N° d'ordre : 1830

THESE

Présentée à

L'UNIVERSITE BORDEAUX I

ECOLE DOCTORALE DE MATHEMATIQUES ET INFORMATIQUE

Par **Xavier-François Roblot**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITE : MATHEMATIQUES PURES

Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon

---

Soutenue le 26 juin 1997

Après avis de :

MM.	G. GRAS	Professeur	Université de Franche-Comté	**Rapporteurs**
	D. HAYES	Professeur	Université du Massachusetts	

Devant la commission d'examen formée de :

MM.	Ph. CASSOU-NOGUES	Professeur	Université Bordeaux I	**Président**
	F. DIAZ y DIAZ	Professeur	Université Bordeaux I	**Examinateurs**
	D. FORD	Professeur	Université Concordia	
	M. OLIVIER	Professeur	Université Bordeaux I	
	D. SOLOMON	Chargé de Recherche	King's College London	**Rapporteur**

- 1997 -

Arrivé au terme de ces trois années de thèse, je me dois de remercier tous ceux et celles qui m'ont aidé et soutenu.

Tout d'abord ma gratitude va à mes deux directeurs de thèse, Francisco Diaz y Diaz et Michel Olivier, qui m'ont accompagné durant ce travail avec toutes leurs disponibilités et leurs compétences. Je les remercie tout particulièrement d'avoir su diriger mes recherches tout en me laissant une grande liberté de manœuvre.

Je tiens à remercier également Henri Cohen et Jacques Martinet pour l'atmosphère conviviale de recherche qu'ils ont su créer au sein du laboratoire A2X, notamment dans le petit groupe de théorie algorithmique des nombres auquel j'ai eu la chance d'appartenir.

Je suis très sensible à l'honneur que m'ont fait Georges Gras et David Hayes qui ont accepté d'être mes rapporteurs. Et je tiens à exprimer ma plus sincère gratitude à ce dernier ainsi qu'à David Solomon pour l'intérêt constant qu'ils ont porté à mon travail.

Je remercie également Philippe Cassou-Noguès et David Ford qui ont accepté d'être membres de mon jury.

Je suis redevable à Mauricette Jaubert et Daniel Ynbourg pour le soin et la diligence qu'ils ont apporté à l'impression de cette thèse, et à Emmanuel Tollis pour son aide concernant le calcul des fonctions L.

Finalement, j'exprime toute mon amitié et ma sympathie à tous mes camarades de travail de la salle 100 et d'ailleurs, à mes amis et à mes parents.

SOMMAIRE

INTRODUCTION

Ce travail de thèse s'inscrit dans deux orientations disctinctes : d'une part, le premier chapitre décrit une nouvelle méthode de factorisation des polynômes dans un corps de nombres, ainsi qu'une méthode de factorisation des polynômes modulo un idéal premier. Ce chapitre s'accompagne d'un grand nombre d'applications et d'exemples. D'autre part, les chapitres 2 et 3 sont dévolus à la description d'une méthode explicite de construction de certains corps de classes de rayon via les conjectures de Stark, le chapitre 3 étant plus particulièrement consacré à la construction du corps de classes de Hilbert ; le dernier chapitre donne quelques applications ou remarques concernant les exemples construits grâce aux méthodes développées dans les deux chapitres précédents.

Ces dernières années ont vu l'apparition de multiples algorithmes fournissant des réponses satisfaisantes aux problèmes effectifs de base de la théorie algorithmique des corps de nombres (calcul du discriminant, d'une base d'entiers, décomposition des nombres premiers, calcul d'un système d'unités fondamentales, du groupe des classes...). Ainsi, il est possible de calculer tous ces objets dans des corps de nombres de discriminant raisonnable allant jusqu'au degré 25.

Néanmoins, il est apparu qu'on atteignait les limites actuelles de ces algorithmes et des ordinateurs et que, si on souhaitait s'aventurer plus loin, il devenait nécessaire de ne plus considérer uniquement des extensions de $\mathbb{Q}$, mais de travailler désormais avec des extensions relatives. C'est ainsi qu'ont commencé à apparaître des généralisations des algorithmes absolus au cas relatif, et avec l'arrivée de telles méthodes, des corps de nombres de degré de plus en plus grand sont devenus accessibles ; on peut à présent s'attaquer à des corps imprimitifs de degré 100 et plus.

Le premier chapitre de cette thèse s'inscrit dans ce travail de généralisation des algorithmes absolus au cas relatif en présentant un nouvel algorithme de factorisation des polynômes dans un corps de nombres, ainsi qu'une généralisation de l'algorithme de Berlekamp de factorisation des polynômes modulo un nombre premier, aux idéaux premiers d'un corps de nombres. L'algorithme de factorisation dans un corps de nombres utilise le fait que tout corps de nombres k peut se plonger dans $\mathbb{Q}_p$ pour certains nombres premiers p et les méthodes connues de factorisation p-adique. Le point crucial ici étant de retranscrire les informations obtenues dans $\mathbb{Q}_p$ en des informations dans k ; on utilise pour cela la méthode de réduction LLL appliquée à certains réseaux.

Les méthodes usuelles impliquent de factoriser sur $\mathbb{Q}$ un polynôme de degré égal au produit du degré du polynôme à factoriser dans k par le degré du corps de nombres k, et donc, ne sont plus vraiment performantes dès que le degré du polynôme ou du corps de nombres augmente trop. En revanche, l'algorithme présenté ici n'obéit pas à de telles contraintes et a permis de calculer la factorisation de polynôme de degré 20 sur un corps de même degré en un temps raisonnable (quelques minutes).

L'algorithme de factorisation des polynômes dans un corps de nombres modulo un idéal premier est une généralisation de l'algorithme dû à Berlekamp ; on a simplement inclus le cas pair qui n'est pas pris en considération dans le travail initial de Berlekamp.

Après avoir exposé ces deux algorithmes, on illustre leur utilité par de multiples applications et exemples. En effet, la factorisation des polynômes que ce soit dans un corps de nombres ou modulo un idéal premier est un outil essentiel. Citons entre autres : calcul des automorphismes d'un corps, décomposition des idéaux premiers dans une extension relative, calcul d'une pseudo-base de l'anneau des entiers d'un corps de nombres vu comme module sur l'anneau des entiers d'un sous-corps, test d'inclusion à isomorphisme près... Ce chapitre se termine par une présentation de l'algorithme ROUND 4 relatif.

L'idée selon laquelle les valeurs d'une fonction zêta (ou d'une fonction L) en certains points entiers fournit de nombreuses informations sur la structure à laquelle elle est attachée n'est pas nouvelle. Ainsi, il existe de nombreuses constructions permettant de construire de telles fonctions à partir de corps de nombres, courbes elliptiques, formes modulaires *etc*...

Les conjectures de Stark reposent sur l'idée que les fonctions L attachées aux caractères d'un groupe des classes de rayon contiennent non seulement des informations sur le corps de base lui-même, mais aussi sur l'extension abélienne de ce corps associée à ce groupe par la théorie du corps de classes. C'est en quelque sorte une généralisation du fait que certaines fonctions L de Dirichlet sur $\mathbb{Q}$ font apparaître des racines de l'unité qui sont des éléments privilégiés des corps cyclotomiques.

Une application immédiate (et utilisée d'ailleurs par Stark lui-même) est de se servir de ces conjectures pour trouver des éléments générateurs des corps de classes de rayon, et de fournir ainsi une réponse au XIIe problème de Hilbert. Un premier obstacle survient lorsque les fonctions L considérées ont un zéro d'ordre strictement plus grand que 1 au point $s = 0$. En effet, dans ce cas, ce n'est plus une mais plusieurs unités que fait apparaître la conjecture à travers leur régulateur ; il n'est alors pas possible de les dissocier. C'est pourquoi on est obligé de supposer que le corps de base sur lequel on travaille est totalement réel. Pour des raisons analogues, on est aussi forcé de se restreindre aux corps de classes de rayon non ramifiés aux places infinies.

Après avoir rappelé une forme des conjectures de Stark dans le cas abélien, on est donc amené à faire ces deux restrictions concernant la signature du corps de base k et celle de son extension abélienne L. Avec ces restrictions, la conjecture de Stark permet de construire explicitement un élément primitif de l'extension, fournissant ainsi une réponse explicite mais conjecturale. L'idée est d'appliquer la conjecture à une extension quadratique K/L abélienne sur k et vérifiant certaines conditions aux places finies et infinies. Cette méthode reposant sur des conjectures et des calculs approchés, on développe dans ce même chapitre une procédure de vérification de la construction afin de pouvoir certifier les résultats obtenus. On utilise également la théorie de Kummer afin de construire des corps de classes de rayon ramifiés aux places infinies à partir de ceux construits par les conjectures de Stark. On présente aussi dans ce chapitre un exemple de construction et de vérification, ainsi qu'une section dévolue à une restriction technique concernant cette méthode.

Le troisième chapitre est consacré à l'application du chapitre précédent pour la construction du corps de classes de Hilbert de corps totalement réels. En effet, de nombreux points de la construction se simplifient notablement dans ce cas. On expose aussi une autre construction du corps de classes de Hilbert quand le nombre de classes vaut 2 par la théorie de Kummer. Ces méthodes ont été utilisées pour calculer explicitement le corps de classes de Hilbert des premiers corps totalement réels de degré 2, 3 et 4 (voir les tables données en annexe).

Le dernier chapitre montre ce que pourrait être une exploitation de ces tables ou de cette méthode. Cependant, il est à noter que les concepts et les résultats qui y sont exposés restent très simples et ne font appel qu'à des outils élémentaires.

En conclusion, l'algorithme de factorisation présenté dans cette thèse étant une généralisation de l'algorithme sur $\mathbb{Q}$, il est vraisemblable qu'il ne pourra être notablement amélioré que quand de nouvelles méthodes plus efficaces auront été découvertes pour l'algorithme absolu. Il est certes possible d'utiliser la factorisation modulo un idéal premier puis un relèvement de Hensel plutôt que la factorisation p-adique ; cependant, il est apparu après de multiples essais que la méthode p-adique était de loin préférable. Néanmoins, cette option reste une possibilité future pour d'éventuelles améliorations.

Pour ce qui est de la méthode de construction de corps de classes de rayon via les conjectures de Stark, beaucoup de choses restent encore à découvrir. Tout d'abord, il reste à établir l'existence du corps K nécessaire à la construction (voir section 2.7) ou de trouver des contre-exemples. Il serait également utile de trouver des nouvelles méthodes de réduction lors des calculs afin d'éviter l'explosion des nombres à gérer. Il reste à régler aussi les autres cas, *ie* quand le corps de base n'est plus totalement réel. Cela suppose de travailler avec des fonctions L dont le zéro en $s = 0$ est d'ordre strictement plus grand que 1. Pour de telles hypothèses, les conjectures sur les fonctions L font apparaître plusieurs unités et le problème se pose de comment séparer ces unités. De surcroît, dans un tel cas, de multiples formes de la conjecture existent et il serait utile de procéder à des constructions explicites afin de tester ces différentes formulations. Un autre axe de recherche dans ce domaine est de travailler non plus avec des fonctions L complexes, mais de considérer plutôt des fonctions p-adiques. Il semble que dans ce domaine, du point de vue algorithmique, beaucoup reste à faire.

Pour finir, il reste évidemment à démontrer ces conjectures. Si les outils algorithmiques ne sont pas d'une grande aide pour cela, ils permettent néanmoins de calculer explicitement des exemples sur lesquels il est alors possible de chercher quelques indices pour cette démonstration. En ce sens, les tables construites peuvent aussi avoir leur utilité.

CHAPITRE 0

QUELQUES NOTATIONS, DÉFINITIONS ET RÉSULTATS

0.1. Groupes et caractères

Les références pour cette section sont : [**26**] pour le début et [**5**], Algebraic Supplement, pour la théorie des caractères.

Soit G un groupe, l'*élément neutre* de G est noté 1_G ou plus simplement 1 quand il n'y a pas de risque de confusion. On désigne par $|G|$ le *cardinal* de G. Le *centre* de G, noté $Z(G)$, est l'ensemble des éléments de G qui commutent avec tous les autres éléments. Pour un sous-groupe distingué H de G, on dénote par $(G : H)$ l'*indice* de H dans G.

Soit G un groupe abélien de type fini ; pour un nombre premier p, le *p-rang* de G, noté $r_p(G)$, est le nombre de composantes cycliques de G d'ordre divisible par p. Il ne dépend pas du choix de la décomposition de G en composantes cycliques et, bien sûr, tout nombre premier p divise l'ordre d'une composante cyclique infinie.

On a également la formule :

$$(G : G^p) = p^{r_p(G)},$$

et le nombre de sous-groupes d'indice p de G est :

$$\frac{p^{r_p(G)} - 1}{p - 1}.$$

Soit G un groupe abélien fini ; on désigne par $\hat{G}$ le *groupe des caractères* de G, *ie* des homomorphismes de groupes de G dans $\mathbb{C}^\times$. C'est un groupe isomorphe à G. Les deux formules de sommation suivantes sont très utiles. Pour tout caractère χ sur G, on a :

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| \text{ si } \chi = 1_{\hat{G}} \\ 0 \text{ sinon} \end{cases}$$

et pour tout élément g de G :

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| \text{ si } g = 1_G \\ 0 \text{ sinon} \end{cases}$$

Soit H un sous-groupe de G ; alors tous les caractères de H peuvent être étendus à des caractères de G et ceci de $(G : H)$ façons distinctes. De même, on peut relever tout caractère du groupe quotient G/H en un caractère de G de manière canonique. Pour un caractère fixé de G/H, le caractère obtenu s'appelle alors le *caractère induit*. Un caractère de G est dit *primitif* s'il n'existe pas de sous-groupe non trivial H de G et de caractère de G/H dont il soit le caractère induit.

0.2. Corps de nombres

Les références pour cette section sont : [**5**], [**29**] et [**34**].

Soit k un *corps de nombres*, *ie* une extension algébrique finie de $\mathbb{Q}$. On désigne par $[k : \mathbb{Q}]$ son *degré*. L'anneau des *entiers algébriques* de k est noté $\mathcal{O}_k$; c'est un anneau de Dedekind dont le discriminant est appelé le *discriminant* du corps k et on le désigne par d_k. On note $\mathcal{D}_k$ la *différente* de k ; c'est le dual de $\mathcal{O}_k$ pour la forme trace et sa norme absolue vaut $|d_k|$. On appelle *signature* du corps k le couple d'entiers (r_1, r_2) tel que $r_1 + 2r_2 = [k : \mathbb{Q}]$ où r_1 est le nombre de plongements réels de k et $2r_2$ le nombre de plongements complexes. A chaque plongement v de k dans $\mathbb{C}$, on associe une *place infinie* notée $|.|_v$

Le groupe des *idéaux fractionnaires* de k est noté I_k et le sous-groupe des *idéaux principaux* P_k. Le groupe quotient I_k/P_k est un groupe fini noté Cl_k et appelé le *groupe des classes* de k ; son cardinal h_k est le *nombre de classes*. Pour tout idéal fractionnaire $\mathfrak{a}$ de k, on désigne par $\mathcal{N}\mathfrak{a}$ la *norme absolue* de cet idéal définie comme le cardinal du quotient $(\mathcal{O}_k/\mathfrak{a})$ si l'idéal $\mathfrak{a}$ est entier et étendue par multiplicativité à tous les idéaux. A chaque idéal premier $\mathfrak{p}$, on associe une *valuation* $\mathrm{val}_\mathfrak{p}$, une *place finie* $|.|_\mathfrak{p}$ et finalement le corps *complété* de k en cette place $k_\mathfrak{p}$.

Le groupe des éléments inversibles de $\mathcal{O}_k$ est appelé le groupe des *unités* de k et noté E_k. C'est un $\mathbb{Z}$-module (multiplicatif) de rang $r := r_1 + r_2 - 1$ dont la partie de torsion W_k est formée par les *racines de l'unité* contenues dans k.

Soit K une extension finie de k. On note $\mathfrak{d}_{K/k}$ le *discriminant relatif* ; c'est un idéal entier de k. On désigne par $N_{K/k}$ et $T_{K/k}$ la *norme* et la *trace* de K sur k. Pour tout idéal premier $\mathfrak{P}$ de K, l'idéal $\mathfrak{p} := \mathfrak{P} \cap k$ est un idéal premier de k. On dit que $\mathfrak{P}$ est *au-dessus* de $\mathfrak{p}$ et que $\mathfrak{p}$ est *au-dessous* de $\mathfrak{P}$; on utilise la même terminologie pour les places infinies. On définit l'*indice de ramification* $e_\mathfrak{P}(K/k)$, et le *degré résiduel* $f_\mathfrak{P}(K/k)$, respectivement par :

$$e_\mathfrak{P}(K/k) := \mathrm{val}_\mathfrak{P}(\mathfrak{p}\mathcal{O}_K)$$

et :

$$\mathcal{N}\mathfrak{P} = \mathcal{N}\mathfrak{p}^{f_\mathfrak{P}(K/k)}.$$

Si cette extension est galoisienne, on désigne par $\mathrm{Gal}(K/k)$ son *groupe de Galois*. Dans ce cas, l'indice de ramification et le degré résiduel ne dépendent que de $\mathfrak{p}$ et on les note plutôt $e_\mathfrak{p}(K/k)$ et $f_\mathfrak{p}(K/k)$, ou plus simplement $e_\mathfrak{p}$ et $f_\mathfrak{p}$ quand il n'y a pas de risque de confusion. Pour w une place de K, l'ensemble des éléments de $\mathrm{Gal}(K/k)$ qui stabilise cette place forme le *groupe de décomposition* de w ; on le note $D_w(K/k)$. Dans le cas où l'extension est *abélienne*, il ne dépend que de la place v de k au-dessous de w et on écrit plutôt $D_v(K/k)$ ou plus simplement D_v quand il n'y a pas de risque de confusion.

0.3. Théorie du corps de classes

Les références pour cette section sont : [**34**] et [**43**].

Soit $\mathfrak{m}$ un *module* de k, *ie* le produit formel d'un idéal entier de k noté $\mathfrak{m}_0$ et d'un ensemble de places infinies réelles de k noté $\mathfrak{m}_\infty$. On note $I_k(\mathfrak{m})$ le groupe des idéaux fractionnaires de k premiers avec $\mathfrak{m}_0$. Le sous-groupe des idéaux engendrés par un élément *congru multiplicativement à 1 modulo* $\mathfrak{m}$ est désigné par $P_k(\mathfrak{m})$. Le groupe quotient $\mathrm{Cl}_k(\mathfrak{m}) := I_k(\mathfrak{m})/P_k(\mathfrak{m})$ est appelé le *groupe des classes de rayon modulo* $\mathfrak{m}$. Les sous-groupes de $\mathrm{Cl}_k(\mathfrak{m})$ sont appelés les *groupes de congruence modulo* $\mathfrak{m}$. Pour un idéal $\mathfrak{a}$ de k premier avec $\mathfrak{m}_0$, $[\mathfrak{a}]_\mathfrak{m}$ désigne la classe de $\mathfrak{a}$ dans $Cl_k(\mathfrak{m})$.

Soit $\mathfrak{n}$ un module divisant $\mathfrak{m}$, *ie* $\mathfrak{n}_0 \mid \mathfrak{m}_0$ et $\mathfrak{n}_\infty \subset \mathfrak{m}_\infty$; il existe une surjection canonique notée $s_{\mathfrak{m},\mathfrak{n}}$ de $\mathrm{Cl}_k(\mathfrak{m})$ sur $\mathrm{Cl}_k(\mathfrak{n})$. Un module $\mathfrak{m}$ est appelé un *conducteur* s'il n'admet pas de diviseur strict $\mathfrak{n}$ pour lequel cette surjection est un isomorphisme. A chaque groupe de congruence $\mathcal{H}$ modulo $\mathfrak{m}$ et à chaque diviseur $\mathfrak{n}$ de $\mathfrak{m}$, on peut associer le sous-groupe $\mathcal{H}_\mathfrak{n}$ modulo $\mathfrak{n}$ défini par $\mathcal{H}_\mathfrak{n} := s_{\mathfrak{m},\mathfrak{n}}(\mathcal{H})$. On dit que le module $\mathfrak{m}$ est le *conducteur* du groupe de congruence $\mathcal{H}$ s'il n'existe pas de diviseur strict $\mathfrak{n}$ de $\mathfrak{m}$ tel que $\mathrm{Cl}_k(\mathfrak{m})/\mathcal{H}$ soit isomorphe à $\mathrm{Cl}_k(\mathfrak{n})/\mathcal{H}_\mathfrak{n}$ par l'application induite par $s_{\mathfrak{m},\mathfrak{n}}$.

La théorie du corps de classes permet d'associer à un couple $(\mathcal{H}, \mathfrak{m})$ où $\mathcal{H}$ est un groupe de congruence modulo $\mathfrak{m}$, une extension abélienne finie de k. Le *conducteur* de cette extension est le conducteur du groupe $\mathcal{H}$.

Cette correspondance est bijective si on se restreint aux couples $(\mathcal{H}, \mathfrak{m})$ où $\mathcal{H}$ est un groupe de congruence de conducteur $\mathfrak{m}$.

L'extension associée au couple $(1, \mathfrak{m})$ est appelée le *corps de classes de rayon modulo* $\mathfrak{m}$ et noté $k(\mathfrak{m})$. En particulier, l'extension associée au couple $(1, \mathcal{O}_k)$ est le *corps de classes de Hilbert*, noté H_k.

Soit K une extension abélienne de k de conducteur $\mathfrak{f}$. Les idéaux premiers ramifiées dans K/k sont exactement les idéaux premiers divisant $\mathfrak{f}_0$; les places infinies réelles de k qui deviennent complexes dans K sont exactement celles contenues dans $\mathfrak{f}_\infty$. Le *groupe des normes* de K/k est le groupe engendré par $P_k(\mathfrak{f})$ et les normes des idéaux de K premiers avec $\mathfrak{f}_0\mathcal{O}_K$. En quotientant ce groupe par $P_k(\mathfrak{f})$, on obtient le groupe de congruence $\mathcal{H}$ associé à K modulo $\mathfrak{f}$. Pour un idéal premier $\mathfrak{p}$ non ramifié dans K/k, son degré résiduel dans l'extension K/k est alors l'ordre de sa classe dans $\mathrm{Cl}_k(\mathfrak{f})/\mathcal{H}$.

Le groupe $Cl_k(\mathfrak{f})/\mathcal{H}$ est isomorphe au groupe de Galois de K/k, l'isomorphisme étant donné par l'*application d'Artin*. On définit cette application pour un idéal premier $\mathfrak{p}$ non ramifié dans K/k en lui associant son *Frobenius* dans $\mathrm{Gal}(K/k)$, noté $\sigma_\mathfrak{p}$ et défini comme l'unique élément de ce groupe de Galois tel que :

$$\sigma_\mathfrak{p}(\alpha) \equiv \alpha^{\mathcal{N}\mathfrak{p}} \pmod{\mathfrak{P}}$$

pour tout $\alpha \in K$, où $\mathfrak{P}$ est un idéal premier de K au-dessus de $\mathfrak{p}$. Ce Frobenius est également un générateur du groupe de décomposition $D_\mathfrak{p}(K/k)$. On étend cette application à tous les idéaux de $I_k(\mathfrak{f})$ par multiplicativité.

CHAPITRE 1

FACTORISATION DES POLYNÔMES DANS UN CORPS DE NOMBRES ET MODULO UN IDÉAL PREMIER

La factorisation des polynômes à coefficients rationnels est un outil indispensable de la théorie algorithmique des nombres. Elle intervient dans de multiples problèmes concernant l'étude des corps de nombres sur $\mathbb{Q}$. Avec le développement des méthodes relatives (*cf* [**9**], [**11**], [**12**], [**15**]...), la factorisation des polynômes sur un corps de nombres devient de même un outil primordial.

On présente dans ce chapitre un nouvel algorithme s'inspirant directement de celui utilisé sur $\mathbb{Q}$ et plus perfomant en général que ceux déjà existant (*cf* [**8**], [**25**], [**36**], [**44**] et [**55**]). Cet algorithme utilisant la factorisation p-adique, les deux premières sections sont consacrées à la présentation de deux méthodes de factorisation dans $\mathbb{Q}_p[X]$. On décrit également une méthode de factorisation des polynômes modulo un idéal premier suivant la technique proposée par Berlekamp (*cf* [**4**]) pour les corps $\mathbb{F}_p$.

Finalement, on termine ce chapitre par un certain nombre d'exemples d'applications de ces algorithmes.

1.1. Factorisation p-adique : méthode de Buchmann-Lenstra

Soit S le polynôme à coefficients dans $\mathbb{Q}_p$ que l'on cherche à factoriser. La première chose à faire est de multiplier S par un entier p-adique assez grand de manière à ce que ses coefficients soient des entiers p-adiques. Ainsi, on suppose désormais que le polynôme S est à coefficients entiers.

Comme S est connu par une approximation de ses coefficients dans $\mathbb{Z}[X]$, on peut aussi supposer sans perte de généralité que S est à coefficients entiers et irréductible dans $\mathbb{Z}[X]$ (*cf* [**25**] ou [**8**] section 3.5 pour une méthode de factorisation sur $\mathbb{Z}$). De plus, comme S est irréductible dans $\mathbb{Q}[X]$, il est séparable dans $\mathbb{Q}_p[X]$.

On note θ une racine de S dans une clôture algébrique fixée de $\mathbb{Q}$. La factorisation de S dans $\mathbb{Q}_p[X]$ est intimement liée à la décomposition du nombre premier p dans le corps de nombres $k := \mathbb{Q}(\theta)$.

On fixe un entier $n \geq 1$ qui représente la précision voulue sur les coefficients des facteurs irréductibles de S (*i.e.* on cherche une approximation de ses coefficients modulo p^n).

Soit $\mathcal{O}$ un ordre p-maximal de k obtenu par exemple à l'aide des algorithmes Round 2 ou Round 4. On commence par décomposer le nombre premier p dans cet ordre en utilisant la méthode décrite dans [**8**] section 6.2. On obtient :

$$p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

où les idéaux $\mathfrak{p}_i$ sont premiers (dans $\mathcal{O}$) et deux à deux distincts. De plus, on connait une représentation de ces idéaux sous la forme :

$$\mathfrak{p}_i := p\mathcal{O} + \gamma_i\mathcal{O}$$

pour un élément $\gamma_i \in \mathcal{O}$.

En appliquant le lemme de Nakayama au $\mathbb{F}_p$-espace vectoriel $\mathcal{O}/\mathfrak{p}_i^{e_i}$, on déduit que le quotient $\mathcal{A}_i := \mathcal{O}/\mathfrak{p}^{ne_i}$ est un $\mathbb{Z}/p^n\mathbb{Z}$-module libre. En particulier, on peut en calculer une base $\{\alpha_1, \ldots, \alpha_r\}$ (*cf* [**8**] section 2.3).

La multiplication par θ étant un homomorphisme de $\mathcal{A}_i$, on note $S_i(X)$ son polynôme caractéristique sur cette base. C'est aussi le polynôme caractéristique d'un élément primitif de $\mathcal{A}_i$ qui, une fois relevé dans $\mathbb{Z}$, donne une approximation à p^n près d'un facteur irréductible de S dans $\mathbb{Z}_p[X]$.

Il suffit alors de procéder de même pour tout les idéaux $\mathfrak{p}_i$ au-dessus de p pour en déduire des approximations de tous les facteurs irréductibles de S dans $\mathbb{Z}_p[X]$ (*cf* [**53**] section 1.4 pour un algorithme complet).

1.2. Factorisation p-adique : méthode Round 4

L'algorithme Round 4 est un algorithme compliqué mais très efficace qui calcule un ordre p maximal de k pour tout premier p en "cassant" l'ordre de départ par des méthodes p-adiques. Il peut aussi être utilisé pour scinder le polynôme S afin de calculer sa factorisation p-adique. On peut trouver un exposé complet de l'algorithme Round 4 et de ses applications dans [**20**], [**21**] et [**22**]. On y reviendra également dans la dernière section en discutant de sa généralisation au cas relatif.

Le critère suivant est déterminant pour la suite :

Proposition 1.1 (Critère d'irréductibilité)**.** *Soit T un polynôme de $\mathbb{Z}_p[X]$ tel que :*

$$T(X) \equiv t(X)^e \pmod{p}$$

où t est un polynôme irréductible modulo p.

Si $e = 1$ ou si T est un polynôme d'Eisenstein en t, alors T est un polynôme irréductible de $\mathbb{Q}_p[X]$.

Si le polynôme S vérifie le critère, il est irréductible dans $\mathbb{Q}_p[X]$ et la factorisation est terminée. Sinon, deux cas sont possibles : ou bien S admet plusieurs facteurs irréductibles modulo p, ou bien S admet un unique facteur irréductible pour lequel il n'est pas un polynôme d'Eisenstein.

Dans le premier cas, l'algorithme Round 4 permet de construire explicitement deux facteurs (non nécessairement irréductibles) de S dans $\mathbb{Q}_p[X]$; il suffit alors d'appliquer récursivement cette méthode à chacun de ces deux polynômes.

Dans le second cas, l'algorithme Round 4 permet de construire en un nombre fini d'étapes un élément de k qui engendre localement le même ordre que θ et dont le polynôme caractéristique est ou bien irréductible par le critère précédent - ce qui prouve que le polynôme S est irréductible, ou bien admet plusieurs facteurs irréductibles modulo p. Il est alors possible dans ce cas de déduire de cette factorisation une factorisation non triviale de S.

Il est très important de noter pour finir que cette méthode utilise des polynômes p-adiques dont on ne connait qu'une approximation. Ainsi, pour que les polynômes et leurs approximations aient la même factorisation dans $\mathbb{Q}_p[X]$, il est nécessaire de travailler avec une précision suffisamment grande (et parfois supérieure à celle demandée). Le théorème de Stabilité Structurale que l'on peut trouver dans [**44**] permet de déterminer une précision suffisante pour assurer cette propriété essentielle.

1.3. Factorisation des polynômes dans un corps de nombres

Commençons par fixer un certain nombre de notations et énoncer quelques résultats.

Soit k un corps de nombres de degré N. On note (r_1, r_2) la signature de k et $\{\sigma_i\}_{1 \leq i \leq N}$ ses plongements ordonnés avec les conventions usuelles : les σ_i sont réels pour $1 \leq i \leq r_1$ et complexes pour $r_1 + 1 \leq i \leq N$ avec :

$$\overline{\sigma}_{r_1+j} = \sigma_{r_1+r_2+j}$$

pour $1 \leq j \leq r_2$. La T_2-norme d'un élément $\alpha \in k$ est définie par :

$$T_2(\alpha) := \sum_{i=1}^{N} |\sigma_i(\alpha)|^2.$$

Cette T_2-norme est la norme euclidienne du $\mathbb{Q}$-espace vectoriel de $\mathbb{R}^N$ obtenu en associant à un élément $\alpha \in k$ le vecteur dont les r_1 premières composantes sont données par $\sigma_i(\alpha)$ pour $1 \leq i \leq r_1$ et les $2r_2$ dernières par les couples :

$$(\Re(\sigma_i(\alpha)) + \Im(\sigma_i(\alpha)), \Re(\sigma_i(\alpha)) - \Im(\sigma_i(\alpha)))$$

pour $r_1 + 1 \leq i \leq r_1 + r_2$. Notons que si l'on restreint ce plongement à un idéal fractionnaire ou à un ordre de k, on obtient un réseau de $\mathbb{R}^N$.

Soit $\mathcal{L}$ un réseau de $\mathbb{R}^N$. Pour toute base $\mathcal{B} = \{b_1, \ldots, b_N\}$ de $\mathcal{L}$, on définit le domaine fondamental associé par :

$$D_{\mathcal{B}} := \{(x_1 b_1, \ldots, x_N b_N) \text{ avec } -1/2 < x_i \leq 1/2 \text{ pour tout } 1 \leq i \leq N\}.$$

Ce domaine ne contient pas d'autre point du réseau que l'origine, et tout point $x \in \mathbb{R}^N$ s'écrit de manière unique sous la forme $x = y + l$, où l est le point du réseau $\mathcal{L}$ le plus proche de x et $y \in D_{\mathcal{B}}$.

On note $V(\mathcal{L})$ le volume du réseau $\mathcal{L}$ (à savoir le volume du domaine $D_{\mathcal{B}}$, indépendant du choix de la base). Le défaut d'orthogonalité de la base $\mathcal{B}$ est défini par :

$$\delta_{\mathcal{B}} := \frac{\prod_i ||b_i||}{V(\mathcal{L})},$$

où $||.||$ est la norme euclidienne de $\mathbb{R}^N$.

En vertu de l'inégalité de Hadamard, ce défaut est supérieur ou égal à 1. Si la base $\mathcal{B}$ est LLL-réduite (*cf* [**37**]), ce défaut est inférieur à :

$$2^{N(N-1)/4}. \tag{1.3.1}$$

Soit $\mathbf{x}$ un vecteur de $\mathbb{R}^N$, on note $\lfloor \mathbf{x} \rceil$ le vecteur de $\mathbb{Z}^N$ obtenu en arrondissant chaque composante de $\mathbf{x}$ à l'entier le plus proche avec la convention que $n + 1/2$ s'arrondit à $n + 1$ pour $n \in \mathbb{Z}$.

Soit S le polynôme de $k[X]$ que l'on veut factoriser. On commence par multiplier ce polynôme par un entier algébrique convenable pour qu'il soit à coefficients dans $\mathcal{O}_k[X]$. Notons qu'on ne peut pas parler néanmoins de factorisation dans $\mathcal{O}_k[X]$ puisque l'anneau des entiers de k peut ne pas être principal. Ainsi, même si on considère essentiellement des polynômes à coefficients dans $\mathcal{O}_k$, on parlera uniquement de factorisation dans $k[X]$.

On suppose sans perte de généralité que S est séparable, sinon il n'est pas très difficile de se ramener à ce cas en remplaçant S par :

$$\frac{S}{\mathrm{PGCD}(S, S')}$$

ce qui ne change pas les facteurs irréductibles de S.

L'idée est la suivante : soit $\mathfrak{p}$ un idéal premier de k non ramifié et de degré résiduel 1 au-dessus d'un nombre premier p. Le complété de k en $\mathfrak{p}$ est $\mathbb{Q}_p$; ainsi, $\mathcal{O}_k[X]$ se plonge dans $\mathbb{Z}_p[X]$ et tout facteur irréductible de S dans $\mathcal{O}_k[X]$ est produit d'un certain nombre de facteurs irréductibles de S dans $\mathbb{Z}_p[X]$.

La méthode consiste donc à calculer la factorisation de S dans $\mathbb{Q}_p[X]$ par une des deux méthodes précédentes avec une précision suffisamment grande ; puis, à l'aide des différentes notions introduites sur les réseaux, de "reconstruire" à partir de cette factorisation les diviseurs de S dans $\mathcal{O}_k[X]$.

Remarque : On pourrait aussi choisir un idéal premier de degré résiduel plus grand que 1 et utiliser la méthode de factorisation modulo un idéal premier expliquée plus loin, puis un relèvement de Hensel pour obtenir la précision nécessaire ; le reste de la méthode étant tout à fait similaire. Cependant, il s'avère que dans la pratique les algorithmes relatifs de factorisation modulo un idéal premier et de relèvement de Hensel sont beaucoup moins performant que les algorithmes de factorisation p-adique (notamment l'algorithme Round 4). Il est donc ici préférable de travailler dans $\mathbb{Q}_p[X]$ plutôt que d'utiliser des méthodes relatives.

On commence par la généralisation suivante des bornes de Mignotte (*cf* [**40**]).

Théorème 1.2. *Soient $S(X) = \sum_{i=0}^{m} s_i X^i$ et $D(X) = X^l + \sum_{j=0}^{l-1} d_j X^j$ deux polynômes à coefficients dans k tels que D divise S.*

Alors, si on pose $T_2(S) := \sum_{i=0}^{m} T_2(s_i)$*, on a pour tout* j *:*

$$T_2(d_j) \leq \binom{l-1}{j} T_2(S) \left[\binom{l-1}{j} + 2\binom{l-1}{j-1} \right] + \binom{l-1}{j-1}^2 T_2(s_m).$$

Démonstration : Pour chaque plongement σ de k, le polynôme $\sigma(D)$ divise le polynôme $\sigma(S)$ dans $\mathbb{C}[X]$. En appliquant les bornes de Mignotte, on obtient :

$$|\sigma(d_j)| \leq \binom{l-1}{j} |\sigma(S)| + \binom{l-1}{j-1} |\sigma(t_m)| \quad \text{avec} \quad |\sigma(S)| = \left(\sum_{j=0}^{m} |\sigma(t_j)|^2 \right)^{1/2}.$$

Il suffit alors de prendre le carré de cette expression et de sommer sur tous les plongements de k. □

Soit $\tilde{D}$ une approximation d'un diviseur de S dans $\mathbb{Z}_p[X]$ connue à $\mathfrak{p}^n$ près. Supposons que ce diviseur soit en fait une approximation d'un diviseur D de S dans $\mathcal{O}_k[X]$. Alors, pour tout coefficient $\tilde{\delta}$ de $\tilde{D}$, si δ est le coefficient correspondant de D, on doit avoir :

$$\tilde{\delta} \equiv \delta \pmod{\mathfrak{p}^n}. \tag{1.3.2}$$

On sait majorer $T_2(\delta)$ grâce au théorème précédent ; on va voir maintenant comment on peut utiliser cette connaissance afin d'obtenir un exposant n suffisamment grand pour caractériser de manière unique l'élément δ.

Théorème 1.3. *Soient* $\mathfrak{q}$ *un idéal premier de norme* q *et* n *un entier positif non nul.*
Alors, chaque élément non nul α *de* $\mathfrak{q}^n$ *vérifie :*

$$T_2(\alpha) \geq N q^{2n/N}.$$

Démonstration : L'inégalité entre moyenne arithmétique et moyenne géométrique donne :

$$\sum_{i=1}^{N} \frac{|\sigma_i(\alpha)|^2}{N} \geq \left(\prod_{i=1}^{N} |\sigma_i(\alpha)|^2 \right)^{1/N},$$

et ainsi $T_2(\alpha) \geq N |N_{K/\mathbb{Q}}(\alpha)|^{2/N}$.

Mais, comme α est non nul, la norme de $\mathfrak{q}^n$ divise la norme de α et on obtient :

$$T_2(\alpha) \geq N \mathcal{N}(\mathfrak{q}^n)^{2/N} = N q^{2n/N}. \quad \square$$

Corollaire 1.4. *Soit* n *un entier tel que :*

$$n \geq \frac{N}{2} \frac{\ln(2C/N)}{\ln p}$$

où $C > 0$ *(par exemple,* C *est une borne supérieure pour tous les coefficients d'un éventuel diviseur de* S *dans* $\mathcal{O}_k[X]$ *donnée par le théorème 1.2).*

Alors, pour chaque diviseur $\tilde{D}$ *de* S *dans* $\mathbb{Z}_p[X]$*, il existe au plus un unique polynôme* D *tel que* D *est congru à* $\tilde{D}$ *modulo* $\mathfrak{p}^n$ *et dont les coefficients sont tous de* T_2*-norme inférieure strictement à* C*.*

Démonstration : Il suffit de vérifier que pour un $\alpha \in \mathbb{Z}_p$ donné, il existe au plus un unique $\beta \in \mathcal{O}_k$ tel que $T_2(\beta) < C$ et $\beta \equiv \alpha \pmod{\mathfrak{p}^n}$.

Supposons qu'il existe deux éléments β_1 et β_2 possédant ces deux propriétés. On a alors :

$$\pi := \beta_1 - \beta_2 \in \mathfrak{p}^n$$

et

$$T_2(\pi) \leq T_2(\beta_1) + T_2(\beta_2) < 2C.$$

D'où il découle que $T_2(\pi) < N p^{2n/N}$ et donc, en vertu du théorème précédent, $\pi = 0$ et $\beta_1 = \beta_2$. □

On fixe à présent pour la suite une constante $C > 0$ qui majore la T_2-norme de tous les coefficients d'un éventuel diviseur de S dans $\mathcal{O}_k[X]$. On sait désormais qu'il existe au plus un unique diviseur D de S congru à un diviseur $\tilde{D}$ de $\mathbb{Z}_p[X]$ donné si la précision n vérifie l'inégalité donnée dans le corollaire 1.4. Néanmoins, pour obtenir une méthode efficace permettant de calculer ce polynôme, il est nécessaire de travailler avec une

précision plus grande que celle donnée par le corollaire. Pour cela, on utilise le résultat suivant sur les réseaux (utilisé également par A.K. Lenstra dans le but de factoriser les polynômes sur un corps de nombres par une technique différente, *cf* [**36**]) :

Proposition 1.5. *Soient $\mathcal{L}$ un réseau de $\mathbb{R}^N$ et $\mathcal{B}$ une base de ce réseau.*
Alors, le domaine fondamental $D_{\mathcal{B}}$ contient une boule centrée à l'origine de rayon R avec :

$$R \geq \frac{m_{\mathcal{B}}}{2\delta_{\mathcal{B}}},$$

où $m_{\mathcal{B}} := \mathrm{Inf}_{b\in\mathcal{B}} ||b||$.

Soit n un entier tel que :

$$n > \frac{N}{2}\frac{\ln(C/N) + \left(\frac{N(N-1)}{4} + 1\right)\ln 2}{\ln p}. \tag{1.3.3}$$

En utilisant l'algorithme 2.11 de [**8**], on commence par calculer une approximation $\tilde{S}$ de S dans $\mathbb{Q}_p[X]$ à $\mathfrak{p}^n$ près ; en particulier, $\tilde{S}$ est à coefficients dans $\mathbb{Z}$. Puis, au moyen d'un des deux algorithmes décrits précédemment, on factorise $\tilde{S}$ dans $\mathbb{Z}_p[X]$ avec une précision p^n. On calcule également une $\mathbb{Z}$-base $\mathcal{B}$ LLL-réduite (pour la T_2-norme) de l'idéal $\mathfrak{p}^n$ sur une base d'entiers fixée de k.

Soit $\tilde{D}$ une approximation d'un diviseur de $\tilde{S}$ dans $\mathbb{Z}_p[X]$. Le corollaire 1.4 affirme qu'il existe au plus un unique diviseur D de S dans $\mathcal{O}_k[X]$ congru à $\tilde{D}$ modulo $\mathfrak{p}^n$. Voici comment on le calcule : soit $\tilde{\delta}$ un coefficient de $\tilde{D}$, on cherche à déterminer le coefficient correspondant δ de D et on a $T_2(\delta) < C$ par hypothèse.

D'après le théorème 1.3, on sait que :

$$m_{\mathcal{B}} \geq nq^{2k/n}$$

et donc, par la proposition 1.5 et l'inégalité 1.3.1 du fait que la base $\mathcal{B}$ est LLL-réduite, le domaine fondamental de $\mathcal{B}$ contient une boule centrée à l'origine de rayon plus grand que C.

Il suit que δ est l'unique élément de $\mathcal{O}_k$ congru à $\tilde{\delta}$ modulo $\mathfrak{p}^n$ dont le plongement est contenu dans le domaine fondamental $D_{\mathcal{B}}$. En effet, tout autre nombre $\delta' \in \mathcal{O}_k$ congru à $\tilde{\delta}$ vérifie $T_2(\delta') \geq C$ puisqu'il est en dehors du domaine fondamental et donc ne peut être solution.

La construction de cet élément est immédiate. On note M la matrice de la $\mathbb{Z}$-base $\mathcal{B}$ et $\tilde{d}$ le vecteur colonne exprimant $\tilde{\delta}$ sur cette base. Le point du réseau le plus près de $\tilde{d}$ est donné par le vecteur $\lfloor M^{-1}\tilde{d}\rceil$; on note ce vecteur v. Le vecteur d définissant δ sur la base d'entiers est alors obtenu en posant :

$$d := \tilde{d} - Mv. \tag{1.3.4}$$

Il ne reste plus qu'à associer tous ces résultats pour obtenir l'algorithme de factorisation (on pourra comparer avec l'algorithme de factorisation dans $\mathbb{Q}[X]$ donné dans [**8**] algorithme 3.5.7).

Algorithme 1.6. *Soit S un polynôme à coefficients dans $\mathcal{O}_k$; l'algorithme calcule la factorisation de S dans $k[X]$.*

1. *On pose $S_2 \leftarrow \mathrm{PGCD}(S, S')$ puis $S_0 \leftarrow S/S_2$. En utilisant, par exemple, l'algorithme 6.2.9 de* [**8**]*, on détermine un idéal premier $\mathfrak{p}$ de k non ramifié et de degré résiduel 1.*

2. *Soit n le plus petit entier vérifiant 1.3.3. Par l'algorithme 2.11 de* [**9**]*, on calcule une approximation $\tilde{S}$ à $\mathfrak{p}^n$ près de S_0 dans $\mathbb{Z}_p[X]$; puis, à l'aide d'une des deux méthodes précédentes, on factorise le polynôme $\tilde{S}$ dans $\mathbb{Z}_p[X]$:*

$$\tilde{S}(X) \equiv \prod_{i=1}^{g} \tilde{D}_i(X) \pmod{p^n}.$$

3. *On calcule la matrice d'une base LLL-réduite pour la T_2-norme de $\mathfrak{p}^n$ exprimée sur une base d'entiers fixée de k. On pose $r \leftarrow 1$, $\mathcal{E} \leftarrow \{\tilde{D}_1, \ldots, \tilde{D}_g\}$ et $\mathcal{F} \leftarrow \emptyset$.*

4. *Soit $\tilde{D}$ le produit de r éléments distincts de $\mathcal{E}$. Au moyen de la construction donnée par la formule 1.3.4, on calcule l'unique polynôme $D \in \mathcal{O}_k[X]$ susceptible de diviser S_0 et congru à $\tilde{D}$ modulo $\mathfrak{p}^n$. Puis, on teste si D divise effectivement S_0. Si oui, on ôte de $\mathcal{E}$ les facteurs irréductibles de $\tilde{D}$, on pose $\mathcal{F} \leftarrow \mathcal{F} \cup \{D\}$ et*

$S_0 \leftarrow S_0/D$. S'il existe des produits de r facteurs de $\mathcal{E}$ qui n'ont pas encore été testés, on recommence cette étape.

5. *On pose $r \leftarrow r+1$. Si $r \leq \deg(S_0)/2$, on repart à l'étape précédente. Sinon, on pose $\mathcal{F} \leftarrow \mathcal{F} \cup \{S_0\}$.*

6. *Pour chaque $S_i \in \mathcal{F}$, on calcule le plus grand entier f_i tel que $S_i(X)^{f_i}$ divise $S_2(X)$. Puis on pose $e_i \leftarrow 1+f_i$. On renvoie la factorisation de S dans $\mathcal{O}_k[X]$:*

$$S(X) = \prod_i D_i(X)^{e_i}.$$

1.4. Factorisation des polynômes modulo un idéal premier

La méthode de factorisation des polynômes à coefficients dans un corps de nombres modulo un idéal premier expliquée ici est une généralisation directe de la méthode de Berlekamp (*cf* [**4**] ou [**8**] section 3.4).

