X^3 - 6X^2 + 4X - 2 && \text{pour } d = 163. \end{aligned}$$

Soit $\xi \in \mathfrak{O}_{K(2)}$ un entier de la forme

$$\xi = u + xf(\sqrt{-d}) + yf(\sqrt{-d})^2$$

avec $u, x, y \in \mathbb{Z}$. Soit $\mathrm{Gal}(K(2)/K) = \{1, \sigma, \sigma^2\}$, $\omega = \exp(2\pi i/3)$ et

$$(\xi|1) = \xi + \xi^{\sigma} + \xi^{\sigma^2},$$
$$(\xi|\sigma) = \xi + \omega\xi^{\sigma} + \omega^2\xi^{\sigma^2},$$
$$(\xi|\sigma^2) = \xi + \omega^2\xi^{\sigma} + \omega\xi^{\sigma^2},$$

les trois résolvantes associées à $\mathrm{Gal}(K(2)/K)$ et construites sur ξ.

Appelons $\alpha = f(\sqrt{-d})$, $\beta = \alpha^{\sigma}$ et $\gamma = \alpha^{\sigma^2}$ les trois racines de $Q(X)$. Alors on a

$$(\xi|\sigma)(\xi|\sigma^2) = rx^2 + sxy + ty^2,$$

avec

$$r = \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \alpha\gamma - \beta\gamma,$$
$$s = 2\alpha^3 + 2\beta^3 + 2\gamma^3 - \alpha\beta^2 - \alpha\gamma^2 - \beta\gamma^2 - \alpha^2\beta - \alpha^2\gamma - \beta^2\gamma,$$
$$t = \alpha^4 + \beta^4 + \gamma^4 - \alpha^2\beta^2 - \alpha^2\gamma^2 - \beta^2\gamma^2.$$

Les coefficients r, s et t sont des fonctions symétriques en α, β et γ, c'est-à-dire, des nombres entiers. Si l'on fait le calcul, on obtient

$$(\xi|\sigma)(\xi|\sigma^2) = 2R(x, y),$$

avec $R(x, y)$ égal à

$$\begin{aligned}
&-x^2 + 3xy + 6y^2 && \text{pour } d = 11,\\
&3x^2 + 9xy + 2y^2 && \text{pour } d = 19,\\
&2x^2 + 17xy + 20y^2 && \text{pour } d = 43,\\
&5x^2 + 31xy + 38y^2 && \text{pour } d = 67,\\
&12x^2 + 141xy + 404y^2 && \text{pour } d = 163.
\end{aligned}$$

Supposons qu'on a trouvé un $(u, x, y) \in \mathbb{Z}^3$ tel que l'entier ξ associé,

$$\xi = u + xf(\sqrt{-d}) + yf(\sqrt{-d})^2,$$

vérifie $(\xi|1) = \pm 1$ et que $R(x, y) = \pm 1$. Puisque $D_{K(2)/K} = 4\mathfrak{O}_K$, on aura pour ξ l'égalité

$$((\xi|1)^2(\xi|\sigma)^2(\xi|\sigma^2)^2)\mathfrak{O}_K = D_{K(2)/K}.$$

Mais

$$D_{K(2)/K}(\xi, \xi^{\sigma}, \xi^{\sigma^2}) = (\xi|1)^2(\xi|\sigma)^2(\xi|\sigma^2)^2,$$

donc

$$D_{K(2)/K}(\xi, \xi^{\sigma}, \xi^{\sigma^2}) = D_{K(2)/K},$$

et par conséquent ξ engendre une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$.

Il est facile de trouver des couples $(x, y) \in \mathbb{Z}^2$ tels que $R(x, y) = -1$. Prenons, par exemple, (x, y) égal à $(1, 0)$ (resp. $(-1, 4)$, $(7, -1)$, $(9, -2)$, $(5, -1)$) pour $d = 11$ (resp. $d = 19$, $d = 43$, $d = 67$, $d = 163$).

