THEORIE DES NOMBRES
BESANCON

Années 1984/85-1985/86
Fascicule 2

GROUPE DES CLASSES ET UNITES FONDAMENTALES DE LA 4-EXTENSION NON RAMIFIEE DE $\mathbb{Q}(\sqrt{-p})$ AVEC p PREMIER ET $p \equiv 1\ (8)$

Hedi AMARA

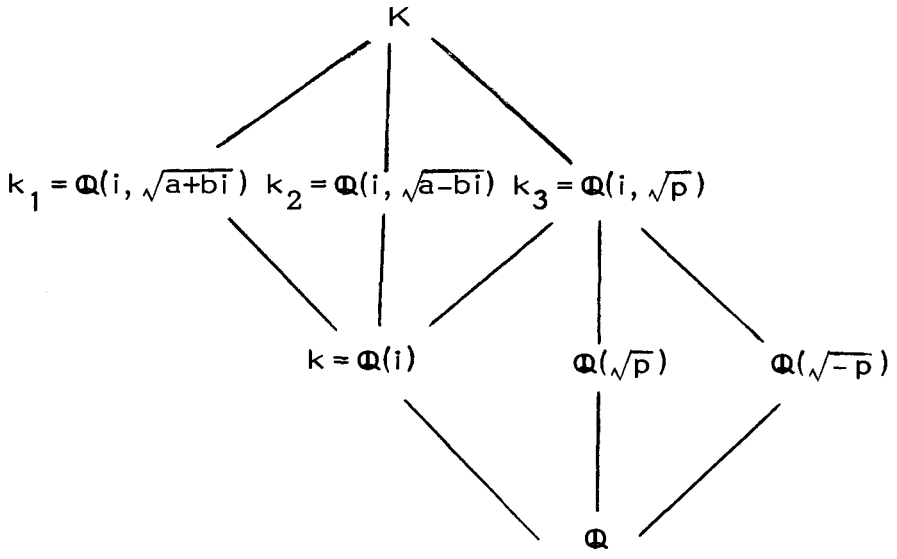
GROUPE DES CLASSES ET UNITES FONDAMENTALES DE LA 4-EXTENSION NON RAMIFIEE DE $\mathbb{Q}(\sqrt{-p})$ AVEC p PREMIER ET $p \equiv 1 \quad (8)$

Hedi AMARA

Il est bien connu (voir par exemple [3]) que le 2-groupe des classes de $\mathbb{Q}(\sqrt{-p})$, où p est un nombre premier congru à 1 (mod 8) , est cyclique d'ordre supérieur ou égal à 4 . Il existe donc une unique extension K de degré 4 non ramifiée de $\mathbb{Q}(\sqrt{-p})$; on vérifie facilement que si a et b sont deux entiers positifs vérifiant :

$$p = a^2 + b^2 \ , \ a \text{ impair et } \ 4/b \ ,$$

on a le diagramme suivant :



K est donc une extension bicyclique de $k = \mathbb{Q}(i)$, diédrale sur $\mathbb{Q}$.

Dans [1] nous avons établi un théorème qui ramène le calcul du nombre des classes de K à ceux de k_1, k_2, k_3 et à un calcul d'un indice d'unités.

Une adaptation d'une méthode de Wada faite dans [4] permet alors de calculer cet indice et de dégager un système d'unités fondamentales de K en fonction des unités fondamentales de k_1 , k_2 et k_3 .

1. RAPPEL DES RESULTATS DE [1] ET [4] .

On désigne pour tout corps de nombres K par : $\mathcal{H}_K$, $\mathcal{H}'_K$, h_K , U_K et E_K le groupe des classes , le groupe des classes d'ordre impair , le nombre des classes , le groupe des unités et le groupe des unités modulo la torsion .

