À mes parents.

À Nassreddine.

À la mémoire de Abdenbi.

Remerciements

Tout d'abord, je tiens à exprimer ma plus profonde gratitude à mon directeur de thèse Maurice MIGNOTTE pour son soutien indéfictible, pour sa patience, sa disponibilité, ses conseils et ses constants encouragements. Sans son appui, cette thèse n'aurait pu être réalisée.

Je remercie vivement le Professeur Yann BUGEAUD qui m'a fait l'honneur de participer au jury et d'y assumer la fonction de rapporteur interne. Je le remercie aussi pour les conversations enrichissantes que j'ai eu avec lui. Qu'il en trouve ici le témoignage de ma reconnaissance.

Je tiens à remercier également les Professeurs Georges RHIN et Eugène DUBOIS qui m'ont fait l'honneur d'être rapporteurs sur ma thèse. Mes remerciements vont aussi à Henri LOMBARDI qui a bien voulu faire partie du Jury.

Merci à Mohamed ATLAGH de m'avoir soutenu quand il le fallait, et durant une période difficile. Qu'il en trouve ici le témoignage de ma reconnaissance. Je n'oublie pas non plus Abdelkader SAIDI pour son soutien et ses conseils.

Je ne saurais oublier de remercier la famille Lgasbaoui pour la chaleur et l'hospitalité qu'elle m'a prodiguées ces deux dernières années. Qu'elle en trouve ici l'expression de ma profonde gratitude.

Merci à Denis pour les petites "tâches" informatiques et à Hedi pour son sens de l'humour.

Enfin, je dédie cette thèse à mes parents, mes frères, mes soeurs, mes amis et à tous ceux qui m'ont aidé un jour.

Table des matières

Chapitre 0

Introduction

Introduction et description des résultats obtenus

La motivation initiale de ce travail était l'étude arithmétique de certains nombres entiers apparaissant dans des critères sur l'équation de Catalan[1] (voir par exemple [3], [19], et [26]). Certains de ces entiers sont très grands et il est donc impossible de les factoriser. La contribution principale de ce travail consiste à montrer que des considérations de théorie algébrique des nombres permettent d'obtenir une factorisation partielle de ces entiers.

Soit C_p le corps p-ième cyclotomique $\mathbb{Q}(e^{2i\pi/p})$, où p est un nombre premier impair. Kummer a montré que le nombre de classes h du corps C_p peut se factoriser sous la forme $h = h^+ \cdot h^-$ où h^+ est le nombre de classes de $C_p^+ = C_p \cap \mathbb{R}$ et h^- est un entier. L'essentiel de ce travail porte sur l'étude du terme h^- pour les corps cyclotomiques; il prend en partie sa source dans un article de D. H. Lehmer qui établit une factorisation fondamentale de $h^-(p)$ de C_p en entiers $h_e(p)$ spécifiques[2] sous la forme :

$$h^-(p) = \prod_{ef=p-1;\, f \text{impair}} h_e(p);$$

et obtint à l'aide de cette formule des informations arithmétiques.

Ce travail est composé de quatre chapitres :

Le chapitre I est consacré à des définitions et des rappels; d'abord sur les corps des nombres en particulier les corps cyclotomiques et sur le groupe

1. La conjecture de Catalan enfin démontrée par Mihăilescu [23]

2. D'une façon précise $h_e(p) = p^{[e/p-1]} \frac{2}{(2p)^{e/2}} \mathrm{N}_{\mathbb{Q}(\zeta_e)/\mathbb{Q}}(\mathrm{M}_e(p))$; où $\mathrm{M}_e(p) \in \mathbb{Z}[\zeta_e]$ et $p-1 = ef$; avec f impair

de classes d'idéaux; ensuite nous donnons quelques résultats sur les corps de type CM [3].

Le chapitre II regroupe en détail le travail de Lehmer paru dans l'article [11] et qui porte précisément sur le h^- des corps cyclotomiques, ainsi que quelques compléments et exemples originaux. Un programme en GP Pari (voir Annexe I) donne des exemples de calcul de $h_e(p)$.
Soit $h_e(p) = q_1 q_2 ... q_t$ la factorisation canonique de $h_e(p)$ en un produit de puissances de nombres premiers distincts $q_i\,(i = 1,...,t)$. Chaque q_i premier avec e est de la forme $ex + 1$ (théorème 2.3.4, p. 25).

Dans le chapitre III, nous avons utilisé l'expression analytique du nombre de classes relatif pour montrer que $h_e(p)$ décrit ci-dessus correspond au nombre de classes relatif d'un certain sous-corps de C_p. Plus précisément, si on désigne par K_p le sous-corps cyclique imaginaire maximal de C_p, dont le degré sur $\mathbb{Q}$ est une puissance de deux, alors on a le théorème suivant (théorème 3.2.4, p. 49):

Théorème *On a la relation*

$$h_e(p) = h^-(K_p) \quad si \quad e = 2^d,\, d \geq 1.$$

Comme application de ce théorème, le nombre de classes relatif du sous-corps $\mathbb{Q}(\zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9)$ de $\mathbb{Q}(\zeta_{13})$ est égal à 1. Pour d'autres sous-corps (cf. Annexe I), nous avons calculé, et ce en utilisant un programme écrit en GP Pari, le nombre de classes relatif de ces sous-corps.

La majoration du nombre de classes d'un corps de nombres a suscité l'intérêt de plusieurs mathématiciens, et ce depuis Kummer. Nous avons établi une majoration du nombre de classes relatif $h^-(K_p)$ en fonction du nombre premier p et de la valuation 2-adique de $p-1$:

Proposition. *Soit* $t = v_2(p-1)$. *Posons* $c_1 = (2 + \gamma - \log \pi)/(4\pi) = 0.1139\ldots$, γ *étant la constante d'Euler.*

3. Un corps de type CM est une extension quadratique totalement imaginaire d'un corps totalement réel.

a) Si $K_p = \mathbb{Q}(\zeta_p)$ *alors*

$$h^-(K_p) \leq 2p^{2^{t-2}+1}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}.$$

b) Si $K_p \neq \mathbb{Q}(\zeta_p)$ *alors*

$$h^-(K_p) \leq 2p^{2^{t-2}}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}.$$

De plus cette inégalité est stricte dans le cas où $t = 1$.

Nous nous sommes particulièrement intéressés dans ce travail à la factorisation du nombre de classes relatif $h^-(K_p)$ de K_p. Ainsi dans le chapitre IV nous avons cherché—entre autres—à repérer les nombres premiers $q \equiv 1+2^m \pmod{2^{m+1}}$, $(m \geq 1)$ qui divisent $h^-(K_p)$. Voici un bref parcours de ce chapitre:

– **Les facteurs de** $h^-(K_p)$ **de type** $q \equiv 3 \pmod 4$ **(**$m = 1$**).**

En utilisant la transitivité de la norme, on remarque que le nombre de classes relatif $h^-(K_p)$ de K_p est essentiellement une norme dans l'extension $\mathbb{Q}(i)/\mathbb{Q}$, c'est-à-dire :

$$h^-(K_p) \simeq \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(A + iB) = A^2 + B^2,$$

où $A, B \in \mathbb{Z}$. Un programme écrit en GP Pari calcule les composantes A et B. On a le résultat suivant:

Proposition. *On a les équivalences suivantes:*

$$q \mid h^-(K_p) \Leftrightarrow q \mid \mathrm{pgcd}(A, B) \Leftrightarrow q^2 \mid h^-(K_p).$$

Du point de vue de la factorisation de h^-, une telle proposition est très importante: le calcul du pgcd de deux entiers est très peu coûteux et on peut donc facilement trouver les facteurs premiers q de h^- qui vérifient $q \equiv 3 \pmod 4$. Les composantes A et B peuvent être calculées par le programme de Roy (voir Annexe II). Nous avons donné deux tables, la première regroupe des valeurs de $h^-(K_p)$, et leur factorisation en nombres premiers, ainsi que les nombres premiers $q \equiv 3 \pmod 4$ divisant $h^-(K_p)$. Ces calculs sont établis

à l'aide du programme de Roy expliqué à la fin de chapitre IV. La deuxième table regroupe les composantes A et B et leur plus grand commun diviseur.

– **Les facteurs de $h^-(K_p)$ de type $q \equiv 5 \pmod 8$ ($m = 2$)**

Le facteur $h^-(K_p)$ de K_p s'exprime aussi essentiellement comme une norme dans l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, c'est-à-dire :

$$h^-(K_p) \simeq \mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(C + D\sqrt{2}) = C^2 - 2D^2,$$

où $C, D \in \mathbb{Z}$.
On a le résultat suivant:

Proposition. *On a les équivalences suivantes:*

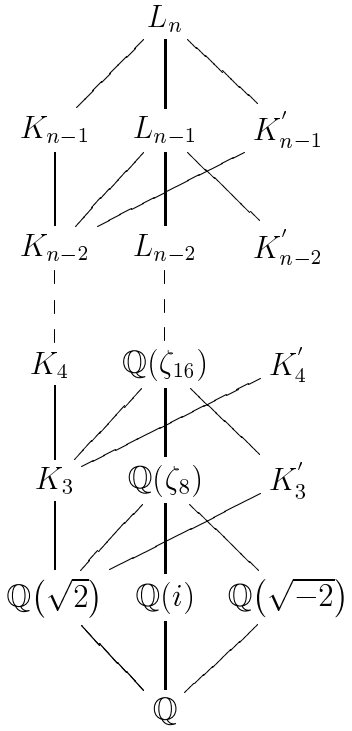
$$q \mid h^-(K_p) \Leftrightarrow q \mid \gcd(C,D) \Leftrightarrow q^2 \mid h^-(K_p).$$

La même remarque que précédemment s'applique, cette proposition est très importante: le calcul du pgcd de deux entiers est très peu coûteux et on peut donc facilement trouver les facteurs premiers q de h^- qui vérifient $q \equiv 5 \pmod 8$. Nous avons donné dans ce cas aussi une table regroupant des exemples des valeurs de $h^-(K_p)$, et leur factorisation en nombres premiers, ainsi que les nombres premiers $q \equiv 5 \pmod 8$ divisant $h^-(K_p)$.

La preuve de la première proposition utilise le fait qu'il existe un sous-corps de $\mathbb{Q}(\zeta_8)$ dans lequel $q \equiv 3 \pmod 4$ reste inerte, à savoir $\mathbb{Q}(i)$, et la deuxième utilise le fait qu'il existe un sous-corps de $\mathbb{Q}(\zeta_8)$ dans lequel $q \equiv 5 \pmod 8$ reste inerte, à savoir $\mathbb{Q}(\sqrt{2})$.
Pour $m \geq 3$, dans le même ordre d'idées, et dans le but d'utiliser le même procédé que précédement, il est naturel de se demander s'il existe un sous-corps de $\mathbb{Q}(\zeta_{2^n})$ dans lequel un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ reste inerte. Ceci nous a amené à déterminer la structure du "treillis" des sous-corps de $\mathbb{Q}(\zeta_{2^n})$, et d'étudier la décomposition d'un tel premier dans ces sous-corps; nous avons obtenu les résultats suivants :

1- **Sous-corps du corps cyclotomique $\mathbb{Q}(\zeta_{2^n})$, $n \geq 2$.**

Notons $L_n = \mathbb{Q}(\zeta_{2^n})$. Posons $K_{n-1} = \mathbb{Q}(\theta_n)$, $\theta_n = \zeta_{2^n} + \zeta_{2^n}^{-1}$, et $K'_{n-1} = \mathbb{Q}(\theta'_n)$, $\theta'_n = \zeta_{2^n} - \zeta_{2^n}^{-1}$.
La structure du "treillis" des sous-corps de L_n peut être décrite par le schéma suivant:



2- **Décomposition dans les sous-corps L_j.**

Soit n, $m \geq 2$. Posons $l = \min(m, n)$. Nous avons démontré le résultat suivant:

Théorème.
Un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-1} premiers distincts dans le corps cyclotomique $L_n = \mathbb{Q}(\zeta_{2^n})$.

Le théorème précédent donne la décomposition dans les sous-corps L_j $(j < n)$ de L_n car si le sous-corps en question est de la forme L_j avec $j < n$, alors on applique ce théorème à L_j; dans ce cas, un nombre premier $q \equiv 1+2^m$

(mod 2^{m+1}) se décompose en 2^{l_j-1} premiers distincts dans le corps cyclotomique L_j, où $l_j = \min(j, m)$. En particulier, pour déterminer la décomposition d'un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ dans L_n, $n \geq m$, il suffit de regarder cette décomposition dans le corps cyclotomique L_m. Les idéaux premiers de $\mathbb{Z}[\zeta_{2^n}]$ au-dessus de q se déduisent alors par extension des idéaux premiers de $\mathbb{Z}[\zeta_{2^m}]$ au-dessus de q.
Comme application, nous avons donné la décomposition explicite d'un premier $q \equiv 9 \pmod{16}$ dans $\mathbb{Q}(\zeta_{2^n})$ pour tout $n \geq 3$. D'autres exemples ont été traités à l'aide de GP Pari (cf. Annexe III).

3- **Décomposition dans les sous-corps K_j et K_j'**

Soient $n \geq 3$, $m \geq 2$ et $l = \min(m, n)$. Avec les notations du théorème précédent, on a le résultat suivant :

Théorème. *Un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-2} premiers distincts dans K_{n-1} ou K_{n-1}'.*

Nous déduisons de cette étude qu'il n'existe pas de sous-corps de $\mathbb{Q}(\zeta_{2^n})$ dans lequel un tel premier reste inerte. Ces résultats ont fait l'objet d'un article paru dans les Comptes rendus mathématiques (Canada) (cf. [6]). Nous avons obtenu le résultat suivant (théorème 4.6.3, p. 79):

Théorème.
Soit K_p le sous-corps de $\mathbb{Q}(e^{2i\pi/p})$ de degré 2^n sur $\mathbb{Q}$, où n est la valuation 2-adique de $p-1$. Soit $m \leq n$.
Si $q \equiv 1 + 2^m \pmod{2^{m+1}}$ divise $h^-(K_p)$, alors $q^{2^{n-m}}$ divise $h^-(K_p)$. De plus si $q^\mu \mid\mid h^-(K_p)$, alors $\mu = 2^{n-m} \cdot l$, où l est un entier.

Chapitre 1

Corps de nombres et nombre de classes

Ce chapitre est consacré à des définitions et des rappels; d'abord sur les corps de nombres, en particulier les corps cyclotomiques, et sur le groupe de classes d'idéaux; ensuite nous donnons quelques résultats sur les corps de type CM.

1.1 Corps de nombres algébriques

Un corps de nombres algébriques (ou simplement corps de nombres) K est une extension finie du corps des rationnels $\mathbb{Q}$. Un élément α de K est dit entier si, et seulement si, il existe un polynôme

$$P(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X^n,$$

où les $a_i \in \mathbb{Z}$, tel que $P(\alpha) = 0$. L'ensemble des entiers de K est un anneau qu'on note A_K. C'est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$. A_K est un anneau de Dedekind, chaque (idéal) premier p de $\mathbb{Z}$ se factorise, d'une manière unique, dans A_K sous forme

$$pA_K = \prod_{i=1}^{g} \mathcal{P}_i^{e_i},$$

où les $\mathcal{P}_i$ sont tous les idéaux premiers de A_K au-dessus de p (i.e. $\mathcal{P}_i \cap \mathbb{Z} = (p)$),
e_i : l'indice de ramification de $\mathcal{P}_i$ relativement à l'extension $K/\mathbb{Q}$. On note
$f_i = [\bar{K}_i : \bar{\mathbb{Q}}]$: le degré résiduel de $\mathcal{P}_i$ relativement à l'extension $K/\mathbb{Q}$, avec

$$\bar{K}_i = A_K/\mathcal{P}_i \quad \text{et} \quad \bar{\mathbb{Q}} = \mathbb{Z}/p\mathbb{Z}$$

sont les corps résiduels respectivement de $\mathcal{P}_i$ et p.
Les entiers e_i, f_i, g_i sont reliés par l'équation

$$\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}] = n.$$

Le discriminant du corps K est défini par

$$\begin{aligned} D_K &= D(x_1, \ldots, x_n)\mathbb{Z} \\ &= det((tr((x_i x_j)))\mathbb{Z} \\ &= (det(\sigma_i(x_j))_{i,j})^2\mathbb{Z}, \end{aligned}$$

avec tr l'application trace :

$$x \in K \longmapsto tr(x) = tr(r_x),$$

où r_x est l'application linèaire $r_x(y) = xy$; $y \in K$,
$\{x_1, \ldots, x_n\}$ une $\mathbb{Z}$-base quelconque de A_K;
les σ_i $(i = 1, \ldots, n)$ sont les $\mathbb{Q}$-plongements de K dans une clôture algébrique de $\mathbb{Q}$.

Théorème 1.1.1. *(Dedekind) Un idéal premier (p) de $\mathbb{Z}$ est ramifié dans K si et seulement si (p) divise D_K.*

Démonstration.
Voir [8] page 35.

Soient K_1 et K_2 deux sous-extensions d'un corps de nombres K, on dit que K_1 et K_2 sont $\mathbb{Q}$-linéairement disjoints si elles vérifient l'une des trois conditions équivalentes suivantes :
i) Tout système de K_1 libre sur $\mathbb{Q}$, est libre sur K_2 .

ii) Tout système de K_2 libre sur $\mathbb{Q}$, est libre sur K_1.
iii) Si $(e_i)_{i\in I}$ est un système de K_1, libre sur $\mathbb{Q}$ et $(f_j)_{j\in J}$ est un système de K_2, libre sur $\mathbb{Q}$, alors $(e_i f_j)_{(i,j)\in I\times J}$ est un système de K_1K_2 libre sur $\mathbb{Q}$.

Théorème 1.1.2. *Soient K_1 et K_2 deux sous-extensions d'un corps de nombres K, $\mathbb{Q}$-linéairement disjoints. On suppose que D_{K_1} et D_{K_2} sont premiers entre eux. Alors $A_{K_1K_2} = A_{K_1}A_{K_2}$ et $D_{K_1K_2} = D_{K_1}^{n_2}D_{K_2}^{n_1}$ où $n_1 = [K_1 : \mathbb{Q}]$ et $n_2 = [K_2 : \mathbb{Q}]$.*

Démonstration.
Voir [10] pages 68 et 69.

Proposition 1.1.3. *Soient K_1 et K_2 deux sous-extensions d'un corps de nombres K. On suppose que $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ sont galoisiennes et que $K_1 \cap K_2 = \mathbb{Q}$. Alors K_1 et K_2 sont $\mathbb{Q}$-linéairement disjoints.*

Démonstration.
L'extension $K_1/\mathbb{Q}$ est galoisienne finie, donc d'après le théorème de l'élément primitif, il existe $\theta \in K_1$ tel que $K_1 = \mathbb{Q}(\theta)$. D'autre part, le polynôme $\mathrm{Irr}(\theta/K_2)$ divise $\mathrm{Irr}(\theta/\mathbb{Q})$ et comme $K_1/\mathbb{Q}$ est normale (car elle est galoisienne), alors $\mathrm{Irr}(\theta/K_2)$ est scindé sur K_1 et par suite

$$\mathrm{Irr}(\theta/K_2) \in K_1[X];$$

ainsi

$$\mathrm{Irr}(\theta/K_2) \in (K_1 \cap K_2)[X] = \mathbb{Q}[X],$$

donc le polynôme $\mathrm{Irr}(\theta/\mathbb{Q})$ divise $\mathrm{Irr}(\theta/K_2)$, d'où

$$\mathrm{Irr}(\theta/K_2) = \mathrm{Irr}(\theta/\mathbb{Q}),$$

donc

$$[K_2(\theta) : K_2] = [K_1 : \mathbb{Q}],$$

et comme $K_1/\mathbb{Q}$ est finie, alors K_1 et K_2 sont $\mathbb{Q}$-linéairement disjoints. □

1.2 Corps cyclotomiques

Soient m un entier positif, Ω une clôture algébrique de $\mathbb{Q}$ et ζ_m une racine primitive m-ième de l'unité dans Ω (i.e. un élément d'ordre m dans Ω^*). On appelle corps cyclotomique toute extension de $\mathbb{Q}$ de la forme $\mathbb{Q}(\zeta_m)$, c'est une extension galoisienne finie de $\mathbb{Q}$ à groupe de Galois canoniquement isomorphe au groupe des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$. On suppose que $m = p^\alpha$, p un nombre premier et α un entier positif.

Proposition 1.2.1. *Soit $\zeta = \zeta_{p^\alpha}$ une racine primitive p^α-ième de l'unité dans une clôture algébrique Ω de $\mathbb{Q}$. Dans le corps cyclotomique $\mathbb{Q}(\zeta)$ on a les résultats suivants :*
a) $Irr(\zeta/\mathbb{Q}) = \Phi_{p^\alpha}(X)$: c'est le p^α-ième polynôme cyclotomique (donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = (p-1)p^{\alpha-1}$).
b) $D_{\mathbb{Q}(\zeta)} = \pm p^{(p\alpha-\alpha-1)p^{\alpha-1}}$;
avec le signe "moins" lorsque $p^\alpha = 4$ ou $p \equiv 3 \pmod 4$ et le signe "plus" dans tous les autres cas.
c) On a $A_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.

Démonstration. Voir [29] page 43.

En combinant les résultats de théorème 1.1.1, proposition 1.1.3 et proposition 1.2.1 on trouve le :

Théorème 1.2.2. *Soient m un entier positif et $K = \mathbb{Q}(\zeta_m)$ un corps cyclotomique. Alors on a :*
a) $Irr(\zeta_m/\mathbb{Q}) = \Phi_m(X)$: le m-ième polynôme cyclotomique,
b) $A_K = \mathbb{Z}[\zeta_m]$, les premiers de $\mathbb{Z}$ ramifiés dans K sont les diviseurs de m, plus précisément si $m = p^\alpha q$ $(pgcd(p,q) = 1)$ alors p a pour indice de ramification relativement à K le nombre $\phi(p^\alpha) = (p-1)p^{\alpha-1}$.

Démonstration.
Voir [29] p. 42 et 43 ou [8] p. 52.

1.2.1 Théorème de Kronecker-Weber

C'est l'un des théorèmes les plus importants en théorie des nombres, il a été énoncé par Kronecker en 1853, mais la preuve qui en a été donnée était incomplète. En 1886 Weber donna une première preuve de ce théorème. Tous les deux s'appuyaient sur les résolvantes de Lagrange. En 1896, Hilbert donna une preuve liée à l'analyse des groupes de ramification ([29] p. 321). Enfin, ce théorème est une conséquence de la théorie du corps de classes.

Théorème 1.2.3. *Toute extension abélienne finie de $\mathbb{Q}$ est une sous-extension d'un corps cyclotomique.*

Démonstration.
Voir [8] page 198.

Soit $K/\mathbb{Q}$ une extension abélienne finie, d'après le théorème précédent, il existe un entier positif m tel que $K \subset \mathbb{Q}(\zeta_m)$.

Définition 1.2.4. *Soit K un corps de nombres abélien; le plus petit entier positif m tel que $K \subset \mathbb{Q}(\zeta_m)$ est appelé le conducteur de K, et noté f_K.*

Nous finissons cette section par un résultat indiquant le nombre de racines de l'unité dans un corps cyclotomique (cf. [4]):

Théorème 1.2.5. *Soit $\zeta_m = e^{2i\pi/m}$, $K = \mathbb{Q}(\zeta_m)$ et W_K le groupe de racines de l'unité contenues dans K. Si m est pair, alors les seules racines de l'unité dans K sont les racines m-ièmes de l'unité et on a donc $W_K \backsimeq (\mathbb{Z}/m\mathbb{Z})$. Si m est impair, alors les seules racines de l'unité dans K sont les racines $(2m)$-ièmes de l'unité et on a donc $W_K \backsimeq (\mathbb{Z}/2m\mathbb{Z})$.*

Démonstration.
Si m est impair, alors

$$\zeta_{2m} = -\zeta_{2m}^{m+1} = -\zeta_m^{(m+1)/2};$$

ceci implique que

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m}).$$

Il suffit alors d'établir le théorème pour m pair. Supposons que $\theta \in \mathbb{Q}(\zeta_m)$ soit une racine k-ième primitive de l'unité avec $k \nmid m$. Alors $\mathbb{Q}(\zeta_m)$ contient

une racine primitive r-ième de l'unité, où $r = \text{ppcm(k, m)} > m$, par suite

$$\mathbb{Q}(\zeta_r) \subset \mathbb{Q}(\zeta_m) \Rightarrow \phi(r) = [\mathbb{Q}(\zeta_r) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m),$$

où ϕ est la fonction d'Euler. Or m est pair et m est un diviseur propre de r, donc $\phi(m)$ est un diviseur propre de $\phi(r)$, par suite $\phi(m) < \phi(r)$; d'où une contradiction. Par conséquent les racines m-ièmes de l'unité sont les seules racines de l'unité dans $\mathbb{Q}(\zeta_m)$. □

Exemple.
Soient p un nombre premier impair, K un sous-corps imaginaire de $\mathbb{Q}(\zeta_p)$ et w_K le nombre de racines de l'unité de K, alors

$$w_K = \begin{cases} 2, & \text{si} \quad K \neq \mathbb{Q}(\zeta_p), \\ 2p, & \text{si} \quad K = \mathbb{Q}(\zeta_p). \end{cases}$$

1.3 Nombre de classes

1.3.1 Groupe de classes d'idéaux

Définition 1.3.1. *On appelle idéal fractionnaire de A_K tout A_K-module $\mathcal{A}$ tel qu'il existe un entier d de A_K vérifiant $d\mathcal{A} \subset A_K$. Un idéal fractionnaire est dit entier si, et seulement si, il est inclus dans A_K.*

L'ensemble des idéaux fractionnaires de K est un groupe qu'on note par $\mathcal{I}$. L'ensemble $\mathcal{I}_{\text{p}}$ des idéaux fractionnaires principaux est un sous-groupe de $\mathcal{I}$. Le groupe quotient C_K de $\mathcal{I}$ par $\mathcal{I}_{\text{p}}$ est appelé groupe des classes de K.

La finitude de groupe de classes a été démontrée par Dirichlet :

Théorème 1.3.2 (Dirichlet). *Pour tout corps de nombres K, le groupe de classes d'idéaux de K est fini.*

Démonstration.
Voir [25] p. 71.

En général l'ordre du groupe C_K est noté h_K ou h, et est appelé nombre de classes de K (au sens ordinaire).

1.3.2 Unités de corps de nombres

Soit n le degré de K sur $\mathbb{Q}$, alors il existe exactement n $\mathbb{Q}$-isomorphismes distincts σ_i de K dans le corps des nombres complexes. On note r_1 le nombre des indices i tels que $\sigma_i(K)$ soit contenu dans le corps des nombres réels et $2r_2$ le nombre des indices tels que $\sigma_i(K)$ ne soit pas contenu dans le corps des nombres réels. Alors on a : $n = r_1 + 2r_2$.

Définition 1.3.3. *On appelle unité de K tout élément de A_K dont l'inverse est aussi un élément de A_K. L'ensemble des unités de K est un groupe qu'on note E_K.*

Théorème 1.3.4 (Théorème des unités de Dirichlet). *Soient $r = r_1 + r_2 - 1$ et U le groupe des racines de l'unité contenues dans K. Alors il existe r unités $\epsilon_1, \ldots, \epsilon_r$ appelées unités fondamentales de K telles que le groupe E_K est le produit direct du groupe U et du groupe engendré par les unités $\epsilon_1, \ldots, \epsilon_r$. Autrement dit, toute unité ϵ de K s'écrit d'une manière unique sous la forme $\epsilon = \xi\epsilon_1^{n_1}\epsilon_2^{n_2}\ldots\epsilon_r^{n_r}$, où ξ est une racine de l'unité contenue dans K et $n_i \in \mathbb{Z}$ pour $1 \leq i \leq r$.*

Démonstration. Voir [25] p. 72.

