A. Hédi
Nagoya Math. J.
Vol. 103 (1986), 127-132

CYCLES CANONIQUES D'IDEAUX REDUITS ET NOMBRE DES CLASSES DE CERTAINS CORPS QUADRATIQUE REELS

AMARA HÉDI

Introduction

Soit $h(m)$ le nombre des classes de $Q(\sqrt{m})$, $m > 0$. Dans [1], [3] et [5] des conditions suffisantes pour que $h(m) > 1$ sont établies, lorsque $m = 4q^2 + 1$, $m = q^2 + 4$ et $m = q^2 \pm 2$. Dans le présent travail on dégage, par l'algorithme de Chatelet, des cycles principaux canoniques d'idéaux réduits pour ces cas. On retrouve alors les résultats de [1], [3] et [5] et on démontre des critères de divisibilité de $h(m)$ dont certains se trouvent dans [4].

§ 1. Principe de l'algorithme de Chatelet [2]

Soit m un entier sans facteur carré et positif. On note: $k = Q(\sqrt{m})$, $\bigcirc_k$ l'anneau des entiers de k qui admet une Z-base $\{1, \theta\}$ avec $\theta = (1 + \sqrt{m})/2$ si $m \equiv 1\ (4)$ et $\theta = \sqrt{m}$ sinon et $F(X) = X^2 - SX + P$ avec $S = \theta + \theta^r$ et $P = \theta\,\theta^r$ où θ^r est le conjugué de θ. Chaque classe d'idéaux de k contient un idéal $\mathfrak{A}$ sans facteur rationnel (S.F.R.) défini par: tout diviseur premier $\mathfrak{P}$ de $\mathfrak{A}$ est soit décomposé avec $\mathfrak{P}^r$ qui ne divise pas $\mathfrak{A}$ soit ramifié avec $\mathfrak{P}^2$ qui ne divise pas. Un idéal $\mathfrak{A}$ S.F.R. est tel que:

$$\mathfrak{A} = aZ + (\theta - c)Z = (a, \theta - c)$$

a est la norme de $\mathfrak{A}$, $c \in Z$ (racine de $\mathfrak{A}$), avec $F(c) \equiv 0(a)$. On prendra c vérifiant: $0 < \theta - c < a$. Un idéal S.F.R. est dit réduit si et seulement si il admet deux racines dans l'intervalle $]\theta^r, \theta[$. Si $\mathfrak{A} = (a, \theta - c)$ est réduit et $F(c) = -ab$ on appelle successeur de $\mathfrak{A}$ l'idéal S.F.R. $\mathfrak{B} = (b, \theta - c')$ où c' vérifie: $c' - S + c \equiv 0(b)$ et $0 < \theta - c' < b$. On a alors:

$$\mathfrak{B} = \frac{\theta^r - c}{a}\,\mathfrak{A}$$

Received March 11, 1985.

L'es sentiel de l'algorithme de Chatelet est résumé dans le théorème suivant:

THÉORÈME. 1) *L'ideal S.F.R* $(a, \theta - c)$, *avec* $F(c) = -ab$, *est réduit si et seulement si*

$$(a + b)^2 < S^2 - 4P.$$

2) *Dans l'ensemble fini des idéaux réduits la relation "il existe une chaine de* $\mathfrak{A}$ *vers* $\mathfrak{B}$, $\mathfrak{A} = \mathfrak{A}_0, \mathfrak{A}_1, \cdots, \mathfrak{A}_n = \mathfrak{B}$ *telle que pour tout* $0 \leq i \leq n - 1$, $\mathfrak{A}_{i+1}$ *soit le successeur de* $\mathfrak{A}_i$*" est une relation déquivalence. Ses classes sont cycles d'idéaux réduits.*

3) *Les cycles d'idéaux réduits représentent proprement les classes d'idéaux de k.*

4) *Soit* $\mathfrak{A}_0; \cdots; \mathfrak{A}_{l-1}$ *un cycle quelconque d'idéaux réduits avec* $\mathfrak{A}_i = (a_i, \theta - c_i)$ *alors* $\rho = \prod_{i=0}^{l-1}(c_i - \theta^r)/a_i$ *est l'unité fondamentale de k.*

§ 2. Groupe des classes de certains corps quadratiques

Dans la suite $h(m)$ désigne le nombre des classes de $k = Q(\sqrt{m})$ et ρ_m l'uni té fondamentale de k.