THEOREME [1] :

1) $\mathcal{H}'_K \simeq \mathcal{H}'_{k_1} \times \mathcal{H}'_{k_2} \times \mathcal{H}'_{k_3}$

2) $h_K = \frac{a}{4} h_{k_1} \cdot h_{k_2} \cdot h_{k_3}$ où $a = [E_K : E_{k_1} E_{k_2} E_{k_3}]$

Soit ε_i une unité fondamentale de k_i ($i = 1, 2, 3$) et

$$A = \{ \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_1\varepsilon_2, \varepsilon_1\varepsilon_3, \varepsilon_2\varepsilon_3, \varepsilon_1\varepsilon_2\varepsilon_3 \} .$$

Pour tout $\varepsilon \in U_{k_1} \times U_{k_2} \times U_{k_3}$, tel que : $N_{K/k_i}(\varepsilon)$ est un carré dans K , on pose :

$$B_1^2 = N_{K/k_1}(\varepsilon) , \quad B_2^2 = N_{K/k_3}(\varepsilon) , \quad B_3^2 = (N_{K/k_3}(\varepsilon))^{\tau}$$

où :

$$\tau \in \mathrm{Gal}(K/k_3) \quad \text{et} \quad \tau \neq 1 .$$

Posons en plus :

$$b = N_{k_i/k}(B_i) , \quad \theta = B_1B_2B_3 + b(B_1+B_2+B_3)$$

et :

$$c = \mathrm{Trace}_{K/k}(\theta) .$$

On a la proposition suivante :

PROPOSITION : [1] et [4]

1) Si n désigne le nombre des éléments de l'ensemble A qui sont des carrés modulo les racines de l'unité , alors :

$$a = n + 1 .$$

2) Pour tout $\varepsilon \in U_{k_1} \times U_{k_2} \times U_{k_3}$, tel que $N_{K/k_i}(\varepsilon)$ est un carré dans k_i pour tout $i \in \{1, 2, 3\}$, on a :

ε est un carré dans $K \Leftrightarrow c$ est un carré dans K .

2. DETERMINATION DE L'INDICE a .

i) Comme $D_{k_1/k}$ et $D_{k_2/k}$ sont les nombres premiers $a + bi$ et $a - bi$, alors $N_{k_1/k}(\varepsilon_1)$ et $N_{k_2/k}(\varepsilon_2)$ appartiennent à $\{\pm i\}$, si bien que :

$N_{k/k_3}(\zeta \varepsilon_1)$, $N_{k/k_3}(\zeta \varepsilon_2)$ sont dans $\{\pm i\}$ pour tout $\zeta \in \{\pm 1 , \pm i\}$.

Par conséquent ε_1 et ε_2 ne sont pas des carrés dans K modulo les racines de l'unité .

ii) $N_{K/k_1}(\zeta \varepsilon_1 \varepsilon_2) = \pm i \varepsilon_1^2$ pour tout $\zeta \in \{\pm 1 , \pm i\}$ et donc $\varepsilon_1 \varepsilon_2$ n'est pas un carré dans K modulo les racines de l'unité .

iii) On peut prendre pour ε_3 l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$.

Soient S et T deux entiers positifs tels que $\varepsilon_3 = S + T\sqrt{p}$; alors :

$$B_1 = i , \quad B_2 = i , \quad B_3 = \varepsilon_3^T = S - T\sqrt{p} ;$$

$$b = -1 \quad \text{et} \quad \theta = -2S - 2i + 2T\sqrt{p} ;$$

$$c = Tr_{K/k}(\theta) = -4(2S + 2i) = -8i(1 - iS)$$

d'où c est un carré dans $K \Leftrightarrow 1 - iS$ est un carré dans K .

$S^2 + 1 = pT^2 = (a + bi)(a - bi)T^2$ (dans $\mathbb{Z}[i]$) .

Supposons donc que $a + bi$ divise $1 - iS$:

$$1 - iS = \gamma(a + bi) \text{ , avec } \gamma \in \mathbb{Z}[i] \text{ et } N(\gamma) = T^2 \text{ .}$$

Comme γ est sans facteur rationnel on a :

$$\gamma = \nu^2 \text{ ou } \gamma = i\nu^2 \text{ avec } \nu \in \mathbb{Z}[i] \text{ .}$$

$\gamma = i\nu^2$ est impossible car sinon :

$$\nu = c + di$$

$$\nu^2 = c^2 - d^2 + 2cdi$$

$$i\nu^2 = -2cd + i(c^2 - d^2)$$

$$1 - iS = (a+bi)[-2cd + i(c^2 - d^2)]$$

et donc :

$$-2cda - b(c^2 - d^2) = 1 \text{ .}$$

Ceci est absurde (b est pair) .