Remarque. L'ensemble $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ s'appelle un système fondamental d'unités de K.

1.3.3 Idéaux à l'infini

On garde les notations précédentes.

Définition 1.3.5. *On appelle valeur absolue toute application $||$ de K dans $\mathbb{R}$ vérifiant :*
i) $| x | > 0$ sauf pour $x = 0$, auquel cas $| x | = 0$;
ii) $\forall x \in K$, $\forall y \in K$, $| xy | = | x || y |$;
iii) $\forall x \in K$, $\forall y \in K$, $| x + y | \leq | x | + | y |$.

Remarque. Une valeur absolue est dit non archimédienne si, et seulement, si $\forall x \in K$, $\forall y \in K$, $| x + y | \leq \max \{| x | , | y |\}$.

On définit une relation d'équivalence sur l'ensemble des valeurs absolues par : $\mid x \mid$ est équivalente à $\mid x \mid_1$ si, et seulement, si on a : $\forall x \in K$, $\mid x \mid < 1 \Longleftrightarrow \mid x \mid_1 < 1$.

Enfin on donne la définition suivante (voir [8] p. 110):

Définition 1.3.6. *On appelle idéal à l'infini toute classe d'équivalence qui contient l'une des valeurs absolues suivantes :* $\mid \sigma_i(x) \mid$ *où* $i \in \{1, \ldots, r\}$.

1.4 Corps de type CM

Définition 1.4.1. *Soit K un corps de nombres. On dit que K est un corps de type CM si K est totalement imaginaire i.e. $\sigma(K) \cap (\mathbb{C} \setminus \mathbb{R}) \neq \emptyset$, pour tout $\mathbb{Q}$-plongement σ de K dans $\mathbb{C}$ et K est une extension quadratique d'un corps totalement réel K_0 i.e. $\sigma(K_0) \subset \mathbb{R}$ pour tout $\mathbb{Q}$-plongement σ de K_0 dans $\mathbb{C}$.*

Exemples:

- Toute extension imaginaire finie et abélienne de $\mathbb{Q}$ est un corps de type CM.
- Soit ζ_n une racine $n^{ème}$ primitive de l'unité. Le corps cyclotomique $K = \mathbb{Q}(\zeta_n)$ est un corps de type CM. Plus précisément, on a $K = K^+(\sqrt{\triangle})$ avec $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ le sous-corps réel maximal de K, et $\triangle \in K^+$ totalement négatif.

Remarque.
Un corps de type CM est obtenu par l'adjonction à un corps totalement réel K_0 d'une racine carrée d'un nombre appartenant à K_0 dont tous ses conjugués sont négatifs (i.e. totalement négatif).

Théorème 1.4.2. *Soit K un corps de type CM, K^+ son sous-corps réel maximal, h et h^+ leurs nombres de classes respectifs. Alors h^+ divise h. Le nombre $h^- = h/h^+$ est dit nombre de classes relatif de K.*

Pour démontrer ce résultat, on a besoin du lemme suivant:

Lemme 1.4.3. *Soit K/L une extension de corps de nombres, telle qu'il n'existe pas de sous-extension abélienne F/L non triviale et non ramifiée (pour les premiers finis et infinis). Alors h_L divise h_K où h_L et h_K sont respectivement les nombres de classes de L et K.*

Preuve du lemme.
Soit L^1 le corps de Hilbert de L (i.e. l'extension abélienne maximale non ramifiée de L). Par la théorie du corps de classes, si on note $cl(L)$ le groupe de classes de L, alors

$$\mathrm{Gal}(L^1/L) \simeq \mathrm{cl}(L).$$

On a

$$L^1 \cap K = L,$$

car sinon $L^1 \cap K/L$ serait une extension abélienne non ramifiée et qui est non triviale; ceci contredit l'hypothèse. Donc K et L^1 sont L-linéairement disjoints, par suite

$$[KL^1 : K] = [L^1 : L] = h_L.$$

Or KL^1/K est abélienne non ramifiée entraîne que $KL^1 \subset K^1$. Donc

$$[KL^1 : K] \text{ divise } [K^1 : K] = h_K,$$

c'est-à-dire h_L divise h_K. □

Démonstration du théorème.
L'extension K/K^+ est totalement ramifiée pour les premiers infinis, ceci entraîne que K/K^+ satisfait aux conditions du lemme et donc h^+ divise h. □

1.4.1 L'indice $\mathcal{Q}$ d'un corps de type CM.

Théorème 1.4.4. *Soit K un corps de type CM et soient E le groupe des unités de K, E^+ celui de K^+ et W le groupe des racines de l'unité contenues dans K. Alors $\mathcal{Q}=[E, WE^+]=1$ ou 2.*

Pour démontrer ce théorème on a besoin du lemme suivant : (voir [29] p. 4 lemme 1.6)

Lemme 1.4.5. *Soit ε un entier de K (K corps de nombres quelconque) tel que pour tout $\mathbb{Q}$-plongement σ de K, $\mid \sigma(\varepsilon) \mid$=1. Alors ε est une racine de l'unité.*

Démonstration du théorème.
Soit l'application

$$\phi : E \to W, \varepsilon \mapsto \frac{\varepsilon}{\bar{\varepsilon}}.$$

Pour tout $\mathbb{Q}$-plongement σ de K, $\sigma(\bar{\varepsilon}) = \overline{\sigma(\varepsilon)}$, car K est un corps de type CM. On a

$$\mid \sigma(\phi(\varepsilon)) \mid = \mid \frac{\sigma(\varepsilon)}{\sigma(\bar{\varepsilon})} \mid = \mid \frac{\sigma(\varepsilon)}{\overline{\sigma(\varepsilon)}} \mid = 1;$$

et par le lemme précédent $\phi(\varepsilon)$ est une racine de l'unité. Donc ϕ est bien définie.
Considérons maintenant l'application

$$\psi : E \to W/W^2, \varepsilon \mapsto \phi(\varepsilon) \pmod{W^2},$$

et montrons que

$$\mathrm{Ker}\psi = WE^+.$$

Soit $\varepsilon \in WE^+$, $\varepsilon = \xi\varepsilon_1$, avec $\xi \in W$ et $\varepsilon_1 \in E^+$; alors

$$\phi(\varepsilon) = \xi^2 \in W^2 \Longrightarrow \varepsilon \in \mathrm{Ker}\psi.$$

Inversement, soit $\varepsilon \in E$ tel que $\phi(\varepsilon)$=$\xi^2 \in W^2$. Posons $\varepsilon_1 = \xi^{-1}\varepsilon$, $\phi(\varepsilon) = \xi^2$ ce qui implique que $\varepsilon = \xi^2\bar{\varepsilon}$. Donc ε_1=$\xi\bar{\varepsilon}$. $\varepsilon_1 \in E^+$ car $\bar{\varepsilon_1} = \bar{\xi}\varepsilon = \xi^{-1}\varepsilon$; ceci entraîne que ε_1 est réel et par suite $\varepsilon_1 \in E^+$. D'où l'égalité.
Remarquons que

$$E/WE^+ \subset W/W^2$$

et prouvons que $\mid W/W^2 \mid = 2$. L'application

$$\theta : W \to W^2, x \mapsto x^2$$

est surjective et Ker$\theta = \{\pm 1\}$. D'où $\mid W/W^2 \mid = 2$. Par conséquent

$$[E : WE^+] = 1 \text{ ou } 2.$$

Remarque. Si $\phi(E) = W$ alors $\mathcal{Q} = 2$ et si $\phi(E) = W^2$ alors $\mathcal{Q} = 1$.

Corollaire 1.4.6. *Soit $K = \mathbb{Q}(\zeta_n)$. Alors $\mathcal{Q} = 1$ si n est une puissance d'un nombre premier, et $\mathcal{Q} = 2$ sinon.*

Démonstration. Voir [29] p. 39.

Théorème 1.4.7. *Soit C le groupe de classes d'idéaux de $\mathbb{Q}(\zeta_n)$ et C^+ celui de $\mathbb{Q}(\zeta_n)^+$. L'application naturelle $C^+ \to C$ est une injection.*

Démonstration. Voir [29] p. 40.

1.4.2 Régulateur d'un corps de nombres

Soient L un corps de nombres, W le groupe des racines de l'unité contenues dans L, et $r = r_1 + r_2 - 1$ où r_1 le nombre de $\mathbb{Q}$-isomorphismes réels de L et $2r_2$ le nombre de ceux qui sont complexes. Soit $\{\varepsilon_1,\varepsilon_2,...,\varepsilon_r\}$ un système d'unités indépendantes de L i.e. si $\varepsilon_1^{a_1}\varepsilon_2^{a_2}...\varepsilon_r^{a_r} = \xi$, avec $\xi \in W$ et $a_i \in \mathbb{Z}$; alors $a_i = 0$ et $\xi = 1$. Notons $\sigma_1,...,\ \sigma_{r_1},\ \sigma_{r_1+1},...,\ \sigma_{r+1},\ \bar{\sigma}_1,...,\ \bar{\sigma}_{r_1},\ \bar{\sigma}_{r_1+1},...,\ \bar{\sigma}_{r+1}$ les plongements de L dans $\mathbb{C}$, avec σ_j, $1 \leqslant j \leqslant r_1$, réel et σ_j, $\bar{\sigma}_j$, $r_1 + 1 \leqslant j \leqslant r + 1$ est une paire de plongements complexes. Finalement $\delta_j = 1$ si σ_j est réel et $\delta_j = 2$ si σ_j est complexe. Le régulateur est:

$$R_L(\varepsilon_1, \varepsilon_2,..., \varepsilon_r) = \mid det(\delta_i log \mid \varepsilon_j^{\sigma_i} \mid)_{1\leqslant i,j\leqslant r} \mid .$$

Le cas intéressant est lorsque $\{\varepsilon_1, \varepsilon_2,..., \varepsilon_r\}$ est une base du groupe des unités modulo les racines de l'unité, dans ce cas le régulateur est indépendant de la base choisie; on le note R_L et on l'appelle **Régulateur** de L.

Remarque.
Si $\{\varepsilon_1, \varepsilon_2,..., \varepsilon_r\}$ est une base des unités de K^+ modulo ± 1, alors $\delta_i = 1$ pour

K^+, $\delta_i = 2$ pour K, et on a

$$R_K(\varepsilon_1, \varepsilon_2,..., \varepsilon_r) = 2^r R_{K^+}(\varepsilon_1, \varepsilon_2,..., \varepsilon_r) = 2^r R_{K^+}.$$

Lemme 1.4.8. *Soient ε_1, ε_2,...,ε_r des unités indépendantes d'un corps de nombres K qui engendrent un sous-groupe A des unités de K modulo les racines de l'unité, et $\eta_1, \eta_2..., \eta_r$ engendrent un sous-groupe B. Si $A \subset B$ d'indice fini; alors*

$$[A : B] = \frac{R_K(\varepsilon_1, \varepsilon_2,..., \varepsilon_r)}{R_K(\eta_1,..., \eta_r)}.$$

Démonstration. Voir [29] p. 41.

Proposition 1.4.9. *Soit K un corps de nombres et soit K^+ son corps réel maximal. Alors,*

$$\frac{R_K}{R_{K^+}} = \frac{2^r}{\mathcal{Q}}$$

où $r = \frac{deg(K/\mathbb{Q})}{2}$ ($r_1 = 0$, $r = r_2 - 1$).

Démonstration.
On applique le lemme précédent avec $A = WE^+$, $B = E$, $\{\varepsilon_1, \varepsilon_2,...,\varepsilon_r\}$ une base de E^+ modulo W et $\{\eta_1, \eta_2...,\eta_r\}$ celle de E modulo W. On a alors

$$[E : WE^+] = \mathcal{Q} = \frac{R_K(\varepsilon_1, \varepsilon_2,..., \varepsilon_r)}{R_K(\eta_1,..., \eta_r)} = 2^r \frac{R_{K^+}}{R_K}.$$

Chapitre 2

Le nombre de classes relatif des corps cyclotomiques

2.1 Introduction.

Soit p un nombre premier impair. On considère le corps cyclotomique $C_p = \mathbb{Q}(e^{2i\pi/p})$ et on pose $C_p^+ = \mathbb{Q}(e^{2i\pi/p} + e^{-2i\pi/p})$. On sait depuis Kummer que le nombre de classes de C_p est $h = h^+ \cdot h^-$ où h^+ est le nombre de classes de C_p^+ et h^- est un entier. Le facteur h^- a été introduit et étudié par Kummer puis par d'autres, en particulier par Lehmer dans plusieurs papiers. Nous regroupons dans ce chapitre en détail le travail de ce dernier paru dans l'article [11]; et nous proposons quelques compléments ainsi que des exemples originaux.

2.2 Notations et lemmes.

Soit g une racine primitive modulo p, avec $1 < g < p$. Pour $n \in \mathbb{N}$ posons $g_n \equiv g^n \pmod{p}$, $0 < g_n < p$. Posons aussi

$$\zeta = e^{\frac{2i\pi}{p}},\ \xi = e^{\frac{2i\pi}{p-1}},$$

et

$$F = F_p(X) = \sum_{n=0}^{p-2} g_n X^n.$$

Kummer avait prouvé [9] que le nombre de classes relatif est

$$h^-(p) = (2p)^{-\frac{p-3}{2}} | \prod_{n=0}^{\frac{p-3}{2}} F_p(\xi^{2n+1})|. \tag{1}$$

On note par $\Phi_k(X)$ le $k^{\text{ième}}$ polynôme cyclotomique, et pour un entier positif m on pose

$$\Omega_m(X) = \prod_{0<\mu\leq m,\ \mu\ impair} (X - \rho^\mu),\ \rho = e^{\frac{2i\pi}{m}}.$$

Lemme 2.2.1. *Si $m = 2^l m'$, avec m' impair, alors*

$$\Omega_m(X) = \prod_{\delta|m'} \Phi_{m/\delta}(X).$$

Démonstration.

$$\Omega_m(X) = \prod_{0<\mu\leq m,\ \mu\ impair} (X-\rho^\mu) = \prod_{\delta|m'} \prod_{(t,\, m/\delta)=1} (X-\rho^{t\delta}) = \prod_{\delta|m'} \Phi_{m/\delta}(X). \qquad \square$$

Dans l'ensemble $\mathbb{Z}[X]$ des polynômes à coefficients entiers, on définit la fonction de Pierce

$$P \in \mathbb{Z}[X] \longmapsto \Phi^*(P) = \prod_{\beta,\ P(\beta)=0} \Phi_k(\beta) \in \mathbb{Q}$$

où k est un entier fixé.

Remarque.

Désignons par $\mathrm{Res}(\Phi_k, P)$ le résultant des polynômes Φ_k et P. Si P est unitaire alors $\Phi^*(P) = \mathrm{Res}(\Phi_k, P)$ est un entier.

Une variante de la formule (1) de Kummer consiste à remplacer F_p par un polynôme unitaire:

Lemme 2.2.2. *Si $G(X) = G_p(X) = \sum_{n=0}^{p-2} g_n X^{p-n-2}$, alors*

$$h^-(p) = (2p)^{-\frac{p-3}{2}} \prod_{n=0}^{\frac{p-3}{2}} G_p(\xi^{2n+1}).$$

Démonstration.

Il est clair que $G_p(X) = X^{p-2}F_p(X^{-1})$; donc

$$\mid G_p(\xi^{2n+1}) \mid = \mid \xi^{2n+1} \mid\mid F_p(\xi^{2n+1}) \mid = \mid F_p(\xi^{2n+1}) \mid = \mid F_p(\xi^{2n'+1}) \mid , \, n' = \frac{p-3}{2} - n.$$

D'où le résultat à un signe près. Remarquons que

- Si $n \neq n'$ alors

$$G_p(\xi^{2n+1})G_p(\xi^{2n'+1}) = \mid G_p(\xi^{2n+1}) \mid^2 \geq 0.$$

- Si $n = n'$ alors $n = n' = \frac{p-3}{4}$, où $p \equiv 3 \pmod 4$, $\xi^{2n+1} = -1$ et

$$G_p(\xi^{2n+1}) = G_p(-1) = \sum_{n=0}^{p-2} g_n(-1)^{p-n-2} = -\sum_{\nu=0}^{p-2} \nu \left(\frac{\nu}{p}\right) = ph(\sqrt{-p}), (cf.\ [2]\ \text{p. } 344)$$

  où $h(\sqrt{-p})$ est le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$.

Ainsi le signe du produit dans le lemme est positif, ceci achève la démonstration. □

Cette preuve montre au passage un résultat bien connu [18]:

Corollaire 2.2.3. *Si p est un nombre premier congru à 3 modulo 4 alors $h^-(p)$ est divisible par $h(\sqrt{-p})$.*

2.3 Théorèmes de factorisation

2.3.1 Premier théorème de factorisation

Théorème 2.3.1. *Soit $p - 1 = 2^l w$, avec w impair. Alors*

$$(2p)^{\frac{p-3}{2}} h^-(p) = (-1)^{\frac{p-1}{2}} \prod_{d|w} \mathrm{Res}(\Phi_{2^l d}(X), G_p(X)).$$

Démonstration.

$$\begin{aligned}
(2p)^{\frac{p-3}{2}}h^-(p) &= \prod_{v=0}^{\frac{p-3}{2}} G_p(\xi^{2v+1}) \\
&= \mathrm{Res}(G_p(X),\Omega_{p-1}(X)) \\
&= (-1)^{\frac{(p-1)(p-2)}{2}}\mathrm{Res}(\Omega_{p-1}(X),G_p(X)) \quad (\deg G_p = p-2, \deg\Omega_{p-1} = \frac{p-1}{2}) \\
&= (-1)^{\frac{p-1}{2}}\prod_{i=0}^{p-1}\Omega_{p-1}(\alpha_i) \qquad (G_p(\alpha_i)=0) \\
&= (-1)^{\frac{p-1}{2}}\prod_{i=0}^{p-1}\prod_{\delta|w}\Phi_{p-1/\delta}(\alpha_i) \quad \text{(lemme 2.2.1)} \\
&= (-1)^{\frac{p-1}{2}}\prod_{i=0}^{p-1}\prod_{d|w}\Phi_{2^l d}(\alpha_i) \\
&= (-1)^{\frac{p-1}{2}}\prod_{d|w}\prod_{i=0}^{p-1}\Phi_{2^l d}(\alpha_i) \\
&= (-1)^{\frac{p-1}{2}}\prod_{d|w}\Phi^*_{2^l d}(G_p)
\end{aligned}$$

G_p est unitaire, d'après la remarque précédente $\Phi^*_{2^l d}(G_p)$ est un entier; par conséquent on a une factorisation en nombres entiers. □

2.3.2 Le deuxième théorème de factorisation

Le terme à droite du théorème 2.3.1 doit contenir au moins $\frac{p-3}{2}$ facteurs 2 et p. Les facteurs premiers de $\Phi^*_{2^l d}(G_p)$ qui divisent d sont dits *intrinsèques.*

Définition 2.3.2. *Un nombre premier π est dit caractéristique lorsque $\pi \neq 2, p$ et $\pi \nmid d$ mais π divise $\Phi^*_{2^l d}(G_p)$.*

Lemme 2.3.3. *Soit π un premier caractéristique. Alors*

$$\pi^\mu \| \Phi^*_{2^l d}(G_p) \Longrightarrow \pi^\mu \equiv 1 \pmod{2^l d}.$$

Démonstration. Ce résultat est dû à Kummer [9].

Nous reformulons ce résultat comme suit :

Théorème 2.3.4. *Soit q un facteur caractéristique primaire de $\Phi^*_{2^l d}(G_p)$ alors*

$$q \equiv 1 \pmod{2^l d}.$$

2.4 Simplification de caractère somme

Dans la suite nous utiliserons les notations suivantes :
p est un nombre premier impair, g une racine primitive modulo p,
$p-1 = ef$, f impair, $\mathbf{e}$=2.71828... le nombre de Neper,

$$\tau = \frac{e}{(e, \mathrm{Ind}_g 2)}, \alpha = \mathbf{e}^{2i\pi/e},$$

et pour un entier k

$$\chi(k) = \chi_e(k) = \begin{cases} \alpha^{\mathrm{Ind}_g k}, & \text{si } p \nmid k, \\ 0, & \text{si } p \mid k. \end{cases}$$

Nous posons aussi

$$M_e(p) = \sum_{k=0}^{p-1} k\chi_e(k), \quad m_e(p) = \sum_{k=0}^{\frac{p-2}{2}} \chi_e(k), \quad \gamma = \frac{\varphi(e)}{\varphi(\tau)},$$

où φ est la fonction d'Euler.

Lemme 2.4.1. *Si $(r, e) = \delta$ et $e = e_1\delta$ alors*

$$\prod_{(t,e)=1} (X - \mathbf{e}^{2i\pi rt/e}) = \Phi_{e_1}(X)^{\varphi(e)/\varphi(\tau)}.$$

Démonstration.
Le polynôme

$$\psi(X) = \prod_{(t,e)=1} (X - \mathbf{e}^{2i\pi rt/e})$$

est unitaire de degré $\varphi(e)$. De plus ses racines sont les racines $e_1^{\text{ièmes}}$ primitives de l'unité et sont de même ordre de multiplicité. Ecrivons

$$\psi(X) = \Phi_{e_1}(X)^{\nu},$$

et prenons les degrés, il vient que

$$\varphi(e) = \nu\varphi(e_1);$$

c'est-à-dire

$$\nu = \frac{\varphi(e)}{\varphi(e_1)}.$$

Ce qui clôt la démonstration. □

Lemme 2.4.2. *Si* $K = \mathbb{Q}(\mathbf{e}^{2i\pi/e})$ *alors*

$$N_{K/\mathbb{Q}}(2 - \chi_e(2)) = \varphi(e_1)^{\varphi(e)/\varphi(\tau)} = \varphi_\tau(2)^\gamma$$

où N dénote la norme algébrique.

Démonstration.
On applique le lemme précédent avec $r = \text{Ind}_g 2$, $e_1 = \tau$, et X=2. □

Lemme 2.4.3. *On a*

$$(2 - \bar{\chi_e}(2))M_e(p) = -pm_e(p).$$

Démonstration.
Le caractère χ_e est un caractère impair, c'est-à-dire que $\chi_e(-1) = -1$. En effet:

$$\chi_e(-1) = \chi_e(p-1) = \alpha^{\text{Ind}_g(p-1)} = \mathbf{e}^{\pi i(p-1)/e} = (-1)^f = -1.$$

Notons $M' = \sum_{k<p/2} k\chi_e(k)$. Alors

$$M_e(p) - M' = \sum_{p/2<k\leq p-1} k\chi_e(k);$$

posons $r = p - k$, alors

$$\begin{aligned} M_e(p) - M' &= \sum_{r<p/2} (p-r)\chi_e(p-r) \\ &= \sum_{r<p/2} (p-r)\chi_e(-r) \\ &= p\chi_e(-1)m_e(p) - \chi_e(-1)M', \end{aligned}$$

donc

$$M_e(p) = -p\chi_e(-1)m_e(p) + 2M'. \tag{2}$$

D'autre part,

$$M_e(p) = \sum_{k\,pair} k\chi_e(k) + \sum_{k\,impair} (k)\chi_e(k).$$

En faisant le changement $k = 2k'$ dans le premier terme et $k = 2k' + 1$ dans le second , on obtient

$$\begin{aligned} M_e(p) &= \sum_{k<p/2} (2k)\chi_e(2k) + \sum_{k<p/2} (2k+1)\chi_e(2k+1) \\ &= 2\chi_e(2)M' + \sum_{k<p/2} (p-2k)\chi_e(p-2k) \quad (\text{par le changement } k' = \frac{p-1-2k}{2}) \\ &= 2\chi_e(2)M' + \sum_{k<p/2} p\chi_e(2)(-2k) - 2\sum_{k<p/2} k\chi_e(-2k) \\ &= 2\chi_e(2)M' - p\chi_e(2)m_e(p) + 2\chi_e(2)M' \\ &= \chi_e(2)(4M' - pm_e(p)). \end{aligned}$$

D'où

$$\bar{\chi_e}(2)M_e(p) = 4M' - pm_e(p). \tag{3}$$

Multiplions (2) par 2 et en soustrayant à (3) on obtient le lemme. □

Théorème 2.4.4. *On a les relations*

$$\Phi_e^*(G_p) = \mathrm{Res}(\Phi_e, G_p) = (-1)^{\phi(e)} p^{\phi(e)} \mathrm{N}_e(m_e(p))/(\Phi_\tau(2))^\gamma$$

Démonstration.

$$\begin{aligned}
\mathrm{Res}(\Phi_e,G_p) &= (-1)^{\phi(e)(p-2)}\mathrm{Res}(G_p,\Phi_e)\\
&= (-1)^{\phi(e)}\prod_{(t,\,e)=1} G_p(\alpha^t)\\
&= (-1)^{\phi(e)}\prod_{(t,\,e)=1}\sum_{n=1}^{p-1} g_n\alpha^{t(p-n-2)}\\
&= (-1)^{\phi(e)}\prod_{(t,\,e)=1}\alpha^{t(p-2)}\prod_{(t,\,e)=1}\sum_{n=1}^{p-1} g_n\alpha^{-nt}\\
&= (-1)^{\phi(e)}\mathrm{N}_e(\alpha)^{p-2}\prod_{(t,\,e)=1}\sum_{n=1}^{p-1} g_n\alpha^{nt}\\
&= \prod_{(t,\,e)=1}\sum_{n=1}^{p-1} g_n\alpha^{nt}\\
&= \mathrm{N}_e(\sum_{n=1}^{p-1} g_n\alpha^{n}).
\end{aligned}$$

Posons $g_n = k$. Quand n parcourt $\{1,\ldots,p-1\}$, k parcourt aussi $\{1,\ldots,p-1\}$. De plus, comme $g^n \equiv g_n \pmod p$, alors $\mathrm{Ind}_g(g_n)= n$. Donc

$$\sum_{n=1}^{p-1} g_n\alpha^n = \sum_{k=1}^{p-1} k\chi_e(k),$$

d'où

$$\mathrm{Res}(\Phi_e, G_p) = \mathrm{N}_e(M_e(p)).$$

Le résultat découle maintenant des lemmes 2.4.2 et 2.4.3. □

Posons $W = W_e(p) = W_e(p,t) = \sum_{n=1}^{(p-1)/2}(\epsilon_n - \epsilon_{n-1})\alpha^{nt}$, où

$$\epsilon_n = \begin{cases} 1, & \text{si } g_n < p/2,\\ 0, & \text{sinon.}\end{cases}$$

Lemme 2.4.5. *Avec les notations précédentes on a*

$$(1-\alpha)m_e(p) = 2W_e(p,1).$$

Démonstration. Pour simplifier la notation, posons $p = 2r + 1$. On a

$$\alpha^r = (\alpha^{e/2})^f = (-1)^f = -1,$$

et

$$g_{n+r} \equiv g^r g^n \equiv -g_n \pmod{p},$$

autrement dit $g_{n+r} = p - g_n$ et $\epsilon_{n+r} = 1 - \epsilon_n$. En utilisant ces remarques on a la suite de relations

$$\begin{aligned} m_e(p) = \sum_{k=1}^{r} \alpha^{\mathrm{Ind}_g k} &= \sum_{t=0}^{p-2} \epsilon_t \alpha^t \\ &= \sum_{\nu=0}^{r-1} (\epsilon_\nu \alpha^\nu + \epsilon_{\nu+r} \alpha^{\nu+r}) \\ &= \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \sum_{\nu=0}^{r-1} (1 - \epsilon_\nu) \alpha^\nu \\ &= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \sum_{\nu=0}^{r-1} \alpha^\nu \\ &= 2 \sum_{\nu=0}^{r-1} \epsilon_\nu \alpha^\nu - \frac{2}{1-\alpha}, \end{aligned}$$

ceci implique que

$$(1 - \alpha) m_e(p) = 2 \sum_{n=1}^{r} (\epsilon_n - \epsilon_{n-1}) \alpha^n = 2 W_e(p, 1),$$

utilisant le fait que $\epsilon_r = 0$.