Soient $\mathfrak{p}$ un idéal premier de k et S un polynôme de degré m à coefficients dans $\mathbb{F}_\mathfrak{p}[X]$ où $\mathbb{F}_\mathfrak{p}$ désigne le corps résiduel $(\mathcal{O}_k/\mathfrak{p})$. On note p la caractéristique de $\mathbb{F}_\mathfrak{p}$ et $q := \mathcal{N}\mathfrak{p} = p^f$, de telle sorte que $\mathbb{F}_\mathfrak{p} \cong \mathbb{F}_q$.

Soit S le polynôme à coefficients dans $\mathbb{F}_\mathfrak{p}[X]$ que l'on souhaite factoriser (le plus souvent, le polynôme S est donné comme un polynôme à coefficients dans $\mathcal{O}_k[X]$). On commence par se ramener au cas où S est séparable. Cependant, dans cette section, cette étape est plus délicate que dans les sections précédentes car on travaille désormais en caractéristique $p > 0$.

Pour cela, on écrit :

$$S(X) = \prod_{i=1}^{g} A_i(X)^i$$

où les polynômes A_i sont séparables et premiers entre eux. On calcule maintenant la dérivée :

$$S'(X) = \sum_{j=1}^{g} \left(jA_j'(X)A_j(X)^{j-1} \prod_{\substack{i=1 \\ i\neq j}}^{g} A_i(X) \right).$$

Un calcul élémentaire (*cf* [**8**] section 3.4.2) donne alors :

$$\mathrm{PGCD}(S, S') = \prod_{\substack{i=1 \\ p|i}}^{g} A_i(X)^i \prod_{\substack{i=1 \\ p\nmid i}}^{g} A_i(X)^{i-1}.$$

On pose :

$$U(X) := \frac{S(X)}{\mathrm{PGCD}(S(X), S'(X))} = \prod_{p\nmid i} A_i(X).$$

Pour n assez grand, par exemple $n = \deg(S)$, on a :

$$V(X) := \frac{S(X)}{\mathrm{PGCD}(S(X), U(X)^n)} = \prod_{p|i} A_i(X)^i,$$

et donc il existe un polynôme $W(X)$ tel que $W(X)^p = V(X)$. Pour déterminer ce polynôme, on écrit :

$$V(X) = \sum_{i=1}^{l} v_i X^{ip}$$

et on pose :

$$W(X) := \sum_{i=1}^{l} v_i^{q/p} X^i = \prod_{p|i} A_i(X)^{i/p}.$$

Il suffit d'appliquer ce même processus au polynôme $W(X)$ ce qui permet de déterminer le produit des polynômes A_i dont l'indice i est divisible une et une seule fois par p. En appliquant plusieurs fois ce processus, on détermine un polynôme séparable qui a exactement les mêmes facteurs irréductibles que S.

On obtient l'algorithme suivant :

Algorithme 1.7. *Soit S un polynôme à coefficients dans $\mathbb{F}_\mathfrak{p}[X]$. Cet algorithme détermine un polynôme A séparable et divisible exactement par les mêmes facteurs irréductibles que S.*

1. *On pose $W(X) \leftarrow S(X)$, $A(X) \leftarrow 1$.*

2. *On calcule :*

$$U(X) \leftarrow W(X)/\operatorname{PGCD}(W(X), W'(X))$$

puis

$$V(X) \leftarrow W(X)/\operatorname{PGCD}(W(X), U(X)^d)$$

où $d := \deg(W)$. On pose $A(X) \leftarrow A(X)U(X)$.

3. *Si $\deg(V) > 0$, on peut écrire $V(X) = \sum_i v_i X^{pi}$, on pose alors $W(X) \leftarrow \sum_i v_i^{q/p} X^i$ et on repart à l'étape précédente. Sinon, on renvoie le polynôme A et l'algorithme se termine.*

On peut à présent supposer sans perte de généralité que le polynôme S est séparable. On utilise le théorème suivant (*cf* [**4**]) :

Théorème 1.8 (Berlekamp)**.** *Soit S un polynôme séparable à coefficients dans $\mathbb{F}_\mathfrak{p}$ et de degré m. On écrit :*

$$S(X) = \prod_{i=1}^{g} S_i(X)$$

la factorisation de S dans $\mathbb{F}_\mathfrak{p}[X]$.

Alors, pour tout polynôme $A \in \mathbb{F}_\mathfrak{p}[X]$ de degré strictement plus petit que m, les deux assertions suivantes sont équivalentes :

(i) *Pour tout $1 \leq i \leq g$, il existe $a_i \in \mathbb{F}_\mathfrak{p}$ tel que :*

$$A(X) \equiv a_i \pmod{S_i(X)}.$$

(ii) *le polynôme A vérifie l'équation :*

$$A(X)^q \equiv A(X) \pmod{S(X)}.$$

Remarque : Pour tout choix des $a_i \in \mathbb{F}_\mathfrak{p}$, le théorème chinois permet de déterminer un unique polynôme A à coefficients dans $\mathbb{F}_\mathfrak{p}$ dont le degré est strictement plus petit que m et vérifiant :

$$A(X) \equiv a_i \pmod{S_i(X)}$$

pour tout i. Ainsi, il existe q^g solutions distinctes à (i).

Démonstration : On montre que (i) implique (ii). On a :

$$A(X)^q \equiv a_i^q \pmod{S_i(X)},$$

or $a_i^q = a_i$ puisque $a_i \in \mathbb{F}_\mathfrak{p}$. D'où il s'ensuit que $A(X)^q \equiv A(X) \pmod{S_i(X)}$ pour tout i. Les polynômes $S_i(X)$ sont premiers deux à deux dans $\mathbb{F}_\mathfrak{p}[X]$, donc cette congruence est toujours vraie modulo leur produit $S(X)$.

Maintenant, on prouve que (ii) implique (i). On a l'identité polynomiale :

$$X^q - X = \prod_{a \in \mathbb{F}_\mathfrak{p}} (X - a).$$

En remplaçant X par $A(X)$, on trouve que $A(X)^q - A(X) = \prod_a (A(X) - a)$. Et S divise par hypothèse ce produit.

Soit S_i un facteur irréductible de S, alors S_i divise également le produit des $A(X) - a$, $a \in \mathbb{F}_\mathfrak{p}$; mais, comme S_i est irréductible dans $\mathbb{F}_\mathfrak{p}[X]$, ceci implique qu'il existe un élément $a_i \in \mathbb{F}_\mathfrak{p}$ tel que :

$$S_i(X) \mid (A(X) - a_i).$$

Ceci termine la démonstration de l'équivalence. □

Les solutions de (ii) forment un $\mathbb{F}_\mathfrak{p}$-espace vectoriel de dimension g. On utilise la méthode suivante pour déterminer une base de cet espace vectoriel. On écrit pour tout $1 \leq j \leq m-1$:

$$X^{jq} \equiv \sum_{i=0}^{m-1} r_{i,j} X^i \pmod{S(X)}.$$

On pose $A(X) := \sum_{j=0}^{m-1} c_j X^j$, la condition (ii) devient :

$$A(X)^q = \sum_{j=0}^{m-1} c_j X^{jq} \equiv \sum_{j=0}^{m-1} c_j \sum_{i=0}^{m-1} r_{i,j} X^i \pmod{S(X)}$$

d'où les coefficients c_i doivent vérifier :

$$c_i = \sum_{j=0}^{m-1} c_j r_{i,j}$$

pour tout i.

Ainsi, le calcul des coefficients c_i se ramène au calcul du noyau de la matrice $R - \mathrm{Id}$ où R est la matrice des $r_{i,j}$ et Id est la matrice identité $(m-1) \times (m-1)$. On calcule ainsi une base $A_1(X), \ldots, A_g(X)$ des solutions de (ii).

Un des avantages de cette méthode est que le rang de ce noyau est le nombre de facteurs irréductibles de S. En particulier, si ce rang est 1, alors S est irréductible dans $\mathbb{F}_\mathfrak{p}[X]$. On suppose désormais que le nombre de facteurs est $g \geq 2$.

Dans ce cas, une fois connues les solutions de (ii), on sait qu'il en existe une, disons $A(X)$, telle que $a_1 \neq a_2$ avec les notations du théorème 1.8. Il s'ensuit que $A(X) - a_1$ est divisible par $S_1(X)$ mais pas par $S_2(X)$. Le PGCD de $A(X) - a_1$ et de $S(X)$ fournit donc une factorisation non triviale de S. L'idée est donc de calculer un certain nombre de tels PGCD pour "casser" S jusqu'à obtenir une factorisation de S en g polynômes, auquel cas on sait que tous ces polynômes sont irréductibles et que la factorisation est finie.

La principale difficulté qui apparaît alors est la détermination des a_i. En effet, on ne sait rien sur ces éléments si ce n'est qu'ils existent et, si q est grand, une recherche exhaustive de ces éléments devient vite une tâche fastidieuse. On utilise donc plutôt le résultat suivant :

Proposition 1.9. *Soient $b_1, \ldots, b_g$ des éléments choisis au hasard dans $\mathbb{F}_\mathfrak{p}$. On pose :*

$$A(X) := \sum_{i=1}^{g} b_i A_i(X).$$

Puis, si $p = 2$, on pose :

$$D(X) := A(X) + A(X)^2 + A(X)^4 + \cdots + A(X)^{q/2}$$

et si p est impair, on pose :

$$D(X) := A(X)^{(q-1)/2} - 1.$$

Alors, le PGCD *de S et de D est un facteur non trivial de $S(X)$ avec une probabilité supérieure ou égale à 4/9.*

Démonstration : On note a_i les éléments de $\mathbb{F}_\mathfrak{p}$ tels que la condition (ii) du théorème 1.8 soit vérifiée, *ie* $A(X) \equiv a_i \pmod{S_i(X)}$.

Examinons le cas pair. On pose $U(X) = X + X^2 + X^4 + \cdots + X^{q/2}$. On a alors :

$$U(X)(U(X) + 1) = X^q - X$$

et ces deux polynômes sont premiers entre eux. Ainsi, si on note respectivement $\mathcal{E}$ et $\mathcal{E}'$ l'ensemble des racines de $U(X)$ et $U(X)+1$ respectivement, on a $\mathcal{E} \cap \mathcal{E}' = \emptyset$ et $\mathcal{E} \cup \mathcal{E}' = \mathbb{F}_\mathfrak{p}$. De plus, il est clair que $\operatorname{card} \mathcal{E}' = \operatorname{card} \mathcal{E} = q/2$. On a :

$$D(X) = \prod_{x \in \mathcal{E}} (A(X) - x).$$

Le PGCD de D et de S est égal à 1 quand aucun des facteurs irréductibles de S ne divisent D, *ie* quand aucun des a_i n'est dans $\mathcal{E}$; cet événement a une probabilité :

$$\left(\frac{q/2}{q}\right)^g.$$

Le PGCD de D et de S est égal à S quand tous les facteurs irréductibles de S divisent D, *ie* quand tous les a_i sont dans $\mathcal{E}$; dans ce cas, la probabilité est aussi :

$$\left(\frac{q/2}{q}\right)^g.$$

Ainsi, la probabilité que le PGCD de D et de S fournisse un diviseur non trivial est :

$$1 - \left(\frac{1}{2}\right)^g - \left(\frac{1}{2}\right)^g \geq 1/2$$

puisque $g \geq 2$. (On note qu'elle ne dépend pas de q.)

Dans le cas impair, on trouve $D(X) = \prod_{x\in\mathcal{E}}(A(X) - x)$ avec $\mathcal{E} = (\mathbb{F}_\mathfrak{p}^\times)^2$. D'où, à l'aide du même raisonnement que ci-dessus, la probabilité que le PGCD de S et de D soit non trivial est :

$$1 - \left(\frac{q-1}{2q}\right)^g - \left(\frac{q+1}{2q}\right)^g \geq 4/9,$$

cette valeur minimale étant atteinte pour $q = 3$ et $g = 2$. □

On obtient ainsi l'algorithme probabiliste de factorisation du polynôme S :

Algorithme 1.10. *Soit S un polynôme à coefficients dans $\mathbb{F}_\mathfrak{p}[X]$. Cet algorithme calcule sa factorisation dans $\mathbb{F}_\mathfrak{p}[X]$.*

1. *On commence par calculer grâce à l'algorithme 1.7, un polynôme S_0 séparable et divisible exactement par les mêmes facteurs irréductibles que S.*

2. *On calcule par récurrence les coefficients $r_{i,j}$ tels que :*

$$X^{jq} \equiv \sum_{i=0}^{m-1} r_{i,j}X^i \pmod{S(X)}.$$

3. *Soit R la matrice dont les entrées sont les $r_{i,j}$; on calcule le noyau de $R - \mathrm{Id}$ avec un dérivé de l'algorithme 2.3.1 de* [**8**]. *On en déduit des polynômes $A_1, \ldots, A_g$ formant une base de l'ensemble des solutions du théorème 1.8. On pose $\mathcal{F} \leftarrow \{S_0\}$ et $k \leftarrow 1$.*

4. *Si $k = g$, alors on va à l'étape* **6**. *Sinon, on choisit des éléments $a_i \in \mathbb{F}_\mathfrak{p}$ au hasard, on calcule $A(X) \leftarrow \sum_i a_i A_i(X)$ puis on pose :*

$$\begin{aligned} D(X) &\leftarrow A(X) + A(X)^2 + \cdots + A(X)^{q/2} \text{ si } p = 2, \\ D(X) &\leftarrow A(X)^{(q-1)/2} - 1 \text{ sinon .} \end{aligned}$$

5. *On pose $\mathcal{G} \leftarrow \emptyset$. Pour tout $B \in \mathcal{F}$, on calcule $C \leftarrow \mathrm{PGCD}(B, D)$. Si $\deg(C) > 0$ et $\deg(C) < \deg(B)$, on pose $\mathcal{G} \leftarrow \{D, B/D\}$ et $k \leftarrow k+1$, sinon $\mathcal{G} \leftarrow \{B\}$. Une fois considérés tous les éléments de $\mathcal{F}$, on pose $\mathcal{F} \leftarrow \mathcal{G}$ et on repart à l'étape précédente.*

6. *Pour chaque polynôme $S_i \in \mathcal{F}$, on calcule le plus grand entier e_i tel que $S_i(X)^{e_i}$ divise S. On retourne la factorisation :*

$$S(X) = \prod_{i=1}^{g} S_i(X)^{e_i}$$

et l'algorithme se termine.

1.5. Applications de la factorisation des polynômes dans un corps de nombres

Nous allons donner à présent un certain nombre d'applications de la factorisation des polynômes dans un corps de nombres en illustrant chacun d'eux par un exemple. Notons que cet exemple a été choisi plus pour sa simplicité que pour illustrer les performances de l'algorithme. L'ensemble des calculs a été effectué en utilisant le système PARI ([**3**]).

Avant de commencer, on remarque que dans [**36**], la dernière factorisation donnée est incomplète. En effet, la factorisation du polynôme :

$$S(X) = X^9 + 9X^8 + 36X^7 + 69X^6 + 36X^5 - 99X^4 - 303X^3 - 450X^2 - 342X - 226$$

sur le corps de nombres défini par une racine θ du polynôme $X^9 - 15X^6 - 87X^3 - 125$ fait apparaître un terme de degré 6 :

$$S_6(X) = X^6 + 6X^5 + 15X^4 + (\theta^3 + 5)X^3 + (3\theta^3 - 30)X^2 + (3\theta^3 - 39)X + \theta^6 - 14\theta^3 - 101,$$

qui n'est pas irréductible. On trouve qu'il admet la factorisation suivante :

$$S_6(X) = D_1(X)D_2(X)D_3(X)$$

avec :

$$\begin{aligned}
D_1(X) &= X^2 + \left(-\frac{2}{15}\theta^7 + \frac{7}{3}\theta^4 + \frac{79}{15}\theta + 2\right)X + \\
&\qquad \left(\frac{1}{25}\theta^8 - \frac{2}{15}\theta^7 - \frac{3}{5}\theta^5 + \frac{7}{3}\theta^4 - \frac{87}{25}\theta^2 + \frac{79}{15}\theta + 1\right) \\
D_2(X) &= X^2 + \left(\frac{2}{15}\theta^7 - \frac{7}{3}\theta^4 - \frac{94}{15}\theta + 2\right)X + \\
&\qquad \left(\frac{1}{25}\theta^8 + \frac{2}{15}\theta^7 - \frac{3}{5}\theta^5 - \frac{7}{3}\theta^4 - \frac{87}{25}\theta^2 - \frac{94}{15}\theta + 1\right) \\
D_3(X) &= X^2 + (\theta + 2)X + \left(\frac{1}{25}\theta^8 - \frac{3}{5}\theta^5 - \frac{87}{25}\theta^2 + \theta + 1\right).
\end{aligned}$$

Dans la suite, soit K le corps de nombres défini par $K := \mathbb{Q}(\Theta)$ où Θ est racine d'un polynôme unitaire, entier et irréductible $T(X)$. On définit également le corps k par $k := \mathbb{Q}(\theta)$ où θ est racine d'un polynôme unitaire, entier et irréductible $t(X)$.

Nous allons illustrer les applications suivantes en prenant :

$$T(X) := X^6 - 8X^4 - 6X^3 + 7X^2 + 6X + 1,$$

puis pour Θ la racine de T telle que :

$$\Theta \approx -1.962$$

et $\theta := \sqrt{2}$. (Dans ce cas, K est le corps de classes de rayon $\mathfrak{p}_{103}$ de k où $\mathfrak{p}_{103}$ est un des deux idéaux de k au-dessus de 103. Ce corps a été construit grâce aux méthodes décrites dans le chapitre suivant).

1.5.1. Inclusion à isomorphisme près. Le corps k est inclus dans le corps K à isomorphisme près si et seulement si l'élément primitif θ ou un des ses conjugués est inclus dans K. Ceci est équivalent à dire que la factorisation du polynôme $t(X)$ admet un terme linéaire dans $\mathcal{O}_K[X]$, disons $X - \alpha$. L'élément α est alors un conjugué de θ sur $\mathbb{Q}$. On peut déterminer si k est réellement un sous-corps de K en comparant des valeurs approchées suffisamment précises de θ et de α dans $\mathbb{C}$.

Si les deux corps K et k sont de même degré sur $\mathbb{Q}$, on en déduit qu'ils sont isomorphes. (Notons qu'on peut remplacer $\mathbb{Q}$ par un sous-corps commun $E \subset K \cap k$; dans ce cas, si la factorisation du polynôme irréductible de θ sur E admet un terme linéaire (*cf* application suivante pour le calcul de ce polynôme), ceci prouve que k est inclus dans K à un E-isomorphisme près .)

Exemple : On trouve la factorisation suivante :

$$t(X) = (X - (2\Theta^5 - \Theta^4 - 15\Theta^3 - 5\Theta^2 + 14\Theta + 5))(X - (-2\Theta^5 + \Theta^4 + 15\Theta^3 + 5\Theta^2 - 14\Theta - 5)),$$

puis :

$$\sqrt{2} = -2\Theta^5 + \Theta^4 + 15\Theta^3 + 5\Theta^2 - 14\Theta - 5. \tag{1.5.5}$$

Ce qui prouve que $k \subset K$ (Remarquons qu'il suffisait dans ce cas de montrer que k est inclus dans K à un $\mathbb{Q}$-isomorphisme près pour montrer qu'il y a effectivement inclusion puisque le corps k est galoisien.)

1.5.2. Polynôme irréductible relatif. Supposons que k est inclus dans K. Alors, l'élément Θ admet un polynôme irréductible sur k. Ce polynôme est obtenu en factorisant $T(X)$ dans $\mathcal{O}_k[X]$. Chacun des facteurs de degré $[K : k]$ est le polynôme irréductible d'un conjugué de Θ par un $\mathbb{Q}$-automorphisme de k. Pour déterminer exactement lequel de ces facteurs est le polynôme irréductible de Θ, il faut calculer des valeurs approchées des racines de ces facteurs et comparer avec une approximation de Θ dans $\mathbb{C}$.

Exemple : La factorisation de $T(X)$ dans $\mathcal{O}_k[X]$ donne :

$$T(X) = (X^3 - \sqrt{2}X^2 + (-\sqrt{2} - 3)X - 1)(X^3 + \sqrt{2}X^2 + (\sqrt{2} - 3)X - 1).$$

En regardant des approximations des racines de ces polynômes dans $\mathbb{C}$, on trouve que le polynôme irréductible de Θ sur k est :

$$T_k(X) := X^3 + \sqrt{2}X^2 + (\sqrt{2} - 3)X - 1. \tag{1.5.6}$$

1.5.3. Automorphismes d'un corps. En appliquant le raisonnement du premier exemple au corps K lui-même, on peut déterminer quels sont les automorphismes de K. Suivant le choix qu'on fait de factoriser le polynôme irréductible absolu de Θ ou bien le polynôme irréductible relatif de Θ sur un sous-corps k, on obtient les $\mathbb{Q}$-automorphismes de K ou bien les k-automorphismes de K. A chaque fois, ces automorphismes sont donnés sous la forme d'une substitution :

$$\Theta \mapsto Q(\Theta)$$

avec $Q(X) \in K[X]$ et $X - Q(\Theta)$ un facteur linéaire du polynôme irréductible.

Exemple : On factorise $T(X)$ dans $\mathcal{O}_K[X]$, on trouve :

$$\begin{aligned} T(X) = (X - \Theta)(X - (\Theta^5 - \Theta^4 - 7\Theta^3 + \Theta^2 + 6\Theta))(X - (\Theta^5 - 8\Theta^3 - 6\Theta^2 + 7\Theta + 5)) \\ (X^3 + (2\Theta^5 - \Theta^4 - 15\Theta^3 - 5\Theta^2 + 14\Theta + 5)X^2 + (2\Theta^5 - \Theta^4 - 15\Theta^3 - 5\Theta^2 + 14\Theta + 2)X - 1). \end{aligned} \tag{1.5.7}$$

Le corps K admet donc 3 $\mathbb{Q}$-automorphismes (en particulier, il n'est pas galoisien) qui sont donnés par :

$$\begin{aligned} \sigma_0 &: \Theta \mapsto \Theta \\ \sigma_1 &: \Theta \mapsto \Theta^5 - \Theta^4 - 7\Theta^3 + \Theta^2 + 6\Theta \\ \sigma_2 &: \Theta \mapsto \Theta^5 - 8\Theta^3 - 6\Theta^2 + 7\Theta + 5. \end{aligned}$$

Si on utilise l'expression de $\sqrt{2}$ donnée par 1.5.5, on obtient :

$$\sigma_0(\sqrt{2}) = \sigma_1(\sqrt{2}) = \sigma_2(\sqrt{2}) = \sqrt{2}$$

et donc ces 3 automorphismes sont en fait des k-automorphismes.

En effet, si on exprime les coefficients du polynôme irréductible de Θ sur k (*cf* formule 1.5.6) en fonction de Θ, on trouve :

$$X^3 + (-2\Theta^5 + \Theta^4 + 15\Theta^3 + 5\Theta^2 - 14\Theta - 5)X^2 + (-2\Theta^5 + \Theta^4 + 15\Theta^3 + 5\Theta^2 - 14\Theta - 8)X - 1$$

qui est le produit des trois facteurs linéaires apparaissant plus haut dans la factorisation 1.5.7.

1.5.4. Clôture galoisienne et groupe de Galois. En factorisant le polynôme T dans $\mathcal{O}_K[X]$, on obtient les $\mathbb{Q}$-automorphismes de K en prenant les facteurs linéaires de cette factorisation. Tout autre facteur irréductible de degré ≥ 2 est le polynôme irréductible d'un conjugué de Θ sur $\mathbb{Q}$ qui n'est pas inclus dans K, disons Ψ. On pose alors $K_1 := K(\Psi)$ et on factorise T dans ce corps. Si cette factorisation n'admet que des termes linéaires, alors K_1 est galoisien sur $\mathbb{Q}$ et même c'est la clôture galoisienne de $K/\mathbb{Q}$. Sinon, on définit le corps K_2 en rajoutant au corps K_1 une racine d'un facteur irréductible de degré ≥ 2 et ainsi de suite...

On obtient à la fin la clôture galoisienne N de $K/\mathbb{Q}$. En examinant à chaque étape les extensions K_{n+1}/K_n, on en déduit des informations sur les blocs d'imprimitivité des racines de T et ceci permet parfois d'en déduire la structure de $\mathrm{Gal}(N/\mathbb{Q})$ (en particulier, quand ce groupe de Galois est résoluble, voir [**33**]).

Exemple : On sait dans l'exemple précédent que le corps K n'est pas galoisien. Soit Ψ une racine dans $\mathbb{C}$ du facteur irréductible de degré 3 qui apparaît dans 1.5.7. On pose $K_1 := \mathbb{Q}(\Theta, \Psi)$. On calcule le polynôme irréductible d'un élément primitif Θ_1 de ce corps, on trouve (après réduction absolue *cf* [**8**] section 4.4.2 ou par la méthode de réduction relative utilisée au chapitre 3) :

$$T_1(X) = X^{18} - 46X^{16} + 826X^{14} - 7398X^{12} + 35205X^{10} - 87540X^8 + 104881X^6 - 55510X^4 + 11452X^2 - 648.$$

On vérifie alors que la factorisation du polynôme T dans $K_1[X]$ n'admet que des termes linéaires ce qui prouve que l'extension $K_1/\mathbb{Q}$ est galoisienne et donc que K_1 est la clôture galoisienne de K sur $\mathbb{Q}$.

Le groupe de Galois du polynôme T est donc un groupe transitif de degré 6 et d'ordre 18. En consultant les tables des groupes transitifs (par exemple, celles données dans [**6**]), on trouve qu'il existe un unique groupe avec ces deux propriétés. Le groupe de Galois de T est donc isomorphe à :

$$C_3 \times S_3.$$

1.5.5. Racines n-ièmes d'un nombre algébrique. Soit α un élément de k. Pour tout entier $n \geq 1$, trouver les racines n-ièmes de α dans k revient à factoriser le polynôme :

$$X^n - \alpha.$$

En effet, tout facteur linéaire de cette factorisation, disons $X - \beta$, donne une solution :

$$\beta^n = \alpha.$$

D'un autre côté, si β est une racine n-ième de α dans k, alors le polynôme irréductible $X - \beta$ divise $X^n - \alpha$.

Donc, toutes les racines n-ièmes de α dans k sont données par tous les facteurs linéaires de la factorisation de $X^n - \alpha$.

Un exemple d'application consiste à trouver les racines de l'unité contenues dans un corps de nombres k. On note N le degré absolu de k et n l'ordre du sous-groupe des racines de l'unité contenues dans $k^\times$. Alors, on a $\mathbb{Q}(\zeta_n) \subset k$ où ζ_n est une racine primitive d'ordre n de l'unité. En particulier, le degré absolu du corps $\mathbb{Q}(\zeta_n)$ divise N, *ie* $\phi(n) \mid N$ où ϕ est la fonction indicatrice d'Euler. On est donc amené à résoudre l'équation :

$$\phi(n) = N.$$

Soit p un nombre premier divisant n, alors $p-1$ doit diviser N. On commence par construire l'ensemble des nombres premiers p tels que $(p-1) \mid N$. Pour tous ces nombres, soit e_p le plus grand entier tel que $(p-1)p^{e_p-1}$ divise N.

On factorise alors le polynôme cyclotomique $\Phi_{p^f}(X)$ pour $1 \leq f \leq e_p$ dans k pour tous les nombres premiers p trouvés ci-dessus. Ou bien il se factorise totalement et donc k contient les racines primitives de l'unité d'ordre p^f, ou bien il reste irréductible et donc k ne contient pas ces racines (on peut améliorer sensiblement cet algorithme, *cf* [**8**] algorithme 4.9.10 pour plus de détails).

Exemple : soit E le corps de nombres défini par une racine $\varkappa$ du polynôme irréductible :

$$X^6 - 3X^5 + 6X^4 + 3X^3 - 9X^2 - 18X + 36.$$

En appliquant le raisonnement ci-dessus, on trouve les nombres premiers 2, 3 et 7 avec les exposants 2, 2 et 1. On a bien sûr pour commencer la factorisation triviale de $\Phi_2(X) = X - 1$ qui donne la racine -1. Puis, on

factorise $\Phi_4(X) = X^2 + 1$ dans $E[X]$, on trouve qu'il est irréductible. Ensuite, on regarde la factorisation de $\Phi_3(X) := X^2 + X + 1$, on obtient :

$$\Phi_3(X) = \left(X - \left(\frac{1}{36}\varkappa^5 + \frac{5}{12}\varkappa^2 - 1\right)\right)\left(X - \left(-\frac{1}{36}\varkappa^5 - \frac{5}{12}\varkappa^2\right)\right)$$

ce qui prouve que E contient les racines primitives d'ordre 3 de l'unité et fournit une expression explicite de ces racines en fonction de $\varkappa$. On trouve que les polynômes $\Phi_9(X) = X^6 + X^3 + 1$ et $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ sont irréductibles dans $E[X]$.

Donc le sous-groupe des unités de torsion de E est le groupe cyclique d'ordre 6 engendré par :

$$\frac{1}{36}\varkappa^5 + \frac{5}{12}\varkappa^2.$$

1.6. Applications de la factorisation modulo un idéal premier

On reprend l'ensemble des notations du début de la section précédente, en supposant de plus que k est inclus dans K.

1.6.1. Critère de Dedekind relatif. On rappelle que T_k désigne le polynôme irréductible de Θ sur k. Une première tâche lorsque l'on considère une extension relative est de calculer son discriminant et une pseudo-base de son anneau d'entiers (*cf* [**9**] pour la définition d'une pseudo-base).

On sait pour commencer qu'il existe un idéal entier $\mathfrak{I}(\Theta)$, appelé l'indice de Θ dans $\mathcal{O}_K$, tel que :

$$\mathfrak{d}_{K/k} = \mathfrak{I}(\Theta)^2 \operatorname{disc}(T_k)$$

(on peut aussi voir cet idéal comme l'indice de $\mathcal{O}_k[\Theta]$ considéré comme sous-$\mathcal{O}_k$-module de $\mathcal{O}_K$).

Pour un idéal premier $\mathfrak{p}$ de k, on dit que l'ordre $\mathcal{O}_k[\Theta]$ est $\mathfrak{p}$-*maximal* si l'indice $\mathfrak{I}(\Theta)$ n'est pas divisible par $\mathfrak{p}$. Cet ordre est maximal, *ie* $\mathcal{O}_K = \mathcal{O}_k[\Theta]$ si et seulement si il est $\mathfrak{p}$-maximal pour tous les idéaux premiers $\mathfrak{p}$ de k. Dans le cas absolu, *ie* $k = \mathbb{Q}$, il existe un critère très efficace dû à Dedekind qui permet de déterminer si l'ordre $\mathbb{Z}[\Theta]$ est p-maximal et, si ce n'est pas le cas, de construire un ordre plus grand que ce dernier (*cf* [**8**] th. 6.1.4).

Dans le cas relatif, on a l'analogue suivant :

Théorème 1.11. *Soit τ un élément de k tel que $\operatorname{val}_{\mathfrak{p}}(\tau) = -1$ et $\operatorname{val}_{\mathfrak{q}}(\tau) \geq 0$ pour tout idéal premier $\mathfrak{q}$ distinct de $\mathfrak{p}$ (un tel élément existe en vertu du théorème d'approximation). On désigne par $\bar{}$ la réduction d'un élément ou d'un polynôme modulo $\mathfrak{p}$.*

On écrit la factorisation :

$$\overline{T_k(X)} = \prod_{i=1}^{r} \overline{T_i(X)^{e_i}}.$$

Puis, on pose :

$$g(X) := \prod_{i=1}^{r} T_i(X).$$

Alors, on a :

(a) *le $\mathfrak{p}$-radical $I_{\mathfrak{p}}$ de $\mathcal{O}_k[\Theta]$ (ie l'ensemble des éléments $x \in \mathcal{O}_k[\Theta]$ tels que $x^n \in \mathfrak{p}\mathcal{O}_k[\Theta]$ pour n assez grand) est donné par :*

$$I_{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_k[\Theta] + g(\Theta)\mathcal{O}_k[\Theta].$$

Et donc un élément $x := A(\Theta) \in \mathcal{O}_k[\Theta]$ appartient à $I_{\mathfrak{p}}$ si et seulement si $\overline{g} \mid \overline{A}$.

(b) *Soit $h(X) \in \mathcal{O}_k[X]$ un relèvement du quotient $\overline{T}/\overline{g}$. On pose :*

$$f(X) := \tau(g(X)h(X) - T(X)) \in \mathcal{O}_k[X].$$

L'ordre $\mathcal{O}_k[\Theta]$ est $\mathfrak{p}$-maximal si et seulement si $\operatorname{PGCD}(\overline{f}, \overline{g}, \overline{h}) = \overline{1}$.

(c) *Soit U un relèvement dans $\mathcal{O}_k[X]$ du quotient :*

$$\frac{\overline{T}}{\mathrm{PGCD}(\overline{f},\overline{g},\overline{h})},$$

on définit un nouvel ordre par :

$$\tilde{\mathcal{O}} := \mathcal{O}_k[\Theta] + U(\Theta)\mathfrak{p}^{-1}\mathcal{O}_k[\Theta].$$

Cet ordre contient $\mathcal{O}_k[\Theta]$ et même :

$$(\tilde{\mathcal{O}} : \mathcal{O}_k[\Theta]) = \mathfrak{p}^m$$

où m est le degré du polynôme $\mathrm{PGCD}(\overline{f},\overline{g},\overline{h})$.

Démonstration : On remarque pour commencer que l'élément τ est défini de telle sorte que la multiplication par τ revient localement à diviser par $\mathfrak{p}$. On définit l'idéal fractionnaire $\mathcal{O}_\tau$ par $\mathfrak{p}^{-1} = \tau\mathcal{O}_\tau$. Les éléments de $\mathcal{O}_\tau$ sont des $\mathfrak{p}$-entiers ; en particulier, il est possible de les réduire modulo $\mathfrak{p}$. Il est nécessaire de considérer tous ces objets car le corps k n'est pas *a priori* principal.

La démonstration suivante suit celle du théorème 6.1.4 de [**8**] ; elle est également intiment liée à l'algorithme Round 2 relatif tel qu'il apparaît dans [**12**].

Démontrons l'assertion (a). Il est clair que $\mathfrak{p}\mathcal{O}_k[\Theta] \subset I_\mathfrak{p}$ par définition. D'un autre côté, les exposants e_i sont tous majorés par $m := [K : k]$, d'où il s'ensuit que $\overline{T}(X) \mid \overline{g}(X)^m$ et $g(\Theta)^m \equiv 0 \pmod{\mathfrak{p}}$. On a donc :

$$\mathfrak{p}\mathcal{O}_k[\Theta] + g(\Theta)\mathcal{O}_k[\Theta] \subset I_\mathfrak{p}.$$

Réciproquement, soit $x := A(\Theta) \in I_\mathfrak{p}$. Il existe un entier $m \geq 1$ tel que $\overline{x}^m \in \mathfrak{p}\mathcal{O}_k[\Theta]$. En considérant l'isomorphisme canonique :

$$\frac{\mathcal{O}_k[\Theta]}{\mathfrak{p}\mathcal{O}_k[\Theta]} \cong \frac{\mathbb{F}_\mathfrak{p}[X]}{\overline{T}(X)\mathbb{F}_\mathfrak{p}[X]}$$

défini en envoyant $\overline{\Theta}$ sur la classe de X, on montre que $\overline{T}(X)$ divise $\overline{A}(X)^m$. Ainsi, chaque facteur irréductible de $\overline{T}$ dans $\mathbb{F}_\mathfrak{p}[X]$ divise $\overline{A}$ et donc $\overline{g} \mid \overline{A}$, ce qui termine la preuve de (a).

Pour (b), on remarque que si $\mathrm{PGCD}(\overline{f},\overline{g},\overline{h}) = 1$, alors $\overline{U} = \overline{T}$, d'où $U(\Theta) \in \mathfrak{p}\mathcal{O}_k[\Theta]$, ce qui implique $\tilde{\mathcal{O}} = \mathcal{O}_k[\Theta]$. Ainsi, pour démontrer (b), il suffit de montrer que cette dernière égalité équivaut à $\mathcal{O}_k[\Theta]$ $\mathfrak{p}$-maximal. Pour cela, on va prouver que $\tilde{\mathcal{O}}$ est l'ordre $\mathcal{O}'$ de la proposition 2.3 de [**12**] ce qui démontrera en même temps que $\tilde{\mathcal{O}}$ est un ordre et qu'il est $\mathfrak{p}$-maximal.

L'ordre $\mathcal{O}'$ est défini par :

$$\mathcal{O}' := \{x \in K \ / \ xI_\mathfrak{p} \subset I_\mathfrak{p}\},$$

donc $x \in \mathcal{O}'$ si et seulement si :

$$x\mathfrak{p} \in I_\mathfrak{p} \quad \text{et} \quad xg(\Theta) \in I_\mathfrak{p}$$

par (a). Mais, puisque $I_\mathfrak{p}$ est inclus dans $\mathcal{O}_k[\Theta]$, la première condition implique qu'il existe un polynôme $A_1(X) \in \mathcal{O}_\tau[X]$ tel que :

$$x = \tau A_1(\Theta).$$

On admet pour l'instant le lemme suivant :

Lemme 1.12. *Soit $x := \tau A_1(\Theta)$ un élément de K avec $A_1(X) \in \mathcal{O}_\tau[X]$.*

(i) *$x\mathfrak{p} \in I_\mathfrak{p}$ si et seulement si $\overline{g} \mid \overline{A}_1$.*
(ii) *On pose $\overline{s} := \overline{g}/\,\mathrm{PGCD}(\overline{f},\overline{g})$. Alors, $xg(\Theta) \in I_\mathfrak{p}$ si et seulement si $\overline{hs} \mid \overline{A}_1$.*

Ainsi, on trouve que $x \in \mathcal{O}'$ si et seulement si $\overline{g}$ et $\overline{hs}$ divisent tous deux $\overline{A}_1$ dans $\mathbb{F}_\mathfrak{p}[X]$. Cette condition est équivalente au fait que leur PPCM dans $\mathbb{F}_\mathfrak{p}[X]$ divise $\overline{A}_1$ et on trouve :

$$\begin{aligned}
\mathrm{PPCM}(\overline{g}, \overline{hs}) &= \mathrm{PPCM}(\overline{s}\,\mathrm{PGCD}(\overline{f}, \overline{g}), \overline{hs}) \\
&= \overline{s}\,\mathrm{PPCM}(\mathrm{PGCD}(\overline{f}, \overline{g}), \overline{h}) \\
&= \overline{s}\frac{\mathrm{PGCD}(\overline{f}, \overline{g})\overline{h}}{\mathrm{PGCD}(\overline{f}, \overline{g}, \overline{h})} \\
&= \frac{\overline{gh}}{\mathrm{PGCD}(\overline{f}, \overline{g}, \overline{h})} \\
&= \frac{\overline{T}}{\mathrm{PGCD}(\overline{f}, \overline{g}, \overline{h})} \\
&= \overline{U}.
\end{aligned}$$

Il s'ensuit donc que $x \in \tilde{\mathcal{O}}$ si et seulement si :

$$A_1(X) \in U(X)\mathcal{O}_\tau[X] + \mathfrak{p}\mathcal{O}_\tau[X],$$

ou encore :

$$\begin{aligned}
x \quad = \tau A_1(\Theta) \quad &\in U(\Theta)\tau\mathcal{O}_\tau[\Theta] + \tau\mathfrak{p}\mathcal{O}_\tau[\Theta] \\
&\in U(\Theta)\mathfrak{p}^{-1}\mathcal{O}_k[\Theta] + \mathcal{O}_k[\Theta] = \tilde{\mathcal{O}}.
\end{aligned}$$

Pour finir, il reste à démontrer la formule relative à l'indice. Pour cela, il suffit de remarquer qu'un système de représentants du quotient

$$\frac{\mathcal{O}_k[\Theta]}{U(\Theta)\mathfrak{p}^{-1}\mathcal{O}_k[\Theta]}$$

est obtenu en considérant les relèvements dans $\mathcal{O}_k[X]$ des polynômes de $\mathbb{F}_\mathfrak{p}[X]$ de degré plus petit que m. □

Il reste à démontrer le lemme.

Démonstration : On note π une uniformisante en $\mathfrak{p}$ telle que :

$$\tau\pi \equiv 1 \pmod{\mathfrak{p}}.$$

Démontrons (i). On a $\pi x \in I_\mathfrak{p}$ d'où :

$$\pi\tau A_1(\Theta) \in I_\mathfrak{p},$$

ce qui implique que $\overline{g}$ divise $\overline{\pi\tau A_1} = \overline{A}_1$ par (a).

Réciproquement, si $\overline{g} \mid \overline{A}_1$, on écrit :

$$A_1(X) = g(X)B(X) + C(X),$$

avec $B(X) \in \mathcal{O}_\tau[X]$ et $C(X) \in \mathfrak{p}\mathcal{O}_\tau[X]$. Et il en découle :

$$\begin{aligned}
x\mathfrak{p} \in \tau\mathfrak{p}A_1(\Theta) \quad &\subset \quad g(\Theta)\tau\mathfrak{p}\mathcal{O}_\tau[\Theta] + \tau\mathfrak{p}^2\mathcal{O}_\tau[\Theta] \\
&= \quad g(\Theta)\mathcal{O}_k[\Theta] + \mathfrak{p}\mathcal{O}_k[\Theta] = I_\mathfrak{p}.
\end{aligned}$$

Pour (ii), on remarque que $xg(\Theta) \in I_\mathfrak{p}$ si et seulement si il existe deux polynômes $A_2(X) \in \mathfrak{p}\mathcal{O}_k[X]$ et $A_3 \in \mathcal{O}_k[X]$ tels que :

$$\tau A_1(\Theta)g(\Theta) = A_2(\Theta) + g(\Theta)A_3(\Theta),$$

ou encore :

$$\pi\tau A_1(\Theta)g(\Theta) = \pi A_2(\Theta) + \pi g(\Theta)A_3(\Theta),$$

et donc il existe un polynôme $A_4 \in \mathcal{O}_\tau[X]$ tel que :

$$\pi\tau A_1(X)g(X) = \pi A_2(X) + \pi g(X)A_3(X) + A_4(X)T(X). \tag{1.6.8}$$

En réduisant modulo $\mathfrak{p}$, on obtient que :

$$\overline{A_1 g} = \overline{A_4 T},$$

et donc $\overline{A}_1 = \overline{A_4 h}$. Ainsi, on peut écrire :

$$\pi\tau A_1(X) = h(X)A_4(X) + A_5(X) \tag{1.6.9}$$

avec $A_5(X) \in \mathfrak{p}\mathcal{O}_\tau[X]$.

En remplaçant 1.6.9 dans 1.6.8, on trouve que $xg(\Theta) \in I_\mathfrak{p}$ si et seulement si il existe quatre polynômes $A_2(X) \in \mathfrak{p}\mathcal{O}_k[X]$, $A_3(X) \in \mathcal{O}_k[X]$, $A_4(X) \in \mathcal{O}_\tau[X]$ et $A_5(X) \in \mathfrak{p}\mathcal{O}_\tau[X]$ tels que :

$$(g(X)h(X) - T(X))A_4(X) = \pi A_2(X) + g(X)(\pi A_3(X) - A_5(X)).$$

En multipliant par τ, on montre que ceci équivaut à :

$$f(X)A_4(X) = B_2(X) + g(X)A_6(X),$$

où $B_2 = \tau\pi A_2 \in \mathfrak{p}\mathcal{O}_k[X]$ et $A_6 = \tau(\pi A_3 - A_5) \in \mathcal{O}_k[X]$. En réduisant à nouveau modulo $\mathfrak{p}$, on obtient $\overline{g} = \overline{fA_4}$ et donc $\overline{s}$ divise $\overline{A}_4$. Ainsi, on a montré que $\overline{hs} \mid \overline{A}_1$. □

Exemple : Le discriminant de T_k est $\mathfrak{p}_{103}^2$ où $\mathfrak{p}_{103}$ est l'idéal premier de k au-dessus de 103 donné par $\mathfrak{p}_{103} := 103\mathcal{O}_k + (-38 + \sqrt{2})\mathcal{O}_k$. On applique le critère de Dedekind à cet idéal.

On choisit pour élément τ :

$$\tau := \frac{38}{103} + \frac{1}{103}\sqrt{2}.$$

La factorisation de T_k modulo $\mathfrak{p}_{103}$ est :

$$T_k(X) = (X^3 + 47)^3 \pmod{\mathfrak{p}_{103}}$$

d'où on trouve $g(X) = X + 47$, $h(X) = (X + 47)^2$ et :

$$f(X) = \left(\frac{38}{103} + \frac{1}{103}\sqrt{2}\right)\Big((X + 47)^3 - (X^3 + \sqrt{2}X^2 + (\sqrt{2} - 3)X - 1)\Big)$$
$$= (52 + \sqrt{2})X^2 + (2446 + 64\sqrt{2})X + (38304 + 1008\sqrt{2}).$$

Il s'ensuit que $\overline{f(X)} = \overline{-13X^2 + 37X - 24}$ et :

$$\mathrm{PGCD}(\overline{f}, \overline{g}, \overline{h}) = \mathrm{PGCD}(\overline{f}, \overline{g}) = \overline{1}$$

donc l'ordre $\mathcal{O}_k[\Theta]$ est $\mathfrak{p}_{103}$-maximal et :

$$\mathcal{O}_K = \mathcal{O}_k[\Theta].$$

1.6.2. Décomposition des idéaux premiers dans les extensions relatives. Soit $\mathfrak{p}$ un idéal premier de k ne divisant pas l'indice de Θ. Dans ce cas, la décomposition de l'idéal $\mathfrak{p}$ dans l'extension relative K/k est donnée par la factorisation de T_k modulo $\mathfrak{p}$. Plus exactement, on a :

Théorème 1.13 (Dedekind)**.** *Soit $\mathfrak{p}$ un idéal premier ne divisant pas $\mathfrak{I}(\Theta)$. Supposons que T_k admette la factorisation suivante modulo $\mathfrak{p}$:*

$$T_k(X) \equiv \prod_{i=1}^{g} T_i(X)^{e_i} \pmod{\mathfrak{p}},$$

où les polynômes T_i sont des polynômes unitaires de $\mathcal{O}_k[X]$, irréductibles modulo $\mathfrak{p}$.

Alors, il existe exactement g idéaux premiers $\mathfrak{P}_i$ dans K au-dessus de $\mathfrak{p}$ et ils sont donnés par :

$$\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_K + T_i(\Theta)\mathcal{O}_K$$

pour tout i. De plus, l'indice de ramification de $\mathfrak{P}_i/\mathfrak{p}$ est l'exposant e_i et le degré résiduel de $\mathfrak{P}_i/\mathfrak{p}$ est le degré du polynôme $T_i(X)$.

Démonstration : Voir le théorème 2.27 de [**44**]. □

Exemple : On veut étudier la décomposition des deux idéaux premiers $\mathfrak{p}_{103}$ et $\mathfrak{q}_{103}$ de k dans l'extension K/k. Grâce à l'exemple précédent, on sait que l'ordre $\mathcal{O}_k[\Theta]$ est $\mathfrak{p}$-maximal pour tous les idéaux premiers $\mathfrak{p}$, donc on peut utiliser le théorème ci-dessus.

