

EXTENSIONS DIEDRALES DE DEGRE 2ℓ (ℓ PREMIER ≥ 5)
CONTENANT UN CORPS QUADRATIQUE IMAGINAIRE EUCLIDIEN
ET ORDRES MONOGENES

Jean COGNARD

Extensions diédrales de degré 2ℓ (ℓ premier ≥ 5)
contenant un corps quadratique imaginaire euclidien
et ordres monogènes

par Jean COUGNARD

§1 Introduction .

Soit N/K une extension algébrique de degré fini de corps de nombres ; \mathbb{Z}_N et \mathbb{Z}_K désignant la clôture intégrale de \mathbb{Z} dans chacun de ces corps , on dit que \mathbb{Z}_N est \mathbb{Z}_K -monogène s'il existe un élément θ de N tel que $\mathbb{Z}_N = \mathbb{Z}_K[\theta]$. On se propose de démontrer :

Théorème . Soit K un corps quadratique imaginaire dont l'anneau des entiers \mathbb{Z}_K est euclidien et N/\mathbb{Q} une extension diédrale de degré 2ℓ (ℓ premier ≥ 5) contenant K , alors \mathbb{Z}_N n'est pas \mathbb{Z}_K -monogène , sauf éventuellement pour une des extensions diédrales de degré 14 contenant $\mathbb{Q}(j)$ et de conducteur relatif $7^2 \times 43$.

§2 Rappels .

Désignons par w le nombre des racines de l'unité contenues dans K . Dans un travail précédent [Co] on avait utilisé la méthode développée par M.N. Gras ([G1], [G2]) pour les extensions abéliennes de \mathbb{Q} et on avait démontré les résultats suivants (avec les mêmes notations) :

Pour que \mathbb{Z}_N soit \mathbb{Z}_K -monogène il faut :

- soit que N/K soit non ramifiée ,
- soit que $p = w\ell + 1$ soit premier et que au plus les idéaux au-dessus de p soient ramifiés dans N/K ,
- soit que $w = 4$, $\ell = 5$ et seuls les idéaux au-dessus de 5 soient ramifiés dans N/K ,
- soit que $w = 6$, $\ell = 7$ et seuls les idéaux au-dessus de 7 ou 43 soient ramifiés dans N/K .

On va décomposer la démonstration du théorème en deux parties. Dans la première on suppose que le discriminant $\Delta(N/K)$ de N/K est la puissance d'un idéal premier de \mathbb{Z} ; dans la seconde on suppose que $w = 6$, $\ell = 7$ et $\Delta(N/K) = (7^2 \times 43)^6$.

Dans la première partie de la démonstration on a soit $p = w \ell + 1$ premier, soit $w \neq 2$ et $\ell = w + 1$ premier. Notons par q le nombre premier égal soit à p , soit à ℓ tel que $\Delta(N/K)$ soit une puissance de q . On se place dans une situation un peu plus générale que celle de l'énoncé et on fait les hypothèses :

- H1- le nombre de classes de K est premier à ℓ
- H2- les idéaux premiers de \mathbb{Z}_K au-dessus de q sont principaux
- H3- $K = \mathbb{Q}(\sqrt{-d})$, d entier > 0 avec $d \not\equiv 19 \pmod{24}$.

Remarquons que les corps quadratiques imaginaires dont l'anneau des entiers est principal sont les $\mathbb{Q}(\sqrt{-d})$ avec $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ et que parmi eux seuls ceux où $d \not\equiv 19 \pmod{24}$ ont un anneau d'entiers euclidien.

Le discriminant $\Delta(N/K)$ est la puissance $(\ell - 1)$ -ème d'un idéal \mathfrak{f} engendré par un élément de \mathbb{Z} et norme dans N/K d'un idéal entier \mathfrak{F} de N . Par ailleurs si $\mathbb{Z}_N = \mathbb{Z}_K[\theta]$, il est facile de démontrer que $\mathfrak{F} = (\theta - \sigma(\theta))$ où σ désigne un générateur de $\text{Gal}(N/K)$. Pour démontrer le théorème, il suffit de prouver que \mathfrak{F} n'est pas principal et pour cela de constater que le Frobenius de l'idéal \mathfrak{F} dans une extension non ramifiée de N n'est pas réduit à l'élément neutre.

