

GILLES ROBERT

Une curieuse symétrie des unités elliptiques

Séminaire de théorie des nombres de Grenoble, tome 7 (1978-1979), exp. n° 4, p. 1-20

http://www.numdam.org/item?id=STNG_1978-1979__7__A4_0

© Institut Fourier – Université de Grenoble, 1978-1979, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

UNE CURIEUSE SYMETRIE DES UNITES ELLIPTIQUES

par Gilles ROBERT

Les résultats présentés dans ce texte ont été exposés au séminaire de théorie des nombres de Grenoble, le 8 mars 1979.

INTRODUCTION

Notre remarque essentielle est l'existence d'une symétrie, liée au Spiegelung de Leopoldt, qui paraît conserver un certain module de p -torsion T construit à l'aide d'unités elliptiques.

Les paragraphes 6 et 7 du présent travail s'appuient sur deux textes en cours de rédaction :

- a) L'un [12] donnant une description complète de T en termes de congruences entre valeurs de séries d'Eisenstein ; une description incomplète est implicite dans [11] §§ 3 et 6 .
- b) L'autre [13] établissant, dans un \mathbb{Z}_p -réseau de formes modulaires convenable, certaines congruences modulo p entre séries d'Eisenstein.

Plus précisément, l'exactitude des exemples numériques que nous proposons dans le paragraphe 7 repose sur a) ; celle du théorème énoncé paragraphe 6 repose sur b) .

IV.2

§1 - NOTATIONS

Soient \mathbb{Q} le corps des nombres rationnels, \mathbb{F}_q le corps fini à q éléments, et μ_m le groupe des racines m -ièmes de l'unité. Pour chaque corps de nombres N ,

$$(N : \mathbb{Q}) < +\infty ,$$

on note $R(N)$ l'anneau des entiers, $Z(N)$ le groupe des unités, $e(N)$ le groupe des racines de l'unité, et $Cl(N)$ le groupe des classes d'idéaux de N ; on pose

$$e_N = |e(N)| \quad , \quad h_N = |Cl(N)| .$$

Soient K un corps quadratique imaginaire, H_0 le corps de classes de Hilbert de K , et notons

$$R = R(K) \quad , \quad e = e_K \quad , \quad h = h_K .$$

Fixons un nombre premier $p \geq 3$, inerte dans K , de sorte que $R/p \simeq \mathbb{F}_q$ avec $q = p^2$, et désignons par H le corps de classes de rayon de K de conducteur (p) . Si $Cl(p)$ désigne le groupe de classes de rayon modulo (p) de K , on a le diagramme commutatif ci-contre

$$\begin{array}{ccccccc} 0 & \longrightarrow & (R/p)^{\times}/e(K) & \longrightarrow & Cl(p) & \longrightarrow & Cl(K) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & G_0 & \longrightarrow & G & \longrightarrow & Gal(H_0/K) \longrightarrow 0 \end{array}$$

où les lignes sont exactes, où G (resp. G_0) désigne le groupe de Galois de l'extension H/K (resp. H/H_0), et où les flèches verticales sont les isomorphismes induits par l'application de réciprocité d'Artin de K . En particulier, on a

$$|G_0| = (H:H_0) = (p^2-1)/e \quad , \quad |G| = (H:K) = h \cdot |G_0| .$$

Pour mémoire, rappelons la décomposition de p dans l'extension H/K : l'idéal premier (p) de K se décompose totalement dans H_0/K , et chacun des idéaux premiers q de H_0 au-dessus de p se ramifie totalement dans H/H_0 .

§2 - UNITES ELLIPTIQUES

Soit $u : H \rightarrow \mathbb{C}$ un plongement de H dans le corps \mathbb{C} des nombres complexes et notons θ l'élément de H défini par

$$u(\theta) = \varphi_{(p)}(C_0) ,$$

où C_0 désigne la classe unité de $Cl(p)$, et où $\varphi_{(p)}(C_0)$ est le nombre réel défini comme dans [10] § 2.2, cf. aussi [1] et [4].

Considérons alors l'idéal

$$J \stackrel{\text{dfn}}{=} \{a \in \mathbb{Z}[G] \mid e(H)^a = \{1\}\}$$

de l'algèbre de groupe $\mathbb{Z}[G]$; le quotient $\mathbb{Z}[G]/J$ est donc cyclique d'ordre e_H . Soit D le groupe des éléments de H dont la puissance $(12p)$ -ième appartient à θ^J ; d'après [2], on a

$$D^{12p} = \theta^J ;$$

notons alors C le groupe des unités elliptiques de H défini par

$$C \stackrel{\text{dfn}}{=} D \cap Z(H) .$$

Si $I(G)$ désigne l'idéal d'augmentation de $\mathbb{Z}[G]$, posons

$$J_0 \stackrel{\text{dfn}}{=} \{\text{éléments de } J \text{ de degré } 0\} = J \cap I(G) ,$$

de sorte que le quotient $I(G)/J_0$ est cyclique d'ordre e_H/e ; le groupe C est caractérisé par les deux propriétés suivantes :

$$\text{i) } C^{12p} = \theta^{J_0} , \quad \text{ii) } e(H) \subset C .$$

Celles-ci prouvent que C ne dépend pas du choix du plongement $u : H \rightarrow \mathbb{C}$, et montrent que C est un $\mathbb{Z}[G]$ -module "essentiellement" monogène.