Lemme 2.4.6.

$$N_e(m_e(p)) = N_e(W_e(p, 1)) \cdot 2^{J(e)},$$

où

$$J(e) = \begin{cases} \phi(e) - 1, & \text{si } e = 2^k, k \geq 1, \\ \phi(e), & \text{sinon.} \end{cases}$$

Démonstration.

Dans le lemme précédent on prend les normes, il vient que

$$\mathrm{N}_e(1 - \alpha) \mathrm{N}_e(m_e(p)) = 2^{\phi(e)} \mathrm{N}_e(W_e(p, 1)),$$

or d'aprés le théorème de Lebesgue [13]:

$$\mathrm{N}_e(1-\alpha)=\prod_{(t,\,e)=1}(1-\alpha^t)=\Phi_e(1)=\begin{cases}2, & \text{si } e=2^k, k\geq 1,\\ 1, & \text{sinon.}\end{cases}$$

Le lemme en découle immédiatement. □

2.5 Théorème principal de Lehmer

Dans cette section, p désigne toujours un nombre premier impair, g une racine primitive modulo p, l'entier e parcourt les diviseurs de $p-1$ dont les codiviseurs sont impairs, $\tau=\dfrac{e}{(e,\mathrm{Ind}_g 2)}$ et $\gamma=\dfrac{\varphi(e)}{\varphi(\tau)}$.

Théorème 2.5.1. *Si* $h_e(p)=p^{[e/p-1]}N_e(W_e(p,1))\Phi_\tau(2)^{-\gamma}$ *alors*

$$h^-(p)=\prod_{e,\,\frac{p-1}{e}\text{ impair}} h_e(p).$$

Démonstration.

Posons $p-1=2^\lambda w$, $e=2^\lambda d$ $(d\mid w)$, $\tau=\tau(d)$. Notons que $\sum_{d|w}\phi(2^\lambda d)=\frac{p-1}{2}$.

Les théorèmes 2.2.1 et 2.3.4 entraînent

$$\begin{aligned}
(2p)^{\frac{p-3}{2}}h^-(p) &= (-1)^{\frac{p-1}{2}}\prod_{d|w}(-1)^{\phi(e)}p^{\phi(e)}\mathrm{N}_e(m_e(p))\Phi_\tau(2)^{-\gamma}\\
&= p^{(p-2)/2}\prod_{d|w}\mathrm{N}_e(W_e(p,1))\cdot 2^{J(e)}\Phi_\tau(2)^{-\gamma} \qquad \text{(cf. lemme 2.3.6)}\\
&= p^{(p-2)/2}\cdot 2^{\sum_{d|w}J(e)}\prod_{d|w}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma}\\
&= p^{(p-2)/2}\cdot 2^{J(2^\lambda)+\sum_{d|w,\,d\neq 1}J(2^\lambda d)}\prod_{d|w}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma}\\
&= p^{(p-2)/2}\cdot 2^{\phi(2^\lambda)-1+\sum_{d|w,\,d\neq 1}\phi(2^\lambda d)}\prod_{d|w}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma}\\
&= p^{(p-2)/2}\cdot 2^{\frac{p-3}{2}}\prod_{d|w}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma},
\end{aligned}$$

par suite

$$\begin{aligned} h^-(p) &= p\prod_{d|w} \mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma} \\ &= \prod_{d|w} p^{[e/p-1]}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma}, \end{aligned}$$

d'où

$$h^-(p) = \prod_{e,\, \frac{p-1}{e}\ \text{impair}} h_e(p). \qquad (4) \quad \square$$

Remarques.

1) Le nombre premier p divise le terme $\Phi_\tau(2)$ car

$$\tau(w) = \frac{p-1}{(p-1, \mathrm{Ind}_g 2)} = \mathrm{Ord}_p 2.$$

En effet:

$$2^\tau - 1 = \Phi_\tau(2) \prod_{d|\tau,\, d\neq\tau} \Phi_d(2) \equiv 0 \pmod p,$$

ceci entraîne que

$$p \mid \Phi_\tau(2) \prod_{d|\tau,\, d\neq\tau} \Phi_d(2),$$

comme τ est l'ordre de 2 modulo p, alors $p \nmid \prod_{d|\tau,\, d\neq\tau} \Phi_d(2)$; par suite p divise $\Phi_\tau(2)$.

2) On trouve dans l'article [17] de J. M. Masley, une interprétation de la formule (4) via la théorie du corps de classes. $\square$

Nous illustrons le théorème 2.5.1 par l'exemple de $p = 31$. Dans ce cas $g = 3$, $\lambda = 1$, $\mathrm{Ind}_3(2) = 24$. Nous regroupons différents éléments dans le tableau suivant :

e	$\tau(e)$	$\gamma(e)$	$\Phi_\tau(2)^\gamma$	$\mathrm{N}_e(W_e)$
2	1	1	1	3
6	1	2	1	3
10	5	1	31	31
30	5	2	31^2	31

D'où

$$h^-(31) = 31 \cdot 3 \cdot 3 \cdot \frac{31}{31} \cdot \frac{31}{31^2} = 9.$$

2.5.1 Cas spéciaux

Nous allons détérminer les paramètres τ et γ dans le cas où pgcd $(2^\lambda d, \mathrm{Ind}_g(2)) = \delta$ est spécifié.

- $\delta = 1$, $\tau = e$, $\gamma = \frac{\phi(e)}{\phi(\tau)} = 1$

- $\delta = 2$, $\tau = e/2$, $e = 2^\lambda d$. Deux cas sont à envisager:

  1) $\lambda = 1$, $\gamma = 1$.

  2) $\lambda \geq 2$, $\gamma = \frac{2^{\lambda-1}\phi(d)}{2^{\lambda-2}\phi(d)} = 2$

  donc

$$\gamma = \begin{cases} 1, & \text{si } 2 \mid\mid e, \\ 2, & \text{sinon.} \end{cases}$$

- $\delta = 4$, $\tau = e/4$, $e = 2^\lambda d$.

  1) $\lambda = 2$, $\gamma = \frac{\phi(e)}{\phi(\tau)} = 2$,

  2) $\lambda > 2$, $\gamma = \frac{2^{\lambda-1}\phi(d)}{2^{\lambda-3}\phi(d)} = 4$

  donc

$$\gamma = \begin{cases} 2, & \text{si } 4 \mid\mid e, \\ 4, & \text{sinon.} \end{cases}$$

- $\delta = q$ (impair), $\tau = e/q$, écrivons $e = q^\alpha \cdot r$, avec $\mathrm{pgcd}(q, r) = 1$. On distingue alors deux cas :

  1) $\alpha = 1$, $\phi(e) = (q-1)\phi(r)$, $\phi(\tau) = \phi(r)$, $\gamma = \frac{\phi(e)}{\phi(\tau)} = q - 1$,

  2) $\alpha \geq 2$, $\phi(e) = (q-1)q^{\alpha-1}\phi(r)$, $\phi(\tau) = \phi(q^{\alpha-1}r) = (q-1)q^{\alpha-2}\phi(r)$, $\gamma = \frac{\phi(e)}{\phi(\tau)} = q$

d'où

$$\gamma = \begin{cases} q-1, & \text{si } q \,||\, e, \\ q, & \text{sinon.} \end{cases}$$

- $\delta = 2q$, écrivons $e = 2^\lambda q^\alpha r$, on a à distinguer quatre cas :

  1) $\lambda = 1$, $\alpha = 1$, $e = 2qr$, $\tau = r$, donc $\gamma = q-1$,
  2) $\lambda = 1$, $\alpha \geq 2$, $\phi(e) = (q-1)q^{\alpha-1}\phi(r)$, $\tau = e/2q = q^{\alpha-1}r$, $\phi(\tau) = (q-1)q^{\alpha-2}\phi(r)$, ainsi $\gamma = q$,
  3) $\alpha = 1$ $\lambda \geq 2$, $\phi(e) = (q-1)q^{\alpha-1}\phi(r)$, $\tau = e/2q = 2^{\lambda-1}r$, $\phi(\tau) = 2^{\lambda-2}\phi(r)$, donc $\gamma = 2(q-1)$,
  4) $\lambda \geq 2$, $\alpha \geq 2$, $\phi(e) = 2^{\lambda-1}(q-1)q^{\alpha-1}\phi(r)$, $\phi(\tau) = 2^{\lambda-2}(q-1)q^{\alpha-2}\phi(r)$, d'où $\gamma = 2q$,

  donc

$$\gamma = \begin{cases} q-1, & \text{si } 2 \,||\, e, q \,||\, e, \\ q, & \text{si } 2 \,||\, e, q^2 \mid e, \\ 2(q-1) & \text{si } 4 \mid e, q \,||\, e, \\ 2q, & \text{sinon.} \end{cases}$$

Nous récapitulons ces résultats dans le tableau ci-dessous qui figure dans [11] mais sans les explications précédentes:

δ	τ	γ
1	e	1
2	$e/2$	$\begin{cases} 1, & \text{si } 2 \,\|\| \, e, \\ 2, & \text{sinon.} \end{cases}$
4	$e/4$	$\begin{cases} 2, & \text{si } 4 \,\|\| \, e, \\ 4, & \text{sinon.} \end{cases}$
q	e/q	$\begin{cases} q-1, & \text{si } q \,\|\| \, e, \\ q, & \text{sinon.} \end{cases}$
$2q$	$e/2q$	$\begin{cases} q-1, & \text{si } 2 \,\|\| \, e, q \,\|\| \, e, \\ q, & \text{si } 2 \,\|\| \, e, q^2 \mid e, \\ 2(q-1) & \text{si } 4 \mid e, q \,\|\| \, e, \\ 2q, & \text{sinon.} \end{cases}$

Un autre cas simple est lorsque p est *un nombre premier de Fermat*, p est alors de la forme

$$p = 2^{2^\nu} + 1.$$

On a dans ce cas:

$$\lambda = 2^\nu, \quad w = 1, \quad e = 2^{2^\nu}, \quad \text{et} \quad \tau(e) = \mathrm{Ord}_p(2) = 2^{\nu+1},$$

car

$$2^{2^{\nu+1}} = (p-1)^2 \equiv 1 \pmod{p};$$

d'autre part on a

$$\gamma(e) = \frac{\phi(e)}{\phi(\tau)} = 2^{2^\nu - \nu - 1},$$

et

$$\Phi_\tau(X) = X^{2^\nu} + 1;$$

par suite

$$\Phi_\tau(2) = 2^{2^\nu} + 1 = p.$$

Exemple. Pour $p = 257$, on a $\nu = 3$, $\gamma(e) = 16$,

$$h^-(257) = \frac{1}{p^{15}} \mathrm{N}_{256}(W_{256}),$$

$h^-(257) = 257 \cdot 20738946049 \cdot 10229977445639119615612986981834190371496 97,$

sa factorisation en nombres premiers (voir Annexe II).

2.6 Facteurs intrinsèques

Dans cette section nous étudions les propriétés des facteurs premiers intrinsèques de $h^-(p)$. Nous commençons par ceux qui sont impairs.

2.6.1 Facteurs intrinsèques impairs

Théorème 2.6.1. *Soit $p-1=ef$, f impair. Soit q un facteur premier de f. Alors q divise h_{eq} si et seulement si q divise h_e.*

Démonstration.

Nous savons que

$$\mathrm{Res}(\Phi_{eq}, G_p) = \mathrm{N}_{eq}(M_{eq}(p)) = \prod_{(t,\,eq)=1} \sum_{n=1}^{p-1} g_n \alpha_1^{tn},$$

où $\alpha_1 = \mathbf{e}^{2i\pi/eq}$; donc $\alpha_1^q = \alpha$. En utilisant la formule multinomiale,

$$(X_1 + \cdots + X_{p-1})^q = X_1^q + \cdots + X_{p-1}^q + qF(X_1, \ldots, X_{p-1})$$

où $F \in \mathbb{Z}[X_1, \ldots, X_{p-1}]$, on a

$$\mathrm{Res}^q(\Phi_{eq}, G_p) = \prod_{(t,\,eq)=1} \sum_{n=1}^{q} g_n^q \alpha_1^{qtn} + q\Psi,$$

où $\Psi \in \mathbb{Z}[\alpha_1]$. On obtient

$$\mathrm{Res}^q(\Phi_{eq}, G_p) = \prod_{(t,\,eq)=1} \sum_{n=1}^{q} g_n^q \alpha^{tn} + q\Psi, \qquad (\,\alpha_1^q = \alpha\,)$$

d'où

$$\mathrm{Res}^q(\Phi_{eq}, G_p) \equiv \left(\prod_{(t,\,e)=1} \sum_{n=1}^{p-1} g_n \alpha^{tn} \right)^{\phi(eq)/\phi(e)} \pmod{q},$$

par suite

$$\Phi_{eq}^* \equiv \Phi_e^{*\mu} \pmod{q},$$

où

$$\mu = \begin{cases} 1, & \text{si } q \mid e, \\ q-1, & \text{sinon.} \end{cases}$$

En particulier, $q \mid \Phi_{eq}^*$ est équivalent à $q \mid \Phi_e^*$. □

Exemple.

Prenons $p = 379$, $p - 1 = 2 \cdot 3^2 \cdot 7$. On a $3 \mid h_2 = 3$. Par suite, d'après le théorème précédent, $3 \mid h_6 = 3 \cdot 13$, $3 \mid h_{18} = 3 \cdot 991$ et $3 \mid h_{54} = 3 \cdot 29997973$.

Remarque.

Nous montrerons dans le chapitre 3, que pour $e = 2^\lambda$, $h_{2^\lambda}(p)$ est égal au nombre de classes relatif du sous-corps K_p de $\mathbb{Q}(e^{2i\pi/p})$ de degré $e = 2^\lambda$; ainsi le théorème précédent contient le théorème 3 de Metsänkylä [18]. En effet: soit

$$q \mid h_{2^\lambda}(p) \, (= h^-(K_p)),$$

donc d'après le théorème 2.6.1

$$q \mid h_{2^\lambda q}(p),$$

d'où

$$q^2 \mid h^-(p).$$

Par conséquent si $q^t \mid h^-(K_p)$ alors $q^{t+1} \mid h^-(p)$.

2.6.2 Facteur intrinsèque 2

Nous donnons dans cette section des propriétés et quelques remarques concernant le facteur intrinsèque 2.

Si $p \equiv 3 \pmod 4$ alors $h_2(p)$ est impair.
Si $e = 2^l$ alors $h_e(p)$ est impair ([29], théorème 10.4).
Si $e = 2^l d$, avec $d > 1$ alors

$$v_2(h_e(p)) \equiv 0 \pmod \nu,$$

où v_2 désigne la valuation 2-adique et $\nu = \mathrm{Ord}_d(2)$ l'ordre de 2 modulo d. Autrement dit, il existe $j \geq 0$ tel que

$$2^{j\nu} \mid h_e(p).$$

Remarques.

1) L'entier j peut être égal à 1 comme le montre l'exemple suivant

$$h_{62}(311) = 2^{10} \cdot 9918966461 \quad \text{et} \quad \mathrm{Ord}_{31}(2) = 5.$$

2) Newman [22] avait conjecturé que si $h^-(p)$ est pair et si $2^m \mid h^-(p)$ alors nécessairement $m \geq 2$. Metsänkylä ([18], théorème 1) montrait cette conjecture.
Dans le cas où $e = 2^l d$, avec $d > 1$, nous savons qu'il existe

$$j \geq 0 \quad \text{tel que} \quad 2^{j\nu} \mid h_e(p).$$

Comme

$$\nu = \mathrm{Ord}_d(2),$$

alors $\nu \geq 2$. Et donc si 2 divise $h_e(p)$ alors $j \geq 1$, par suite $j\nu \geq 2$ et la conjecture de Newman en découle immédiatement.

3) Notons aussi que $2^{j\nu} \equiv 1 \pmod{d}$ donc $2^{j\nu}$ apparaît comme facteur caractéristique primaire : $2^{j\nu} = dx + 1$.

4) On trouve dans [12] une table donnant des valeurs de $h^-(p)$ et leur factorisation en nombres premiers, pour $200 < p < 521$.

Chapitre 3

Le nombre de classes relatif de certains sous-corps du corps cyclotomique $\mathbb{Q}(\zeta_p)$

Dans ce chapitre nous utiliserons l'expression analytique du nombre de classes relatif pour montrer que $h_e(p)$, décrit dans le chapitre précédent, correspond au nombre de classes relatif d'un certain sous-corps K_p de $\mathbb{Q}(\zeta_p)$ lorsque e est une puissance de 2. Nous donnerons aussi une majoration de ce nombre de classes relatif.

3.1 Préliminaires sur les caractères et conducteurs.

Nous regroupons dans cette section quelques résultats sur la théorie des caractères et conducteurs dont nous aurons besoin.

3.1.1 Caractères de groupes abéliens finis.

On appelle caractère d'un groupe abélien fini G tout homomorphisme $\chi : G \to \mathbb{C}^*$, où $\mathbb{C}^*$ est le groupe multiplicatif de $\mathbb{C}$.
Soient χ_1, χ_2 deux caractères de G, on définit le produit

$$\chi_1\chi_2(\sigma) = \chi_1(\sigma)\chi_2(\sigma), \forall\sigma \in G.$$

L'ensemble des caractères de G est noté $\hat{G}$. Muni de la multiplication ainsi définie, $\hat{G}$ est un groupe abélien dont l'élément neutre est l'homomorphisme trivial

$$\chi_0 : G \to \mathbb{C}^*,$$

$\chi_0(\sigma) = 1, \forall \sigma \in G$; appelé caractère unité.

Définition 3.1.1. *Soient H un sous-groupe de G, et $\mathcal{X}$ un sous-groupe de $\hat{G}$. On définit les sous-groupes respectifs de $\hat{G}$ et G suivants:*
$H^\perp = \{\chi \in \hat{G} \mid \chi(\sigma) = 1, \forall \sigma \in H\}$, *et* $\mathcal{X}^\perp = \{\sigma \in G \mid \chi(\sigma) = 1, \forall \chi \in \mathcal{X}\}$.

On vérifie immédiatement que:
i) $H \subset (H^\perp)^\perp$,
ii) $(HH')^\perp = H^\perp \cap H'^\perp$,
iii) *Si* $H \subset H'$ *alors* $H'^\perp \subset H^\perp$,
iv) $H^\perp = (H^{\perp\perp})^\perp$,

pour tous sous-groupes H et H' de G.

Propriétés
Soient G un groupe abélien fini, et H un sous-groupe de G. Alors on a:
1) $\overline{\hat{G/H}} \simeq H^\perp$
2) $(\hat{G}/H^\perp) \simeq \hat{H}$,
3) $H^{\perp\perp} = H$,
4) Si H' est un sous-groupe de G alors $H^\perp H'^\perp = (H \cap H')^\perp$.

3.1.2 Caractères résiduels

Ce sont les caractères du groupe de classes résiduelles de $(\mathbb{Z}/m\mathbb{Z})^*$ (m entier positif). Soit $d \mid m$, l'application

$$\Pi_{dm} : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*, \quad \bar{a} \mod m \longmapsto \bar{a} \mod d$$

est un homomorphisme de groupes surjectif, il induit un homomorphisme injectif:

$$i_{dm} : \overline{\hat{(\mathbb{Z}/d\mathbb{Z})^*}} \to \overline{\hat{(\mathbb{Z}/m\mathbb{Z})^*}}$$

$$\chi \longmapsto i_{dm}(\chi) = \chi \circ \Pi_{dm}.$$

On vérifie que

$$\mathrm{Im} i_{dm} = \{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^*} \mid \mathrm{Ker}\Pi_{dm} \subset \mathrm{Ker}\chi\};$$

et

$$\Pi_{dm} = \Pi_{dd_1} \circ \Pi_{d_1 m}$$

pour tout multiple d_1 de d tel que $d_1 \mid m$.

3.1.3 Caractères de Dirichlet et conducteurs

Soit χ un caractère résiduel modulo m, l'application définie par:

$$\widetilde{\chi} : \mathbb{Z} \to \mathbb{C},\ a \longmapsto \widetilde{\chi}(a) = \begin{cases} \chi(\bar{a}) & \text{si pgcd(a, m)} = 1, \\ 0, & \text{sinon,} \end{cases}$$

est appelée caractère modulaire associé à χ. On conserve la notation χ pour $\widetilde{\chi}$.

Réciproquement, toute application $\chi : \mathbb{Z} \to \mathbb{C}$ telle que
i) $\chi(a) = 0, \forall a \in \mathbb{Z}$ tel que $\mathrm{pgcd}(a, m) \neq 1$,
ii) $\chi(aa') = \chi(a)\chi(a'), \forall a, a' \in \mathbb{Z}$ tels que $\mathrm{pgcd}(a, m) = \mathrm{pgcd}(a', m) = 1$,
iii) $\chi(a) \neq 0, \forall a \in \mathbb{Z}$ tel que $\mathrm{pgcd}(a,m) = 1$

définit un caractère résiduel modulo m.

L'entier

$$f_\chi = \inf\{d \mid m \text{ et } \chi \in \mathrm{Im} i_{dm}\}$$

s'appelle le conducteur de χ. Lorsque $\mathcal{X}$ est un sous-groupe de $\widehat{(\mathbb{Z}/m\mathbb{Z})^*}$, il sera dit groupe de caractères résiduels modulo m et le conducteur de $\mathcal{X}$ est défini par

$$f_{\mathcal{X}} = \mathrm{ppmc}\{f_\chi \mid \chi \in \mathcal{X}\}.$$

Un caractère résiduel est dit primitif si $f_\chi = m$ i.e. $\forall d \mid m\,(d \neq m)$, $\exists a \in \mathbb{Z}$ tel que

$$a \equiv 1 \pmod{d} \text{ et } \chi(\bar{a} \pmod{m}) \neq 1.$$

Définition 3.1.2. *Un caractère de Dirichlet est un caractère modulaire dont le caractère résiduel est un caractère primitif.*

3.1.4 Correspondance θ_m et conducteur.

On définit l'application θ_m (cf. [24]) comme suit:
Pour chaque sous-extension K de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, soit H le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$ correspondant à $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$, et

$$\mathcal{X} = H^{\perp} = \{\chi \in \widehat{\overline{(\mathbb{Z}/m\mathbb{Z})^*}} \mid \chi(\sigma) = 1, \forall \sigma \in H\}.$$

L'application θ_m associe à $K/\mathbb{Q}$ le groupe $\mathcal{X}$. On a le théorème suivant:

Théorème 3.1.3. *L'application θ_m est une bijection entre l'ensemble des sous-corps de $\mathbb{Q}(\zeta_m)$ et l'ensemble des groupes de caractères résiduels modulo m. Si $\theta_m(K) = \mathcal{X}$, alors*

$$f_K = f_{\mathcal{X}} \text{ et } \widehat{\overline{\mathrm{Gal}(K/\mathbb{Q})}} \simeq \mathcal{X},$$

où f_K est le conducteur de K.

Remarques.
1) Soit χ un caractère de $(\mathbb{Z}/m\mathbb{Z})^*$ et soit f_χ son conducteur. Alors

$$\mathrm{Ker}\Pi_{f_\chi m} \subset \mathrm{Ker}\chi.$$

2) Soit $\mathcal{X}$ un groupe de caractères résiduels modulo m. On a

$$\cap_{\chi \in \mathcal{X}} \mathrm{Ker}\chi = \mathcal{X}^{\perp}.$$

3) $\mathrm{Inv}(\mathrm{Ker}\Pi_{dm}) = \mathbb{Q}(\zeta_d)$. En effet, le fait que l'application Π_{dm} soit surjective entraîne que

$$(\mathbb{Z}/m\mathbb{Z})^*/\mathrm{Ker}\Pi_{dm} \simeq (\mathbb{Z}/d\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}).$$

Démonstration du théorème 3.1.3.
L'application θ_m est la composée de deux bijections:
i) la correspondance de Galois qui associe à K, $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$,
ii) l'application qui associe à chaque sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, son orthogonal, qui est une bijection décroissante (au sens de l'inclusion). Donc l'application θ_m est une bijection croissante (au sens de l'inclusion) entre

l'ensemble des sous-corps de $\mathbb{Q}(\zeta_m)$ et l'ensemble des groupes de caractères résiduels modulo m.
Montrons que $f_K = f_{\mathcal{X}}$. Posons $f = f_{\mathcal{X}}$. On a

$$\Pi_{f_\chi m} = \Pi_{f_\chi f} \circ \Pi_{fm}$$

pour tout $\chi \in \mathcal{X}$, par suite

$$\mathrm{Ker}\Pi_{fm} \subset \mathrm{Ker}\Pi_{f_{\mathcal{X}} m}, \forall \chi \in \mathcal{X},$$

ainsi

$$\mathrm{Ker}\Pi_{fm} \subset \cap_{\chi\in\mathcal{X}}\mathrm{Ker}\Pi_{f_{\mathcal{X}} m} \subset \cap_{\chi\in\mathcal{X}}\mathrm{Ker}\chi = \mathcal{X}^{\perp} (= \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K),$$

d'où

$$K \subset \mathrm{Inv}(\mathrm{Ker}\Pi_{f_{\mathcal{X}} m}) = \mathbb{Q}(\zeta_f),$$

ce qui implique $f_K \leq f_{\mathcal{X}}$. D'autre part, on a $K \subset \mathbb{Q}(\zeta_{f_K})$

donc

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{f_K})) \subset H\,(= \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)) \Longrightarrow H^{\perp} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{f_K}))^{\perp}$$

comme

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{f_K}))^{\perp} \simeq \overline{\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})/\hat{\mathrm{Gal}}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{f_K}))} = \overline{(\mathbb{Z}/\hat{f_K}\mathbb{Z})^*}$$

alors $\mathcal{X} \subset \overline{(\mathbb{Z}/\hat{f_K}\mathbb{Z})^*}$

ce qui implique $f_\chi \mid f_K$, $\forall \chi \in \mathcal{X}$ ainsi $f \mid f_K$, comme $f_K \leq f_{\mathcal{X}}$ alors $f = f_K$.

Proposition 3.1.4. *Soient X_1 et X_2 deux groupes de caractères de Dirichlet correspondant aux sous-corps K_1 et K_2 de $\mathbb{Q}(\zeta_m)$ respectivement. Alors on a:*
1) $X_1 \subset X_2 \Leftrightarrow K_1 \subset K_2$,
2) Le groupe engendré par X_1 et X_2 correspond au produit K_1K_2.

Démonstration.
1) Soient H_1 et H_2 les sous-groupes de $(\mathbb{Z}/m\mathbb{Z})^*$ correspondant à $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1))$ et $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_2)$ respectivement. Par définition $X_1 = H_1^\perp$ et $X_2 = H_2^\perp$. On a les équivalences

$$\begin{aligned} X_1 \subset X_2 &\Leftrightarrow H_1^\perp \subset H_2^\perp \\ &\Leftrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1) \supset \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_2) \\ &\Leftrightarrow \mathrm{Inv}(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1)) \subset \mathrm{Inv}(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_2)) \\ &\Leftrightarrow K_1 \subset K_2. \end{aligned}$$

2) Soit H le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$ correspondant au produit $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1K_2)$ et soit $X = H^\perp$. Alors

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1K_2) &= \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_1) \cap \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K_2) \\ &\Leftrightarrow H = H_1 \cap H_2 \\ &\Leftrightarrow H^\perp = (H_1 \cap H_2)^\perp = H_1^\perp H_2^\perp \\ &\Leftrightarrow X = X_1X_2. \end{aligned}$$

3.2 Formules analytiques pour le nombre de classes relatif

Soit K un corps abélien imaginaire, ou plus généralement un corps de type CM, c'est-à-dire une extension quadratique totalement imaginaire d'un corps totalement réel K_0. Le nombre de classes de K est mis sous la forme $h_K = h^- h_{K_0}$. La théorie du corps de classes interprète h^- comme un nombre de classes relatif et donc un entier (cf. chap.1, théorème 1.4.2).