On a

$$(\xi|1) = 3u + (\alpha+\beta+\gamma)x + (\alpha^2+\beta^2+\gamma^2)y.$$

Puisque $\alpha+\beta+\gamma$ est égal à 2 (resp. 0, 2, 2, 6) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$) et $\alpha^2+\beta^2+\gamma^2$ est égal à 0 (resp. 4, 4, 8, 28) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$), si l'on considère le vecteur (u,x,y) égal à $(-1,1,0)$ (resp. $(-5,-1,4)$, $(-3,7,-1)$, $(-1,9,-2)$, $(-1,5,-1)$) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$) et ξ l'entier correspondant, on a $(\xi|1)=1$ pour d égal à 19 et 43 et $(\xi|1)=-1$ pour d égal à 11, 67 et 163. On a donc montré le théorème suivant :

THÉORÈME (Schertz). *Soit $K=\mathbb{Q}(\sqrt{-d})$, f la fonction modulaire de Schläfli et $\xi = u + xf(\sqrt{-d}) + yf(\sqrt{-d})^2$ avec (u,x,y) égal à $(-1,1,0)$ (resp. $(-5,-1,4)$, $(-3,7,-1)$, $(-1,9,-2)$, $(-1,5,-1)$) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$). Alors ξ engendre une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$ pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$).* ∎

Soit j la fonction modulaire de Klein. On sait que $j(\sqrt{-d})$ est un entier pour d égal à 11, 19, 43, 67 et 163. Plus précisément, $j(\sqrt{-d})$ est égal à -2^{15} (resp. $-2^{15}3^3$, $-2^{18}3^35^3$, $-2^{15}3^35^311^3$, $-2^{18}3^35^323^329^3$) pour $d=11$ (resp. $d=19$, $d=43$, $d=67$, $d=163$). Grâce à la formule d'interpolation de Lagrange, il est possible de construire trois polynômes $R(X)$, $S(X)$ et $T(X)$ à coefficients rationnels et de degré inférieur ou égal à quatre tels que le vecteur $(R(j(\sqrt{-d})), S(j(\sqrt{-d})), T(j(\sqrt{-d})))$ coïncide avec le vecteur (u,x,y) du théorème précédent. Alors la fonction g définie par

$$g = R(j) + S(j)f + T(j)f^2$$

est une fonction modulaire pour un sous-groupe Δ de $\Gamma(1)$ d'indice 72 qui contient $\Gamma(48)$ et $g(\sqrt{-d})$ est égale à la valeur ξ du théorème pour les cinq valeurs de d qui nous intéressent. On a donc le corollaire suivant.

COROLLAIRE. *Soit $K=\mathbb{Q}(\sqrt{-d})$ avec d égal à* 11, 19, 43, 67 *et* 163 *et soit $\tau \in \mathbb{H}$ tel que $\mathfrak{O}_K = \mathbb{Z}\tau + \mathbb{Z}$. Il existe une fonction g modulaire pour un sous-groupe Δ de $\Gamma(1)$ d'indice* 72 *qui contient $\Gamma(48)$ telle que $g(\tau)$ engendre une base normale de $\mathfrak{O}_{K(2)}$ sur $\mathfrak{O}_K$.* ∎

Bibliographie

[1] B. J. Birch, *Weber's class invariants*, Mathematika 16 (1969), 283–294.

[2] E. Brown and C. J. Parry, *The imaginary bicyclic biquadratic fields with class-number* 1, J. Reine Angew. Math. 260 (1973), 118–120.

[3] E. J. Gómez Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier*, J. Théor. Nombres Bordeaux 6 (1994), 95–116.

[4] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, New York, 1981.
[5] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. 10 (1956), 65–85.
[6] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.
[7] —, *Elliptic Functions*, 2nd ed., Springer, New York, 1987.
[8] R. L. Long, *Algebraic Number Theory*, Marcel Dekker, New York, 1977.
[9] J. Martinet et J.-J. Payan, *Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne*, J. Reine Angew. Math. 228 (1967), 15–37.
[10] R. Schertz, lettre à Ph. Cassou-Noguès du 4-2-91.
[11] H. Weber, *Lehrbuch der Algebra*, Bd. III, Braunschweig, 1908.

DEPARTAMENTO DE MATEMÁTICAS
FACULTAD DE CIENCIAS
UNIVERSIDAD DEL PAÍS VASCO
APARTADO 644
48080 BILBAO, ESPAÑA
E-mail: MTPGOAYE@LG.EHU.ES

Reçu le 30.9.1994 (2675)