Pour N sous-corps de H contenant K , on définit le groupe $C(N)$ des unités elliptiques de N par

$$C(N) \stackrel{\text{dfn}}{=} C \cap Z(N) = e(N) \cdot N_{H/N} C ,$$

où $N_{H/N}$ désigne la norme relative à l'extension H/N . Soit $N_0 = H_0 \cap N$; comme p est totalement décomposé dans N_0/K , on a

$$C(N) \cap N_0 = e(N_0) ,$$

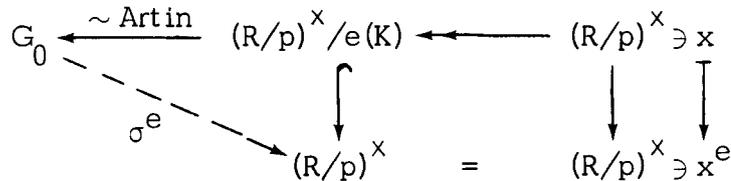
et une formule analytique pour le nombre de classes s'énonce ainsi :

$$(1) [Z(N) : Z(N_0).C(N)] = h_N/h_{N_0} ,$$

cf. [10] §6.4 et [2] .

§3 - CARACTERES DU GROUPE DE GALOIS RELATIF

Notons σ^{e^1} le caractère fondamental de G_0 , qui rend commutatif le diagramme



ci-contre. Les caractères du groupe abélien G_0 à valeurs dans le corps R/p , assez gros , sont alors les homomorphismes

$$\sigma^k \stackrel{\text{dfn}}{=} (\sigma^e)^{k/e} ,$$

où k désigne un entier divisible par e . Précisément, si χ est un caractère de G_0 à valeurs dans R/p , la condition

$$\chi = \sigma^k , \quad 0 \leq k/e \leq |G_0|-1 ,$$

détermine un unique entier k divisible par e ; un tel entier k est dit associé à G_0 .

Pour chaque $(R/p)[G]$ -module M et chaque entier k associé à G_0 , notons M_k la σ^k -composante de M sur laquelle G_0 agit par σ^k . Comme l'algèbre de groupe $(R/p)[G_0]$ est semi-simple, on a donc un isomorphisme de $(R/p)[G]$ -modules

$$M \simeq \bigoplus_{k \text{ associés à } G_0} M_k ;$$

notamment, M_0 est le plus grand sous-module de M dont les éléments sont fixés par G_0 .

Remarque. - Soit $\nu : G \rightarrow \mathbb{F}_p$ le caractère de G défini par son action sur $\mu_p \subset H$. Alors, on a

$$\nu|_{G_0} = \sigma^{p+1}.$$

Le lemme suivant complète la description de C .

LEMME 1. - Soit k un entier associé à G_0 , $k \neq 0$ et $\neq p+1$. Alors, la σ^k -composante $C \otimes (R/p)_k$ de $C \otimes (R/p)$ est un $(R/p)[G]_k$ -module libre de rang 1.

Démonstration. - Choisissons un plongement $u : H \rightarrow \mathbb{C}$, et définissons θ comme dans le §1.2. Alors, la commutativité du diagramme

$$\begin{array}{ccc} C \otimes (R/p)_k & \xrightarrow{\psi_u} & (R/p)[G]_k \\ \downarrow \text{? } k \neq p+1 & & \downarrow \text{? } k \neq p+1 \\ e^{J_0} \otimes (R/p)_k & \xrightarrow[\sim]{k \neq 0} & J \otimes (R/p)_k \end{array}$$

ci-contre, définit un isomorphisme de $(R/p)[G]$ -modules

$$\psi_u : C \otimes (R/p)_k \xrightarrow{\sim} (R/p)[G]_k.$$

§4 - L'INVOLUTION MIROIR

Pour k entier associé à G_0 , définissons le miroir $m(k)$ de k comme l'entier associé à G_0 tel que

$$\sigma^{m(k)} = (\nu|_{G_0}) \cdot \sigma^{-pk};$$

autrement dit, l'entier $m(k)$ est caractérisé par les relations :

- i) $m(k) \equiv p+1-pk \pmod{p^2-1}$,
- ii) $0 \leq m(k)/e \leq |G_0|-1$.

On a $m(m(k)) = k$, de sorte que l'application $k \rightarrow m(k)$ définit sur l'ensemble des entiers associés à G_0 une involution sans points fixes; en effet, le quotient

IV.6

$$t(k) \stackrel{\text{dfn}}{=} (m(k)-k)/(p+1) ,$$

qui vérifie l'identité

$$t(m(k)) + t(k) = 0 ,$$

est un entier impair. En particulier, on a

$$\sigma^{m(k)} = (\nu|_{G_0})^{t(k)} \cdot \sigma^k ,$$

d'où le lemme suivant.

LEMME 2. - Pour chaque entier k associé à G_0 , l'application

$$\sum n_g \cdot g \mapsto \sum \nu(g)^{-t(k)} n_g \cdot g$$

définit un (R/p) -isomorphisme, noté j_k , de $(R/p)[G]_k$ sur $(R/p)[G]_{m(k)}$; précisément, pour tous $a \in (R/p)[G]_k$ et $g \in G$, on a

$$j_k(a) \cdot g = \nu(g)^{t(k)} j_k(a \cdot g) .$$

Les isomorphismes j_k et $j_{m(k)}$ sont inverses l'un de l'autre.

Combinant les lemmes 1 et 2, on obtient ainsi le corollaire suivant .