Dans les paragraphes 3, 4, 5 on traite le premier cas, l'idéal \mathfrak{f} est engendré par le nombre premier q et les hypothèses H1, H2, H3 sont supposées vérifiées.

§3 Problèmes de ramification.

Lorsque $q = \ell = w + 1$ avec $w \neq 2$, il est évident que q est décomposé dans \mathbb{Z}_K . Ecrivons $q\mathbb{Z}_K = \mathfrak{q}_1 \mathfrak{q}_2$; ces idéaux sont sauvagement ramifiés dans N/K et $\Delta(N/K) = (\mathfrak{q}_1^2 \mathfrak{q}_2^2)^{\ell-1}$, le conducteur de N/K est égal à $\mathfrak{q}_1^2 \mathfrak{q}_2^2$ et N est inclus dans le composé des extensions $K^{(\mathfrak{q}_i^2)}/K$ de conducteur \mathfrak{q}_i^2 et de degré ℓ .

Si $p = w \ell + 1$ est premier et $\Delta(N/K) = p^{\ell-1}$, l'idéal p n'est pas ramifié dans K/\mathbb{Q} , sinon il serait totalement et modérément ramifié dans une extension non cyclique. Montrons maintenant que p n'est pas inerte dans K/\mathbb{Q} . Si p était inerte dans K/\mathbb{Q} , le degré de la ℓ -extension de K de conducteur p serait égal à la ℓ -partie de $\frac{\varphi(p)}{w}$ (φ indicateur d'Euler généralisé) or $\frac{\varphi(p)}{w} = \ell \chi(p+1)$. Cette extension est

composée de K et du sous-corps réel maximal de $\mathbb{Q}^{(p)}$, elle est abélienne sur \mathbb{Q} . On peut donc écrire $q\mathbb{Z}_K = q_1 q_2$ et N est inclus dans le composé des extensions $K^{(q_i)}/K$ de conducteur q_i et de degré ℓ .

Si $q = \ell$ (resp. $q = p = w\ell + 1$) on note K_i ($i = 1, 2$) l'extension de K de degré ℓ et de conducteur q_i^2 (resp. q_i) et $L = K_1 K_2$. On constate que L est aussi le composé de N et de L_1 , l'extension cyclique de \mathbb{Q} de degré premier ℓ dont le discriminant est une puissance de q .

§4 Démonstration de la non-monogénéité dans le premier cas.

Admettons le lemme suivant dont la démonstration est reportée au § 5.

Lemme 1. Si les hypothèses H_1, H_2, H_3 sont vérifiées et si f est une puissance d'un nombre premier de \mathbb{Z} , l'idéal q_1 (resp. q_2) est inerte dans K_2 (resp. K_1).

On peut alors démontrer la proposition :

Proposition 1. Le ℓ -nombre de classes de N est égal à ℓ .

Démonstration : Si ce nombre était multiple de ℓ^2 , ℓ diviserait le nombre de classes de L . D'après le lemme 1, un seul idéal est ramifié dans L/K_1 ; l'application de la formule des classes ambiges ($[C]$) montre que ℓ divise le nombre de classes de K_1 . Comme un seul idéal est ramifié dans K_1/K on peut à nouveau appliquer la formule des classes ambiges ce qui donne une contradiction avec l'hypothèse H_1 .

Soient q_i' les idéaux premiers de \mathbb{Z}_N au-dessus des idéaux q_i .

Proposition 2. Les idéaux q_i' ont même image dans la ℓ -composante du groupe des classes de \mathbb{Z}_N .

Démonstration : Soient H le corps de classes de Hilbert de N , \mathfrak{H} le groupe des classes de N . L'application d'Artin induit un isomorphisme entre la ℓ -composante de \mathfrak{H} et $\text{Gal}(L/N)$ qui est celle de $\text{Gal}(H/N)$.