3.2.1 Cas des sous-corps d'un corps cyclotomique

Au cours de cette section :

p désigne un nombre premier impair, C_p le corps cyclotomique de conducteur p. On a un isomorphisme

$$G = \mathrm{Gal}(C_p/\mathbb{Q}) \backsimeq (\mathbb{Z}/p\mathbb{Z}).^{\cdot}$$

Un générateur de G est

$$\sigma : \zeta_p \to \zeta_p^g;$$

où g est une racine primitive modulo p. Soit χ un caractère de Dirichlet de $(\mathbb{Z}/p\mathbb{Z})^*$, les nombres de Bernoulli généralisés $B_{1,\chi}$ sont définis par

$$B_{1,1} = -1/2, \quad B_{1,\chi} = \frac{1}{p}\sum_{a=1}^{p-1}\chi(a)a \qquad \text{pour } \chi \neq 1.$$

Soit K un sous-corps imaginaire de degré n de C_p, donc n est pair,

Il est bien connu (voir [29] p. 43) que le nombre de classes relatif de K est donné par la formule:

$$h^-(K) = \mathcal{Q}_{\mathcal{K}} w_K \prod_{\chi}\left(\frac{-1}{2}B_{1,\chi}\right),$$

où χ parcourt les caractères impairs[1] de $\mathrm{Gal}(K/\mathbb{Q})$; ces caractères opèrent trivialement sur $\mathrm{Gal}(C_p/K)$ (cf. section 3.1.4),
w_K est le nombre de racines de l'unité dans K, et $\mathcal{Q}_K$ est l'indice de l'unité de Hasse de K, $\mathcal{Q}_K \in \{1, 2\}$. En fait $\mathcal{Q}_K = 1$ en vertu de résultat suivant dû à Latimer (cf. [28], proposition 2.1):

Lemme 3.2.1. *Pour tout sous-corps imaginaire K de $\mathbb{Q}(\zeta_p)$, on a* $\mathcal{Q}_{\mathcal{K}} = 1$.

Nous donnons ici une preuve de H-W-Lenstra (cf. [28]) :

Démonstration. .
Soient H le groupe de Galois de $K/\mathbb{Q}$, σ un générateur de H, et u unité de K. Soit n le degré de K sur $\mathbb{Q}$. Il suffit de montrer que $\overline{u}/u = \eta^2$ pour une racine de l'unité η, ainsi $u/\overline{\eta}$ est une unité réelle (section 1.4.1 page 19).

1. C'est-à-dire tels que $\chi(-1) = -1$.

Soit $v = uu^{\sigma} \dots u^{\sigma^{n/2-1}}$. Alors $\overline{u}/u = v^{\sigma}/v$, et $v\overline{v}$ est une norme de u, qui est égale à 1. Par conséquent v est une racine de l'unité. Le groupe H opère trivialement sur le groupe des racines des unités modulo les carrés, par suite v^{σ}/v est carré d'une racine de l'unité. □

Rappelons que (cf. chap1., théorème 1.2.5)

$$w_K = \begin{cases} 2, & \text{si } K \neq C_p, \\ 2p, & \text{si } K = C_p. \end{cases}$$

En résumé on a:

$$h^-(K) = \begin{cases} 2p \prod_{\chi} \left(\frac{-1}{2} B_{1,\chi}\right), & \text{si } K = \mathbb{Q}(\zeta_p), \\ 2 \prod_{\chi} \left(\frac{-1}{2} B_{1,\chi}\right), & \text{si } K \neq \mathbb{Q}(\zeta_p). \end{cases}$$

Notons X_K le groupe des caractères primitifs de Dirichlet qui opère trivialement sur $\mathrm{Gal}(C_p/K)$, et X_K^- l'ensemble des caractères $\chi \in X_K$ tels que $\chi(-1) = -1$. Pour chaque sous-groupe cyclique X de X_K choisissons un générateur $\psi \in X$, et notons n_ψ l'ordre de ψ, N_ψ la norme dans $\mathbb{Q}(\zeta_{n_\psi})/\mathbb{Q}$, et finalement Y_K^- l'ensemble de tels générateurs ψ qui sont impairs. Alors on a le résultat suivant (cf. [15], page 147 formule (3.8)):

Proposition 3.2.2.

$$h^-(K) = \mathcal{Q}_K w_K \prod_{\psi \in Y_{K^-}} N_\psi \left(\frac{-1}{2} B_{1,\psi}\right) \tag{2.1}$$

avec

$$B_{1,\chi} = -\frac{1}{2 - \bar{\chi}(2)} S_\chi, \tag{2.2}$$

où

$$S_\chi = \sum_{1 \leq x \leq f_\chi/2} \chi(x)$$

est un entier algébrique.

Démonstration. On a

$$\begin{aligned} h^-(K) &= Q_K w_K \prod_{\chi\in X_K^-}\left(\frac{-1}{2}B_{1,\chi}\right) \\ &= Q_K w_K \prod_{\chi\in X_K^-}\left(\frac{-1}{2f_\chi}\sum_{a=1}^{p-1}\chi(a)a\right) \\ &= Q_K w_K \prod_{\psi\in Y_K^-}\prod_{(u,n_\psi)=1}\left(\frac{-1}{2f_\chi}\sum_{a=1}^{p-1}\psi^u(a)a\right) \\ &= Q_K w_K \prod_{\psi\in Y_K^-}\prod_{(u,n_\psi)=1}\left(\frac{-1}{2}B_{1,\psi^u}\right) \\ &= Q_K w_K \prod_{\psi\in Y_{K-}} \mathrm{N}_\psi\left(\frac{-1}{2}B_{1,\psi}\right), \end{aligned}$$

d'où (2.1).
L'égalité (2.2) découle du lemme suivant [5]:

Lemme 3.2.3. *Soit χ un caractère de Dirichlet impair de conducteur f. Si $f \not\equiv 2 \pmod 4$, alors*

$$\sum_{0<a<f/2}\chi(a)a = \frac{f}{2-\bar\chi(2)}\sum_{1\le a\le f/2}\chi(a).$$

Démonstration.
Si $f \nmid 2$ alors, d'une part on a

$$\begin{aligned} -\sum_{0<a<f}\chi(a)a &= -\sum_{0<a<f,\,2|a}(\chi(a)a+\chi(f-a)(f-a)) \\ &= -\sum_{0<a<f/2}\chi(2a)(2a)\sum_{0<a<f/2}\chi(2a)(f-2a). \end{aligned}$$

Par suite

$$-\overline{\chi}(2)\sum_{0<a<f}\chi(a)a = \sum_{0<a<f}(f-4a)\chi(a). \tag{3.1}$$

D'autre part,

$$\begin{aligned} -\sum_{0<a<f} \chi(a)a &= -\sum_{0<a<f/2} \chi(a)(a) - \sum_{0<a<f/2} \chi(f-a)(f-a) \\ &= -\sum_{0<a<f/2} \chi(a)(a) + \sum_{0<a<f/2} \chi(a)(f-a) \\ &= \sum_{0<a<f} (f-2a)\chi(a). \end{aligned}$$

De (3.1) et la dernière relation on tire

$$\sum_{0<a<f/2} \chi(a)a = \frac{f}{2-\bar{\chi}(2)} \sum_{1\leq a\leq f/2} \chi(a).$$

Maintenant si $4 \mid f$, alors $\chi(2) = 0$ et $\chi(x + \frac{f}{2}) = -\chi(x)$. On a

$$\begin{aligned} \sum_{0<a<f} \chi(a)a &= \sum_{0<a<f/2} \chi(a)a + \sum_{0<a<f/2} \chi\Big(a+\frac{f}{2}\Big)\Big(a+\frac{f}{2}\Big) \\ &= \sum_{0<a<f/2} \chi(a)a - \sum_{0<a<f/2} \chi(a)\Big(a+\frac{f}{2}\Big) \\ &= -\frac{f}{2} \sum_{0<a<f/2} \chi(a). \end{aligned}$$

D'où le lemme. □

Remarque.

Si χ est d'ordre m, alors S_χ appartient à $\mathbb{Z}[\zeta_m]$, l'anneau des entiers algébriques du corps cyclotomique $\mathbb{Q}(\zeta_m)$.

3.2.2 Etude de cas d'un sous-corps particulier : théorème principal

Pour tout diviseur e de $p-1$ dont le codiviseur est impair, notons K_e l'unique sous-corps imaginaire cyclique de C_p tel que $[K_e : \mathbb{Q}] = e$.
Reprenons les notations de section 2.3 du chapitre 2: Soit g une racine primitive modulo p, avec $1 < g < p$. Pour $n \in \mathbb{N}$ posons $g_n \equiv g^n \pmod{p}$,

$0 < g_n < p$. $p-1 = ef$, f impair, $\mathbf{e}$=2.71828... le nombre de Neper,

$$\tau = \frac{e}{(e, \mathrm{Ind}_g 2)}, \alpha = \mathbf{e}^{2i\pi/e},$$

et pour un entier k

$$\chi(k) = \chi_e(k) = \begin{cases} \alpha^{\mathrm{Ind}_g k}, & \text{si } p \nmid k, \\ 0, & \text{si } p \mid k. \end{cases}$$

On pose

$$M_e(p) = \sum_{k=0}^{p-1} k\chi_e(k), \quad m_e(p) = \sum_{k=0}^{\frac{p-2}{2}} \chi_e(k), \quad \gamma = \frac{\varphi(e)}{\varphi(\tau)},$$

où φ est la fonction d'Euler. On définit aussi

$$W = W_e(p) = W_e(p,t) = \sum_{n=1}^{(p-1)/2} (\epsilon_n - \epsilon_{n-1})\alpha^{nt},$$

où

$$\epsilon_n = \begin{cases} 1, & \text{si } g_n < p/2, \\ 0, & \text{sinon.} \end{cases}$$

Enfin,

$$h_e(p) = p^{[e/p-1]} \mathrm{N}_e(W_e(p,1)) \Phi_\tau(2)^{-\gamma}.$$

Nous démontrons le théorème suivant:

Théorème 3.2.4. *On a la relation suivante:*

$$h_e(p) = h^-(K_e) \quad si \quad e = 2^d, d \geq 1.$$

Pour simplifier les notations, on pose $X_{K_e} = X_e$, $w_{K_e} = w_e$, et $\mathcal{Q}_{K_e} = \mathcal{Q}_e$.

Lemme 3.2.5. *On a $X_e =< \chi_e >$ où χ_e est le caractère de C_p défini par*

$$\chi(k) = \chi_e(k) = \begin{cases} \alpha^{Ind_g k}, & si\ p \nmid k, \\ 0, & si\ p \mid k. \end{cases}$$

Démonstration.

Il est facile de vérifier que

$$\mathrm{Gal}(C_p/K_e) =< \sigma^e > .$$

D'autre part

$$\chi_e(\sigma^e) = \chi_e(g^e) = \alpha^e = 1.$$

Donc χ_e opère trivialement sur $\mathrm{Gal}(C_p/K_e)$, par suite $\chi_e \in X_e$ (cf. section 2.1.4). Comme χ_e est d'ordre e et que

$$\mid X_e \mid = \mid \mathrm{Gal}(K_e/\mathbb{Q}) \mid = e,$$

alors $X_e = < \chi_e >$.

Remarque. On peut vérifier que

$$\begin{aligned} K_e &= \mathbb{Q}(Tr_{\mathbb{Q}(\zeta_p)/K_e}(\zeta_p)) \\ &= \mathbb{Q}(\zeta_p + \sigma^e(\zeta_p) + \ldots + \sigma^{e(f-1)}(\zeta_p)) \\ &= \mathbb{Q}(\zeta_p + \zeta_p^{g^e} + \ldots + \zeta_p^{g^{e(f-1)}}). \end{aligned}$$

Lemme 3.2.6. *Une extension cyclique imaginaire de degré une puissance de 2, ne peut contenir un sous-corps imaginaire propre.*

Démonstration.
Soit L une telle extension; alors les sous-corps de L sont emboîtés, c'est-à-dire l'un est inclus dans l'autre. Comme L est imaginaire, le sous-corps réel maximal L^+ est tel que $[L : L^+] = 2$. Donc tous les sous-corps propres de L sont inclus dans L^+, ils sont donc réels.

Démonstration du théorème 3.2.4
On a $\mathcal{Q}_e = 1$, $w_e = 2$ ou $2p$. Le caractère χ_e est impair, en effet: comme

$$g^{p-1/2} \equiv -1 \pmod{p}$$

alors

$$\chi_e(-1) = \alpha^{p-1/2} = (-1)^f = -1$$

car f est impair. Montrons que Y_e^- est réduit à un élément. Soit X un sous-groupe de X_e et K le sous-corps associé à X alors d'après la proposition 3.1.4 , $K \subset K_e$. Or K_e est une extension cyclique imaginaire de degré une puissance de 2, le lemme 3.2.6, implique que K est réel ou $K = K_e$. Par conséquent chaque sous-groupe cyclique propre X de X_e est un groupe de

caractères pairs. L'unique sous-groupe cyclique de X_e dont le générateur est impair est X_e. Un représentant de ce groupe (lemme 3.2.5) est χ_e. D'où $Y_e{}^- = \{\chi_e\}$. On a

$$h^-(K_e) = \begin{cases} 2\mathrm{N}_e\left(\frac{-1}{2}B_{1,\chi_e}\right), & \text{si } e \neq p-1, \\ 2p\mathrm{N}_e\left(\frac{-1}{2}B_{1,\chi_e}\right), & \text{si } e = p-1 = 2^d. \end{cases}$$

Remarquons que

$$B_{1,\chi_e} = \frac{1}{p}\sum_{1\leq a\leq p/2}\chi_e(a)a = \frac{1}{p}M_e(p).$$

D'après la section 2.4. lemme 2.4.3, on a

$$B_{1,\chi_e} = -\frac{1}{2-\bar{\chi_e}(2)}m_e(p).$$

On a

$$\begin{aligned} h_e(p) &= p^{[\frac{e}{p-1}]}\mathrm{N}_e(W_e(p,1))\Phi_\tau(2)^{-\gamma} \\ &= p^{[\frac{e}{p-1}]}2^{-J(e)}\mathrm{N}_e(m_e(p))\Phi_\tau(2)^{-\gamma} \qquad \text{(lemme 2.4.6)} \\ &= p^{[\frac{e}{p-1}]}2^{-J(e)}(-1)^{\phi(e)}\mathrm{N}_e(2-\bar{\chi_e}(2))\mathrm{N}_e(B_{1,\chi_e})\Phi_\tau(2)^{-\gamma} \\ &= p^{[\frac{e}{p-1}]}2^{-J(e)}(-1)^{\phi(e)}\Phi_\tau(2)^{\gamma}\mathrm{N}_e(B_{1,\chi_e})\Phi_\tau(2)^{-\gamma} \qquad \text{(lemme 2.4.2)} \\ &= p^{[\frac{e}{p-1}]}2^{-J(e)}(-1)^{\phi(e)}\mathrm{N}_e(B_{1,\chi_e}). \end{aligned}$$

Premier cas: Si $p-1 = e = 2^d$, alors $K_e = C_p$, et $J(e) = \phi(e) - 1$ (cf. lemme 2.4.6) on a

$$\begin{aligned} h_e &= p2^{-J(e)}(-1)^{\phi(e)}\mathrm{N}_e(B_{1,\chi_e}) \\ &= p2^{-J(e)}\mathrm{N}_e(-B_{1,\chi_e}) \\ &= p\frac{1}{2^{\phi(e)-1)}}\mathrm{N}_e(-B_{1,\chi_e}) \\ &= 2p\mathrm{N}_e(\frac{-1}{2}B_{1,\chi_e}) \\ &= h^-(C_p). \end{aligned}$$

Deuxième cas: Si $p-1 \neq e$ alors

$$\begin{aligned} h_e &= 2^{-J(e)}(-1)^{\phi(e)}\mathrm{N}_e(B_{1,\chi_e}) \\ &= \frac{1}{2^{\phi(e)-1}}\mathrm{N}_e(-B_{1,\chi_e}) \\ &= 2\mathrm{N}_e(\frac{-1}{2}B_{1,\chi_e}) \\ &= h^-(K_e). \end{aligned}$$

3.2.3 Exemple numérique

Considérons un exemple simple: $p = 13$. Alors $e \in \{4, 12\}$, $g = 2$, $\mathrm{Ind}_g(2) = 1$. Pour $e = 4$, $\alpha = e^{2i\pi/4} = i$ et on a

$$\tau = \frac{4}{(4,1)} = 4, \quad \Phi_4(X) = X^2 + 1, \quad \Phi_4(2) = 5, \quad \gamma = \frac{\phi(e)}{\phi(\tau)} = \frac{\phi(4)}{\phi(4)} = 1$$

et

$$\epsilon_0 = 1, \epsilon_1 = 1, \epsilon_2 = (4 \bmod 13 < p/2) = 1, \epsilon_3 = (8 \bmod 13 < p/2) = 0,$$

$$\epsilon_4 = (16 \bmod 13 < p/2) = 1, \epsilon_5 = (32 \bmod 13 < p/2) = 1, \epsilon_6 = (64 \bmod 13 = 12 < 7) = 0.$$

Donc

$$W_4 = \sum_{n=1}^{6}(\epsilon_n - \epsilon_{n-1})\alpha^n = -i^3 + i^4 - i^6 = 2 + i,$$

d'où

$$\mathrm{N}_4(W_4) = \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(2 + i) = 5.$$

Par suite on a

$$h_4 = \mathrm{N}_4(W_4) \times \Phi_4(2)^{-1} = 5 \times \frac{1}{5} = 1.$$

Ici $K_4 = \mathbb{Q}(\zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9)$ (cf. remarque) et on a

$$h^-(K_4) = h_4 = 1.$$

On trouvera dans l'annexe I un programme donnant d'autres exemples.

3.3 Majoration de $h^-(K_p)$

On notera dans cette section K_p le sous-corps maximal de $\mathbb{Q}(\zeta_p)$ de degré une puissance de 2. Le but de cette section est de majorer le nombre de classes relatif $h^-(K_p)$ en fonction de p et de la valuation 2-adique de $p-1$. Pour cela on a besoin des deux lemmes suivants :

Lemme 3.3.1. *(voir [16] ou [27])*
a) Le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$, $p \equiv 3 \pmod 4$, satisfait l'inégalité

$$h(\sqrt{-p}) < \frac{\sqrt{p}}{2\pi}(\log p + 2 + \gamma - \log \pi).$$

b) Soient N un corps imaginaire de degré $2n \geq 2$, w_N le nombre de racines de l'unité dans N, h_N^- son nombre de classes relatif et Q_N l'indice de Hasse ($Q_N \in \{1,2\}$). Soit A_N le quotient des discriminants de N et N^+, le sous-corps réel maximal de N, et $c_1 = (2+\gamma-\log\pi)/(4\pi) = 0.1139\ldots$, γ étant la constante d'Euler. Alors

$$h_N^- \leq Q_N w_N \sqrt{A_N}\Big(\frac{1}{4\pi n}\log A_N + c_1\Big)^n.$$

Lemme 3.3.2. *(formule du discriminant de Hasse (cf. [29])*
Soient K un corps de nombres et X_K le groupe de caractères de Dirichlet associé. Alors le discriminant de K est donné par la formule

$$d(K) = (-1)^{r_2} \prod_{\chi \in X_K} f_\chi,$$

où $2r_2$ est le nombre des $\mathbb{Q}$-isomorphismes complexes de K et f_χ le conducteur du caractère χ.

A l'aide de ces deux lemmes nous démontrons le résultat suivant :

Proposition 3.3.3. *Soit $t = v_2(p-1)$.*
a) Si $K_p = \mathbb{Q}(\zeta_p)$ alors

$$h^-(K_p) \leq 2p^{2^{t-2}+1}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}.$$

b) Si $K_p \neq \mathbb{Q}(\zeta_p)$ alors

$$h^-(K_p) \leq 2p^{2^{t-2}}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}.$$

De plus cette inégalité est stricte dans le cas où $t = 1$.

Démonstration.
Appliquons le premier lemme au corps $N = K_p$, $n = 2^{t-1}$, et $Q_p = 1$ (d'après le lemme 3.2.1). Rappelons que (chapitre 1, p. 14)

$$w_p = \begin{cases} 2, & \text{si} \quad K_p \neq \mathbb{Q}(\zeta_p), \\ 2p, & \text{si} \quad K_p = \mathbb{Q}(\zeta_p). \end{cases}$$

Premier cas : $K_p \neq \mathbb{Q}(\zeta_p)$.
Tout caractère non principal de K_p est de conducteur p. Comme le caractère principal est de conducteur égal à 1, il vient donc d'après la formule de discriminant de Hasse (lemme 3.3.2) que

$$d_{K_p} = (-1)^{r_2}\prod_{\chi\in X_{K_p}} f_\chi = p^{2^t-1} \qquad (r_2 \text{ est pair}),$$

et

$$d_{K_p^+} = \prod_{\chi(-1)=1} f_\chi = p^{2^{t-1}-1} \qquad (r_2 = 0);$$

d'où $A_p = \frac{d_{K_p}}{d_{K_p^+}} = p^{2^{t-1}}$. Par suite on a

$$h^-_{K_p} \leq Q_p w_p \sqrt{A_p}\Big(\frac{1}{4\pi\cdot 2^{t-1}}\log A_p + c_1\Big)^{2^{t-1}},$$

d'où

$$h^-_{K_p} \leq 2p^{2^{t-2}}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}.$$

Si $t = 1$ c'est-à-dire $p \equiv 3 \pmod 4$, cette inégalité devient :

$$h(\sqrt{-p}) \leq 2\sqrt{p}\Big(\frac{1}{4\pi}\log p + c_1\Big),$$

or $c_1 = (2 + \gamma - \log\pi)/(4\pi)$; donc

$$h(\sqrt{-p}) \leq \frac{\sqrt{p}}{2\pi}\Big(\log p + 2 + \gamma - \log\pi\Big).$$

Mais cette inégalité est stricte d'après a) du lemme 3.3.1.
Deuxième cas : $K_p = \mathbb{Q}(\zeta_p)$.
Dans ce cas $w_p = 2p$, et en suivant la même démarche on obtient l'inégalité

$$h^-_{K_p} \leq 2p^{2^{t-2}+1}\Big(\frac{1}{4\pi}\log p + c_1\Big)^{2^{t-1}}. \qquad \square$$

Remarques.
1) Quelquefois h^- est vraiment très grand. Pour en avoir une idée M. Mignotte et Y. Roy (voir [20]) ont calculé[2] le nombre de classes relatif $h^-(K_p)$ de K_p pour $p = 3 \times 2^{18} + 1 = 786433$ (degré de K_p est égal 2^{18}), le nombre $h^-(K_p)$ a plus de 285000 chiffres !

2) T. Lepistö dans [14] a donné une majoration de nombres de classes relatif $h^-(p)$ de corps $\mathbb{Q}(\zeta_p)$, plus précisément il a montré que :

$$\log\Big(\frac{h^-(p)}{G(p)}\Big) \leq 5\log\log p + 15.49 + \frac{4.66}{\log p};$$

où $G(p)$ est la fonction introduite par Kummer : $G(p) = 2p\Big(\frac{p}{4\pi^2}\Big)^{\frac{p-1}{4}}$. Lepistö a donné également une minoration explicite de $h^-(p)$, montrant ainsi que la majoration précédente ne peut être substantiellement améliorée.

2. La durée de ce calcul est inférieure à 200 minutes.

Chapitre 4

Décomposition d'un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ dans les sous-extensions de $\mathbb{Q}(\zeta_{2^n})$, $n, m \geq 2$.

Introduction

On se propose, dans un premier temps, de montrer qu'un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-1} ($l = \min(m, n)$) premiers distincts du corps cyclotomique $\mathbb{Q}(\zeta_{2^n})$, pour tout $n, m \geq 2$, et dans un deuxième temps on détermine la décomposition d'un tel nombre premier dans les sous-extensions de $\mathbb{Q}(\zeta_{2^n})$. Ensuite des exemples sont traités à l'aide de GP Pari [1]. Nous avons aussi étudié dans ce chapitre, les facteurs de $h^-(K_p)$ (qu'on notera simplement h_p^-) de type $q \equiv 2^m + 1 \pmod{2^{m+1}}$, $m \geq 1$.

4.1 Rappels et notations.

Nous rappelons ici trois théorèmes essentiels. Le premier, dû à Dedekind, montre un lien entre la factorisation d'un idéal premier et celle, modulo cet idéal premier, d'un polynôme irreductible; il s'énonce comme suit (cf. [10]):

Théorème 4.1.1. *(Dedekind). Soient A un anneau de Dedekind et K*

son corps de fractions. Soient E une extension finie séparable de K et B la clôture intégrale de A dans E. Supposons que $B = A[\alpha]$ pour un certain élément α de E. Soient $F(X) = Irr(\alpha,K)$, et $\mathfrak{p}$ un idéal premier de A. Soient $\bar{F}$ la réduction de F modulo $\mathfrak{p}$ et

$$\bar{F}(X) = \bar{P}_1(X)^{e_1} \dots \bar{P}_r(X)^{e_r}$$

la factorisation de $\bar{F}$ dans $(A/\mathfrak{p})[X]$. Alors

$$\mathfrak{p} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

est la factorisation de $\mathfrak{p}$ dans B et e_i est l'indice de ramification de $\mathfrak{B}$ sur $\mathfrak{p}$ et où

$$\mathfrak{B}_i = \mathfrak{p}B + P_i(\alpha)B = (\mathfrak{p}, P_i(\alpha)),$$

avec $P_i \in A[X]$ unitaire dont la réduction modulo $\mathfrak{p}$ est $\bar{P}_i$.