COROLLAIRE. - Soit k comme dans le lemme 1 . Alors, l'application j_k induit -via ψ_u - un (R/p) -isomorphisme, noté $j_k^{(u)}$, de $C \otimes (R/p)_k$ sur $C \otimes (R/p)_{m(k)}$.

§5 - MODULES GALOISIENS DE p-TORSION

Il s'agit de $(R/p)[G]$ -modules liés à l'existence de classes d'idéaux d'ordre p dans le corps H .

Le premier est le module

$$Cl(H)^{(p)} \stackrel{\text{dfn}}{=} Cl(H) \otimes (R/p) ,$$

difficilement accessible au calcul.

D'autre part, introduisons le groupe U des unités semi-locales de H , i.e. le groupe des unités de l'anneau

$$R(H) \otimes \mathbb{Z}_p = \prod_{q|p} R(H)_q,$$

où le produit est pris sur tous les idéaux premiers q de H au-dessus de p , et où $R(H)_q$ désigne le complété en q de $R(H)$; pour n entier ≥ 0 , on note $U^{(n)}$ le sous-groupe de U formé des unités $u = (u_q)_{q|p}$ telles que

$$u_q \equiv 1 \pmod{q^n \cdot R(H)_q}$$

pour toute place q de H au-dessus de p . Plongeons $Z(H)$ dans U par l'application diagonale; le groupe Z_{pr} des unités p -primaires de H est l'intersection

$$Z_{pr} = Z(H) \cap (U^p \cdot U^{(n)}),$$

avec $n = p(p+1)/e$, cf. e.g. [6]. Nous définissons alors notre second $(R/p)[G]$ -module par

$$T \stackrel{\text{dfn}}{=} (C \cap Z_{pr} / C^p) \otimes R.$$

On possède une description complète de T , en termes de congruences entre valeurs de séries d'Eisenstein, cf. [12].

On note aussi T_{ell} le sous-module de T , défini par

$$T_{ell} \stackrel{\text{dfn}}{=} (C \cap Z(H)^p / C^p) \otimes R.$$

Pour chaque sous-corps N de H contenant K , de degré relatif $(H:N)$ premier à p , soit

$$\varepsilon_N = (H:N)^{-1} \cdot \sum_{g \in \text{Gal}(H/N)} g$$

l'idempotent de l'algèbre $(R/p)[G]$ associé à N , et posons

$$Cl(N)^{(p)} \stackrel{\text{dfn}}{=} \varepsilon_N \cdot Cl(H)^{(p)}, \quad T(N) \stackrel{\text{dfn}}{=} \varepsilon_N \cdot T, \quad T(N)_{ell} \stackrel{\text{dfn}}{=} \varepsilon_N \cdot T_{ell}.$$

On a les identités

$$Cl(N)^{(p)} = Cl(N) \otimes (R/p), \quad T(N) = (C(N) \cap Z_{pr} / C(N)^p) \otimes R, \\ T(N)_{ell} = (C(N) \cap Z(H)^p / C(N)^p) \otimes R.$$

Le lemme et la proposition ci-dessous expriment une partie des relations existant entre les modules $T(N)_{\text{ell}}$, $T(N)$ et $Cl(N)^{(p)}$.

LEMME 3. - Soient M et N deux sous-corps de H contenant K , tels que

$M \subset N$ et $(H:M) \not\equiv 0 \pmod{p}$.

Alors, les trois propriétés suivantes sont équivalentes :

$$i) \quad Cl(N)^{(p)} \setminus Cl(N)_0^{(p)} = Cl(M)^{(p)} \setminus Cl(M)_0^{(p)} .$$

ii) Le quotient $(h_N/h_{N_0}) \cdot (h_M/h_{M_0})^{-1}$, où l'on a posé $N_0 = H_0 \cap N$ et $M_0 = H_0 \cap M$, est une unité p-adique.

$$iii) \quad T(N)_{\text{ell}} = T(M)_{\text{ell}} .$$

Démonstration. - L'équivalence $i) \Leftrightarrow ii)$ résulte du fait que l'algèbre de groupe $\mathbb{F}_p[\text{Gal}(H/M_0)]$ est semi-simple.

Pour prouver l'équivalence $ii) \Leftrightarrow iii)$ observons d'abord que la formule (1) du §1.1 prouve l'identité

$$[Z(N) : C(N) \cdot Z(N_0) \cdot Z(M)] = a \cdot (h_N/h_{N_0}) \cdot (h_M/h_{M_0})^{-1} ,$$

où a est un entier, premier à p dès que $(N:M) \not\equiv 0 \pmod{p}$.

Considérons alors les modules de p -torsion

$$A = (C(N) \cdot Z(N_0) \cdot Z(M)) \cap Z(H)^p / C(N)^p \cdot Z(N_0)^p \cdot Z(M)^p ,$$

$$B = C(N) \cap Z(H)^p / (C(M) \cap Z(H)^p) \cdot C(N)^p ,$$

de sorte que $ii)$ (resp. $iii)$) équivaut à $A = \{0\}$ (resp. $B = \{0\}$) ; il nous suffit donc de vérifier que la flèche naturelle

$$f : B \rightarrow A$$

est un isomorphisme. Mais, comme le degré $(H:M)$ et l'ordre du groupe fini $C(N_0) = e(N_0)$ sont premiers à p , on a les identités

$$\begin{aligned} C(N) \cap (C(N)^p \cdot Z(N_0)^p \cdot Z(M)^p) &= (C(N) \cap (Z(N_0)^p \cdot Z(M)^p)) \cdot C(N)^p \\ &= (C(N) \cap Z(M)^p) \cdot C(N)^p = (C(M) \cap Z(H)^p) \cdot C(N)^p , \end{aligned}$$

$$\begin{aligned} (C(N) \cdot Z(N_0) \cdot Z(M)) \cap Z(H)^p &= ((C(N) \cdot Z(M)) \cap Z(H)^p) \cdot Z(N_0)^p \\ &= (C(N) \cap Z(H)^p) \cdot Z(N_0)^p \cdot Z(M)^p, \end{aligned}$$

qui prouvent respectivement la trivialité du noyau et du conoyau de f et complètent la démonstration du lemme.