(1) $$m = 4q^2 + 1.$$

On a:

$$\theta = \frac{1 + \sqrt{m}}{2}, \quad F(X) = X^2 - X - q^2 \quad \text{et} \quad [\theta] = q.$$

Des deux valeurs suivantes:

$$F(q) = -q \quad et \quad F(1) = -q^2$$

On peut construire le cycle pincipal, en effet les ideaux $(1, \theta - q)$, $(q, \theta - q)$ et $(q, \theta - 1)$ sont réduits et on a:

$$(\theta^r - q)(1, \theta - q) = (q, \theta - 1)$$
$$\left(\frac{\theta^r - 1}{q}\right)(q, \theta - 1) = (q, \theta - q)$$
$$\left(\frac{\theta^r - q}{q}\right)(q, \theta - q) = (1, \theta - q)$$

c'est donc:

$$(1, \theta - q) \longrightarrow (q, \theta - 1) \longrightarrow (q, \theta - q)$$

et

$$\rho_m = \frac{(q - \theta^r)^2(1 - \theta^r)}{q^2} = 2q + \sqrt{4q^2 + 1}$$

i) Si q n'est pas premier, alors $q = ab$ et de $F(q) = -q = -ab$ on a les deux idéaux $(a, \theta - q)$ et $(b, \theta - q)$, qui sont réduits, du fait que:

$$(a + b)^2 \leq (ab)^2 = q^2 < 4q^2 + 1 = S^2 - 4P$$

ii) Si $q = a^n$, somme dans i) les idéaux:

$$(a, \theta - q), \cdots, (a^{n-1}, \theta - q), (a^n, \theta - q) \text{ sont réduits.}$$

LEMME. *Four tout* $1 \leq i \leq n$ *on a*:

$$(a^i, \theta - q) = (a, \theta - q)^i$$

Démonstration. Posons $\mathfrak{A} = (a^n, \theta - q)$.

Un diviseur premier $\mathfrak{P}$ de $\mathfrak{A}$ et décomposé avec $N(\mathfrak{P}) = p$ et divise a. Plus précisément si $a = p_1^{s_1} \cdots p_r^{s_r}$ alors

$$\mathfrak{A} = \mathfrak{P}_1^{ns_1} \cdots \mathfrak{P}_r^{ns_r} \quad \text{où} \quad N(\mathfrak{P}_i) = p_i$$

et donc $\mathfrak{A} = \mathfrak{B}^n$. Comme:

$$\theta - q \in \mathfrak{B}^n \subset \mathfrak{B}^{n-1} \subset \cdots \subset \mathfrak{B}$$

on a $\theta - q \in \mathfrak{B}^i$ pour tout: $1 \leq i \leq n$ et $\mathfrak{B}^i = (a^i, \theta - q)$ pour tout $1 \leq i \leq n$. Comme aucun des idéaux $(a^i, \theta - q)\, 1 \leq i \leq n - 1$ n'est dans le cycle principal, la classe de $(a, \theta - q)$ est d'ordre n.

THÉORÈME 1. *Soit* $m = 4q^2 + 1$.

1) *Si* $m = 4q^2 + 1$, q *non premier, alors* $h(m) > 1$ [1].
2) *Si* $m = 4a^{2n} + 1$, *alors* n *divise* $h(m)$ [4].

(2) $$m = q^2 + 1,\ q \text{ impair}$$

On a

$$\theta = \sqrt{q^2 + 1}, \qquad F(X) = X^2 - q^2 - 1$$

et $[\theta] = q$. Comme $F(q) = -1$ le cycle principal ne contient que $(1, \theta - q)$ et:

$$\rho_m = q - \theta^r = q + \sqrt{q^2 + 1}$$

Si $q = a^n$ on a:

$$F(q-1) = -2q = -2a^n$$

Les ideaux $(2, \theta - q + 1)$, $(a, \theta - q + 1)$, $\cdots$, $(a^n, \theta - q + 1)$ sont réduits et non principaux. Comme dans 1) on a:

$$(a^i, \theta - q + 1) = (a, \theta - q + 1)^i \qquad \text{pour tout } 1 \leq i \leq n$$

Puisque $(2, \theta - q + 1)$ est premier ramifié, sa classe est d'ordre 2 et $(2, \theta - q + 1)^r = (2, \theta - q + 1)$ si bien que:

$$c\ell[(a, \theta - q + 1)^n] = c\ell(a^n, \theta - q + 1) = c\ell(2, \theta - q + 1)$$

et donc $(a, \theta - q + 1)$ est d'ordre 2n.

THÉORÈME 2.

Si $m = a^{2n} + 1$ et a impair, alors $2n$ divise $h(m)$.