Le deuxième théorème donne une condition nécessaire et suffisante de la non-ramification dans un produit d'extensions (cf. [7], Satz 42, page 59):

Théorème 4.1.2. *Soient L et K deux extensions algébriques de degré fini d'un corps k. Un idéal premier $\mathfrak{p}$ de k ne se ramifie pas (resp. se décompose complètement) dans l'extension composée LK si et seulement si il ne se ramifie pas (resp. se décompose complètement) à la fois dans L et dans K.*

Le troisième théorème porte sur la décomposition des nombres premiers dans les corps cyclotomiques (cf. [29]) :

Théorème 4.1.3. *Soit $m \geq 1$ entier et soit q un nombre premier. Supposons que $q \nmid m$ et soit f le plus petit entier positif tel que $q^f \equiv 1 \pmod{m}$, alors q se décompose en $g = \phi(m)/f$ idéaux premiers distincts de $\mathbb{Q}(\zeta_m)$ dont chacun est de degré résiduel égal à f. En particulier, q se décompose complètement si et seulement si $q \equiv 1 \pmod{m}$.*

4.2 Sous-corps de $\mathbb{Q}(\zeta_{2^n})$, $n \geq 2$

Dans cette section nous déterminons les sous-corps du corps cyclotomique $\mathbb{Q}(\zeta_{2^n})$, $n \geq 2$. On note $L_n = \mathbb{Q}(\zeta_{2^n})$. Le cas $n = 2$ se réduit à $L_2 = \mathbb{Q}(i)$

dont les sous-corps sont triviaux. Nous supposerons alors que $n \geq 3$. On a:

Théorème 4.2.1. *Les sous-corps de L_n de degré relatif égal à 2 sont K_{n-1}, L_{n-1} et K'_{n-1}, ayant posé $K_{n-1} = \mathbb{Q}(\theta_n)$ où $\theta_n = \zeta_{2^n} + \zeta_{2^n}^{-1}$, et $K'_{n-1} = \mathbb{Q}(\theta'_n)$ où $\theta'_n = \zeta_{2^n} - \zeta_{2^n}^{-1}$.*

Démonstration.
On note $G(m)$ le groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^*$ pour $m > 1$ entier. On sait que le groupe de Galois du corps cyclotomique $L_n = \mathbb{Q}(e^{2i\pi/m})$ est isomorphe au groupe $G(m)$, où l'action de $a \in G(m)$ est $\zeta \mapsto \zeta^a$, ayant posé $\zeta = e^{2i\pi/m}$. En particulier, le groupe de Galois du corps L_n qui nous intéresse est isomorphe à $G_n := G(2^n)$. La structure de ce groupe (rappelons que l'on suppose $n \geq 3$) est bien connue: le groupe G_n est représenté par les éléments $\pm 5^k$, pour $0 \leq k < 2^{n-2}$, il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ (voir [21]), il n'est donc pas cyclique. Par la théorie de Galois, on sait que les sous-corps de L_n correspondent aux sous-groupes de G_n. En particulier, les sous-corps $\mathcal{K}$ de L_n tels que $[L_n : \mathcal{K}] = 2$ correspondent aux éléments d'ordre deux de G_n. Il est clair que les éléments d'ordre deux de G_n admettent pour représentants

$$\alpha_1 = -1,\ \alpha_2 = 5^{2^{n-3}} \text{ et } \alpha_3 = -5^{2^{n-3}},$$

notons $\mathcal{K}_j$ le sous-corps de L_n laissé invariant par le groupe $H_j = \{1, \alpha_j\}$ pour $j = 1$, 2 et 3. Pour chaque j, le corps $\mathcal{K}_j$ est une extension galoisienne de $\mathbb{Q}$ de groupe de Galois G_n/H_j.
Etudions maintenant plus en détail chacun des corps $\mathcal{K}_j$ et notons ψ_j la surjection canonique

$$G_n \to G_n/H_j.$$

Notons que le groupe G_n/H_j est d'ordre 2^{n-2}. Posons $\zeta_n = e^{2i\pi/2^n}$ pour simplifier les notations.
Pour $j = 1$, l'élément $\psi_j(5)$ est d'ordre 2^{n-2} dans G_n/H_1, ce groupe est donc cyclique. Le corps $\mathcal{K}_1$ est égal à $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = K_n$, donc

$$\mathcal{K}_1 = \mathbb{Q}(\cos(2\pi/2^n))$$

est le sous-corps réel maximal de L_n et il est cyclique.
Pour $j = 2$, l'élément $\psi_j(5)$ est d'ordre 2^{n-3} dans G_n/H_j, ce groupe n'est

donc pas cyclique pour $n > 3$. Le corps $\mathcal{K}_2$ est égal à $\mathbb{Q}(\zeta_n^2)$, donc

$$\mathcal{K}_2 = L_{n-1}.$$

Pour $j = 3$, l'élément $\beta = \psi_j(5)$ vérifie $\beta^{2^{n-3}} = -1$, il est donc d'ordre 2^{n-2} dans G_n/H_3, ce qui montre que ce groupe est cyclique. Le corps $\mathcal{K}_3$ est égal à $\mathbb{Q}(\zeta_n - \zeta_n^{-1})$, donc

$$\mathcal{K}_3 = \mathbb{Q}(i\sin(2\pi/2^n)) = K'_n$$

est un sous-corps cyclique de L_n. □

Remarque.

1) Le sous-corps K'_{n-1} ne peut contenir un sous-corps imaginaire propre car K'_{n-1} est une extension cyclique imaginaire de degré une puissance de 2 (cf. lemme 3.2.6).

2) $L_n = \mathbb{Q}(i, \theta_n) = \mathbb{Q}(i, \theta'_n)$. En effet, on a :

$$[L_n : \mathbb{Q}(\theta_n)] = [L_n : \mathbb{Q}(i, \theta_n)][\mathbb{Q}(i, \theta_n) : \mathbb{Q}(\theta_n)] = 2.$$

Or

$$\mathbb{Q}(\theta_n) \subsetneq \mathbb{Q}(i, \theta_n) \subset L_n,$$

donc

$$[\mathbb{Q}(i, \theta_n) : \mathbb{Q}(\theta_n)] = 2,$$

par suite $L_n = \mathbb{Q}(i, \theta_n)$. De même

$$\mathbb{Q}(i) \subsetneq \mathbb{Q}(i, \theta'_n) \subset L_n,$$

on en déduit que $L_n = \mathbb{Q}(i, \theta'_n)$. □

Pour la commodité d'écriture, on pose $L_1 = K_1 = \mathbb{Q}$ et $K'_1 = \mathbb{Q}(i) = L_2$. Avec les notations du théorème 4.2.1, on vérifie aisément que :

$$\theta_n = \sqrt{2 + \theta_{n-1}} \qquad \text{et} \qquad \theta'_n = i\sqrt{2 - \theta_{n-1}}.$$

Avec ces deux relations de récurrence on déduit que

$$K_{n-2} \subset K_{n-1} \cap K_{n-1}^{'}, \text{ pour tout } n \geq 3;$$

par ailleurs on a :

$$[K_{n-1} : K_{n-2}] = 2 = [K_{n-1} : K_{n-1} \cap K_{n-1}^{'}][K_{n-1} \cap K_{n-1}^{'} : K_{n-2}].$$

Si $[K_{n-1} : K_{n-1} \cap K_{n-1}^{'}] = 1$ alors $K_{n-1} = K_{n-1} \cap K_{n-1}^{'}$, implique

$$K_{n-1} \subset K_{n-1}^{'},$$

comme

$$[L_n : K_{n-1}] = [L_n : K_{n-1}^{'}] = 2,$$

alors

$$K_{n-1} = K_{n-1}^{'},$$

ce qui est absurde. Donc

$$[K_{n-1} \cap K_{n-1}^{'} : K_{n-2}] = 1,$$

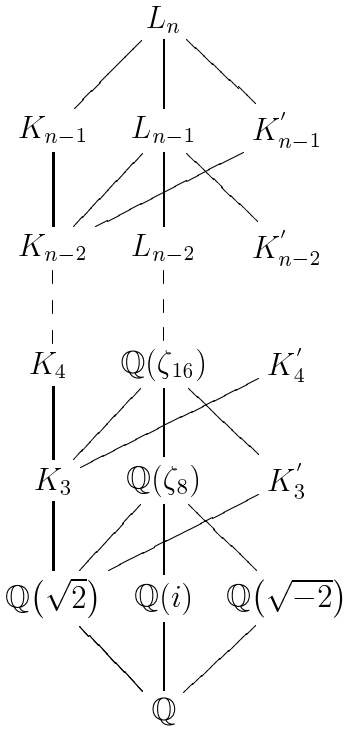
par suite

$$K_{n-2} = K_{n-1} \cap K_{n-1}^{'}.$$

Les autres sous-corps vérifient:

$$K_{j-1} = K_j \cap K_j^{'} \quad (2 \leq j < n) \quad \text{et} \quad L_{j-1} \subset L_j, \quad (2 \leq j \leq n).$$

Nous traduisons ces faits par le diagramme suivant:



La structure précédente du "treillis" des sous-corps de L_n permet de déterminer les corps de nombres abéliens de conducteur 2^n, $n \geq 3$. Plus précisément on a le corollaire suivant :

Corollaire 4.2.2. *Les corps de nombres abéliens de conducteur* 2^n, $n \geq 3$, *sont* $\mathbb{Q}(\zeta_{2^n})$, $\mathbb{Q}(\cos(\pi/2^{n-1}))$ *et* $\mathbb{Q}(i\sin(\pi/2^{n-1}))$.

Démonstration. Soit K un corps de nombres abélien de conducteur 2^n, $n \geq 3$. Donc n est le plus petit entier tel que $K \subset \mathbb{Q}(\zeta_{2^n})$. Par suite K est un sous-corps de $\mathbb{Q}(\zeta_{2^n})$. Notons que le corps $\mathbb{Q}(\zeta_{2^n})$ est de conducteur 2^n et pour tout $m < n, K \neq \mathbb{Q}(\zeta_{2^m})$ car le conducteur de K est égal 2^n. Supposons que $K \neq \mathbb{Q}(\zeta_{2^n})$; la structure précédente montre qu'il existe un entier $n_0 \leq n$ tel que $K = K_{n_0-1}$ ou $K = K'_{n_0-1}$. Supposons $K = K_{n_0-1}$; comme $K = K_{n_0-1} \subset \mathbb{Q}(\zeta_{2^{n_0}})$; ceci entraîne que $n \leq n_0$ puisque 2^n est le conducteur de K. D'où $n = n_0$ et $K = K_{n_-1}$. Le même raisonnement se fait si $K = K'_{n_0-1}$. Ce qui démontre le corollaire. □

Introduisons la définition suivante :

Définition 4.2.3. *Les sous-corps de L_n de la forme $L_j, 1 \leqslant j \leqslant n$ sont dits de type I; et les sous-corps de la forme K_j ou $K_j^{'}$ $(2 \leqslant j < n)$ sont dits de type II.*

4.3 Décomposition dans les sous-corps de type I

Soit $n,\ m \geq 2$. Posons $l = \min(m, n)$. Nous démontrons le théorème suivant :

Théorème 4.3.1. *Un nombre premier $q \equiv 1+2^m \pmod{2^{m+1}}$ se décompose en 2^{l-1} premiers distincts dans le corps cyclotomique $L_n = \mathbb{Q}(\zeta_{2^n})$.*

Pour la démonstration du théorème 4.3.1 on a besoin du lemme suivant :

Lemme 4.3.2. *Soit $n > m$. Si $q \equiv 1 + 2^m \pmod{2^{m+1}}$ alors $q^{2^{n-m}} \equiv 1 \pmod{2^n}$ et $q^{2^{n-m-1}} \equiv 1 + 2^{n-1} \pmod{2^n}$.*

Démonstration du lemme

La preuve se fait par récurrence sur n.

Pour $n = m + 1$, $q \equiv 1 + 2^m \pmod{2^{m+1}} \Rightarrow q \equiv 1 \pmod{2^m} \Rightarrow q^2 \equiv 1 \pmod{2^{m+1}} \Rightarrow q^2 \equiv 1 \pmod{2^n}$ et $q \equiv 1 + 2^m \pmod{2^{m+1}}$.

Supposons que le lemme est vrai pour $n \geq m + 1$, montrons qu'il l'est pour $n + 1$.

On a

$$q^{2^{n-m}} \equiv 1 \pmod{2^n} \Longrightarrow (q^{2^{n-m}})^2 \equiv 1 \pmod{2^{n+1}},$$

d'où $q^{2^{n+1-m}} \equiv 1 \pmod{2^{n+1}}$. D'autre part, par hypothèse de récurrence,

$$\begin{aligned} q^{2^{n-m-1}} &\equiv 1 + 2^{n-1} \pmod{2^n} \Longrightarrow 2^n \mid (q^{2^{n-m-1}} - 2^{n-1} - 1), \\ 2^{n+1} &\mid (q^{2^{n-m-1}} - 2^{n-1} - 1)(q^{2^{n-m-1}} + 2^{n-1} + 1), \\ 2^{n+1} &\mid q^{2^{n-m}} - (2^{n-1} + 1)^2, \\ 2^{n+1} &\mid q^{2^{n-m}} - 2^n - 1 - 2^{2(n-1)}. \end{aligned}$$

Comme $2^{n+1} \mid 2^{2(n-1)}$ pour $n \geq 3$, alors $2^{n+1} \mid q^{2^{n-m}} - 2^n - 1$. Par conséquent $q^{2^{n-m}} \equiv 1 + 2^n \pmod{2^{n+1}}$. □

Démonstration du théorème 4.3.1.
Si $n \leq m$, alors $q \equiv 1 + 2^m \pmod{2^{m+1}} \Rightarrow q \equiv 1 \pmod{2^n}$; donc q se décompose complètement dans le corps cyclotomique L_n [3, théorème 2.13 page 14] c'est-à-dire en $\phi(2^n) = 2^{n-1}$ idéaux premiers distincts.
Si $n > m$, alors le lemme 3.3.2 entraîne que l'entier $f_{n,m} = 2^{n-m}$ est le plus petit entier positif tel que $q^{f_{n,m}} \equiv 1 \pmod{2^n}$; et par [3, théorème 2.13 page 14], q se décompose en $\phi(2^n)/f_{n,m}$ premiers distincts, soit donc $2^{n-1}/2^{n-m}$ $=2^{m-1}$ idéaux premiers distincts. Ce qui démontre le théorème. □

Remarque. Le théorème 4.3.1 donne la décomposition dans les sous-corps de L_n de type I, car si le sous-corps en question est de la forme L_j avec $j < n$, alors on applique le théorème 4.3.1 à L_j; dans ce cas, un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l_j-1} premiers distincts dans le corps cyclotomique L_j, où $l_j = \min(j, m)$. □

Le théorème 4.3.1 montre en particulier que pour déterminer la décomposition d'un nombre premier $q \equiv 1+2^m \pmod{2^{m+1}}$ dans L_n, $n \geq m$, il suffit de regarder cette décomposition dans le corps cyclotomique L_m. Les idéaux premiers de $\mathbb{Z}[\zeta_{2^n}]$ au-dessus de q se déduisent alors par extension des idéaux premiers de $\mathbb{Z}[\zeta_{2^m}]$ au-dessus de q.

Pour illustrer ces remarques, nous donnons dans la suite des applications et des exemples.

4.4 Applications et exemples

Notons $\Phi_n(X) = X^{2^{n-1}} + 1 = \mathrm{Irr}(\zeta_{2^n}, \mathbb{Q})$. Considérons le cas où $m = 3$; d'après le théorème 4.3.1, un premier $q \equiv 9 \pmod{16}$ se décompose en quatre idéaux premiers distincts dans $\mathbb{Q}(\zeta_{2^n})$ pour tout $n \geq 3$. Nous allons déterminer explicitement cette décomposition. Pour ce faire, énonçons le lemme suivant:

Lemme 4.4.1. *Soit $q \equiv 9 \pmod{16}$. Alors il existe $a, b \in \mathbb{Z}$ tels que*

$$a^4 \equiv -1 \pmod{q} \quad et \quad a^2 \equiv -b^2 \pmod{q}.$$

Démonstration. Comme $q \equiv 9 \pmod{16}$, 8 divise $q-1$. Or $(\mathbb{Z}/q\mathbb{Z})^*$ est cyclique d'ordre $q-1$, il existe donc $a \in \mathbb{Z}$ d'ordre 8 modulo q. On a $a^8 - 1 \equiv 0 \pmod{q}$, ce qui implique

$$(a^4-1)(a^4+1) \equiv 0 \pmod{q};$$

on en déduit que

$$a^4 \equiv -1 \pmod{q}.$$

Posons $b = a^3$ alors

$$a^2 \equiv -b^2 \pmod{q}. \qquad \square$$

On utilise le lemme précédent pour factoriser, modulo q, le polynôme cyclotomique $\Phi_n(X)$, on a:

$$\Phi_n(X) = X^{2^{n-1}} + 1 \equiv X^{2^{n-1}} - a^4 \pmod{q}$$

$$= (X^{2^{n-2}} - a^2)(X^{2^{n-2}} + a^2)$$

$$\equiv (X^{2^{n-2}} - a^2)(X^{2^{n-2}} - b^2) \pmod{q};$$

donc

$$\Phi_n(X) \equiv (X^{2^{n-3}} - a)(X^{2^{n-3}} + a)(X^{2^{n-3}} - b)(X^{2^{n-3}} + b) \pmod{q},$$

d'où la décomposition dans $\mathbb{Z}[\zeta_{2^n}]$ pour $n \geq 3$ ([29], Proposition 2.14):

$$(q) = (q, \zeta_8 - a)(q, \zeta_8 + a)(q, \zeta_8 - b)(q, \zeta_8 + b).$$

Par exemple, pour $q = 41, 73$ et 89, on a dans $\mathbb{Z}[\zeta_{2^n}]$ pour $n \geq 3$:

$$(41) = (41, \zeta_8 - 3)(41, \zeta_8 + 3)(41, \zeta_8 - 14)(41, \zeta_8 + 14),$$

$$(73) = (73, \zeta_8 - 10)(73, \zeta_8 + 10)(73, \zeta_8 - 22)(73, \zeta_8 + 22),$$

$$(89) = (89, \zeta_8 - 12)(89, \zeta_8 + 12)(89, \zeta_8 - 37)(89, \zeta_8 + 37).$$

- Autre exemple: cas $m = 4$.

À l'aide de GP-Pari [1], on obtient :

$$(17) = (17, i+4)(17, i+13) \text{ dans } \mathbb{Z}[i],$$
$$(17) = (17, \zeta_8+2)(17, \zeta_8+8)(17, \zeta_8+9)(17, \zeta_8+15) \text{ dans } \mathbb{Z}[\zeta_8],$$
et
$$(17) = (17, \zeta_{16}+3)(17, \zeta_{16}+5)(17, \zeta_{16}+6)(17, \zeta_{16}+7)(17, \zeta_{16}+10)$$
$$(17, \zeta_{16}+11)(17, \zeta_{16}+12)(17, \zeta_{16}+14)$$

dans $\mathbb{Z}[\zeta_{2^n}]$ pour $n \geq 4$.

4.5 Décomposition dans les sous-corps de type II

Soient $n \geq 3$, $m \geq 2$ et $l = \min(m, n)$. Avec les notations du théorème 4.2.1 de la section 4.2, on a le théorème suivant:

Théorème 4.5.1. *Un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-2} premiers distincts dans K_{n-1} ou K'_{n-1}.*

Démonstration.
1er cas: $n > m$.
Considérons le corps L_n, $n \geq 3$. Soit g_n le nombre des idéaux premiers de K_{n-1} qui figurent dans la décomposition de q. Il s'agit de montrer que $g_n = 2^{m-2}$. On désigne par $f_{K/\mathbb{Q}}$ le degré résiduel de q dans l'extension $K/\mathbb{Q}$.
On sait que

$$f_{K_{n-1}/\mathbb{Q}} \cdot g_n = [K_{n-1} : \mathbb{Q}] = 2^{n-2},$$

or

$$f_{n,m} = f_{L_n/K_{n-1}} \cdot f_{K_{n-1}/\mathbb{Q}} = 2^{n-m},$$

et comme

$$f_{L_n/K_{n-1}} \leqslant [L_n : K_{n-1}] = 2,$$

alors

$$f_{L_n/K_{n-1}} = 1 \text{ ou } 2;$$

ceci entraîne que

$$f_{K_{n-1}/\mathbb{Q}} = 2^{n-m} \text{ ou } f_{K_{n-1}/\mathbb{Q}} = 2^{n-m-1}.$$

Par suite $g_n = 2^{m-2}$ ou $g_n = 2^{m-1}$.
Montrons par récurrence sur $n > m$ que $g_n = 2^{m-2}$.
Pour $n = m+1$, si $g_{m+1} = 2^{m-1}$ alors comme $[K_m : \mathbb{Q}] = 2^{m-1}$, l'entier q se décompose complètement sur K_m. Or q se décompose complètement sur $\mathbb{Q}(i)$ (car $q \equiv 1 \pmod 4$ pour $m \geq 2$). Donc d'après Hasse ([7], Satz 42, page 59), q se décompose complètement sur $L_{m+1} = \mathbb{Q}(i, \theta_{m+1})$, ce qui est absurde par le théorème 3.3.1. Donc la propriété est vraie pour $n = m+1$.
Supposons qu'elle est vraie pour $n > m$ et montrons qu'elle est vraie pour $n+1$; c'est-à-dire que $g_{n+1} = 2^{m-2}$. L'hypothèse de récurrence entraîne que $g_n = 2^{m-2}$, $f_{K_{n-1}/\mathbb{Q}} = 2^{n-m}$ et $f_{L_n/K_{n-1}} = 1$.

Soit $\tilde{q}$ un idéal premier de K_{n-1} au-dessus de q, par hypothèse de récurrence, $\tilde{q}$ se décompose en deux idéaux premiers distincts de L_n. Si $\tilde{q}$ se décompose dans K_n alors par Hasse ([7], Satz 42, page 59), $\tilde{q}$ se décompose complètement dans $L_{n+1} = K_n L_n$; ce qui est absurde car $f_{L_{n+1}/K_{n-1}} = f_{n+1,m}/f_{K_{n-1}/\mathbb{Q}} = 2^{n+1-m}/2^{n-m} = 2$. Donc $\tilde{q}$ est inerte dans K_n; par suite $f_{K_n/K_{n-1}} = 2$, ceci entraîne que $f_{L_{n+1}/K_n} = 1$; d'où $g_{n+1} = 2^{m-2}$. Pour le sous-corps K'_{n-1}, on suit les mêmes étapes en remarquant que $L_{m+1} = \mathbb{Q}(i, \theta'_{m+1})$ et $L_{n+1} = K'_n L_n$.
2ème cas : $m \geq n$.
D'après le théorème 4.3.1, $f_{n,m} = 1$, par suite $f_{K_{n-1}/\mathbb{Q}} = 1$; par conséquent $g_n = 2^{n-2}$. Le même raisonnement se fait pour K'_{n-1} . □

Remarque. Le théorème 4.5.1 donne la décomposition dans les sous-corps de L_n de type II, car si le sous-corps en question est de la forme K_j ou K'_j avec $j < n$ on se place dans le corps cyclotomique L_{j+1} de façon que K_j ou K'_j soit de degré relatif égal à 2 et on applique le théorème 4.5.1. Si on pose $l_j = \min(j+1, m)$, alors un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en $2^{l_j - 2}$ premiers distincts dans K_j ou dans K'_j . □

Le théorème 4.5.1 montre en particulier que pour déterminer la décom-

position d'un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ dans K_{n-1} (resp. dans $K_n^{'}$), $n \geq m$, il suffit de regarder cette décomposition dans K_{m-1} (rappelons que $K_{m-1} \subset K_n \cap K_n^{'} = K_{n-1}$). Alors les idéaux premiers de $\mathbb{Z}[\theta_n]$ (resp. de $\mathbb{Z}[\theta_{n+1}^{'}]$) au-dessus de q se déduisent par extension des idéaux premiers de $\mathbb{Z}[\theta_m]$ au-dessus de q.
Pour illustrer ces remarques, considérons le cas $m = 4$; d'après le théorème 3.1, un premier $q \equiv 17 \pmod{32}$ se décompose en quatre idéaux premiers distincts dans le corps $K_3 = \mathbb{Q}(\theta_4) = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Par exemple pour $q = 17, 103$, et 241, on a dans $\mathbb{Z}[\sqrt{2+\sqrt{2}}]$:

$$(17) = (17, \sqrt{2+\sqrt{2}}+5)(17, \sqrt{2+\sqrt{2}}+8)(17, \sqrt{2+\sqrt{2}}+9)(17, \sqrt{2+\sqrt{2}}+12),$$
$$(103) = (103, \sqrt{2+\sqrt{2}}+8)(103, \sqrt{2+\sqrt{2}}+36)(103, \sqrt{2+\sqrt{2}}+77)$$
$$(103, \sqrt{2+\sqrt{2}}+105),$$
$$(241) = (241, \sqrt{2+\sqrt{2}}+54)(241, \sqrt{2+\sqrt{2}}+71)(241, \sqrt{2+\sqrt{2}}+170)$$
$$(241, \sqrt{2+\sqrt{2}}+187);$$

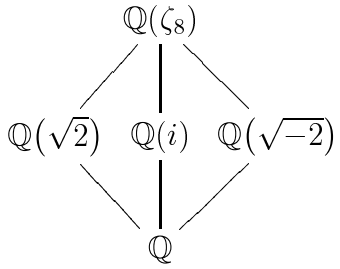
d'où—par extension des idéaux—la décomposition dans $\mathbb{Z}[\theta_n]$ ou dans $\mathbb{Z}[\theta_{n+1}^{'}]$, $n \geq 4$:

$$(17) = (17, \sqrt{2+\sqrt{2}}+5)(17, \sqrt{2+\sqrt{2}}+8)(17, \sqrt{2+\sqrt{2}}+9)(17, \sqrt{2+\sqrt{2}}+12),$$
$$(103) = (103, \sqrt{2+\sqrt{2}}+8)(103, \sqrt{2+\sqrt{2}}+36)(103, \sqrt{2+\sqrt{2}}+77)$$
$$(103, \sqrt{2+\sqrt{2}}+105),$$
$$(241) = (241, \sqrt{2+\sqrt{2}}+54)(241, \sqrt{2+\sqrt{2}}+71)(241, \sqrt{2+\sqrt{2}}+170)$$
$$(241, \sqrt{2+\sqrt{2}}+187).$$

4.5.1 Les facteurs de h_p^- de type $q \equiv 3 \pmod 4$ $(m = 1)$

Posons $t = v_2(p-1)$, la valuation 2-adique de $p-1$.
Nous supposerons que $t \geqslant 3$. Le corps cyclotomique $\mathbb{Q}(\zeta_8)$ contient trois

sous-corps quadratiques à savoir $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$.



Pour $m = 1$, $q \equiv 3 \pmod 4$.
On a, $q \equiv 3 \pmod 4 \Rightarrow q^2 \equiv 1 \pmod 4 \Rightarrow q$ se décompose en $\phi(4)/2$ premiers distincts dans $\mathbb{Q}(i)$ i.e. q reste inerte dans $\mathbb{Q}(i)$. Autrement dit le polynôme $X^2 + 1$ est irréductible modulo q; ce qui revient à dire encore que -1 n'est pas résidu quadratique modulo q.
Le nombre de classes relatif h_p^- de K_p est essentiellement une norme dans l'extension $\mathbb{Q}(i)/\mathbb{Q}$, c'est-à-dire :

$$h^-(K_p) \simeq \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(A + iB) = A^2 + B^2,$$

où $A, B \in \mathbb{Z}$. Les composantes A et B sont calculées à l'aide du programme de Roy (voir Annexe II). On a le résultat suivant:

Proposition 4.5.2. *On a les équivalences suivantes:*

$$q \mid h_p^- \Leftrightarrow q \mid \mathrm{pgcd}(A, B) \Leftrightarrow q^2 \mid h_p^-.$$

Démonstration. On a

$$\begin{aligned} q \mid h_p^- &\Rightarrow q \mid A^2 + B^2 \\ &\Rightarrow A^2 + B^2 \equiv 0 \pmod q \\ &\Rightarrow q \mid A \text{ et } q \mid B, \end{aligned}$$

sinon, supposons par exemble que $q \nmid B$, donc B sera inversible modulo q par suite

$$(A/B)^2 + 1 \equiv 0 \pmod q$$

et donc -1 est résidu quadratique modulo q, contradiction avec ce qui précède. D'où

$$q \mid \mathrm{pgcd}(A, B),$$

par suite

$$q^2 \mid h_p^-.$$

La réciproque est immédiate. □

Du point de vue de la factorisation de h^-, une telle proposition est très importante: le calcul du pgcd de deux entiers est très peu coûteux et on peut donc facilement trouver les facteurs premiers q de h^- qui vérifient

$$q \equiv 3 \pmod 4.$$

Nous donnons deux tables, la première regroupe les valeurs de h_p^-, et sa factorisation en nombre premiers, ainsi que les nombres premiers

$$q \equiv 3 \pmod 4$$

divisant h_p^- (3ème colonne). Ces calculs sont établis à l'aide du programme de Roy.