A l'image d'un idéal premier \mathfrak{P} de \mathbb{Z}_N correspond l'automorphisme de Frobenius $\left(\frac{L/N}{\mathfrak{P}}\right)$. Les idéaux $q_i^!$ étant inertes dans L/N , leurs images dans \mathfrak{H} engendrent sa ℓ -composante. Montrons qu'elles sont égales : Si τ est un élément d'ordre 2 de $\text{Gal}(N/\mathbb{Q})$ on a $\tau q_1^! = q_2^!$ et τ opère trivialement sur $\text{Gal}(L/N)$ par automorphisme intérieur puisque $L = NL_1$; on en déduit :

$$\left(\frac{L/N}{q_2^!}\right) = \left(\frac{L/N}{\tau q_1^!}\right) = \tau \left(\frac{L/N}{q_1^!}\right) \tau = \left(\frac{L/N}{q_1^!}\right).$$

Par l'hypothèse H2, $q_i^!$ est d'ordre ℓ dans \mathfrak{H} , \mathfrak{F} dont la classe est le carré ou la puissance quatrième de celle de $q_i^!$ n'est pas principal.

§5 Démonstration du lemme 1.

L'idéal q_1 étant principal est décomposé dans le corps de classes de Hilbert de K , le degré ℓ de K_2/K étant premier au nombre de classes de K , pour que q_1 ne soit pas inerte dans K_2/K , il faut que q_1 appartienne au rayon modulo q_2 (q_2^2 si $q = \ell$).

Si $K = \mathbb{Q}(\sqrt{-d})$ avec $-d \not\equiv 1 \pmod{4}$, pour que q_1 appartienne au rayon modulo q_2 il faut et il suffit que :

$$q_1 = (a + b\sqrt{-d}) \text{ avec } a + b\sqrt{-d} \equiv 1 \pmod{(a - b\sqrt{-d})} \quad a, b \in \mathbb{Z}$$

ce qui implique $(a - 1)^2 + db^2 \equiv 0 \pmod{(a^2 + db^2)}$ avec $q = a^2 + db^2$
ceci équivaut à $2a - 1 \equiv 0 \pmod{(a^2 + db^2)}$.

$a = 0$ étant impossible envisageons d'abord $a > 0$
la congruence implique $0 < a^2 < 2a - 1$ ce qui est impossible.

Si $a < 0$, en multipliant par -1 et en changeant de notation, on est conduit à $2a + 1 \equiv 0 \pmod{(a^2 + db^2)}$ avec $a > 0$

ce qui donne $a^2 < a^2 + db^2 \leq 2a + 1$

ce qui impose $(a - 1)^2 < 2$ avec a entier, $a > 0$.

On en déduit soit que $a = 1$ ce qui donne $q = 3$ soit $a = 2$ qui donne $q = 5$.
La condition $p = 2\ell + 1$ avec ℓ premier, $\ell \geq 5$, nous conduit à $q = \ell = 5$,
 $a = 2$, $b = \pm 1$, $d = 1$. On est alors dans le cas où le conducteur est q_2^2
ce qui conduit aux congruences

$$2 + i \equiv i^r \pmod{(2 - i)^2} \quad 0 \leq r \leq 3$$

dont on vérifie immédiatement qu'aucune n'est satisfaite.

Il résulte de ceci que si q_1 est décomposé dans K_2 c'est que $-d \equiv 1 \pmod{4}$. La condition q_1 appartient au rayon modulo q_2 donne :

$$a + b \frac{-1 + \sqrt{-d}}{2} \equiv 1 \quad \left(a - b \frac{1 + \sqrt{-d}}{2} \right) \quad a, b \in \mathbb{Z}$$

qui conduit à :

$$\left(a - 1 - \frac{b}{2} \right)^2 + \frac{bd^2}{4} \equiv 0 \quad \left(\left(a - \frac{b}{2} \right)^2 + \frac{db^2}{4} \right) \text{ avec } q = \left(a - \frac{b}{2} \right)^2 + \frac{db^2}{4}$$

$$\text{soit } 1 - 2a + b \equiv 0 \quad \left(a^2 - ab + b^2 \frac{(1+d)}{4} \right).$$

Etudions cette congruence suivant le signe de $1 - 2a + b$.

