THÉORIE DES NOMBRES

BESANÇON

Année 1983 - 1984

GROUPE DES UNITÉS ET NOMBRE DE CLASSES DE CERTAINES EXTENSIONS DIÉDRALES DE DEGRÉ 8 DE $\mathbb{Q}$

Jean COUGNARD

GROUPE DES UNITES ET NOMBRE DE CLASSES

DE CERTAINES EXTENSIONS DIEDRALES DE DEGRE 8 DE $\mathbb{Q}$

par Jean COUGNARD

Un des problèmes majeurs de la théorie des nombres algébriques est celui de la détermination du nombre des classes d'idéaux de l'anneau des entiers d'un corps de nombres algébriques. Nous donnons ici une méthode permettant de répondre à cette question pour certaines extensions diédrales de degré 8 de $\mathbb{Q}$ (précisées dans la première partie). Pour cela, on rapproche des algorithmes existants, tout en modifiant l'un d'entre eux.

Un théorème de Brauer [B], modifié par Walter [W], ramène le calcul du nombre des classes d'une extension galoisienne à celui de ses sous-corps et à celui d'indices de groupes d'unités. Dans le cas des extensions diédrales, ces formules ont été améliorées par C. Castela [C].

Dans la situation où l'on se place, il faut déterminer le nombre de classes d'une extension de degré 4 de $\mathbb{Q}$ contenant un corps quadratique imaginaire euclidien ; cela peut être fait au moyen d'un travail de H. Amara [A]. Cette étape nous permet également de calculer une unité fondamentale de ce corps biquadratique. Il est alors possible, en adaptant un travail de Wada, de déterminer le groupe des unités de l'extension diédrale. La connaissance de l'action du groupe de Galois permet alors de terminer la détermination du nombre de classes cherché :

Le § 1 fixe les notations pour l'extension diédrale, le § 2 rappelle ce que devient la formule de Walter, le § 3 indique comment adapter l'article de Wada pour calculer le groupe des unités, le § 4 résume le travail de Amara. La faisabilité de la méthode est vérifiée sur un exemple numérique qui n'a rien de glorieux, l'auteur ayant travaillé avec une H.P. 15 C.

§ 1 - Extension diédrale de degré 8 :

Soit $N/\mathbb{Q}$ une extension diédrale de degré 8, son groupe de Galois G est engendré par deux éléments σ et τ vérifiant les relations :

$$\sigma^4 = 1 = \tau^2 \quad ; \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

Nous appelons G_o (resp. G_1, G_o', G_1' et H) le sous-groupe de G engendré par τ (resp. $\tau\sigma$, τ et σ^2, $\tau\sigma$ et σ^2, σ).

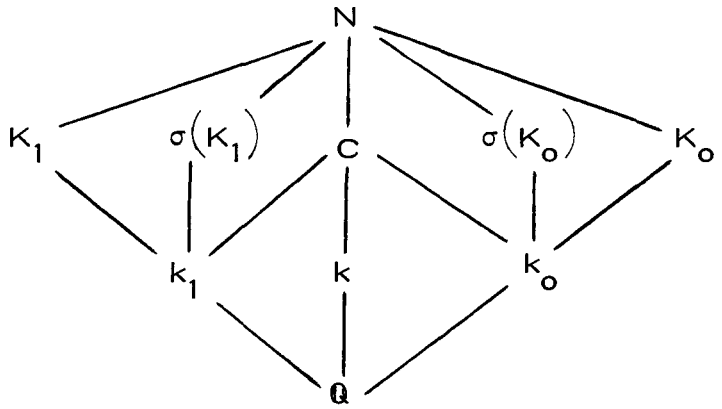
Le corps invariant par G_o (resp. G_1, G_o', G_1', H) est noté K_o (resp. K_1, k_o, k_1, k).

Les autres sous-groupes de G sont :

$\sigma G_o \sigma^{-1}$ engendré par $\tau\sigma^2$ dont le corps des invariants est $\sigma(K_o)$

$\sigma G_1 \sigma^{-1}$ engendré par $\tau\sigma^3$ dont le corps des invariants est $\sigma(K_1)$

et le centre de G engendré par σ^2 dont le corps des invariants est C, ce qui nous donne le diagramme suivant :



Dans tout ce qui suit, le corps k_o est supposé être un corps quadratique imaginaire dont l'anneau des entiers est euclidien pour la norme.

Pour chaque corps K, on note r_K, c_K, E_K, Cl_K, h_K son nombre de places réelles, complexes, son groupe des unités, son groupe des classes, son nombre de classes. Le corps k_o étant complexe, pour un plongement de N dans une clôture algébrique de $\mathbb{Q}$, le groupe de décomposition de la place à l'infini est soit G_1, soit $\sigma G_1 \sigma^{-1}$; on en déduit que

$r_{k_1} = 2$, $r_k = r_{k_o} = 0$ puis que $r_{K_1} = r_{\sigma(K_1)} = 2$; $r_{K_o} = r_{\sigma(K_o)} = 0$, ce qui permet de déterminer le rang, $rg\left(E_K\right)$, du groupe des unités de chaque corps K :

$$rg\left(E_c\right) = rg\left(E_{K_o}\right) = rg\left(E_{\sigma(K_o)}\right) = rg\left(E_{k_1}\right) = 1 ;$$

$$rg\left(E_{K_1}\right) = rg\left(E_{\sigma(K_1)}\right) = 2 \quad ; \quad rg\left(E_N\right) = 3.$$

§ 2 - Le théorème de Walter ([W], [C] chapitres I et II) :

. Pour tout sous-groupe G' de G, $\widetilde{G'}$ désigne l'élément $\sum_{g \in G'} g$ de $\mathbb{Z}[G]$ et $n(G')$ le degré $[N : N^{G'}]$; si $\mathfrak{M}$ est un $\mathbb{Z}[G]$-module, $\mathfrak{M}^{G'}$ est le sous-groupe de $\mathfrak{M}$ formé des éléments invariants par G', $w_2(G')$ le nombre de racines 2^p-ièmes de l'unité contenues dans $N^{G'}$.

On note $1_{G'}^{G}$ le caractère de G obtenu par l'induction de G' à G du caractère identité de G' [S1].

. Pour tout sous-groupe E' de E_N, $\overline{E'}$ est l'image de E' dans le quotient $\overline{E}_N$ de E_N par son groupe de torsion.

. N étant considéré comme plongé dans C, on note D le sous-groupe de G engendré par la conjugaison complexe.

. Si $\mathfrak{M}$ et $\mathfrak{M}'$ sont deux $\mathbb{Z}[G]$-modules, sans torsion, de même rang, plongés dans un même espace vectoriel V, $[\mathfrak{M} : \mathfrak{M}']$ est l'indice de $\mathfrak{M}'$ dans $\mathfrak{M}$ ([S2] ch. 4).