Table 1.

$p \equiv 9 \pmod{16}$	h_p^-	$q \equiv 3 \pmod 4$
30697	$12058353 = 3^2 \cdot 1339817$	3
30169	$6684849 = 3^4 \cdot 82529$	3
31321	$105633 = 3^2 \cdot 11^2 \cdot 97$	[3, 11]
160313	$20175929 = 19^2 \cdot 55889$	19
170873	$15896169 = 3^4 \cdot 443^2$	[3, 443]
171641	$16762833 = 3^2 \cdot 17 \cdot 331^2$	[3, 331]
175673	$69248593 = 193 \cdot 599^2$	599
178873	$276354361 = 23^2 \cdot 522409$	23
189961	$10560824321 = 19^2 \cdot 41 \cdot 193 \cdot 3697$	19
198377	$95722529 = 7^2 \cdot 17 \cdot 114913$	7
$p \equiv 17 \pmod{32}$	h_p^-	$q \equiv 3 \pmod 4$
8369	$2625703857 = 3^4 \cdot 7^2 \cdot 661553$	[3, 7]
189961	$10560824321 = 19^2 \cdot 41 \cdot 193 \cdot 3697$	19
150193	$220631484849559297 = 47^2 \cdot 30449 \cdot 42209 \cdot 77713$	47
158161	$70099418153313 = 3^4 \cdot 17 \cdot 241 \cdot 211233809$	3
409841	$8678618238916577 = 7^2 \cdot 269761 \cdot 656561393$	7
483953	$569292208504289 = 3^4 \cdot 19373977882769$	3
493169	$14428510446029809 = 433 \cdot 1367^2 \cdot 17831857$	1367
498833	$102497309624738673 = 3^4 \cdot 17^3 \cdot 193 \cdot 1217 \cdot 1096561$	3
499729	$26301183749801489 = 127^2 \cdot 415697 \cdot 3922753$	127
$p \equiv 33 \pmod{64}$	h_p^-	$q \equiv 3 \pmod 4$
167521	$3925679129769278763939594453 77 = 7^4 \cdot 10177 \cdot 165626997985718636033$	7
176609	$4051318023701582762099128505 93 = 31^2 \cdot 449 \cdot 938915713657030135669537 \cdot$	31
198937	$18540729 = 3^2 \cdot 337 \cdot 6113$	3
211681	$1141296921124448560424513000417 = 47^2 \cdot 14369 \cdot 767521 \cdot 215868769 \cdot 217018273$	47
292577	$1858267026448242750643798826272 1 = 47^2 \cdot 7649 \cdot 64577 \cdot 244208737 \cdot 69737870369$	47
293729	$2996271842312167737851939544001 = 31^2 \cdot 257 \cdot 9850039681 \cdot 1231648328870273$	31

La deuxième table regroupe les composantes A et B et leur plus grand commun diviseur qu'on notera tout simplement (A, B).

Table 2.

$p \equiv 9 \pmod{16}$	$[A,\ B]$	(A, B)
30697	[3645,3291]	3
30169	$[927, -3537]$	3^2
31321	$[-429, -165]$	$3 \cdot 11$
160313	[5187,3667]	19
170873	[3987,3987]	$3^2 \cdot 443$
171641	[2979,4965]	$3 \cdot 331$
175673	$[-2995, -11381]$	599
178873	[−4531,23069]	23
189961	[145331,741]	19
198377	[−13797,1043]	7
$p \equiv 17 \pmod{32}$	$[A,\ B]$	(A, B)
8369	$[48195, -54117]$	$3^2 \cdot 7$
189961	[145331,741]	19
150193	$[478268663, -461001145]$	47
158161	$[2476701, -11578635]$	3^2
409841	[−129448627,24500805]	7
483953	[−46185723,31709043]	3^2
493169	[135867497,101965897]	1367
498833	$[-299181861, -339830595]$	$3^2 \cdot 17$
499729	[−134094093,186067573]	127
$p \equiv 33 \pmod{64}$	$[A,\ B]$	(A, B)
167521	$[-782522439274275, -415685527756373]$	7^2
176609	$[795175481746885, -421852531068531]$	31
198937	$[4887, -3633]$	3
211681	[1474224807997803,330537528478595]	47
292577	[−5800060330092909,1877402646276869]	47
293729	$[-208106615130131, -2439105434654971]$	31

4.5.2 Les facteurs de h_p^- de type $q \equiv 5 \pmod 8$ $(m = 2)$

Pour $m = 2$, $q \equiv 5(\pmod 8)$. On a,

$$q \equiv 5 \pmod 8 \Rightarrow \left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = -1,$$

donc 2 n'est pas résidu quadratique modulo q. Autrement dit le polynôme $X^2 - 2$ est irréductible modulo q; par conséquent q est inerte dans le sous corps $\mathbb{Q}(\sqrt{2})$.
Par transitivité de la norme, le nombre de classes relatif $h^-(K_p)$ de K_p s'exprime aussi essentiellement comme une norme dans l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, c'est-à-dire :

$$h_p^- \simeq \mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(C + D\sqrt{2}) = C^2 - 2D^2,$$

où $C, D \in \mathbb{Z}$. On a le résultat suivant:

Proposition 4.5.3. *On a les équivalences suivantes:*

$$q \mid h_p^- \Leftrightarrow q \mid \mathrm{pgcd}(C, D) \Leftrightarrow q^2 \mid h_p^-.$$

Démonstration. On a

$$\begin{aligned} q \mid h_p^- &\Rightarrow q \mid C^2 - 2D^2 \\ &\Rightarrow C^2 - 2D^2 \equiv 0 \pmod q \\ &\Rightarrow q \mid C \text{ et } q \mid D, \end{aligned}$$

sinon, supposons par exemble que $q \nmid D$ donc D sera inversible modulo q par suite

$$(C/D)^2 - 2 \equiv 0 \pmod q$$

et donc 2 est résidu quadratique modulo q, contradiction avec ce qui précède. D'où

$$q \mid \mathrm{pgcd}(C,D),$$

par suite

$$q^2 \mid h_p^-.$$

La réciproque est immédiate. □

La même remarque que précédemment s'applique, cette proposition est très importante: le calcul du pgcd de deux entiers est très peu coûteux et on peut donc facilement trouver les facteurs premiers q de h^- qui vérifient

$$q \equiv 5 \pmod 8.$$

Nous donnons une table regroupant des exemples des valeurs de h_p^-, et sa factorisation en nombre premiers, ainsi que les nombres premiers

$$q \equiv 5 \pmod 8$$

divisant h_p^- (3ème colonne).

Table 3.

$p \equiv 9 \pmod{16}$	h_p^-	$q \equiv 5 \pmod 8$
403721	$340491825 = 3^2 \cdot 5^2 \cdot 97 \cdot 15601$	5
405401	$4945345825 = 5^2 \cdot 7^2 \cdot 4037017$	5
408041	$3230129489 = 17 \cdot 37^2 \cdot 138793$	37
422249	$269738177 = 37^2 \cdot 197033$	37
434521	$3313929425 = 5^2 \cdot 17 \cdot 7797481$	5
434857	$15305213417 = 13^2 \cdot 90563393$	13
443689	$746100041 = 97 \cdot 173^2 \cdot 257$	173
466649	$1428933025 = 5^2 \cdot 13^2 \cdot 41 \cdot 73 \cdot 113$	[5, 13]
481433	$4790909961 = 3^2 \cdot 17 \cdot 37^2 \cdot 89 \cdot 257$	37
485081	$4464343225 = 5^2 \cdot 17 \cdot 37^2 \cdot 7673$	[5, 37]
491273	$144316025 = 5^2 \cdot 7^2 \cdot 117809$	5
$p \equiv 17 \pmod{32}$	h_p^-	$q \equiv 5 \pmod 8$
17489	$80851500625 = 5^4 \cdot 7^2 \cdot 17 \cdot 97 \cdot 1601$	5
454577	$18093215656930625 = 5^4 \cdot 28949145051089$	5
467729	$6106655334660625 = 5^4 \cdot 680993 \cdot 14347649$	5

4.6 Les facteurs de h_p^- de type $q \equiv 2^m+1 \pmod{2^{m+1}}$, $m \geq 3$

Rappelons un résultat de Ray Steiner [27]:

Proposition 4.6.1. *Soient p et q deux nombres premiers impairs. Posons $v_2(p-1) = t$, où v_2 désigne la valuation 2-adique, $d = 2^t$. Supposons que $v_2(p-1) > v_2(q-1)$. Si $q \mid h^-(K_p)$ alors $q^f \mid h^-(K_p)$ où f est l'ordre de q modulo d.*

Pour démontrer cette proposition nous avons besoin de certains outils.

4.6.1 Interprétation de nombre de classes relatif en terme d'ordre d'un groupe

Soit K un corps de nombres, $cl(K)$ le groupe de classes de K et $cl^+(K)$ le groupe de classes de son sous-corps réel maximal K^+. On a une application naturelle injective (théorème 4.14 de [29]): j: $cl^+(K) \longrightarrow cl(K)$. Notons $cl^-(K)$ le conoyau de cette application, $cl^-(K) = \mathrm{Coker}(j) = cl(K)/cl^+(K)$. Le groupe $cl^-(K)$ est appelé groupe de classes relatif de K. Soient h_K et h_K^+ les nombres de classes respectivement de K et K^+. Alors $\mid cl^-(K) \mid = \frac{h_K}{h_K^+} = h_K^-$, où h_K^- étant le nombre de classes relatif de K. On a la suite exacte de groupes suivante:

$$0 \longrightarrow cl^+(K) \xrightarrow{j} cl(K) \longrightarrow 0.$$

4.6.2 L'action de $1 + J$ sur un corps de type CM.

Soit K un corps de type CM, et soit $G = \mathrm{Gal(K/\mathbb{Q})}$. Alors G opère sur le groupe $cl(K)$ et $cl(K)$ est un G-module. Comme K est de type CM, la conjugaison complexe J commute avec les automorphismes de G. L'application

$$1 + J : cl(K) \longrightarrow cl^+(K)$$

est surjective (théorème 10.1 de [29]), par suite

$$cl(K)/\mathrm{Ker}(1+J) \simeq cl^+(K) \Rightarrow \mid \mathrm{Ker}(1+J) \mid = \frac{h_K}{h_K^+} = h_K^-.$$

Remarque. L'application $1+J$ n'est que l'application norme dans K/K^+; et d'après la théorie du corps des classes [29], cette application est surjective.

Soit A un groupe abélien fini tel que la conjugaison complexe J opère sur A. L'application $(1-J)$ opère sur A de la façon suivante, pour $a \in A$,

$$(1-J)a = a - Ja$$

si le groupe A est defini additivement; et

$$(1-J)a = a/Ja$$

si le groupe A est defini multiplicativement. On supposera dans la suite que le groupe A est additif. On a alors la proposition :

Proposition 4.6.2. *Si l'ordre de A est impair, alors il existe deux sous-groupes A^+ et A^- tels que A est somme directe de A^+ et A^-: $A = A^+ \oplus A^-$.*

Démonstration. Posons $\mid A \mid = 2m+1$. Soit $a \in A$, on a

$$(2m+1)a = 0$$

ce implique que

$$a = 2(-ma) \in 2A,$$

donc

$$A \subset 2A,$$

par suite

$$A = 2A.$$

Posons $A^+ = \frac{1+J}{2}A$ et $A^- = \frac{1-J}{2}A$. Vérifions que $A^+ = \mathrm{Ker}(1-J)$ et $A^- = \mathrm{Ker}(1+J)$. Soit $a \in A^+$ donc $a = \frac{1+J}{2}a_1$, $a_1 \in A$. On a

$$(1-J)a = \frac{(1-J)(1+J)}{2}a_1 = \frac{1-J^2}{2}a_1 = 0,$$

d'où

$$a \in \mathrm{Ker}(1-J).$$

Réciproquement si

$$a \in \mathrm{Ker}(1-J)$$

alors

$$a = Ja$$

implique

$$a = (1 + J)a - a,$$

soit donc $a = (\frac{1+J}{2})a$, d'où l'égalité. De la même manière on montre que

$$A^- = \mathrm{Ker}(1 + J).$$

Prouvons maintenant que $A = A^+ \oplus A^-$. Soit $a \in A$; il est clair que

$$a = \frac{1 + J}{2}a + \frac{1 - J}{2}a.$$

D'autre part, soit $a \in A^+ \cap A^-$, donc

$$a \in \mathrm{Ker}(1 - J) \cap \mathrm{Ker}(1 + J),$$

implique $a = Ja$ et $a = -Ja$, d'où

$$2a = 0,$$

par suite $a = 0$, donc

$$A^+ \cap A^- = \{0\}.$$

Par conséquent

$$A = A^+ \oplus A^-.$$

Remarque. D'après la démonstration, on a

$$A^+ = \mathrm{Ker}(1 - J) = \frac{1 + J}{2}A,$$

et

$$A^- = \mathrm{Ker}(1 + J) = \frac{1 - J}{2}A.$$

Preuve de la proposition de Steiner

Soit K_p le sous-corps de degré $d = 2^t$ sur $\mathbb{Q}$. D'après le théorème 10.4 de [29], $h^-(K_p)$ est impair. Supposons que $v_2(q-1) < v_2(p-1)$. Soit A le sous-groupe de $cl(K_p)$ formé des éléments d'ordre 1 ou q. Alors A est un q-groupe c'est-à-dire son ordre est une puissance de q. Comme q est impair, d'après la proposition précédente, nous avons la décomposition suivante :

$$A = A^+ \oplus A^-,$$

où

$$A^+ = \frac{1+J}{2}A$$

et

$$A^- = \frac{1-J}{2}A,$$

J étant la conjugaison complexe. Soit

$$G = \mathrm{Gal}(K_p/\mathbb{Q}) =< \sigma > .$$

L'application σ est d'ordre d, et $\sigma^{d/2} = J$. Le groupe de Galois G opère sur le sous-groupe A^-. Soit v un élément de A^-, et Ω_v son orbite suivant G. Supposons que $\mid \Omega_v \mid < d$. Montrons qu'il existe $0 < i < d$, $i \mid d$ et $\sigma^i(v) = v$. Comme $\mid \Omega_v \mid < d$, il existe i et j avec $i < j$ tels que $\sigma^i(v) = \sigma^j(v)$ i.e. $\sigma^{j-i}(v) = v$. Soit i le plut petit entier non nul tel que $\sigma^i(v) = v$. Considérons la division euclidienne de d par i, $d = li + r$ avec $0 \leq r < i$; on a

$$\sigma^d(v) = \sigma^{li+r}(v) = v \Rightarrow \sigma^r(\sigma^{li}(v)) = \sigma^r(v) = v,$$

comme $r < i$, alors $r = 0$ et par suite $i \mid d$.

Remarquons que $i \mid d/2$ car $i < d = 2^t$, par suite $\sigma^{d/2}(v) = v$. Par ailleurs $v \in A^- = \mathrm{Ker}(1+J)$ (voir la remarque) ce qui implique $Jv = -v$; on en déduit —puisque $\sigma^{d/2} = J$— que $v = 0$. Par conséquent l'orbite de tout élément non nul de A^- a d éléments. Nous savons que chaque orbite est une classe d'équivalence pour la relation

$$v_1 \varrho\, v_2 \Rightarrow \exists g \in G, v_2 = g.v_1.$$

Soit $\{v_i, i \in I\}$ une famille de représentants de G-orbites distinctes de A^-. Les Ω_{v_i} $(i \in I)$ forment une partition de A^-, d'où

$$|A^-| = \sum_{i \in I} |\Omega_{v_i}|,$$

par suite

$$|A^-| \equiv 1 \pmod{d}.$$

Supposons que $q^m = |A^-|$, $q^m \equiv 1 \pmod{d}$ entraîne que $f \mid m$, car f est l'ordre de q modulo d; par suite q^f divise $\mid A^- \mid$. D'autre part l'application

$$1 + J : cl(K) \longrightarrow cl^+(K)$$

est surjective et

$$\mid \mathrm{Ker}(1 + J) \mid = h_K^-.$$

Considérons la réstriction de $1 + J$ au sous-groupe A, notée $(1 + J)_{|A}$. Alors

$$\mathrm{Ker}((1 + J)_{|A}) = \frac{1 - J}{2} A = A^-,$$

implique $\mid A^- \mid$ divise h_K^-. Donc $q^f \mid h_K^-$. □

Remarques.

1) Si $v_2(q - 1) \geq v_2(p - 1)$, alors $f = 1$.

2) L'ordre de multiplicité avec lequel un nombre premier q divise $h^-(K_p)$ peut être supérieur ou égal à l'ordre f de q modulo d; comme le montrent les exemples suivants :

$p = 30697$,

$h^-(K_p) = 12058353 = 3^2 \cdot 1339817$, $q = 3$, $v_2(p - 1) = 3$, $\mathrm{Ord}_8(3) = 2$.

$p = 30169$,

$h^-(K_p) = 6684849 = 3^4 \cdot 82529$, $q = 3$, $v_2(p - 1) = 3$. Dans ce dernier exemple, l'ordre de multiplicité avec lequel 3 divise $h^-(K_p)$ est égal à 4 qui est supérieur à $\mathrm{Ord}_8(3) = 2$.

Nous démontrons le théorème suivant:

Théorème 4.6.3. *Posons $[K_p : \mathbb{Q}] = 2^n$ et $m \leq n$.*
Si $q \equiv 1 + 2^m \pmod{2^{m+1}}$ divise $h^-(K_p)$, alors $q^{2^{n-m}}$ divise $h^-(K_p)$. De plus si $q^\mu \mid\mid h^-(K_p)$, alors $\mu = 2^{n-m} \cdot l$, où l est un entier.

Démonstration. Le lemme 4.3.2 montre que 2^{n-m} est l'ordre de q modulo 2^n; et d'après la proposition de Steiner, $q^{2^{n-m}}$ divise $h^-(K_p)$. Par ailleurs, si $q^\mu \mid\mid h^-(K_p)$ alors q^μ est un facteur caractéristique primaire, donc d'après le théorème 2.3.4 chapitre 2, $q^\mu \equiv 1 \pmod{2^n}$, par conséquent $\mu = 2^{n-m} \cdot l$.

4.6.3 Applications et exemples

1) Considérons le cas où $p \equiv 9 \pmod{16}$; à l'aide du pogramme de Roy (annexe II), nous avons cherché les nombres premiers $q \equiv 9 \pmod{16}$ qui divisent le nombre de classes relatif h_p^-. Ainsi nous avons regroupé dans ce cas précis, quelques exemples dans les tables 4 et 5 ci-dessous. Notons bien que dans ce cas, $v_2(p-1) = v_2(q-1) = 3$.

Table 4.

$p \equiv 9 \pmod{16}$	h_p^-	$q \equiv 9 \pmod{16}$
313	233	233
457	41	41
569	521	521
601	$34153 = 7^2 \cdot 17 \cdot 41$	41
617	73	73
1097	233	233
1129	$369 = 3^2 \cdot 41$	41
1321	$10489 = 17 \cdot 617$	617
1433	30937	30937
1657	12809	12809
1721	$25297 = 41 \cdot 617$	[41, 617]
1753	$697 = 17 \cdot 41$	41
1801	$10001 = 73 \cdot 137$	[73, 137]
1913	112361	112361
2153	$7913 = 41 \cdot 193 \cdot$	41
2297	$5617 = 41 \cdot 137 \cdot$	[41, 137]
2377	11657	11657
2441	387433	387433
2521	$1241 = 17 \cdot 73$	73
2633	6473	6473
2729	5417	5417
2953	2473	2473
2969	284489	284489

Table 5.

$p \equiv 9 \pmod{16}$	h_p^-	$q \equiv 9 \pmod{16}$
30137	$13064057 = 97 \cdot 134681$	134681
30313	$723937 = 41 \cdot 17657$	[41, 17657]
32441	$425153 = 17 \cdot 89 \cdot 281$	[89, 281]
33289	$563137 = 601 \cdot 937$	[601, 937]
35401	$570433 = 41 \cdot 13913$	[41, 13913]
37897	$95489 = 17 \cdot 41 \cdot 137$	[41, 137]
38153	$767233 = 41 \cdot 18713$	[41, 18713]
38377	$17258177 = 281 \cdot 61417$	[281, 61417]
38569	$20702529 = 3^2 \cdot 2300281$	2300281
40169	$22072489 = 337 \cdot 65497$	65497
40361	60543529	60543529
41593	$8141225 = 5^2 \cdot 137 \cdot 2377$	[137, 2377]
42089	$39459753 = 3^2 \cdot 41 \cdot 106937$	[41, 106937]
43481	12780697	12780697
44041	$360401 = 73 \cdot 4937$	[73, 4937]
45497	$2530721 = 857 \cdot 2953$	[857, 2953]
45833	873113	873113
46889	$23101025 = 5^2 \cdot 924041$	924041
47161	37541113	37541113
47881	$421931273 = 8273 \cdot 51001$	51001
48889	295081	295081
49081	3735737	3735737

3) Nous donnons aussi une table des valeurs de h_p^- où $p \equiv 17 \pmod{32}$. Dans ce cas $v_2(p-1) = t = 4$. D'après le théorème 4.6.3, si $q \mid h_p^-$ alors $q^2 \mid h_p^-$.

Table 6.

$p \equiv 17 \pmod{32}$	h_p^-	$q \equiv 9 \pmod{16}$
53777	$99524835649 = 17 \cdot 73^2 \cdot 1098593$	73
183569	$191533089437201 = 41^2 \cdot 146609 \cdot 777169$	41
266417	$2849099691276017 = 89^2 \cdot 359689394177$	89
300497	$707926019603041 = 17 \cdot 41^2 \cdot 24772580033$	41

Remarque. Le nombre de classes relatif de K_p croit avec la valuation 2-adique de $p-1$, comme le montre l'exemple suivant:
$p = 7681$, $v_2(p-1) = 9$;
On a:
$h^-(K_p) = 150683621502752159028920720569713704052533317139292214947454059608691521378158872826115919779296565069652693302858269178693952808386761008285878133965142167410834860238636127629142844895703977374600327918407671316056752610012843833371325733764118837693476148562741597349998284783184551783807489$

4.7 Explication du programme de Roy

Nous utiliserons dans cette section les notations adoptées par le programme de Roy. Posons `v=valuation(p-1,2)`, $d = 2^v$, $dd = d/2$ et g une racine primitive modulo le nombre premier impair p, `g=lift(primroot(p))`. Le programme de Roy utilise le fait que $h^-(Kp)$ est essentiellement une norme et il la calcule par une méthode récursive à l'aide de la tour des corps intermédiaires entre le corps des racines 2^v-ièmes de l'unité et $\mathbb{Q}$ en utilisant la transitivité de la norme i.e. les corps des racines 2^k-ièmes de l'unité pour k allant de v à 1, en divisant chaque fois le degré par 2. Dans la partie pratique son programme s'arrête au sous-corps $\mathbb{Q}(i)$.

4.7.1 Etapes du programme de Roy et détails.

```
\\ CALCUL DE H-(p)
#
{hm(p,v,fc,r,s)=\
    v=valuation(p-1,2);
      fc=if(p==2^v+1,p,1);
```

```
      if(v==1,r=classno(-p),r=hmoins(p,v,fc));
      print("p=",p,"; hm=",r,"; z(p)");
  }
{hmoins(p,v,fc   ,d,dd,ta)=\
  d=2^v; dd=d/2;
  ta=yrsum(p,d);
  ta=yrmod(ta,dd);
  forstep(k=v,3,-1, ta=yrfor(ta,2^(k-1)));
  print(ta);ta=yrfor(ta,2);
   fc*(2*ta[1])/(2*p)^dd\
   }
\\ sum( g^j mod p)
{yrsum(p,d   ,g,ta,a,k,j)=\
  g=lift(primroot(p)); ta=vector(d,j,0); a=1;
  for(j=0,(p-3)/2, k=j%d+1;ta[k]=ta[k]+(a+a-p);a=(a*g)%p;);
  ta\
}
\\ mod(A(X), 1+X^k)
{yrmod(ta,k  ,n)=n=length(ta); vector(k,j,ss(j,n))}
{ss(j,n ,r,s,b)=\
  r=j; s=0; b=1;
  while(r<=n, if(b>0, s =s+ta[r], s =s-ta[r]); r=r+k; b=-b);
  s\
}
\\  C(X)=mod( A(X)*A(-X),1+X^d ); C(sqrt(X))
{yrfor(ta,d  ,j)=vector(d/2,j,yrb(j-1)-yrbd(j-1))}
{yrb(j  ,k)=(-1)^j*ta[j+1]^2 + 2*sum(0,k=0,j-1,(-1)^k *ta[k+1] *ta[j+j-k+1])}
{yrbd(j  ,k,dd)=dd=d/2+j;(-1)^dd*ta[dd+1]^2+2*sum(0,k=2*j+1,dd-1,
(-1)^k*ta[k+1]*ta[dd+dd-k+1])}
```

- Cas $v = 1$:

La fonction `hm(p,v,fc,r,s)` calcule le nombre de classes relatif h_p^- du sous-corps quadratique $K_p = \mathbb{Q}(\sqrt{-p})$ à l'aide de la fonction `classno(-p)`. La

condition `fc` prend la valeur p si $p-1=2^v$ et 1 sinon.

- Cas $v \neq 1$:

La fonction `hmoins(p,v,fc,d,dd,ta)}` calcule $h_p^- = h^-(K_p)$.
On a besoin du lemme suivant:

Lemme 4.7.1. *Posons $d=2^v$, $\alpha = \mathbf{e}^{2i\pi/d}$, g une racine primitive modulo p. Pour $n \in \mathbb{N}$ on pose aussi $g_n \equiv g^n \pmod p$, $0 < g_n < p$. Alors*

$$h_p^- = p^{[d/p-1]} \frac{2}{(2p)^{d/2}} \mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\mathrm{M}_d(p));$$

où $\mathrm{M}_d(p) = \sum_{j=0}^{\frac{p-3}{2}} (2g_j - p)\alpha^j$.

Démonstration. On sait que (cf. chapitre 2, page 28)

$$\mathrm{M}_d(p) = \sum_{k=1}^{p-1} k\chi_d(k) = \sum_{n=1}^{p-1} g_n \alpha^n.$$

Posons $r = \frac{p-1}{2}$, alors on a successivement les égalités suivantes:

$$\begin{aligned}
\mathrm{M}_d(p) &= \sum_{j=1}^{r-1} g_j\alpha^j + \sum_{j=r}^{p-1} g_j\alpha^j \\
&= \sum_{j=1}^{r-1} g_j\alpha^j + \sum_{j=0}^{r} g_{j+r}\alpha^{j+r} \\
&= \sum_{j=1}^{r-1} g_j\alpha^j - \sum_{j=0}^{r}(p-g_j)\alpha^j \qquad (\text{car } g_{j+r} = p-g_r, \text{ et } \alpha^r = -1) \\
&= \sum_{j=0}^{r-1}(2g_j - p)\alpha^j,
\end{aligned}$$

utilisant le fait que $g_0 = 1$ et $g_r = p-1$. Ce qui démontre le lemme.

A l'aide du lemme précédent, $\mathrm{M}_e(p)$ peut être considéré comme un vecteur de dimension $\frac{p-1}{2}$:

$$\mathrm{M}_e(p) \sim [A_1, A_2, \ldots, A_d] = \mathtt{ta},$$

où $A_j = 2g_j - p$ pour $j = 0, \ldots, \frac{p-3}{2}$.
Comme

$$\alpha^{n+d} = \alpha^n$$

pour tout n, alors $\mathrm{M}_e(p)$ peut être réduit à un vecteur de dimension d.