1) Si $1 - 2a + b < 0$ la congruence s'écrit :

$$1 - 2 \left(a - \frac{b}{2} \right) \leq - \left(a - \frac{b}{2} \right)^2 - \frac{db^2}{4} < 0$$

$$\text{ce qui donne } 0 < \left(a - \frac{b}{2} \right)^2 < 2 \left(a - \frac{b}{2} \right) - 1$$

soit :

$$\left[\left(a - \frac{b}{2} \right) - 1 \right]^2 < 0 \quad \text{ce qui est impossible.}$$

2) Si $1 - 2a + b > 0$ on obtient :

$$(*) \quad 0 \leq \left(a - \frac{b}{2} \right)^2 < \left(a - \frac{b}{2} \right)^2 + \frac{db^2}{4} \leq 1 - 2 \left(a - \frac{b}{2} \right)$$

$$\text{d'où } \left(a - \frac{b}{2} \right)^2 + 2 \left(a - \frac{b}{2} \right) - 1 < 0$$

$$\text{soit } \frac{-1 - \sqrt{5}}{2} < a - \frac{b}{2} < \frac{-1 + \sqrt{5}}{2}$$

ce qui, joint à la condition de départ $a - \frac{b}{2} < \frac{1}{2}$, donne pour $a - \frac{b}{2}$ les valeurs $-\frac{3}{2}, -1, -\frac{1}{2}, 0$. Etudions chacune de ces possibilités :

a) Si $a - \frac{b}{2} = 0$ les inégalités (*) donnent $0 < db^2 \leq 4$ qui joint à $d \equiv 3 \pmod{4}$ impose $d = 3$, $b^2 = 1$ ce qui est impossible puisque $a - \frac{b}{2} = 0$ implique la parité de b .

b) Si $a - \frac{b}{2} = -\frac{1}{2}$, b est impair et les inégalités (*) donnent $0 < db^2 < 7$ ce qui joint à $d \equiv 3 \pmod{4}$ conduit à $b^2 = 1$, $d = 3$ ou 7 . Pour chacun de ces cas on a

• α) $b = 1$, $d = 3$ alors $a = 0$ et $a + b\omega = \frac{-1 + \sqrt{-3}}{2}$ qui est une unité et donc n'engendre pas un idéal premier.

• β) $b = -1$, $d = 3$ alors $a = -1$, $a + b\omega = -1 - \frac{-1 + \sqrt{-3}}{2}$ est encore une unité.

• γ) $b = 1$, $d = 7$ alors $a = 0$, $a + b\omega = \frac{-1 + \sqrt{-7}}{2}$ dont la norme 2 devrait être un nombre premier impair.

• δ) $b = -1$, $d = 7$ alors $a = -1$, $a + b\omega = -1 - \frac{-1 + \sqrt{-7}}{2}$
a encore pour norme 2.

c) Si $a - \frac{b}{2} = -1$ les inégalités (*) deviennent $0 < db^2 \leq 8$ on trouve $d = 3$ ou 7 ce qui ne convient pas du fait de la parité de b .

d) Si $a - \frac{b}{2} = -\frac{3}{2}$, b est impair, les inégalités (*) deviennent $0 < db^2 \leq 7$ ce qui impose $b^2 = 1$, $d = 3$ ou 7 .

• α) $b = 1$, $d = 3$ alors $a = -1$, $a + b\omega = -1 + \frac{-1 + \sqrt{-3}}{2}$
qui donne $q = 3$ ce qui est exclu.

• β) $b = -1$, $d = 3$ alors $a = -2$, $a + b\omega = -2 - \frac{-1 + \sqrt{-3}}{2}$
qui donne aussi $q = 3$.

• γ) $b = 1$, $d = 7$ alors $a = -1$, $a + b\omega = -1 + \frac{-1 + \sqrt{-7}}{2}$ dont la norme est 4 alors que ce devrait être un nombre premier impair.

• δ) $b = -1$, $d = 7$ alors $a = -2$, $a + b\omega = -2 - \frac{-1 + \sqrt{-7}}{2}$ dont la norme est également 4.

3) Si $1 - 2a + b = 0$, b est impair et $a = \frac{b+1}{2}$, on obtient $a + b\omega = \frac{1+b\sqrt{-d}}{2}$ avec b impair. Le nombre premier q est égal à $\frac{1+db^2}{4}$.

a) Si $d = 3$, $q = 7 = \ell$, $b = \pm 3$ ce qui donne les idéaux de $\mathbb{Q}(j)$ au-dessus de 7 . Dans ce cas le conducteur est q_2^2 , il faut, en fait, regarder les congruences $\frac{1+3\sqrt{-3}}{2} \equiv (-j)^r \left(\left(\frac{1-3\sqrt{-3}}{2} \right)^2 \right)$, $0 \leq r \leq 5$, dont on vérifie qu'elles n'ont pas de solution.

b) Il reste à envisager $q = p = 2\ell + 1$ ce qui nous donne : $db^2 = 8\ell + 3$, comme b est impair, on en déduit $d \equiv 3 \pmod{8}$.