On peut alors définir un $\mathbb{Z}[G]$-module L par la suite exacte

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G]\widetilde{D} \longrightarrow L \longrightarrow 0$$

où $\mathbb{Z}[G]\widetilde{D}$ est l'idéal à gauche de $\mathbb{Z}[G]$ engendré par $\widetilde{D}$, et l'injection envoie l'entier n sur $n\widetilde{G}$. On peut montrer (cf. [W]) que L et $\overline{U}$ ont même rang (*théorème de Herbrand*) *et que :*

Théorème (th. 4.1 dans [W]) : Si M est un sous-$\mathbb{Z}[G]$-module de $\overline{E}_N$, $\mathbb{Z}[G]$ isomorphe à L, la relation

(1) $$\sum_{G' \subset G} a(G')\, I_{G'}^{G} = 0, \qquad a(G') \in \mathbb{Z}$$

conduit à l'égalité :

(2) $$\prod_{G'} h(G')^{a(G')} = \prod_{G'} \left(n(G')\, w_2(G') \left[\overline{E_N^{G'}} : M^{G'}\right] \right)^{a(G')}.$$

En appliquant ce théorème à une extension diédrale de degré 8 $N/\mathbb{Q}$, on démontre (cf. [C] chapitre II) les relations :

(3) $$h_N = h_{K_o} \cdot h_k h_{K_1} \times \frac{w_2(N)}{w_2(K_o)\, w_2(k)\, w_2(K_1)} \times \frac{\left[\overline{E}_N : M\right]}{\left[\overline{E_N^{G_o}} : M^{G_o}\right] \cdot \left[\overline{E_N^{H}} : M^{H}\right] \left[\overline{E_N^{G_1}} : M^{G_1}\right]}$$

(4) $$\frac{h_{K_o}}{h_{k_o}} = \frac{h_{K_1}}{h_{k_1}} \cdot \frac{w_2(K_o)}{w_2(k_o)} \times \frac{w_2(k_1)}{w_2(K_1)} \times \frac{\left[\overline{E_N^{G_o}} : M^{G_o}\right]}{\left[\overline{E_N^{G'_o}} : M^{G'_o}\right]} \times \frac{\left[\overline{E_N^{G'_1}} : M^{G'_1}\right]}{\left[E_N^{G_1} : M^{G_1}\right]}.$$

On sait aisément déterminer le nombre des classes d'un corps quadratique [Ch], donc si on connaît h_{K_o} et l'action de G sur E_N la formule (4) nous donne h_{K_1}.

La formule (3) permet alors de calculer h_N.

§ 3 - Les unités de N :

Supposons connu le groupe E_{K_o}.

Lorsqu'une extension $L/\mathbb{Q}$ est composée d'extensions quadratiques de $\mathbb{Q}$, il est possible de déterminer son nombre de classes connaissant ceux des corps quadratiques. Ces méthodes, antérieures à celle de Walter, relèvent du théorème de Brauer déjà évoqué (faisant lui-même appel aux propriétés des fonctions zéta) et nécessitent la connaissance du groupe des unités. La méthode utilisée dans [Wa] peut s'appliquer ici, d'une part pour déterminer E_C, puis connaissant E_{K_o} et, bien entendu $E_{\sigma(K_o)} = \sigma(E_{K_o})$, déterminer E_N. Indiquons comment procéder et prenons des notations simplifiées pour alléger la démonstration.

Considérons une extension L/F à groupe de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Gal $(L/F) = \{Id, \alpha, \rho, \mu = \alpha\rho\}$ puis désignons par L_1 (resp. L_2, L_3) le corps invariant par α (resp. ρ, μ), par E_i le groupe des unités de L_i et par E celui de L.

Soit ε une unité de L, on a l'identité

$$\varepsilon^2 = \frac{(\varepsilon\varepsilon^{\alpha})(\varepsilon\varepsilon^{\rho})}{(\varepsilon\varepsilon^{\mu})^{\alpha}}$$

et donc ε^2 appartient au sous-groupe $E_1 E_2 E_3$ de L^*. Si les $(\varepsilon_{i,j})_{1 \le j \le r_i}$ forment un système de générateurs de E_i $(i = 1,2,3)$. Il faut regarder quels sont, parmi les éléments $\prod_{i,j} \varepsilon_{i,j}^{t_{i,j}}$ (avec $t_{i,j} = 0$ ou 1), ceux qui sont des carrés dans L. Les racines carrées de ces unités, ajoutées aux $\varepsilon_{i,j}$ forment un système de générateur de E.

Soit donc maintenant ε un élément de $E_1 E_2 E_3$. Si ε est un carré dans L, les $N_{L/L_i}(\varepsilon)$ sont dans E_i^2. Cette propriété peut être vérifiée si on connaît les groupes E_i avec suffisamment de précision. Supposons donc que les $N_{L/L_i}(\varepsilon)$ appartiennent à E_i^2 pour chaque i. On peut alors choisir des B_i dans E_i tels que

$$B_1^2 = N_{L/L_1}(\varepsilon), \quad B_2^2 = N_{L/L_2}(\varepsilon), \quad B_3^2 = N_{L/L_3}(\varepsilon)^{\alpha}$$

et $$B_1 B_2 B_3 = \varepsilon B_3^2.$$

Par conséquent, ε est un carré dans L si et seulement si $B_1 B_2 B_3$ en est un. Posons alors : $b = N_{L_i/F}(B_i)$

$$\xi = B_1 B_2 B_3 + b(B_1 + B_2 + B_3)$$

$$c = Tr_{L/F}(\xi).$$

On a alors l'identité

$$B_1 B_2 B_3 c = \xi^2.$$

Donc $B_1 B_2 B_3$ est un carré dans L si et seulement si l'élément c de F

en est un. La vérification de cette dernière propriété revient à tester si le quotient de deux éléments de F est un carré dans F. Dans la situation du § 1, le corps F est soit $\mathbb{Q}$, soit k_o, le test est donc utilisable.

Il ne nous reste plus qu'à déterminer l'unité fondamentale et le nombre des classes de K_o.

§ 4 - Unité fondamentale et groupe des classes de K_o :

Dans cette partie, on reprend l'article de Amara [A]. Les résultats sont énoncés dans l'ordre où ils sont utilisés.