L'objet de la fonction `yrsum(p,d)` est de calculer les éléments `ta[k]` ($k = 1, \ldots, d$) du vecteur `ta` modulo d. Ainsi on obtient un vecteur de dimension d:

$$\texttt{ta} \sim [A_1^{'}, A_2^{'}, \ldots, A_d^{'}].$$

Puisque

$$\alpha^{n+d/2} = -\alpha^n$$

pour tout n, le vecteur `ta` peut être compressé en un vecteur de dimension $d/2$:

$$\texttt{ta} \sim [A_1^{''}, A_2^{''}, \ldots, A_{d/2}^{''}],$$

où $A_j^{''} = A_j - A_{j+d/2}$.
La fonction `yrmod(ta, d)` calcule alors les éléments $A_j^{''}$.

Pour expliquer et comprendre la dernière partie du programme c'est-à-dire la procédure `yrfor`, un rappel sur les polynômes s'avère nécessaire.

4.7.2 Rappel sur les polynômes

Nous supposerons que d est un entier pair.
Si $A(X) = \sum_{i=0}^{d-1} a_i X^i$ et $B(X) = \sum_{i=0}^{d-1} b_i X^i$ alors

$$C(X) = A(X) \cdot B(X) = \sum_{k=0}^{2d-2} c_k X^k$$

avec

$$\begin{cases} c_k = \sum_{i=0}^{k} a_i b_{k-i}, & k = 0, 1, \ldots, d-2, d-1, \\ c_{d+k} = \sum_{i=k+1}^{d-1} a_i b_{d+k-i}, & k = 0, 1, \ldots, d-2. \end{cases}$$

Si $C(X) = A(X) \cdot A(-X)$ alors $C(X) = \sum_{j=0}^{d-1} c_{2j} X^{2j}$ avec

$$\begin{cases} c_{2j} = \sum_{i=0}^{2j} (-1)^i a_i a_{2j-i}, \\ \\ c_{d+2j} = \sum_{i=2j+1}^{d-1} (-1)^i a_i a_{d+2j-i}, \end{cases} \quad (j = 0, 1, \ldots, \tfrac{d-2}{2})$$

ou encore, grace à la symétrie des sommes

$$\begin{cases} c_{2j} = (-1)^j \cdot a_j^2 + 2 \sum_{i=0}^{j-1} (-1)^i a_i a_{2j-i}, \\ \\ c_{d+2j} = (-1)^{j+d/2} \cdot a_{d/2+j}^2 + 2 \sum_{i=2j+1}^{d/2+j-1} (-1)^i a_i a_{d+2j-i}. \end{cases} \quad (j = 0, 1, \ldots, \tfrac{d-2}{2})$$

4.7.3 Polynôme réduit modulo un autre polynôme

Soit $A(X)$ un polynôme réduit modulo $1 + X^d$ où $d = 2^v$, v entier positif. $A(X) = \sum_{i=0}^{d-1} a_i X^i$. Posons

$$B(X) = A(X) \cdot A(-X) = \sum_{i=0}^{2d-2} b_i X^i.$$

On a

$$B(X) = B(-X) \Rightarrow b_{2j+1} = 0 \quad \forall j;$$

ceci implique

$$B(X) = \sum_{j=0}^{d-1} b_{2j} X^{2j}.$$

On a successivement les égalités suivantes:

$$\begin{aligned} B(X) &= \sum_{j=0}^{d-1} b_{2j} X^{2j} \\ &= \sum_{j=0}^{\frac{d-2}{2}} b_{2j} X^{2j} + \sum_{j=d/2}^{d-1} b_{2j} X^{2j} \\ &= \sum_{j=0}^{\frac{d-2}{2}} b_{2j} X^{2j} + \sum_{j=0}^{\frac{d-2}{2}} b_{d+2j} X^{d+2j} \\ &= \sum_{j=0}^{\frac{d-2}{2}} (b_{2j} + b_{d+2j} \cdot X^d) X^{2j}. \end{aligned}$$

Soit $C(X) = \mathrm{mod}(B(X), 1+X^d)$, le polynôme $B(X)$ réduit modulo $1+X^d$. Alors

$$C(X) = \sum_{j=0}^{\frac{d-2}{2}} (b_{2j} - b_{d+2j}) X^{2j}.$$

Soit $F(X) = C(\sqrt{X})$

$$F(X) = \sum_{j=0}^{\frac{d-2}{2}} (b_{2j} - b_{d+2j}) X^{j}.$$

Alors $F(X)$ est un polynôme réduit modulo $1+X^{d/2}$.

Revenons maintenant à la procédure `yrfor`. D'après le programme de Roy `ta =yrmod(ta, dd)` est un vecteur de dimension $d' = dd = d/2$. Le programme calcule `yrfor(ta, 2^(k-1))` qui est un vecteur de dimension 2^{k-2} où k allant de v à 2. Nous allons vérifier que l'élément `ta[1]` dans le programme de Roy correspond bien à la norme $\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\mathrm{M}_d(p))$. La transitivité de la norme implique que

$$\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\mathrm{M}_d(p)) = \mathrm{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_{d'})}(\mathrm{M}_d(p)));$$

Posons $A(\zeta_{d'}) = \mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_{d'})}(\mathrm{M}_d(p))$, où $A(X)$ est un polynôme de $\mathbb{Z}[X]$ de degré $d'-1$. Alors on a

$$\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\mathrm{M}_d(p)) = \mathrm{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(\mathrm{A}(\zeta_{d'})) = \mathrm{N}_{\mathbb{Q}(\zeta_{d'/2})/\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}(\zeta_{d'/2})}(\mathrm{A}(\zeta_{d'})).$$

Notons que l'isomorphisme $\zeta_{d'} \longmapsto -\zeta_{d'}$ engendre le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q}(\zeta_{d'/2}))$, par suite

$$\mathrm{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}(\zeta_{d'/2})}(\mathrm{A}(\zeta_{d'})) = \mathrm{A}(\zeta_{d'}) \cdot \mathrm{A}(-\zeta_{d'}).$$

Considérons le polynôme $\mathrm{A}(X)$ réduit modulo $1+X^{d'}$, $A(X) = \sum_{i=0}^{d'-1} a_i X^i$. Posons $B(X) = A(X) \cdot A(-X)$; et $C(X) = \mathrm{mod}(B(X), 1+X^{d'})$, le polynôme $B(X)$ réduit modulo $1+X^{d'}$. D'après ce qui précède sur les polynômes,

$$C(X) = \sum_{j=0}^{\frac{d'-2}{2}} (b_{2j} - b_{d'+2j}) X^{2j},$$

où

$$\begin{cases} b_{2j} = (-1)^j \cdot a_j^2 + 2\sum_{i=0}^{j-1}(-1)^i a_i a_{2j-i}, \\ \\ b_{d'+2j} = (-1)^{j+d'/2} \cdot a_{d'/2+j}^2 + 2\sum_{i=2j+1}^{d'/2+j-1}(-1)^i a_i a_{d'+2j-i}. \end{cases} \quad (j = 0, 1, \ldots, \tfrac{d'-2}{2})$$

La fonction `yrfor(ta,dd)` est un vecteur de dimension $d'/2$ et dont les élements sont $b_{2j} - b_{d'+2j}$; où —dans le programme—

$$b_{2j} = \texttt{yrb(j-1)}, b_{d'+2j} = \texttt{yrbd(j-1)}$$

et

$$a_j = \texttt{ta}[j+1].$$

Soit $F(X) = C(\sqrt{X})$

$$F(X) = \sum_{j=0}^{\frac{d'-2}{2}} (b_{2j} - b_{d+2j}) X^j.$$

Alors $F(X)$ est un polynôme réduit modulo $1 + X^{d'/2}$, et $F(\zeta_{d'})$ correspond exactement à $\mathrm{A}(\zeta_{d'}) \cdot \mathrm{A}(-\zeta_{d'})$.

Le programme calcule ensuite les éléments du vecteur `ta=yrfor(ta,d'/2)` par le même processus que précédemment, et ainsi de suite jusqu'au calcul du vecteur `ta=yrfor(ta, 2)` qui est un vecteur de dimension 1. Finalement on a

$$\texttt{ta[1]} = \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)}(\ldots(\mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_{dd})}(\mathrm{M}_d(p));$$

d'où

$$\texttt{ta[1]} = \mathrm{N}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\mathrm{M}_d(p)).$$

Enfin l'instruction

```
fc*(2*ta[1])/(2*p)^dd
```

calcule le facteur h_p^- (voir lemme 4.7.1).

Annexes

Annexe I: Programme donnant d'autres exemples

```
{proc2(p,e)=\
 g=znprimroot(p); G=lift(g); e=2^valuation(p-1,2);
 tau=e/gcd(e,znlog(2,g));
 phi=polcyclo(tau); phi2=subst(phi,x,2);
 alpha=Mod(x,polcyclo(e));
 gam=eulerphi(e)/eulerphi(tau);
 tabeps=vector((p-1)/2,j,((G^j)\%p<p/2));
 W=sum(n=2,(p-1)/2,(tabeps[n]-tabeps[n-1])*alpha^n,(tabeps[1]-1)*alpha);
 W=lift(W);
 P = W*prod(j=1,(e/2)-1,subst(W,x,x^(2*j+1)));
 Q=lift(Mod(P,polcyclo(e)));
 if(p-1==e,Q=Q*p);
 h=Q/phi2^gam;
 print("p=",p," "  "degre de Ke=", 2^valuation(p-1,2), " h-(Ke)=" "",h);
 }
 forprime(p=3,251,proc2(p))
p=3 degre de Ke=2 h-(Ke)=1
p=5 degre de Ke=4 h-(Ke)=1
p=7 degre de Ke=2 h-(Ke)=1
p=11 degre de Ke=2 h-(Ke)=1
p=13 degre de Ke=4 h-(Ke)=1
p=17 degre de Ke=16 h-(Ke)=1
p=19 degre de Ke=2 h-(Ke)=1
```

```
p=23 degre de Ke=2 h-(Ke)=3
p=29 degre de Ke=4 h-(Ke)=1
p=31 degre de Ke=2 h-(Ke)=3
p=37 degre de Ke=4 h-(Ke)=1
p=41 degre de Ke=8 h-(Ke)=1
p=43 degre de Ke=2 h-(Ke)=1
p=47 degre de Ke=2 h-(Ke)=5
p=53 degre de Ke=4 h-(Ke)=1
p=59 degre de Ke=2 h-(Ke)=3
p=61 degre de Ke=4 h-(Ke)=1
p=67 degre de Ke=2 h-(Ke)=1
p=71 degre de Ke=2 h-(Ke)=7
p=73 degre de Ke=8 h-(Ke)=89
p=79 degre de Ke=2 h-(Ke)=5
p=83 degre de Ke=2 h-(Ke)=3
p=89 degre de Ke=8 h-(Ke)=113
p=97 degre de Ke=32 h-(Ke)=3457
p=101 degre de Ke=4 h-(Ke)=5
p=103 degre de Ke=2 h-(Ke)=5
p=107 degre de Ke=2 h-(Ke)=3
p=109 degre de Ke=4 h-(Ke)=17
p=113 degre de Ke=16 h-(Ke)=17
p=127 degre de Ke=2 h-(Ke)=5
p=131 degre de Ke=2 h-(Ke)=5
p=137 degre de Ke=8 h-(Ke)=17
p=139 degre de Ke=2 h-(Ke)=3
p=149 degre de Ke=4 h-(Ke)=9
p=151 degre de Ke=2 h-(Ke)=7
p=157 degre de Ke=4 h-(Ke)=5
p=163 degre de Ke=2 h-(Ke)=1
p=167 degre de Ke=2 h-(Ke)=11
p=173 degre de Ke=4 h-(Ke)=5
p=179 degre de Ke=2 h-(Ke)=5
```

```
p=181 degre de Ke=4 h-(Ke)=25
p=191 degre de Ke=2 h-(Ke)=13
p=193 degre de Ke=64 h-(Ke)=192026280449
p=197 degre de Ke=4 h-(Ke)=5
p=199 degre de Ke=2 h-(Ke)=9
p=211 degre de Ke=2 h-(Ke)=3
p=223 degre de Ke=2 h-(Ke)=7
p=227 degre de Ke=2 h-(Ke)=5
p=229 degre de Ke=4 h-(Ke)=17
p=233 degre de Ke=8 h-(Ke)=1433
p=239 degre de Ke=2 h-(Ke)=15
p=241 degre de Ke=16 h-(Ke)=2209
p=251 degre de Ke=2 h-(Ke)=7
```

Annexe II: Programme de Roy calculant $h^-(K_p)$

Le programme de Roy utilise le fait que $h^-(K_p)$ est essentiellement une norme et il la calcule par une méthode récurssive en divisant chaque fois le degré par 2. Dans la partie pratique son programme s'arrête au sous-corps $\mathbb{Q}(i)$.

```
\\ CALCUL DE H-(p)
\\ optimise avec des vecteurs (30-3-95).
#
{hm(p,v,fc,r,s)=\
    v=valuation(p-1,2);
      fc=if(p==2^v+1,p,1);
      if(v==1,r=classno(-p),r=hmoins(p,v,fc));
      print("p=",p,"; hm=",r,"; z(p)");
  }
{hmoins(p,v,fc   ,d,dd,ta)=\
  d=2^v; dd=d/2;
  ta=yrsum(p,d);
  ta=yrmod(ta,dd);
  forstep(k=v,3,-1, ta=yrfor(ta,2^(k-1)));
  print(ta);ta=yrfor(ta,2);
   fc*(2*ta[1])/(2*p)^dd\
   }
\\ sum( g^j mod p)
```

```
{yrsum(p,d   ,g,ta,a,k,j)=\
  g=lift(primroot(p)); ta=vector(d,j,0); a=1;
  for(j=0,(p-3)/2, k=j%d+1;ta[k]=ta[k]+(a+a-p);a=(a*g)%p;);
  ta\
}
\\ mod(A(X), 1+X^k)
{yrmod(ta,k  ,n)=n=length(ta); vector(k,j,ss(j,n))}
{ss(j,n ,r,s,b)=\
  r=j; s=0; b=1;
  while(r<=n, if(b>0, s =s+ta[r], s =s-ta[r]); r=r+k; b=-b);
  s\
}
\\  C(X)=mod( A(X)*A(-X),1+X^d ); C(sqrt(X))
{yrfor(ta,d  ,j)=vector(d/2,j,yrb(j-1)-yrbd(j-1))}
{yrb(j  ,k)=(-1)^j*ta[j+1]^2 + 2*sum(0,k=0,j-1,(-1)^k *ta[k+1] *ta[j+j-k+1])}
{yrbd(j  ,k,dd)=dd=d/2+j;(-1)^dd*ta[dd+1]^2+2*sum(0,k=2*j+1,dd-1,(-1)^k*ta[k+1]*
```

Applications numériques

```
? forprime(p=3,300,hm(p);print("degre de Kp=",2^valuation(p-1,2)))

p=3; hm=1; z(p)
degre de Kp=2
[-3, -1]
p=5; hm=1; z(p)
degre de Kp=4
p=7; hm=1; z(p)
degre de Kp=2
p=11; hm=1; z(p)
degre de Kp=2
[-13, -13]
```

```
p=13; hm=1; z(p)
degre de Kp=4
[117912, 196520]
p=17; hm=1; z(p)
degre de Kp=16
p=19; hm=1; z(p)
degre de Kp=2
p=23; hm=3; z(p)
degre de Kp=2
[29, -29]
p=29; hm=1; z(p)
degre de Kp=4
p=31; hm=3; z(p)
degre de Kp=2
[-37, 37]
p=37; hm=1; z(p)
degre de Kp=4
[-3362, -3362]
p=41; hm=1; z(p)
degre de Kp=8
p=43; hm=1; z(p)
degre de Kp=2
p=47; hm=5; z(p)
degre de Kp=2
[53, 53]
p=53; hm=1; z(p)
degre de Kp=4
p=59; hm=3; z(p)
degre de Kp=2
[-61, 61]
p=61; hm=1; z(p)
degre de Kp=4
p=67; hm=1; z(p)
```

```
degre de Kp=2
p=71; hm=7; z(p)
degre de Kp=2
[-31974, -138554]
p=73; hm=89; z(p)
degre de Kp=8
p=79; hm=5; z(p)
degre de Kp=2
p=83; hm=3; z(p)
degre de Kp=2
[-15842, -237630]
p=89; hm=113; z(p)
degre de Kp=8
[-5015957500401255040, -83264894506660833664]
p=97; hm=3457; z(p)
degre de Kp=32
[303, -101]
p=101; hm=5; z(p)
degre de Kp=4
p=103; hm=5; z(p)
degre de Kp=2
p=107; hm=3; z(p)
degre de Kp=2
[-545, -327]
p=109; hm=17; z(p)
degre de Kp=4
[-3913136664, 6521894440]
p=113; hm=17; z(p)
degre de Kp=16
p=127; hm=5; z(p)
degre de Kp=2
p=131; hm=5; z(p)
degre de Kp=2
```

```
[-112614, 187690]
p=137; hm=17; z(p)
degre de Kp=8
p=139; hm=3; z(p)
degre de Kp=2
[-447, -447]
p=149; hm=9; z(p)
degre de Kp=4
p=151; hm=7; z(p)
degre de Kp=2
[-157, -471]
p=157; hm=5; z(p)
degre de Kp=4
p=163; hm=1; z(p)
degre de Kp=2
p=167; hm=11; z(p)
degre de Kp=2
[519, 173]
p=173; hm=5; z(p)
degre de Kp=4
p=179; hm=5; z(p)
degre de Kp=2
[-1267, -181]
p=181; hm=25; z(p)
degre de Kp=4
p=191; hm=13; z(p)
degre de Kp=2
[71658581362817442489115722913528460586977427456,
  230013715152037176452267035217882562837021655O4]
p=193; hm=192026280449; z(p)
degre de Kp=64
[197, 591]
p=197; hm=5; z(p)
```

```
degre de Kp=4
p=199; hm=9; z(p)
degre de Kp=2
p=211; hm=3; z(p)
degre de Kp=2
p=223; hm=7; z(p)
degre de Kp=2
p=227; hm=5; z(p)
degre de Kp=2
[-687, -1145]
p=229; hm=17; z(p)
degre de Kp=4
[3148762, -4886010]
p=233; hm=1433; z(p)
degre de Kp=8
p=239; hm=15; z(p)
degre de Kp=2
[-1268399362936, -1268399362936]
p=241; hm=2209; z(p)
degre de Kp=16
p=251; hm=7; z(p)
degre de Kp=2
[-16648419352336863488639645413887249390925619904664509536407788790615230387782315027956186997730053668188554412259214448437093180360042315031717898055216732412044821220875552819301292774708536672256006,
 3265062207226771856752127220044776499523342188116792395824139419234018870801607372532479136340831077437323741605845187674853304696613864970029021538601668333550439275842794350402365102039632731491532816]
p=257; hm=5452485023419230873223822625555964461476422854662168321; z(p)
degre de Kp=256
p=263; hm=13; z(p)
```

```
degre de Kp=2
[-1345, 269]
p=269; hm=13; z(p)
degre de Kp=4
p=271; hm=11; z(p)
degre de Kp=2
[831, 1385]
p=277; hm=17; z(p)
degre de Kp=4
[473766, -789610]
p=281; hm=17; z(p)
degre de Kp=8
p=283; hm=3; z(p)
degre de Kp=2
[-879, 879]
p=293; hm=9; z(p)
degre de Kp=4
?

? forprime(p=1000,4000, if(p%16==1, print(factor(hm(p))),))

p=1009; hm=642497
[193, 1; 3329, 1]
p=1153; hm=22549970876411799188534509100675141468874486 2849
[1153, 1; 4481, 1; 436457272256819904113494310480332812529 93, 1]
p=1201; hm=481601
[401, 1; 1201, 1]
p=1217; hm=746054010421964262019201
[193, 1; 769, 1; 5026742289777884353, 1]
p=1249; hm=208108798561
[17, 2; 720099649, 1]
p=1297; hm=142273
[17, 1; 8369, 1]
```

```
p=1361; hm=1194097
[17, 1; 70241, 1]
p=1409; hm=5119896538419984459698860021229102077588791530060 9
[169217, 1; 3025639586105405756926821785771584461129077 77, 1]
p=1489; hm=2816977
[97, 1; 113, 1; 257, 1]
p=1553; hm=157633
[7, 2; 3217, 1]
p=1601; hm=40916067823300529430023968 1
[52917943297, 1; 7731983760907073, 1]
p=1697; hm=3756019991873
[30881, 1; 121628833, 1]
p=1777; hm=296369
[296369, 1]
p=1873; hm=21701809
[17, 1; 241, 1; 5297, 1]
p=1889; hm=63216398428097
[17, 2; 218741863073, 1]
p=2017; hm=129366846095713
[97, 1; 1333678825729, 1]
p=2081; hm=161125696056673
[161125696056673, 1]
p=2113; hm=153864939381905272798122873 7
[6572801, 1; 234093409159816755137, 1]
p=2129; hm=2926337
[2926337, 1]
p=2161; hm=28953329
[17, 1; 641, 1; 2657, 1]
p=2273; hm=100644579779873
[16993, 1; 5922708161, 1]
p=2417; hm=22465153
[22465153, 1]
p=2593; hm=127020405770869748609
```

```
[257, 1; 449, 1; 12641, 1; 87078832993, 1]
p=2609; hm=29607937
[193, 1; 153409, 1]
p=2657; hm=1053785511841
[118529, 1; 8890529, 1]
p=2689; hm=984932996680800879017189027209209510989309833509637284378889
[257, 1; 224129, 1; 1340454828273409, 1; 127562589585810242098992150152052505 7,
1]
p=2753; hm=10581970027943844040629685792 1
[257, 1; 873571431169, 1; 471340741974337, 1]
p=2801; hm=37731041
[17, 1; 1249, 1; 1777, 1]
p=2833; hm=814529
[337, 1; 2417, 1]
p=2897; hm=54660961
[593, 1; 92177, 1]
p=3041; hm=1319464597816993
[31607297, 1; 41745569, 1]
p=3089; hm=31768753
[31768753, 1]
p=3121; hm=7276001
[7276001, 1]
p=3137; hm=33354676927466718942404898664 97
[193, 1; 172822160245941548924377713 29, 1]
p=3169; hm=12188294713647841
[10273, 1; 1186439668417, 1]
p=3217; hm=11748241
[17, 1; 257, 1; 2689, 1]
p=3313; hm=50652721
[7, 2; 97, 1; 10657, 1]
p=3329; hm=208124311979269946885833321841946239206157136098709588662932444675174
402844395237036284993935678921828094699869787202835507 3
[257, 1; 6656706817, 1; 121655083791903789785150571938599102843941688369462789 10
```

```
916135101755612303873585542600220350709784612512534364l7, 1]
p=3361; hm=4144474736075809
[4481, 1; 15233, 1; 60716833, 1]
p=3457;
hm=185469298626235679570634021840615881776955046800462555378088833
```