PROPOSITION. - Soient M et N comme dans le lemme 3 . Alors, les modules $T(N)$ et $Cl(N)^{(p)}$ sont liés par les relations suivantes :

- i) si $T(N) = T(M)$, on a $T(N)_{\text{ell}} = T(M)_{\text{ell}}$ et donc
 $Cl(N)^{(p)} \setminus Cl(N)_0^{(p)} = Cl(M)^{(p)} \setminus Cl(M)_0^{(p)} ;$
- ii) si $\mu_p \subset N$ et $Cl(N)^{(p)} = Cl(N)_0^{(p)}$ (resp. = $\{0\}$) , on a
 $T(N) = T(N)_{p+1}$ (resp. = $\{0\}$) .

Démonstration. - On a $T(N) = T(M)$ si et seulement si les deux inclusions naturelles

$$\begin{aligned} Z(M) \cap Z_{\text{pr}} / Z(M) \cap Z(H)^p &\hookrightarrow Z(N) \cap Z_{\text{pr}} / Z(N) \cap Z(H)^p, \\ Z(M) \cap Z(H)^p / Z(M)^p &\hookrightarrow Z(N) \cap Z(H)^p / Z(N)^p, \end{aligned}$$

sont des isomorphismes, d'où l'implication

$$T(N) = T(M) \implies T(N)_{\text{ell}} = T(M)_{\text{ell}} ;$$

celle-ci, jointe au lemme 3, prouve l'assertion i) de la proposition. Quant à l'assertion ii) elle est démontrée dans [11] § 6 .

§ 6 - QUESTIONS ET PROBLEME ; UNE REPOSE PARTIELLE

Les exemples que nous avons pu traiter, cf. §7 infra, suggèrent l'existence de liens plus étroits entre $Cl(N)^{(p)}$ et $T(N)_{\text{ell}}$ ainsi que l'existence d'une sorte de dualité entre les modules T_k et $T_{m(k)}$. Précisément, on est conduit à avancer les hypothèses de travail suivantes :

Question 1. - Soient N un sous-corps de H contenant K tel que $(H:N) \not\equiv 0 \pmod{p}$, et k un entier associé à G_0 , $k \neq 0$.
A-t-on l'équivalence

$$Cl(N)_k^{(p)} = \{0\} \iff (T(N)_{\text{ell}'_k}) = \{0\} ?$$

Question 2. - Est-il vrai que pour tout couple d'entiers k et \bar{k} associés à G_0 , $k \neq 0$ et $\neq p+1$, tels que $\bar{k} = m(k)$, on a la décomposition en somme directe

$$T_k = (T_{\text{ell}'_k}) \oplus \text{Im}(j_{\bar{k}}^{(u)} | (T_{\text{ell}'_k})^-)$$

du $(R/p)[G]$ -module T_k ?

Nous ne savons répondre ni à l'une ni à l'autre de ces deux questions ; cependant, la question 2 ci-dessus conduit à poser le problème suivant :

Problème. - Déterminer l'ensemble $A(K,p)$ des entiers k associés à G_0 , $k \neq 0$ et $\neq p+1$, tels que l'application $j_k^{(u)}$ induit un (R/p) -isomorphisme de T_k sur $T_{m(k)}$.

Remarque. - Si $k \in A(K,p)$, on a $|T_k| = |T_{m(k)}|$.

Le fait étonnant est que la description de T_k en termes de (valeurs de) séries d'Eisenstein nous permet de prouver que $A(K,p)$ est "presque" aussi grand que possible : on a l'inégalité

$$|A(K,p)| \geq |G_0| \cdot (p-3)/(p-1).$$

En effet, soit $I(e,p)$ l'ensemble des entiers k associés à G_0 , $k \neq 0$ et $\neq p+1$, tels que chacun des $(p+1-e)/e$ caractères

$$\sigma^i, \quad 0 < i < p+1, \quad e|i,$$

soit distinct de σ^k et de σ^{pk} ; on a donc

$$|I(e,p)| = |G_0| - 2(p+1)/e = (p-3)(p+1)/e,$$

et le théorème ci-dessous fournit une réponse partielle au problème précédent.

THEOREME. - Pour tout corps quadratique imaginaire K , tel que
 $|e(K)| = e$, et tout nombre premier $p \geq 5$ inerte dans K , on a
l'inclusion

$$I(e, p) \subset A(K, p) .$$

Dans [12] , nous réduisons l'assertion de ce théorème aux congruences correspondantes entre séries d'Eisenstein ; pour la démonstration de celles-ci, se rapporter à [13] .