En résumé :

$1 - iS = (a + bi)\nu^2$, et donc $1 - iS$ est un carré dans K .

iv) ε_3 étant un carré dans K alors $\varepsilon_1\varepsilon_3$, $\varepsilon_2\varepsilon_3$ et $\varepsilon_1\varepsilon_2\varepsilon_3$ ne sont pas des carrés dans K modulo les racines de l'unité .

THEOREME :

1) $h_K = \frac{1}{2} h_{k_1} . h_{k_2} . h_{k_3}$

2) ε_1 , ε_2 , $\sqrt{\varepsilon_3}$ est un système fondamental d'unités de K , où $\sqrt{\varepsilon_3} = \frac{1+i}{2}(\sqrt{1 - iS} - i\sqrt{1 + iS})$ avec $\varepsilon_3 = S + T\sqrt{p}$.

REMARQUE :

Dans la démonstration de iii) on peut dégager le résultat suivant :

Si $\varepsilon = S + T\sqrt{p}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ ($p \equiv 1$ (8) et premier) alors :

Pour tout nombre premier q qui divise T on a : $q \equiv 1$ (4) .

3. EXEMPLES .

a) $p = 17$

$k_1 = \mathbb{Q}(i, \sqrt{1+4i})$, $k_2 = \mathbb{Q}(i, \sqrt{1-4i})$ et $k_3 = \mathbb{Q}(i, \sqrt{17})$.

Par l'algorithme de [2] on a :

$$h_{k_1} = h_{k_2} = 1 \ , \quad \varepsilon_1 = \frac{1+\sqrt{1+4i}}{2} \quad \text{et} \quad \varepsilon_2 = \frac{1+\sqrt{1-4i}}{2} \ .$$

D'autre part :

$$h_{k_3} = 2 \quad \text{et} \quad \varepsilon_3 = 4 + \sqrt{17} \ .$$

Ainsi pour $K = \mathbb{Q}(i, \sqrt{1+4i}, \sqrt{17})$ on a :

$$h_K = 1 \text{ et } \left\{ \frac{1+\sqrt{1+4i}}{2} , \frac{1+\sqrt{1-4i}}{2} , \frac{1+i}{2}\left(\sqrt{1-4i} - i\sqrt{1+4i}\right) \right\}$$

est un système d'unités fondamentales .

b) $p = 2137$

$k_1 = \mathbb{Q}(i, \sqrt{29+36i})$, $k_2 = \mathbb{Q}(i, \sqrt{29-36i})$ $k_3 = \mathbb{Q}(i, \sqrt{2137})$ et

$$K = \mathbb{Q}(i, \sqrt{29+36i}, \sqrt{2137}) \ .$$

D'après [1] on a :

$$h_{k_1} = h_{k_2} = 7 \ , \quad \varepsilon_1 = \frac{(1+i)\sqrt{29+36i} - 3 - 9i}{2} \quad \varepsilon_2 = \overline{\varepsilon}_1 \text{ et } h_{k_3} = 8 \ .$$

Comme le 2-groupe des classes de K est cyclique , alors :

$$\mathcal{H}_K \simeq \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}} \ .$$

BIBLIOGRAPHIE .

[1] H. AMARA :

Détermination de la structure du groupe des classes, et de l'unité fondamentale des extensions quadratiques relatives d'un corps quadratique imaginaire principal .
Thèse de 3^{eme} cycle . Grenoble (1977) .

[2] H. AMARA :

Groupe des classes et unité fondamentale des extensions quadratiques relatives à un corps quadratique imaginaire principal .
Pacific Math. J. Vol. 96 N° 1 (1981) .

[3] H. COHN - G. COOKE :

Parametric form of an eight class-field .
Acta arith. XXX (1976) .

[4] J. COUGNARD :

Groupe des unités et nombre des classes de certaines extensions diédrales de degré 8 de $\mathbb{Q}$.
Publ. Math. Fac. Sc. Besançon (Théorie des nombres)
Année 1983-84 .

Hédi Amara
Département de Mathématiques
Faculté des Sciences
1060 TUNIS
TUNISIE