Puisque l'anneau des entiers $\mathbb{Z}_{k_o}$ de k_o est euclidien, donc principal, il existe $\theta \in K_o$ tel que $\mathbb{Z}_{K_o} = \mathbb{Z}_{k_o}[\theta]$ et tout idéal entier I de $\mathbb{Z}_{K_o}$ possède une $\mathbb{Z}_{k_o}$ base $\{a, \theta - c\}$ où a et c sont deux entiers de $\mathbb{Z}_{k_o}$: le nombre a engendré la norme dans K_o/k_o de l'idéal I et si f est le polynôme irréductible de θ dans K_o/k_o, on a la congruence

$$f(c) \equiv 0 \quad (a).$$

Le corps N étant considéré comme un sous-corps de $\mathbb{C}$, pour chaque élément x de N, on note $|x|$ son module. On définit alors :

Définition 1 : Un idéal entier I de base $\{a, \theta - c\}$ sur $\mathbb{Z}_{k_o}$ $\left(\text{noté } I = (a, \theta - c)\right)$ est dit réduit si et seulement si il vérifie la propriété suivante : pour tout $\xi \in I$, $\xi \neq 0$, on a :

$$|a| \leq \sup\left(|\xi|, |\xi^{\sigma^2}|\right).$$

Lemme II ([A] lemme IV 1) : Soit $I = (a, \theta - c)$ un idéal entier avec $|\theta - c| < |a|$, pour que I soit réduit, il faut et il suffit que pour tout $\xi = \lambda a + \mu(\theta - c)$ dans I avec λ et μ non nuls et vérifiant :

$$|\mu| < \frac{2|a|}{|\theta - \theta^{\sigma^2}|}, \qquad |\lambda| < 1 + |\mu|$$

on ait :

$$|a| \leq \sup\left(|\xi|, |\xi^{\sigma^2}|\right).$$

On peut démontrer que dans chaque classe d'idéaux il y a un idéal réduit (cf. [Sm] Ch. II).

Bien entendu, un idéal est réduit si et seulement si son conjugué sur k_o est réduit.

Démontrons maintenant qu'il n'y a qu'un nombre fini d'idéaux réduits : Si $|a|^2 = N_{K_o/\mathbb{Q}}(I) > \left(\frac{2}{\pi}\right)^2 \sqrt{D_{K_o/\mathbb{Q}}}$, on peut d'après le Théorème de Minkowski trouver $\xi \in I$ tel que :

$$|\xi| < |a|, \quad |\xi^{\sigma^2}| < |a|$$

et donc l'idéal I n'est pas réduit. Donc pour que l'idéal entier I soit réduit, il faut que $|a|^2 \leq \left(\frac{2}{\pi}\right)^2 \sqrt{D_{K_o/\mathbb{Q}}}$. Il ne peut donc y avoir qu'un nombre fini d'idéaux réduits.

Il va donc falloir déterminer tous les idéaux réduits de K_o et les regrouper classe par classe, ce qui va se faire au moyen de cycles d'idéaux.

On peut donc déjà faire la liste des premières étapes de l'algorithme.

1. Dresser la liste à une unité près des entiers a de k_o vérifiant $|a|^2 \leq \frac{4}{\pi^2} \sqrt{D_{K/\mathbb{Q}}}$.
2. Chercher pour chacun de ces entiers a, les entiers c de k_o intérieurs au disque de centre θ, de rayon a, vérifiant $f(c) \equiv 0$ (a).
3. Pour chaque a, identifier les c obtenus dont la différence est divisible par a.
4. Eliminer les idéaux non réduits au moyen du lemme II.

La proposition suivante nous donne une condition nécessaire et suffisante pour que deux idéaux soient dans la même classe.

<u>Proposition III</u> ([A] prop. I.2) : <u>Soient</u> $I = (a, \theta - c_1)$ <u>et</u> $J = (b, \theta - c_2)$ <u>deux idéaux réduits. Pour que</u> JI^{-1} <u>soit principal, il faut et il suffit qu'il existe dans</u> I <u>un élément</u> h_o <u>tel que</u> $|h_o| < |a|$ <u>et vérifiant</u> :

(i) $J = \left(h_o^{\tau}/a\right) I$ <u>et</u> $N_{K_o/k_o}(h_o) = \varepsilon ab$ <u>où</u> ε <u>est une unité de</u> k_o.

(ii) <u>Pour tout</u> $h \in I - \{0\}$ <u>tel que</u> $|h| < |h_o|$ <u>on a</u> $|h_o^{\sigma^2}| \leq |h^{\sigma^2}|$

cette dernière condition est appelée condition de réduction et tout élément $h' \in I - \{0\}$ et vérifiant (ii) est appelé élément réduit dans I.

Il existe des éléments réduits "naturels" :

Lemme IV ([A] Lemme II 3) : Soient u une unité de $\mathbb{Z}_{K_o}$ et $I = (a, \theta - c)$, si $|u| < 1$ alors ua est un élément réduit de I.

Soient h' un élément réduit de I, u une unité de $\mathbb{Z}_{K_o}$ et h un élément de I tel que $|h| < |uh'|$ ceci entraîne $|u^{-1}h| < |h'|$ puis, h' étant réduit, $|h'^{\sigma^2}| \leq |u^{-\sigma^2} h^{\sigma^2}|$ soit $|(uh')^{\sigma^2}| \leq |h^{\sigma^2}|$. L'ensemble R_I des éléments réduits de l'idéal I est infini. En conservant les notations du lemme IV, considérons les éléments h de I tels que $|au| < |h| < |a|$, puisque $h \in I$ on ne peut avoir $|h^{\sigma^2}| < |a| = |a^{\sigma^2}|$ car alors

$$|h|\,|h^{\sigma^2}| = N_{K_o/\mathbb{Q}}(h) < |a|\,|a^{\sigma^2}| = N_{K_o/\mathbb{Q}}(I).$$

On a donc soit

$$|a^{\sigma^2}| \leq |h^{\sigma^2}| \leq |(au)^{\sigma^2}|$$

soit

$$|h^{\sigma^2}| > |(au)^{\sigma^2}|$$

il n'y a qu'un nombre fini d'éléments de I vérifiant simultanément :

$$|au| < |h| < |a|$$

$$|a| \leq |h^{\sigma^2}| \leq |au^{\sigma^2}|.$$

Choisissons-en un, h_1, tel que h^{σ^2} soit minimal. Il est alors immédiat que, pour tout $h' \in I$ tel que $|h'| < |h_1|$, on a :

$$|h'^{\sigma^2}| \geq |h_1^{\sigma^2}|.$$

En remarquant (cf. [A] lemme I.3) que deux éléments réduits de I, ξ et π, ont même module si et seulement si $\xi = \pi\varepsilon$ où ε est une unité de $\mathbb{Z}_{K_o}$, on peut construire une suite $(h_n)_{n \in \mathbb{N}}$ et une application surjective φ

de $\mathbb{N}$ dans l'ensemble des modules des éléments de $R_I \cup \{|a|\}$ de la façon suivante :

$$h_o = a \qquad \text{et} \qquad \varphi(0) = |h_o|$$

puis $\varphi(n) = |h_n|$ où h_n est un des éléments de $I - \{0\}$ vérifiant :

(i) $|h_n| < |h_{n-1}|$

(ii) pour tout $h \in I - \{0\}$ et $|h| < |h_{n-1}|$ on a $|h^{\sigma^2}| \geq |h_n^{\sigma^2}|$.