Annexe III

```
        GP/PARI CALCULATOR Version 2.0.16 (beta)
                i686 running linux (ix86 kernel) 32-bit version
                (readline v2.2 enabled, extended help available)
                          Copyright (C) 1989-1999 by
          C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier.
Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.
   realprecision = 28 significant digits
   seriesprecision = 16 significant terms
   format = g0.28
parisize = 4000000, primelimit = 500000

\\ D{\'e}composition dans L_n : n=2,3,4,5,6 et m=2.
? L2(q)=Mod(1,q)*x^2+Mod(1,q)
? L3(q)=Mod(1,q)*x^4+Mod(1,q)
? L4(q)=Mod(1,q)*x^8+Mod(1,q)
? L5(q)=Mod(1,q)*x^16+Mod(1,q)
? L6(q)=Mod(1,q)*x^32+Mod(1,q)

? forprime(q=3,100,if(q%8==5,print("q=",q);print(factor(L2(q)));
print(factor(L3(q)));;print(factor(L4(q)));print(factor(L5(q)));
print(factor(L6(q))),))

q=5
[Mod(1, 5)*x + Mod(2, 5), 1; Mod(1, 5)*x + Mod(3, 5), 1]
```

```
[Mod(1, 5)*x^2 + Mod(2, 5), 1; Mod(1, 5)*x^2 + Mod(3, 5), 1]
[Mod(1, 5)*x^4 + Mod(2, 5), 1; Mod(1, 5)*x^4 + Mod(3, 5), 1]
[Mod(1, 5)*x^8 + Mod(2, 5), 1; Mod(1, 5)*x^8 + Mod(3, 5), 1]
[Mod(1, 5)*x^16 + Mod(2, 5), 1; Mod(1, 5)*x^16 + Mod(3, 5), 1]

q=13
[Mod(1, 13)*x + Mod(5, 13), 1; Mod(1, 13)*x + Mod(8, 13), 1]
[Mod(1, 13)*x^2 + Mod(5, 13), 1; Mod(1, 13)*x^2 + Mod(8, 13), 1]
[Mod(1, 13)*x^4 + Mod(5, 13), 1; Mod(1, 13)*x^4 + Mod(8, 13), 1]
[Mod(1, 13)*x^8 + Mod(5, 13), 1; Mod(1, 13)*x^8 + Mod(8, 13), 1]
[Mod(1, 13)*x^16 + Mod(5, 13), 1; Mod(1, 13)*x^16 + Mod(8, 13), 1]

q=29
[Mod(1, 29)*x + Mod(12, 29), 1; Mod(1, 29)*x + Mod(17, 29), 1]
[Mod(1, 29)*x^2 + Mod(12, 29), 1; Mod(1, 29)*x^2 + Mod(17, 29), 1]
[Mod(1, 29)*x^4 + Mod(12, 29), 1; Mod(1, 29)*x^4 + Mod(17, 29), 1]
[Mod(1, 29)*x^8 + Mod(12, 29), 1; Mod(1, 29)*x^8 + Mod(17, 29), 1]
[Mod(1, 29)*x^16 + Mod(12, 29), 1; Mod(1, 29)*x^16 + Mod(17, 29), 1]

q=37
[Mod(1, 37)*x + Mod(6, 37), 1; Mod(1, 37)*x + Mod(31, 37), 1]
[Mod(1, 37)*x^2 + Mod(6, 37), 1; Mod(1, 37)*x^2 + Mod(31, 37), 1]
[Mod(1, 37)*x^4 + Mod(6, 37), 1; Mod(1, 37)*x^4 + Mod(31, 37), 1]
[Mod(1, 37)*x^8 + Mod(6, 37), 1; Mod(1, 37)*x^8 + Mod(31, 37), 1]
[Mod(1, 37)*x^16 + Mod(6, 37), 1; Mod(1, 37)*x^16 + Mod(31, 37), 1]

q=53
[Mod(1, 53)*x + Mod(23, 53), 1; Mod(1, 53)*x + Mod(30, 53), 1]
[Mod(1, 53)*x^2 + Mod(23, 53), 1; Mod(1, 53)*x^2 + Mod(30, 53), 1]
[Mod(1, 53)*x^4 + Mod(23, 53), 1; Mod(1, 53)*x^4 + Mod(30, 53), 1]
[Mod(1, 53)*x^8 + Mod(23, 53), 1; Mod(1, 53)*x^8 + Mod(30, 53), 1]
[Mod(1, 53)*x^16 + Mod(23, 53), 1; Mod(1, 53)*x^16 + Mod(30, 53), 1]
```

```
q=61
[Mod(1, 61)*x + Mod(11, 61), 1; Mod(1, 61)*x + Mod(50, 61), 1]
[Mod(1, 61)*x^2 + Mod(11, 61), 1; Mod(1, 61)*x^2 + Mod(50, 61), 1]
[Mod(1, 61)*x^4 + Mod(11, 61), 1; Mod(1, 61)*x^4 + Mod(50, 61), 1]
[Mod(1, 61)*x^8 + Mod(11, 61), 1; Mod(1, 61)*x^8 + Mod(50, 61), 1]
[Mod(1, 61)*x^16 + Mod(11, 61), 1; Mod(1, 61)*x^16 + Mod(50, 61), 1]
------------------------------------------------------------
\\m=3
? L2(q)=Mod(1,q)*x^2+Mod(1,q)
? L3(q)=Mod(1,q)*x^4+Mod(1,q)
? L4(q)=Mod(1,q)*x^8+Mod(1,q)
? L5(q)=Mod(1,q)*x^16+Mod(1,q)
? L6(q)=Mod(1,q)*x^32+Mod(1,q)

? forprime(q=3,100,if(q%16==9,print("q=",q);;print(factor(L2(q)));
print(factor(L3(q)));;print(factor(L4(q)));print(factor(L5(q)));
print(factor(L6(q))),))

q=41
[Mod(1, 41)*x + Mod(9, 41), 1; Mod(1, 41)*x + Mod(32, 41), 1]
[Mod(1, 41)*x + Mod(3, 41), 1; Mod(1, 41)*x + Mod(14, 41), 1;
 Mod(1, 41)*x + Mod(27, 41), 1; Mod(1, 41)*x + Mod(38, 41), 1]
[Mod(1, 41)*x^2 + Mod(3, 41), 1; Mod(1, 41)*x^2 + Mod(14, 41), 1;
 Mod(1, 41)*x^2 + Mod(27, 41), 1; Mod(1, 41)*x^2 + Mod(38, 41), 1]
[Mod(1, 41)*x^4 + Mod(3, 41), 1; Mod(1, 41)*x^4 + Mod(14, 41), 1;
 Mod(1, 41)*x^4 + Mod(27, 41), 1; Mod(1, 41)*x^4 + Mod(38, 41), 1]
[Mod(1, 41)*x^8 + Mod(3, 41), 1; Mod(1, 41)*x^8 + Mod(14, 41), 1;
 Mod(1, 41)*x^8 + Mod(27, 41), 1; Mod(1, 41)*x^8 + Mod(38, 41), 1]

q=73
[Mod(1, 73)*x + Mod(27, 73), 1; Mod(1, 73)*x + Mod(46, 73), 1]
[Mod(1, 73)*x + Mod(10, 73), 1; Mod(1, 73)*x + Mod(22, 73), 1;
 Mod(1, 73)*x + Mod(51, 73), 1; Mod(1, 73)*x + Mod(63, 73), 1]
```

```
[Mod(1, 73)*x^2 + Mod(10, 73), 1; Mod(1, 73)*x^2 + Mod(22, 73), 1;
 Mod(1, 73)*x^2 + Mod(51, 73), 1; Mod(1, 73)*x^2 + Mod(63, 73), 1]
[Mod(1, 73)*x^4 + Mod(10, 73), 1; Mod(1, 73)*x^4 + Mod(22, 73), 1;
 Mod(1, 73)*x^4 + Mod(51, 73), 1; Mod(1, 73)*x^4 + Mod(63, 73), 1]
[Mod(1, 73)*x^8 + Mod(10, 73), 1; Mod(1, 73)*x^8 + Mod(22, 73), 1;
 Mod(1, 73)*x^8 + Mod(51, 73), 1; Mod(1, 73)*x^8 + Mod(63, 73), 1]

q=89
[Mod(1, 89)*x + Mod(34, 89), 1; Mod(1, 89)*x + Mod(55, 89), 1]
[Mod(1, 89)*x + Mod(12, 89), 1; Mod(1, 89)*x + Mod(37, 89), 1;
 Mod(1, 89)*x + Mod(52, 89), 1; Mod(1, 89)*x + Mod(77, 89), 1]
[Mod(1, 89)*x^2 + Mod(12, 89), 1; Mod(1, 89)*x^2 + Mod(37, 89), 1;
 Mod(1, 89)*x^2 + Mod(52, 89), 1; Mod(1, 89)*x^2 + Mod(77, 89), 1]
[Mod(1, 89)*x^4 + Mod(12, 89), 1; Mod(1, 89)*x^4 + Mod(37, 89), 1;
 Mod(1, 89)*x^4 + Mod(52, 89), 1; Mod(1, 89)*x^4 + Mod(77, 89), 1]
[Mod(1, 89)*x^8 + Mod(12, 89), 1; Mod(1, 89)*x^8 + Mod(37, 89), 1;
 Mod(1, 89)*x^8 + Mod(52, 89), 1; Mod(1, 89)*x^8 + Mod(77, 89), 1]
 ------------------------------------------------------------
\\m=4.

? forprime(q=3,200,if(q%32==17,print("q=",q);;print(factor(L2(q)));
print(factor(L3(q)));print(factor(L4(q)));print(factor(L5(q)));
print(factor(L6(q))),))

q=17
[Mod(1, 17)*x + Mod(4, 17), 1; Mod(1, 17)*x + Mod(13, 17), 1]
[Mod(1, 17)*x + Mod(2, 17), 1; Mod(1, 17)*x + Mod(8, 17), 1;
 Mod(1, 17)*x + Mod(9, 17), 1; Mod(1, 17)*x + Mod(15, 17), 1]
[Mod(1, 17)*x + Mod(3, 17), 1; Mod(1, 17)*x + Mod(5, 17), 1;
 Mod(1, 17)*x + Mod(6, 17), 1; Mod(1, 17)*x + Mod(7, 17), 1;
 Mod(1, 17)*x + Mod(10, 17), 1; Mod(1, 17)*x + Mod(11, 17), 1;
 Mod(1, 17)*x + Mod(12, 17), 1; Mod(1, 17)*x + Mod(14, 17), 1]
[Mod(1, 17)*x^2 + Mod(3, 17), 1; Mod(1, 17)*x^2 + Mod(5, 17), 1;
```

```
 Mod(1, 17)*x^2 + Mod(6, 17), 1; Mod(1, 17)*x^2 + Mod(7, 17), 1;
 Mod(1, 17)*x^2 + Mod(10, 17), 1; Mod(1, 17)*x^2 + Mod(11, 17), 1;
 Mod(1, 17)*x^2 + Mod(12, 17), 1; Mod(1, 17)*x^2 + Mod(14, 17), 1]
[Mod(1, 17)*x^4 + Mod(3, 17), 1; Mod(1, 17)*x^4 + Mod(5, 17), 1;
 Mod(1, 17)*x^4 + Mod(6, 17), 1; Mod(1, 17)*x^4 + Mod(7, 17), 1;
 Mod(1, 17)*x^4 + Mod(10, 17), 1; Mod(1, 17)*x^4 + Mod(11, 17), 1;
 Mod(1, 17)*x^4 + Mod(12, 17), 1; Mod(1, 17)*x^4 + Mod(14, 17), 1]

q=113
[Mod(1, 113)*x + Mod(15, 113), 1; Mod(1, 113)*x + Mod(98, 113), 1]
[Mod(1, 113)*x + Mod(18, 113), 1; Mod(1, 113)*x + Mod(44, 113), 1;
 Mod(1, 113)*x + Mod(69, 113), 1; Mod(1, 113)*x + Mod(95, 113), 1]
[Mod(1, 113)*x + Mod(35, 113), 1; Mod(1, 113)*x + Mod(40, 113), 1;
 Mod(1, 113)*x + Mod(42, 113), 1; Mod(1, 113)*x + Mod(48, 113), 1;
 Mod(1, 113)*x + Mod(65, 113), 1; Mod(1, 113)*x + Mod(71, 113), 1;
 Mod(1, 113)*x + Mod(73, 113), 1; Mod(1, 113)*x + Mod(78, 113), 1]
[Mod(1, 113)*x^2 + Mod(35, 113), 1; Mod(1, 113)*x^2 + Mod(40, 113), 1;
 Mod(1, 113)*x^2 + Mod(42, 113), 1; Mod(1, 113)*x^2 + Mod(48, 113), 1;
 Mod(1, 113)*x^2 + Mod(65, 113), 1; Mod(1, 113)*x^2 + Mod(71, 113), 1;
 Mod(1, 113)*x^2 + Mod(73, 113), 1; Mod(1, 113)*x^2 + Mod(78, 113), 1]
[Mod(1, 113)*x^4 + Mod(35, 113), 1; Mod(1, 113)*x^4 + Mod(40, 113), 1;
 Mod(1, 113)*x^4 + Mod(42, 113), 1; Mod(1, 113)*x^4 + Mod(48, 113), 1;
 Mod(1, 113)*x^4 + Mod(65, 113), 1; Mod(1, 113)*x^4 + Mod(71, 113), 1;
 Mod(1, 113)*x^4 + Mod(73, 113), 1; Mod(1, 113)*x^4 + Mod(78, 113), 1]



 ---------------------------------------------------
\\m=5 .
forprime(q=3,200,if(q%64==33,print("q=",q);;print(factor(L2(q)));
print(factor(L3(q)));;print(factor(L4(q)));print(factor(L5(q)));
print(factor(L6(q))),))

q=97
```

```
[Mod(1, 97)*x + Mod(22, 97), 1; Mod(1, 97)*x + Mod(75, 97), 1]
[Mod(1, 97)*x + Mod(33, 97), 1; Mod(1, 97)*x + Mod(47, 97), 1;
 Mod(1, 97)*x + Mod(50, 97), 1; Mod(1, 97)*x + Mod(64, 97), 1]
[Mod(1, 97)*x + Mod(8, 97), 1; Mod(1, 97)*x + Mod(12, 97), 1;
 Mod(1, 97)*x + Mod(18, 97), 1; Mod(1, 97)*x + Mod(27, 97), 1;
 Mod(1, 97)*x + Mod(70, 97), 1; Mod(1, 97)*x + Mod(79, 97), 1;
 Mod(1, 97)*x + Mod(85, 97), 1; Mod(1, 97)*x + Mod(89, 97), 1]
[Mod(1, 97)*x + Mod(19, 97), 1; Mod(1, 97)*x + Mod(20, 97), 1;
 Mod(1, 97)*x + Mod(28, 97), 1; Mod(1, 97)*x + Mod(30, 97), 1;
 Mod(1, 97)*x + Mod(34, 97), 1; Mod(1, 97)*x + Mod(42, 97), 1;
 Mod(1, 97)*x + Mod(45, 97), 1; Mod(1, 97)*x + Mod(46, 97), 1;
 Mod(1, 97)*x + Mod(51, 97), 1; Mod(1, 97)*x + Mod(52, 97), 1;
 Mod(1, 97)*x + Mod(55, 97), 1; Mod(1, 97)*x + Mod(63, 97), 1;
 Mod(1, 97)*x + Mod(67, 97), 1; Mod(1, 97)*x + Mod(69, 97), 1;
 Mod(1, 97)*x + Mod(77, 97), 1; Mod(1, 97)*x + Mod(78, 97), 1]
[Mod(1, 97)*x^2 + Mod(19, 97), 1; Mod(1, 97)*x^2 + Mod(20, 97), 1;
 Mod(1, 97)*x^2 + Mod(28, 97), 1; Mod(1, 97)*x^2 + Mod(30, 97), 1;
 Mod(1, 97)*x^2 + Mod(34, 97), 1; Mod(1, 97)*x^2 + Mod(42, 97), 1;
 Mod(1, 97)*x^2 + Mod(45, 97), 1; Mod(1, 97)*x^2 + Mod(46, 97), 1;
 Mod(1, 97)*x^2 + Mod(51, 97), 1; Mod(1, 97)*x^2 + Mod(52, 97), 1;
 Mod(1, 97)*x^2 + Mod(55, 97), 1; Mod(1, 97)*x^2 + Mod(63, 97), 1;
 Mod(1, 97)*x^2 + Mod(67, 97), 1; Mod(1, 97)*x^2 + Mod(69, 97), 1;
 Mod(1, 97)*x^2 + Mod(77, 97), 1; Mod(1, 97)*x^2 + Mod(78, 97), 1]
-----------------------------------------------------------------
\\D{\'e}composition dans des sous_-corps de type II de  Q(\zeta_{64}).

F1(q)=Mod(1,q)*x^2-Mod(2,q)\\=Irr(Q,\sqrt{2})(polynome minimal de K2)

F2(q)=Mod(1,q)*x^4+Mod(-4,q)*x^2+Mod(2,q)\\=Irr(Q,\sqrt{2+\sqrt {2}})
(poly-minimal de K3)

F3(q)= Mod(1,q)*X^8+Mod(-8,q)*X^6+Mod(20,q)*X^4+ Mod(- 16,q)*X^2
+Mod(2,q)\\=Irr(Q,\sqrt{2+\sqrt {2+\sqrt {2}}}) (poly-minimal de K4)
```

```
F4(q)=Mod(1,q)*X^16+Mod(-16,q)*X^14+Mod(104,q)*X^12+Mod(-352,q)*X^10+
Mod(660,q)*X^8+Mod(-672,q)*X^6 +Mod(336,q)*X^4+Mod(-64,q)*X^2 +Mod(2,q)
\\=Irr(Q,\sqrt{2+\sqrt{2+\sqrt {2+\sqrt {2}}}}) (poly-minimal de K5)

\\m=2
forprime(q=3,50,if(q%8==5,print("q=",q);print(factor(F1(q)));
print(factor(F2(q)));print(factor(F3(q)));print(factor(F4(q))),))

q=5
Mat([Mod(1, 5)*x^2 + Mod(3, 5), 1])
Mat([Mod(1, 5)*x^4 + Mod(1, 5)*x^2 + Mod(2, 5), 1])
Mat([Mod(1, 5)*X^8 + Mod(2, 5)*X^6 + Mod(4, 5)*X^2 + Mod(2, 5), 1])
Mat([Mod(1, 5)*X^16 + Mod(4, 5)*X^14 + Mod(4, 5)*X^12 + Mod(3, 5)*X^10 +
 Mod(3, 5)*X^6 + Mod(1, 5)*X^4 + Mod(1, 5)*X^2 + Mod(2, 5), 1])

q=13
Mat([Mod(1, 13)*x^2 + Mod(11, 13), 1])
Mat([Mod(1, 13)*x^4 + Mod(9, 13)*x^2 + Mod(2, 13), 1])
Mat([Mod(1, 13)*X^8 + Mod(5, 13)*X^6 + Mod(7, 13)*X^4 + Mod(10, 13)*X^2 +
Mod(2, 13), 1])
Mat([Mod(1, 13)*X^16 + Mod(10, 13)*X^14 + Mod(12, 13)*X^10 + Mod(10, 13)*X^8 +
Mod(4, 13)*X^6 + Mod(11, 13)*X^4 + Mod(1, 13)*X^2 + Mod(2, 13), 1])

q=29
Mat([Mod(1, 29)*x^2 + Mod(27, 29), 1])
Mat([Mod(1, 29)*x^4 + Mod(25, 29)*x^2 + Mod(2, 29), 1])
Mat([Mod(1, 29)*X^8 + Mod(21, 29)*X^6 + Mod(20, 29)*X^4 + Mod(13, 29)*X^2 +
Mod(2, 29), 1])
Mat([Mod(1, 29)*X^16 + Mod(13, 29)*X^14 + Mod(17, 29)*X^12 +
Mod(25,29)*X^10 +Mod(22, 29)*X^8 + Mod(24, 29)*X^6 + Mod(17, 29)*X^4 +
Mod(23, 29)*X^2 + Mod(2, 29), 1])
```

```
q=37
Mat([Mod(1, 37)*x^2 + Mod(35, 37), 1])
Mat([Mod(1, 37)*x^4 + Mod(33, 37)*x^2 + Mod(2, 37), 1])
Mat([Mod(1, 37)*X^8 + Mod(29, 37)*X^6 + Mod(20, 37)*X^4 + Mod(21, 37)*X^2 +
Mod(2, 37), 1])
Mat([Mod(1, 37)*X^16 + Mod(21, 37)*X^14 + Mod(30, 37)*X^12 + Mod(18,
37)*X^10 +Mod(31, 37)*X^8 + Mod(31, 37)*X^6 + Mod(3, 37)*X^4 + Mod(10, 37)*X^2 +
 Mod(2, 37), 1])
------------------------------------------------------------------------
\\m=3
? forprime(q=3,100,if(q%16==9,print("q=",q);print(factor(F1(q)));
print(factor(F2(q)));print(factor(F3(q)));print(factor(F4(q))),))

q=41
[Mod(1, 41)*x + Mod(17, 41), 1; Mod(1, 41)*x + Mod(24, 41), 1]
[Mod(1, 41)*x^2 + Mod(15, 41), 1; Mod(1, 41)*x^2 + Mod(22, 41), 1]
[Mod(1, 41)*X^4 + Mod(37, 41)*X^2 + Mod(19, 41), 1; Mod(1, 41)*X^4 +
 Mod(37, 41)*X^2 + Mod(26, 41), 1]
[Mod(1, 41)*X^8 + Mod(33, 41)*X^6 + Mod(20, 41)*X^4 + Mod(25, 41)*X^2 +
 Mod(19, 41), 1; Mod(1, 41)*X^8 + Mod(33, 41)*X^6 + Mod(20, 41)*X^4 +
 Mod(25, 41)*X^2 + Mod(26, 41), 1]

q=73
[Mod(1, 73)*x + Mod(32, 73), 1; Mod(1, 73)*x + Mod(41, 73), 1]
[Mod(1, 73)*x^2 + Mod(30, 73), 1; Mod(1, 73)*x^2 + Mod(39, 73), 1]
[Mod(1, 73)*X^4 + Mod(69, 73)*X^2 + Mod(34, 73), 1; Mod(1, 73)*X^4 +
 Mod(69, 73)*X^2 + Mod(43, 73), 1]
[Mod(1, 73)*X^8 + Mod(65, 73)*X^6 + Mod(20, 73)*X^4 + Mod(57, 73)*X^2 +
 Mod(34, 73), 1; Mod(1, 73)*X^8 + Mod(65, 73)*X^6 + Mod(20, 73)*X^4 +
 Mod(57, 73)*X^2 + Mod(43, 73), 1]

q=89
[Mod(1, 89)*x + Mod(25, 89), 1; Mod(1, 89)*x + Mod(64, 89), 1]
```

```
[Mod(1, 89)*x^2 + Mod(23, 89), 1; Mod(1, 89)*x^2 + Mod(62, 89), 1]
[Mod(1, 89)*X^4 + Mod(85, 89)*X^2 + Mod(27, 89), 1; Mod(1, 89)*X^4 +
 Mod(85, 89)*X^2 + Mod(66, 89), 1]
[Mod(1, 89)*X^8 + Mod(81, 89)*X^6 + Mod(20, 89)*X^4 + Mod(73, 89)*X^2 +
 Mod(27, 89), 1; Mod(1, 89)*X^8 + Mod(81, 89)*X^6 + Mod(20, 89)*X^4 +
 Mod(73, 89)*X^2 + Mod(66, 89), 1]
?


------------------------------------------------------------------------
\\m=4
? forprime(q=3,400,if(q%32==17,print("q=",q);print(factor(F1(q)));
print(factor(F2(q)));print(factor(F3(q)));print(factor(F4(q))),))

q=17
[Mod(1, 17)*x + Mod(6, 17), 1; Mod(1, 17)*x + Mod(11, 17), 1]
[Mod(1, 17)*x + Mod(5, 17), 1; Mod(1, 17)*x + Mod(8, 17), 1;
 Mod(1, 17)*x +Mod(9, 17), 1; Mod(1, 17)*x + Mod(12, 17), 1]
[Mod(1, 17)*X^2 + Mod(3, 17), 1; Mod(1, 17)*X^2 + Mod(6, 17), 1;
 Mod(1, 17)*X^2 + Mod(7, 17), 1; Mod(1, 17)*X^2 + Mod(10, 17), 1]
[Mod(1, 17)*X^4 + Mod(13, 17)*X^2 + Mod(7, 17), 1; Mod(1, 17)*X^4 +
 Mod(13, 17)*X^2 + Mod(10, 17), 1; Mod(1, 17)*X^4 + Mod(13, 17)*X^2 +
 Mod(11, 17), 1; Mod(1, 17)*X^4 + Mod(13, 17)*X^2 + Mod(14, 17), 1]

q=113
[Mod(1, 113)*x + Mod(51, 113), 1; Mod(1, 113)*x + Mod(62, 113), 1]
[Mod(1, 113)*x + Mod(8, 113), 1; Mod(1, 113)*x + Mod(36, 113), 1;
 Mod(1, 113)*x + Mod(77, 113), 1; Mod(1, 113)*x + Mod(105, 113), 1]
[Mod(1, 113)*X^2 + Mod(6, 113), 1; Mod(1, 113)*X^2 + Mod(34, 113), 1;
 Mod(1, 113)*X^2 + Mod(75, 113), 1; Mod(1, 113)*X^2 + Mod(103, 113), 1]
[Mod(1, 113)*X^4 + Mod(109, 113)*X^2 + Mod(10, 113), 1; Mod(1, 113)*X^4 +
 Mod(109, 113)*X^2 + Mod(38, 113), 1; Mod(1, 113)*X^4 + Mod(109, 113)*X^2 +
 Mod(79, 113), 1; Mod(1, 113)*X^4 + Mod(109, 113)*X^2 + Mod(107, 113), 1]
```

```
q=241
[Mod(1, 241)*x + Mod(22, 241), 1; Mod(1, 241)*x + Mod(219, 241), 1]
[Mod(1, 241)*x + Mod(54, 241), 1; Mod(1, 241)*x + Mod(71, 241), 1;
 Mod(1, 241)*x + Mod(170, 241), 1; Mod(1, 241)*x + Mod(187, 241), 1]
[Mod(1, 241)*X^2 + Mod(52, 241), 1; Mod(1, 241)*X^2 + Mod(69, 241), 1;
 Mod(1, 241)*X^2 + Mod(168, 241), 1; Mod(1, 241)*X^2 + Mod(185, 241), 1]
[Mod(1, 241)*X^4 + Mod(237, 241)*X^2 + Mod(56, 241), 1; Mod(1, 241)*X^4 +
 Mod(237, 241)*X^2 + Mod(73, 241), 1; Mod(1, 241)*X^4 + Mod(237, 241)*X^2 +
 Mod(172, 241), 1; Mod(1, 241)*X^4 + Mod(237, 241)*X^2 + Mod(189, 241), 1]

q=337
[Mod(1, 337)*x + Mod(26, 337), 1; Mod(1, 337)*x + Mod(311, 337), 1]
[Mod(1, 337)*x + Mod(99, 337), 1; Mod(1, 337)*x + Mod(116, 337), 1;
 Mod(1, 337)*x + Mod(221, 337), 1; Mod(1, 337)*x + Mod(238, 337), 1]
[Mod(1, 337)*X^2 + Mod(97, 337), 1; Mod(1, 337)*X^2 + Mod(114, 337), 1;
 Mod(1, 337)*X^2 + Mod(219, 337), 1; Mod(1, 337)*X^2 + Mod(236, 337), 1]
[Mod(1, 337)*X^4 + Mod(333, 337)*X^2 + Mod(101, 337), 1; Mod(1, 337)*X^4 +
 Mod(333, 337)*X^2 + Mod(118, 337), 1; Mod(1, 337)*X^4 + Mod(333, 337)*X^2 +
 Mod(223, 337), 1; Mod(1, 337)*X^4 + Mod(333, 337)*X^2 + Mod(240, 337), 1]
?
```

Bibliographie

[1] C. Batut, H. Cohen, et M. Olivier, *User s Guide to PARI-GP,* Université Bordeaux, 351 Cours de la Libération, May 1995. Obtainable via anonymous ftp from megrez.math.u-bordeaux.fr.

[2] Z. Borevitch et I. Shafarevich: *Théorie des nombres.* Gauthiers-Villard (1967).

[3] Y. Bugeaud, G. Hanrot, *Un nouveau critère pour l'équation de Catalan,* Mathematika, 47, 2000, p. 63-73.

[4] Esmonde, Jody ; Murty, M. Ram, *Problems in algebraic number theory*, Springer, New York, (1999).

[5] K. Feng, *On the first factor of the class number of a cyclotomic field,* Proc. Amer. Math. Soc. V. 84, N. 4 (1982).

[6] S. Gannoukh, *Décomposition d'un premier* $q \equiv 1+2^m \pmod{2^{m+1}}$ *dans les sous-extensions de* $\mathbb{Q}(\zeta_{2^n})$, $n, m \geq 2$; C. R. Math. Rep. Acad. Sci. Canada, 25 (2003), no. 1, p. 7–12.

[7] H. Hasse, *Vorlesungen über Klassenkörpertheorie,* Physica-Verlag. Würzburg, 1967.

[8] J. J. Janusz: *Algebraic Number fields.* Academic Press, (1997).

[9] E. Kummer, *Bestimmung der Anzahl nicht äquivalenter Classen für die aus* λ *ten Wurzelp der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben,* J. Reine Angew. Math., V. 40, 1850, pp. 43-116.

[10] S. Lang, *Algebraic number theory.* Addisson-Wesley: Reading, MA, 1970.

[11] D. Lehmer, *Prime factors of cyclotomic class numbers*, Math. comp. Vol. 31, No. (1977), p. 599-607.

[12] D. Lehmer J. M. Masley, *Table of cyclotomic class numbers h*(p) and their factors for 200 < p < 521* , Math. comp. Vol. 32, N. (1978), p. 577-582.

[13] V. A. Lebesgue, *Dimostrazione dell'irreduttibilità dell'equazione formata con le radici primitive dell'unità*, Ann. Mat. Pura Appl., v.2, 1859, pp. 232-237.

[14] T. Lepistö, *On the growth of the first factor of the class number of the prime cyclotomic field*, Ann. Acad. Sci. Fenn. Ser. A1 Math., No. 577 (1974), 21 pp.

[15] R. L. Long, *Algebraic number theory*, Monographs and textbooks in pure and applied mathematics; 41, (1977).

[16] S. Louboutin, *Majorations explicites de | L(1,χ) | (suite),* C. R. Acad. Sci. Paris 323 (1996),p. 443-446. MR 93m:11084.

[17] J. M. Masley, *On the first factor of the class number of the prime Cyclotomic fields*, Journal of number theory 10, p. 273-290 (1978).

[18] T. Metsänkylä, *On prime factors of the relative class numbers of cyclotomic fields,* Ann. Univ. Turku. Ser. A I, No. 149, 1971, 8 pp.

[19] M. Mignotte, *A criterion on Catalan's equation,* J. Numb. Th., 52, 1995, p. 280-283.

[20] M. Mignotte, *On the computation of the factor h^- of certain CM-fields*, AAECC 13, Honolulu, Nov. 1999.

[21] M. Mignotte, *Mathematics for Computer algebra*, Springer, New York, (1992).

[22] M. Newman, *A table of the first factor for prime cyclotomic fields,* Math. comp. 24 (1970), p. 215-219.

[23] Mihăilescu, Preda, *Primary cyclotomic units and proof of Catalan's conjecture*, J. Reine angew. Math., to appear.

[24] B. Oriat: *Sur l'article de H. W. Leopoldt intitulé Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkorper.* Séminaire. Université de Besançon, (1974-1975).

[25] P. Samuel: *Théorie algébrique des nombres.* Hermann, Paris. (1967).

[26] W. Schwarz, *A note on Catalan's equation,* Acta Arith., 29, 1976, p. 197-209.

[27] R. Steiner, *Class number bound and Catalan equation*, Math. comp. V 67, N 223, (1998) p. 1317-1322.

[28] M. A. Shokrollahi, *Relative class number of imaginary abelien fields of prime conducteur below 10000* Math. comp. V 68, N 228,(1999) p. 1717-1728.

[29] L. C. Washington, *Introduction to cyclotomic fields,* 2nd ed., Graduate Texts in Mathematics **83** , Springer, New York, 1997.