Si on regarde l'égalité modulo 3 :

$db^2 \equiv 2\ell \pmod{3}$, comme $\ell \geq 5$ on a $b \not\equiv 0 \pmod{3}$. Par conséquent : $d \equiv 2\ell \pmod{3}$; comme $2\ell + 1$ est premier $\ell \equiv 2 \pmod{3}$.

On obtient facilement $d \equiv 3 \pmod{8}$ et $d \equiv 1 \pmod{3}$ soit $d \equiv 19 \pmod{24}$ ce qui est interdit par l'hypothèse H3.

Pour terminer la démonstration du théorème, il reste à étudier les extensions diédrales de degré 14 contenant $\mathbb{Q}(j) = K$, le conducteur de N/K étant $7^2 \times 43$.

§ 6 Extensions diédrales imaginaires de degré 14 et de discriminant

$$3^7 (7^2 \times 43)^{12} .$$

On écrit $7 \mathbb{Z} [j] = \mathfrak{d}_1 \mathfrak{d}_2$ avec $\mathfrak{d}_1 = (1 - 2j)$, $\mathfrak{d}_2 = (3 + 2j)$

$43 \mathbb{Z} [j] = \mathfrak{p}_1 \mathfrak{p}_2$ avec $\mathfrak{p}_1 = (1 - 6j)$, $\mathfrak{p}_2 = (7 + 6j)$

et on considère les corps $K \binom{\mathfrak{d}_1^2}{1}$, $K \binom{\mathfrak{d}_2^2}{2}$, $K \binom{\mathfrak{p}_1}{1}$, $K \binom{\mathfrak{p}_2}{2}$; le composé L de ces corps est une extension abélienne de degré 7^4 de $\mathbb{Q}(j)$ dont le groupe de Galois est du type (7, 7, 7, 7), c'est le corps des genres des extensions diédrales de \mathbb{Q} , et de discriminant $3^7 (7^2 \times 43)^{12}$. Soit N une telle extension, on note \mathfrak{p}_1^i (resp. $\mathfrak{p}_2^i, \mathfrak{d}_1^i, \mathfrak{d}_2^i$) l'idéal de \mathbb{Z}_N au-dessus de \mathfrak{p}_1 (resp. $\mathfrak{p}_2, \mathfrak{d}_1, \mathfrak{d}_2$), pour démontrer que \mathbb{Z}_N n'est pas \mathbb{Z}_K -monogène il suffit de démontrer que l'idéal ambige $I = (\mathfrak{d}_1^i \mathfrak{d}_2^i)^2 \mathfrak{p}_1^i \mathfrak{p}_2^i$ n'est pas principal. Le principe de la démonstration reste le même; on considère l'image de I par l'application d'Artin dans le groupe de Galois de l'extension H/N (où H est le corps de classes de Hilbert de N). L'idéal I est principal si et seulement si cette image est l'élément neutre et on a un premier renseignement en étudiant sa restriction à L.

Lemme. L'idéal I n'est principal que pour au plus un corps.

Démonstration: La restriction à L de l'image d'un idéal premier \mathfrak{P} par l'application d'Artin dans $\text{Gal}(H/N)$ est égale à l'automorphisme de Frobenius $\left(\frac{L/N}{\mathfrak{P}}\right)$. Il suffit donc de démontrer que $\left(\frac{L/N}{\mathfrak{d}_1^i \mathfrak{d}_2^i \mathfrak{p}_1^i \mathfrak{p}_2^i}\right) \neq 1$.