(3) $\qquad m = q^2 + 4, \quad q$ impair :

On a:

$$\theta = \frac{1 + \sqrt{q^2 + 4}}{2}, \qquad F(X) = X^2 - X - k^2 - k - 1$$

où

$$q = 2k + 1 \quad \text{et} \quad [\theta] = k + 1$$

Comme $F(k+1) = -1$ le cycle principal est réduit à $(1, \theta - k - 1)$ et

$$\rho_m = k + 1 - \theta^r = \frac{q + \sqrt{q^2 + 4}}{2}.$$

D'autre part:

$$F(k) = -(2k + 1) = -q$$

et comme $q^2 < S^2 - 4P = q^2 + 4$ on obtient un théorème du même type que dans 1)

THÉORÈME 3. *Soit $m = q^2 + 4$ et q impair.*

1) *Si q est non premier, alors $h(m) > 1$.* [3]
2) *Si $q = a^n$, alors n divise $h(m)$.* [4]

(4) $\qquad m = q^2 + 2, \qquad q$ impair :

On a:

$$\theta = \sqrt{q^2 + 2}, \quad F(X) = X^2 - q^2 - 2 \quad \text{et} \quad [\theta] = q .$$

Comme $F(q) = -2$ le cycle principal est le suivant:

$$(1, \theta - q) \longrightarrow (2, \theta - q)$$

et

$$\rho_m = \frac{(q - \theta^r)^2}{2} = q^2 + 1 + q\sqrt{q^2 + 2}$$

THÉORÈME 4 [5]. *Soit* $m = q^2 + 2$, q impair. Si q est divisible par un nombre premier p, avec $p \equiv \pm 1$ (8), alors $h(m) > 1$.

Démonstration. Comme 2 est un carré mod p, soit $a \in \{1, \cdots, p - 1\}$ tel que:

$$a^2 = 2 + \lambda p \quad \text{et} \quad 0 < \lambda < p$$

On pose $c = a + (b - 1)p$ où $q = bp$, or

$$\begin{aligned} F(c) &= -p[2bp - \lambda + 2ab - 2a) - p] \\ &= -pd \end{aligned}$$

Comme $p + d \leq 2bp$ on a:

$$(p + d)^2 \leq 4b^2p^2 < S^2 - 4P = 4b^2p^2 + 8$$

les idéaux $(p, \theta - c)$, $(d, \theta - c)$ sont donc réduits et non principaux.

(5) $$m = q^2 - 2, \qquad q \text{ impair}.$$

On a:

$$\theta = \sqrt{q^2 - 2}, \quad F(X) = X^2 - q^2 + 2 \quad \text{et} \quad [\theta] = q - 1$$

Des deux valeurs:

$$F(q - 1) = -(2q - 3) \quad \text{et} \quad F(q - 2) = -2(2q - 3)$$

On construit le cycle principal:

$$\begin{aligned} &(1, \theta - q + 1) \longrightarrow (2q - 3, \theta - q + 2) \longrightarrow (2, \theta - q + 2) \\ &\longrightarrow (2q - 3, \theta - q + 1) \end{aligned}$$

et on a:

$$\rho_m = \frac{(\theta + q - 1)^2(\theta + q - 2)^2}{2(2q - 3)^2} = q^2 - 1 + q\sqrt{q^2 - 2} .$$

Si $q = (p^n + 3)/2$ *et* p impair on a:

$$F(q - 1) = -p^n$$

Les idéaux $(p, \theta - q + 1), \cdots, (p^n, \theta - q + 1)$ sont réduits et $(p, \theta - q + 1)$ est d'ordre n.

THÉORÈME 5. *Si* $m = (p^{2n} + 6p^n + 1)/4$ $(q = (p^n + 3)/2)$ *avec* p *impair, alors* n *divise* $h(m)$.

BIBLIOGRAPHIE

[1] N. C. Ankeney, S. Chowla and H. Hasse, On the class number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **217** (1965), 217–220.
[2] A. Chatelet, Les corps quadratiques. Monographie de l'enseignement Mathématiques. Genève (1962).
[3] S. D. Lang, Note on the class number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **290** (1977), 70–72.
[4] T. Nakahara, On real quadratic fields whose ideal class groups have a cyclic p-subgroup, Rep. Fac. Sci. Engin., Saga Univ., **6** (1978), 15–26.
[5] H. Yokoi, On the diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field, Nagoya Math. J., **91** (1983), 151–161.

Departement de Mathématiques
Faculte des Sciences
1060, Tunis
Republique Tunisienne