On peut alors démontrer :

Théorème V : Soient $I = (a, \theta - c)$ un idéal réduit, $R_I = \{\varepsilon h_n\}$ $\left(n \in \mathbb{N} - \{0\},\ \varepsilon \in \mathbb{Z}_{k_o}^*\right)$ l'ensemble des éléments réduits de I. On définit les idéaux I_n par $I_n = \left(h_{n/a}^{\sigma^2}\right) I$. Les propriétés suivantes sont vérifiées :

(i) Il existe $d \geq 0$ tel que, pour tout n, $I_{n+d} = I_n$, les idéaux I_n sont en nombre fini, ils constituent le cycle de I.

(ii) Les idéaux réduits équivalents à I sont ceux du cycle de I.

(iii) Soit d' le plus petit entier naturel non nul tel que $I_{d'} = I$ alors $h_{d'/a}$ est une unité fondamentale de $\mathbb{Z}_{K_o}$.

Pour construire le cycle de l'idéal réduit I, il suffit de savoir déterminer, pour chaque idéal réduit J, le premier élément de la suite R_J associée. Ceci peut être fait de la façon suivante :

Lemme VI ([A] lemme IV.2) : Soient $I = (a, \theta - c)$ un idéal réduit, M_I l'ensemble de ses racines (c'est-à-dire les entiers c de k_o vérifiant $\theta - c \in I$). Il existe dans M_I un unique élément c_I appelé racine minimale et vérifiant :

(i) $|\theta - c_I| < |a|$.

(ii) Pour tout $c \in M_I$ avec $|\theta - c| < |a|$ on a $|\theta^{\sigma^2} - c_I| \leq |\theta^{\sigma^2} - c|$.

Proposition VII ([A] Lemme IV. 3) : Si $I = (a, \theta - c_1)$ est un idéal réduit, c_1 sa racine minimale et $R_1 = \{\varepsilon h_i\}_{i \in \mathbb{N} - \{0\}}$, $\varepsilon \in \mathbb{Z}_{k_o}^*$, si on écrit $h_1 = \lambda_o a + \mu_o(\theta - c_1)$, on a les inégalités :

$$|\mu_o| < \frac{|a| + |\theta^{\sigma^2} - c_1|}{|\theta - \theta^{\sigma^2}|}, \qquad |\lambda_o| < 1 + |\mu_o|.$$

La construction de l'idéal I_1, successeur de I, est facilitée par la remarque ([A] remarque IV. 5) :

Soient $I = (a, \theta - c_1)$ un idéal réduit, c_1 sa racine minimale et $h_1 = \lambda_o a + \mu_o(\theta - c_1)$ le premier des éléments réduits de I (à une unité de k_o près).

Si $\lambda_o \mu_o = 0$ alors $h_1 = \theta - c_1$ et $I_1 = (b, \theta - c)$ avec $b = f(c_1)/a$ et $c = \theta + \theta^{\sigma^2} - c_1$.

Sinon, λ_o et μ_o sont premiers entre eux et on a $I_1 = (b, \theta - c)$ avec $b = N_{K_o/k_o}(h_1)/a$ et $c = -\left[\lambda_o \lambda_1 a - \lambda_o \mu_1 c_1 + \lambda_1 \mu_o(\theta + \theta^{\sigma^2} - c_1) + \mu_o \mu_1 \frac{f(c_1)}{a}\right]$ où λ_1 et μ_1 sont deux entiers de k tels que :

$$\lambda_o \mu_1 - \mu_o \lambda_1 = 1.$$

Ayant l'idéal réduit I_1, on recommence la construction pour obtenir le cycle de I.

[A] H. AMARA : Groupe des classes et unités fondamentales des extensions quadratiques relatives à un corps quadratique imaginaire principal. Pacific Journal of Mathematics, vol. 96, n°1, (1981), 1-12.

[B] R. BRAUER : Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischer Körpers. Math. Nachr 4, (1951), 158-174.

[C] C. CASTELA : Nombre de classes d'idéaux d'une extension diédrale d'un corps de nombres. Thèse de troisième cycle, Bordeaux I, (1978).

[Ch] A. CHATELET : L'arithmétique des corps quadratiques. Enseignement Mathématique, n° 9, Genève, (1962).

[S1] J.-P. SERRE : Représentation linéaire des groupes finis. Deuxième édition, Hermann, (1971).

[S2] J.-P. SERRE : Corps locaux. Seconde édition, Hermann, (1968).

[Sm] R. SMADJA : Calculs effectifs sur les idéaux des corps de nombres algébriques. Publication du Laboratoire de Mathématiques de l'U.E.R. de Luminy (Université d'Aix-Marseille), Mars 1976.

[Wa] H. WADA : On the class number and the unit group of certain algebraic number fields. Journal Fac. Sci. Univ. Tokyo 13, (1966), pp. 201-209.

[W] C. D. WALTER : Brauer's class number relation. Acta Arithmetica XXXV, (1979), pp. 33-40.

Venons-en maintenant à l'exemple numérique. Choisissons $N = \mathbb{Q}\left(\sqrt{1+i}, \sqrt{1-i}\right)$ et fixons $K_o = \mathbb{Q}\left(\sqrt{1+i}\right)$, $k_o = \mathbb{Q}(i)$.

§ 5 - Nombre de classes de $\mathbb{Q}\left(\sqrt{1+i}\right)$:

L'idéal premier au-dessus de 2 dans $\mathbb{Z}[i]$ étant engendré par $(1+i)$, on a $\theta = \sqrt{1+i}$ et le discriminant de K_o/k_o est engendré par $4(1+i)$ et donc $D_{K_o/\mathbb{Q}} = 16 \times 2 \times 16 = 2^9$.

On devra avoir $|a|^2 \leq \frac{4}{\pi^2}\sqrt{512} \# 9.1705$.

Soit $0 < |a| \leq 3{,}0283$.

Les normes a possibles, à une unité de $\mathbb{Z}[i]$ près, sont

$1,\ 2,\ 3,\ 1+i,\ 1+2i,\ 2+i,\ 2+2i$ qui ont pour modules

$1,\ 2,\ 3,\ \sqrt{2},\ \sqrt{5},\ \sqrt{5},\ 2\sqrt{2}$.