Précisons tout d'abord la structure de $\text{Gal}(L/K)$. Soit $I_{\mathfrak{p}_1}$ (resp. $I_{\mathfrak{p}_2}, I_{\mathfrak{d}_1}, I_{\mathfrak{d}_2}$) le groupe d'inertie de \mathfrak{p}_1 (resp. $\mathfrak{p}_2, \mathfrak{d}_1, \mathfrak{d}_2$) dans $\text{Gal}(L/K)$ et σ_1 (resp. σ_2, ν_1, ν_2) un générateur de $I_{\mathfrak{p}_1}$ (resp. $I_{\mathfrak{p}_2}, I_{\mathfrak{d}_1}, I_{\mathfrak{d}_2}$). On peut fixer sans ambiguïté ces générateurs. On sait que \mathfrak{d}_2 est inerte dans $K \binom{\mathfrak{d}_1^2}{1}$. On pose donc :

$$\nu_{1/K} \binom{\mathfrak{d}_1^2}{1} = \left(\frac{K \binom{\mathfrak{d}_1^2}{1} / K}{\mathfrak{d}_2}\right) \quad \text{et} \quad \nu_{2/K} \binom{\mathfrak{d}_2^2}{2} = \left(\frac{K \binom{\mathfrak{d}_2^2}{2} / K}{\mathfrak{d}_1}\right) .$$

Rappelons que la conjugaison complexe τ opère sur $\text{Gal}(L/N)$ et sur le groupe des idéaux fractionnaires de K ; les propriétés fonctorielles de l'application d'Artin montrent que $\tau v_1 \tau = v_2$.

De même p_2 est inerte dans $K^{(p_1)}/K$, on pose :

$$\sigma_{1/K}^{(p_1)} = \left(\frac{K^{(p_1)}/K}{p_2} \right) \quad \text{et} \quad \sigma_{2/K}^{(p_2)} = \left(\frac{K^{(p_2)}/K}{p_1} \right)$$

on en déduit $\tau \sigma_1 \tau = \sigma_2$.

On peut vérifier sans trop de difficulté les congruences suivantes :

$$\begin{aligned} (3+2j)^5 &\equiv -(1-6j) \pmod{\mathfrak{L}_1^2} & (3+2j)^3 &\equiv -j^2(7+6j) \pmod{\mathfrak{L}_1^2} \\ (7+6j)^3 &\equiv -j^2(1-2j) \pmod{p_1} & (7+6j)^4 &\equiv -(3+2j) \pmod{p_1} \end{aligned}$$

D'où l'on déduit :

$$\left(\frac{K^{(\mathfrak{L}_1^2)}/K}{p_1} \right) = v_{1/K}^5 \pmod{\mathfrak{L}_1^2} ; \quad \left(\frac{K^{(\mathfrak{L}_1^2)}/K}{p_2} \right) = v_{1/K}^3 \pmod{\mathfrak{L}_1^2} ;$$

$$\left(\frac{K^{(p_1)}/K}{\mathfrak{L}_1} \right) = \sigma_{1/K}^3 \pmod{p_1} ; \quad \left(\frac{K^{(p_1)}/K}{\mathfrak{L}_2} \right) = \sigma_{1/K}^4 \pmod{p_1}$$

et au moyen de la conjugaison par τ :

$$\left(\frac{K^{(\mathfrak{L}_2^2)}/K}{p_2} \right) = v_{2/K}^5 \pmod{\mathfrak{L}_2^2} ; \quad \left(\frac{K^{(\mathfrak{L}_2^2)}/K}{p_1} \right) = v_{2/K}^3 \pmod{\mathfrak{L}_2^2} ;$$

$$\left(\frac{K^{(p_2)}/K}{\mathfrak{L}_2} \right) = \sigma_{2/K}^3 \pmod{p_2} ; \quad \left(\frac{K^{(p_2)}/K}{\mathfrak{L}_1} \right) = \sigma_{2/K}^4 \pmod{p_2} .$$

On est maintenant à même de déterminer les groupes de décomposition des idéaux p_i et \mathfrak{L}_i dans L/K . On pourra alors déterminer les automorphismes de Frobenius des idéaux $p_i^!$, $\mathfrak{L}_i^!$ au-dessus de p_i , \mathfrak{L}_i dans $\text{Gal}(L/N)$. Soit $D_{\mathfrak{L}_1}$ le groupe de décomposition de \mathfrak{L}_1 dans