On factorise ce polynôme modulo $\mathfrak{p}_{103}$, on obtient :

$$T_k(X) \equiv (X+47)^3 \pmod{\mathfrak{p}_{103}},$$

ce qui prouve que $\mathfrak{p}_{103}$ est totalement ramifié dans K/k et que l'unique idéal premier de K au-dessus de $\mathfrak{p}_{103}$ est donné par :

$$\mathfrak{P}_{103} := \mathfrak{p}_{103}\mathcal{O}_K + (\Theta+47)\mathcal{O}_K.$$

On considère à présent la décomposition de $\mathfrak{q}_{103}$ dans K/k. On a :

$$T_k(X) \equiv (X+6)(X+18)(X+41) \pmod{\mathfrak{q}_{103}}.$$

Donc l'idéal $\mathfrak{q}_{103}$ est totalement décomposé dans K/k et les trois idéaux au-dessus sont donnés par :

$$\begin{aligned}
\mathfrak{Q}_{103,1} &:= \mathfrak{q}_{103}\mathcal{O}_K + (\Theta+6)\mathcal{O}_K,\\
\mathfrak{Q}_{103,2} &:= \mathfrak{q}_{103}\mathcal{O}_K + (\Theta+18)\mathcal{O}_K,\\
\mathfrak{Q}_{103,3} &:= \mathfrak{q}_{103}\mathcal{O}_K + (\Theta+41)\mathcal{O}_K.
\end{aligned}$$

1.6.3. Racines $\mathfrak{p}$-adiques de polynômes. Une autre application de la factorisation des polynômes modulo un idéal premier est le calcul des racines $\mathfrak{p}$-adiques d'un polynôme. On a pour cela le résultat bien connu (*cf* [**7**] lemme 3.1) :

Théorème 1.14 (Hensel)**.** *Soit F un extension finie de $\mathbb{Q}_p$. Soient $S(X)$ un polynôme à coefficients dans $\mathcal{O}_F$ et $n>0$ un entier. On note $\mathfrak{p}_F$ l'idéal premier de F.*

Supposons qu'il existe $\beta \in \mathcal{O}_F$ tel que :

$$S(\beta) \equiv 0 \pmod{\mathfrak{p}_F^n} \quad \textit{et} \quad S'(\beta) \not\equiv 0 \pmod{\mathfrak{p}_F^n}.$$

Alors, il existe un entier $\alpha \in \mathcal{O}_F$ tel que :

$$S(\alpha) = 0. \quad \square$$

Ainsi, soient $\mathfrak{p}$ un idéal premier et S un polynôme à coefficients dans $\mathcal{O}_k[X]$ (on peut voir S comme une approximation d'un polynôme à coefficients dans $\mathcal{O}_\mathfrak{p}[X]$ où $\mathcal{O}_\mathfrak{p}$ est l'anneau d'entiers du corps complété $k_\mathfrak{p}$). Alors, la détermination des racines de S dans $\mathcal{O}_\mathfrak{p}$ revient essentiellement à factoriser $S(X)$ modulo une puissance adéquate de $\mathfrak{p}$.

En particulier, si $\mathfrak{p}$ ne divise pas le discriminant de S, alors le polynôme S est séparable modulo $\mathfrak{p}$ et les racines de S modulo $\mathfrak{p}$ sont les réductions modulo $\mathfrak{p}$ des racines de S dans $\mathcal{O}_\mathfrak{p}$.

Exemple : Par exemple, on factorise le polynôme $\Phi_8(X) = X^4+1$ modulo l'unique idéal premier $\mathfrak{p}_3$ au-dessus de 3 dans k. On obtient :

$$\Phi_8(X) \equiv (X+2+\sqrt{2})(X+1+\sqrt{2})(X+1+2\sqrt{2})(X+2+2\sqrt{2}) \pmod{\mathfrak{p}_3},$$

ce qui prouve que $k_{\mathfrak{p}_3}$ contient les racines d'ordre 8 de l'unité.

1.6.4. Algorithme Round 4 relatif. On a déjà dit quelques mots sur cet algorithme dans le cas absolu dans la deuxième section. En fait, cet algorithme utilisant essentiellement des calculs p-adiques, il est possible de le généraliser assez facilement au cas relatif. Cependant, on ne donnera pas tous les détails fastidieux de cette généralisation ; on renvoie pour cela au cas absolu (*cf* [**20**], [**21**] et [**22**]).

Pour un idéal premier fixé $\mathfrak{p}$, l'algorithme Round 4 relatif calcule des éléments $\omega_i \in \mathcal{O}_k[\Theta]$ et des entiers $e_i \geq 0$ tels que :

$$\mathcal{O}_{K,\mathfrak{p}} = \omega_1\tau^{e_1}\mathcal{O}_\mathfrak{p} + \cdots + \omega_m\tau^{e_m}\mathcal{O}_\mathfrak{p} \tag{1.6.10}$$

où $\mathcal{O}_{K,\mathfrak{p}}$ est l'ordre maximal de $K_\mathfrak{p} := \prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$, $m := [K:k]$ et l'élément τ est défini comme dans le théorème 1.11. Pour en déduire un ordre $\mathfrak{p}$-maximal de $\mathcal{O}_K$, on utilise le lemme suivant :

Lemme 1.15. *Avec les notations ci-dessus, l'ordre :*

$$\omega_1\mathfrak{p}^{-e_1} + \cdots + \omega_m\mathfrak{p}^{-e_m}$$

est un ordre $\mathfrak{p}$-maximal de $\mathcal{O}_K$.

Démonstration : Soit $\mathcal{O}'$ l'ordre défini dans l'énoncé du lemme. Il est évident que $\mathcal{O}' \subset \mathcal{O}_K$, puisque les éléments $\omega_i\tau^{e_i}$ sont tous des entiers $\mathfrak{p}$-adiques et des éléments de K. On note $\mathfrak{I}$ l'indice de $\mathcal{O}'$ dans $\mathcal{O}_K$; $\mathfrak{I}$ est un idéal entier de k et $\mathcal{O}'$ est $\mathfrak{p}$-maximal si et seulement si $\mathrm{val}_\mathfrak{p}(\mathfrak{I}) = 0$.

On considère la suite exacte :

$$1 \longrightarrow \mathcal{O}' \longrightarrow \mathcal{O}_K \longrightarrow \mathfrak{I} \longrightarrow 1$$

le module $\mathcal{O}_\mathfrak{p}$ étant plat (*cf* [**35**] chap. XVI, §3), on peut tensoriser tous ces $\mathcal{O}_k$-modules par $\mathcal{O}_\mathfrak{p}$ en conservant la suite exacte.

On calcule :

$$\begin{aligned}
\mathcal{O}' \otimes_{\mathcal{O}_k} \mathcal{O}_\mathfrak{p} &= \mathcal{O}_{K,\mathfrak{P}} \text{ par 1.6.10,} \\
\mathcal{O}_K \otimes_{\mathcal{O}_k} \mathcal{O}_\mathfrak{p} &= \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_\mathfrak{P} = \mathcal{O}_{K,\mathfrak{p}} \text{ par [47] chap. II §4 prop. 4,} \\
\mathfrak{I} \otimes_{\mathcal{O}_k} \mathcal{O}_\mathfrak{p} &= \mathfrak{p}^{\mathrm{val}_\mathfrak{p}(\mathfrak{I})}.
\end{aligned}$$

On obtient la suite exacte :

$$1 \longrightarrow \mathcal{O}_{K,\mathfrak{p}} \longrightarrow \mathcal{O}_{K,\mathfrak{p}} \longrightarrow \mathfrak{p}^{\mathrm{val}_\mathfrak{p}(\mathfrak{I})} \longrightarrow 1$$

ce qui démontre que $\mathrm{val}_\mathfrak{p}(\mathfrak{I}) = 0$. □

Ainsi, pour un idéal premier $\mathfrak{p}$ fixé, on va s'intéresser uniquement à la détermination des entiers algébriques ω_i et des exposants e_i tels que l'équation 1.6.10 soit vérifiée.

On commence par fixer un certain nombre de notations et de résultats. On note π une uniformisante de $\mathfrak{p}$ dans $\mathcal{O}_k$ telle que $\tau\pi \equiv 1 \pmod{\mathfrak{p}}$.

Soit α un élément de $\mathcal{O}_{K,\mathfrak{p}}$, on note χ_α son polynôme caractéristique sur $k_\mathfrak{p}$. On dit que α est *primaire* s'il existe un polynôme irréductible $\nu \in \mathbb{F}_\mathfrak{p}[X]$ tel que :

$$\chi_\alpha(X) \equiv \nu(X)^e \pmod{\mathfrak{p}}$$

pour un certain $e \geq 1$. On note alors ν_α un relèvement unitaire du polynôme ν.

Le résultat suivant est une application directe du théorème 1.14 :

Proposition 1.16. *Soient $U(X), V(X) \in \mathcal{O}_\mathfrak{p}[X]$ deux polynômes unitaires tels que :*

$$U(X) \equiv V(X) \pmod{\mathfrak{p}^v}$$

où $v \geq 2\,\mathrm{val}_\mathfrak{p}(\mathrm{disc}(U)) + 1$.

Alors, on a un isomorphisme de $k_\mathfrak{p}$-algèbres :

$$\frac{k_\mathfrak{p}[X]}{(U(X)k_\mathfrak{p}[X])} \cong \frac{k_\mathfrak{p}[X]}{(V(X)k_\mathfrak{p}[X])}.$$

En particulier, ces deux algèbres admettent des anneaux d'entiers isomorphes en tant que $\mathcal{O}_\mathfrak{p}$-modules.

Démonstration : Soit θ une racine de V ; on note $E := k_\mathfrak{p}(\theta)$. Alors, la réduction de θ modulo $\mathfrak{p}^v$, disons $\overline{\theta}$, est une racine de U (modulo $\mathfrak{p}^v$) puisque :

$$U(\theta) \equiv V(\theta) = 0 \pmod{\mathfrak{p}^v}.$$

D'un autre côté, puisque $v > 2\,\mathrm{val}_\mathfrak{p}(\mathrm{disc}(U)) + 1$, le polynôme U est séparable modulo $\mathfrak{p}^v$ et donc $\overline{\theta}$ est une racine simple de $\overline{U}$. En vertu du théorème 1.14, il s'ensuit qu'il existe une racine de U contenue dans E et donc un plongement de $\frac{k_\mathfrak{p}[X]}{(U(X)k_\mathfrak{p}[X])}$ dans $\frac{k_\mathfrak{p}[X]}{(V(X)k_\mathfrak{p}[X])}$. Par symétrie, on obtient un plongement dans l'autre sens, ce qui démontre le résultat. □

On va utiliser ce résultat par le biais suivant :

Corollaire 1.17. *Soit $U(X)$ un polynôme séparable de $\mathcal{O}_\mathfrak{p}[X]$; on note $v := \mathrm{val}_\mathfrak{p}(\mathrm{disc}(U))$. Supposons qu'il existe deux polynômes U_1 et U_2 premiers entre eux tels que :*

$$U(X) \equiv U_1(X)U_2(X) \pmod{\mathfrak{p}^{2v+1}}.$$

On note x la réduction de X modulo $U(X)$ et x_i la réduction de X modulo $U_i(X)$ pour $i = 1, 2$.

Soit $(\epsilon_1(x), \epsilon_2(x))$ un couple d'idempotents orthogonaux de $k_\mathfrak{p}[x]$; alors, le morphisme :

$$\begin{array}{rcl} k_\mathfrak{p}[x_1] \oplus k_\mathfrak{p}[x_2] & \to & k_\mathfrak{p}[x] \\ (V_1(x_1), V_2(x_2)) & \mapsto & \epsilon_1(x)V_1(x) + \epsilon_2 V_2(x) \end{array}$$

est un isomorphisme de $k_\mathfrak{p}$-algèbres. □

Remarque : Dire que ϵ_1 et ϵ_2 sont des idempotents orthogonaux signifie que :

$$\epsilon_1(x) + \epsilon_2(x) = 1 \ \text{ et } \ \epsilon_1(x)\epsilon_2(x) = 0.$$

On peut construire de tels idempotents grâce à l'algorithme suivant :

Algorithme 1.18. *Etant donnés trois polynômes U, U_1 et U_2 vérifiant les hypothèses du corollaire 1.17, cet algorithme calcule un polynôme ϵ tel que ϵ et $1 - \epsilon$ sont des idempotents orthogonaux et deux nouveaux polynômes U_1 et U_2 (la procédure de calcul de ϵ nécessite en effet une modification de ces deux polynômes pour que la construction soit exacte).*

1. *On calcule deux polynômes a_1 et a_2 de $\mathbb{F}_\mathfrak{p}[X]$ tels que :*

$$a_1(X)U_1(X) + a_2(X)U_2(X) \equiv 1 \pmod{\mathfrak{p}}.$$

On pose $\epsilon(x) \leftarrow a_1(x)U_1(x) \bmod \mathfrak{p}$, $v \leftarrow \mathrm{val}_\mathfrak{p}(\mathrm{disc}(U))$ et $k \leftarrow 1$.

2. *Tant que $k \leq 3v + 1$, on pose :*

$$\epsilon(x) \leftarrow 3\epsilon(x)^2 - 2\epsilon(x)^3 \bmod \mathfrak{p}^{2k}$$

puis $k \leftarrow 2k$ et on recommence cette étape.

3. *On pose :*

$$U_1(X) \leftarrow \mathrm{PGCD}(U(X), 1 - \epsilon(X))$$

dans $\mathcal{O}_k[X]$ et $U_2(X) \leftarrow U(X)/U_1(X) \bmod \mathfrak{p}^{2v+1}$. On retourne $\epsilon(x), U_1(x)$ et $U_2(x)$ et l'algorithme se termine.

Soit α un élément de $O_{K,\mathfrak{p}}$; on écrit :

$$\chi_\alpha(X) = X^m + a_1 X^{m-1} + \cdots + a_m,$$

la *valuation* val^* est définie par :

$$\mathrm{val}^*(\alpha) := \mathrm{Min}_i \, \frac{\mathrm{val}_\mathfrak{p}(a_i)}{i} \tag{1.6.11}$$

où a_i parcourt les coefficients non nuls de χ_α.

Le $\mathfrak{p}$-*radical* est l'unique idéal premier de $\mathcal{O}_{K,\mathfrak{p}}$; il est défini par :

$$\mathfrak{I}_\mathfrak{p} := \{\eta \in \mathcal{O}_{K,\mathfrak{p}} \ / \ \mathrm{val}^*(\eta) > 0\}.$$

Pour un élément α primaire, on définit le $\mathfrak{p}$-*radical de* α par $\mathfrak{I}_\alpha := \mathfrak{I}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}[\alpha]$; c'est également l'unique idéal premier de l'anneau $\mathcal{O}_\mathfrak{p}[\alpha]$.

Proposition 1.19. *La valuation* val^* *vérifie les propriétés suivantes :*

- $\alpha \in k_\mathfrak{p} \Rightarrow \mathrm{val}^*(\alpha) = \mathrm{val}_\mathfrak{p}(\alpha)$.
- $\mathrm{val}^*(\alpha + \beta) \geq \mathrm{Min}(\mathrm{val}^*(\alpha), \mathrm{val}^*(\beta))$ *avec égalité si* $\mathrm{val}^*(\alpha) \neq \mathrm{val}^*(\beta)$.
- $\mathrm{val}^*(\alpha\beta) \geq \mathrm{val}^*(\alpha) + \mathrm{val}^*(\beta)$ *avec égalité si α ou β appartient à $k_\mathfrak{p}$.*
- $\mathrm{val}^*(\alpha^n) = n\,\mathrm{val}^*(\alpha)$ *pour $n \in \mathbb{N}$.*
- $\mathrm{val}^*(\alpha) \geq M \Rightarrow \mathrm{val}_i(\alpha_i) \geq M$ *pour tout i, où α_i parcourt les conjugués (sur $k_\mathfrak{p}$) de α et* val_i *est l'unique valuation prolongeant* $\mathrm{val}_\mathfrak{p}$ *à $k_\mathfrak{p}(\alpha_i)$.*
- *si α est primaire,* $\mathrm{val}^*(\alpha) > 0 \Rightarrow \nu_\alpha(X) \equiv X \pmod{\mathfrak{p}}$.
- *si α et β sont primaires,* $\mathrm{val}^*(\alpha) = \mathrm{val}^*(\beta) = 0 \Rightarrow \mathrm{val}^*(\alpha\beta) = 0$.

- *si α et β sont primaires,* $\mathrm{val}^*(\alpha-\beta)>0 \Rightarrow \nu_\alpha(X)\equiv\nu_\beta(X) \pmod{\mathfrak{p}}$.
- *si α est primaire, le quotient $\mathcal{O}_\mathfrak{p}[\alpha]/\mathfrak{I}_\alpha$ est un corps et ν_α est le polynôme irréductible de $\alpha+\mathfrak{I}_\alpha$ sur $\mathbb{F}_\mathfrak{p}$.*

Démonstration : Toutes ces assertions sont des généralisations directes des résultats de [**21**]. □

Soit α un élément primaire de $\mathcal{O}_{K,\mathfrak{p}}$, et $d_\alpha := \deg(\nu_\alpha)$. Ecrivons :

$$\mathrm{val}^*(\nu_\alpha(\alpha)) = l_\alpha/m_\alpha, \tag{1.6.12}$$

où l_α et m_α sont deux entiers positifs premiers entre eux, avec la convention que $(l_\alpha, m_\alpha)=(0,1)$ si $\mathrm{val}^*(\nu_\alpha(\alpha))=0$.

On associe à l'élément α un nouvel élément de $\mathcal{O}_{K,\mathfrak{p}}$ défini par :

$$\eta(\alpha) := \tau^s \nu_\alpha(\alpha)^r, \tag{1.6.13}$$

où les entiers r et s sont positifs (et même $r>0$) et sont choisis minimaux parmi les entiers vérifiant la relation de Bezout :

$$r l_\alpha - s m_\alpha = 1 \ ;$$

(*ie* $r \le m_\alpha$ et $s \le l_\alpha$).

Lemme 1.20. *Pour α un élément primaire, on a :*

$$\mathrm{val}^*(\eta(\alpha)) = 1/m_\alpha.$$

Démonstration : Grâce aux propriétés de val^*, on trouve :

$$\begin{aligned}\mathrm{val}^*(\eta(\alpha)) &= \mathrm{val}^*(\tau^s\nu_\alpha(\alpha)^r) = s\,\mathrm{val}^*(\tau) + r\,\mathrm{val}^*(\nu_\alpha(\alpha))\\ &= -s + r\frac{l_\alpha}{m_\alpha} = 1/m_\alpha. \quad \square\end{aligned}$$

On peut à présent donner une idée assez précise de l'algorithme Round 4 relatif. Il est à noter que cet algorithme est très similaire à celui donné dans [**22**].

L'algorithme procède comme suit : on considère pour commencer l'ordre défini par un élément entier α de K. Si cet ordre est $\mathfrak{p}$-maximal (on utilise le critère de Dedekind pour tester cette propriété), alors on renvoie cet ordre et c'est fini. Sinon, deux cas se présentent : ou bien l'élément α n'est pas primaire et en utilisant le corollaire 1.17 par le biais de l'algorithme 1.18, on peut casser cet ordre en deux ordres explicites ; il suffit alors d'appliquer la même méthode récursivement à chacun de ces deux ordres. Ou bien l'élément α est primaire et dans ce cas, l'algorithme ROUND 4 construit une suite d'éléments de K qui aboutit en un nombre fini d'étapes soit à un élément vérifiant le critère de Dedekind (et on retrouve le premier cas), soit à un élément non primaire (et on retrouve le second) ; c'est la partie la plus complexe de l'algorithme.

Algorithme 1.21. *Etant donnés un polynôme T_k unitaire et irréductible dans $\mathcal{O}_k[X]$ et un idéal premier $\mathfrak{p}$, l'algorithme Round 4 relatif calcule une pseudo-base de K/k (où $K := k(\Theta)$ pour Θ une racine de T_k) au sens de* [**9**] *d'un ordre $\mathfrak{p}$-maximal de K. Cet algorithme fonctionne de manière récursive.*

1. *Appeler la procédure* **Maxord***(T_k) : la réponse est un ensemble d'entiers algébriques $\{\omega_i\}_i$ et d'exposants $e_i \ge 0$ vérifiant 1.6.10. Retourner la pseudo-base $(\omega_i, \mathfrak{p}^{-e_i})_i$ et terminer.*

- **Maxord***(U)*

  Maxord.1. *On factorise U modulo $\mathfrak{p}$.*

  Si U vérifie le critère de Dedekind relatif à $\mathfrak{p}$, on retourne la base calculée par **Dbasis**(U) *et on termine cette procédure.*

  Sinon, si U admet modulo $\mathfrak{p}$ deux facteurs non triviaux premiers entre eux, on retourne la base calculée par **Decomp**(U) *et on termine cette procédure ; sinon, on retourne la base calculée par* **Nilord**(U) *et on termine cette procédure.*

- **Decomp***(U)*

  Decomp.1. *Soient V_1 et V_2 deux facteurs non triviaux de U modulo $\mathfrak{p}$, premiers entre eux et tels que $U \equiv V_1V_2 \pmod{\mathfrak{p}}$. A l'aide de l'algorithme 1.18, on calcule deux idempotents ϵ, $1-\epsilon$ et deux polynômes U_1 et U_2 vérifiant les hypothèses du corollaire 1.17.*

Decomp.2. *On appelle la procédure* **Maxord**(U_1) *: notons* $\{\omega_{1,1}\tau^{e_{1,1}}, \dots, \omega_{1,s_1}\tau^{e_{1,s_1}}\}$ *la base retournée. De même, on note* $\{\omega_{2,1}\tau^{e_{2,1}}, \dots, \omega_{2,s_2}\tau^{e_{2,s_2}}\}$ *la base retournée par la procédure* **Maxord**(U_2).

Decomp.3. *On retourne la base :*

$$\{\epsilon\omega_{1,1}\tau^{e_{1,1}}, \dots, \epsilon\omega_{1,s_1}\tau^{e_{1,s_1}}, (1-\epsilon)\omega_{2,1}\tau^{e_{2,1}}, \dots, (1-\epsilon)\omega_{2,s_2}\tau^{e_{2,s_2}}\}$$

et cette procédure se termine.

- **Nilord**(U)

Nilord.1. *On note* ξ *une racine de* U*. Puis, on pose* $\alpha \leftarrow \xi$.

Nilord.2. *On calcule* χ_α *le polynôme caractéristique de* α*. Puis, soit* ν_α *un facteur irréductible de* χ_α *modulo* $\mathfrak{p}$*. Si* ν_α *n'est pas le seul facteur irréductible de* α *modulo* $\mathfrak{p}$ *alors on retourne la base calculée par* **Decomp**(χ_α) *et cette procédure se termine.*

Nilord.3. *On calcule le discriminant* $\mathcal{D}_\alpha$ *du polynôme* χ_α*. Si* $\mathcal{D}_\alpha = 0$*, on pose* $\alpha \leftarrow \alpha + \pi\xi$ *et on retourne à l'étape* **Nilord.2**.

Nilord.4. *Si* χ_α *vérifie le critère de Dedekind relatif à* $\mathfrak{p}$*, on retourne la base calculée par* **Dbasis**(χ_α) *et cette procédure se termine.*

Nilord.5. *Si* $\mathrm{val}^*(\alpha) > 0$*, on pose* $\alpha \leftarrow \alpha + 1$ *et on retourne à l'étape* **Nilord.2**. *Sinon, on définit* l_α *et* m_α *par la formule 1.6.12 et on calcule* η_α *par 1.6.13. Si* $l_\alpha > 1$*, on remplace* $\alpha \leftarrow \alpha + \eta_\alpha(\alpha)$ *et on retourne à l'étape* **Nilord.2**.

Nilord.6. *Soit* ϕ *l'élément retourné par la procédure* **Bsrch**$(\chi_\alpha, \eta_\alpha, m_\alpha)$*. On calcule* χ_ϕ *son polynôme caractéristique. Si* ϕ *n'est pas primaire, on retourne l'ordre calculé par* **Decomp**(χ_ϕ) *et cette procédure se termine ; sinon, on pose* $\alpha \leftarrow \phi$ *et on retourne à l'étape* **Nilord.2**.

- **Bsrch**$(\chi_\alpha, \eta_\alpha, m_\alpha)$

Bsrch.1. *On pose* $\beta \leftarrow \tau\nu_\alpha(\alpha)^{m_\alpha}$*, puis* $c \leftarrow 1$.

Bsrch.2. *Si* β *n'est pas primaire, on retourne* β *et cette procédure se termine.*

Bsrch.3. *Si* $d_\beta \nmid d_\alpha$ *(où* $d_\alpha := \deg(\nu_\alpha)$ *où* ν_α *est un relèvement unitaire de l'unique facteur irréductible de* χ_α *modulo* $\mathfrak{p}$*), alors il existe* $\phi \in \beta + \mathcal{O}_\mathfrak{p}[\alpha]$ *tel que ou* ϕ *est non primaire ou* $d_\phi = \mathrm{PPCM}(d_\alpha, d_\beta)$ *; on retourne* ϕ *et cette procédure se termine.*

Bsrch.4. *Si* $m_\beta \nmid m_\alpha$*, on calcule un élément* ϕ *tel que* $d_\phi = d_\alpha$ *et* $m_\phi = \mathrm{PPCM}(m_\alpha, m_\beta)$*, on retourne* ϕ *et cette procédure se termine.*

Bsrch.5. *Si* $c = 1$*, on pose* $g \leftarrow m_\alpha \,\mathrm{val}^*(\beta)$*, de telle sorte que* $\mathrm{val}^*(\nu_\alpha(\alpha)^g) = \mathrm{val}^*(\beta)$*. Puis, on pose* $\beta \leftarrow \beta/\nu_\alpha(\alpha)^g$*,* $c \leftarrow c + 1$ *et on retourne en* **Bsrch.2**.

Bsrch.6. *Si* $c = 2$*, on pose* $\gamma \leftarrow \beta$ *et* $\beta \leftarrow \beta^{q^{d_\alpha r}}$*, où la puissance de* $q := \mathcal{N}\mathfrak{p}$ *est suffisamment grande (cf discussion plus loin). Puis, on pose* $c \leftarrow c + 1$ *et on retourne en* **Bsrch.2**.

Bsrch.7. *Si* $\beta \in \mathcal{O}_\mathfrak{p}[\alpha]$*, alors il existe* $h(X) \in \mathcal{O}_\mathfrak{p}[X]$ *tel que* $\phi := \gamma + h(\alpha)$ *n'est pas primaire, on retourne* ϕ *et cette procédure se termine. Sinon, on pose* $\beta \leftarrow \nu_\alpha(\alpha)^g(\gamma - \beta)$*,* $c \leftarrow 1$ *et on repart en* **Bsrch.2**.

- **Dbasis**(T)

Dbasis.1. *En appliquant le théorème 1.11, on calcule une base* $\mathfrak{p}$*-maximal de l'ordre défini par une racine de* T*. Puis on retourne cette base et cette procédure se termine.*

Remarques :

- Beaucoup d'affectations dans cet algorithme ont été données telles quelles par un souci de simplicité (l'algorithme étant déjà assez compliqué par lui-même) ; mais, en fait, pour éviter de travailler avec des nombres trop grands, ces affectations s'entendent le plus souvent modulo une puissance convenable de $\mathfrak{p}$.
- De même, dans la plupart des cas, il est possible de remplacer la notion de discriminant par celle de discriminant réduit, ce qui simplifie également les calculs. On renvoie à [**44**] pour plus de détails sur cette notion.

- Pour prouver que la procédure **Nilord** retourne un résultat en un nombre fini d'étapes, on remarque que la valuation $\mathrm{val}^*(\beta)$ croît à chaque fin de procédure ; or cette valuation est bornée par $\mathrm{val}_{\mathfrak{p}}(\mathcal{D}_\alpha)$. Donc une des quatre possibilités suivantes doit intervenir après un nombre fini d'étapes : ou bien on découvre un élément de Dedekind (*ie* dont le polynôme caractéristique vérifie le critère de Dedekind) et le problème est réglé ; ou bien on découvre un élément non primaire et on applique la procédure **Decomp** (ceci diminue strictement le rang de l'ordre à considérer et donc ne peut intervenir qu'un nombre fini de fois) ; ou bien on trouve un élément θ tel que $d_\theta \nmid d_\alpha$ ou tel que $m_\theta \nmid m_\alpha$ mais chacun de ces cas ne peut intervenir qu'un nombre fini de fois puisque d_α et m_α sont majorés par le degré de l'extension $[K : k]$.
- A l'étape **Bsrch.6**, on veut déterminer une puissance de $q := \mathcal{N}\mathfrak{p}$ suffisamment grande pour avoir :
$$\theta^{q^{d_\alpha r}} \in \mathcal{O}_{\mathfrak{p}}[\alpha]$$
pour tout $\theta \in \mathcal{O}_{\mathfrak{p}}[\alpha] + \mathfrak{I}_{\mathfrak{p}}$. On écrit $\theta = \phi + \psi$ avec $\phi \in \mathcal{O}_{\mathfrak{p}}[\alpha]$ et $\psi \in \mathfrak{I}_{\mathfrak{p}}$. Pour $s \geq 0$, on a par la formule du binôme :
$$\theta^{q^s} = \sum_{i=0}^{q^s} \binom{q^s}{i} \psi^i \phi^{q^s - i}.$$
Si $i > m\delta_\alpha$ où $\delta_\alpha := \mathrm{val}_{\mathfrak{p}}(\mathcal{D}_\alpha)$, on a $\mathrm{val}^*(\psi^i) \geq \delta_\alpha$ puisque $\psi \in \mathfrak{I}_{\mathfrak{p}}$ et donc $\mathrm{val}^*(\psi) \geq 1/m$ (on rappelle que $m := [K : k]$). Il s'ensuit que $\psi^i \in \mathcal{O}_{\mathfrak{p}}[\alpha]$ puisque $\mathcal{D}_\alpha \mathcal{O}_{K,\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}[\alpha]$ et donc ce terme appartient bien à $\mathcal{O}_{\mathfrak{p}}[\alpha]$.
Si $i \leq m\delta_\alpha$, on vérifie d'abord que pour $i = 0$, on a bien $q^s \phi^{q^s} \in \mathcal{O}_k[\alpha]$. On peut donc supposer que $i \neq 0$. Dans ce cas, on calcule :
$$\mathrm{val}^*\left(\binom{q^s}{i}\right) \geq \mathrm{val}^*(q^s) - \mathrm{val}^*(i!) \geq e\left(fs - \frac{i-1}{p-1}\right)$$
où e (respectivement f) est l'indice de ramification (respectivement le degré d'inertie) absolue de $\mathfrak{p}$. Ainsi, il suffit d'avoir $e(fs - (i-1)/(p-1)) \geq \delta_\alpha$ et on peut prendre :
$$s = \left\lceil \frac{\delta_\alpha(p + em - 1) - e - 1}{ef(p-1)} \right\rceil$$
puis $r = \lceil s/d_\alpha \rceil$.
- Il est nécessaire durant la procédure **Decomp** ou, plus exactement dans l'algorithme 1.18 de calculer des PGCD dans l'anneau $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^i$ pour $i > 1$. On renvoie à [**22**] pour plus de détails sur la mise en œuvre de tels calculs.
- L'algorithme étant particulièrement compliqué, il n'a pas encore été possible de procéder à une implémentation complète sur ordinateur. C'est pourquoi on ne donne pas d'exemple de cette application.
- De manière similaire aux résultats de la section 2, il est possible de modifier cet algorithme pour en déduire un algorithme de factorisation $\mathfrak{p}$-adique des polynômes.

CHAPITRE 2

CALCUL DE CERTAINS CORPS DE CLASSES DE RAYON PAR LES UNITÉS DE STARK

Le but de ce chapitre est de décrire une méthode de construction explicite de certains corps de classes de rayon de corps totalement réels. Cette méthode s'inspire des idées originales de Stark et des premiers calculs fait en ce sens dans [**48**] et [**49**] (et développés dans [**50**]) ; comme elle repose sur une formulation simplifiée des conjectures de Stark, cette méthode n'est valide que sous l'hypothèse que cette conjecture est vraie (*cf* [**17**] pour une description récente des résultats obtenus sur cette conjecture). Néanmoins, une fois le résultat obtenu (*ie* une fois connu un élément supposé primitif du corps de classes de rayon), il est possible de vérifier si cet élément définit bien le corps voulu et ainsi obtenir une preuve directe faisant abstraction de la conjecture de départ.

On appliquera cette méthode dans le prochain chapitre pour construire le corps de classes de Hilbert de corps quadratiques, cubiques et quartiques totalement réels. Le contenu des sections 2 et 3 dans le cas où le corps à construire est le corps de classes de Hilbert a fait l'objet d'une note, *cf* [**46**].

2.1. Les conjectures de Stark dans le cas abélien[†]

Soit K/k une extension abélienne de corps de nombres ; on note $G := \mathrm{Gal}(K/k)$ son groupe de Galois et $\mathfrak{f}$ son conducteur. On fixe S un ensemble fini de places de k contenant les places infinies de k ainsi que les places finies de k qui se ramifient dans K.

On peut associer à une telle extension (et à la donnée d'un tel ensemble S) des objets analytiques classiques. Pour $\sigma \in G$, on définit la fonction zêta partielle donnée pour $s \in \mathbb{C}$ avec $\Re(s) > 1$ par la série de Dirichlet :

$$\zeta_S(s,\sigma) := \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_\mathfrak{a}=\sigma}} \mathcal{N}\mathfrak{a}^{-s} \tag{2.1.14}$$

où $\mathfrak{a}$ parcourt les idéaux entiers de k, non divisibles par les idéaux premiers contenus dans S et dont le symbole d'Artin $\sigma_\mathfrak{a}$ vaut σ.

Pour $\chi \in \hat{G}$, on définit une fonction L d'Artin donnée pour $s \in \mathbb{C}$ avec $\Re(s) > 1$ par le produit eulérien :

$$L_S(s,\chi) := \prod_{\mathfrak{p} \notin S} (1 - \chi(\sigma_\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1}$$

[†]La référence pour toute cette section est le chapitre IV de [**52**].

où $\mathfrak{p}$ parcourt les idéaux premiers de k qui ne sont pas dans S. Notons que l'application d'Artin permet de voir le caractère χ comme un caractère de $\mathrm{Cl}_k(\mathfrak{f})$ et, par la même, comme une application de $I_k(\mathfrak{f})$ dans $\mathbb{C}^\times$; ainsi, on note dans la suite $\chi(\mathfrak{a}) := \chi(\sigma_\mathfrak{a})$ pour un idéal $\mathfrak{a} \in I_k(\mathfrak{f})$.

Toutes ces fonctions admettent des prolongements méromorphes à tout le plan complexe (et même holomorphes pour $L_S(s,\chi)$ si le caractère χ est non trivial) et sont liées par les deux formules équivalentes :

$$\zeta_S(s,\sigma) = \frac{1}{[K:k]} \sum_{\chi \in \hat{G}} L_S(s,\chi)\bar{\chi}(\sigma) \quad \text{pour tout } \sigma \in G, \tag{2.1.15}$$

$$L_S(s,\chi) = \sum_{\sigma \in G} \zeta_S(s,\sigma)\chi(\sigma) \quad \text{pour tout } \chi \in \hat{G}. \tag{2.1.16}$$

Pour χ un caractère de G, on note $s(\chi)$ le nombre de places $v \in S$ dont le groupe de décomposition est inclu dans le noyau de χ, *ie* telles que $\chi_{|D_v} = 1$. L'ordre $r(\chi)$ de la fonction $L_S(s,\chi)$ en $s = 0$ est donné par la formule :

$$r(\chi) = s(\chi) \text{ si } \chi \neq 1_{\hat{G}} \text{ et } r(1_{\hat{G}}) = s(1_{\hat{G}}) - 1. \tag{2.1.17}$$

On suppose désormais que S contient une place v totalement décomposée dans K/k et on fixe w une place de K au-dessus de v. En particulier, si $\mathrm{card}(S) \geq 2$, on a $L_S(0,\chi) = 0$ pour tout caractère de G et donc $\zeta_S(0,\sigma) = 0$ pour tout $\sigma \in G$.

Conjecture 2.1 (Stark)**.** *Soit $m := |W_K|$ le nombre de racines de l'unité contenues dans K. Il existe une unité $\varepsilon \in K$ telle que :*

$$\log|\sigma(\varepsilon)|_w = -m\zeta'_S(0,\sigma) \text{ pour tout } \sigma \in G \tag{2.1.18}$$

ou, de manière équivalente par 2.1.16 :

$$L'_S(0,\chi) = -\frac{1}{m}\sum_{\sigma \in G} \chi(\sigma)\log|\sigma(\varepsilon)|_w \text{ pour tout } \chi \in \hat{G}. \tag{2.1.19}$$

(Notons que pour tout $u \in W_K$, l'unité $u\varepsilon$ vérifie aussi 2.1.18.)

De plus, pour une telle unité ε, l'extension $K(\sqrt[m]{\varepsilon})/k$ est abélienne et donc ne dépend que de la classe de ε modulo W_K.

Remarque : Soient ε et ε' deux unités de K vérifiant 2.1.18, alors l'unité $u = \varepsilon'\varepsilon^{-1}$ vérifie $|u|_{w'} = 1$ pour toute place w' au-dessus de v. En particulier, si de telles places sont complexes, il existe des unités u vérifiant de telles conditions qui ne sont pas des racines de l'unité. En fait, on montre (*cf* lemme 2.14) que dans la construction à suivre, si w' est une place complexe, on a $|\varepsilon|_{w'} = 1$.

L'intérêt de cette conjecture est immédiat : à partir d'objets du corps de base (les fonctions zêta partielles), elle permet de construire un objet de l'extension K (les unités ε) par le biais de la formule 2.1.18. Ainsi, on va supposer cette conjecture vraie par la suite afin d'en déduire une méthode de calcul explicite de K. Cependant, plusieurs restrictions sont nécessaires.

La première concerne le fait que, après avoir calculé des valeurs approchées satisfaisantes des fonctions zêta, il faut ôter une valeur absolue associée à la place w fixée pour en déduire des valeurs approchées des conjugués de ε. Mais, ceci n'est possible que si cette valeur absolue est réelle (auquel cas il y a deux possibilités) et non complexe ou $\mathfrak{p}$-adique (auquel cas il y a une infinité de possibilités). On est donc amené à supposer que la place w et aussi par conséquent la place v sont réelles.

La seconde restriction concerne le cas où l'ensemble S contient plus d'une place totalement décomposée.

Proposition 2.2. *Supposons que la place w est réelle et que S contient au moins deux places totalement décomposées dans K/k.*

Alors, la conjecture 2.1 est vraie et on peut choisir $\varepsilon \in k$. Si, de plus, le cardinal de S est supérieur ou égal à 3, alors on a $\varepsilon = \pm 1$.

Démonstration : On ne démontre que la deuxième affirmation qui nous servira plus tard. On peut trouver le reste de la démonstration dans [**52**] chap. IV prop. 3.1.

Soit χ un caractère de G. Si χ est non trivial, on a $s(\chi) \geq 2$ puisque S contient deux places totalement décomposées (et leur groupe de décomposition est trivial) ; sinon, on a $s(1_{\hat{G}}) \geq 3$ puisque S contient au moins trois places.

Dans tous les cas, la formule 2.1.17 donne $r(\chi) \geq 2$ d'où $L'_S(s,\chi) = 0$ et ainsi grâce à 2.1.15 et 2.1.18, on obtient $\log|\sigma(\varepsilon)|_w = 0$ pour tout $\sigma \in G$, d'où $\varepsilon = \pm 1$ puisque la place w est réelle. □

Comme une place complexe est totalement décomposée dans toute extension, pour obtenir de cette conjecture des résultats non triviaux, force est de supposer que les autres places infinies de k distinctes de v sont aussi réelles. On va donc se placer dans le cas où le corps de base k est totalement réel.

On suppose désormais la conjecture 2.1 vraie.

2.2. Applications aux corps totalement réels

Soit k un corps totalement réel (supposé différent de $\mathbb{Q}$). On note $N := [k : \mathbb{Q}]$ son degré ; $v_1, \ldots, v_N$ désignent les plongements de k dans $\mathbb{R}$ et, par extension, les places infinies de k.

Soit $\mathfrak{f}$ un idéal entier de k, on veut construire un élément primitif du corps de classes de rayon $L := k(\mathfrak{f})$. On suppose sans perte de généralité que $\mathfrak{f}$ est le conducteur de cette extension ; sinon, il est toujours possible de se ramener à ce cas en calculant ce conducteur par les méthodes de [**11**]. Le corps L est une extension abélienne totalement réelle de k. Par la proposition 2.2, on sait que les unités de Stark associées à cette extension sont triviales. On est donc amené à considérer une autre extension ; en fait, on va travailler dans une sur-extension de L/k.

Supposons qu'il existe une extension quadratique K de L vérifiant les conditions suivantes :

(a) K/k est une extension abélienne.
(b) La place infinie v_1 est totalement décomposée dans K/k, les autres places infinies se ramifiant dans cette extension.
(c) Tout idéal premier de L ramifié dans L/k (ou de manière équivalente divisant $\mathfrak{f}$) est ramifié ou inerte dans K/L.

On discutera en détail l'existence d'une telle extension à la fin de ce chapitre, dans la dernière section.

Les conditions (a) et (b) permettent d'appliquer à cette extension la conjecture 2.1 : on fixe w une place de K au-dessus de v_1 et on choisit pour S l'ensemble des places infinies de k et des places finies ramifiées dans K/k (S est choisi minimal) ; on note ε l'unité de Stark associée à l'extension K/k, à l'ensemble de places S et à la place w. La place w étant réelle, on assure l'unicité de ε en supposant de plus que $w(\varepsilon) > 0$. La condition (c) imposée ci-dessus est une condition technique qui permet de prouver le résultat suivant :

Théorème 2.3. *L'unité ε engendre K sur k et même sur $\mathbb{Q}$.*

On note τ l'élément non trivial de $\mathrm{Gal}(K/L)$ et $G := \mathrm{Gal}(K/k)$.

Démonstration : Pour v une place contenue dans S, on note $D_v := D_v(K/k)$ son groupe de décomposition dans K/k. On suppose pour commencer que v est finie : ou bien v divise $\mathfrak{f}$ et elle est ramifiée ou inerte dans K/L par la condition (c), ou bien v n'est pas ramifiée dans L/k et elle est ramifiée dans K/L (par le choix de S) ; dans tous les cas, on a $\tau \in D_v$. Maintenant, si v est infinie, ou bien $v \neq v_1$ et v est ramifiée dans K/L par la condition (b) d'où $\tau \in D_v$ (et même $D_v = \{1, \tau\}$), ou bien $v = v_1$ et $D_{v_1} = \{1\}$.

En combinant ces résultats avec la formule 2.1.17, on en déduit :

$$\chi(\tau) \neq 1 \Rightarrow L'(0,\chi) \neq 0. \tag{2.2.20}$$

Soit $\nu \in G$ tel que $\nu(\varepsilon) = \varepsilon$; pour tout $\chi \in \hat{G}$ on obtient par 2.1.19 :

$$\begin{aligned} L'(0,\chi) &= -\frac{1}{2}\sum_{\sigma\in G} \log|\sigma\nu(\varepsilon)|_w \chi(\sigma) \\ &= -\frac{1}{2}\sum_{\delta\in G} \log|\delta(\varepsilon)|_w \chi(\nu^{-1}\delta) \text{ en posant } \delta = \nu\sigma \\ &= -\frac{1}{2}\bar{\chi}(\nu)\sum_{\delta\in G} \log|\delta(\varepsilon)|_w \chi(\delta) \\ &= \bar{\chi}(\nu) L'(0,\chi). \end{aligned}$$

On ainsi a montré :

$$L'(0,\chi) \neq 0 \Rightarrow \chi(\nu) = 1. \tag{2.2.21}$$

En rassemblant les formules 2.2.20 et 2.2.21, on trouve finalement :

$$\nu(\varepsilon) = \varepsilon \Rightarrow \nu \in \bigcap_{\chi(\tau)\neq 1} \text{Ker } \chi$$

où l'intersection est prise sur tous les caractères de G qui sont non triviaux en τ. Pour finir de prouver la première assertion, on montre que ceci implique que $\nu = 1$.

On définit :

$$\hat{G}^+ := \{\chi \in \hat{G} \ / \ \chi(\tau) = 1\}$$
$$\hat{G}^- := \{\chi \in \hat{G} \ / \ \chi(\tau) = -1\},$$

il est facile de voir par la théorie des caractères d'un groupe fini que $\hat{G} = \hat{G}^+ \cup \hat{G}^-$ et que $|\hat{G}^+| = |\hat{G}^-| = \frac{1}{2}|G|$ (*cf* Chapitre 0). De plus, pour tout $\psi \in \hat{G}^-$, on a $\hat{G}^+ = \psi\hat{G}^-$. On fixe un tel ψ et on calcule :

$$\sum_{\chi\in\hat{G}} \chi(\nu) = \sum_{\chi\in\hat{G}^+} \chi(\nu) + \sum_{\chi\in\hat{G}^-} \chi(\nu) = (\psi(\nu)+1)\sum_{\chi\in\hat{G}^-} \chi(\nu) = 2|\hat{G}^-| = |G|,$$

d'où $\nu = 1$.

On démontre la seconde assertion. Soit $w'(\neq w)$ un plongement de K dans $\mathbb{C}$. Si w' divise v_1, on trouve $w'(\varepsilon) \neq w(\varepsilon)$ puisque $K = k(\varepsilon)$ et ceci implique que les images de ε par tous les plongements de K au-dessus d'un plongement fixé de k (en l'occurence ici v_1) sont distinctes. Si w' ne divise pas v_1, ce plongement est complexe. Or, k est totalement réel et $w'(\varepsilon)$ engendre $w'(K)$ corps complexe sur $v'(k)$ corps réel (avec v' l'unique place de k au-dessous de w') d'où $w'(\varepsilon) \in \mathbb{C} \setminus \mathbb{R}$ et ainsi $w'(\varepsilon) \neq w(\varepsilon)$. Donc tous les conjugués de ε sur $\mathbb{Q}$ sont distincts, ce qui prouve que $K = \mathbb{Q}(\varepsilon)$. □

Le principal intérêt de ce résultat est qu'il se transmet au corps L.

Corollaire 2.4. *On pose $\alpha = \varepsilon + \varepsilon^{-1} \in K$.*
Alors, on a $\alpha \in L$ et même $L = \mathbb{Q}(\alpha)$.

Démonstration : On pose $t := N_{K/L}(\varepsilon) = \varepsilon\tau(\varepsilon)$ où $N_{K/L}$ est la norme de K sur L. Soit $\tilde{w}$ la restriction de la place w à L, on obtient par (2.6) :

$$\log|\sigma(t)|_{\tilde{w}} = \log|\sigma(\varepsilon)|_w + \log|\sigma\tau(\varepsilon)|_w = -2(\zeta'_S(0,\sigma) + \zeta'_S(0,\sigma\tau))$$

pour tout $\sigma \in G$.