§7 - EXEMPLES NUMERIQUES

Dans ce paragraphe , pour chacun des 12 couples (K, p) formés d'un corps quadratique imaginaire K de nombre de classes d'idéaux h égal à 1 ou 2 , et d'un nombre premier $p = 3 , 5$ ou 7 inerte dans K tel que

$$Cl(H)^{(p)} \neq \{0\} ,$$

nous explicitons aussi précisément qu'il nous a été possible les $(R/p)[G]$ -modules

$$T \text{ et } Cl(H)^{(p)} .$$

Suivant les valeurs de h et p , ces couples se répartissent

$h \backslash p$	3	5	7
1	0	1	0
2	3	4	4

en nombre comme indiqué par le tableau ci-contre ; si $-D < 0$ désigne le discriminant de K , la liste en est la suivante :

D	115	123	148	163	232	235	267	403
p	3	5;7	5;7	5	3;5	7	5;7	3

Pour la détermination de T nous utilisons les résultats de [12], ainsi que les tables de [11] appendices B et E. Désignons par M le plus petit sous-corps de H contenant $K(\mu_p)$ tel que le groupe de Galois de l'extension H/M fixe T point par point ; d'après la prop. §5, on a donc

$$\text{Cl}(H)^{(p)} = \text{Cl}(M)^{(p)} ,$$

autrement dit le quotient h_H/h_M est premier à p . Dans chacun des 12 cas étudiés, on vérifie l'inclusion

$$M \subset H_0(\mu_p) .$$

Mais, comme $H_0(\mu_p)$ est une extension abélienne de \mathbb{Q} , ceci permet d'utiliser les résultats de H. Hasse [5]. Pour cela, on décompose le caractère de la représentation régulière de $\text{Gal}(M/\mathbb{Q})$ en somme de caractères irréductibles sur \mathbb{Q} , et on calcule la "contribution" de chacun des caractères irréductibles impairs à la p -partie de la composante imaginaire

$$h_M^- = h_M / h_M^+$$

du nombre de classes d'idéaux h_M de M ; ici h_M^+ désigne le nombre de classes d'idéaux du sous-corps réel maximal M^+ de M . Pour chaque caractère irréductible impair de M/\mathbb{Q} , on constate que cette contribution est 1 ou p .

Pour en déduire, à l'aide de la connaissance précise de T , la structure galoisienne du p -groupe de Sylow de $\text{Cl}(M)$ il nous suffit alors de vérifier que le nombre de classes réelles h_M^+ de M est premier à p . C'est l'obstacle le plus sérieux ; en utilisant les résultats fournis par l'inégalité du miroir de H.W. Leopoldt, cf. [7] et [3], on se ramène à la détermination de la p -partie du nombre de classes d'idéaux de certains sous-corps N^+ de M^+ , dont le groupe de Galois est isomorphe à $\mathbb{Z}/2$, $\mathbb{Z}/4$ ou $\mathbb{Z}/6$.

■ Lorsque $\text{Gal}(N^+/\mathbb{Q})$ est isomorphe à $\mathbb{Z}/2$ ou $\mathbb{Z}/4$ nous avons fait appel aux tables suivantes :

- i) table de nombre de classes d'idéaux des corps quadratiques réels ;
- ii) table de nombre de classes d'idéaux des corps cycliques réels de degré 4, établie par M.N. Gras [14] .

■ Lorsque $\text{Gal}(N^+/\mathbb{Q})$ est isomorphe à $\mathbb{Z}/6$ il n'existe pas, à notre connaissance, de table convenable ; aussi, quand nous l'avons pu, nous avons utilisé la majoration de h_N^+ qui résulte des minoration de discriminants (des corps totalement réels) établies par A.M. Odlyzko, cf. [15] et [8], [9] .

■ Lorsque $p = 7$ et $K = \mathbb{Q}(\sqrt{-235})$, nous avons eu besoin d'un calcul direct ; le corps incriminé est

$$N^+ = \mathbb{Q}(\sqrt{7.235}, \cos(2\pi/7)) .$$

Soient $u = (26647 + 657\sqrt{1645})/2$ l'unité fondamentale de $\mathbb{Q}(\sqrt{7.235})$, et $v_i = (\sin(2\pi/7))^i (\sin(3\pi/7))^{3-i} / (\sin(\pi/7))^3$, $i = 1, 2$, une unité de $\mathbb{Q}(\cos(2\pi/7))$ dont la classe engendre la $\sqrt{2^i}$ -composante de $Z(\mathbb{Q}(\cos(2\pi/7))) \otimes (\mathbb{R}/7)$. Comme les corps $\mathbb{Q}(\sqrt{7.235})$ et $\mathbb{Q}(\cos(2\pi/7))$ ne possèdent pas de classes d'idéaux d'ordre 7, on déduit de la formule analytique pour le nombre de classes de N^+ de Leopoldt, cf. e.g. [3], le fait que le corps N^+ possède des classes d'idéaux d'ordre 7 si et seulement si $u.v_1$ ou $u.v_2$ est une puissance 7-ième dans $Z(N^+)$; s'il en était ainsi, l'une des traces

$$t_i \stackrel{\text{dfn}}{=} \sum_{g \in \text{Gal}(N^+/\mathbb{Q})} \sqrt[7]{(u.v_i)^g}, \quad i = 1 \text{ ou } 2 ,$$

serait un entier rationnel. Un calcul facile prouve qu'il n'en est rien : on trouve

$$6,35 < t_1 < 6,37 \quad , \quad 6,95 < t_2 < 6,96 ;$$

ainsi h_N^+ est premier à 7 .