On regarde les éléments c de $\mathbb{Z}[i]$ tel que $|\theta - c| < 3$ et on dresse le tableau suivant :

c	$\lvert\theta - c\rvert$	$f(c) = c^2 - (1+i)$	Décomposition de f(c) en éléments irréductibles
$-2i$	2,6897...	$-5-i$	$-(3-2i)(1+i)$
$1-2i$	2,4571...	$-4-5i$	$-(4+5i)$
$2-2i$	2,6153...	$-1-9i$	$-i(4-5i)(1+i)$
$-1-i$	2,5538...	$-1+i$	$i(1+i)$
$-i$	1,8233...	$-2-i$	$-(2+i)$
$1-i$	1,4584...	$-1-3i$	$-(2+i)(1+i)$
$1-2i$	2,4571...	$-4-5i$	$-(4+5i)$
$3-i$	2,3942...	$7-7i$	$-7i(1+i)$
-1	2,1475...	$-i$	$-i$
0	1,1892...	$-1-i$	$-(1+i)$
1	0,4657...	$-i$	$-i$
2	1,0097...	$3-i$	$-i(2+i)(1+i)$
3	1,9550...	$8-i$	$(3-2i)(2+i)$
4	2,9368...	$15-i$	$-i(8+7i)(1+i)$
$-1+i$	2,1683...	$-1-3i$	$-(2+i)(1+i)$
i	1,2264...	$-2-i$	$-(2+i)$
$1+i$	0,5538...	$-1+i$	$i(1+i)$
$2+i$	1,0532...	$2+3i$	$2+3i$
$3+i$	1,9779...	$7+5i$	$(6-i)(1+i)$
$4+i$	2,9520...	$14+7i$	$7(2+i)$
$-1+2i$	2,6060...	$-4-5i$	$-(4+5i)$
$2i$	1,8957...	$-5-i$	$-(3-2i)(1+i)$
$1+2i$	1,5481...	$-4+3i$	$i(2+i)^2$
$2+2i$	1,7886...	$-1+7i$	$(-4+3i)(1-i)$
$3+2i$	2,4498...	$4+11i$	$4+11i$
$3i$	2,7719...	$-10-i$	$-(10+i)$
$3i+1$	2,5468...	$-9+5i$	$-i(7+2i)(1+i)$
$3i+2$	2,6998...	$-6+11i$	$-6+11i$

qui nous permet de conclure que :

pour $a = 3,\ (1+i)^3,\ 2,\ (1+2i),$ il n'y a aucun c tel que $f(c) \equiv 0\ (a)$.

Pour $a = 2+i$, les valeurs suivantes de c sont telles que $f(c) \equiv 0\ (a)$ $c = -i,\ 1-i,\ 2,\ 3,\ -1+i,\ i,\ 4+i,\ 1+2i,\ 2+2i$.

Parmi celles-ci, les valeurs de c qui suivent satisfont à $|\theta - c| < |2+i|$: $c = -i,\ 1-i,\ 2,\ 3,\ -1+i,\ i,\ 1+2i,\ 2+2i$ mais on a les relations :

$2 = -i+(2+i)$; $-1+i = -i+i(2+i)$; $1+2i = -i+(2+i)(1+i)$

$1-i = i-i(2+i)$; $3 = i-i(2+i)(1+i)$; $2+2i = i+(2+i)$.

On en déduit que les idéaux $(2+i, \theta+i)$; $(2+i, \theta-i)$ sont peut-être réduits.

Pour $a = 1+i$, les valeurs suivantes de c sont telles que $f(c) \equiv 0\ (a)$, $c = -2i$; $2-2i$; $-1-i$; $1-i$; $3-i$; 0 ; 2 ; 4 ; $-1+i$; $1+i$; $3+i$; $2i$; $2+2i$; $3i+1$.

Les seules qui satisfont à $|\theta - c| < |2+i|$ sont :
$c = 0$; $c = 2$; $c = 1+i$.

Toutes ces valeurs sont congrues entre elles modulo $1+i$, on retient donc l'idéal $(1+i, \theta)$ qui est peut-être réduit.

Pour $a = 1$, la congruence est toujours vérifiée mais seuls $c = 1$ et $c = 1+i$ sont tels que $|\theta - c| < 1$.

On obtient donc $(1, \theta - 1) = \mathbb{Z}_{K_o}$.

Les idéaux qui restent après cette étape sont :
$(2+i, \theta+i)$; $(2+i, \theta-i)$; $(1+i, \theta)$; $(1, \theta-1)$ mais les relations $\theta^2 = 1+i$; $(\theta+i)(-\theta+i) = (\theta-i)(-\theta-i) = -1-\theta^2 = -(2+i)$ montrent que tous ces idéaux sont principaux.

On a par conséquent $h_{\mathbb{Z}[\sqrt{1+i}]} = 1$.

§6 - Unité fondamentale de $\mathbb{Q}(\sqrt{1+i})$:

En revenant à la définition d'un idéal réduit, on constate que $\mathbb{Z}_{K_o}$ est réduit. Cherchons sa racine minimale.

Les c tels que $|\theta - c| < 1$ sont $c = 1$; $c = 1+i$.

On a $|-\theta - 1| = 2,1474...$ $\quad |-\theta - (1+i)| = 2,5537...$

La racine minimale est donc $c = 1$.

La proposition VII permet de limiter la recherche de h_1 aux éléments $h = \lambda a + \mu(\theta - 1)$ avec

$$|\mu| < \frac{1 + |-\sqrt{1+i} - 1|}{|\sqrt{1+i} + \sqrt{1+i}|} = 1,32... \qquad |\lambda| < 2,32...$$

ce qui permet de choisir $\mu = 0$, $\mu = 1$ et $\lambda = 0, 1, 1+i, i, -1+i, -1, -1-i, -i, 1-i, 2, 2+i, 1+2i, 2i, -1+2i, -2+i, -2, -2-i, -1-2i, -2i, 1-2i, 2-i$.

On établit alors le tableau suivant :