On définit la fonction méromorphe $Z(s,\sigma) := \zeta_S(s,\sigma) + \zeta_S(s,\sigma\tau)$ pour $s \in \mathbb{C}$ et $\sigma \in G$. Notons que $Z(s,\sigma) = Z(s,\sigma\tau)$ pour tout $\sigma \in G$ et donc on peut définir $Z(s,.)$ sur le groupe quotient $G/ < \tau > \cong \text{Gal}(L/k)$.

Pour $s \in \mathbb{C}$ avec $\Re(s) > 1$, on a par 2.1.14 :

$$Z(s,\sigma) = \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \mathcal{N}\mathfrak{a}^{-s} + \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_{\mathfrak{a}}=\sigma\tau}} \mathcal{N}\mathfrak{a}^{-s} = \sum_{\substack{(\mathfrak{a},S)=1 \\ \tilde{\sigma}_{\mathfrak{a}}=\tilde{\sigma}}} \mathcal{N}\mathfrak{a}^{-s}$$

où $\tilde{\sigma}_{\mathfrak{a}}$ (respectivement $\tilde{\sigma}$) désigne la restriction de $\sigma_{\mathfrak{a}}$ (respectivement de σ) à L. Ainsi, pour $\Re(s) > 1$, la fonction $Z(s, \sigma)$ est la fonction zêta partielle $\tilde{\zeta}_S$ associée à l'extension L/k, à l'ensemble de places S et à l'automorphisme $\tilde{\sigma} \in \mathrm{Gal}(L/k)$. Par unicité du prolongement analytique, on en déduit :

$$\log |\sigma(t)|_{\tilde{w}} = -2\tilde{\zeta}'_S(0, \tilde{\sigma})$$

pour tout $\sigma \in G$.

L'élément t est donc l'unité de Stark associée à l'extension L/k, à l'ensemble de places S et à la place $\tilde{w}^*$. On admet pour l'instant le lemme suivant :

Lemme 2.5. *Si $N = 2$, alors au moins un idéal premier de k se ramifie dans K.*

Ainsi, dans tous les cas (y compris le cas $N = 2$ et $\mathfrak{f} = \mathcal{O}_k$ par le lemme) on trouve que le cardinal de S est ≥ 3 et donc $t = 1$ par la proposition 2.2. On a ainsi montré que l'élément $\alpha = \varepsilon + \tau(\varepsilon)$ est la trace de ε sur L ; en particulier, c'est bien un élément de L.

Maintenant, K est une extension quadratique de $\mathbb{Q}(t, \alpha)$ puisque :

$$\varepsilon^2 - \alpha\varepsilon + t = 0,$$

et $\mathbb{Q}(\alpha, t) = \mathbb{Q}(\alpha)$ car $t \in \mathbb{Q}$. De plus, $\alpha \in L$ et $[K : L] = 2$, d'où on obtient finalement $K = \mathbb{Q}(\alpha)$. □

On conclut cette section en prouvant le lemme 2.5.

Démonstration : On suppose qu'aucun idéal premier de k ne se ramifie dans K, alors le conducteur de K/k est juste $\mathfrak{m} = v_2$. Mais ceci est impossible car alors (avec les résultats et les notations de [**34**] chap. VI) $(\mathcal{O}_k/\mathfrak{m})^\times \cong \{\pm 1\}$ et cette partie est tuée par l'image de -1. Donc le groupe de classes de rayon modulo $\mathfrak{m}$ est égal au groupe de classes et $\mathfrak{m}$ ne peut être conducteur. □

2.3. Méthode de calcul explicite

Dans cette section, notre but est de montrer comment calculer algorithmiquement l'élément α du corollaire 2.4. Il est à noter que des calculs similaires destinés à vérifier numériquement les conjectures de Stark dans le cas de corps cubiques réels de nombre de classes 3 ont été effectués dans [**17**], ainsi que des calculs destinés à la conjecture de Stark $\mathfrak{p}$-adique dans [**16**] (*cf* [**27**] pour plus de détails sur cette conjecture).

La première étape consiste en la construction d'une extension K de L vérifiant les conditions (a-c). Comme des résultats numériques et heuristiques montrent que la "taille" (en tant que nombre complexe) de l'unité ε croît exponentiellement avec la racine carrée de la norme du conducteur de K, on va chercher une extension K vérifiant ces conditions et de conducteur minimal (pour la norme).

Pour cela, on énumère par taille croissante les modules candidats : à savoir les modules composés d'un idéal divisible par $\mathfrak{f}$ et de toutes les places infinies sauf une. Dès que l'un de ces modules, disons $\mathfrak{m}$, est un conducteur, on cherche les sous-corps de $k(\mathfrak{m})$ qui sont des extensions quadratiques de L et de conducteur $\mathfrak{m}$. Toute cette partie qui consiste essentiellement en des calculs sur les groupes de classes de rayon associés à $\mathfrak{f}$ et à $\mathfrak{m}$, peut être effectuée à l'aide des outils décrits dans [**11**].

Une fois un tel corps trouvé, on note $\mathcal{H}$ le groupe de congruence de K modulo $\mathfrak{m}$, *ie* le sous-groupe de $\mathrm{Cl}_k(\mathfrak{m})$ induit par le groupe des normes de K/k. Il faut à présent s'assurer qu'il vérifie bien la condition (c), les deux conditions (a) et (b) étant vérifiées par construction. Pour cela, on a besoin de connaître la décomposition des idéaux premiers divisant $\mathfrak{f}$ dans K/k.

Lemme 2.6. *Soit $\mathfrak{p}$ un idéal premier de k, on note $\mathfrak{m}_\mathfrak{p}$ la partie première à $\mathfrak{p}$ de $\mathfrak{m}$, ie $\mathfrak{m}_\mathfrak{p} := \mathfrak{m}\mathfrak{p}^{-\mathrm{val}_\mathfrak{p}(\mathfrak{m})}$, puis $\mathcal{H}_\mathfrak{p} := s_{\mathfrak{m},\mathfrak{m}_\mathfrak{p}}(\mathcal{H})$.*

Alors, l'indice de ramification de $\mathfrak{p}$ dans K/k est égal au quotient $\frac{(\mathrm{Cl}_k(\mathfrak{m}):\mathcal{H})}{(\mathrm{Cl}_k(\mathfrak{m}_\mathfrak{p}):\mathcal{H}_\mathfrak{p})}$ et le degré résiduel de $\mathfrak{p}$ est égal à l'ordre de la classe de $\mathfrak{p}$ dans $\mathrm{Cl}_k(\mathfrak{m}_\mathfrak{p})/\mathcal{H}_\mathfrak{p}$.

---

* En règle générale, on peut vérifier que les unités de Stark redescendent par la norme aux sous-extensions.

Démonstration : Il est facile de voir que le corps d'inertie de $k(\mathfrak{m})$ est le corps de classes de rayon $k(\mathfrak{m}_\mathfrak{p})$. Maintenant, par la théorie de Galois, le corps d'inertie de K correspond au groupe de congruence $s_{\mathfrak{m},\mathfrak{m}_\mathfrak{p}}(\mathcal{H})$ ce qui prouve la première assertion.

Pour la deuxième assertion, on vérifie que le degré d'inertie de l'idéal premier $\mathfrak{p}$ dans l'extension K/k est celui de $\mathfrak{p}$ dans l'extension K_i/k où K_i est le corps d'inertie de $\mathfrak{p}$; or, ce degré est égal à l'ordre de la classe de $\mathfrak{p}$ dans $\mathrm{Cl}_k(\mathfrak{m}_\mathfrak{p})/\mathcal{H}_\mathfrak{p}$ par la théorie du corps de classes. □

Ainsi, pour un sous-groupe de congruence $\mathcal{H}$ donné, il est possible, toujours grâce aux méthodes expliquées dans [**11**], de tester si le corps correspondant K vérifie bien la condition (c) en calculant explicitement l'indice de ramification et le degré résiduel des idéaux premiers ramifiées dans L/k.

On suppose connu à présent une extension K/k vérifiant les conditions (a-c), *ie* on connaît son conducteur $\mathfrak{m}$ et son groupe de congruence $\mathcal{H}$ dans $\mathrm{Cl}_k(\mathfrak{m})$. On reprend les notations précédentes ; on pose $G := \mathrm{Gal}(K/k)$ le groupe de Galois de cette extension (on a $G \cong \mathrm{Cl}_k(\mathfrak{m})/\mathcal{H}$) et S est l'ensemble des places infinies de k et des places finies ramifiées dans K/k, *ie* divisant $\mathfrak{m}_0$. La place v_1 est définie comme la seule place infinie qui reste réelle dans l'extension K/k.

Pour calculer des valeurs approchées des conjugués de ε, l'unité de Stark associée à cette extension, on doit calculer des valeurs approchées des fonctions zêta partielles définies par 2.1.14. Cependant, il est plus pratique de calculer ces valeurs en utilisant les fonctions L et la formule 2.1.15 car les fonctions L admettent une équation fonctionnelle. Ainsi, soit χ un caractère de G, on commence par calculer une valeur approchée suffisamment précise de $L'_S(0,\chi)$.

Un cas est particulièrement simple. Supposons que $\chi(\tau) = 1$ (où τ est toujours l'élément non trivial de $\mathrm{Gal}(K/L)$). Alors, le corps fixe de χ, disons K_χ (*ie* le sous-corps de K/k correspondant par la théorie de Galois au noyau de χ) est inclus dans L ; en particulier, toutes les places infinies de k sont totalement décomposées dans K_χ/k et par la formule 2.1.17 on obtient $r(\chi) \geq 2$ et donc $L'_S(0,\chi) = 0$.

On suppose désormais que $\chi(\tau) \neq 1$, ce qui équivaut à $\chi(\tau) = -1$. On note $\mathfrak{m}(\chi)$ le conducteur de χ et toujours K_χ le corps fixe de χ. Le corps K_χ n'est pas inclus dans L mais est aussi différent de k (puisque le caractère χ n'est pas trivial). Ainsi, $LK_\chi = K$ et donc $\mathfrak{m}$ divise le PPCM des modules $\mathfrak{f}$ et $\mathfrak{m}(\chi)$. On en conclut que $\mathfrak{m}(\chi)_\infty = \mathfrak{m}_\infty$ puisque la partie infinie de $\mathfrak{f}$ est triviale.

Cependant, si on a égalité entre les deux parties infinies, la partie finie du conducteur de χ peut être un diviseur strict de $\mathfrak{m}_0$ et donc le caractère χ non primitif. On note $G_\chi := \mathrm{Gal}(K_\chi/k)$; le caractère χ est induit par un caractère $\tilde{\chi}$ de G_χ :

$$\chi \ : \ G \twoheadrightarrow G_\chi \xrightarrow{\tilde{\chi}} \mathbb{C}^\times. \tag{2.3.22}$$

Le caractère $\tilde{\chi}$ est alors primitif. Cette remarque permet d'étendre le caractère χ aux idéaux premiers $\mathfrak{p}$ divisant $\mathfrak{m}$ mais non $\mathfrak{m}(\chi)$ en posant :

$$\chi(\mathfrak{p}) := \tilde{\chi}(\mathfrak{p}).$$

On considère ainsi dans la suite que le caractère χ est défini sur $I_k(\mathfrak{m}(\chi))$. On associe au caractère χ une nouvelle fonction L définie pour $s \in \mathbb{C}$ avec $\Re(s) \geq 1$ par le produit eulérien[†] :

$$L(s,\chi) := \prod_{\mathfrak{p} \nmid \mathfrak{m}(\chi)_0} (1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1} \tag{2.3.23}$$

où $\mathfrak{p}$ parcourt les idéaux premiers de k ne divisant pas $\mathfrak{m}(\chi)_0$. Les fonctions $L_S(s,\chi)$ et $L(s,\chi)$ coïncident si et seulement si $\mathfrak{m}(\chi)_0$ et $\mathfrak{m}_0$ ont exactement les mêmes facteurs premiers, en particulier quand le caractère χ est primitif. On définit à présent une fonction L élargie :

$$\Lambda(s,\chi) := C(\chi)^s \Gamma(s/2)\Gamma\left(\frac{s+1}{2}\right)^{N-1} L(s,\chi) \tag{2.3.24}$$

avec :

$$C(\chi) := \sqrt{\frac{d_k \mathcal{N}\mathfrak{m}(\chi)_0}{\pi^N}}$$

[†] Le caractère χ étant ici non trivial, ce produit eulérien converge également en $\Re(s) = 1$.

où Γ désigne la fonction Gamma classique. L'intérêt de cette définition est l'équation fonctionnelle suivante (vérifiée du fait que le caractère χ est considéré primitif dans 2.3.23) :

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\bar{\chi}) \tag{2.3.25}$$

pour tout $s \in \mathbb{C}$, où $W(\chi)$ est un nombre complexe de module 1 appelé constante d'Artin. On peut trouver une démonstration de ce résultat ainsi qu'une définition complète des objets qui y apparaissent (notamment la constante d'Artin) dans le cadre plus général des caractères virtuels dans [**39**] (qui constitue d'ailleurs une excellente introduction à toute cette théorie). L'existence de cette équation fonctionnelle va nous permettre de calculer avec une grande précision des valeurs approchées de $\Lambda(1,\chi)$ et d'en déduire des valeurs approchées de $L'(0,\chi)$ puisque, en exprimant $L(s,\chi)$ en fonction de $\Lambda(1-s,\chi)$ en utilisant 2.3.25 et 2.3.24, puis en faisant tendre s vers 0, on obtient :

Lemme 2.7.

$$L'(0,\chi) = \frac{\Lambda(1,\bar{\chi})}{2\sqrt{\pi^{N-1}}W(\chi)}.$$

Si on pose maintenant :

$$A(\chi) := \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \mathfrak{p}\nmid\mathfrak{m}(\chi)}} (1-\chi(\mathfrak{p})),$$

on trouve :

$$L'_S(0,\chi) = A(\chi)L'(0,\chi).$$

Il faut remarquer que le produit $A(\chi)$ n'est jamais nul (dans le cas où $\chi(\tau) = -1$). En effet, ce produit est nul si et seulement si il existe un idéal premier $\mathfrak{p}$ de k divisant $\mathfrak{m}$, mais non $\mathfrak{m}(\chi)$ tel que $\chi(\mathfrak{p}) = 1$. Notons $\mathfrak{P}$ un idéal de K au-dessus de $\mathfrak{p}$ fixé et $\mathfrak{P}_\chi$ l'unique idéal premier de K_χ au-dessous de $\mathfrak{P}$. Par l'hypothèse (c), on a $\tau(\mathfrak{P}) = \mathfrak{P}$ et donc $\tau|_{K_\chi}(\mathfrak{P}_\chi) = \mathfrak{P}_\chi$. D'où $\tau|_{K_\chi} \in D_\mathfrak{p}(K_\chi/k)$ et c'est donc une puissance, disons e, du Frobenius de $\mathfrak{p}$ dans K_χ/k. Il s'ensuit par 2.3.22 :

$$\chi(\tau) = \tilde{\chi}(\tau|_{K_\chi}) = \chi(\mathfrak{p})^e = 1,$$

ce qui est une contradiction avec l'hypothèse $\chi(\tau) = -1$.

On sait calculer aisément $C(\chi)$ et $A(\chi)$; ainsi, pour obtenir une valeur approchée de $\zeta'_S(0,\chi)$, il suffit désormais de calculer $W(\chi)$ et $\Lambda(1,\chi)$.

Le calcul de la valeur de la fonction Λ au point $s = 1$ se fait en utilisant l'expression suivante dûe à Friedmann (*cf* [**23**]).

Théorème 2.8 (Friedmann)**.** *Pour $\Re(s) > 1$, écrivons la fonction $L(s,\chi)$ sous forme de série de Dirichlet :*

$$L(s,\chi) = \sum_{n\geq 1} a_n(\chi)n^{-s}.$$

On obtient alors :

$$\Lambda(1,\chi) = \sum_{n\geq 1}\Big[a_n(\chi)f(C(\chi)/n,1) + W(\chi)\overline{a_n(\chi)}f(C(\chi)/n,0)\Big]$$

où :

$$f(x,s) = \frac{1}{2i\pi}\int_{\delta-i\infty}^{\delta+i\infty} x^z \frac{\Gamma(z/2)\Gamma(\frac{z+1}{2})^{N-1}}{z-s}dz$$

pour tout réel $\delta > \mathrm{Max}\{\Re(s),0\}$.

Pour en déduire une méthode de calcul, on utilise la procédure développée dans [**53**] et [**54**].

Soit h un entier positif ; on écrit pour z autour de $-h$:

$$\Gamma(z/2)\Gamma\left(\frac{z+1}{2}\right)^{N-1} = \sum_{j=0}^{N-1}\frac{A_{h,j}}{(z+h)^j} + g_h(z)$$

où g_h est une fonction holomorphe en $z = -h$. On calcule ces valeurs pour un entier h donné en utilisant les formules classiques sur la fonction Gamma, voir par exemple [**1**].

Puis, par application directe de la proposition 2.4 de [**53**], on a :

Proposition 2.9. *Soient $N_0, h_0 > 0$ deux entiers ; notons :*

$$g_{n,h}(\chi) := \sum_{k=0}^{N-1} \sum_{j=1}^{N-k} A_{h,j+k} \frac{\ln(C(\chi)/n)^{j-1}}{(j-1)!},$$
$$g'_n(\chi) := \sum_{j=1}^{N+1} A_{0,j-1} \frac{\ln(C(\chi)/n)^{j-1}}{(j-1)!},$$

puis :

$$S(\chi) := \sum_{n=1}^{N_0} a_n(\chi) \left(\frac{C(\chi)\sqrt{\pi}}{n} - \sum_{h=0}^{h_0} \left(\frac{n}{C(\chi)} \right)^h g_{n,h} \right),$$
$$T(\chi) := \sum_{n=1}^{N_0} \overline{a_n(\chi)} \left(g'_n(\chi) - \sum_{h=0}^{h_0} \left(\frac{n}{C(\chi)} \right)^h g_{n,h} \right).$$

Alors, a :

$$\Lambda(1, \chi) = S(\chi) + W(\chi) T(\chi) + \epsilon$$

où l'erreur commise ϵ ne dépend que de N_0 et h_0.

Le choix de N_0 et h_0 doit être fait judicieusement pour contrôler efficacement l'erreur. En particulier, ces deux valeurs sont intimement liées ; les valeurs appropriées peuvent être déterminées grâce aux résultats de [**53**] sections 2.3.2 et 2.3.4.

Pour le calcul des coefficients $a_n(\chi)$ dans l'expression en série de Dirichlet de la fonction $L(s, \chi)$, on procède ainsi : on commence par numéroter les idéaux premiers de k en une suite croissante $(\mathfrak{p}_l)_{l \geq 0}$ telle que $\mathfrak{p}_0 = \mathcal{O}_k$ et $\mathcal{N}\mathfrak{p}_{l+1} \geq \mathcal{N}\mathfrak{p}_l$; puis on définit :

$$I_k(n, h) := \{ \mathfrak{a} \in I_k(\mathfrak{m}(\chi)) \text{ tel que } \mathfrak{p}_l \mid \mathfrak{a} \Rightarrow l \leq h \text{ et } \mathcal{N}\mathfrak{a} = n \}.$$

$I_k(n, h)$ est l'ensemble des idéaux entiers de k, premiers avec la partie finie du conducteur de χ, de norme n, et divisibles uniquement par des idéaux premiers dont l'indice dans la numérotation choisie ci-dessus est plus petit que h. On note $a_{n,h}(\chi) := \sum_{\mathfrak{a} \in I_k(n,h)} \chi(\mathfrak{a})$. Par définition, il est clair que :

$$a_n(\chi) = \lim_{h \to \infty} a_{n,h}(\chi).$$

Mais, en fait, on a même $a_n(\chi) = a_{n,h}(\chi)$ dès que $h > h_n$, où h_n est le plus petit entier tel que $h > h_n \Rightarrow \mathcal{N}\mathfrak{p}_h > n$, puisqu'un idéal de norme n ne peut être divisible que par des idéaux premiers de norme $\leq n$.

On déduit de ces remarques la méthode de calcul suivante :

Lemme 2.10. *On a $a_{1,0}(\chi) = 1$ et $a_{n,0}(\chi) = 0$ pour $n \geq 2$; puis :*

$$a_{n,h}(\chi) = \sum_{k=0}^{v_{n,h}} a_{n/q_h{}^k, h-1}(\chi) \chi(\mathfrak{p}_h)^k,$$

où $q_h := \mathcal{N}\mathfrak{p}_h$, $a_{x,h}(\chi) := 0$ pour $x \in \mathbb{Q} \setminus \mathbb{N}$, et $v_{n,h} := \mathrm{Sup}\{v \geq 0 \text{ tel que } q_h^v | n\}$.

Démonstration : Ce résultat est une conséquence directe de la formule :

$$\sum_{n \geq 1} a_n(\chi) n^{-s} = \prod_{h > 1} \left(1 - \chi(\mathfrak{p}_h) / \mathcal{N}\mathfrak{p}_h^{-s} \right)^{-1},$$

cf [**53**] section 2.2.1 pour les détails. □

Le calcul de la constante d'Artin $W(\chi)$ est plus délicat. On verra dans le chapitre suivant que cette question se résoud plus facilement dans le cas où $\mathfrak{f} = \mathcal{O}_k$, *ie* quand L est le corps de classes de Hilbert de k. Néanmoins, dans le cas général, on est obligé de revenir à la définition. Suivant [**39**], on commence par écrire :

$$W(\chi) = W_\infty(\chi)\frac{\prod_{\mathfrak{p}} \tau_{\mathfrak{p}}(\bar{\chi})}{\sqrt{\mathcal{N}\mathfrak{m}(\chi)}},$$

où $\mathfrak{p}$ parcourt les idéaux premiers de k, $W_\infty(\chi)$ correspond à la partie infinie de χ, et $\tau_{\mathfrak{p}}(\chi)$ est une somme de Gauss locale qui vaut 1 pour presque tout $\mathfrak{p}$ (en fait pour tout $\mathfrak{p}$ qui ne divise pas $\mathcal{D}_k\mathfrak{m}(\chi)_0$), ce qui montre que cette définition est consistante. Dans notre cas, il est facile de voir que :

$$W_\infty(\chi) = i^{1-N}.$$

Reste le calcul de $\tau_{\mathfrak{p}}(\chi)$ pour un idéal premier $\mathfrak{p}$ de k. On définit le caractère additif $\lambda_{\mathfrak{p}}$ de $k_{\mathfrak{p}}$ dans $\mathbb{C}^\times$ de la manière suivante :

$$\lambda_{\mathfrak{p}} \ : \ k_{\mathfrak{p}} \overset{\text{Trace}}{\longrightarrow} \mathbb{Q}_p \twoheadrightarrow \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \overset{z\mapsto e^{2i\pi z}}{\longrightarrow} \mathbb{C}^\times$$

où chacune des applications est évidente. En fait, on peut reformuler ainsi cette construction : soit $x \in k_{\mathfrak{p}}$; on note $T(x)$ sa trace dans $\mathbb{Q}_p$; alors il existe un nombre rationnel r unique modulo 1 tel que $T(x) - r \in \mathbb{Z}_p$, et on pose $\lambda_{\mathfrak{p}}(x) = e^{2i\pi r}$. On peut vérifier que la codifférente $\mathcal{D}_{k_{\mathfrak{p}}}^{-1}$ de $k_{\mathfrak{p}}$ est le plus grand idéal sur lequel $\lambda_{\mathfrak{p}}$ est trivial.

Maintenant, la théorie locale du corps de classes permet de définir une application de $k_{\mathfrak{p}}^\times$ dans $\mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$, où $\mathfrak{P}$ est un idéal premier de K divisant $\mathfrak{p}$, et ce dernier groupe de Galois s'identifie canoniquement à $D_{\mathfrak{p}}$ (groupe de décomposition de $\mathfrak{p}$ dans K/k) (*cf* [**43**] chap. III). En composant cette application avec le caractère χ, on obtient le caractère local $\chi_{\mathfrak{p}}$:

$$\chi_{\mathfrak{p}} \ : \ k_{\mathfrak{p}}^\times \longrightarrow \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \overset{\sim}{\longrightarrow} D_{\mathfrak{p}} \overset{\chi}{\longrightarrow} \mathbb{C}^\times.$$

Le noyau de ce caractère local $\chi_{\mathfrak{p}}$ est de la forme $\mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})} := 1 + \mathfrak{p}^{n_{\mathfrak{p}}}\mathcal{O}_{k_{\mathfrak{p}}}$ où $n_{\mathfrak{p}}$ est la valuation en $\mathfrak{p}$ de $\mathfrak{m}(\chi)$. Si $n_{\mathfrak{p}} \geq 1$, on dit que le caractère χ (ou $\chi_{\mathfrak{p}}$) est ramifié en $\mathfrak{p}$.

Notons R un système de représentants du quotient $\mathcal{U}_{\mathfrak{p}}/\mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ où $\mathcal{U}_{\mathfrak{p}}$ est le groupe des unités locales, et fixons un entier $\mathfrak{p}$-adique c tel que $\mathrm{val}_{\mathfrak{p}}(c) = \mathrm{val}_{\mathfrak{p}}(\mathcal{D}_{\mathfrak{p}}\mathfrak{m}(\chi))$. La somme de Gauss $\tau_{\mathfrak{p}}$ est définie par :

$$\tau_{\mathfrak{p}}(\chi) := \sum_{x\in R} \lambda_{\mathfrak{p}}(xc^{-1})\chi_{\mathfrak{p}}(xc^{-1}).$$

On montre que cette somme ne dépend ni du choix de c, ni du choix de R et que :

$$|\tau_{\mathfrak{p}}(\chi)| = \sqrt{\mathcal{N}\mathfrak{p}^{n_{\mathfrak{p}}}}.$$

Le calcul de cette somme est facile dans le cas où χ n'est pas ramifié en $\mathfrak{p}$. En effet, d'une part, on peut prendre $R = \{1\}$ et la somme se résume à un seul terme :

$$\tau_{\mathfrak{p}}(\chi) = \lambda_{\mathfrak{p}}(c^{-1})\chi_{\mathfrak{p}}(c^{-1}) = \bar{\chi}_{\mathfrak{p}}(c),$$

puisque la trace de c^{-1} sur $\mathbb{Q}_p$ est entière car c appartient à la différente locale. D'autre part, le caractère χ n'étant pas ramifié en $\mathfrak{p}$, on sait calculer explicitement la valeur de $\chi_{\mathfrak{p}}(c)$, puisque dans ce cas l'application d'Artin locale envoie une uniformisante sur le Frobenius, d'où :

Lemme 2.11. *Si le caractère $\chi_{\mathfrak{p}}$ n'est pas ramifié, alors on a :*

$$\tau_{\mathfrak{p}}(\chi) = \bar{\chi}(\mathfrak{p}^e),$$

où e dénote la valuation en $\mathfrak{p}$ de la différente $\mathcal{D}_k$ de k. En particulier, cette somme de Gauss vaut 1 si le caractère n'est pas ramifié en $\mathfrak{p}$ et si $\mathfrak{p}$ ne divise pas $\mathcal{D}_k$.

La calcul de la somme de Gauss $\tau_{\mathfrak{p}}(\chi)$ est moins facile dans le cas où χ est ramifié en $\mathfrak{p}$. Il faut, dans ce cas, résoudre trois problèmes :

- calculer un système de représentants R de $\mathcal{U}_{\mathfrak{p}}/\mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ dans $\mathcal{O}_k$,
- pour $x \in R$, calculer $\lambda_{\mathfrak{p}}(xc^{-1})$,
- pour $x \in R$, calculer $\chi_{\mathfrak{p}}(xc^{-1}) = \bar{\chi}_{\mathfrak{p}}(c)\chi_{\mathfrak{p}}(x)$.

Pour tout entier $n \geq 1$, on a l'isomorphisme canonique :

$$(\mathcal{O}_k/\mathfrak{p}^n)^\times \cong \mathcal{U}_\mathfrak{p}/\mathcal{U}_\mathfrak{p}^{(n)}$$

et il est facile de calculer un système de représentants du quotient de gauche en utilisant les méthodes de [**9**] ou de [**11**] ; le premier point est ainsi résolu.

Pour le deuxième point, soit s un entier positif tel que $p^s x c^{-1}$ soit un $\mathfrak{p}$-entier ; par exemple, $s = \left\lceil \frac{\mathrm{val}_\mathfrak{p}(c)}{e_\mathfrak{p}(k/\mathbb{Q})} \right\rceil$ convient (puisque x n'est pas divisible par $\mathfrak{p}$) où $\lceil a \rceil$ désigne le plus petit entier plus grand que $a \in \mathbb{R}$. La trace locale de $p^s x c^{-1}$ est alors un entier p-adique, et si r est une approximation entière de cette trace à p^s près, on a :

$$\lambda_\mathfrak{p}(xc^{-1}) = e^{2i\pi r/p^s}.$$

On ne connaît pas de méthode particulièrement efficace pour calculer en toute généralité la trace locale de $y := p^s x c^{-1}$. La méthode utilisée ici est plutôt naïve : on commence par calculer le polynôme minimal de y sur $\mathbb{Q}$, disons $M(X)$. Puis, par une des deux méthodes expliquées dans le chapitre 1, on factorise ce polynôme dans $\mathbb{Q}_p[X]$ avec une précision de p^s. On obtient :

$$M(X) \equiv \prod_{i=1}^{g} M_i(X) \pmod{p^s},$$

où les $M_i(X)$ sont des approximations à coefficients entiers des facteurs irréductibles de $M(X)$ dans $\mathbb{Q}_p[X]$.

A chaque facteur $M_i(X)$ correspond un unique idéal premier de $\mathbb{Q}(y)$ au-dessus de p ; en particulier, il existe un unique facteur $M_i(X)$ tel que $M_i(y) \in \mathfrak{p}$. C'est celui correspondant à $\mathfrak{p}'$, l'unique idéal premier de $\mathbb{Q}(y)$ au-dessous de $\mathfrak{p}$. La trace de $y \in \mathbb{Q}(y)_{\mathfrak{p}'}$ sur $\mathbb{Q}_p$ est ainsi (à p^s près) la trace du polynôme $M_i(X)$.

Maintenant, la trace de $y \in k_\mathfrak{p}$ sur $\mathbb{Q}_p$ est le produit de la trace de y dans l'extension $\mathbb{Q}(y)_{\mathfrak{p}'}/\mathbb{Q}_p$ par le degré de l'extension relative locale $k_\mathfrak{p}/\mathbb{Q}(y)_{\mathfrak{p}'}$. Le degré absolu de $k_\mathfrak{p}$ est $m_\mathfrak{p} := e_\mathfrak{p} f_\mathfrak{p}$, et le degré de $[\mathbb{Q}(y)_{\mathfrak{p}'} : \mathbb{Q}]$ est celui de $M_i(X)$, disons m_i. Finalement, on obtient :

$$T_{k_\mathfrak{p}/\mathbb{Q}_p}(y) \equiv \frac{m_\mathfrak{p}}{m_i} \,\mathrm{Trace}\,(M_i(X)) \pmod{p^s}.$$

Soit un idéal premier $\mathfrak{p}$ en lequel χ est ramifié et soit $x \in \mathcal{O}_k$. Le dernier point consiste à calculer $\chi_\mathfrak{p}(x)$ où x est considéré comme un élément du corps local $k_\mathfrak{p}$. Pour cela, on a besoin de mieux connaître le lien entre théorie locale et globale du corps de classes, lien qui passe par la théorie des idèles. On note $\mathcal{I}_k$ le groupe des idèles de k et $\mathcal{P}_k$ le sous-groupe des idèles principaux. Un élément $\iota \in \mathcal{I}_k$ est un produit formel :

$$\iota = \prod_v (\iota_v)_v$$

où v parcourt les places finies et infinies de k. On a un plongement naturel de $k_\mathfrak{p}^\times$ dans $\mathcal{I}_k$ donné en associant à l'élément local a l'idèle :

$$\iota_\mathfrak{p}(a) := (a)_\mathfrak{p} \prod_{v \neq \mathfrak{p}} (1)_v.$$

Pour un module $\mathfrak{m}$, on dit qu'un idèle ι est congru multiplicativement à 1 modulo $\mathfrak{m}$ si :

$$\begin{aligned} &\text{pour tout } \mathfrak{p} \mid \mathfrak{m}_0, \qquad \mathrm{val}_\mathfrak{p}(1-\iota_\mathfrak{p}) \geq \mathrm{val}_\mathfrak{p}(\mathfrak{m}_0), \\ \text{et} \quad &\text{pour tout } v \in \mathfrak{m}_\infty, \qquad \iota_v > 0 \end{aligned}$$

On note $\mathcal{I}_k(\mathfrak{m})$ le groupe des idèles congru multiplicativement à 1 modulo $\mathfrak{m}$. Le groupe des classes d'idèles est le quotient $C_k := \mathcal{I}_k/\mathcal{P}_k$, et le groupe des classes d'idèles de rayon modulo $\mathfrak{m}$ est le quotient $C_k(\mathfrak{m}) := C_k/C_k^\mathfrak{m}$ où $C_k^\mathfrak{m} := \mathcal{I}_k(\mathfrak{m})\mathcal{P}_k/\mathcal{P}_k$ est le groupe de congruence modulo $\mathfrak{m}$ de C_k.

Nanti de ces définitions, on peut réécrire la définition de $\chi_\mathfrak{p}$ comme la composée des applications :

$$\chi_\mathfrak{p} \ : \ k_\mathfrak{p}^\times \hookrightarrow \mathcal{I}_k \twoheadrightarrow C_k \twoheadrightarrow C_k(\mathfrak{m}) \xrightarrow{\kappa_\mathfrak{m}}_{\sim} \mathrm{Cl}_k(\mathfrak{m}) \twoheadrightarrow \mathrm{Cl}_k(\mathfrak{m})/\mathcal{H} \xrightarrow{\sim} G \xrightarrow{\chi} \mathbb{C}^\times.$$

La seule application qui n'est pas déjà connue ici est l'application $\kappa_\mathfrak{m}$. On peut en trouver une construction et une démonstration qu'elle définit bien un isomorphisme entre $C_k(\mathfrak{m})$ et $\mathrm{Cl}_k(\mathfrak{m})$ dans [**43**] chap. IV prop. 8.1.

En fait, on va se servir de cette construction pour déterminer un idéal $\mathfrak{a}$ de $I_k(\mathfrak{m})$ tel que :

$$\chi_{\mathfrak{p}}(x) = \chi(\mathfrak{a}). \tag{2.3.26}$$

En vertu du théorème d'approximation forte, il existe un élément $a \in k^\times$ tel que l'idèle $\iota_{\mathfrak{p}}(x)(a)_v \in \mathcal{I}_k(\mathfrak{m})$. En fait, a doit simplement vérifier :

$$\begin{aligned} \mathrm{val}_{\mathfrak{p}}(1-xa) &\geq \mathrm{val}_{\mathfrak{p}}(\mathfrak{m}), \\ \text{pour tout } \mathfrak{q} \mid \mathfrak{m}_0 \text{ et } \mathfrak{q} \neq \mathfrak{p},\ \mathrm{val}_{\mathfrak{q}}(1-a) &\geq \mathrm{val}_{\mathfrak{q}}(\mathfrak{m}), \\ \text{pour tout } v \in \mathfrak{m}_\infty,\ v(a) &> 0. \end{aligned}$$

Une fois connu un tel élément a, on définit l'idéal $\mathfrak{a}$ par :

$$\mathfrak{a} := \prod_{\substack{\mathfrak{q} \mid (a) \\ \mathfrak{q} \nmid \mathfrak{m}_0}} \mathfrak{q}^{-\mathrm{val}_{\mathfrak{q}}(a)},$$

où $\mathfrak{q}$ parcourt les idéaux premiers de k qui divisent a mais pas $\mathfrak{m}_0$. La proposition citée affirme que $\kappa_{\mathfrak{m}}$ envoie la classe de $\iota_{\mathfrak{p}}(x)$ dans $C_k(\mathfrak{m})$ sur la classe de $\mathfrak{a}$ dans $\mathrm{Cl}_k(\mathfrak{m})$. Ce qui démontre l'assertion 2.3.26.

On sait à présent comment calculer tous les termes de la somme de Gauss $\tau_{\mathfrak{p}}(\chi)$. Il est à remarquer que dans le cas où la norme du conducteur est importante, il s'agit d'une tâche complexe (au sens algorithmique). Cependant, il est bien sûr possible de simplifier ce calcul ; par exemple, on ne calcule les valeurs du caractère $\chi_{\mathfrak{p}}$ que pour un relèvement d'un système de générateurs de $(\mathcal{O}_k/\mathfrak{p}^{n_{\mathfrak{p}}})^\times$ et pour c, les autres valeurs s'en déduisant par multiplicativité.

En réunissant les différentes formules et méthodes données ci-dessus, il est possible de calculer avec une bonne précision les valeurs $C(\chi)$, $A(\chi)$, $\Lambda(1,\chi)$ et $W(\chi)$ et d'en déduire ainsi des valeurs approchées satisfaisantes de $L'_S(0,\chi)$ puis de $\zeta'_S(0,\sigma)$. En remplaçant dans la formule 2.1.18, on en déduit des approximations de $|\sigma(\varepsilon)|_w$ pour tout $\sigma \in G$. Il est à présent nécessaire d'ôter la valeur absolue $|.|_w$, *ie* de déterminer le signe de $\sigma(\varepsilon)$. En fait, on sait déjà que $\varepsilon := w(\varepsilon) > 0$ par construction. De plus, on a le résultat suivant :

Proposition 2.12. *Soit E/F une extension galoisienne de corps de nombres et soit θ un élément de E qui n'est pas un carré dans E.*

Alors, l'extension $E(\sqrt{\theta})/F$ est galoisienne si et seulement si :

$$\text{pour tout } \sigma \in \mathrm{Gal}(E/F),\ \sigma(\theta)\theta^{-1} \in (E^\times)^2.$$

Démonstration : C'est une conséquence directe de la théorie de Kummer. Les extensions quadratiques de E sont en correspondance bijective avec les sous-groupes d'ordre 2 de $E^\times/(E^\times)^2$; en particulier, les extensions galoisiennes sont en correspondance avec les sous-groupes stables par $\mathrm{Gal}(E/F)$. Ainsi, $E(\sqrt{\theta})/F$ est galoisienne si et seulement si $\sigma(\theta)(E^\times)^2 = \theta(E^\times)^2$ pour tout $\sigma \in \mathrm{Gal}(E/F)$. □

La conjecture 2.1 affirme que l'extension $K(\sqrt{\varepsilon})/k$ est abélienne ; elle est donc avant tout galoisienne, d'où :

$$\text{pour tout } \sigma \in G,\ \sigma(\varepsilon) \in \varepsilon w(K^\times)^2,$$

et donc $\sigma(\varepsilon) > 0$, puisque ε est positif et le plongement w est réel.

Corollaire 2.13. *Tous les conjugués de ε au-dessus de la place v_1 sont positifs.*

On peut donc enlever les valeurs absolues, et en déduire des valeurs approchées des conjugués de ε, puis de α sur k. On forme à présent le polynôme réel dont les racines sont les valeurs approchées trouvées, disons $\tilde{P}(X) = X^m + \tilde{\beta}_{m-1}X^{m-1} + \cdots + \tilde{\beta}_0$, où $m := h_k(\mathfrak{m})$ est le degré de L sur k et les $\tilde{\beta}_i$ sont des nombres réels.

Si on note $P(X) = X^m + \beta_{m-1}X^{m-1} + \cdots + \beta_0$ le polynôme irréductible de α sur k, les β_i sont des entiers algébriques de k dont, par construction, les $\tilde{\beta}_i$ sont des approximations en la place v_1. Cependant, cela ne suffit pas pour reconnaître ces coefficients. En effet, il n'est pas difficile de démontrer qu'il existe une infinité d'entiers algébriques de k qui sont aussi proches qu'on le souhaite d'un réel donné. Pour pouvoir reconnaître les coefficients β_i, on a besoin de savoir ce qui se passe en les autres places infinies de k.

Lemme 2.14. *Soit w' une place infinie de K qui ne divise pas v_1 (w' est donc complexe).*

Alors, on a $|\varepsilon|_{w'} = 1$.

Démonstration : Soit σ le plongement complexe associé à w', *ie* pour tout $x \in K$, $\bar{\sigma}(x)\sigma(x) = |x|_{w'}$. On va montrer que $\sigma^{-1}\bar{\sigma} = \tau$. On obtiendra alors :

$$\bar{\sigma}(\varepsilon) = \sigma\tau(\varepsilon) = \sigma(\varepsilon)^{-1},$$

ce qui démontrera le lemme.

Faisons agir σ sur L. Pour $x \in L$, on obtient $\sigma(x) = \bar{\sigma}(x)$ puisque L est totalement réel. Donc $\sigma^{-1}\bar{\sigma}$ restreint à L est l'identité et $\sigma^{-1}\sigma \in \mathrm{Gal}(K/L) =< \tau >$. Mais ce ne peut être l'identité de K sur L car σ est complexe, donc $\sigma^{-1}\bar{\sigma} = \tau$, ce qui achève la démonstration. □

Remarque : Il est à noter que cette affirmation est une partie de la conjecture dans le cas général. Cependant, ici, la construction particulière du corps K permet de montrer que c'est une conséquence des autres hypothèses.

Avec le lemme 2.14, il est possible de majorer les conjugués de α en les places infinies de L qui ne sont pas au-dessus de v_1 (pour une telle place w', on a $|\alpha|_{w'} \leq 2$), et ainsi on obtient des bornes pour les $|\beta_i|_{v_j}$ pour toutes les places v_j $(2 \leq j \leq N)$. On trouve explicitement :

$$|\beta_i|_{v_j} \leq \binom{m}{i} 2^i,$$

pour $0 \leq i \leq m-1$ et $2 \leq j \leq N$. Les coefficients $\tilde{\beta}_i$ et une majoration de l'erreur commise dans les calculs permettent d'obtenir également un encadrement de $|\beta_i|_{v_1}$. Il est bien connu qu'il n'existe dans un corps de nombres fixé, qu'un nombre fini d'entiers algébriques dont tous les conjugués sont dans des intervalles donnés. Reste à déterminer ceux-ci et à trouver parmi eux le coefficient recherché.

Supposons que β soit l'entier algébrique que l'on souhaite identifier, connaissant $\tilde{\beta}$, une approximation de $v_1(\beta)$ avec une erreur absolue de r, *ie* :

$$|v_1(\beta) - \tilde{\beta}| < r,$$

et C une borne pour $|\beta|_i$, pour $2 \leq i \leq N$. Une première méthode est de chercher une relation entière entre les nombres réels $\tilde{\beta}$ et $v_1(\omega_1), \ldots, v_1(\omega_N)$ où les ω_i forment une base d'entiers fixée de k, en utilisant les méthodes de [**8**] section 2.7.2 ou de [**28**], en contrôlant de plus la taille des entiers impliqués, afin que les autres conjugués ne soient pas trop grands.

Cette méthode marche assez bien en général si on dispose d'une précision suffisante et si la taille de $\tilde{\beta}$ est raisonnable : c'est d'ailleurs la méthode utilisée dans [**17**]. Malheureusement, dans le cas général, elle se revèle inefficace ; on utilise plutôt la méthode suivante.

Soit γ un entier de k donné par cette première méthode, *ie* construit de sorte que $|\tilde{\beta} - v_1(\gamma)|$ soit relativement petit (mais pas forcément plus petit que r), mais aussi tel que $|\gamma|_{v_i}$ soit petit pour $2 \leq i \leq N$. On trouve facilement un tel γ et une constante C' de l'ordre de grandeur de C tels que :

$$\begin{aligned} |\tilde{\beta} - v_1(\gamma)| &\leq C' \\ |\gamma|_{v_i} &\leq C' \text{ pour } 2 \leq i \leq N. \end{aligned}$$

Si on écrit maintenant $\eta = \beta - \gamma$, on obtient :

$$T_2(\eta) \leq r^2 + C'^2 + 2rC' + (N-1)(C^2 + C'^2 + 2CC') \approx (4N-3)C^2 \tag{2.3.27}$$

car r est négligeable devant C.

D'un autre côté, on trouve que $T_2(\beta) \leq |\tilde{\beta}|^2 + (N-1)C^2$, et ainsi, il est préférable de travailler avec η plutôt qu'avec β dès que :

$$|\tilde{\beta}| > C\sqrt{3N-2},$$

ce qui est souvent le cas, puisque, comme mentionné plus haut, les calculs effectués tendent à montrer que la taille de $\tilde{\beta}$ croît exponentiellement avec la taille du conducteur de K. En utilisant les méthodes de [**19**] (qui sont également décrites dans [**8**] section 2.7.3) il est possible de trouver tous les entiers algébriques de k vérifiant 2.3.27 ; en éliminant ceux qui ne vérifient pas également les encadrements supplémentaires en chaque autre place infinie de k, notamment en v_1, on finit généralement avec un nombre très réduit d'éléments η candidats à vérifier $\beta = \gamma + \eta$ (le plus souvent un seul).

En procédant de même pour tous les coefficients de $\tilde{P}(X)$ puis en formant tous les polynômes à coefficients dans $\mathcal{O}_k$ qu'ils définissent, on obtient un certain nombre de polynômes $P_i(X)$ et l'un d'eux est conjecturalement le polynôme irréductible de α sur k.

La dernière étape consiste à trouver le bon polynôme parmi les candidats, *ie* vérifier si un des polynômes parmi ceux construits définit bien le corps L. Ceci fait l'objet de la section suivante.

2.4. Vérification du résultat

Soit $P(X)$ un polynôme à coefficients dans $\mathcal{O}_k[X]$; on cherche à savoir s'il est ou non le polynôme irréductible d'un entier algébrique primitif de $L := k(\mathfrak{f})$ (on suppose toujours que $\mathfrak{f}$ est un conducteur). On procède en différentes étapes décrites ci-après.

On vérifie d'abord que le degré de $P(X)$ est bien celui de l'extension L/k (notons que c'est trivialement le cas avec la méthode utilisée ci-dessus).

En calculant le discriminant de $P(X)$, on vérifie que le polynôme est séparable, puis irréductible en utilisant la méthode du chapitre 1. A la fin de cette étape, on note $\tilde{L}$ le corps définit par une racine θ de $P(X)$, on a $[\tilde{L} : k] = [L : k]$.

On calcule le polynôme absolu de θ sur $\mathbb{Q}$ puis, à l'aide de l'algorithme de Sturm (*cf* [**8**] section 4.1.2) on vérifie que le corps $\tilde{L}$ est totalement réel.

Avec les algorithmes de [**12**], on calcule le discriminant relatif de $\tilde{L}/k$ qui doit être égal à celui de L/k.

On vérifie que la factorisation de $P(X)$ dans $\tilde{L}[X]$ n'admet que des facteurs linéaires, ce qui prouve que l'extension $\tilde{L}/k$ est galoisienne. De plus, cette factorisation donne explicitement les k-automorphismes de $\tilde{L}$ et permet ainsi de montrer que l'extension est abélienne et de trouver la structure de son groupe de Galois $\tilde{G} := \mathrm{Gal}(\tilde{L}/k)$ (par exemple, en utilisant la méthode Baby Step - Giant Step de Shanks, *cf* [**8**] section 5.4.1).