De la sorte, on obtient une description complète du p -groupe de Sylow de $\text{Cl}(H)$; en retour, celle-ci permet de préciser le sous-module T_{ell} de T engendré par les unités elliptiques qui sont des puissances p -ièmes dans H . Dans chacun des 12 cas, on vérifie ainsi, pour

chaque couple d'entiers k et \bar{k} , associés à G_0 , tels que $\bar{k} = m(k)$,
les isomorphismes de $(R/p)[G]$ -modules

$$\text{Cl}(H)_k^{(p)} \simeq (T_{\text{ell}})_k, \quad k \neq 0,$$

$$T_k \simeq (T_{\text{ell}})_k \oplus \text{Im}(j_k^{(u)} | (T_{\text{ell}})_{\bar{k}}^-), \quad k \neq 0 \text{ et } \neq p+1,$$

de sorte que la réponse aux questions 1 et 2 du §6 est OUI. On vérifie aussi l'isomorphisme

$$\text{Cl}(H)_0^{(p)} \simeq \text{Hom}_{R/p}((T/T_{\text{ell}})_{p+1}, \mu_p \otimes R),$$

et on constate que la p -extension abélienne non ramifiée maximale L de H est engendrée sur H par les racines p -ièmes des unités p -primaires de H ; en particulier, le groupe de Galois de l'extension L/H est tué par p , et le sous-corps réel maximal $H_0(\mu_p)^+$ de $H_0(\mu_p)$ ne possède pas de classes d'idéaux d'ordre p .

Remarque. - Il serait sûrement instructif de tester les questions 1 et 2 sur un couple (K,p) pour lequel on ait

$$T \neq T(H_0(\mu_p));$$

en effet, nous ne connaissons aucun exemple de cette situation !!!

Rappel. - Les couples (K,p) avec K principal et $p = 11$ ou 13 inerte dans K , sont étudiés dans [11] appendice B; pour le couple $(K,p) = (\mathbb{Q}(\sqrt{-19}), 13)$, la réponse aux questions 1 et 2 est OUI.

DEFINITION. - On note R_p le complété $R \otimes \mathbb{Z}_p$ de l'anneau des entiers R de K .

$$\boxed{p = 3}$$

(a₁) $K = \mathbb{Q}(\sqrt{-115})$, $H_0 = \mathbb{Q}(\sqrt{-23}, \sqrt{5})$. Posons $N = K(\sqrt{69})$. On trouve

$$T = T_4 = T(N)_4 \simeq R/3,$$

$$\text{Cl}(H)^{(3)} = \text{Cl}(H)_0^{(3)} \simeq R/3 ,$$

$$T_{\text{ell}} = \{0\} .$$

Le $(R/3)$ -espace vectoriel T est engendré par la classe de l'unité fondamentale 3-primaire

$$u_{69} = -1 + 3(9 + \sqrt{69})/2$$

du corps $\mathbb{Q}(\sqrt{69})$. Le corps $H(\sqrt[3]{u_{69}})$ est la 3-extension abélienne non ramifiée maximale de H .

(a₂) $K = \mathbb{Q}(\sqrt{-403})$, $H_0 = \mathbb{Q}(\sqrt{-31}, \sqrt{13})$. Situation identique à la précédente, il suffit de remplacer partout 69 par 93; l'unité fondamentale 3-primaire du corps $\mathbb{Q}(\sqrt{93})$ est

$$u_{93} = 1 + 3(9 + \sqrt{93})/2 .$$

(b) $K = \mathbb{Q}(\sqrt{-58})$, $H_0 = \mathbb{Q}(\sqrt{29}, \sqrt{-2})$. Posons $N = K(\sqrt{-87})$. On trouve

$$T = T_4 = T(N)_4 \simeq R/3 ,$$

$$\text{Cl}(H)^{(3)} = \text{Cl}(N)_4^{(3)} \simeq \text{Cl}(\mathbb{Q}(\sqrt{-87})) \otimes R_3 = R/3 ,$$

$$T_{\text{ell}} = T .$$

Soit $u_{29} = 1 + (3 + \sqrt{29})/2$ l'unité fondamentale 3-primaire de $\mathbb{Q}(\sqrt{29})$; la 3-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[3]{u_{29}})$.

p = 5

(a₁) $K = \mathbb{Q}(\sqrt{-163}) = H_0$, cf. [10] appendice. Posons $N_1 = K(\sqrt{5})$ et $N_2 = K(\mu_5)$; on a donc $(N_2 : N_1) = 2$. On trouve

$$T = T_{12} \oplus T_{18} ,$$

avec $T_{12} = T(N_1)_{12} \simeq R/5$ et $T_{18} = T(N_2)_{18} \simeq R/5$,

$$\text{Cl}(H)^{(5)} = \text{Cl}(N_1)_{12}^{(5)} \simeq \text{Cl}(\mathbb{Q}(\sqrt{-5 \cdot 163})) \otimes R_5 = R/5 ,$$

$$T_{\text{ell}} = T_{12} .$$

Le $(R/5)$ -espace vectoriel T_{18} est engendré par la classe de l'unité 5-primaire

$$v = w^2 \cdot w^s$$

de N_2 ; ici w désigne une solution de l'équation quadratique

$$w + w^{-1} = 7 \cdot ((1 + \sqrt{5})/2)^8 \cdot \sqrt{163(5 + \sqrt{5})/2}$$

de discriminant

$$\Delta = (163 \cdot 7^2 + 3571\sqrt{5})/2 = ((1 + \sqrt{5})/2)^8 \cdot (217 + 55\sqrt{5})/2 ,$$

et $s = (a_{163}, H/K)$ l'automorphisme d'Artin de H/K associé à l'idéal a_{163} de K de norme 163 . Le corps $H(\sqrt[5]{v})$ est la 5-extension abélienne non ramifiée maximale de H .

$$\textcircled{a_2} \quad K = \mathbb{Q}(\sqrt{-123}) , \quad H_0 = \mathbb{Q}(\sqrt{41}, \sqrt{-3}) .$$

$\textcircled{a_3}$ $K = \mathbb{Q}(\sqrt{-58})$, $H_0 = \mathbb{Q}(\sqrt{29}, \sqrt{-2})$. Situations identiques à la précédente, il suffit de remplacer $\sqrt{-5 \cdot 163}$ par $\sqrt{-5 \cdot 123}$ (resp. $\sqrt{-5 \cdot 58}$).