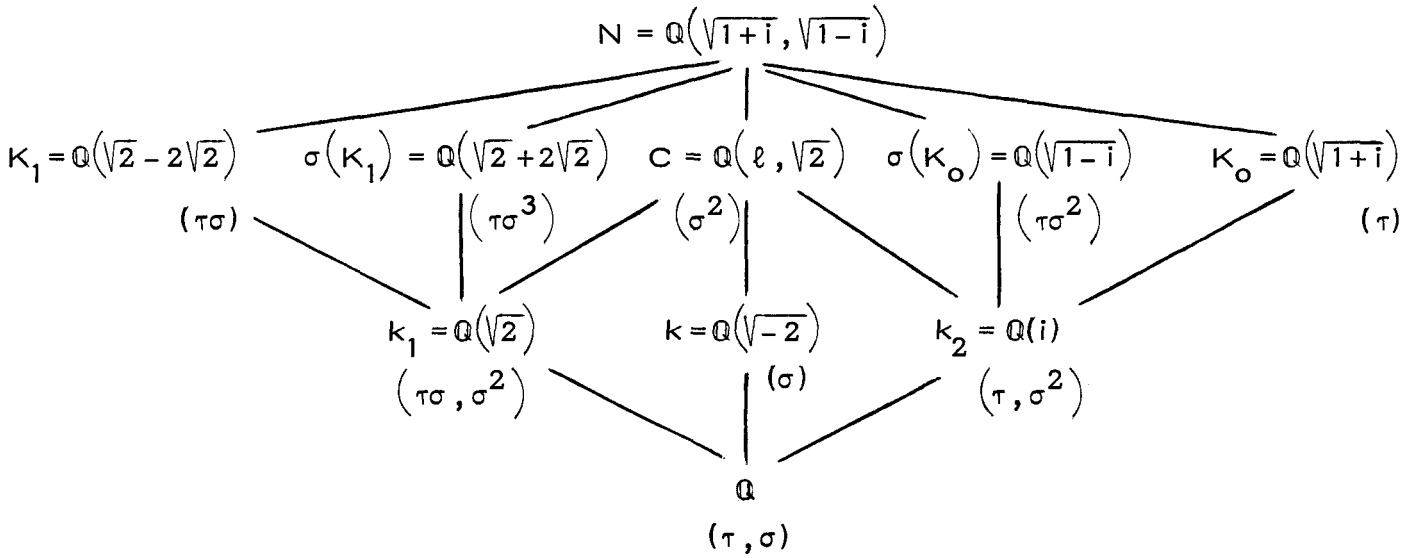
h	$-h^{\sigma^2}$	module de h^{σ^2}
$\theta - 1$	$\theta + 1$	2,1475...
$1+\theta-1$	θ	1,1892...
$1+i+\theta-1$	$\theta - i$	1,2264...
$i+\theta-1$	$1-i+\theta$	2,1683...
$-1+i+\theta-1$	$2-i+\theta$	3,1462...
$-1+\theta-1$	$2+\theta$	3,9534...
$-1-i+\theta-1$	$2+i+\theta$	3,4233...
$-i+\theta-1$	$1+i+\theta$	2,5538...
$1-i+\theta-1$	$\theta+i$	1,8233...
$2+\theta-1$	$\theta-1$	0,4657...
$2+i+\theta-1$	$-1-i+\theta$	0,5538...
$1+2i+\theta-1$	$-2i+\theta$	1,8957...
$2i+\theta-1$	$1-2i+\theta$	2,6060...
$-1+2i+\theta-1$	$2-2i+\theta$	3,4625...
$-2+i+\theta-1$	$3-i+\theta$	4,1347...
$-2+\theta-1$	$3+\theta$	4,1239...
$-2-i+\theta-1$	$3+i-\theta$	4,3493...
$-1-2i+\theta-1$	$2+2i+\theta$	3,9534...
$-2i+\theta-1$	$1+2i+\theta$	3,2299...
$1-2i+\theta-1$	$2i+\theta$	2,6897...
$2-i+\theta-1$	$-1+i+\theta$	1,4584...

Pour $\mu = 0$, le module de h^{σ^2} serait entier donc supérieur à 0,4657. L'élément h_1 est donc égal à $1+\theta$ qui est une unité. Construisons le successeur de $\mathbb{Z}_{K_o}$ dans son cycle, la norme de cet idéal est $b = N_{K_o/k_o}(1+\theta)$; c'est donc une unité et le successeur de $\mathbb{Z}_{K_o}$ est $\mathbb{Z}_{K_o}$.

Le théorème V permet d'affirmer que l'unité fondamentale est $1+\theta$.

§ 7 - Le corps N et ses sous-corps :

On peut établir rapidement le diagramme représentant les sous-corps de N. On indique à côté de chaque corps L un système de générateurs de Gal (N/L).



On peut décrire les éléments du groupe de Galois par leur action sur les éléments de N :

On choisit σ tel que $\sigma(\sqrt{1+i}) = \sqrt{1-i}$ et $\sigma(\sqrt{2}) = -\sqrt{2}$

$\tau(\sqrt{1+i}) = \sqrt{1+i}$ et $\tau(\sqrt{2}) = -\sqrt{2}$

ce qui donne :

	$\sqrt{1+i}$	$\sqrt{1-i}$
σ	$\sqrt{1-i}$	$-\sqrt{1+i}$
σ^2	$-\sqrt{1+i}$	$-\sqrt{1-i}$
σ^3	$-\sqrt{1-i}$	$\sqrt{1+i}$
τ	$\sqrt{1+i}$	$-\sqrt{1-i}$
$\tau\sigma^2$	$-\sqrt{1+i}$	$\sqrt{1-i}$
$\tau\sigma$	$-\sqrt{1-i}$	$-\sqrt{1+i}$
$\tau\sigma^3$	$\sqrt{1-i}$	$\sqrt{1+i}$

§ 8 - Recherche des unités de N :

Le groupe E_C des unités de C est engendré la racine huitième de l'unité $\frac{1+i}{\sqrt{2}}$ et l'unité fondamentale $1+\sqrt{2}$.

Le groupe E_{K_o} des unités de K_o est engendré par i et l'unité fondamentale $1+\sqrt{1+i}$.

Le groupe $E_{\sigma(K_o)}$ des unités de $\sigma(K_o)$ est engendré par i et l'unité fondamentale $1+\sqrt{1-i}$.

Le sous-groupe $E_C E_{K_o} E_{\sigma(K_o)}$ de E_N est donc engendré par $\frac{1+i}{\sqrt{2}}$, $1+\sqrt{2}$, $1+\sqrt{1-i}$, $1+\sqrt{1+i}$.

Il nous faut regarder quels sont, parmi les représentants de $E_C E_{K_o} E_{\sigma(K_o)}$ modulo ses carrés, les éléments qui deviennent des carrés dans N.

. $\frac{1+i}{\sqrt{2}}$ n'est pas un carré dans N car alors N serait le corps des racines 16ème de l'unité, donc une extension abélienne de $\mathbb{Q}$.

. $1+\sqrt{2}$ a pour norme $(1+\sqrt{2})^2$, -1, -1 sur C, K_o, $\sigma(K_o)$ ces éléments sont des carrés de ces corps.

Nous appliquons la méthode de Wada :

$B_1 = 1+\sqrt{2}$, $B_2 = i$, $B_3 = i$ $\qquad B_1 B_2 B_3 = -(1+\sqrt{2}) = (1+\sqrt{2}) B_3^2$

$b = -1$ ce qui donne

$\xi = -2(1+\sqrt{2+i})$ qui a pour trace sur k_o $\quad c = -8(1+i) = 4(1-i)^2(1-i)$

qui est un carré dans N.

La racine carrée de $1+\sqrt{2}$ est égale à $\frac{\xi}{\sqrt{c}\, B_3}$:

$$1+\sqrt{2} = \left[\frac{(1+i+\sqrt{2})\sqrt{1-i}}{2}\right]^2.$$

. $1+\sqrt{1+i}$ a pour normes $(1+\sqrt{1+i})^2$, $-i$, $-i$ sur K_o, C, $\sigma(K_o)$ mais $-i$ n'est pas un carré dans $\sigma(K_o)$.

. Résultat analogue pour $1+\sqrt{1-i}$.

. $\frac{1+i}{\sqrt{2}}\left(1+\sqrt{1+i}\right)$ a pour normes 1, -1, $-i\left(1+\sqrt{1+i}\right)^2$ sur c, $\sigma(K_o)$, K_o mais $-i$ n'est pas un carré dans K_o.