Parvenu à cette étape, on sait que $\tilde{L}/k$ est une extension abélienne de même discriminant, signature et groupe de Galois que L/k. C'est le plus souvent suffisant. Remarquons que pour montrer que $\tilde{L} = L$, il suffit de montrer que le conducteur $\tilde{\mathfrak{f}}$ de $\tilde{L}$ est $\mathfrak{f}$ car on a alors $\tilde{L} \subset L$ puis $\tilde{L} = L$ puisque ces deux corps ont le même degré relatif sur k.

Numérotons $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ les idéaux premiers qui divisent le discriminant relatif $\mathfrak{d}_{\tilde{L}/k}$, puis posons $e_i := \mathrm{val}_{\mathfrak{q}_i}(\mathfrak{d}_{\tilde{L}/k})$. On sait déjà que le conducteur de $\tilde{L}/k$ est de la forme :

$$\tilde{\mathfrak{f}} = \prod_{i=1}^{r} \mathfrak{q}_i^{v_i}$$

avec $v_i \geq 1$ pour tout i. En utilisant la formule explicite de calcul du discriminant d'une extension abélienne donnée dans [**11**], on démontre facilement que :

$$v_i \leq e_i \frac{p}{m(p-1)} \tag{2.4.28}$$

où p est le plus petit nombre premier divisant $m := [\tilde{L} : k] = [L : k]$.

Grâce à ces inégalités, il est possible de construire tous les groupes de congruence des corps pouvant vérifier les mêmes propriétés que $\tilde{L}$. Une telle construction est souvent aisée et aboutit fréquemment à un seul corps, le corps L, ce qui permet de démontrer que $\tilde{L} = L$. Si cette construction ne suffit pas pour conclure, on utilise l'algorithme suivant :

On commence en posant :

$$v_i := \left\lfloor e_i \frac{p}{m(p-1)} \right\rfloor$$

puis :

$$\mathfrak{m} := \prod_{i=1}^{r} \mathfrak{q}_i^{v_i}.$$

On sait que le corps $\tilde{L}$ est un sous-corps du corps de classes de rayon $k(\mathfrak{m})$. On note $\mathcal{K}$ le groupe de congruence de $\tilde{L}$ modulo $\mathfrak{m}$. L'idée est de se servir de la connaissance explicite qu'on a de la décomposition des idéaux premiers dans $\tilde{L}/k$ pour caractériser au mieux le sous-groupe $\mathcal{K}$. Ainsi, on va faire "grossir" ce groupe jusqu'à obtenir le groupe de congruence de $\tilde{L}$ modulo $\mathfrak{m}$.

Le groupe $\mathcal{K}$ est engendré par les classes des idéaux $\mathfrak{p}^{f_\mathfrak{p}}$ où $\mathfrak{p}$ parcourt les idéaux premiers de k ne divisant pas $\mathfrak{m}$ et où $f_\mathfrak{p}$ est le degré résiduel de $\mathfrak{p}$ dans $\tilde{L}/k$. Afin de déterminer le degré résiduel d'un idéal premier par la méthode expliquée au chapitre précédent, on écarte tout d'abord les idéaux premiers qui divisent le discriminant de P ; pour cela, on multiplie le module $\mathfrak{m}$ par tous les idéaux premiers divisant le discriminant de P et qui ne divisent pas déjà $\mathfrak{m}$.

On obtient l'algorithme suivant :

Algorithme 2.15. *Soient $\tilde{L}/k$ une extension finie abélienne définie par une racine d'un polynôme P unitaire et irréductible de $\mathcal{O}_k[X]$, et $\mathfrak{m}$ un module de k tels que $\tilde{L} \subset k(\mathfrak{m})$ et tel que tous les idéaux premiers divisant* $\mathrm{disc}(P)$ *divisent aussi $\mathfrak{m}$. Cet algorithme calcule le conducteur de $\tilde{L}$.*

1. *On pose $\mathcal{K} \leftarrow [1]_\mathfrak{m}$ et $p \leftarrow 1$.*

2. *On remplace p par le plus petit nombre premier $\geq p+1$. Puis, à l'aide de l'algorithme 6.2.9 de* [**8**]*, on décompose le nombre premier p dans k ; désignons par $\mathfrak{p}_i$ pour $1 \leq i \leq g_p$, les idéaux premiers de k au-dessus de p. On pose $i \leftarrow 1$.*

3. *Si $i > g_p$, on retourne à l'étape précédente.*

Sinon, si $\mathfrak{p}_i$ ne divise pas $\mathfrak{m}$, on factorise P modulo $\mathfrak{p}_i$; soit f_i le degré des polynômes irréductibles apparaissant dans cette factorisation (tous ces polynômes ont même degré puisque l'extension $\tilde{L}/k$ est galoisienne).

4. *On pose $\mathcal{K} \leftarrow < \mathcal{K}, [\mathfrak{p}_i]_\mathfrak{m}^{f_i} >$. Si $(\mathrm{Cl}_k(\mathfrak{m}) : \mathcal{K}) = [\tilde{L} : k]$, on calcule le conducteur $\tilde{\mathfrak{f}}$ correspondant au groupe de congruence $\mathcal{K}$ par les algorithmes de* [**11**]*, on retourne le module $\tilde{\mathfrak{f}}$ et l'algorithme se termine. Sinon, on pose $i \leftarrow i+1$ et on retourne à l'étape précédente.*

Pour montrer que cet algorithme se termine, notons $\mathcal{K}_i$ le groupe de congruence obtenu à l'étape **4** de l'algorithme aprés avoir considéré les i premiers nombres premiers rationnels. Il est clair que :

$$\lim_{i \to \infty} \mathcal{K}_i = \mathcal{K}.$$

Ceci implique qu'il existe un indice j tel que $\mathcal{K}_j = \mathcal{K}$ puisque le groupe $\mathrm{Cl}_k(\mathfrak{m})$ est fini.

En fait, si on veut bien admettre l'hypothèse de Riemann généralisée (GRH), on peut faire beaucoup mieux. On peut en effet écrire dans ce cas, un algorithme qui démontre à la fois que l'extension est abélienne et calcule son conducteur. On évite ainsi les calculs compliqués nécessaires à établir que l'extension est galoisienne puis abélienne.

On ne suppose donc plus que l'extension $\tilde{L}/k$ est galoisienne. On note $\tilde{L}^{ab}$ la plus grande sous-extension de $\tilde{L}/k$ qui est abélienne sur k. En utilisant les majorations 2.4.28, on calcule un module $\mathfrak{m}$ tel que $\tilde{L}^{ab} \subset k(\mathfrak{m})$. On note $\mathcal{N}$ le sous-groupe de $I_k(\mathfrak{m})$ engendré par les normes des idéaux de $\tilde{L}$ premiers avec $\mathfrak{m}$ et $P_k(\mathfrak{m})$, et on note $\mathcal{N}^{ab}$ le groupe des normes de $\tilde{L}^{ab}/k$ pour le module $\mathfrak{m}$. Un corollaire direct du théorème 6.5 de [**43**] affirme alors que $\mathcal{N} = \mathcal{N}^{ab}$.

On a aussi le résultat suivant (*cf* [**2**] th. 5.1) :

Théorème 2.16 (Bach, Sorenson)**.** *Soit E/F une extension galoisienne de corps de nombres avec $F \neq \mathbb{Q}$. On note d_E la valeur absolue du discriminant de $E/\mathbb{Q}$, et M le degré de $E/\mathbb{Q}$. Soit $\sigma \in \mathrm{Gal}(E/F)$.*

Alors, il existe un idéal premier $\mathfrak{p}$ de F de degré résiduel 1 dont le Frobenius $\sigma_\mathfrak{p}$ vaut σ et vérifiant (sous GRH) :

$$\mathcal{N}\mathfrak{p} \leq C(E) := (4 \log d_E + \frac{5}{2} M + 5)^2.$$

On utilise ce résultat avec $E = \tilde{L}^{ab}$ et $F = k$. Soit $\mathfrak{p}$ un idéal premier ne divisant $\mathfrak{m}$; on note f son degré résiduel dans $\tilde{L}/k$ (si cet indice n'est pas unique, alors l'extension $\tilde{L}/k$ n'est pas galoisienne et donc *a fortiori* non abélienne et le problème est réglé) et f^{ab} le degré résiduel dans $\tilde{L}^{ab}/k$. La propriété $\mathcal{N} = \mathcal{N}^{ab}$ donne le résultat suivant :

Lemme 2.17.

$$\langle < [\mathfrak{p}]_{\mathfrak{m}}^{f} > = < [\mathfrak{p}]_{\mathfrak{m}}^{f^{ab}} \rangle.$$

Démonstration : (Notons qu'en général, $[\mathfrak{p}]_{\mathfrak{m}}^{f} \neq [\mathfrak{p}]_{\mathfrak{m}}^{f^{ab}}$). Soit a l'ordre de la classe de $\mathfrak{p}$ dans $\mathrm{Cl}_k(\mathfrak{m})$; il est facile de voir que c'est un multiple de f^{ab}, disons $a = f^{ab}b$ (par exemple, en disant que c'est le degré résiduel de $\mathfrak{p}$ dans $k(\mathfrak{m})/k$ qui est une sur-extension de $\tilde{L}^{ab}/k$).

Ainsi, l'ordre de $[\mathfrak{p}^{f^{ab}}]_{\mathfrak{m}}$ est b. D'un autre côté, f^{ab} divise également f et on écrit $f = cf^{ab}$. Puisque $\mathcal{N} = \mathcal{N}^{ab}$, on peut écrire l'équation :

$$\mathfrak{p}^{f^{ab}} = \mathfrak{a}_1\mathfrak{a}_2$$

où $\mathfrak{a}_1 \in \mathcal{N}$ et $\mathfrak{a}_2 \in P_k(\mathfrak{m})$, et en prenant la valuation en $\mathfrak{p}$ on trouve :

$$f^{ab} = nf + la$$

pour deux entiers n et l, car la plus petite puissance de $\mathfrak{p}$ dans $\mathcal{N}$ (resp. $P_k(\mathfrak{m})$) est $\mathfrak{p}^f$ (resp. $\mathfrak{p}^a$). En divisant par f^{ab}, il vient :

$$1 = nc + lb$$

et donc $(b, c) = 1$. Ainsi, l'ordre de $[\mathfrak{p}^f]_{\mathfrak{m}}$ est $a/(a, f) = a/(bf^{ab}, cf^{ab}) = a/f^{ab} = b$. Ce qui démontre le résultat compte tenu du fait qu'on a $< [\mathfrak{p}]_{\mathfrak{m}}^{f} > \subset < [\mathfrak{p}]_{\mathfrak{m}}^{f^{ab}} >$. □

Ainsi, si on note $\mathcal{K}$ le sous-groupe de $\mathrm{Cl}_k(\mathfrak{m})$ engendré par les classes des $\mathfrak{p}^f$ où $\mathfrak{p}$ parcourt les idéaux premiers de degré résiduel 1 ne divisant pas $\mathfrak{m}$ et de norme $\leq C(\tilde{L})$ et où f est le degré résiduel de $\mathfrak{p}$ dans l'extension, alors, il découle du lemme (sous GRH) qu'on a en fait $\mathcal{K} = \mathcal{N}^{ab} = \mathcal{N}$; en particulier, l'extension $\tilde{L}/k$ est abélienne si et seulement si (sous GRH) :

$$(\mathrm{Cl}_k(\mathfrak{m}) : \mathcal{K}) = [\tilde{L} : k].$$

On déduit de tout cela l'algorithme suivant :

Algorithme 2.18. *Soient $\tilde{L}/k$ une extension finie définie par une racine du polynôme P unitaire et irréductible de $\mathcal{O}_k[X]$ et $\mathfrak{m}$ un module de k tels que $\tilde{L}^{ab} \subset k(\mathfrak{m})$ et tel que tous les idéaux premiers divisant* $\mathrm{disc}(P)$ *divisent aussi $\mathfrak{m}$. Cet algorithme ou bien démontre que l'extension $\tilde{L}/k$ est abélienne (sous GRH) et dans ce cas, retourne son conducteur, ou bien l'algorithme démontre que cette extension n'est pas abélienne.*

1. *On pose $\mathcal{K} \leftarrow [1]_{\mathfrak{m}}$ et $p \leftarrow 1$. On calcule également la borne $C(\tilde{L})$ donnée par le théorème 2.16.*

2. *On remplace p par le plus petit nombre premier $\geq p + 1$. Si $p > C(\tilde{L})$, on va à l'étape* **6** *; sinon, à l'aide de l'algorithme 6.2.9 de* [**8**]*, on décompose le nombre premier p dans k. On désigne par $\mathfrak{p}_i$ pour $1 \leq i \leq g_p$ les idéaux premiers de k au-dessus de p. On pose $i \leftarrow 1$.*

3. *Si $i > g_p$, on retourne à l'étape précédente.*

Si le degré résiduel de $\mathfrak{p}_i > 1$, on pose $i \leftarrow i + 1$ et on recommence cette étape.

Si $\mathfrak{p}_i$ ne divise pas $\mathfrak{m}$, on factorise P modulo $\mathfrak{p}_i$ et on pose f_i le degré des polynômes irréductibles de cette factorisation (tous ces polynômes ont même degré sinon l'extension n'est pas abélienne et l'algorithme se termine).

4. *On pose $\mathcal{K} \leftarrow < \mathcal{K}, [\mathfrak{p}_i]_{\mathfrak{m}}^{f_i} >$. Si $(\mathrm{Cl}_k(\mathfrak{m}) : \mathcal{K}) < [\tilde{L} : k]$, l'extension n'est pas abélienne et l'algorithme se termine.*

Sinon, on pose $i \leftarrow i + 1$, et retourne à l'étape précédente.

5. *On vérifie que $(\mathrm{Cl}_k(\mathfrak{m}) : \mathcal{K}) = [\tilde{L} : k]$ et on calcule le conducteur $\tilde{\mathfrak{f}}$ correspondant au groupe de congruence $\mathcal{K}$ au moyen des algorithmes de* [**11**]*. Alors, sous GRH, l'extension $\tilde{L}/k$ est abélienne ; on retourne son conducteur $\tilde{\mathfrak{f}}$ et l'algorithme se termine.*

Remarque : A l'étape **5**, on doit avoir $(\mathrm{Cl}_k(\mathfrak{m}) : \mathcal{K}) \leq [\tilde{L} : k]$, et même égalité à cause du test de l'étape **4**. Si on obtient le résultat contraire, cela implique que le groupe de congruence n'a pas pu être calculé et ceci impliquerait par le théorème 2.16 que l'hypothèse de Riemann généralisée est fausse !

La solution la meilleure pour démontrer que $\tilde{L}/k$ est abélienne est sans doute de commencer par utiliser cet algorithme. Si l'algorithme répond négativement, la question est réglée. Sinon, il y a de grandes chances que

l'extension soit abélienne (autant qu'il y en a de chances que GRH soit vraie) et on peut alors démontrer par des méthodes plus fastidieuses mais inconditionnelles que l'extension est vraiment abélienne.

2.5. Un exemple de construction

L'exemple suivant a été choisi pour sa simplicité ; mais, il illustre assez bien la plupart des difficultés décrites ci-dessus et les moyens de les résoudre.

Soit $k := \mathbb{Q}(\sqrt{2})$. On désigne par v_1 et v_2 les deux places infinies de k :

$$v_1(\sqrt{2}) = \sqrt{2} \text{ et } v_2(\sqrt{2}) = -\sqrt{2}.$$

On cherche à construire le corps de classes de rayon modulo :

$$\mathfrak{f} := 7\mathcal{O}_k.$$

Notons pour commencer que $7\mathcal{O}_k$ est le produit des deux idéaux premiers $\mathfrak{p}_7$ et $\mathfrak{q}_7$ au-dessus de 7 dans k. On vérifie que $\mathfrak{f}$ est bien un conducteur. Le groupe de classes de rayon de k modulo $\mathfrak{f}$ est un groupe cyclique d'ordre 3 engendré par la classe de l'idéal :

$$\mathfrak{a} := 2\mathcal{O}_k.$$

Le corps $L := k(\mathfrak{f})$ est donc une extension abélienne totalement réelle de k de degré 3 et de discriminant relatif $49\mathcal{O}_k$.

Un premier calcul permet de prouver que le corps K défini comme le corps de classes de rayon modulo :

$$\mathfrak{m} := \mathfrak{f}v_1$$

vérifie les conditions (a-c) ; en particulier, les idéaux premiers $\mathfrak{p}_7$ et $\mathfrak{q}_7$ sont respectivement ramifié et inerte dans K/L (On note que dans cet exemple, c'est la place v_2 qui joue le rôle de la place v_1 des sections 2 et 3). Le groupe de classes de rayon modulo $\mathfrak{m}$ est un groupe cyclique d'ordre 6 engendré par la classe de l'idéal :

$$\mathfrak{b} := \mathfrak{a}\mathfrak{p}_{71}$$

où $\mathfrak{p}_{71}$ est un des deux idéaux premiers de k au-dessus de 71. L'ensemble de places S est $\{\mathfrak{p}_7, \mathfrak{q}_7, v_1, v_2\}$.

Soit ζ_6 une racine primitive 6-ième de l'unité ; on note χ le caractère tel que :

$$\chi(\mathfrak{b}) = \zeta_6.$$

Il est clair que l'élément τ non trivial de $\mathrm{Gal}(K/L)$ est associé par l'application d'Artin à la classe de $[\mathfrak{b}]_{\mathfrak{m}}^3$, et donc les caractères non triviaux en τ sont donnés par χ, χ^3 et χ^5. Ils ont pour conducteur respectivement $\mathfrak{m}$, $\mathfrak{q}_7 v_1$ et $\mathfrak{m}$.

On en déduit les facteurs correctifs :

$$A(\chi) = 1,\ A(\chi^3) = 2 \text{ et } A(\chi^5) = 1.$$

Puis on calcule les constantes d'Artin de ces caractères. On obtient :

$$W(\chi) = -i,\ W(\chi^3) = 1 \text{ et } W(\chi^5) = i.$$

En prenant $N_0 := 192$ et $h_0 := 226$ (avec les notations de la proposition 2.9), on calcule des approximations des dérivées des fonctions L_S en $s = 0$. Puis, en appliquant la formule 2.1.15, on trouve :

$$\begin{aligned} \zeta'_S(0, [\mathfrak{b}]_{\mathfrak{m}}) &\approx 0.9049468106, \\ \zeta'_S(0, [\mathfrak{b}]_{\mathfrak{m}}^3) &\approx 1.0072499881, \\ \zeta'_S(0, [\mathfrak{b}]_{\mathfrak{m}}^5) &\approx 0.7352774966. \end{aligned}$$

Le polynôme $\tilde{P}(X)$ défini plus haut est le suivant :

$$X^3 - 18.4852813742X^2 + 111.5685424949X - 219.3086578651.$$

Par la méthode expliquée ci-dessus, on détermine 3 entiers algébriques :

$$\begin{aligned}\beta_2 &:= 6\sqrt{2}-10 \text{ avec } v_2(\beta_2)\approx -18.4852813742\\ \beta_1 &:= -40\sqrt{2}+55 \text{ avec } v_2(\beta_1)\approx 111.5685424949\\ \beta_0 &:= 78\sqrt{2}-109 \text{ avec } v_2(\beta_0)\approx -219.3086578651\end{aligned}$$

Ainsi, on peut conjecturer que le polynôme relatif :

$$P(X) := X^3+(6\sqrt{2}-10)X^2+(-40\sqrt{2}+55)X+(78\sqrt{2}-109)$$

est le polynôme irréductible d'un élément primitif de L sur k. On commence par vérifier qu'il est bien irréductible sur k. Puis par la méthode expliquée dans le chapitre suivant, on réduit ce polynôme. On trouve (et on continue de noter P ce polynôme par abus) :

$$P(X) = X^3-\sqrt{2}X^2-4X+2\sqrt{2}.$$

Soit α une racine de P ; le polynôme irréductible de α sur $\mathbb{Q}$ est :

$$X^6-10X^4+24X^2-8$$

qui est bien de signature $(6,0)$. On note $\tilde{L} := \mathbb{Q}(\alpha)$.

On calcule le discriminant relatif de $\tilde{L}/k$:

$$\mathfrak{d}_{\tilde{L}/k} = 49\mathcal{O}_k = \mathfrak{f}^2$$

donc $\tilde{L}$ et L ont le même discriminant relatif.

En utilisant les méthodes du chapitre 1, on exprime le polynôme P en fonction de α, on trouve :

$$X^3+(-\frac{1}{4}\alpha^5+2\alpha^3-3\alpha)X^2-4X+(\frac{1}{2}\alpha^5-4\alpha^3+6\alpha)$$

dont la factorisation dans $\tilde{L}[X]$ permet de prouver que l'extension $\tilde{L}/k$ est galoisienne (et donc abélienne) de groupe de Galois engendré par l'automorphisme :

$$\sigma : \alpha \mapsto \frac{1}{2}\alpha^3-3\alpha.$$

Finalement, en considérant les inégalités 2.4.28, on démontre que le conducteur de $\tilde{L}$ est $\mathfrak{f}$, ce qui achève de montrer que $L=\tilde{L}$. (En fait, si L/k est une extension abélienne de degré premier p et de conducteur $\mathfrak{f}$, alors le discriminant relatif de L/k est $\mathfrak{f}^{p-1}$.)

Néanmoins, afin d'illustrer la méthode de détermination du conducteur expliquée ci-dessus, on redémontre ce point en utilisant l'algorithme 2.15.

On pose $\mathfrak{m} := \mathfrak{p}_2^2\mathfrak{p}_7^2\mathfrak{q}_7^2$ avec les notations de l'algorithme (on ajoute l'unique idéal premier $\mathfrak{p}_2$ divisant 2 dans ce module car il divise le discriminant de P). Le groupe de classes $\mathrm{Cl}_k(\mathfrak{m})$ est un groupe cyclique d'ordre 21 engendré par la classe $\mathcal{C}$ de l'idéal principal :

$$(19+\sqrt{2})\mathcal{O}_k.$$

Modulo l'unique idéal premier $\mathfrak{p}_3$ au-dessus de 3, on trouve que le polynôme P est irréductible. Ainsi, le groupe $\mathcal{K}$ contient le sous-groupe de $\mathrm{Cl}_k(\mathfrak{m})$ engendré par $[\mathfrak{p}_3]_{\mathfrak{m}}^3$. Mais, ce sous-groupe est d'indice 3 puisque $[\mathfrak{p}_3]_{\mathfrak{m}} = \mathcal{C}^{19}$. Ainsi, $\mathcal{K}$ est le groupe de congruence de $\tilde{L}$ modulo $\mathfrak{m}$. On calcule son conducteur et on trouve :

$$\tilde{\mathfrak{f}} = 7\mathcal{O}_k$$

ce qui redémontre que $\tilde{L}=L$.

2.6. Corps de classes ramifiées à l'infini

Le but de cette section est de montrer que l'hypothèse selon laquelle le rayon $\mathfrak{f}$ ne contient pas de places infinies n'est pas restrictive, et qu'il est possible de construire les corps de classes de rayon ramifiés aux places infinies à partir de corps de classes de rayon sans ramification à l'infini construits par la méthode expliquée dans ce chapitre. Cette méthode utilise la théorie de Kummer ; on peut se réferer à [**15**] pour l'utilisation de cette théorie dans des constructions plus générales.

Soit $\mathfrak{f}$ un conducteur de k ; on suppose cette fois que la partie infinie $\mathfrak{f}_\infty$ de $\mathfrak{f}$ n'est pas triviale. En particulier, si on note $L^+ := k(\mathfrak{f}_0)$ le sous-corps réel maximal de $L := k(\mathfrak{f})$, alors l'extension L/L^+ est une 2-extension abélienne, *ie* une extension abélienne dont le groupe de Galois admet 2 comme exposant. Il est possible de construire cette extension par la théorie de Kummer puisque L^+ contient les racines d'ordre 2 de l'unité. On pose $G := \mathrm{Gal}(L/k)$, $G^+ := \mathrm{Gal}(L^+/k)$ et $G_2 := \mathrm{Gal}(L/L^+)$.

Théorème 2.19 (Kummer)**.** *Soit F un corps de nombres contenant les racines primitives d'ordre n de l'unité.*

Alors les n-extensions E de F, ie les extensions abéliennes finies de F dont le groupe de Galois est d'exposant un diviseur de n, sont en bijection avec les classes Δ de $F^\times/(F^\times)^n$ d'ordre fini. La bijection étant donnée par :

$$\begin{aligned} E/F &\mapsto \Delta = (E^\times)^n \cap F^\times \\ \Delta \in F^\times/(F^\times)^n &\mapsto E = F(\sqrt[n]{\Delta}). \end{aligned}$$

(*cf* [**43**] chap. I §5 et chap. IV §4.)

On montre aussi que si n est un nombre premier et $[E : F] = n^r$, alors r est la dimension du sous-$\mathbb{F}_n$-espace vectoriel Δ. Ainsi, si $[L : L^+] = 2^r$, il existe des entiers algébriques $\alpha_1, \ldots, \alpha_r$ de L^+ qui ne sont pas des carrés dans L^+ et tels que :

$$L = L^+(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_r}).$$

En particulier, L est la composée d'extensions quadratiques $L_i := L^+(\sqrt{\alpha_i})$, toutes ramifiées à l'infini. On peut aisément calculer les groupes de congruence de ces extensions L_i en regardant les sous-groupes de G_2 d'indice 2. On va donc expliquer comment construire l'une de ces extensions quadratiques, disons L_1 ; on obtiendra le corps L en appliquant cette construction aux autres extensions L_i puis en faisant la composée.

On note $\alpha := \alpha_1$ de telle sorte que :

$$L_1 = L^+(\sqrt{\alpha}).$$

Le théorème suivant (*cf* [**29**] th. 118 et 119) permet de caractériser cet élément.

Théorème 2.20 (Hecke)**.** *Soient F un corps de nombres et θ un entier algébrique de F qui n'est pas un carré dans F. On pose $E := F(\sqrt{\theta})$. Quitte à remplacer θ par $\beta^2\theta$ pour $\beta \in F^\times$ (ce qui ne change pas l'extension E/F), on suppose que pour tout idéal premier $\mathfrak{P}$ divisant 2, on a $\mathrm{val}_\mathfrak{P}(\theta) = 0$ ou 1.*

(i) *Pour un idéal premier $\mathfrak{P}$ ne divisant pas 2, $\mathfrak{P}$ est ramifié dans E/F si et seulement si $\mathrm{val}_\mathfrak{P}(\theta) \not\equiv 0 \pmod 2$.*

(ii) *Pour un idéal premier $\mathfrak{P}$ divisant 2. Si $\mathrm{val}_\mathfrak{P}(\theta) = 1$ alors $\mathfrak{P}$ est ramifié ; sinon, $\mathfrak{P}$ ne divise pas θ et dans ce cas $\mathfrak{P}$ est ramifié dans E/F si et seulement si θ n'est pas un carré modulo $\mathfrak{P}^{2a_\mathfrak{P}}$, où $a_\mathfrak{P} := e_\mathfrak{P}(F/\mathbb{Q})$.*

(iii) *Pour une place infinie v de F, v est ramifiée dans E/F si et seulement si $v(\theta) < 0$.*

On commence par supposer, comme dans le théorème précédent, que l'élément α vérifie $\mathrm{val}_\mathfrak{P}(\alpha) = 0$ ou 1 pour tout idéal premier $\mathfrak{P}$ divisant 2, et aussi que c'est un entier algébrique. En effet, par le théorème d'approximation, il existe un élément $\beta \in L^+$ tel que :

$$\begin{aligned} \text{pour tout } \mathfrak{P} \mid 2,\ \mathrm{val}_\mathfrak{P}(\beta) &= -\Big\lfloor \frac{v_\mathfrak{P}(\alpha)}{2} \Big\rfloor \\ \text{pour tout } \mathfrak{Q} \nmid 2,\ \mathrm{val}_\mathfrak{Q}(\beta) &\geq 0 \end{aligned}$$

et il suffit alors de remplacer α par $\beta^2\alpha$.

On note $\mathfrak{r}$ le produit des idéaux premiers de k qui se ramifient dans L_1/L^+. On partage les idéaux de L^+ au-dessus de ces idéaux en deux sous-ensembles :

$$\begin{aligned} S_{0,2} &:= \{ \text{ idéaux premiers } \mathfrak{P} \text{ de } L^+ \text{ tels que } \mathfrak{P} \mid \mathfrak{r}\mathcal{O}_{L^+} \text{ et } \mathfrak{P} \mid 2\}, \\ S_{0,p} &:= \{ \text{ idéaux premiers } \mathfrak{P} \text{ de } L^+ \text{ tels que } \mathfrak{P} \mid \mathfrak{r}\mathcal{O}_{L^+} \text{ et } \mathfrak{P} \nmid 2\} ; \end{aligned}$$

puis, pour les places infinies ramifiées, on pose :

$$S_\infty := \{ \text{ places infinies } w \text{ de } L^+ \text{ telles que } w \text{ est ramifiée dans } L_1/L^+ \}.$$

Si on définit l'idéal $\mathfrak{a}$ par :

$$\mathfrak{a} := \prod_{\mathfrak{P} \in S_{0,p}} \mathfrak{P},$$

alors, le théorème 2.20 affirme l'existence d'un idéal entier $\mathfrak{b}$ premier avec 2, et d'un idéal $\mathfrak{c}$, produit d'un certain nombre d'idéaux distincts de $S_{0,2}$ tels que l'élément α vérifie :

$$(\alpha) = \mathfrak{a}\mathfrak{c}\mathfrak{b}^2. \tag{2.6.29}$$

On peut déterminer explicitement quels sont les idéaux de $S_{0,2}$ qui divisent $\mathfrak{c}$.

Lemme 2.21. *Avec les notations du théorème 2.20, l'idéal premier $\mathfrak{P}$ divisant 2 et ramifié dans E/F divise θ si et seulement si :*

$$v_{\mathfrak{P}}(\mathfrak{d}_{E/F}) \equiv 1 \pmod 2.$$

Démonstration : Le discriminant du polynôme $X^2 - \theta$ est 4θ. En particulier, on a :

$$\mathrm{val}_{\mathfrak{P}}(4\theta) = 2e_{\mathfrak{P}}(L^+/\mathbb{Q}) + \mathrm{val}_{\mathfrak{P}}(\theta).$$

Mais, on sait que ce discriminant diffère du discriminant de l'extension E/F par le carré d'un idéal, d'où il s'ensuit que $\mathrm{val}_{\mathfrak{P}}(\mathfrak{d}_{E/F}) \equiv \mathrm{val}_{\mathfrak{P}}(\theta) \pmod 2$. □

On sait calculer le discriminant de L_1/k par les méthodes de [**11**], ainsi que le discriminant de L^+/k. Grâce à la formule du discriminant dans une tour d'extensions, on obtient :

$$\mathfrak{d}_{L_1/k} = N_{L^+/k}(\mathfrak{d}_{L_1/L^+})\mathfrak{d}^2_{L^+/k}.$$

Soit $\mathfrak{P}$ un idéal premier de L^+, et $\mathfrak{p}$ l'idéal premier de k au-dessous ; on calcule le degré résiduel $f_{\mathfrak{p}}$ à l'aide du lemme 2.6, puis on écrit :

$$\mathrm{val}_{\mathfrak{P}}(\mathfrak{d}_{L_1/L^+}) = \frac{\mathrm{val}_{\mathfrak{p}}(\mathfrak{d}_{L_1/k}) - 2\,\mathrm{val}_{\mathfrak{p}}(\mathfrak{d}_{L^+/k})}{f_{\mathfrak{p}}}.$$

On peut ainsi calculer explicitement la valuation des idéaux premiers au-dessus de 2 qui divisent l'idéal $\mathfrak{c}$ de la formule 2.6.29 et déterminer grâce au lemme 2.21 l'idéal $\mathfrak{c}$ lui-même.

Maintenant qu'on a déterminé les idéaux $\mathfrak{a}$ et $\mathfrak{c}$, on considère l'ensemble des classes d'idéaux $\mathcal{B}_i$ de Cl_{L^+} telles que la classe $\mathcal{B}_i^2[\mathfrak{a}\mathfrak{c}]$ soit la classe principale. De telles classes existent puisqu'on a la relation 2.6.29. Ensuite, on choisit dans chacune de ces classes un idéal entier $\mathfrak{b}_i$ premier avec 2, et on note β_i un générateur de l'idéal entier principal $\mathfrak{a}\mathfrak{c}\mathfrak{b}_i^2$.

Proposition 2.22. *Il existe un unique indice i et une unité u unique modulo $E^2_{L^+}$ tels que :*

$$L_1 = L^+(\sqrt{u\beta_i}).$$

Démonstration : Commençons par montrer l'unicité. Supposons que :

$$L^+(\sqrt{u\beta_i}) = L^+(\sqrt{u'\beta_j}) ;$$

alors il existe un élément non nul $\gamma \in L^+$ tel que $u\beta_i = \gamma^2 u'\beta_j$; d'où $\mathfrak{b}_i^2 = \gamma^2\mathfrak{b}_j^2$ en passant aux idéaux puis en simplifiant. Il s'ensuit que $\mathfrak{b}_i$ et $\mathfrak{b}_j$ sont dans la même classe et donc que $i = j$, puisque l'on a choisi un unique idéal par classe. On trouve alors :

$$u = u'\gamma^2,$$

ce qui prouve que u est bien unique modulo $E^2_{L^+}$.

Démontrons l'existence. Par la formule 2.6.29, l'idéal $\mathfrak{ac}\mathfrak{b}^2$ est principal, donc il existe un indice i tel que $\mathfrak{b} = (\gamma)\mathfrak{b}_i$. D'où il s'ensuit :

$$(\alpha) = \mathfrak{ac}\mathfrak{b}^2 = (\gamma)^2\mathfrak{ac}\mathfrak{b}_i^2 = (\gamma^2)(\beta_i),$$

ie il existe une unité u telle que $\alpha = \gamma^2 u\beta_i$, et donc $L^+(\sqrt{u\beta_i}) = L^+(\sqrt{\alpha}) = L_1$. (Notons que par construction, β_i vérifie aussi la condition $\mathrm{val}_{\mathfrak{P}}(\beta_i) = 0$ ou 1 pour tout $\mathfrak{P} \mid 2$.) $\square$

Si on sait *a priori* que l'un des β_i permet de construire L_1, il reste à déterminer lequel. On commence par remarquer qu'il doit vérifier un certain nombre de congruences en les idéaux premiers au-dessus de 2 ne divisant pas $\mathfrak{c}$, ainsi que des inégalités en les places infinies ; plus exactement, il doit exister une unité u telle que :

- $u\beta_i$ est congru à un carré modulo $\mathfrak{P}^{2a_{\mathfrak{P}}}$ si $\mathfrak{P} \mid 2$ et $\mathfrak{P} \notin S_{0,2}$,
- $u\beta_i$ n'est pas congru à un carré modulo $\mathfrak{P}^{2a_{\mathfrak{P}}}$ si $\mathfrak{P} \in S_{0,2}$ et $\mathfrak{P} \nmid \mathfrak{c}$,
- $w(u\beta_i) < 0$ si et seulement si $w \in S_\infty$.

En considérant les logarithmes discrets d'un système d'unités fondamentales de L^+ et des éléments β_i dans $(\mathcal{O}_{L^+}/\mathfrak{P}^{2a_{\mathfrak{P}}})^\times$, puis les signatures de ces éléments suivant la procédure décrite dans [**11**], on détermine les unités u_i et les éléments β_i convenables.

On aboutit ainsi à un ensemble fini $\{\theta_1 := u_1\beta_1, \ldots, \theta_r := u_r\beta_r\}$ d'éléments de L^+ tels que $L^+(\sqrt{\theta_i})$ est ramifiée uniquement en les idéaux premiers divisant $\mathfrak{r}\mathcal{O}_{L^+}$ et en les places infinies contenues S_∞. L'une des extensions $L^+(\sqrt{\theta_i})$ est l'extension L_1. Puisque que l'on sait à présent que ces extensions ont la bonne ramification, on regarde lesquelles sont abéliennes sur k.

Soit θ un des éléments candidats ; on commence par regarder si l'extension construite est bien galoisienne. Notons que l'on connait explicitement les k-automorphismes de L^+ (*cf* Chapitre 1). Les conditions à vérifier pour que l'extension soit galoisienne sont celles du lemme 2.12. Supposons qu'elle soient vérifiées ; on pose pour $\sigma \in G^+$:

$$\sigma(\theta) = \theta\gamma_\sigma^2$$

avec $\gamma_\sigma \in L^+$. Pour $\sigma \in G^+$, notons $\bar{\sigma}$ un prolongement arbitraire de σ à G. L'égalité précédente donne donc :

$$\bar{\sigma}(\sqrt{\theta}) = \pm\sqrt{\theta}\gamma_\sigma,$$

et on choisit γ_σ de telle sorte que le signe devant le membre de droite soit $+$.

On note τ l'automorphisme non trivial de l'extension quadratique $L^+(\sqrt{\theta})/L^+$. Alors, l'extension $L^+(\sqrt{\theta})/k$ est abélienne si et seulement si :

$$\begin{aligned} \text{pour tout } \sigma \in G^+,\ \tau\bar{\sigma}(\sqrt{\theta}) &= \bar{\sigma}\tau(\sqrt{\theta}), \\ \text{pour tout } \sigma, \nu \in G^+,\ \bar{\sigma}\bar{\nu}(\sqrt{\theta}) &= \bar{\nu}\bar{\sigma}(\sqrt{\theta}). \end{aligned}$$

La première condition est facilement vérifiée :

$$\tau\bar{\sigma}(\sqrt{\theta}) = \tau(\sqrt{\theta}\gamma_\sigma) = -\sqrt{\theta}\gamma_\sigma = \bar{\sigma}(-\sqrt{\theta}) = \bar{\sigma}\tau(\sqrt{\theta}).$$

Pour la seconde, on trouve :

$$\begin{aligned} \bar{\sigma}\bar{\nu}(\sqrt{\theta}) &= \bar{\sigma}(\sqrt{\theta}\gamma_\nu) = \sqrt{\theta}\gamma_\sigma\sigma(\gamma_\nu), \\ \text{et } \bar{\nu}\bar{\sigma}(\sqrt{\theta}) &= \bar{\nu}(\sqrt{\theta}\gamma_\sigma) = \sqrt{\theta}\gamma_\nu\sigma(\gamma_\sigma)\ ; \end{aligned}$$

d'où le lemme :

Lemme 2.23. *L'extension $L^+(\sqrt{\theta})/k$ est abélienne si et seulement si on a :*

$$\gamma_\sigma\sigma(\gamma_\nu) = \gamma_\nu\nu(\gamma_\sigma)$$

pour tout $\sigma, \nu \in G^+$.

Une fois montré que l'extension $L^+(\sqrt{\theta})/k$ est abélienne, il suffit pour prouver que $L^+(\sqrt{\theta}) = L_1$ de montrer que ces deux extensions ont le même sous-groupe de congruence modulo $\mathfrak{f}$, et ceci est une application directe de l'algorithme 2.15.

Il est ainsi possible de construire l'extension L_1 en suivant la méthode expliquée ci-dessus et donc, en appliquant cette construction aux autres extensions L_i/L^+, de construire le corps de classes de rayon $k(\mathfrak{f})$ à partir de son sous-corps réel $k(\mathfrak{f}_0)$.

2.7. Sur l'existence du corps K

Nous terminons ce chapitre en discutant de l'existence d'une extension quadratique de L vérifiant les conditions (a-c). Dans un premier temps, on va considérer le cas où l'on peut construire K en composant $L := k(\mathfrak{f})$ avec une extension quadratique k' de k.

On commence par regarder ce qui se passe localement :

Proposition 2.24. *Soit F une extension de $\mathbb{Q}_p$ de degré m.*
Alors on a :

- $r_2(F^\times) = 2$ *si p est impair*
- $r_2(F^\times) = m + 2$ *si $p = 2$.*

Démonstration : La structure multiplicative de F est la suivante :

$$F^\times = \mu_F \, \mathcal{U}_F^{(1)} \, \pi_F^{\mathbb{Z}}$$

où μ_F est le groupe des racines de l'unité d'ordre premier à p contenues dans F ; c'est un groupe cyclique d'ordre $\mathcal{N}\mathfrak{p}_F - 1$ (où $\mathfrak{p}_F$ désigne l'idéal premier de F) ; $\mathcal{U}_F^{(1)}$ est le groupe des unités principales de F, *ie* les unités congrues à 1 modulo $\mathfrak{p}_F$; c'est un $\mathbb{Z}_p$-module de rang m dont le sous-groupe de torsion est un groupe cyclique fini ; π_F est une uniformisante en $\mathfrak{p}_F$ (*cf* [**47**]).

On considère chaque composante de cette décomposition. On note C_2 le groupe cyclique d'ordre 2.

• Structure de μ_F/μ_F^2 : si $p = 2$, on obtient $\mu_F^2 = \mu_F$ puisque l'ordre de ce groupe est premier à 2, et ce quotient est donc trivial ; sinon, 2 divise l'ordre de μ_F et c'est un groupe cyclique d'où le quotient est isomorphe à C_2 .

• Structure de $\mathcal{U}_F^{(1)}/(\mathcal{U}_F^{(1)})^2$: si $p = 2$, la partie libre du groupe des unités principales donne un quotient isomorphe à C_2^m et la partie de torsion qui est cyclique et non vide (elle contient -1) donne un quotient isomorphe à C_2, d'où le quotient recherché est isomorphe à C_2^{m+1} ; dans le cas où p est impair, on obtient $(\mathcal{U}_F^{(1)})^2 = \mathcal{U}_F^{(1)}$ puisque 2 est inversible dans $\mathbb{Z}_p$ et donc un quotient trivial.

• Structure de $\pi_F^{\mathbb{Z}}/\pi_F^{2\mathbb{Z}}$: dans tous les cas, ce quotient est isomorphe à C_2.

En rassemblant tous ces résultats, on obtient que le 2-rang de $F^\times$ est 2 si p est impair et $m + 2$ si $p = 2$. □

Corollaire 2.25. *Avec les notations de la proposition précédente, le nombre d'extensions quadratiques de F est :*

- 3 *si p est impair,*
- $2^{m+2} - 1$ *si p est pair.*

Démonstration : Par la théorie de Kummer, les extensions quadratiques de F sont en bijection avec les sous-groupes d'indice 2 de $F^\times$. Or, on sait qu'il y a $2^r - 1$ sous-groupes d'indice 2 dans un groupe abélien dont le 2-rang est r. □

Soit $\mathfrak{p}$ un idéal premier divisant $\mathfrak{f}$, on note $D_\mathfrak{p}$ le groupe de décomposition de $\mathfrak{p}$ dans L/k. On a :

$$\begin{aligned} r_2(D_\mathfrak{p}) &\leq 2 \text{ si } \mathfrak{p} \nmid 2, \\ r_2(D_\mathfrak{p}) &\leq n_\mathfrak{p} + 2 \text{ si } \mathfrak{p} \mid 2, \end{aligned}$$

où $n_\mathfrak{p} := [k_\mathfrak{p} : \mathbb{Q}_p]$, puisque par la théorie du corps de classes, ce groupe est isomorphe à un sous-groupe d'indice fini de $k_\mathfrak{p}^\times$. Le nombre d'extensions quadratiques de $k_\mathfrak{p}$ contenues dans $L_\mathfrak{P}$ (pour $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$) est :

$$2^{r_2(D_\mathfrak{p})} - 1.$$

Théorème 2.26. *Il existe une extension quadratique k' de k telle que $K = Lk'$ vérifie les conditions (a-c) si et seulement si pour tout idéal premier $\mathfrak{p}$ divisant $\mathfrak{f}$ on a :*

$$\begin{aligned} r_2(D_\mathfrak{p}) &< 2 \text{ si } \mathfrak{p} \nmid 2, \\ r_2(D_\mathfrak{p}) &< n_\mathfrak{p} + 2 \text{ si } \mathfrak{p} \mid 2. \end{aligned}$$

Démonstration : Soit $\mathfrak{p}$ un idéal premier divisant $\mathfrak{f}$, on note $\mathfrak{P}$ un idéal premier de L fixé au-dessus de $\mathfrak{p}$.

Supposons pour commencer qu'on ait égalité, *ie* que $r_2(D_\mathfrak{p}) = 2$ si $\mathfrak{p} \nmid 2$ ou $r_2(D_\mathfrak{p}) = n_\mathfrak{p} + 2$ si $\mathfrak{p} \mid 2$. Alors, toutes les extensions quadratiques de $k_\mathfrak{p}$ sont contenues dans $L_\mathfrak{P}$. Ainsi, pour toute extension quadratique k' de k, l'extension locale $k'_{\mathfrak{p}'}$ est contenue dans $L_\mathfrak{P}$ et donc la composée des deux corps est $L_\mathfrak{P}$. Il s'ensuit que l'idéal premier $\mathfrak{P}$ est décomposé dans l'extension Lk'/L, ce qui contredit la condition (c). Les inégalités du théorème sont donc nécessaires à l'existence de l'extension k'.

On montre que ces inégalités sont suffisantes. Supposons qu'elles soient vérifiées. En vertu du corollaire 2.25, il existe pour tout $\mathfrak{p}$ divisant $\mathfrak{f}$, un élément $\eta_\mathfrak{p}$ de $k_\mathfrak{p}$ tel que l'extension $k_\mathfrak{p}(\sqrt{\eta_\mathfrak{p}})$ n'est pas incluse dans $L_\mathfrak{P}$, *ie* $\eta_\mathfrak{p}$ n'est pas un carré dans $L_\mathfrak{P}$. On fixe un tel $\eta_\mathfrak{p}$ pour tout $\mathfrak{p}$ et on pose $\varkappa_\mathfrak{p} = e_\mathfrak{p} \operatorname{Max}\{\operatorname{val}_\mathfrak{p}(\eta_\mathfrak{p}), 2\operatorname{val}_\mathfrak{p}(2)\}$, où $e_\mathfrak{p}$ est l'indice de ramification de $\mathfrak{p}$ dans L/k.

Par le théorème d'approximation, il existe un entier algébrique η de k tel que :

- $v_1(\eta) > 0$ et $v_i(\eta) < 0$ pour $2 \leq i \leq N$,
- $\eta \equiv \eta_\mathfrak{p} \pmod{\mathfrak{p}^{\varkappa_\mathfrak{p}+1}}$ pour tout $\mathfrak{p} \mid \mathfrak{f}$.

On affirme alors que l'extension $k' := k(\sqrt{\eta})$ convient. En effet, posons $K := Lk'$; l'extension K/k est abélienne, puisque K est la composée de deux extensions abéliennes de k ; donc la condition (a) est vérifiée.

Par le choix de la signature de η, la place v_1 est totalement décomposée dans l'extension k'/k, les autres places infinies étant ramifiées. En composant avec L, ces propriétés se transmettent à l'extension K/L, ce qui assure la condition (b).