En particulier, il existe une unité 5-primaire v de $N_2 = K(\mu_5)$ dont la classe engendre T_{18} . La 5-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[5]{v})$; nous n'avons pas déterminé explicitement v .

\textcircled{b} $K = \mathbb{Q}(\sqrt{-37})$, $H_0 = \mathbb{Q}(\sqrt{37}, \sqrt{-1})$. Posons $N_1 = K(\sqrt[5]{5 \cdot 37})$, et désignons par N_2 le sous-corps de $H_0(\mu_5)$, cyclique de degré 4 sur K , fixé par l'automorphisme d'Artin $(a_{74}, H/K)$ de H/K associé à l'idéal a_{74} de K de norme 74 ; on a donc

$$N_1 \cdot N_2 = H_0(\mu_5) \quad \text{et} \quad N_1 \cap N_2 = K .$$

On trouve

$$T = T_{12} \oplus T_{18} ,$$

avec $T_{12} = T(N_{112}) \simeq R/5$ et $T_{18} = T(N_{218}) \simeq R/5$,

$$\text{Cl}(H)^{(5)} = \text{Cl}(N_{218})^{(5)} \simeq R/5,$$

$$T_{\text{ell}} = T_{18}.$$

Le $(R/5)$ -espace vectoriel T_{12} est engendré par la classe de l'unité fondamentale 5-primaire

$$u_{185} = 68 + 5\sqrt{185}$$

du corps $\mathbb{Q}(\sqrt{5.37})$. Le corps $H(\sqrt[5]{u_{185}})$ est la 5-extension abélienne non ramifiée maximale de H .

(c) $K = \mathbb{Q}(\sqrt{-267})$, $H_0 = \mathbb{Q}(\sqrt{89}, \sqrt{-3})$. Désignons par N le sous-corps de $H_0(\mu_5)$, cyclique de degré 4 sur K , fixé par l'automorphisme d'Artin $(a_{89}, H/K)$ de H/K associé à l'idéal a_{89} de K de norme 89 ; on a donc

$$H_0 \cdot N = H_0(\mu_5) \quad \text{et} \quad H_0 \cap N = K.$$

On trouve

$$T = T_6 = T(N)_6 \simeq R/5,$$

$$\text{Cl}(H)^{(5)} = \text{Cl}(N)_6^{(5)} \simeq R/5,$$

$$T_{\text{ell}} = T.$$

Soit $u_{89} = 500 + 53\sqrt{89}$ l'unité fondamentale 5-primaire de $\mathbb{Q}(\sqrt{89})$; la 5-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[5]{u_{89}})$.

p = 7

(a) $K = \mathbb{Q}(\sqrt{-123})$, $H_0 = \mathbb{Q}(\sqrt{41}, \sqrt{-3})$. Posons $M_1 = K(\sqrt{21})$, $M_2 = K(\cos(2\pi/7))$ et $N_1 = H_0 \cdot M_1$, $N_2 = H_0 \cdot M_2$; on a donc

$$(N_1 : M_1) = (N_2 : M_2) = 2, \quad N_1 \cdot N_2 = H_0(\mu_7) \quad \text{et} \quad N_1 \cap N_2 = H_0.$$

On trouve

$$T = T_{24} \oplus T_{32},$$

avec $T_{24} = T(N_1)_{24} \simeq (R/7)^2$ et $T_{32} = T(N_2)_{32} \simeq (R/7)^2$,

$$\text{Cl}(H)^{(7)} = \text{Cl}(M_1)_{24}^{(7)} \oplus \text{Cl}(M_2)_{32}^{(7)},$$

avec $\text{Cl}(M_1)_{24}^{(7)} \simeq \text{Cl}(\mathbb{Q}(\sqrt{-7.41})) \otimes R_7 = R/7$ et $\text{Cl}(M_2)_{32}^{(7)} \simeq R/7$

$$T_{\text{ell}} = T(M_1)_{24} \oplus T(M_2)_{32},$$

avec $T(M_1)_{24} \simeq R/7 \simeq T(M_2)_{32}$.