. Résultat analogue pour $\frac{1+i}{\sqrt{2}}\left(1+\sqrt{1-i}\right)$.

. $\left(1+\sqrt{1+i}\right)\left(1+\sqrt{1-i}\right)$ a pour norme $\left(1+\sqrt{1-i}\right)^2 \times (-i)$ sur $\sigma(K_o)$ or cet élément n'est pas un carré dans $\sigma(K_o)$.

. Il reste à considérer $A = \frac{1+i}{\sqrt{2}}\left(1+\sqrt{1+i}\right)\left(1+\sqrt{1-i}\right)$. On a

$N_{N/C}(A) = \left(\frac{1+i}{\sqrt{2}}\right)^2 \quad N_{N/K_o}(A) = \left(1+\sqrt{1+i}\right)^2 \quad N_{N/\sigma(K_o)}(A) = -\left(1+\sqrt{1-i}\right)^2$

qui sont des carrés dans les corps respectifs.

Posons $B_1 = \frac{1+i}{\sqrt{2}}$, $B_2 = -i\left(1+\sqrt{1-i}\right)$, $B_3 = 1-\sqrt{1+i} = \frac{-i}{1+\sqrt{1+i}}$. On a

$B_1 B_2 B_3 = A B_3^2$.

Soit alors $b = -i$, $\xi = B_1 B_2 B_3 + b\left(B_1 + B_2 + B_3\right) = (1-i)\sqrt{2} - 2\sqrt{1-i} - 2$

a pour trace sur k_o : $-8 = \left(2\sqrt{-2}\right)^2$ qui est un carré dans N. On en déduit qu'une racine carrée de $\frac{1+i}{\sqrt{2}}\left(1+\sqrt{1+i}\right)\left(1+\sqrt{1-i}\right)$ est $\frac{1}{2}\left[(1+i)\left(1+\sqrt{1-i}\right)+\sqrt{2}\right]$.

Le groupe E_N est donc engendré par

$$\zeta = \frac{1+i}{\sqrt{2}}, \quad \varepsilon_1 = \frac{\left(1+i+\sqrt{2}\right)\sqrt{1-i}}{2}, \quad \varepsilon_2 = 1+\sqrt{1+i}, \quad \varepsilon_3 = \frac{(1+i)\left(1+\sqrt{1-i}\right)+\sqrt{2}}{2}.$$

Il faut maintenant déterminer l'action du groupe de Galois sur E_N.

§ 9 - Action du groupe de Galois sur E_N et unités des sous-corps :

$$\tau(\zeta) = -\frac{1+i}{\sqrt{2}} = \left(\frac{1+i}{\sqrt{2}}\right)^5 \quad ; \quad \sigma(\zeta) = \frac{-1+i}{\sqrt{2}} = \left(\frac{1+i}{\sqrt{2}}\right)^3$$

$$\tau(\varepsilon_2) = \varepsilon_2 \quad ; \quad \sigma(\varepsilon_2) = 1+\sqrt{1-i} = \zeta^{-1}\varepsilon_2^{-1}\varepsilon_3^2$$

$$\tau(\varepsilon_1) = -\frac{\left(1+i-\sqrt{2}\right)\sqrt{1-i}}{2} = \zeta^6 \varepsilon_1^{-1} \quad ; \quad \sigma(\varepsilon_1) = -\frac{\left(1-i-\sqrt{2}\right)\sqrt{1+i}}{2} = \zeta^2 \varepsilon_1^{-1}$$

$$\tau(\varepsilon_3) = \frac{(1+i)\left(1-\sqrt{1-i}\right)-\sqrt{2}}{2} = \zeta^4 \varepsilon_2 \varepsilon_3^{-1} \quad ; \quad \sigma(\varepsilon_3) = -\frac{2\sqrt{1+i}+(1+i)\sqrt{2}}{2} = \zeta^4 \varepsilon_3 \varepsilon_2^{-1}$$

que l'on peut résumer par le tableau suivant :

	τ	σ
ζ	ζ^5	ζ^3
ε_1	$\zeta^6 \varepsilon_1^{-1}$	$\zeta^2 \varepsilon_1^{-1}$
ε_2	ε_2	$\zeta^{-1} \varepsilon_2^{-1} \varepsilon_3^2$
ε_3	$\zeta^4 \varepsilon_2 \varepsilon_3^{-1}$	$\zeta^4 \varepsilon_3 \varepsilon_2^{-1}$

Il reste à déterminer E_{K_1} et $E_{\sigma(K_1)}$.

L'action du groupe de Galois sur E_N permet de constater rapidement que ε_1 est invariant par $\tau\sigma^3$. Cherchons une autre unité invariante par $\tau\sigma^3$, cette unité de la forme $\zeta^u \varepsilon_2^w \varepsilon_3^t$ vérifie donc

$$\zeta^u \varepsilon_2^w \varepsilon_3^t = \tau\sigma^3\left(\zeta^u \varepsilon_2^w \varepsilon_3^t\right) = \zeta^{-u-t+3w} \varepsilon_2^{-w} \varepsilon_3^{2w+t}$$

ce qui conduit à $w = 0$, $t = 2$, $u = -1$.

Le groupe des unités de $\sigma(K_1)$ est engendré par -1 ; ε_1 ; $\zeta^{-1} \varepsilon_3^2$.

On en déduit que les unités de K_1 sont engendrées par -1 ; $\zeta^2 \varepsilon_1^{-1}$; $\zeta^{-3} \varepsilon_2^{-2} \varepsilon_3^2$.

Le module $\overline{E_N} = E_N/\langle\zeta\rangle$ est sans torsion, engendré par les classes $\overline{\varepsilon_i}$ des éléments ε_i vérifiant donc :

$$\tau\left(\overline{\varepsilon_1}\right) = \sigma\left(\overline{\varepsilon_1}\right) = \overline{\varepsilon_1^{-1}}$$

$$\tau\left(\overline{\varepsilon_2}\right) = \overline{\varepsilon_2} \quad , \quad \sigma\left(\overline{\varepsilon_2}\right) = \overline{\varepsilon_2^{-1}}\,\overline{\varepsilon_3^2}$$

$$\tau\left(\overline{\varepsilon_3}\right) = \overline{\varepsilon_2}\,\overline{\varepsilon_3^{-1}} \quad , \quad \sigma\left(\overline{\varepsilon_3}\right) = \overline{\varepsilon_3}\,\overline{\varepsilon_2^{-1}}.$$

§ 10 - Le module M :

Le sous-corps réel de N est $\sigma(K_1)$, invariant par $\tau\sigma^3$. Si on reprend les notations du § 2, le module M est isomorphe au module L défini

par la suite exacte :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G]\left(1+\tau\sigma^3\right) \longrightarrow L \longrightarrow 0$$

où l'injection est définie par $n \longrightarrow n \sum_{g \in G} g$.