Pour la condition (c), on suppose qu'il existe un idéal premier $\mathfrak{p}$ de k tel que tout idéal $\mathfrak{P}$ de L au-dessus de $\mathfrak{p}$ est décomposé dans K/L. Il s'ensuit que η est un carré dans $L_\mathfrak{P}$, puisque $K = L(\sqrt{\eta})$ et que $\eta_\mathfrak{p}$ est congru à un carré modulo $\mathfrak{P}^{\varkappa_\mathfrak{p}+1}$. On utilise le lemme de Hensel (*cf* théorème 1.14 du chapitre 1) appliqué au corps $L_\mathfrak{P}$, au polynôme $X^2 - \eta_\mathfrak{p}$ et à l'exposant $\varkappa_\mathfrak{p}$.

On trouve que ce polynôme admet une racine simple modulo $\mathfrak{P}^{\varkappa_\mathfrak{p}+1}$ puisque $\eta_\mathfrak{p} \not\equiv 0 \pmod{\mathfrak{P}^{\varkappa_\mathfrak{p}+1}}$ et aussi $2 \not\equiv 0 \pmod{\mathfrak{P}^{\varkappa_\mathfrak{p}+1}}$. Il s'ensuit par le théorème qu'il existe une racine carrée de $\eta_\mathfrak{p}$ dans $L_\mathfrak{P}$, ce qui contredit l'hypothèse de départ.

Ainsi, tous les idéaux premiers divisant $\mathfrak{f}$ sont ramifiés ou inertes dans K/L ce qui donne la condition (c). □

Remarque : Il existe un grand nombre de cas où les hypothèses du théorème 2.26 sont vérifiées. Par exemple, si 4 ne divise pas le nombre de classes $h_k(\mathfrak{f})$ ou si, pour tout idéal premier $\mathfrak{p}$ divisant $\mathfrak{f}$, l'indice de ramification ou le degré résiduel de $\mathfrak{p}$ dans L/k n'est pas divisible par 2.

Cependant, si les conditions du théorème 2.26 ne sont pas vérifiées, il est impossible de ramener le problème de la construction de K à un problème sur k. La construction est donc beaucoup plus difficile.

Localement, cependant, le problème est facilement résolu, *ie* étant donnée E/F une extension ramifiée de $\mathbb{Q}_p$, on sait construire une extension quadratique de E qui est abélienne sur F. Une méthode est la suivante : soit $\mathcal{N}$ le groupe des normes de E sur F, de telle sorte que, par la théorie locale du corps de classes on ait :

$$\operatorname{Gal}(E/F) \cong F^\times/\mathcal{N}.$$

Notons f le plus petit entier positif tel que $\pi_F^f \in \mathcal{N}$; f est le degré résiduel de l'idéal premier $\mathfrak{p}_F$ dans E/F ; soit $\mathcal{U}_\mathcal{N}$ l'intersection de $\mathcal{N}$ avec le groupe des unités de F. On pose :

$$\mathcal{N}' := \mathcal{U}_\mathcal{N} \pi_F^{2f},$$

soit enfin E' l'extension correspondant à $\mathcal{N}'$ par la théorie du corps de classes.

Alors on a $E \subset E'$, puisque $\mathcal{N}' \subset \mathcal{N}$, et $[E' : E] = 2$ puisque $(\mathcal{N}' : \mathcal{N}) = 2$. De plus, E'/F est abélienne par construction. On a donc construit une solution locale. Le problème est qu'il n'y a pas de moyen à ma connaissance pour passer du local au global. En fait, il existe un résultat fondamental (*cf* [**42**] cor. 2 §3) :

Théorème 2.27 (Neukirch)**.** *Soit F un corps de nombres ; on note w le cardinal de W_F, ie le nombre de racines de l'unité contenues dans F, et S un ensemble fini d'idéaux premiers de F.*

Soit G un groupe pro-résoluble d'exposant fini premier avec w et pour $\mathfrak{p} \in S$, soient $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ des extensions locales dont les groupes de Galois $G_{\mathfrak{p}}$ se plongent dans G.

Alors, il existe une extension galoisienne E/F de groupe de Galois isomorphe à G dont la complétion est l'extension $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ pour tout $\mathfrak{p} \in S$. □

Malheureusement, ce théorème exclut le cas où l'exposant de G est pair (et c'est le cas qui nous intéresse) ; et cette hypothèse est capitale pour la démonstration du théorème.

Il ne semble donc pas possible de conclure sur l'existence du corps K dans le cas où les hypothèses du théorème 2.26 ne sont pas vérifiées.

On note pour terminer, que, vu la complexité des calculs dans ce cas (on doit avoir $4 \mid h_k(\mathfrak{f})$), il n'a pas été possible de procéder à des calculs intensifs sur différents exemples pour en déduire une quelconque indication algorithmique sur la validité du résultat.

Néanmoins, à chaque essai, on a toujours réussi à construire un corps K convenable.

CHAPITRE 3

CONSTRUCTION DES CORPS DE CLASSES DE HILBERT DES CORPS TOTALEMENT RÉELS

Dans ce chapitre, on applique la procédure de construction expliquée dans le chapitre précédent pour construire le corps de classes de Hilbert de corps totalement réels quadratiques, cubiques et quartiques. En fait, lorsque le nombre de classes est égal à 2, on a effectué cette construction en utilisant la théorie de Kummer, et on a utilisé la méthode dérivée des conjectures de Stark uniquement quand le nombre de classes est strictement plus grand que 2. On a bien sûr démontré l'exactitude du résultat dans tous les cas.

Les tables, données en appendice, s'étendent jusqu'au discriminant 2000 pour les corps quadratiques (288 corps), 100000 pour les corps cubiques (612 corps) et 500000 pour les corps quartiques (391 corps). Les nombres de classes à considérer vont de 2 à respectivement 11, 9 et 4 pour chaque degré.

Les tables de corps de nombres utilisées sont celles disponibles à l'adresse :

`ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`

et tous les calculs ont été effectués en utilisant la librairie de fonctions du système PARI. Des calculs similaires du corps de classes de Hilbert de certains corps par la méthode de Kummer sont décrits dans [**15**].

3.1. Construction dans le cas $h_k = 2$

La méthode utilisée s'inspire de la construction décrite dans la section 2.6. Elle repose essentiellement sur les théorèmes 2.19 et 2.20. Il est bien sûr possible de construire dans ce cas aussi le corps de classes de Hilbert par la méthode utilisant la conjecture de Stark et décrite dans la section suivante (on n'utilise d'ailleurs nulle part l'hypothèse que $h_k \geq 3$ dans cette section) ; cependant, la construction par la théorie de Kummer étant particulièrement simple, on a jugé préférable de l'utiliser.

Soit k un corps de nombres de nombre de classes $h_k = 2$. On note $\mathfrak{a}$ un idéal entier non principal de k ne divisant pas 2 ; en particulier, la classe $[\mathfrak{a}]$ de cet idéal engendre le groupe de classes de k. On fixe un générateur α de l'idéal principal $\mathfrak{a}^2$. On note également $\eta_0, \ldots, \eta_r$ un système d'unités fondamentales de k où η_0 est un générateur du sous-groupe de torsion et r est le rang des unités de k. Le résultat suivant est un corollaire direct du théorème 2.20 :

Proposition 3.1. *Il existe un unique vecteur* $(a, e_0, \ldots, e_r) \in \{0,1\}^{(r+2)}$ *tel que la racine carrée de :*

$$\theta := \alpha^a \prod_{i=0}^{r} \eta_i^{e_i}$$

engendre le corps de classes de Hilbert de k*, ie* $H_k = k(\sqrt{\theta})$*.*

Démonstration : On commence par démontrer l'existence. Par le théorème 2.19, on sait qu'il existe un élément β de k tel que $H_k = k(\sqrt{\beta})$. De plus, en appliquant le théorème 2.20, on peut choisir cet élément premier avec 2 ; l'idéal principal engendré par β est le carré d'un idéal $\mathfrak{b}$ puisque l'extension H_k/k est non ramifiée.

On distingue deux cas. Si l'idéal $\mathfrak{b}$ est principal engendré par $\gamma \in k$, alors l'élément $u := \beta\gamma^{-2}$ est une unité de k et sa racine carrée engendre H_k sur k. Multiplier cette unité u par un élément de E_k^2 ne change pas l'extension ; donc il existe un vecteur vérifiant l'énoncé du théorème (avec $a = 0$), puisqu'on peut choisir comme système de représentants de E_k/E_k^2 le 2-groupe engendré par les classes des unités η_i.

Si l'idéal $\mathfrak{b}$ n'est pas principal, alors il existe un élément $\gamma \in k$ tel que $\mathfrak{b} = \gamma\mathfrak{a}$ (puisque le groupe de classes de k est d'ordre 2 et engendré par la classe de $\mathfrak{a}$). Dans ce cas, on trouve :

$$\beta\mathcal{O}_k = \mathfrak{b}^2 = \gamma^2\alpha\mathcal{O}_k,$$

et donc il existe une unité u telle que β et $u\alpha$ ne diffèrent que d'un carré et définissent la même extension quadratique de k. Le choix de l'unité se faisant modulo E_k^2, on obtient le résultat avec cette fois-ci $a = 1$.

On montre l'unicité. Supposons qu'il existe $(a', e_0', \ldots, e_r') \in \{0,1\}^{(r+2)}$ tel que $H_k = k(\sqrt{\theta'})$ avec $\theta' := \alpha^{a'}\prod_i \eta_i^{e_i'}$. Puisque $k(\sqrt{\theta}) = k(\sqrt{\theta'})$, il existe un élément $\gamma \in k$ tel que $\theta' = \gamma^2\theta$. Si on passe aux idéaux, on trouve :

$$\theta'\mathcal{O}_k = \mathfrak{a}^{2a'} = \gamma^2\theta\mathcal{O}_k = (\gamma)^2\mathfrak{a}^{2a},$$

d'où $\mathfrak{a}^a = \gamma\mathfrak{a}^{a'}$, puis $[\mathfrak{a}]^a = [\mathfrak{a}]^{a'}$. Mais ceci implique que $a \equiv a' \pmod 2$, puisque $[\mathfrak{a}]$ est d'ordre 2 et donc, $a = a'$ car $a, a' \in \{0,1\}$.

On peut à présent supposer que γ est une unité. On écrit :

$$\gamma = \prod_{i=0}^{r} \eta_i^{g_i}.$$

Il s'ensuit que $e_0' = e_0 + 2g_0 \pmod{w_k}$ et $e_i' = e_i + 2g_i$ pour $1 \le i \le r$ (w_k est l'ordre du sous-groupe de torsion des unités). On en déduit que $e_i' = e_i$ et $g_i = 0$ pour $1 \le i \le r$ (toujours parce que $e_i, e_i' \in \{0,1\}$), mais aussi que $g_0 = 0$ et $e_0 = e_0'$ car 2 divise w_k. Ainsi, on a montré que $\gamma = 1$ et que $(a, e_0, \ldots, e_r) = (a', e_0', \ldots, e_r')$, ce qui achève la démonstration. □

La détermination d'un vecteur convenable peut se faire par recherche exhaustive en testant les $2^{r+2} - 1$ possibilités (le vecteur trivial, avec uniquement des zéros donnant l'élément 1 qui ne convient pas), ou bien en utilisant les méthodes de [**11**] qui consistent à regarder les conditions supplémentaires du théorème 2.20 aux places infinies et aux places au-dessus de 2.

Le corps H_k étant l'unique extension quadratique de k non ramifiée (puisque toute extension quadratique est abélienne), il suffit de trouver un élément θ par l'une ou l'autre méthode, donnant une extension quadratique non ramifiée de k, pour obtenir le corps de classes de Hilbert de k. Il n'y a donc pas de problème de vérification dans ce cas-là.

3.2. Construction dans le cas $h_k \ge 3$

Cette section renvoie directement aux sections 2 et 3 du chapitre précédent. Son but est de montrer comment l'hypothèse que le corps à construire est le corps de classes de Hilbert simplifie certaines parties de la méthode. On reprend l'ensemble des notations du chapitre 2, le corps à construire n'est plus noté L, mais plutôt H_k.

La première simplification concerne la construction d'un corps K convenable.

Lemme 3.2. *Soit α un élément de k tel qu' il existe une place infinie v_1 de k avec $v_1(\alpha) > 0$ et $v_i(\alpha) < 0$ pour $2 \le i \le N$.*

Alors, le corps $K := H_k(\sqrt{\alpha})$ vérifie les conditions (a-c) de la section 2.2.

Démonstration : On commence par remarquer que α n'est pas un carré dans H_k puisque c'est un corps totalement réel et $v_2(\alpha) < 0$. Donc l'extension K/H_k est bien de degré 2.

Ensuite, c'est une extension abélienne de k puisque K est la composée des deux extensions abéliennes H_k/k et $k(\sqrt{\alpha})/k$. Par les conditions imposées aux places infinies de k, la place v_1 est totalement décomposée dans K/k tandis que toutes les autres places infinies se ramifient dans K/H_k.

Maintenant, la dernière condition concernant les idéaux premiers qui se ramifient dans H_k/k est trivialement vérifiée puisque aucun idéal de k n'est ramifié dans H_k/k. □

Néanmoins, si la détermination d'un élément α vérifiant les hypothèses du lemme est très facile et peut être utilisée pour obtenir le corps K, il est préférable de procéder plutôt comme indiqué dans le chapitre 2. C'est à dire déterminer l'extension quadratique de k avec les conditions aux places infinies voulues et de conducteur minimal pour la norme, afin de réduire la complexité des calculs.

En effet, tous les calculs ont montré que pour un conducteur de taille réduite, disons dans le cas cubique qui est le plus parlant, de norme plus petite que 10, les calculs prennent quelques minutes au plus ; tandis que pour des conducteurs plus gros (jusqu'à 64, voir proposition 3.3 plus loin) les calculs peuvent prendre plusieurs heures. La taille du nombre de classes n'intervient en fait que très peu (les corps de classes de Hilbert pour les corps de nombres de classes 6, 7, 8 et 9 ont été calculés beaucoup plus facilement que pour certains corps de nombre de classes 3).

Ainsi, il est peut être intéressant de s'arrêter un instant pour voir quelles bornes on peut donner pour cette norme minimale.

Supposons que k soit un corps quadratique réel d'unité fondamentale u. Alors, si la norme de u est -1, il existe une place infinie v_1 de k telle que $v_1(u) > 0$, et pour l'autre place v_2 on a $v_2(u) < 0$. Ainsi, on peut choisir cette unité u pour construire le corps K en posant $K := H_k(\sqrt{u})$. En particulier, la norme du conducteur minimal est ≤ 16 puisque le conducteur de $H_k(\sqrt{u})/k$ divise $4\mathcal{O}_k$.

Quand k est un corps cubique, les choses se passent encore mieux. En effet, on a une majoration similaire toujours valide.

Proposition 3.3. *Soit k un corps cubique totalement réel.*

Alors, il existe une extension quadratique K de H_k telle qu'une seule place infinie reste réelle dans K tandis que les deux autres places deviennent complexes. De plus, le conducteur de K/k est de norme inférieure à :

$$4^3 = 64.$$

Démonstration : Cette démonstration est dûe à D. Hayes.

On commence par fixer un certain nombre de notations. On note Γ le groupe de Galois de H_k/k et Γ^+ le groupe de Galois de H_k^+/k où H_k^+ est le corps de classes au sens strict, *ie* on permet de la ramification aux places infinies dans H_k^+/k mais pas dans H_k/k. Pour v_i une place infinie (réelle) de k, on note c_i un générateur de son groupe de décomposition dans Γ^+ qu'on appelle la conjugaison complexe en v_i (le groupe de décomposition de v_i est d'ordre 1 ou 2 suivant que cette place reste réelle ou devienne complexe dans H_k^+/k).

On note $\mathfrak{S}$ l'application qui envoie un élément $\alpha \in k^\times$ sur le vecteur $(a_1, a_2, a_3) \in {\mathbb{F}_2}^3$ avec $a_i = 0$ si $v_i(\alpha) > 0$ et $a_i = 1$ sinon. En particulier, l'image de -1 est le vecteur $\mathbf{1} := (1, 1, 1)$. On note $\mathbf{E}$ l'image du groupe des unités par $\mathfrak{S}$, *ie* $\mathbf{E} := \mathfrak{S}(E_k)$. On désigne par $\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}$ la base canonique de ${\mathbb{F}_2}^3$ (*ie* la base formée des colonnes de la matrice identité 3×3), et par ψ l'application qui envoie le vecteur $\mathbf{e_i}$ sur la conjugaison c_i. On note $\Gamma_\infty := \mathrm{Gal}(H_k^+/H_k)$; par la théorie du corps de classes (*cf* [**43**]), le noyau de ψ est $\mathbf{E}$ et donc $\Gamma_\infty \cong {\mathbb{F}_2}^3/\mathbf{E}$.

Le $\mathbb{F}_2$-espace vectoriel ${\mathbb{F}_2}^3$ est muni du produit scalaire classique :

$$\mathbf{a}.\mathbf{b} = (a_1, a_2, a_3).(b_1, b_2, b_3) := a_1b_1 + a_2b_2 + a_3b_3.$$

On note $\mathbf{E}_0$ l'ensemble des éléments de $\mathbf{u} \in \mathbf{E}$ tels que $\mathbf{u}.\mathbf{1} = 0$. On a la décomposition :

$$\mathbf{E} = \mathbf{E}_0 \oplus \mathbb{F}_2\mathbf{1}.$$

Supposons pour commencer que $\dim \mathbf{E} = 1$ ou 2. Alors, la dimension de $\mathbf{E}_0$ est 0 ou 1. En particulier, soit $\mathbf{u}$ un vecteur engendrant $\mathbf{E}_0$ (ou $\mathbf{u} = \mathbf{0}$ si $\dim \mathbf{E}_0 = 0$), il existe un indice i tel que $u_i = 0$ (on utilise le fait que $\mathbf{u}.\mathbf{1} = 0$ et que $\mathbf{u}$ a trois composantes). Sans perte de généralité, on peut supposer que $i = 1$ et donc le vecteur $\mathbf{e_1}$ appartient au dual de $\mathbf{E}$. On définit à présent la forme linéaire ϕ de ${\mathbb{F}_2}^3$ dans $\mathbb{F}_2$ de la manière suivante :

$$\phi(e_1) := 0 \quad \text{et} \quad \phi(e_2) = \phi(e_3) := 1.$$

Si $\phi(\mathbf{u}) \neq 0$, alors on doit avoir $\mathbf{u} = \mathbf{e_2}$ ou $\mathbf{e_3}$, disons $\mathbf{E}_2$. Mais, dans ce cas, pour une unité u de k telle que $\mathfrak{S}(-u) = \mathbf{e_2}$, on a $v_2(u) > 0$, $v_1(u) < 0$ et $v_3(u) < 0$; on pose $K := H_k(\sqrt{u})$ et le résultat est démontré. Notons que le conducteur de K/k divise $4\mathcal{O}_k$ qui est de norme 64.

Sinon, *ie* $\phi(\mathbf{u}) = 0$, on a $\mathbf{E} \subset \mathrm{Ker}\ \phi$ et soit K le sous-corps de H_k^+ fixé par $\Delta := \psi(\mathrm{Ker}\ \phi)$. Alors, le corps K convient.

En effet, il est clair que $\Delta \cap \Gamma = \{1\}$ et donc $H_k \subset K$. Ensuite, en regardant l'image inverse de ψ, on trouve que l'indice de Δ dans Γ_∞ est égal au cardinal de ${\mathbb{F}_2}^3/\mathrm{Ker}\ \phi$ et ce cardinal vaut 2 car le noyau de ϕ est un hyper-plan. Donc K est une extension quadratique de H_k. Maintenant, la conjugaison c_1 agit trivialement sur K puisque $\mathbf{e_1} \in \mathrm{Ker}\ \phi$ et donc $c_1 \in \Delta$. A l'inverse, les vecteurs $\mathbf{e_2}$ et $\mathbf{e_3}$ ne sont pas dans ce noyau, donc ils ont une action non triviale sur K. La place réelle v_1 reste donc réelle dans K tandis que les places v_2 et v_3 deviennent complexes. Le corps K convient ; on remarque que le conducteur de K/k est de norme 1 puisque le corps K est un sous-corps de H_k^+.

Supposons pour terminer que $\dim \mathbf{E} = 2$ ou 3. Alors, on affirme qu'il existe un indice i tel que $\mathbf{e_i}$ appartiennent à $\mathbf{E}$. Ceci implique qu'il existe une unité u tel que $\mathfrak{S}(-u) = \mathbf{e_i}$ et il suffit alors de prendre $K := H_k(\sqrt{u})$ comme ci-dessus.

On montre donc cette affirmation. Puisque la dimension de $\mathbf{E}$ est au moins de 2, son dual contient au plus un vecteur non nul, disons $\mathbf{s}$. On note que $\mathbf{s} \neq \mathbf{1}$ puisque $\mathbf{1}.\mathbf{1} = 1$ et $\mathbf{1} \in \mathbf{E}$. Ainsi, il existe au moins un indice i tel que $s_i = 0$ et donc $\mathbf{e_i}$ appartient au dual du dual de $\mathbf{E}$, *ie* à $\mathbf{E}$ lui-même. □

Remarques :

- On note pour commencer que dans le cas où $K \subset H_k^+$, ce corps n'est pas *a priori* constructible par la méthode donnée dans le lemme 3.2. Dans les autres cas, la borne 4^3 est souvent bien supérieure à la norme effectivement trouvée, mais elle est cependant la meilleure possible (elle est atteinte par exemple pour le cas $X^3 - X^2 - 54X + 169$). Il est possible de prouver un résultat similaire pour le degré 5 avec une borne de 4^5.
- Dans le cas où le degré est pair, il n'y a pas de réponse immédiate. Cependant, on peut démontrer que le conducteur de K/k n'est pas de norme 1, *ie* K n'est pas inclus dans H_k^+/k.

Une fois connu le corps K par son conducteur $\mathfrak{m}$ et son groupe de congruence $\mathcal{H}$ modulo $\mathfrak{m}$, on s'intéresse aux caractères χ de $G := \mathrm{Gal}(K/k)$ tels que $\chi(\tau) \neq 1$ où τ est toujours l'élément non trivial de $\mathrm{Gal}(K/H_k)$. Dans le cas général, il est parfois nécessaire de calculer un facteur correctif $A(\chi)$; dans le cas non ramifié, un tel problème ne se pose pas.

Lemme 3.4. *Soit χ un caractère de G tel que $\chi(\tau) \neq 1$.*
Alors, le conducteur de χ est $\mathfrak{m}$; en particulier, le facteur correctif $A(\chi)$ vaut 1.

Démonstration : Le corps fixe K_χ de χ est une extension non triviale de k qui n'est pas un sous-corps de H_k. Donc la composée $K_\chi H_k$ est le corps K lui-même ; ainsi, le conducteur de K/k divise le conducteur de K_χ. Ceci montre que les deux conducteurs sont égaux puisque $K_\chi \subset K$. Le deuxième point est une conséquence directe du premier et de la définition de $A(\chi)$. □

La dernière simplification concerne le calcul de la constante d'Artin $W(\chi)$:

Lemme 3.5. *Soit ψ un caractère de G tel que $\psi(\tau) = -1$.*
Alors, pour tout caractère χ de G tel que $\chi(\tau) = -1$, la constante d'Artin vaut :

$$W(\chi) = \widetilde{\overline{\psi}\chi}(\mathcal{D}_k \mathfrak{m}_0) W(\psi),$$

où $\widetilde{\overline{\psi}\chi}$ est la restriction du caractère au groupe $\mathrm{Gal}(H_k/k)$ (c'est donc un caractère de Cl_k) et $\mathcal{D}_k$ est la différente de k. En particulier, si $K = H_k(\sqrt{\alpha})$ avec $\alpha \in k^\times$, on a :

$$W(\chi) = \tilde{\chi}(\mathcal{D}_k \mathfrak{m}_0).$$

Démonstration : On a $\overline{\psi}\chi(\tau) = 1$ donc le caractère $\overline{\psi}\chi$ est un caractère non ramifié. On applique le corollaire 2 de [**51**] §1 ; par la formule du passage local-global, on en déduit que :

$$W(\chi) = W(\psi\overline{\psi}\chi) = \widetilde{\overline{\psi}\chi}(\mathcal{D}_k \mathfrak{m}_0) W(\psi)$$

car le conducteur de χ est $\mathfrak{m}_0$ par le lemme 3.4. Ceci démontre le premier point.

Pour le second point, on observe que dans ce cas on peut décomposer $G :=< \tau > \times\Gamma$ où Γ s'identifie canoniquement au groupe de Galois de H_k/k. Ainsi, on peut choisir pour ψ le caractère définie par :

$$\psi(\tau) = -1 \text{ et } \psi(\gamma) = 1 \text{ pour tout } \gamma \in \Gamma.$$

Le caractère ψ est un caractère réel et donc, il s'ensuit par le théorème 1 de [**24**] que $W(\psi) = 1$; de plus, il est clair que $\tilde{\psi} = 1$, ce qui termine la démonstration. □

3.3. Vérification du résultat dans le cas $h_k \geq 3$

Tout comme pour la section précédente, cette section renvoie à la section 4 du chapitre 2. On explique comment dans cette construction, certaines parties peuvent être simplifiées.

Soit $P(X)$ un polynôme à coefficients dans $\mathcal{O}_k[X]$ et de degré h_k. On cherche à savoir si le corps $\tilde{H} := k(\theta)$, où θ est une racine de P, est le corps de classes de Hilbert de k.

On procède pour commencer de manière similaire à la section 2.4. On vérifie que le polynôme est séparable puis irréductible sur k ; puis, on calcule le discriminant relatif de l'extension $\tilde{H}/k$.

Une fois qu'on a vérifié que le corps $\tilde{H}$ a le même degré sur k que H_k et est non ramifié, il ne reste plus qu'à montrer que l'extension $\tilde{H}/k$ est abélienne. En effet, par la propriété de maximalité qui caractérise le corps de classes de Hilbert, on obtient alors que $\tilde{H} \subset H_k$ et donc $\tilde{H} = H_k$ puisqu'ils ont le même degré relatif sur k. Pour cela, on procède différemment suivant la valeur de h_k. (On utilise [**6**] pour la liste des groupes de Galois possibles).

- si $h_k = 3$, alors le groupe de Galois de la clôture galoisienne de $\tilde{H}/k$ est ou bien C_3 et l'extension est abélienne et le résulat est démontré, ou bien $S_3 \cong D_3$, le groupe diédral d'ordre 6 ; mais, dans ce dernier cas, l'extension k admet une extension de degré 2 non ramifiée car D_3 admet un quotient d'ordre 2, donc $2 \mid h_k$ ce qui est impossible.

Malheureusement, dès le degré 4, il n'est plus possible de raisonner ainsi. On commence donc par prouver que l'extension $\tilde{H}/k$ est galoisienne par la méthode du premier chapitre puis on procède différement suivant les valeurs de h_k.

- si $h_k = 4, 5, 7, 9$ ou 11, à chaque fois les groupes de Galois de degré et d'ordre h_k sont abéliens et donc $\tilde{H}/k$ est abélienne.
- si $h_k = 6$ ou 10, les groupes possibles sont respectivement C_6, D_3 et C_{10}, D_5. Le groupe de Galois de P est le groupe cyclique si et seulement si il existe un idéal premier $\mathfrak{p}$ ne divisant pas $\mathrm{disc}(P)$ tel que P soit irréductible modulo $\mathfrak{p}$. Or, la théorie du corps de classes affirme que si la classe de l'idéal $\mathfrak{p}$ engendre le groupe de classes, alors $\mathfrak{p}$ est inerte dans H_k/k. Ainsi, on choisit un tel idéal premier $\mathfrak{p}$ en supposant de plus qu'il ne divise pas $\mathrm{disc}(P)$. Alors, l'extension $\tilde{H}/k$ est le corps de classes de Hilbert de k si et seulement si P est irréductible modulo $\mathfrak{p}$.
- si $h_k = 8$, les groupes possibles sont $C_2^3, C_2 \times C_4, C_8$ (abéliens) et D_4, H_8 (non abéliens). Il n'est pas possible à ma connaissance de procéder dans ce cas comme pour les autres cas. On remarque que $|Z(D_4)| = |Z(H_8)| = 2$ et donc, il suffit de démontrer que le cardinal du centre du groupe $\mathrm{Gal}(\tilde{H}/k)$ est > 2 pour obtenir le résultat. Comme on connaît explicitement les k-automorphismes de $\tilde{H}$, on peut vérifier cette condition par des calculs directs.

3.4. Une méthode de réduction

A plusieurs reprises, on a mentionné le fait que la taille de l'unité de Stark avait tendance à croître très rapidement.

Par exemple, reprenons l'exemple cité ci-dessus : le corps cubique k totalement réel est défini par une racine θ du polynôme irréductible :

$$X^3 - X^2 - 54X + 169.$$

Ce corps a un nombre de classes égal à 4 et si on applique la construction, on obtient un conducteur de norme 64 (le maximum possible) et le polynôme relatif :

$$X^4 + (-3528046877492054726163414580801 6\theta^2 + 3231072356285186140529459350582 72\theta - 7308432148574394116104436839222 48)X^3 + (3046217551805694728073980669263830417745 92\theta^2 - 2789801174599694042854781415694641673213 5536\theta + 6310311359296404754192492302803645435213 496)X^2 + (-4679821092966341111255702936914740015282478 72\theta^2 + 4285895593482777790284983158372673319654896 128\theta - 9694359545960650320446173916968997346978477 472)X + (4832713481343022658115447713738163939403362329 6\theta^2 - 4425918214134996368776848771653215654712263860 48\theta + 1001107972720687523472338554868331152269024965 776).$$

Il est bien sûr impensable de laisser un tel polynôme pour décrire le corps de classes de Hilbert de k. On est donc amené à mettre au point une méthode de réduction.

En fait, la méthode de réduction qu'on va présenter ici n'est pas nouvelle, elle est tout simplement adaptée de la méthode POLRED de [**8**] section 4.4.2 (*cf* aussi [**10**]). Son intérêt est qu'elle est très efficace puisqu'elle permet de remplacer le polynôme précédent par le nouveau polynôme :

$$X^4 + (\theta - 8)X^2 + 1.$$

La méthode utilisée dans l'algorithme POLRED est la suivante : soit E un corps de nombres (le plus souvent E est défini comme un corps de rupture d'un polynôme irréductible à coefficients dans $\mathbb{Z}$). On commence par calculer son anneau des entiers $\mathcal{O}_E$, puis on considère la forme quadratique définie positive T_2 (*cf* chapitre 1, section 3) qui donne à cet anneau une structure de réseau. En particulier, pour toute constante $C > 0$, il existe un nombre fini d'entiers algébriques dont la T_2-norme est inférieure à C. L'algorithme POLRED consiste à chercher un élément primitif de $E/\mathbb{Q}$ dont la T_2-norme est petite (en effectuant par exemple une réduction LLL sur le réseau défini par $\mathcal{O}_E$) ou carrément minimale (en cherchant les entiers algébriques de petite norme par la méthode de [**19**]). Les propriétés de cette norme, notamment vis-à-vis des fonctions symétriques, permettent d'affirmer que le polynôme irréductible d'un élément de petite T_2-norme aura de (relativement) petits coefficients (*cf* [**8**] section 4.4.2 ou [**10**] pour plus de détails).

Le problème, si on cherche à généraliser cet algorithme au cas relatif, est que la notion de T_2-norme relative n'est pas vraiment satisfaisante. En fait, plusieurs choix sont possibles et sont présentés dans [**18**] qui généralise les résultats de l'algorithme LLL ([**37**]) et de l'algorithme de Fincke-Pohst ([**19**]) au cas relatif. Cependant, ils ne fournissent pas de résultats suffisamment réduits. La procédure utilisée va donc plutôt se ramener au cas absolu. Néanmoins, il est parfois bien utile de commencer par une première réduction suivant les méthodes de [**18**] pour diminuer un tant soit peu la taille du polynôme à réduire avant d'utiliser la méthode suivante.

Soit K/k une extension relative de corps de nombres définie par $K = k(\alpha)$ où α est une racine d'un polynôme unitaire et irréductible à coefficients dans $\mathcal{O}_k[X]$. On commence par calculer une pseudo-base de $\mathcal{O}_K$ comme $\mathcal{O}_k$-module (au sens de [**9**]) en utilisant par exemple l'algorithme ROUND 2 de [**12**] ou bien l'algorithme ROUND 4 relatif présenté dans le chapitre 1. On obtient :

$$\mathcal{O}_K = \bigoplus_{i=1}^{m} P_i(\alpha)\mathfrak{A}_i$$

où les $P_i(X)$ sont des polynômes de $\mathcal{O}_k[X]$ et les $\mathfrak{A}_i$ des idéaux fractionnaires de k. En particulier, on peut voir $\mathcal{O}_k$ et les idéaux $\mathfrak{A}_i$ comme des $\mathbb{Z}$-modules de rang $N := [k : \mathbb{Q}]$ et on peut en déduire l'écriture suivante :

$$\mathcal{O}_K = \bigoplus_{i=1}^{m}\bigoplus_{j=1}^{N} Q_{i,j}(\beta)\mathbb{Z}$$

où les $Q_{i,j}$ sont des polynômes à coefficients rationnels, et β est une combinaison linéaire à coefficients entiers $\beta := \alpha + t\theta$ (où $k = \mathbb{Q}(\theta)$) telle que $K = \mathbb{Q}(\beta)$ (un tel élément existe puisque $K = \mathbb{Q}(\theta, \alpha)$, *cf* [**34**] chap. V §4 th. 4.6). On obtient ainsi une base d'entiers de $K/\mathbb{Q}$. On aurait pu aussi calculer directement cette base d'entiers, mais cela suppose de travailler avec le polynôme irréductible de β sur $\mathbb{Q}$; or, vu la taille du polynôme relatif de α sur k, ce polynôme a de trop gros coefficients ; l'un des avantages des méthodes relatives est justement de rendre possible de tels calculs en les décomposant en des calculs relatifs plus simples.

Une fois connue cette base d'entiers, on peut lui appliquer la méthode usuelle : *ie* calculer la matrice donnée par l'application bilinéaire associée à la T_2-norme et rechercher les minima du réseau qu'elle définit. On note que dans notre cas la situation est simplifiée par le fait que les corps considérés sont tous totalement réels ; en effet, cette matrice est à coefficients entiers puisque l'application bilinéaire f associée à T_2 est donnée par :

$$f(x, y) = T_{K/\mathbb{Q}}(xy)$$

pour $x, y \in K$.

En considérant les entiers algébriques de K par T_2-norme croissante, on détermine le premier qui engendre K sur k en calculant son polynôme relatif caractéristique (ce polynôme est séparable si et seulement si l'élément est primitif) et on obtient ainsi le résultat escompté.

En fait, la méthode utilisée ici est très similaire à celle décrite dans [**10**], si ce n'est qu'elle tire partie des outils relatifs comme la réduction LLL relative, le calcul de pseudo-base ou les polynômes relatifs, pour simplifier des calculs qui seraient impossibles sinon.

La plupart des polynômes obtenus lors des calculs étant d'une taille comparable à celui présenté ci-dessus, on a pensé préférable (et plus utile) de ne pas les inclure dans les tables ; mais, au contraire, de les remplacer par les polynômes réduits calculés par cette méthode.

CHAPITRE 4

QUELQUES APPLICATIONS ET CONSTRUCTIONS PARTICULIÈRES

Dans ce dernier chapitre, on s'intéresse à diverses notions en relation avec le corps de classes de Hilbert ou les corps de classes de rayon. Certaines de ces notions donnent lieu à des constructions explicites grâce aux méthodes développées ; d'autres concernent des propriétés particulières qui sont apparues en examinant les tables obtenus. Ce chapitre n'a en aucun cas une prétention d'exhaustivité, mais donne plutôt un aperçu d'éventuelles applications des tables construites et données en annexes.

4.1. Extensions scindées de corps de classes

Soit E/F une extension de corps de nombres. On dit que l'extension est *scindée* s'il existe une extension F' de $\mathbb{Q}$ telle que :

$$F \cap F' = \mathbb{Q} \quad \text{et} \quad FF' = E.$$

Dans ce cas, on dit aussi que le corps F' *scinde* l'extension E/F. Il n'y a pas en général unicité du corps F' ; il est clair cependant qu'on a $[F' : \mathbb{Q}] = [F : E]$. Cette terminologie provient du cas où $F/\mathbb{Q}$ et $E/\mathbb{Q}$ sont des extensions galoisiennes ; l'extension E/F est alors scindée si et seulement si la suite exacte :

$$1 \longrightarrow \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(E/\mathbb{Q}) \longrightarrow \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow 1 \tag{4.1.30}$$

est scindée.

On a utilisé l'algorithme de recherche de sous-corps de [**32**] pour trouver lesquelles des extensions H_k/k calculées dans nos tables étaient scindées ; cela revient, en effet, à trouver un sous-corps k' de H_k de degré h_k sur $\mathbb{Q}$ et disjoint de k. Il est apparu que l'extension était très souvent scindée, et même, dans le cas quadratique, tous les exemples considérés ont donné des extensions scindées (*cf* théorème 4.2 ou proposition 4.3).

Plusieurs résultats ont été démontrés dans cette direction (*cf* [**14**]). Néanmoins, il s'avère vite nécessaire d'admettre que le corps k est galoisien afin de pouvoir tirer profit de la suite exacte 4.1.30.

Un autre axe de recherche est de ne plus supposer k galoisien, mais plutôt de regarder la plus grande extension abélienne $\tilde{k}/\mathbb{Q}$ telle que $k\tilde{k}/k$ soit non ramifiée. On dit alors que $k\tilde{k}$ est le *corps de classes de genre* de k. On ne s'intéressera pas à cette notion ici ; on renvoie à [**30**] pour un exposé complet de la théorie du corps de classes de genre.

On a le premier résultat :

Théorème 4.1. *Supposons que k est galoisienne de degré N et que $(N, h_k) = 1$.*
Alors, l'extension H_k/k est scindée.

Démonstration : Le corps H_k est galoisien sur $\mathbb{Q}$; en effet, notons H' un corps conjugué de H_k, alors k est un sous-corps de H' puisque $k/\mathbb{Q}$ est galoisien. De plus, l'extension H'/k est abélienne et non ramifiée car ces propriétés se transmettent aux corps conjugués. Il s'ensuit que $H' \subset H_k$ en vertu de la maximalité de H_k et donc $H' = H_k$ ce qui démontre cette assertion.

On obtient donc la suite exacte (transcription directe de 4.1.30) :

$$1 \longrightarrow \mathrm{Gal}(H_k/k) \longrightarrow \mathrm{Gal}(H_k/\mathbb{Q}) \longrightarrow \mathrm{Gal}(k/\mathbb{Q}) \longrightarrow 1$$

et cette suite est scindée car les groupes $\mathrm{Gal}(H_k/k)$ et $\mathrm{Gal}(k/\mathbb{Q})$ sont d'ordre premier entre eux par le théorème 6.16 de [**31**] (je remercie Y. Eichenlaub qui m'a indiqué ce résultat). □

On peut aussi démontrer un résultat dans le même sens sans avoir besoin de faire d'hypothèse sur le nombre de classes de k, mais seulement sur k (*cf* [**14**]) :

Théorème 4.2 (Wyman, Gold, Cornell, Rosen)**.** *Soit $k/\mathbb{Q}$ une extension cyclique.*
Alors, l'extension H_k/k est scindée.

En particulier, dans le cas quadratique, l'extension est toujours scindée. On peut aussi donner une démonstration élémentaire et directe de ce résultat si k est une extension cyclique de degré premier :

Proposition 4.3. *Soit $k/\mathbb{Q}$ une extension cyclique de degré premier l.*
Alors, l'extension H_k/k est scindée.

Démonstration : L'extension $H_k/\mathbb{Q}$ est galoisienne (*cf* la démonstration du théorème 4.1). On note $\Gamma := \mathrm{Gal}(H_k/\mathbb{Q})$, $G := \mathrm{Gal}(H_k/k)$ et τ un générateur de $\mathrm{Gal}(k/\mathbb{Q})$. Le groupe G s'identifie par l'application d'Artin au groupe Cl_k. Soit $\nu \in \Gamma \setminus G$, on note $H :=< \nu >$. On affirme que $H \cap G = \{1\}$.

En effet, on a $\Gamma = GH$ et $G|_k = \{1\}$, d'où il existe un nombre entier f ne divisant pas l'ordre de ν tel que $\tau = \nu^f|_k$. De plus, il existe un nombre premier p dont un Frobenius dans $H_k/\mathbb{Q}$ est ν par le théorème de Tchebotarev (*cf* [**43**] th. 6.4). Le Frobenius de p dans $k/\mathbb{Q}$ est non trivial puisque c'est la restriction de ν à k, et cette restriction est non triviale du fait que τ est la restriction d'une puissance de ν. Ainsi, l'unique idéal premier au-dessus de p dans k est principal et donc p est totalement décomposé dans H_k/k par la théorie du corps de classes ; donc aucune puissance de ν, si ce n'est la puissance triviale, ne peut appartenir à G. Ce qui prouve le résultat.

Puisque G et H sont disjoint, on a $|\Gamma| = |G| \times |H|$ d'où $|H| = l$ et ν est d'ordre l. Ceci démontre que l'extension de groupe :

$$1 \longrightarrow G \longrightarrow \Gamma \longrightarrow \langle \tau \rangle \longrightarrow 1$$

est scindée et donc l'extension H_k/k est scindée par le sous-corps de H_k fixe par ν. (Merci à D. Solomon.) □

Un corollaire amusant est le suivant :

Corollaire 4.4. *Il n'existe pas d'extension cyclique d'ordre un nombre premier impair et de nombre de classes 2.*

Démonstration : Supposons le contraire et notons k une telle extension et l son degré. Alors, l'extension H_k/k est scindée par une extension quadratique $\tilde{k}$. Comme composée des deux extensions abéliennes k et $\tilde{k}$, le corps H_k est une extension abélienne de $\mathbb{Q}$ de degré $2l$; en particulier, elle est cyclique.

Il existe donc un nombre premier p inerte dans $H_k/\mathbb{Q}$. Il est aussi inerte dans $k/\mathbb{Q}$, ce qui implique que l'unique idéal premier au-dessus de p dans k est principal et donc totalement décomposé dans H_k/k par la théorie du corps de classes. Mais, ceci fournit une contradiction. On peut trouver un résultat plus général dans le même sens dans [**56**] ex. 10.2. □

On considère à présent les résultats explicites obtenus par le calcul. Bien entendu, tous les corps quadratiques considérés admettent une extension scindée d'après le théorème 4.2 ; il n'y a donc pas grand chose à dire dans ce cas.

Pour les corps cubiques, on en trouve 194 qui admettent une extension de corps de classes de Hilbert scindée (soit 32%) et pour les corps quartiques, il y en a 178 (soit 44%). Dans tous les cas, il en existe beaucoup ne relevant pas de la situation des théorèmes 4.1 ou 4.2.

Un fait remarquable en degré 4 : plus de 100 corps de nombres de classes 2 admettent une extension de corps de classes de Hilbert scindée par le corps $\mathbb{Q}(\sqrt{5})$; cela répresente plus de 58% des corps quartiques de nombre de classes 2 dont l'extension de corps de Hilbert est scindée. En degré 3, on retrouve 43 fois le corps cyclique cubique de discriminant 81 ; il s'agit en fait du sous-corps réel maximal du neuvième corps cyclotomique. Le même corps $\mathbb{Q}(\sqrt{5})$ se retrouve également en degré 2 avec 48 occurences. Tous ces exemples sont en fait à relier avec la théorie du corps de classes de genre (*cf* [**30**]) puisque dans chacun des cas, le corps qui scinde l'extension est abélien sur $\mathbb{Q}$.

4.2. Classes de Steinitz de l'extension H_k/k

Soit k un corps de nombres ; on note $\mathcal{O}_k$ son anneau d'entiers. C'est un anneau de Dedekind et la théorie générale des anneaux de Dedekind (*cf* [**41**] par exemple) affirme que tout $\mathcal{O}_k$-module M de type fini et sans torsion admet l'isomorphisme (de $\mathcal{O}_k$-modules) :

$$M \simeq \bigoplus_{i=1}^{m-1} \mathcal{O}_k \oplus \mathfrak{a},$$

où $\mathfrak{a}$ est un idéal de k. On montre que la classe $[\mathfrak{a}]$ de l'idéal $\mathfrak{a}$ est un invariant du module M, on l'appelle la *classe de Steinitz* de M ; en particulier, le module M est $\mathcal{O}_k$-libre si et seulement si cette classe est la classe principale.

On s'intéresse maintenant au cas où $M := \mathcal{O}_{H_k}$, l'anneau des entiers du corps de classes de Hilbert de k ; soit $\mathcal{S}$ la classe de Steinitz de $\mathcal{O}_{H_k}$. La question est de savoir si ce $\mathcal{O}_k$-module est libre, *ie* quand est-ce que la classe $\mathcal{S}$ est la classe triviale. Une première réponse est immédiate :

Proposition 4.5. *Supposons h_k impair.*
Alors, $\mathcal{O}_{H_k}$ est un $\mathcal{O}_k$-module libre.

Démonstration : La classe $\mathcal{S}^2$ est la classe du discriminant de H_k/k. Or cette classe est la classe principale puisque $\mathfrak{d}_{H_k/k} = \mathcal{O}_k$. Le résultat s'ensuit en remarquant que pour h_k impair, il n'y a pas de classe d'ordre 2. □

Le fait que le discriminant de H_k/k soit trivial permet également de connaître directement la classe de Steitnitz $\mathcal{S}$ de $\mathcal{O}_{H_k}$ en calculant le discriminant d'un polynôme relatif définissant H_k. Plus exactement, on a :

Proposition 4.6. *Supposons que $H_k = k(\alpha)$ où α est racine du polynôme irréductible et unitaire $P(X) \in \mathcal{O}_k[X]$. Soit $\mathfrak{a}$ l'idéal principal engendré par le discriminant de P.*

Alors, l'idéal $\mathfrak{a}$ est le carré d'un idéal $\mathfrak{i}$ appartenant à la classe $\mathcal{S}$. En particulier, le module $\mathcal{O}_{H_k}$ est $\mathcal{O}_k$-libre si et seulement si l'idéal $\mathfrak{i}$ est principal.

Démonstration : L'ordre $\mathcal{O}_k[\alpha]$ est un sous-$\mathcal{O}_k$-module de $\mathcal{O}_{H_k}$; ainsi, il existe un idéal entier $\mathfrak{i}$ tel que $(\mathcal{O}_{H_k} : \mathcal{O}_k[\alpha]) = \mathfrak{i}$. On a alors :

$$\mathfrak{a} = \mathfrak{i}^2 \mathfrak{d}_{H_k/k},$$

et donc $\mathfrak{a} = \mathfrak{i}^2$ ce qui prouve que l'idéal $\mathfrak{a}$ est un carré. Pour finir, notons que l'idéal $\mathfrak{i}$ est dans la classe de $\mathcal{S}$ puisque la classe de Steinitz de $\mathcal{O}_{H_k}$ est obtenu en multipliant la classe de Steinitz du module libre $\mathcal{O}_k[\alpha]$ par la classe de $\mathfrak{i}$. □

Exemple : Soit $k := \mathbb{Q}(\sqrt{817})$. Le nombre de classes de k est 5 et son corps de classes de Hilbert est le corps $k(\theta)$ avec :

$$\theta^5 - 15\theta^3 + 44\theta + (2\sqrt{817} - 1) = 0.$$

Le discriminant du polynôme irréductible de θ sur k est :

$$94809169 = 9737^2,$$

donc $\mathcal{O}_{H_k}$ est un $\mathcal{O}_k$-module libre.