Le $(R/7)$ -espace vectoriel $(T(N_1)/T(M_1))_{24}$ (resp. $(T(N_2)/T(M_2))_{32}$) est engendré par la classe de l'unité fondamentale 7-primaire

$$u_{861} = -1 + 7(3.7^2 + 5\sqrt{861})/2$$

du corps $\mathbb{Q}(\sqrt{7.123})$ (resp. d'une unité 7-primaire v de N_2). Le corps $H(\sqrt[7]{u_{861}}, \sqrt[7]{v})$ est la 7-extension abélienne non ramifiée maximale de H .

$$\textcircled{b} \quad K = \mathbb{Q}(\sqrt{-37}), \quad H_0 = \mathbb{Q}(\sqrt{37}, \sqrt{-1}). \quad \text{Posons } N = K(\sqrt{7}, \cos(2\pi/7));$$

on a donc

$$H_0 \cdot N = H_0(\mu_7) \quad \text{et} \quad H_0 \cap N = K.$$

On trouve

$$T = T_8 = T(N)_8 \simeq R/7,$$

$$\text{Cl}(H)^{(7)} = \text{Cl}(N)_8^{(7)} \simeq R/7,$$

$$T_{\text{ell}} = T.$$

Soit $u_{37} = 6 + \sqrt{37}$ l'unité fondamentale 7-primaire de $\mathbb{Q}(\sqrt{37})$; la 7-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[7]{u_{37}})$.

$$\textcircled{c} \quad K = \mathbb{Q}(\sqrt{-267}), \quad H_0 = \mathbb{Q}(\sqrt{89}, \sqrt{-3}). \quad \text{Posons } N_1 = K(\sqrt{-7}),$$

$N_2 = K(\cos(2\pi/7))$ et $N = N_2(\sqrt{21})$; on a donc

$$N_1 \cdot N_2 = K(\mu_7), \quad N_1 \cap N_2 = K \quad \text{et} \quad N_2 = N \cap K(\mu_7).$$

On trouve

$$T = T_8 \oplus T_{24} \oplus T_{32},$$

avec $T_8 = T(N)_8 \simeq R/7$, $T_{24} = T(N_1)_{24} \simeq R/7$ et $T_{32} = T(N_2)_{32} \simeq R/7$,

$$\text{Cl}(H)^{(7)} = \text{Cl}(N)^{(7)} = \text{Cl}(N)_8^{(7)} \oplus \text{Cl}(N_2)_{32}^{(7)} ,$$

avec $\text{Cl}(N)_8^{(7)} \simeq R/7 \simeq \text{Cl}(N_2)_{32}^{(7)} ,$

$$T_{\text{ell}} = T_8 \oplus T_{32} .$$

Le $(R/7)$ -espace vectoriel $T(N_1)_{24}$ est engendré par la classe de l'unité fondamentale 7-primaire

$$u_{1869} = -1 + 5.7(15.7^2 + 17\sqrt{1869})/2$$

du corps $\mathbb{Q}(\sqrt{7.267})$. Soit $u_{89} = 500 + 53\sqrt{89}$ l'unité fondamentale 7-primaire de $\mathbb{Q}(\sqrt{89})$; la 7-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[7]{u_{1869}}, \sqrt[7]{u_{89}})$.

(d) $K = \mathbb{Q}(\sqrt{-235})$, $H_0 = \mathbb{Q}(\sqrt{5}, \sqrt{-47})$. Posons $N_1 = K(\cos(2\pi/7))$ et $N_2 = K(\mu_7)$; on a donc $(N_2 : N_1) = 2$. On trouve

$$T = T_{16} \oplus T_{40} ,$$

avec $T_{16} = T(N_1)_{16} \simeq R/7$ et $T_{40} = T(N_2)_{40} \simeq R/7$,

$$\text{Cl}(H)^{(7)} = \text{Cl}(N_1)_{16}^{(7)} \simeq R/7 ,$$

$$T_{\text{ell}} = T_{16} .$$

Le $(R/7)$ -espace vectoriel T_{40} est engendré par la classe d'une unité 7-primaire v de N_2 ; la 7-extension abélienne non ramifiée maximale de H est le corps $H(\sqrt[7]{v})$.

BIBLIOGRAPHIE

- [1] R. GILLARD, Unités elliptiques et unités cyclotomiques, (1979) à paraître.
- [2] R. GILLARD et G. ROBERT, Groupes d'unités elliptiques, Bull. Soc. Math. France, 107 (1979) à paraître.
- [3] G. GRAS, Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier, 27 (1977) 1-66 .
- [4] B.H. GROSS, On the factorization of p-adic L-series, (1979) à paraître.

- [5] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin (1952).
- [6] H. HASSE, Bericht über neuere Untersuchungen und Probleme der algebraischen Zahlkörper II, 2^{te} Auflage, Physica Verlag, Würzburg-Wien (1965).
- [7] H.W. LEOPOLDT, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. rein. u. and. Math., 199 (1958) 165-174.
- [8] J. MASLEY, Odlyzko bounds and class number problems, dans Algebraic Number fields (A. Fröhlich editor, 1977) 465-473.
- [9] G. POITOU, Minorations de discriminants (d'après A.M. Odlyzko), exp. Bourbaki 470 (février 1976).
- [10] G. ROBERT, Unités elliptiques, Bull. Soc. math. France, mémoire 36 (1973).
- [11] G. ROBERT, Nombres de Hurwitz et unités elliptiques, Ann. Scient. Ec. Norm. Sup., (4) 11 (1978) 297-389.
- [12] G. ROBERT, Un critère logarithmique de p-primarité (titre provisoire), en cours de rédaction.
- [13] G. ROBERT, Congruences entre séries d'Eisenstein dans le cas supersingulier (titre provisoire), en cours de rédaction.

Tables

- [14] M.N. GRAS, Tables numériques du nombre de classes et des unités des extensions cycliques réelles de degré 4 de \mathbb{Q} , Publ. math. Univ. Besançon, (1977-1978, fascicule II).
- [15] A.M. ODLYZKO, Discriminants bounds, lettre, 29 nov. 1976.