Les relations dans $\mathbb{Z}[G]$ montrent que la base sur $\mathbb{Z}$ de $\mathbb{Z}[G]\left(1+\tau\sigma^3\right)$ est $1+\tau\sigma^3$, $\sigma+\tau\sigma^2$, $\sigma^2+\tau\sigma$, $\sigma^3+\tau$.

Le sous-module, image de $\mathbb{Z}$, a pour base $1+\sigma+\sigma^2+\sigma^3+\tau\left(1+\sigma+\sigma^2+\sigma^3\right)$, on choisit alors pour base de $\mathbb{Z}[G]\left(1+\tau\sigma^3\right)$

$1+\sigma+\sigma^2+\sigma^3+\tau\left(1+\sigma+\sigma^2+\sigma^3\right)$; $1+\tau\sigma^3$, $\sigma+\tau\sigma^2$, $\sigma^2+\tau\sigma$.

Le module L est engendré par e_1, e_2, e_3 qui sont les classes de $1+\tau\sigma^3$, $\sigma+\tau\sigma^2$, $\sigma^2+\tau\sigma$.

Déterminons l'action de G sur L :

$$\sigma(e_1) = e_2, \quad \sigma(e_2) = e_3, \quad \sigma(e_3) = -(e_1+e_2+e_3)$$

$$\tau(e_1) = -(e_1+e_2+e_3), \quad \tau(e_2) = e_3, \quad \tau(e_3) = e_2.$$

On constate en plus que $\left(1+\sigma+\sigma^2+\sigma^3\right)e_1 = 0$, $\tau\sigma^3(e_1) = e_1$.

Si on prend $\varepsilon = \overline{\varepsilon}_1\ \overline{\varepsilon}_3$, on constate facilement que le $\mathbb{Z}[G]$ module engendré par ε dans $\overline{E_N}$ est isomorphe à L ; on choisit $M = \mathbb{Z}[G]\varepsilon$ qui a pour $\mathbb{Z}$-base

$$\varepsilon, \quad \sigma(\varepsilon) = \overline{\varepsilon}_1^{-1}\,\overline{\varepsilon}_2^{-1}\,\overline{\varepsilon}_3, \quad \sigma^2(\varepsilon) = \overline{\varepsilon}_1\,\overline{\varepsilon}_3^{-1}$$

et est d'indice 2 dans $\overline{E_N}$.

§ 11 - <u>Calcul des indices et des nombres de classes</u> :

Si on reprend les formules 3 et 4 du § 2, on voit qu'interviennent les indices $[\overline{E_N^H} : M^H]$; $[\overline{E_N^{G'_o}} : M^{G'_o}]$, les corps k et k'_o étant quadratiques imaginaires, ces indices sont donc égaux à 1.

Il faut maintenant déterminer M^{G_o}, M^{G_1}, $M^{G'_1}$. Les relations que l'on a trouvées entre les éléments de L montrent que

L^{G_1} est engendré par e_2 et e_1+e_3

$L^{G'_1}$ est engendré par e_1+e_3

L^{G_o} est engendré par $e_2 + e_3$

comme groupes abéliens.

Calcul de $[\overline{E_N} : M]$: $\overline{E_N}$ a pour base sur $\mathbb{Z}$: $\bar{\varepsilon}_1$, $\bar{\varepsilon}_2$, $\bar{\varepsilon}_3$.

L'image de M dans $\overline{E_N}$ a pour $\mathbb{Z}$-base : $\bar{\varepsilon}_1\,\bar{\varepsilon}_3$, $\bar{\varepsilon}_1^{-1}\,\bar{\varepsilon}_2^{-1}\,\bar{\varepsilon}_3$, $\bar{\varepsilon}_1\,\bar{\varepsilon}_3^{-1}$.

L'indice $[\overline{E_N} : M] = 2$.

Calcul de $[\overline{E_N^{G_o}} : M^{G_o}]$: $E_N^{G_o}$ est engendré par -1 et ε_2 donc $\overline{E_N^{G_o}}$ est engendré par $\bar{\varepsilon}_2$, M^{G_o} est engendré par $\sigma(\varepsilon)\sigma^2(\varepsilon) = \bar{\varepsilon}_2^{-1}$, son image dans $\overline{E_N}$ est engendrée par $\bar{\varepsilon}_2$ et $[\overline{E_N^{G_o}} : M^{G_o}] = 1$.

Calcul de $[\overline{E_N^{G_1}} : M^{G_1}]$: $E_N^{G_1}$ est engendré par -1, $\zeta^2\,\varepsilon_1^{-1}$, $\zeta^{-3}\,\varepsilon_2^{-2}\,\varepsilon_3^2$ donc $\overline{E_N^{G_1}}$ admet pour générateurs $\bar{\varepsilon}_1$, $\bar{\varepsilon}_2^{-1}\,\bar{\varepsilon}_3$; l'image de M^{G_1} a pour générateurs $\sigma(\varepsilon) = \bar{\varepsilon}_1^{-1}\,\bar{\varepsilon}_2^{-1}\,\bar{\varepsilon}_3$ et $\varepsilon\,\sigma^2(\varepsilon) = \bar{\varepsilon}_1^2$, on en déduit que

$$[\overline{E_N^{G_1}} : M^{G_1}] = 1 .$$

Calcul de $[\overline{E_N^{G_1'}} : M^{G_1'}]$: $E_N^{G_1'}$ a pour système de générateurs : -1, ε_1^2 donc la base de $\overline{E_N^{G_1'}}$ est $\bar{\varepsilon}_1^2$, $M^{G_1'}$ a pour base $\varepsilon\,\sigma^2(\varepsilon) = \varepsilon_1^2$ donc $[\overline{E_N^{G_1'}} : M^{G_1'}] = 1$.

On sait par ailleurs que $w_2(N) = 8$, $w_2(K_o) = 4 = w_2(k_o)$, $w_2(K_1) = w_2(k_1) = 2$, $h_k = h_{K_o} = 1$.

La formule 4 nous donne :

$$\frac{1}{1} = \frac{h_{K_1}}{1} \times \frac{4 \times 2}{4 \times 2} \times \frac{1}{1} \times \frac{1}{1} \qquad \text{soit} \qquad h_{K_1} = 1 = h_{\sigma(K_1)} .$$

En reportant dans la formule 3

$$h_N = 1 \times 1 \times 1 \times \frac{8}{4 \times 2 \times 2} \times \frac{2}{1 \times 1} = 1.$$

On peut remarquer que l'existence d'une unité de Minkowski imposerait à tous les indices de groupes d'unités d'être égaux à 1 ce qui donnerait $h_N = \frac{1}{2}$.

Université de Besançon et C.N.R.S.
Laboratoire de Mathématiques
U.A. 741
Faculté des Sciences
F 25030 BESANCON CEDEX