Supposons à présent que l'extension H_k/k est scindée par le corps $\tilde{k}$. Alors, on définit le $\mathcal{O}_k$-module M' comme le module engendré par les éléments de $\mathcal{O}_k$ et $\mathcal{O}_{\tilde{k}}$; on peut aussi écrire :

$$M' = \mathcal{O}_k \otimes_{\mathbb{Z}} \mathcal{O}_{\tilde{k}}.$$

M' est un sous-$\mathcal{O}_k$-module de $\mathcal{O}_{H_k}$ et, par les propriétés du produit tensoriel, l'indice de M' dans $\mathcal{O}_{H_k}$ est l'idéal entier $\mathfrak{i}$ tel que $\mathfrak{i}^2 = d_{\tilde{k}}\mathcal{O}_k$ (toujours grâce au fait que l'extension H_k/k est non ramifiée). On en déduit le résultat suivant :

Proposition 4.7. *Supposons que l'extension H_k/k est scindée et que tout idéal premier $\mathfrak{p}$ au-dessus d'un nombre premier p ramifié est principal.*

Alors, la classe de Steinitz $\mathcal{S}$ de $\mathcal{O}_{H_k}$ est la classe principale, autrement dit le $\mathcal{O}_k$-module $\mathcal{O}_{H_k}$ est libre.

Démonstration : Tout nombre premier divisant $d_{\tilde{k}}$ doit être ramifié dans $k/\mathbb{Q}$ et ainsi, tout idéal premier $\mathfrak{p}$ divisant $d_{\tilde{k}}\mathcal{O}_k$ est principal. D'où il s'ensuit que l'idéal $\mathfrak{i}$ (avec les notations ci-dessus) est principal, et donc, puisque M' est par construction un $\mathcal{O}_k$-module libre, on obtient que $\mathcal{O}_{H_k}$ est lui aussi libre. □

Exemple : Soit k le corps cubique cyclique de discriminant 163^2 et engendré sur $\mathbb{Q}$ par une racine θ du polynôme irréductible :

$$X^3 - X^2 - 54X + 169.$$

Il est de nombre de classes 4 et le seul nombre premier ramifié dans cette extension est 163 et il est totalement ramifié ; soit $\mathfrak{p}$ l'unique idéal premier au-dessus de 163 ; on trouve :

$$\mathfrak{p} = (\theta^2 + 2\theta - 37)\mathcal{O}_k.$$

On en déduit alors que le $\mathcal{O}_k$-module $\mathcal{O}_{H_k}$ est libre sans même avoir à calculer le corps de classes de Hilbert.

En utilisant un raisonnement analogue à cette démonstration et une connaissance explicite de quand et comment l'extension H_k/k est scindée, on peut donner une réponse exhaustive dans le cas le plus simple.

Proposition 4.8. *Soit $k := \mathbb{Q}(\sqrt{d})$ un corps quadratique réel de nombre de classes 2 où d est un entier positif sans facteur carré. Supposons qu'il existe un diviseur strict e de d (ie $e \neq 1, d$) tel que $e \equiv 1 \pmod 4$.*

Alors, il existe un idéal entier $\mathfrak{e}$ de k tel que :

$$\mathfrak{e}^2 = e\mathcal{O}_k$$

et la classe $\mathcal{S}$ est la classe de $\mathfrak{e}$. En particulier, le $\mathcal{O}_k$-module $\mathcal{O}_{H_k}$ est libre si et seulement si l'idéal $\mathfrak{e}$ est principal.

Démonstration : On va montrer que $H_k = k(\sqrt{e})$. On peut supposer sans perte de généralité que e est impair car $H_k = k(\sqrt{d/e})$ puisque $e \mid d$, et si 2 divise e alors 2 ne divise pas d/e.

On utilise le théorème 2.20. Soit $\mathfrak{p}$ un idéal premier de k ne divisant pas 2 ; ou bien $\mathfrak{p}$ divise e, et alors $\mathfrak{p}$ divise d et donc est ramifié dans $k/\mathbb{Q}$ et on trouve $\mathrm{val}_{\mathfrak{p}}(e) = 2$, ou bien $\mathfrak{p}$ ne divise pas e. Dans tous les cas, il découle de ce théorème que $\mathfrak{p}$ est non ramifié dans $k(\sqrt{e})/k$ pour tout idéal premier $\mathfrak{p} \nmid 2$. Maintenant, soit $\mathfrak{p}$ un idéal premier au-dessus de 2 ; l'hypothèse $e \equiv 1 \pmod 4$ assure que e est congru à un carré modulo $\mathfrak{p}^{2a}$ où a est l'indice de ramification de $\mathfrak{p}$. Ainsi, l'extension $k(\sqrt{e})/k$ est non ramifiée pour $\mathfrak{p} \mid 2$. Donc $k(\sqrt{e})$ est bien le corps de classes de Hilbert de k.

Le raisonnement qui précède la proposition 4.7 implique que si $\mathfrak{i}$ est l'indice dans $\mathcal{O}_{H_k}$ de $\mathcal{O}_k[\sqrt{e}]$, alors $\mathfrak{i}^2 = e\mathcal{O}_k$ ou $4e\mathcal{O}_k$. Ainsi, l'idéal entier $\mathfrak{e} = \mathfrak{i}$ ou $\frac{1}{2}\mathfrak{i}$ vérifie bien $\mathfrak{e}^2 = e\mathcal{O}_k$ et est dans la classe de $\mathfrak{i}$ qui est aussi la classe $\mathcal{S}$. □

Remarque : Notons que pour tout diviseur strict $e \equiv 1 \pmod 4$ de d, la classe de $\mathfrak{e}$ est toujours la même, *ie* la classe de $\mathcal{S}$.

Exemple : On applique ce théorème au corps k avec $d := 105 = 3.5.7$. On prend $e = 5$. Soit $\mathfrak{p}$ l'idéal premier de k vérifiant $\mathfrak{p}^2 = e\mathcal{O}_k$; on trouve que :

$$\mathfrak{p} = (-2\sqrt{105} + 11)\mathcal{O}_k,$$

et donc le module $\mathcal{O}_{H_k}$ est $\mathcal{O}_k$-libre.

4.3. Extensions non abéliennes non ramifiées

Soient k un corps de nombres et H_k son corps de classes de Hilbert. On suppose que $H_k \neq k$, *ie* k n'est pas principal. Supposons aussi que H_k n'est pas principal et soit $H_k^{(2)}$ le corps de classes de Hilbert de H_k.

Alors, l'extension $H_k^{(2)}/k$ est non ramifiée mais n'est pas abélienne.

La détermination de telles extensions non ramifiées et non abéliennes n'est pas en général une tâche facile. Notamment, si on utilise la méthode décrite dans les chapitres 2 et 3, il est nécessaire de travailler dans H_k pour calculer son groupe de classes et son corps de classes de Hilbert. De plus, pour que H_k ait de bonnes chances d'être non principal, il ne doit pas être de degré ou de discriminant trop petits, ce qui rend les calculs encore plus compliqués.

Le problème se simplifie notablement quand l'extension H_k/k est scindée. Supposons que le corps $\tilde{k}$ scinde l'extension et que, de surcroît, il n'est pas principal ; on note $\tilde{H}_k$ son corps de classes de Hilbert. Alors, le corps $H_k\tilde{H}_k$ est une extension non ramifiée de k et non abélienne. Notons qu'en général, $H_k\tilde{H}_k$ est strictement inclus dans $H_k^{(2)}$, le deuxième étage de la tour de corps de classes de Hilbert de k.

On a utilisé des exemples de corps admettant une extension de corps de classes de Hilbert scindée pour construire quelques extensions non ramifiées et non abéliennes.

Exemple : Soit $k := \mathbb{Q}(\sqrt{2.229})$; l'extension de corps de classes de Hilbert de k est de degré 2 et est scindée par le corps $\tilde{k} := \mathbb{Q}(\sqrt{229})$. Or, le corps $\tilde{k}$ a pour nombre de classes 3 et son extension de corps de classes de Hilbert est scindée par le corps k' défini par une racine du polynôme $X^3 - 4X - 1$.

Ainsi, le corps composé $K := k\tilde{k}k'$ est une extension relative non ramifiée et non abélienne de degré 6 du corps quadratique k. On a $K := \mathbb{Q}(\alpha)$, où α est racine du polynôme irréductible :

$$X^{12} + 4X^{11} - 36X^{10} - 96X^9 + 412X^8 + 668X^7 - 1954X^6 - 1540X^5 + 4084X^4 + 664X^3 - 3088X^2 + 636X + 241.$$

Il est possible de travailler directement dans le corps quartique $k\tilde{k}$ et de montrer que ce corps a pour nombre de classes 3 ; ainsi, le corps K est le deuxième étage de la tour de classes de Hilbert de k. On peut vérifier également que le corps K est principal et donc que cette tour s'arrête à cet étage.

Le corps $k := \mathbb{Q}(\sqrt{290})$ a pour nombre de classes 4 ; son corps de classes de Hilbert est donné par le composé des corps k et $\tilde{k}$ où ce dernier est un corps de rupture du polynôme irréductible $X^4 - 17X^2 + 36$. Notons que dans cet exemple, si on souhaite travailler directement dans le corps de classes de Hilbert de k, il faut travailler dans un corps de degré 8 et si le calcul du groupe de classes de ce corps ne pose pas trop de problème, la construction de son corps de classes de Hilbert est plus difficile.

Le corps $\tilde{k}$ a pour nombre de classes 2 et son extension de corps de classes de Hilbert n'est pas scindée ; on note $\tilde{H}_k$ son corps de classes de Hilbert. L'extension K/k où $K := k\tilde{H}_k$ est une extension relative de degré 8 (degré absolu 16) non abélienne et non ramifiée. On démontre que K est le deuxième étage de la tour de corps de classes de Hilbert de k en calculant directement le nombre de classes de H_k, et aussi que c'est le dernier en prouvant que K est principal. Le corps K est engendré sur $\mathbb{Q}$ par une racine du polynôme :

$$X^{16} - 4X^{15} - 34X^{14} + 144X^{13} + 363X^{12} - 1724X^{11} - 1474X^{10} + 9292X^9 + 659X^8 - 23776X^7 + 9482X^6 + 25140X^5 - 18207X^4 - 5012X^3 + 6224X^2 - 1148X + 49.$$

Un troisième exemple est fourni par le corps $k := \mathbb{Q}(\theta)$ avec $\theta^3 - \theta^2 - 92\theta - 236 = 0$. Ce corps est cyclique de discriminant 277^2 et de nombre de classes 4. En vertu du théorème 4.2 ou de la proposition 4.3, on sait que son extension de corps de classes de Hilbert est scindée par un corps $\tilde{k}$; on trouve pour $\tilde{k}$ le corps de rupture du polynôme $X^4 - X^3 - 11X^2 + 4X + 12$. Ce corps a pour nombre de classes 2 et en composant k avec $\tilde{H}_k$, le corps de classes de Hilbert de $\tilde{k}$, on obtient une extension relative K/k de degré 8 non abélienne et non ramifiée.

Le corps K est engendré par une racine du polynôme :

$$X^{24} - X^{23} - 53X^{22} + 120X^{21} + 992X^{20} - 3549X^{19} - 6404X^{18} + 42411X^{17} - 16548X^{16} \\ - 207733X^{15} + 336648X^{14} + 254034X^{13} - 1032121X^{12} + 407583X^{11} + 1128782X^{10} \\ - 1108564X^9 - 338538X^8 + 795092X^7 - 117798X^6 - 210356X^5 \\ + 64829X^4 + 16842X^3 - 5868X^2 + 184X + 16.$$

On montre également que le corps K est le deuxième étage de la tour de corps de classes de Hilbert de k. La question de savoir si c'est le dernier étage est plus délicate à résoudre. Les bornes d'Odlyzko (*cf* [**45**]) ne permettent pas de conclure puisque le racine 42-ième du discriminant d'une éventuelle extension quadratique de K non ramifiée est supérieure de $0,03\%$ à la borne inférieure correspondant à ce degré et à cette signature. Néanmoins, on peut montrer en utilisant le système PARI ([**3**]) que sous l'hypothèse de Riemann généralisée, ce corps est bien principal.

4.4. Corps de petits discriminants

La théorie du corps de classes permet de décrire les extensions abéliennes d'un corps donné en travaillant uniquement dans ce corps. Ainsi, en appliquant les méthodes de [**11**], on peut calculer explicitement le degré et le conducteur de certaines extensions abéliennes d'un corps de nombres.

Plus exactement, si on se fixe un degré pour le corps de base k, un degré pour l'extension abélienne K et, pour chaque degré possible de K, une borne supérieure pour le discriminant de K, il existe un algorithme permettant de construire tous les corps K possibles à condition qu'on dispose de tables de corps de nombres k suffisamment étendues pour contenir tous les corps k qu'on aura à considerer. La méthode est expliquée en détail dans [**11**] et reprise dans [**13**] pour construire un grand nombre de corps totalement complexes de petits discriminants par une telle recherche exhaustive. La notion importante pour mesurer la taille du discriminant d'un corps est la notion de *root discriminant* qui est défini comme la racine N-ième de la valeur absolue du discriminant absolu de K où $N := [K : \mathbb{Q}]$; on note :

$$rd_K := |d_K|^{1/[K:\mathbb{Q}]}.$$

Dans ce travail, on n'a pas cherché à faire une telle recherche exhaustive ; on s'est plutôt concentré sur la recherche de corps totalement réels de petits discriminants qui sont des extensions abéliennes de corps réels quadratiques ou cubiques et constructibles par la méthode développée dans cette thèse. En effet, l'intérêt ici n'est pas de trouver de tels corps par la donnée du corps de base et du conducteur (comme c'est le cas pour la plupart des corps de [**13**]), mais de fournir pour ces corps un polynôme irréductible les caractérisant. On s'est également restreint à considérer des corps K de degré absolu ≥ 8 puisqu'il existe des tables étendues pour les degrés inférieurs.

Exemples : Soit $k := \mathbb{Q}(\sqrt{2})$. Soit $\mathfrak{p}$ un idéal premier au-dessus de 41 et K le corps de classes de rayon $\mathfrak{p}$. C'est une extension de degré 4 de k. Le corps K est le corps de rupture du polynôme :

$$X^8 - 4X^7 + 14X^5 - 8X^4 - 12X^3 + 7X^2 + 2X - 1,$$

son discriminant est $2^{12}.41^3$ et son root discriminant est supérieur de 3% à la borne d'Odlyzko correspondante.

Le corps de classes de rayon 7 du corps quadratique $k := \mathbb{Q}(\sqrt{3})$ est une extension $K/\mathbb{Q}$ de degré 12 et de discriminant $2^{12}.3^6.7^{10}$; son root discriminant est supérieur de 8% à la borne d'Odlyzko. On a $K = \mathbb{Q}(\theta)$ où θ est racine du polynôme :

$$X^{12} - 11X^{10} + 44X^8 - 78X^6 + 60X^4 - 16X^2 + 1.$$

Le corps $k := \mathbb{Q}(\theta)$ avec :

$$\theta^3 - \theta^2 - 36\theta + 18 = 0,$$

a pour nombre de classes 7 et son corps de classes de Hilbert est le corps de rupture du polynôme de degré 21 :

$$X^{21}+6X^{20}-9X^{19}-112X^{18}-57X^{17}+759X^{16}+840X^{15}-2547X^{14}-3384X^{13}$$
$$+4943X^{12}+6438X^{11}-6095X^{10}-6298X^{9}+4740X^{8}+3058X^{7}$$
$$-2015X^{6}-730X^{5}+424X^{4}+79X^{3}-38X^{2}-3X+1.$$

Ce corps a pour discriminant $2^{14}.5303^7$ et son root discriminant est de 8,5% supérieur aux bornes d'Odlyzko.

4.5. Construction de certains groupes de Galois

On utilise la théorie du corps de classes pour réaliser certains groupes de Galois, puis on donne des constructions explicites de ces corps.

On commence par un lemme qui est à rapprocher des résultats de la section 2 :

Lemme 4.9. *Soit k un corps de nombres galoisien ; on note H_k le corps de classes de Hilbert de k et on suppose que $k \neq H_k$.*

Alors, l'extension $H_k/\mathbb{Q}$ est galoisienne mais non cyclique.

Démonstration : Le fait que l'extension $H_k/\mathbb{Q}$ est galoisienne a déjà été démontré lors de la preuve du théorème 4.1. Maintenant, supposons que cette extension soit cyclique ; on raisonne de manière similaire à la démonstration de la proposition 4.3.

Il existe un nombre premier p qui est inerte dans $H_k/\mathbb{Q}$, et donc il existe un unique idéal principal au-dessus de p dans k, à savoir $p\mathcal{O}_k$. Puisque cet idéal est principal, il se décompose totalement dans l'extension H_k/k par la théorie du corps de classes ce qui nous donne une contradiction. Donc l'extension $H_k/\mathbb{Q}$ ne peut être cyclique. □

Une première application est classique et concerne la réalisation des groupes diédraux :

Proposition 4.10. *Soit k un corps quadratique de groupe de classes cyclique d'ordre impair n avec $n \leq 11$. Alors, le groupe de Galois de $H_k/\mathbb{Q}$ est le groupe diédral D_n d'ordre $2n$.*

Démonstration : C'est une conséquence immédiate du lemme puisque les seuls groupes de Galois possibles sont C_{2n} et D_n par le théorème 4.1. □

Notons que, sous ces hypothèses, l'extension H_k/k est scindée par un corps k' de degré n et dont le groupe de Galois est isomorphe à D_n.

Exemples : On donne pour tout entier impair n entre 3 et 11, un polynôme de degré n dont le corps de rupture $\tilde{k}$ a pour groupe de Galois D_n. On indique également le discriminant du corps quadratique k dont le corps de classes de Hilbert est obtenu en composant k et $\tilde{k}$.

$n=3$	X^3-4X-1	229
$n=5$	$X^5-X^4-5X^3+4X^2+3X-1$	401
$n=7$	$X^7-2X^6-7X^5+10X^4+13X^3-10X^2-X+1$	577
$n=9$	$X^9-3X^8-10X^7+38X^6+5X^5-107X^4+58X^3+78X^2-60X-1$	1129
$n=11$	$X^{11}-5X^{10}-4X^9+54X^8-53X^7-127X^6+208X^5+69X^4$ $-222X^3+29X^2+56X-5$	1297

En fait, on peut faire de même pour les degrés supérieurs. Ainsi, soit k un corps cubique cyclique de nombre de classes p, nombre premier distinct de 3. Alors, en appliquant un des résultats 4.1, 4.2 ou 4.3, on obtient que l'extension H_k/k est scindée par un corps $\tilde{k}$ de degré p ; on sait également que $H_k/\mathbb{Q}$ est une extension galoisienne. Donc, le groupe de Galois de $H_k/\mathbb{Q}$ est ou bien C_{3p}, ou bien $C_p \rtimes C_3$ (le produit semi-direct du groupe C_p par le groupe C_3). Le premier cas étant impossible d'après le lemme, le groupe de Galois est donc $C_p \rtimes C_3$. De plus, le corps $\tilde{k}$ n'étant pas galoisien (sinon il serait abélien et on se retrouverait dans le cas cyclique), sa clôture galoisienne est le corps H_k.

Exemples : Le seul exemple disponible parmi les corps cubiques considérés est pour $p = 7$. Le corps k est le corps cyclique cubique de discriminant 313^2. Le corps $\tilde{k}$ est alors le corps de rupture du polynôme suivant, il a pour groupe de Galois $C_7 \rtimes C_3$:

$$X^7 - X^6 - 15X^5 + 20X^4 + 33X^3 - 22X^2 - 32X - 8.$$

4.6. Corps CM diédraux principaux[†]

Un corps de nombres N est dit à multiplication complexe, ou corps CM, si c'est un corps totalement complexe, extension quadratique d'un corps totalement réel, noté N^+. Ces corps possèdent un certain nombre de propriétés, notamment si on suppose que le corps $N/\mathbb{Q}$ est galoisien ou abélien.

On sait d'après les travaux d'Odlyzko qu'il n'existe qu'un nombre fini de corps CM galoisiens principaux. Tous les corps CM abéliens principaux ont été déterminées par Yamamura (*cf* [**57**]), d'autres travaux ont également permis de déterminer ces corps dans de nombreux cas (*cf* [**38**] par exemple). Le travail de Y. Lefeuvre consiste à déterminer les corps CM diédraux principaux.

Soit N un corps CM diédral ; on suppose que son degré absolu est de la forme $4p$ où p est un nombre premier impair. Le sous-corps réel maximal N^+ est alors une extension diédrale de degré $2p$. En utilisant divers ingrédients, on obtient une minoration effective de h_N^- (défini comme le quotient h_N/h_{N^+}) croissante avec p et le conducteur de N^+/k où k est l'unique sous-corps quadratique réel de $N^+/\mathbb{Q}$. On obtient ainsi une liste finie de corps N susceptibles d'être principaux. On doit alors vérifier si c'est effectivement le cas.

Exemple : On note $k := \mathbb{Q}(\sqrt{2.5.7})$ et on considère l'unique extension cyclique N de k de conducteur $5v_1v_2$ et de degré relatif 10 (où v_1, v_2 sont les places infinies de k). Le corps N est un corps CM diédral de degré 20, dont le sous-corps réel maximal est l'unique extension abélienne N^+ de k de conducteur 5 et de degré relatif 5. On trouve que $h_N^- = 1$; ainsi, pour vérifier si le corps N est principal ou non, il est nécessaire de calculer le nombre de classes de N^+, et pour cela de connaître explicitement ce corps.

On utilise alors la méthode expliquée dans le chapitre 2, en tenant compte du fait qu'ici on ne cherche pas à construire le corps de classes de rayon $k(5)$ qui est de degré relatif 20 (ce qui serait une tâche trop fastidieuse et nécessiterait en plus de redescendre au corps N^+), mais directement le corps N^+ en modifiant la méthode exposée dans le cas plus général d'une extension abélienne quelconque.

On trouve le polynôme absolu (après réduction) :

$$X^{10} - 40X^8 + 605X^6 - 4310X^4 + 14400X^2 - 17920.$$

On calcule le nombre de classes de N^+ : on trouve $h_{N^+} = 2$. Ainsi, le corps N^+ n'est pas principal et le corps N non plus.

[†]Cette application m'a été suggérée par Y. Lefeuvre (Université de Caen)

Bibliographie

1. M. Abramowitz, I.A. Stegun, *Handbook of Mathematical Functions*, Dover Publication, New York, 1972
2. E. Bach, J. Sorenson, *Explicit Bounds for Primes in Residue Classes*, Math. Comp. **65** (1996), p. 1717–1735
3. C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *User's Guide to PARI-GP*, 1997
4. E. Berlekamp, *Factoring Polynomials over Large Finite Fields*, Math. Comp. **24** (1970), p. 713–735
5. Z.I. Borevitch, I.R. Shafarevitch, *Number Theory*, Academic Press, New York, 1966
6. G. Butler, J. McKay, *The Transitive Groups of Degree up to Eleven*, Comm. Algebra **11** (1983), p. 863–911
7. J.W.S. Cassels, *Local Fields*, Cambridge Univ. Press, 1986
8. H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer-Verlag, Berlin, 1993
9. H. Cohen, *Hermite and Smith Normal Form Algorithms over Dedekind Domain*, Math. Comp. **65** (1996), p. 1681–1699
10. H. Cohen, F. Diaz y Diaz, *A Polynomial Reduction Algorithm*, Sém. Th. Nombres Bordeaux (série 2), **3** (1991), p. 351–360
11. H. Cohen, F. Diaz y Diaz, M. Olivier, *Computing Ray Class Groups, Conductors and Discriminants*, Math. Comp., à paraître
12. H. Cohen, F. Diaz y Diaz, M. Olivier, *Algorithmic Techniques for Relative Extensions of Number Fields*, prépublication A2X, 1996
13. H. Cohen, F. Diaz y Diaz, M. Olivier, *A Table of Totally Complex Number Fields of Small Discriminants*, prépublication A2X, 1997
14. G. Cornell, M. Rosen, *A Note on the Splittinig of the Hilbert Class Fields*, J. Number Theory **11** (1988), p. 152–158
15. M. Daberkow, M. Pohst, *Computations with Relative Extensions of Number Fields with an Application to the Construction of Hilbert Class Fields*, Proc. ISAAC'95, 1995
16. D. Dummit, D. Hayes, *Checking the* $\mathfrak{p}$*-adic Stark Conjecture when* $\mathfrak{p}$ *is Archimedian*, ANTS II (ed. H. Cohen), LN in Comp. Sci. **1122** (1996), p. 91–97
17. D. Dummit, J. Sands, B. Tangedal, *Computing Stark Units for Totally Real Cubic Fields*, Math. Comp. (à paraître)
18. C. Fieker, M. Pohst, *Lattices over Number Fields*, ANTS II (ed. H. Cohen), LN in Comp. Sci. **1122** (1996), p. 147–157
19. U. Fincke, M. Pohst, *Improved Methods for Calculating Vectors of Short Length*, Math. Comp. **44** (1985), p. 463–471
20. D. Ford, *On the Computation of the Maximal Order in a Dedekind Domain*, Thèse, Ohio State University, 1978
21. D. Ford, *The Construction of Maximal Orders over a Dedekind Domain*, J. Symbol. Comp. **4** (1987), p. 69–75
22. D. Ford, P. Létard, textslImplementing the Round Four Maximal Order Algorithm, Sém. Th. Nombres de Bordeaux **6** (1994), p. 39–80
23. E. Friedman, *Hecke's Integral Formula*, Sém. Th. Nombres de Bordeaux (1987-1988)
24. A. Fröhlich, J. Queyrut, *On the Functional Equation of the Artin L-function for Characters of Real Representations*, Inv. Math. **20** (1973), p. 125–138
25. K. Geddes, S. Czapor, G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Press, Boston, Dordrecht, London, 1992
26. M. Hall, *The Theory of Groups*, Macmillan Company, 1959
27. D. Hayes, *The Refined* $\mathfrak{p}$*-adic Abelian Stark Conjectures in Function Fields*, Invent. Math. **94** (1989), p. 505–527
28. J. Hastad, B. Just, J.C. Lagarias, C.P. Schnorr, *Polynomial Time Algorithms for Finding Integer Relations among Real Numbers*, Siam J. Comput. **18** (1989), p. 859–881
29. E. Hecke, *Lectures on the Theory of Algebraic Numbers*, GTM **77**, Springer-Verlag, Berlin, 1981
30. M. Ishida, *The Genus Fields of Algebraic Number Fields*, LN in Math. **555**, Springer-Verlag, Berlin, 1976
31. N. Jacobson, *Basic Algebra II*, W.H. Freeman and Co., 1980
32. J. Klüners, M. Pohst, *On Computing Subfields*, J. Symbol. Comp. **11** (1996)
33. S. Landau, G.L. Miller, *Solvability by Radicals is in Polynomial Time*, J. Comput. Syst. Sci. **30** (1985), p. 179–208
34. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970
35. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1994
36. A.K. Lenstra, *Factoring Polynomials over Algebraic Number Fields*, LN in Comp. Sci. **144** (1982), p. 32–39
37. A.K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann. **261** (1982), p. 515–534
38. S. Louboutin, *Determination of All Non-Normal Quartic CM-fields and All Non Abelian Normal Octic CM-fields with Class Number One*, Acta Arith. **67** (1994), p. 47–62
39. J. Martinet, *Character Theory and Artin L-functions*, Algebraic Number Fields (ed. A. Frölich), Academic Press, London, 1977
40. M. Mignotte, *An Inequality about Factors of Polynomials*, Math. Comp. **28** (1974), p. 1153–1157
41. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN - Polish Scientific Publishers, Warszawa, 1973

42. J. Neukirch, *On Solvable Number Fields*, Invent. Math. **53** (1979), p. 135–164
43. J. Neukirch, *Class Field Theory*, Grundlehren der math. Wiss. **280**, Springer-Verlag, 1986
44. M. Pohst, H. Zassenhauss, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989
45. G. Poitou, *Minorations de Discriminants (d'après A. M. Odlyzko)*, Sém. Bourbaki, LN in Math. **567** (1976)
46. X.-F. Roblot, *Unités de Stark et corps de classes de Hilbert*, C. R. Acad. Sci. Paris **323** (1996), p. 1165–1168
47. J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962
48. H.M. Stark, *Class Fields for Real Quadratic Fields and L-series at 1*, Algebraic Number Fields (ed. A. Frölich), Academic Press, London, 1977
49. H.M. Stark, *Hilbert's Twelfth Problem and L-series*, Bull. Am. Math. Soc. **83** (1997), p. 1072–1074
50. H.M. Stark, *Values of L-functions at $s = 1$. I. L-functions for quadratic forms*, Advances in Math. **7** (1971), p. 301–343 ; *II. Artin L-functions with Rational Characters*, *ibid.* **17** (1975), p. 60–92 ; *III. Totally Real Fields and Hilbert's Twelfth Problem*, *ibid.* **22** (1976), p. 64–84 ; *IV. First Derivatives at $s = 0$*, *ibid.* **35** (1980), p. 197–235
51. J.T. Tate, *Local Constants*, Algebraic Number Fields (ed. A. Frölich), Academic Press, London, 1977
52. J.T. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$*, Birkhaüser, Boston, 1984
53. E. Tollis, *Calculs dans les Corps de Nombres : Étude Algorithmique de la Fonction Zêta de Dedekind*, Thèse, Université Bordeaux I, 1996
54. E. Tollis, *Zeros of Dedekind Zeta Functions in the Critical Strip*, Math. Comp. (à paraître)
55. B. Trager, *Algebraic Factoring and Rational Function Integration*, Proceedings of SYMPOSAC '76 (1976), p. 219–226
56. L. Washington, *Introduction to Cyclotomic Fields (2e ed.)*, GTM **83**, Springer-Verlag, New-York, 1996
57. K. Yamamura, *The Determination of the Imaginary Abelian Number Fields with Class Number One*, Math. Comp. **62** (1984), p. 899-921

APPENDICE

TABLES DE CORPS DE CLASSES DE HILBERT DE CORPS TOTALEMENT RÉELS DE DEGRÉ 2, 3 ET 4

On donne dans cette appendice les résultats obtenus lors du calcul du corps de classes de Hilbert de corps totalement réels. Ces corps ont été construits grâce aux méthodes développées et expliquées dans les chapitres 2 et 3. Pour chaque corps considéré, on fournit le polynôme irréductible d'un élément primitif θ du corps de base (celui donné par les tables utilisées), puis le discriminant absolu du corps de base et le polynôme relatif d'un élément primitif du corps de classes de Hilbert (ce polynôme est à coefficients dans $\mathbb{Q}[\theta]$). Ces polynômes ont été réduits et vérifiés suivant les procédures du chapitre 3.

A.1. Corps quadratiques

La table suivante donne le corps de classes de Hilbert des 288 corps quadratiques réels non principaux de discriminant ≤ 2000. Parmi ces corps, il y en a 194 de nombre de classes 2, 24 de nombre de classes 3, 41 de nombre de classes 4, 9 de nombre de classes 5, 9 de nombre de classes 6, 4 de nombre de classes 7, 5 de nombre de classes 8, 1 de nombre de classes 9 et 1 de nombre de classes 11.

X^2-10	40	$X^2+\theta X+2$
X^2-15	60	$X^2-X+(-\theta-4)$
X^2-X-16	65	$X^2+(-\theta-4)$
X^2-X-21	85	$X^2+(\theta-6)$
X^2-26	104	$X^2-X+(-\theta-5)$
X^2-X-26	105	$X^2+(-\theta-6)$
X^2-30	120	$X^2-X+(\theta-7)$
X^2-34	136	$X^2+X+(\theta-6)$
X^2-35	140	$X^2+X+(-\theta-8)$
X^2-X-36	145	$X^4-X^3+(\theta-7)X^2+(-\theta+7)X+(-2\theta+13)$
X^2-39	156	$X^2+X+(-\theta-6)$
X^2-X-41	165	X^2-5
X^2-42	168	$X^2+X+(\theta-7)$
X^2-X-46	185	$X^2+(\theta-11)$
X^2-51	204	$X^2+X+(-\theta-7)$
X^2-X-51	205	$X^2+(\theta-12)$
X^2-55	220	$X^2+X+(\theta-12)$
X^2-X-55	221	$X^2+(-\theta-7)$
X^2-X-57	229	$X^3-X^2+(\theta-8)X+(\theta-8)$
X^2-58	232	$X^2+X+(\theta-9)$
X^2-X-64	257	$X^3-X^2+(-\theta-8)X+(2\theta+15)$
X^2-66	264	$X^2-X+(-\theta-10)$
X^2-X-66	265	$X^2+(-\theta-14)$
X^2-X-68	273	$X^2+(-\theta-8)$
X^2-70	280	$X^2-X+(-\theta-15)$
X^2-X-71	285	X^2-5

X^2-74	296	$X^2-X+(-\theta-11)$
X^2-X-76	305	$X^2+(\theta-17)$
X^2-78	312	$X^2+X+(-\theta-9)$
X^2-79	316	$X^3-X^2+(\theta-9)X+(-2\theta+18)$
X^2-X-80	321	$X^3-X^2+(\theta-10)X+(-2\theta+19)$
X^2-82	328	$X^4-2X^3+(\theta-9)X^2+(-\theta+10)X+(-5\theta+45)$
X^2-X-86	345	$X^2+(-\theta-18)$
X^2-87	348	X^2-3
X^2-X-89	357	$X^2+(\theta-10)$
X^2-91	364	$X^2-X+(\theta-10)$
X^2-X-91	365	$X^2+(\theta-20)$
X^2-X-94	377	$X^2+(\theta-11)$
X^2-95	380	$X^2+X+(\theta-20)$
X^2-X-96	385	$X^2+(\theta-21)$
$X^2-X-100$	401	$X^5-X^4+(\theta-11)X^3+(\theta-10)X^2+(-2\theta+21)X+(-2\theta+21)$
X^2-102	408	$X^2+X+(\theta-10)$
X^2-106	424	$X^2+X+(-\theta-15)$
$X^2-X-107$	429	$X^2+(\theta-12)$
X^2-110	440	X^2-5
X^2-111	444	$X^2-X+(\theta-12)$
$X^2-X-111$	445	$X^4-X^3+(-\theta-11)X^2+(\theta+11)X+(4\theta+40)$
X^2-114	456	$X^2-X+(\theta-16)$
X^2-115	460	$X^2+X+(\theta-24)$
$X^2-X-116$	465	$X^2+(-\theta-24)$
$X^2-X-117$	469	$X^3+(\theta-13)X+(2\theta-22)$
$X^2-X-118$	473	$X^3-X^2+(\theta-12)X+(-2\theta+23)$
X^2-119	476	$X^2-X+(\theta-11)$
$X^2-X-120$	481	$X^2+(\theta-13)$
$X^2-X-121$	485	$X^2+(-\theta-25)$
X^2-122	488	$X^2-X+(-\theta-17)$
X^2-123	492	$X^2-X+(-\theta-13)$
$X^2-X-123$	493	$X^2+(\theta-12)$
$X^2-X-126$	505	$X^4-X^3+(-\theta-11)X^2+(\theta+11)X+(4\theta+43)$
X^2-130	520	$X^4-2X^3+(-\theta-11)X^2+(\theta+12)X+(5\theta+57)$
$X^2-X-133$	533	$X^2+(-\theta-13)$
$X^2-X-136$	545	$X^2+(-\theta-28)$
X^2-138	552	$X^2+X+(-\theta-19)$
$X^2-X-140$	561	$X^2+(-\theta-12)$
$X^2-X-141$	565	$X^2+(\theta-30)$
X^2-142	568	$X^3-X^2+(-\theta-12)X+(2\theta+24)$
X^2-143	572	$X^2-X+(\theta-14)$
$X^2-X-144$	577	$X^7-X^6-13X^5+(\theta+21)X^4+(-3\theta+19)X^3-19X^2+(4\theta-26)X-7$
X^2-146	584	$X^2+X+(-\theta-20)$
$X^2-X-152$	609	$X^2+(-\theta-12)$
X^2-154	616	$X^2+X+(-\theta-21)$
X^2-155	620	$X^2+X+(\theta-32)$
$X^2-X-157$	629	$X^2+(\theta-14)$
X^2-159	636	$X^2-X+(-\theta-16)$
$X^2-X-161$	645	$X^2+(-\theta-33)$
$X^2-X-166$	665	$X^2+(-\theta-34)$
X^2-170	680	$X^4-2X^3+(-\theta-13)X^2+(\theta+14)X+(6\theta+78)$
$X^2-X-171$	685	$X^2+(-\theta-35)$

$X^2 - X - 172$	689	$X^4 - 14X^2 + (2\theta - 1)X - 13$
$X^2 - 174$	696	$X^2 + X + (\theta - 13)$
$X^2 - X - 174$	697	$X^6 - 2X^5 - 14X^4 + (-\theta + 14)X^3 + (\theta + 41)X^2 + 5\theta X + 25$
$X^2 - X - 176$	705	$X^2 + (-\theta - 36)$
$X^2 - 178$	712	$X^2 - X + (\theta - 24)$
$X^2 - 182$	728	$X^2 - X + (\theta - 17)$
$X^2 - 183$	732	$X^2 + X + (\theta - 18)$
$X^2 - X - 183$	733	$X^3 - X^2 + (\theta - 14)X + (\theta - 14)$
$X^2 - X - 185$	741	$X^2 + (\theta - 18)$
$X^2 - 186$	744	$X^2 - X + (-\theta - 25)$
$X^2 - X - 186$	745	$X^2 + (-\theta - 38)$
$X^2 - 187$	748	$X^2 - X + (-\theta - 15)$
$X^2 - 190$	760	$X^2 + X + (\theta - 39)$
$X^2 - X - 190$	761	$X^3 - X^2 + (-\theta - 14)X + (2\theta + 27)$
$X^2 - 194$	776	$X^2 + X + (\theta - 26)$
$X^2 - X - 194$	777	$X^4 + (\theta - 18)X^2 + (3\theta - 41)X + (2\theta - 29)$
$X^2 - 195$	780	$X^4 - 15X^2 + 2\theta X - 14$
$X^2 - X - 196$	785	$X^6 - 3X^5 - 11X^4 + (2\theta + 26)X^3 + (-3\theta - 29)X^2 + (\theta + 16)X - 3$
$X^2 - X - 198$	793	$X^4 - 16X^2 + (2\theta - 1)X - 13$
$X^2 - X - 201$	805	$X^2 + (-\theta - 41)$
$X^2 - 202$	808	$X^2 + X + (\theta - 27)$
$X^2 - 203$	812	$X^2 - X + (\theta - 14)$
$X^2 - X - 204$	817	$X^5 - 15X^3 + 44X + (2\theta - 1)$
$X^2 - 210$	840	$X^4 - 2X^3 + (-\theta - 15)X^2 + (\theta + 16)X + (7\theta + 101)$
$X^2 - 215$	860	$X^2 - 5$
$X^2 - X - 215$	861	$X^2 + (\theta - 16)$
$X^2 - X - 216$	865	$X^2 + (-\theta - 44)$
$X^2 - 218$	872	$X^2 + X + (-\theta - 29)$
$X^2 - 219$	876	$X^4 - 2X^3 + (-\theta - 14)X^2 + (\theta + 15)X + (5\theta + 74)$
$X^2 - X - 221$	885	$X^2 + (-\theta - 45)$
$X^2 - 222$	888	$X^2 - X + (\theta - 15)$
$X^2 - 223$	892	$X^3 - X^2 + (\theta - 15)X + (-2\theta + 30)$
$X^2 - X - 224$	897	$X^4 - X^3 + (\theta - 18)X^2 + (\theta - 16)X + (-2\theta + 31)$
$X^2 - X - 225$	901	$X^4 - X^3 + (\theta - 18)X^2 + (\theta - 15)X + (-3\theta + 47)$
$X^2 - 226$	904	$X^8 - 18X^6 + 82X^4 + 2\theta X^3 - 117X^2 - 6\theta X - 8$
$X^2 - X - 226$	905	$X^4 - 16X^2 + (2\theta - 1)X - 15$
$X^2 - 230$	920	$X^2 + X + (-\theta - 47)$
$X^2 - 231$	924	$X^4 - 15X^2 + 2\theta X - 17$
$X^2 - 235$	940	$X^6 - 3X^5 - 12X^4 + (-2\theta + 29)X^3 + (3\theta - 34)X^2 + (-\theta + 19)X - 2$
$X^2 - X - 237$	949	$X^2 + (\theta - 22)$
$X^2 - 238$	952	$X^2 + X + (-\theta - 18)$
$X^2 - X - 239$	957	$X^2 + (\theta - 16)$
$X^2 - X - 241$	965	$X^2 + (-\theta - 49)$
$X^2 - X - 242$	969	$X^2 + (\theta - 19)$
$X^2 - 246$	984	$X^2 + X + (\theta - 16)$
$X^2 - X - 246$	985	$X^6 - X^5 - 18X^4 + 12X^3 + (-3\theta + 57)X^2 + (\theta - 19)X + (6\theta - 97)$
$X^2 - 247$	988	$X^2 - X + (-\theta - 22)$
$X^2 - X - 248$	993	$X^3 - X^2 + (\theta - 18)X + (2\theta - 33)$
$X^2 - X - 250$	1001	$X^2 + (\theta - 23)$
$X^2 - X - 251$	1005	$X^2 + (\theta - 52)$
$X^2 - X - 252$	1009	$X^7 - 2X^6 - 16X^5 + (-\theta + 14)X^4 + (-\theta + 35)X^3 + (2\theta - 26)X^2 + (2\theta - 36)X - 1$

X^2-254	1016	$X^3-X^2+(\theta-18)X+(2\theta-32)$
X^2-255	1020	$X^4-17X^2+2\theta X-15$
X^2-258	1032	$X^2+X+(-\theta-34)$
X^2-259	1036	$X^2+X+(\theta-16)$
$X^2-X-259$	1037	$X^2+(\theta-20)$
$X^2-X-261$	1045	$X^4-X^3+(-\theta-16)X^2+(\theta+16)X+(6\theta+94)$
X^2-266	1064	$X^2+X+(\theta-35)$
$X^2-X-266$	1065	$X^2+(-\theta-54)$
X^2-267	1068	$X^2+X+(-\theta-25)$
$X^2-X-268$	1073	$X^2+(\theta-17)$
$X^2-X-271$	1085	$X^2+(-\theta-55)$
$X^2-X-273$	1093	$X^5-X^4-18X^3+12X^2+(\theta+55)X+(\theta-11)$
X^2-274	1096	$X^4-17X^2+2\theta X-14$
$X^2-X-275$	1101	$X^3+(\theta-18)X+(2\theta-34)$
$X^2-X-276$	1105	$X^4-2X^3-16X^2+(-2\theta+18)X+(\theta-21)$
$X^2-X-278$	1113	$X^2+(-\theta-18)$
X^2-282	1128	$X^2+X+(\theta-37)$
$X^2-X-282$	1129	$X^9-4X^8-11X^7+45X^6+(\theta+21)X^5+(-\theta-116)X^4$ $+(-3\theta-4)X^3+(\theta+43)X^2-3X-1$
X^2-286	1144	$X^2+X+(\theta-25)$
$X^2-X-286$	1145	$X^4+(-\theta-17)X^2+(7\theta+115)$
X^2-287	1148	$X^2+X+(\theta-17)$
$X^2-X-289$	1157	$X^2+(-\theta-25)$
X^2-290	1160	$X^4-21X^2+2\theta X+6$
X^2-291	1164	$X^4+(\theta-20)X^2+(\theta-15)X+(-6\theta+102)$
$X^2-X-291$	1165	$X^2+(-\theta-59)$
$X^2-X-293$	1173	$X^2+(-\theta-21)$
X^2-295	1180	$X^2+X+(\theta-60)$
$X^2-X-296$	1185	$X^2+(\theta-61)$
$X^2-X-297$	1189	$X^2+(-\theta-17)$
X^2-298	1192	$X^2+X+(\theta-39)$
X^2-299	1196	$X^2+X+(-\theta-26)$
$X^2-X-301$	1205	$X^2+(-\theta-61)$
$X^2-X-302$	1209	$X^2+(\theta-27)$
X^2-303	1212	$X^2-X+(\theta-28)$
$X^2-X-305$	1221	$X^4-18X^2-3X+(2\theta+36)$
$X^2-X-307$	1229	$X^3-X^2+(\theta-21)X+(\theta-15)$
X^2-310	1240	$X^2+X+(-\theta-63)$
$X^2-X-310$	1241	$X^2+(-\theta-22)$
$X^2-X-311$	1245	$X^2+(-\theta-63)$
X^2-314	1256	$X^2+X+(\theta-41)$
$X^2-X-314$	1257	$X^3-X^2+(-\theta-18)X+(2\theta+35)$
$X^2-X-315$	1261	$X^2+(\theta-28)$
$X^2-X-316$	1265	$X^2+(-\theta-64)$
X^2-318	1272	$X^2-X+(\theta-19)$
X^2-319	1276	$X^2+X+(-\theta-18)$
$X^2-X-320$	1281	$X^2+(\theta-21)$
$X^2-X-321$	1285	$X^2+(\theta-66)$
X^2-322	1288	$X^4+(-\theta-19)X^2+(-\theta-18)X+(4\theta+72)$
X^2-323	1292	$X^4-2X^3+(-\theta-18)X^2+(\theta+19)X+(5\theta+90)$
$X^2-X-324$	1297	$X^{11}-22X^9+166X^7-516X^5+(2\theta-1)X^4+626X^3+$ $(-6\theta+3)X^2-165X+(2\theta-1)$