$\text{Gal}(L/K^{(\mathfrak{L}_1^2)})$; pour tout corps M , $K \subset M \subset L$, tel que \mathfrak{L}_1 ne soit pas ramifié dans M/K et $\mu = \left(\frac{N/K}{I_1} \right)^{(\mathfrak{L}_1^2)}$ où I_1 est l'idéal premier de $K^{(\mathfrak{L}_1^2)}$

au-dessus de \mathfrak{L}_1 , on a :

$$\mu/M = \left(\frac{M/K}{N_{K(\mathfrak{L}_1^2)/K}(\mathfrak{I}_1)} \right) = \left(\frac{M/K}{\mathfrak{L}_1} \right).$$

On en déduit donc $\mu/K(\mathfrak{L}_1^2) = \nu_2$, $\mu/K(\mathfrak{p}_1) = \sigma_1^3$; $\mu/K(\mathfrak{p}_2) = \sigma_2^4$ et

par conséquent $\mu = \nu_2 \sigma_1^3 \sigma_2^4$. Le groupe $D_{\mathfrak{L}_1}$ est donc engendré par ν_1 et $\nu_2 \sigma_1^3 \sigma_2^4$. Par conjugaison le groupe de décomposition $D_{\mathfrak{L}_2}$ de \mathfrak{L}_2 dans L/K est engendré par ν_2 et $\nu_1 \sigma_1^4 \sigma_2^3$.

Procédons de la même manière avec \mathfrak{p}_1 . Soient \mathfrak{P}_1 l'idéal au-

dessus de \mathfrak{p}_1 dans $K^{(\mathfrak{p}_1)}$ et $\mu = \left(\frac{L/K^{(\mathfrak{p}_1)}}{\mathfrak{P}_1} \right)$, pour tout corps M , $K \subset M \subset L$, tel que \mathfrak{p}_1 ne soit pas ramifié dans M/K , on a :

$$\mu/M = \left(\frac{M/K}{N_{K^{(\mathfrak{p}_1)}/K}(\mathfrak{P}_1)} \right) = \left(\frac{M/K}{\mathfrak{p}_1} \right).$$

On a donc :

$$\mu/K(\mathfrak{p}_2) = \sigma_2, \quad \mu/K(\mathfrak{L}_1^2) = \nu_1^5, \quad \mu/K(\mathfrak{L}_2^2) = \nu_2^3 \quad \text{d'où } \mu = \sigma_2 \nu_1^5 \nu_2^3.$$

Le groupe $D_{\mathfrak{p}_1}$ est engendré par σ_1 et $\sigma_2 \nu_1^5 \nu_2^3$; par conjugaison le groupe $D_{\mathfrak{p}_2}$ est engendré par σ_2 et $\sigma_1 \nu_1^3 \nu_2^5$.

Le composé des extensions diédrales de \mathbb{Q} contenues dans L est le sous-corps de L invariant par $\sigma_1 \sigma_2$ et $\nu_1 \nu_2$; l'extension diédrale dont le conducteur sur K est 7^2 (resp. 43) est également invariante par σ_1, σ_2 (resp. ν_1, ν_2); le groupe de Galois de L sur cette extension est engendré par $\nu_1 \nu_2, \sigma_1 \sigma_2, \sigma_1 \sigma_2^{-1}$ (resp. $\sigma_1 \sigma_2, \nu_1 \nu_2, \nu_1 \nu_2^{-1}$). Il y a donc six extensions diédrales de degré 14, contenant $\mathbb{Q}(j)$ et dont le conducteur sur $\mathbb{Q}(j)$ est $7^2 \cdot 43$; ce sont les corps N_i où N_i est le sous-corps de L invariant par $\sigma_1 \sigma_2, \nu_1 \nu_2, \nu_1 \nu_2^{-1} \sigma_1 \sigma_2^{-i}$ ($1 \leq i \leq 6$).

Soit \mathfrak{P} un des idéaux \mathfrak{p}_r , \mathfrak{q}_s et \mathfrak{P}' l'idéal premier de N_i au-dessus de \mathfrak{P} . Pour tout corps M , $K \subset M \subset L$, tel que \mathfrak{P} ne soit pas

ramifié dans M/K , on a $\left(\frac{L/N_i}{\mathfrak{P}'}\right)/M = \left(\frac{M/K}{N_{N_i/K}(\mathfrak{P}')}\right) = \left(\frac{M/K}{\mathfrak{P}}\right)$.

Si on écrit $\left(\frac{L/N_i}{\mathfrak{q}'_1}\right) = \mu = (v_1 v_2)^a (\sigma_1 \sigma_2)^b (v_1 v_2^{-1} \sigma_1^i \sigma_2^{-i})^c$

on a : $\mu / \left(\frac{\mathfrak{q}'_2}{K}\right) = v_2$ donc $a - c = 1$, $\mu / \left(\frac{\mathfrak{p}'_1}{K}\right) = \sigma_1^3$ donc $b + ic = 3$

$\mu / \left(\frac{\mathfrak{p}'_2}{K}\right) = \sigma_2^4$ donc $b - ic = 4$

il en résulte que $b = 0$, $c = 3i^*$, $a = 1 + 3i^*$ où i^* est l'inverse de i modulo 7. Par conséquent :

$\left(\frac{L/N_i}{\mathfrak{q}'_1}\right) = v_1^{1-i^*} v_2^3 \sigma_1^3 \sigma_2^4$ et $\left(\frac{L/N_i}{\mathfrak{q}'_2}\right) = v_1 v_2^{1-i^*} \sigma_1^4 \sigma_2^3$.

De la même manière, si $\mu = \left(\frac{L/N_i}{\mathfrak{p}'_1}\right) = v_1^{a+c} v_2^{a-c} \sigma_1^{b+ic} \sigma_2^{b-ic}$

on a $\mu / \left(\frac{\mathfrak{q}'_1}{K}\right) = v_1^5$ donc $a + c = 5$; $\mu / \left(\frac{\mathfrak{q}'_2}{K}\right) = v_2^3$ donc $a - c = 3$

$\mu / \left(\frac{\mathfrak{p}'_2}{K}\right) = \sigma_2$ donc $b - ic = 1$,

il en résulte $a = 4$, $c = 1$, $b = 1 + i$ et :

$\left(\frac{L/N_i}{\mathfrak{p}'_1}\right) = v_1^5 v_2^3 \sigma_1^{1+2i} \sigma_2$ et $\left(\frac{L/N_i}{\mathfrak{p}'_2}\right) = v_1^3 v_2^5 \sigma_1 \sigma_2^{1+2i}$.

L'automorphisme de Frobenius associé à $(\mathfrak{q}'_1 \mathfrak{q}'_2)^2 \mathfrak{p}'_1 \mathfrak{p}'_2$ est :

$v_1^{5-2i^*} v_2^{5-2i^*} \sigma_1^{2+2i} \sigma_2^{2+2i}$

il est nul si et seulement si $i = 6$.

Ce qui donne au plus un corps pour lequel l'idéal I peut être principal. Remarquons que :

$$\left(\frac{L/N_6}{p_1^1}\right) = \left(\frac{L/N_6}{\ell_2^1}\right)^5 \quad \text{et} \quad \left(\frac{L/N_6}{\ell_1^1}\right) = \left(\frac{L/N_6}{p_2^1}\right)^3$$

et qu'il y a donc des classes ambiges dans le genre principal .

- [C] C. CHEVALLEY : Sur la théorie du corps de classes dans les corps finis et les corps locaux. J. of the Fac. of Sc., Tokyo, Vol. II, Part 9 (1933) .
- [Co] J. COUGNARD : Sur la monogénéité de l'anneau des entiers d'une extension diédrale imaginaire de degré $2p$ (p premier ≥ 5) .
Soumis à publication .
- [G1] M.-N. GRAS : Non monogénéité de l'anneau des entiers des extensions cycliques de \mathbb{Q} de degré premier $\ell \geq 5$. A paraître dans J. of Number Theory .
- [G2] M.-N. GRAS : Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de \mathbb{Q} . Publ. Math. Fac. Sc. Besançon 1983-84.

Addenda

Dans la démonstration du lemme 1 (§5) un cas a été oublié au point 3).

Il faut ajouter :

c) Si $d = 3$, $q = 6\ell + 1$ l'égalité de q avec $\frac{1 + db^2}{4}$ avec b impair conduit à $\frac{b-1}{2} \cdot \frac{b+1}{2} = 2\ell$ ce qui est impossible avec $\ell \geq 5$.

Jean COUGNARD
U.A. 741 CNRS
Faculté des Sciences
25030 Besançon Cedex
(France)