X^2-326	1304	$X^3-X^2+(\theta-18)X+(2\theta-36)$
X^2-327	1308	$X^2+X+(-\theta-30)$
$X^2-X-327$	1309	$X^2+(\theta-24)$
$X^2-X-328$	1313	$X^4+(-\theta-19)X^2+(3\theta+53)$
X^2-330	1320	$X^4-23X^2+2\theta X+15$
X^2-335	1340	$X^2-X+(\theta-68)$
$X^2-X-336$	1345	$X^6-3X^5-15X^4+(2\theta+34)X^3+(-3\theta-37)X^2+(\theta+20)X-5$
$X^2-X-338$	1353	$X^2+(\theta-19)$
X^2-339	1356	$X^2-X+(-\theta-31)$
$X^2-X-341$	1365	$X^4-2X^3-18X^2+(2\theta+18)X+(-\theta-20)$
$X^2-X-343$	1373	$X^3-X^2+(-\theta-21)X+(3\theta+55)$
X^2-346	1384	$X^6-19X^4+55X^2+2\theta X+2$
$X^2-X-346$	1385	$X^2+(-\theta-70)$
$X^2-X-348$	1393	$X^5-17X^3+58X+(2\theta-1)$
$X^2-X-351$	1405	$X^2+(\theta-72)$
X^2-354	1416	$X^2-X+(-\theta-46)$
$X^2-X-354$	1417	$X^2+(-\theta-30)$
X^2-355	1420	$X^2-X+(-\theta-72)$
$X^2-X-357$	1429	$X^5-X^4-18X^3+24X^2+(-\theta+52)X+(3\theta-50)$
X^2-359	1436	$X^3-X^2+(\theta-19)X+(-2\theta+38)$
X^2-362	1448	$X^2-X+(\theta-47)$
X^2-366	1464	$X^2+X+(-\theta-21)$
$X^2-X-366$	1465	$X^2+(-\theta-74)$
$X^2-X-367$	1469	$X^2+(\theta-32)$
X^2-370	1480	$X^4-25X^2+2\theta X+26$
X^2-371	1484	$X^2+X+(-\theta-20)$
$X^2-X-372$	1489	$X^3-X^2+(\theta-21)X+1$
X^2-374	1496	$X^2-X+(\theta-26)$
$X^2-X-376$	1505	$X^2+(\theta-77)$
$X^2-X-377$	1509	$X^3-22X+(2\theta-1)$
$X^2-X-378$	1513	$X^2+(-\theta-26)$
$X^2-X-379$	1517	$X^2+(-\theta-19)$
$X^2-X-383$	1533	$X^2+(\theta-24)$
$X^2-X-384$	1537	$X^2+(\theta-21)$
X^2-386	1544	$X^2-X+(-\theta-50)$
$X^2-X-386$	1545	$X^2+(-\theta-78)$
X^2-390	1560	$X^4-21X^2+2\theta X-14$
X^2-391	1564	$X^2-X+(-\theta-27)$
$X^2-X-391$	1565	$X^2+(\theta-80)$
X^2-394	1576	$X^2-X+(-\theta-51)$
X^2-395	1580	$X^2-X+(\theta-80)$
$X^2-X-395$	1581	$X^2+(\theta-28)$
$X^2-X-396$	1585	$X^2+(-\theta-80)$
X^2-399	1596	$X^8-20X^6-2\theta X^5+20X^4+6\theta X^3+115X^2+2\theta X+4$
$X^2-X-400$	1601	$X^7-2X^6-20X^5+(\theta+36)X^4+(-2\theta+77)X^3+(-5\theta-118)X^2+(10\theta-4)X-51$
$X^2-X-401$	1605	$X^2+(\theta-82)$
X^2-402	1608	$X^2+X+(\theta-52)$
X^2-403	1612	$X^2+X+(\theta-34)$
X^2-406	1624	$X^2+X+(-\theta-21)$
X^2-407	1628	$X^2+X+(\theta-20)$
X^2-410	1640	$X^4-27X^2+2\theta X+39$

$X^2-X-410$	1641	$X^5-X^4-21X^3+(-\theta+21)X^2+(\theta+60)X+(2\theta-43)$
X^2-411	1644	$X^2+X+(-\theta-37)$
$X^2-X-411$	1645	$X^2+(\theta-84)$
$X^2-X-412$	1649	$X^2+(-\theta-28)$
$X^2-X-413$	1653	$X^2+(\theta-22)$
X^2-415	1660	$X^2+X+(\theta-84)$
X^2-418	1672	$X^2+X+(-\theta-54)$
$X^2-X-419$	1677	$X^4-18X^2+(2\theta-1)X-26$
$X^2-X-421$	1685	$X^2+(\theta-86)$
X^2-426	1704	$X^2+X+(\theta-55)$
$X^2-X-426$	1705	$X^8-21X^6+(\theta-8)X^5+(\theta+80)X^4+(-7\theta+1)X^3+(-\theta+65)X^2+10X-1$
X^2-427	1708	$X^6-X^5-20X^4+31X^3+(\theta+68)X^2+(-3\theta-129)X+(2\theta+36)$
$X^2-X-429$	1717	$X^2+(\theta-30)$
X^2-430	1720	$X^2-X+(-\theta-87)$
$X^2-X-432$	1729	$X^2+(-\theta-36)$
X^2-434	1736	$X^4-19X^2-2\theta X-24$
X^2-435	1740	$X^4-23X^2+2\theta X-6$
$X^2-X-436$	1745	$X^4-X^3+(\theta-22)X^2+(-\theta+22)X+(-8\theta+171)$
$X^2-X-437$	1749	$X^2+(\theta-22)$
X^2-438	1752	$X^4-X^3+(-\theta-24)X^2+3X+(9\theta+189)$
X^2-439	1756	$X^5-X^4-21X^3+5X^2+(2\theta+64)X+(2\theta+48)$
$X^2-X-440$	1761	$X^7-3X^6-22X^5+(\theta+84)X^4-6\theta X^3+(9\theta-164)X^2+(2\theta-34)X+(-6\theta+129)$
$X^2-X-441$	1765	$X^6+X^5-22X^4-18X^3+(-3\theta+88)X^2+(-\theta+48)X+(8\theta-166)$
X^2-442	1768	$X^8-25X^6+2\theta X^5+105X^4-16\theta X^3+294X^2-4\theta X+4$
$X^2-X-442$	1769	$X^2+(\theta-23)$
X^2-443	1772	$X^3-X^2+(\theta-21)X+(2\theta-42)$
$X^2-X-445$	1781	$X^2+(-\theta-37)$
$X^2-X-446$	1785	$X^8-20X^6+121X^4-215X^2+(2\theta-1)X+21$
X^2-447	1788	X^2-3
X^2-451	1804	$X^2+X+(-\theta-21)$
X^2-455	1820	$X^4-23X^2+2\theta X-10$
X^2-458	1832	$X^2+X+(\theta-59)$
$X^2-X-458$	1833	$X^2+(\theta-39)$
X^2-462	1848	$X^4-X^3+(\theta-26)X^2+(-3\theta+63)X+(2\theta-43)$
$X^2-X-463$	1853	$X^2+(-\theta-31)$
X^2-466	1864	$X^2-X+(\theta-60)$
$X^2-X-466$	1865	$X^2+(-\theta-94)$
$X^2-X-467$	1869	$X^2+(-\theta-27)$
X^2-470	1880	$X^2+X+(\theta-95)$
X^2-471	1884	$X^2+X+(\theta-42)$
$X^2-X-471$	1885	$X^4-2X^3-22X^2+(-2\theta+24)X+(\theta-15)$
X^2-474	1896	$X^2+X+(\theta-61)$
$X^2-X-474$	1897	$X^5-X^4-25X^3+(\theta-14)X^2+(3\theta+93)X+49$
$X^2-X-475$	1901	$X^3-X^2+(\theta-25)X+(-3\theta+69)$
$X^2-X-476$	1905	$X^2+(-\theta-96)$
$X^2-X-480$	1921	$X^2+(-\theta-32)$
X^2-482	1928	$X^2+X+(\theta-62)$
$X^2-X-482$	1929	$X^3-X^2+(\theta-24)X+(2\theta-45)$
X^2-483	1932	$X^4-21X^2+2\theta X-20$
$X^2-X-484$	1937	$X^6+(\theta-26)X^4+(-15\theta+341)X^2+(56\theta-1261)$

$X^2 - X - 486$	1945	$X^2 + (-\theta - 98)$
$X^2 - X - 489$	1957	$X^3 + (-\theta - 24)X + (2\theta + 44)$
$X^2 - X - 490$	1961	$X^2 + (\theta - 23)$
$X^2 - X - 491$	1965	$X^2 - 5$
$X^2 - 494$	1976	$X^2 + X + (\theta - 41)$
$X^2 - X - 496$	1985	$X^2 + (-\theta - 100)$
$X^2 - 498$	1992	$X^2 + X + (\theta - 64)$
$X^2 - 499$	1996	$X^5 - 22X^3 + 2\theta X^2 + 5X - 2\theta$

A.2. Corps cubiques

La table suivante donne le corps de classes de Hilbert des 612 corps cubiques réels non principaux de discriminant ≤ 100000. Parmi ces corps, il y en a 290 de nombre de classes 2, 267 de nombre de classes 3, 21 de nombre de classes 4, 18 de nombre de classes 5, 7 de nombre de classes 6, 7 de nombre de classes 7, 1 de nombre de classes 8 et 1 de nombre de classes 9.

$X^3 - X^2 - 9X + 10$	1957	$X^2 + (\theta - 1)X + (-\theta + 1)$
$X^3 - X^2 - 9X + 8$	2597	$X^3 + (-\theta - 1)X^2 + \theta X + (\theta - 1)$
$X^3 - X^2 - 14X + 23$	2777	$X^2 + (\theta^2 + \theta - 13)$
$X^3 - 21X - 28$	3969	$X^3 - \theta X^2 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 5)X + 1$
$X^3 - 21X - 35$	3969	$X^3 + \theta X^2 + (\theta + 2)X + 1$
$X^3 - X^2 - 11X + 12$	3981	$X^2 + X + (\theta - 3)$
$X^3 - 12X - 10$	4212	$X^3 - X^2 + (\theta^2 - \theta - 12)X + (\theta^2 - \theta - 11)$
$X^3 - X^2 - 16X + 8$	4312	$X^3 + (-\theta - 1)X^2 + (\frac{1}{2}\theta^2 + \frac{1}{2}\theta - 4)X - 1$
$X^3 - 14X - 14$	5684	$X^3 - \theta X^2 + (2\theta + 2)$
$X^3 - X^2 - 12X - 1$	6809	$X^2 + (-\theta - 3)$
$X^3 - 12X - 1$	6885	$X^3 + (\theta - 1)X^2 - \theta X - \theta$
$X^3 - X^2 - 23X + 48$	7053	$X^2 + (\theta - 4)$
$X^3 - X^2 - 25X + 45$	7220	$X^3 + (-\theta - 1)X^2 + (\frac{1}{2}\theta^2 + \theta - \frac{9}{2})X + (\frac{-1}{2}\theta^2 - \theta + \frac{17}{2})$
$X^3 - X^2 - 24X - 35$	7537	$X^2 + X + (-\theta - 3)$
$X^3 - X^2 - 17X - 16$	8069	$X^4 + (\theta - 2)X^3 + 2X^2 + (\theta^2 - 4\theta - 5)X + (-\theta^2 + 4\theta + 5)$
$X^3 - X^2 - 30X + 64$	8281	$X^3 + (\theta - 7)X + (\theta - 3)$
$X^3 - X^2 - 30X - 27$	8281	$X^3 + (\theta - 7)X + (\frac{-2}{3}\theta^2 + \frac{8}{3}\theta + 10)$
$X^3 - X^2 - 27X - 43$	8468	$X^2 + X + (-\theta - 3)$
$X^3 - 14X - 9$	8789	$X^2 - X + (\theta - 4)$
$X^3 - 21X - 8$	8829	$X^3 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 7)X^2 + (\frac{-1}{2}\theta^2 - \frac{1}{2}\theta + 14)X + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 9)$
$X^3 - X^2 - 21X - 26$	9301	$X^2 + X + (-\theta - 3)$
$X^3 - 14X - 7$	9653	$X^3 - \theta X^2 + (2\theta + 1)$
$X^3 - X^2 - 23X - 13$	9800	$X^3 + (-\theta - 6)X + (-\theta - 4)$
$X^3 - X^2 - 16X + 22$	9996	$X^3 + (-\theta - 1)X^2 + \theta X + (2\theta - 3)$
$X^3 - X^2 - 18X - 17$	10273	$X^2 + (-\theta - 4)$
$X^3 - X^2 - 17X - 14$	10309	$X^3 + (-\theta - 5)X - 1$
$X^3 - X^2 - 14X - 1$	10889	$X^2 + X + (-\theta - 3)$
$X^3 - X^2 - 15X + 16$	11197	$X^2 + (\theta - 4)$
$X^3 - X^2 - 20X - 22$	11324	$X^2 + X + (-\theta - 3)$
$X^3 - X^2 - 17X - 13$	11348	$X^2 + X + (-\theta - 3)$
$X^3 - X^2 - 30X + 71$	11417	$X^3 + (\theta - 1)X^2 + (-2\theta + 4)X + (\theta - 6)$
$X^3 - X^2 - 15X - 4$	12197	$X^2 + X + (-\theta - 3)$
$X^3 - 23X - 36$	13676	$X^2 + X + (-\theta - 4)$
$X^3 - 39X - 91$	13689	$X^3 - X^2 + (-\theta - 7)X + (-\theta - 1)$

$X^3-39X-26$	13689	$X^3-X^2+(\theta-7)X+(\frac{-1}{2}\theta^2+\frac{3}{2}\theta+12)$
$X^3-X^2-18X-14$	13768	$X^2+X+(-\theta-3)$
$X^3-X^2-16X-6$	13916	$X^3+(-\theta-1)X^2+\theta X+(2\theta+1)$
$X^3-30X-44$	13932	$X^3-X^2+(\frac{1}{2}\theta^2-\theta-16)X+(-\theta^2+2\theta+29)$
$X^3-30X-59$	14013	$X^2+X+(-\theta-4)$
$X^3-16X-9$	14197	$X^2+(-\theta-4)$
$X^3-36X-45$	14661	$X^3-\theta X^2+(\frac{1}{3}\theta^2-1)X+(-\theta-2)$
$X^3-X^2-16X+15$	14945	$X^3+(-\theta-1)X^2+\theta X+(2\theta-2)$
$X^3-X^2-37X+64$	15141	$X^3+(\theta-1)X^2+(\frac{1}{3}\theta^2-\theta-\frac{10}{3})X+(\frac{-1}{3}\theta^2+\frac{7}{3})$
$X^3-X^2-25X+21$	15188	$X^2+X+(\theta-5)$
$X^3-19X-21$	15529	$X^2+X+(-\theta-4)$
$X^3-38X-76$	15884	$X^3+(\frac{1}{2}\theta^2-\theta-19)X+(\frac{1}{2}\theta^2-\theta-17)$
$X^3-16X-1$	16357	$X^4-2X^3+(\theta-3)X^2+(-\theta+4)X+(-\theta+4)$
$X^3-37X-83$	16609	$X^2+(\theta^2-3\theta-29)$
$X^3-28X-28$	16660	$X^3+(-\theta-7)X+(\frac{-1}{2}\theta^2-\theta+5)$
$X^3-X^2-16X+1$	16905	$X^3+(-\theta-1)X^2+\theta X+2\theta$
$X^3-32X-65$	16997	$X^2+(-\theta-4)$
$X^3-X^2-30X-49$	17417	$X^2+(-\theta-4)$
$X^3-40X-94$	17428	$X^2+X+(-\theta-4)$
$X^3-X^2-22X+39$	17609	$X^2+X+(\theta-5)$
$X^3-X^2-44X-69$	17689	$X^3+(\theta-9)X+(\frac{-2}{3}\theta^2+\frac{10}{3}\theta+14)$
$X^3-X^2-44X+64$	17689	$X^3+(\theta-9)X+(\theta-5)$
$X^3-X^2-17X+16$	17989	$X^2+X+(\theta-5)$
$X^3-X^2-38X+88$	18097	$X^2+X+(\theta-5)$
$X^3-X^2-23X-27$	18228	$X^3+(\theta^2-2\theta-22)X+(2\theta^2-5\theta-38)$
$X^3-39X-78$	18252	$X^3+(\frac{-1}{2}\theta^2+\frac{3}{2}\theta+13)X^2+(\frac{-1}{2}\theta^2+\frac{1}{2}\theta+19)X+(\frac{-1}{2}\theta^2+\frac{3}{2}\theta+17)$
$X^3-21X-26$	18792	$X^3+(-\theta-1)X^2+\theta X+(2\theta+3)$
$X^3-X^2-41X-85$	19220	$X^3+(-\theta-6)X+(-\theta-3)$
$X^3-X^2-35X+88$	19429	$X^2+X+(\theta^2+2\theta-29)$
$X^3-X^2-17X-1$	19604	$X^3+(\theta-1)X^2-\theta X-\theta$
$X^3-36X-18$	19764	$X^3-\theta X^2+(\frac{1}{3}\theta^2-1)X+(-\theta-1)$
$X^3-X^2-39X-36$	19821	$X^4-X^3-7X^2+(\frac{1}{3}\theta^2-\frac{1}{3}\theta-7)X+(\frac{1}{3}\theta^2-\frac{4}{3}\theta-3)$
$X^3-28X-50$	20308	$X^2+X+(\theta^2-2\theta-24)$
$X^3-36X-9$	20493	$X^3-\theta X^2+(\frac{1}{3}\theta^2-1)X-\theta$
$X^3-36X-1$	20733	$X^5-7X^3+(\frac{-1}{3}\theta^2-\frac{1}{3}\theta+\frac{32}{3})X^2+(\frac{1}{3}\theta^2-\frac{2}{3}\theta-\frac{17}{3})X+1$
$X^3-42X-63$	21021	$X^3+(-\theta-7)X+(\frac{1}{3}\theta^2+\theta-4)$
$X^3-X^2-22X-22$	21208	$X^2+X+(-\theta-5)$
$X^3-X^2-36X+18$	21212	$X^7+2X^6-7X^5+(\frac{1}{3}\theta^2-\frac{1}{3}\theta-20)X^4+(\frac{2}{3}\theta^2-\frac{2}{3}\theta-8)X^3$ $+(\frac{-1}{3}\theta^2+\frac{1}{3}\theta+11)X^2+(\frac{-1}{3}\theta^2+\frac{1}{3}\theta+7)X+1$
$X^3-X^2-28X+24$	21308	$X^4+(\theta-1)X^3+(\frac{1}{2}\theta^2-\frac{1}{2}\theta-5)X^2+(\theta-1)X+1$
$X^3-X^2-37X-55$	21364	$X^3+(\frac{-1}{2}\theta^2+2\theta+\frac{3}{2})X+(\theta^2-4\theta-12)$
$X^3-X^2-29X+64$	21469	$X^2+X+(\theta-5)$
$X^3-30X-28$	21708	$X^3+(\frac{-1}{2}\theta^2+\theta+10)X^2+(\frac{-1}{2}\theta^2-\theta+23)X+(-\theta^2+2\theta+23)$
$X^3-X^2-44X+20$	21737	$X^2+X+(\frac{1}{4}\theta^2+\frac{1}{4}\theta-\frac{27}{2})$
$X^3-X^2-30X-20$	21805	$X^3+(\frac{1}{2}\theta^2-\frac{1}{2}\theta-17)X+(-\theta^2+2\theta+27)$
$X^3-24X-35$	22221	$X^2+X+(-\theta-4)$
$X^3-26X-42$	22676	$X^2+X+(-\theta-4)$
$X^3-20X-18$	23252	$X^2+X+(-\theta-4)$
$X^3-X^2-18X-1$	23297	$X^2+(-\theta-4)$
$X^3-X^2-44X-95$	23377	$X^2+X+(\theta^2-4\theta-33)$
$X^3-X^2-36X+91$	23665	$X^2+X+(\theta-5)$
$X^3-20X-17$	24197	$X^2+(-\theta-4)$

$X^3 - X^2 - 43X + 120$	24437	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 19X - 6$	24749	$X^2 + X + (\theta - 5)$
$X^3 - 26X - 41$	24917	$X^2 + (-\theta - 5)$
$X^3 - 21X - 21$	25137	$X^3 - \theta X^2 + (3\theta + 3)$
$X^3 - X^2 - 43X - 91$	25492	$X^2 + (\theta^2 - 4\theta - 33)$
$X^3 - 22X - 25$	25717	$X^2 + X + (-\theta - 4)$
$X^3 - 24X - 33$	25893	$X^2 + (-\theta - 4)$
$X^3 - 23X - 29$	25961	$X^2 + (\theta - 6)$
$X^3 - 30X - 55$	26325	$X^3 + X^2 + (-\theta^2 + 4\theta + 11)X + (-\theta^2 + 4\theta + 14)$
$X^3 - 42X - 84$	26460	$X^3 - \theta X^2 + (\frac{1}{2}\theta^2 - 10)X + (\frac{-1}{2}\theta^2 + \theta + 8)$
$X^3 - 36X - 77$	26541	$X^2 + X + (-\theta - 4)$
$X^3 - 30X - 8$	26568	$X^3 + X^2 + (\frac{1}{2}\theta^2 - 18)X + (\theta^2 - 33)$
$X^3 - X^2 - 54X + 169$	26569	$X^4 + (\theta - 8)X^2 + 1$
$X^3 - X^2 - 38X - 73$	26825	$X^2 + (-\theta - 4)$
$X^3 - X^2 - 22X + 33$	26873	$X^2 + (\theta - 6)$
$X^3 - 19X - 4$	27004	$X^2 + X + (-\theta - 4)$
$X^3 - 21X - 19$	27297	$X^3 + (\theta - 1)X^2 - \theta X + (-2\theta - 2)$
$X^3 - 29X - 51$	27329	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 30X + 8$	27881	$X^3 + (-\theta - 1)X^2 + \theta X + (4\theta - 1)$
$X^3 - X^2 - 30X + 12$	27885	$X^3 - X^2 + (-\theta - 7)X + (\frac{1}{2}\theta^2 + \frac{3}{2}\theta - 4)$
$X^3 - 28X - 47$	28165	$X^5 - X^4 + (-\theta - 8)X^3 + 3X^2 + (4\theta + 16)X + (\theta + 4)$
$X^3 - X^2 - 41X + 93$	28212	$X^3 + X^2 + (\theta - 7)X + (-\theta + 4)$
$X^3 - X^2 - 53X + 153$	28212	$X^3 - X^2 + (\theta - 7)X + (-2\theta + 11)$
$X^3 - X^2 - 37X - 47$	28212	$X^3 + (\theta - 1)X^2 + (\frac{1}{2}\theta^2 - \theta - \frac{13}{2})X + \theta$
$X^3 - X^2 - 43X + 103$	28392	$X^3 - 7X + \theta$
$X^3 - X^2 - 22X - 17$	28473	$X^2 + (-\theta - 4)$
$X^3 - 34X - 69$	28669	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 29X - 42$	28677	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 37X - 69$	29204	$X^3 + (\theta^2 - 4\theta - 33)X + (-2\theta^2 + 6\theta + 54)$
$X^3 - 26X - 39$	29237	$X^3 - \theta X^2 + (2\theta + 3)$
$X^3 - 57X - 19$	29241	$X^3 + X^2 + (\theta - 9)X + (\frac{-2}{5}\theta^2 + \frac{11}{5}\theta + \frac{31}{5})$
$X^3 - 57X - 152$	29241	$X^3 + X^2 + (\frac{1}{2}\theta^2 - \frac{5}{2}\theta - 28)X + (\theta^2 - 3\theta - 45)$
$X^3 - X^2 - 23X + 36$	29253	$X^3 + (-\theta - 1)X^2 + \theta X + (3\theta - 5)$
$X^3 - 20X - 9$	29813	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 23X - 20$	30037	$X^3 + (-\theta - 1)X^2 + \theta X + (3\theta + 3)$
$X^3 - X^2 - 48X + 141$	30273	$X^2 + (\theta - 5)$
$X^3 - X^2 - 22X + 30$	30776	$X^2 + X + (\theta - 5)$
$X^3 - 35X - 42$	30968	$X^3 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 22)X + (-\theta^2 + \theta + 35)$
$X^3 - X^2 - 40X + 106$	30972	$X^2 + X + (\theta - 5)$
$X^3 - 25X - 34$	31288	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 48X - 63$	31425	$X^3 - X^2 + (\frac{1}{3}\theta^2 - \frac{4}{3}\theta - 18)X + (\frac{1}{3}\theta^2 - \frac{1}{3}\theta - 12)$
$X^3 - 45X - 55$	31425	$X^3 + (\theta - 8)X + (\frac{1}{3}\theta^2 - \frac{5}{3}\theta - \frac{17}{3})$
$X^3 - X^2 - 38X - 48$	31425	$X^3 + \theta X^2 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 7)X + (\theta + 2)$
$X^3 - 35X - 72$	31532	$X^4 - X^3 + (-\theta - 6)X^2 + X + 1$
$X^3 - 21X - 14$	31752	$X^3 - \theta X^2 + (3\theta + 2)$
$X^3 - 20X - 1$	31973	$X^5 + (\theta - 8)X^3 + (\theta - 5)X^2 + (-\theta + 7)X + 1$
$X^3 - X^2 - 34X - 24$	32009	$X^3 + X^2 - 6X + (-\theta - 1)$
$X^3 - 41X - 95$	32009	$X^3 - X^2 + (-\theta - 6)X + (\theta + 4)$
$X^3 - X^2 - 20X - 1$	32009	$X^3 + (-\theta - 6)X + (\theta + 3)$
$X^3 - X^2 - 52X + 159$	32009	$X^3 + X^2 + (\theta^2 + 3\theta - 42)X + (2\theta^2 + 6\theta - 82)$
$X^3 - X^2 - 36X + 89$	32081	$X^2 + (\theta - 5)$
$X^3 - 30X - 53$	32157	$X^3 - X^2 - 9X + (\theta^2 - 4\theta - 20)$

$X^3 - X^2 - 20X + 14$	32204	$X^5 + X^4 + (\theta - 8)X^3 + (\theta - 7)X^2 + 3X + 1$
$X^3 - 42X - 14$	32340	$X^3 + (\frac{1}{3}\theta^2 - \frac{1}{3}\theta - \frac{59}{3})X + (\frac{-2}{3}\theta^2 + \frac{2}{3}\theta + \frac{97}{3})$
$X^3 - X^2 - 20X + 1$	32737	$X^2 + (\theta - 5)$
$X^3 - X^2 - 21X + 22$	32821	$X^2 + X + (\theta - 5)$
$X^3 - 49X - 112$	32977	$X^3 + (-\theta - 12)X + (-\theta - 8)$
$X^3 - 25X - 33$	33097	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 44X + 57$	33369	$X^3 + (\frac{-1}{3}\theta^2 - \frac{7}{3}\theta - 1)X + (-\theta^2 - 5\theta + 12)$
$X^3 - 39X - 62$	33372	$X^3 - X^2 + (\frac{-1}{2}\theta^2 + \frac{5}{2}\theta + 3)X + 3$
$X^3 - X^2 - 45X - 79$	33428	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 24X + 38$	33452	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 47X + 136$	33709	$X^2 + X + (-\theta^2 - 4\theta + 27)$
$X^3 - 22X - 18$	33844	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 37X - 39$	34196	$X^2 + (-\theta - 5)$
$X^3 - 21X - 10$	34344	$X^3 + (\theta - 1)X^2 - \theta X + (-2\theta - 1)$
$X^3 - X^2 - 33X + 29$	34868	$X^2 + (-\theta - 6)$
$X^3 - X^2 - 43X + 34$	35013	$X^2 + X + (\theta - 7)$
$X^3 - X^2 - 34X - 16$	35401	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 34X - 57$	35537	$X^4 + (-\theta - 6)X^2 + 1$
$X^3 - X^2 - 43X + 25$	35828	$X^3 + (\theta + 1)X^2 + (\frac{1}{3}\theta^2 + \theta - \frac{13}{3})X + (\frac{1}{3}\theta^2 - \frac{10}{3})$
$X^3 - X^2 - 25X - 24$	36677	$X^2 + (-\theta - 5)$
$X^3 - 23X - 21$	36761	$X^2 + X + (-\theta - 4)$
$X^3 - 21X - 1$	37017	$X^3 + (-\theta + 1)X^2 - \theta X + 2\theta$
$X^3 - X^2 - 37X + 92$	37093	$X^3 + (-\theta + 1)X^2 + (\theta^2 - 25)X + (-2\theta^2 - 5\theta + 71)$
$X^3 - X^2 - 53X + 163$	37108	$X^2 + X + (\theta - 5)$
$X^3 - 26X - 35$	37229	$X^4 + X^3 + (-\theta - 6)X^2 - X + 1$
$X^3 - X^2 - 33X - 53$	37300	$X^3 - X^2 - 6X + (-\theta + 4)$
$X^3 - 40X - 90$	37300	$X^3 - X^2 + (-\theta - 6)X + (2\theta + 9)$
$X^3 - X^2 - 44X - 6$	37436	$X^3 + X^2 + (\theta - 12)X + (\frac{1}{3}\theta^2 + \frac{1}{3}\theta - 21)$
$X^3 - 31X - 55$	37489	$X^2 + X + (-\theta - 4)$
$X^3 - 30X - 51$	37773	$X^2 - X + (\theta - 6)$
$X^3 - 28X - 43$	37885	$X^2 + X + (-\theta - 4)$
$X^3 - X^2 - 23X + 29$	38612	$X^3 + (-\theta - 1)X^2 + \theta X + (3\theta - 4)$
$X^3 - X^2 - 37X + 57$	38612	$X^3 + (\theta - 1)X^2 + (\frac{1}{2}\theta^2 - \theta - \frac{25}{2})X + (\frac{1}{2}\theta^2 - \frac{43}{2})$
$X^3 - X^2 - 30X + 62$	38840	$X^5 + X^4 + (-\theta - 7)X^3 + (-\theta^2 - 3\theta + 17)X^2 + (\theta + 6)X + (\theta^2 + 3\theta - 17)$
$X^3 - 45X - 18$	39528	$X^2 + (\frac{1}{3}\theta^2 - 16)$
$X^3 - X^2 - 48X - 88$	39800	$X^2 + X + (\frac{1}{2}\theta^2 - \frac{3}{2}\theta - 21)$
$X^3 - 28X - 42$	40180	$X^3 - \theta X^2 + (4\theta + 6)$
$X^3 - X^2 - 32X + 70$	40396	$X^2 + X + (\theta - 5)$
$X^3 - 54X - 99$	40581	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 49X + 144$	40709	$X^2 + (-\theta^2 - 4\theta + 28)$
$X^3 - 52X - 139$	40765	$X^2 + X + (-\theta - 6)$
$X^3 - 57X - 161$	40905	$X^3 + (-\theta^2 + 4\theta + 38)X^2 + (-\theta^2 + 3\theta + 51)X + (-2\theta^2 + 8\theta + 82)$
$X^3 - X^2 - 53X + 111$	41332	$X^3 + X^2 + (\frac{1}{3}\theta^2 + \frac{1}{3}\theta - 20)X + (\frac{2}{3}\theta^2 + \frac{2}{3}\theta - 37)$
$X^3 - X^2 - 35X - 59$	41332	$X^3 + (\theta^2 - 3\theta - 31)X + 1$
$X^3 - X^2 - 23X - 11$	41332	$X^3 + (-\theta - 8)X + 3$
$X^3 - X^2 - 25X - 21$	41684	$X^2 + X + (-\theta - 5)$
$X^3 - 49X - 126$	41944	$X^3 - 13X + (\theta^2 - 3\theta - 29)$
$X^3 - 59X - 74$	42104	$X^2 + (-\theta - 7)$
$X^3 - X^2 - 26X - 25$	42305	$X^4 - 2X^3 + (-\theta - 6)X^2 + (\theta + 7)X + 2$
$X^3 - X^2 - 43X - 88$	42325	$X^2 + X + (-\theta - 5)$
$X^3 - 38X - 81$	42341	$X^2 + (-\theta - 5)$

$X^3-22X-1$	42565	$X^4+(-\theta-8)X^2+(-\theta^2-2\theta+11)X+(-\theta-4)$
$X^3-25X-27$	42817	$X^3-X^2+(-\theta-6)X+(\theta+4)$
$X^3-61X-179$	42817	$X^3-X^2+(-\theta-6)X+(2\theta+10)$
$X^3-X^2-34X-55$	42817	$X^3+(-\theta-6)X+(\theta+3)$
$X^3-X^2-38X-32$	42817	$X^3-X^2-6X+(-\theta+3)$
$X^3-48X-100$	43092	$X^3+(\frac{-1}{2}\theta^2+\theta+16)X^2+(-\theta^2+3\theta+51)X+(\frac{-3}{2}\theta^2+3\theta+59)$
$X^3-56X-140$	43316	$X^3-13X+(\frac{1}{2}\theta^2-19)$
$X^3-X^2-22X+1$	43449	$X^4-2X^3-5X^2+6X+(\theta+3)$
$X^3-X^2-58X-132$	43757	$X^3+(\frac{1}{2}\theta^2-\frac{5}{2}\theta-28)X+(-\theta^2+3\theta+43)$
$X^3-X^2-56X-4$	43820	$X^2+(-\theta-7)$
$X^3-X^2-22X+6$	44504	$X^2+X+(-\theta-5)$
$X^3-X^2-56X+12$	44616	$X^3+(\theta+1)X^2+(\frac{1}{2}\theta^2+\frac{1}{2}\theta-10)X+(2\theta+7)$
$X^3-X^2-58X+186$	44648	$X^2+X+(\theta^2+3\theta-46)$
$X^3-X^2-27X+46$	44869	$X^2+X+(\theta-5)$
$X^3-39X-46$	45036	$X^3-X^2-10X+(\frac{-1}{2}\theta^2+\frac{5}{2}\theta+20)$
$X^3-X^2-41X-80$	45205	$X^2+(-\theta-5)$
$X^3-X^2-23X+22$	45325	$X^3+(\theta+1)X^2+\theta X+(-3\theta+3)$
$X^3-36X-12$	45684	$X^3-\theta X^2+(\frac{1}{2}\theta^2-7)X+(-\theta-1)$
$X^3-54X-90$	45684	$X^3+(-\theta-9)X+(-\theta-5)$
$X^3-X^2-23X-6$	45717	$X^3+(\theta+1)X^2+\theta X+(-3\theta-1)$
$X^3-X^2-24X+29$	45809	$X^2+(\theta-5)$
$X^3-X^2-26X-23$	45841	$X^2+(\theta-6)$
$X^3-X^2-48X+54$	45868	$X^2+X+(\theta-7)$
$X^3-X^2-54X-112$	46193	$X^2+X+(-\theta-5)$
$X^3-60X-174$	46548	$X^3+X^2+(-\theta-6)X+(-2\theta-10)$
$X^3-36X-4$	46548	$X^3+X^2-6X+(\theta-2)$
$X^3-X^2-47X+134$	46589	$X^5+2X^4-6X^3+(\theta^2+3\theta-41)X^2+(\theta^2+2\theta-32)X-1$
$X^3-X^2-69X-183$	46644	$X^3+(\frac{1}{2}\theta^2-3\theta-\frac{43}{2})X^2+(\frac{1}{2}\theta^2-4\theta-\frac{23}{2})X+1$
$X^3-X^2-43X+116$	46813	$X^3+(-\theta-1)X^2+(\theta^2+2\theta-25)X+(-\theta+1)$
$X^3-X^2-44X+92$	46844	$X^3+(-\theta-12)X+(\theta+10)$
$X^3-X^2-43X-57$	46952	$X^2+X+(-\theta-5)$
$X^3-X^2-38X+94$	47032	$X^2+X+(\theta^2+2\theta-33)$
$X^3-X^2-72X+225$	47089	$X^3+(\theta-13)X+(\frac{1}{3}\theta^2+\frac{5}{3}\theta-21)$
$X^3-X^2-72X-209$	47089	$X^3+(\theta-13)X+(3\theta^2-17\theta-135)$
$X^3-X^2-50X-39$	47353	$X^2+(\frac{1}{3}\theta^2-\frac{2}{3}\theta-17)$
$X^3-X^2-51X-97$	47432	$X^3-13X+(-\theta^2+3\theta+29)$
$X^3-X^2-41X+107$	47636	$X^2+X+(\theta^2+2\theta-35)$
$X^3-X^2-45X+97$	47860	$X^3+(\theta-1)X^2+(\frac{1}{2}\theta^2-\frac{19}{2})X+(\theta-2)$
$X^3-X^2-61X+185$	47860	$X^3+(\frac{1}{2}\theta^2+\theta-\frac{61}{2})X+(\theta^2+3\theta-49)$
$X^3-X^2-51X+81$	47860	$X^3+(-\theta+1)X^2+(\frac{1}{3}\theta^2-\frac{1}{3}\theta-3)X+(-\theta+2)$
$X^3-X^2-60X-44$	47977	$X^2+(-\theta-7)$
$X^3-X^2-49X+58$	48173	$X^2+(\frac{1}{3}\theta^2-\frac{52}{3})$
$X^3-X^2-66X+212$	48389	$X^2+(\frac{1}{2}\theta^2+\frac{3}{2}\theta-29)$
$X^3-X^2-52X+136$	48396	$X^2+(\theta-6)$
$X^3-X^2-51X-118$	48461	$X^6+3X^5+(\theta-6)X^4+(2\theta-17)X^3+(\theta^2-7\theta-14)X^2$ $+(\theta^2-8\theta-5)X+(-3\theta^2+16\theta+83)$
$X^3-63X-144$	48924	$X^3-\theta X^2+(\frac{1}{3}\theta^2-1)X+(-2\theta-5)$
$X^3-31X-51$	48937	$X^2+(-\theta-6)$
$X^3-68X-33$	49133	$X^2+(-\theta-8)$
$X^3-X^2-48X-106$	49292	$X^2+X+(-\theta-5)$
$X^3-X^2-23X+1$	49588	$X^3+(-\theta-1)X^2+\theta X+3\theta$
$X^3-X^2-23X+14$	49757	$X^2+X+(-\theta-5)$

$X^3 - X^2 - 26X + 38$	49928	$X^3 + X^2 + (\theta - 6)X - 1$
$X^3 - 43X - 66$	50104	$X^7 - 3X^6 - 7X^5 + 22X^4 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 11)X^3 + (-\theta^2 + \theta - 1)X^2 + 2X + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 2)$
$X^3 - X^2 - 23X + 4$	50437	$X^2 + X + (\theta - 5)$
$X^3 - 50X - 129$	50693	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 43X - 53$	50700	$X^3 - \theta X^2 + (\frac{1}{2}\theta^2 - \frac{21}{2})X + (-\theta - 6)$
$X^3 - 37X - 75$	50737	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 23X + 8$	50813	$X^3 + (-\theta - 1)X^2 + \theta X + (3\theta - 1)$
$X^3 - 30X - 46$	50868	$X^3 + (\theta - 1)X^2 - \theta X + (-3\theta - 5)$
$X^3 - X^2 - 44X + 88$	50908	$X^2 + (\theta - 6)$
$X^3 - X^2 - 28X - 29$	51153	$X^2 + (-\theta - 7)$
$X^3 - X^2 - 31X + 62$	51181	$X^2 + (-\theta - 6)$
$X^3 - 26X - 26$	52052	$X^6 + (\theta + 1)X^5 + (\theta^2 + \theta - 19)X^4 + (-\theta^2 + 2\theta + 43)X^3 + (\theta^2 + \theta - 19)X^2 + (\theta + 1)X + 1$
$X^3 - X^2 - 30X + 57$	52185	$X^3 + (\theta + 1)X^2 + \theta X + (-4\theta + 8)$
$X^3 - X^2 - 44X - 90$	52332	$X^3 + (\theta - 1)X^2 + (2\theta - 1)X + (3\theta^2 - 15\theta - 61)$
$X^3 - X^2 - 24X + 22$	52396	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 41X + 106$	52645	$X^7 - X^6 - 11X^5 + (\theta^2 + 4\theta - 19)X^4 + (-2\theta^2 - 8\theta + 72)X^3 + (-\theta^2 - 3\theta + 39)X^2 + (\theta - 1)X - 1$
$X^3 - 42X - 56$	52920	$X^3 + (\frac{1}{2}\theta^2 - 2\theta - 28)X + (\frac{-3}{2}\theta^2 + 48)$
$X^3 - X^2 - 24X + 21$	53121	$X^2 + (\theta - 5)$
$X^3 - X^2 - 57X - 142$	53333	$X^2 + X + (-\theta - 5)$
$X^3 - 43X - 99$	53401	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 60X + 48$	53589	$X^2 + X + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta - 18)$
$X^3 - X^2 - 51X + 127$	53704	$X^3 + (\frac{-1}{2}\theta^2 - 3\theta + \frac{13}{2})X + (\frac{-3}{2}\theta^2 - 7\theta + \frac{71}{2})$
$X^3 - X^2 - 25X - 12$	53789	$X^3 - \theta X^2 + (\theta - 1)X + (\theta + 1)$
$X^3 - X^2 - 51X - 27$	54292	$X^3 - 13X + (\frac{1}{3}\theta^2 - \frac{7}{3}\theta - 19)$
$X^3 - 54X - 146$	54324	$X^3 - X^2 + (-\theta - 6)X + (\theta + 5)$
$X^3 - 24X - 6$	54324	$X^3 + X^2 - 6X + (-\theta - 1)$
$X^3 - 36X - 70$	54324	$X^3 - X^2 + (-\theta - 6)X + (2\theta + 9)$
$X^3 - X^2 - 49X + 142$	54381	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 52X - 38$	54492	$X^5 - 2X^4 - 7X^3 + (\frac{-1}{3}\theta^2 + \theta + \frac{64}{3})X^2 + (\frac{1}{3}\theta^2 - \theta - \frac{40}{3})X - 1$
$X^3 - 28X - 35$	54733	$X^3 - \theta X^2 + (4\theta + 5)$
$X^3 - 37X - 74$	54760	$X^3 + X^2 + (\theta - 7)X + (\theta^2 - 3\theta - 27)$
$X^3 - 38X - 4$	54764	$X^2 + X + (\theta - 6)$
$X^3 - X^2 - 58X - 146$	55272	$X^3 + (-\theta^2 + 5\theta + 23)X + (2\theta^2 - 10\theta - 61)$
$X^3 - X^2 - 40X + 101$	55297	$X^2 + (\theta - 5)$
$X^3 - X^2 - 24X - 1$	55409	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 50X - 113$	55585	$X^2 + X + (\theta^2 - 4\theta - 39)$
$X^3 - 68X - 211$	55661	$X^2 + X + (\theta^2 - 4\theta - 52)$
$X^3 - X^2 - 53X + 137$	55700	$X^3 - 7X + (-\theta - 1)$
$X^3 - X^2 - 73X - 213$	55700	$X^3 - X^2 + (\theta^2 - 5\theta - 54)X + (-2\theta^2 + 10\theta + 106)$
$X^3 - X^2 - 54X + 90$	55768	$X^7 - 2X^6 + (\frac{-1}{3}\theta^2 + \frac{1}{3}\theta)X^5 + (\frac{2}{3}\theta^2 - \frac{8}{3}\theta + 6)X^4 + (\theta^2 + 2\theta - 9)X^3 + (\frac{-7}{3}\theta^2 + \frac{22}{3}\theta - 5)X^2 + (\frac{-2}{3}\theta^2 - \frac{16}{3}\theta + 11)X + (2\theta^2 - 4\theta + 1)$
$X^3 - X^2 - 70X - 199$	56137	$X^2 + (\theta^2 - 5\theta - 51)$
$X^3 - X^2 - 69X + 198$	56333	$X^2 + X + (\frac{1}{3}\theta^2 + \frac{2}{3}\theta - 21)$
$X^3 - X^2 - 25X + 26$	56677	$X^6 - X^5 - 9X^4 + (-\theta^2 + 26)X^3 + (2\theta^2 - 28)X^2 + (-\theta + 13)X + (-\theta - 1)$
$X^3 - 75X - 170$	56700	$X^3 + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta - \frac{25}{2})X^2 + (\frac{-1}{2}\theta^2 + \frac{5}{2}\theta + 44)X + (\frac{3}{4}\theta^2 - \frac{3}{4}\theta - \frac{89}{2})$
$X^3 - X^2 - 28X + 45$	56777	$X^2 + X + (-\theta - 7)$
$X^3 - X^2 - 39X - 70$	57077	$X^2 + X + (-\theta - 5)$
$X^3 - 72X - 190$	57588	$X^3 + (-\theta - 9)X + (\theta + 6)$

$X^3 - X^2 - 71X + 45$	57588	$X^3 - 9X + (\frac{-1}{5}\theta^2 - \frac{2}{5}\theta + 9)$
$X^3 - X^2 - 53X + 75$	57588	$X^3 + (\frac{1}{3}\theta^2 + \frac{1}{3}\theta - 21)X + (\frac{1}{3}\theta^2 + \frac{1}{3}\theta - 18)$
$X^3 - X^2 - 35X + 78$	57909	$X^2 + X + (\theta - 5)$
$X^3 - 53X - 116$	58049	$X^2 + X + (-\theta - 6)$
$X^3 - 47X - 115$	58217	$X^2 + (-\theta - 6)$
$X^3 - 26X - 21$	58397	$X^4 - 2X^3 - 5X^2 + 6X + (-\theta + 4)$
$X^3 - X^2 - 25X + 24$	58469	$X^8 - 4X^7 + (\theta - 5)X^6 + (-3\theta + 29)X^5 + (-2\theta + 4)X^4 + (9\theta - 61)X^3 + \theta X^2 + (-6\theta + 36)X + (-2\theta + 11)$
$X^3 - X^2 - 51X + 36$	59045	$X^3 + (\theta - 17)X + (\frac{-2}{3}\theta^2 + \frac{8}{3}\theta + 21)$
$X^3 - X^2 - 30X - 34$	59192	$X^3 + (-\theta - 1)X^2 + \theta X + (4\theta + 5)$
$X^3 - X^2 - 34X + 73$	59457	$X^2 + (\theta - 6)$
$X^3 - 59X - 168$	59468	$X^2 + X + (-\theta^2 + 5\theta + 32)$
$X^3 - X^2 - 65X - 176$	59749	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 42X + 109$	60169	$X^2 + X + (\theta - 5)$
$X^3 - 57X - 136$	60345	$X^3 - X^2 + (\frac{1}{2}\theta^2 - \frac{5}{2}\theta - 32)X + (-\theta^2 + 5\theta + 63)$
$X^3 - X^2 - 28X + 43$	60513	$X^2 + X + (\theta - 5)$
$X^3 - 63X - 30$	60993	$X^2 + X + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta - \frac{33}{2})$
$X^3 - X^2 - 64X - 36$	61004	$X^2 + X + (-\theta - 7)$
$X^3 - X^2 - 82X + 64$	61009	$X^3 + (\theta - 11)X + (\frac{-1}{3}\theta^2 + 2\theta + \frac{31}{3})$
$X^3 - X^2 - 82X + 311$	61009	$X^3 + (\theta - 11)X + (-2\theta + 8)$
$X^3 - 59X - 146$	61496	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 37X + 86$	61909	$X^2 + (\theta - 7)$
$X^3 - X^2 - 25X + 19$	62004	$X^3 - X^2 + (\theta - 7)X + 1$
$X^3 - X^2 - 59X + 189$	62004	$X^3 - X^2 + (\theta - 7)X + (\theta - 4)$
$X^3 - X^2 - 57X - 141$	62004	$X^3 - 7X + (-\theta + 2)$
$X^3 - 56X - 154$	62132	$X^3 + (-\theta^2 + 5\theta + 23)X + (-2\theta^2 + 10\theta + 61)$
$X^3 - X^2 - 40X + 36$	62168	$X^4 + (-\theta - 1)X^3 + (\frac{1}{2}\theta^2 + \frac{1}{2}\theta - 8)X^2 + (-\theta - 1)X + 1$
$X^3 - 63X - 14$	62181	$X^3 + (\theta - 15)X + (\frac{-1}{4}\theta^2 - \frac{3}{4}\theta + \frac{45}{2})$
$X^3 - X^2 - 75X + 100$	62341	$X^4 + (\frac{-1}{5}\theta^2 + \frac{1}{5}\theta + 10)X^3 + (\frac{-2}{5}\theta^2 - \frac{8}{5}\theta + 36)X^2 + (\frac{-3}{5}\theta^2 + \frac{8}{5}\theta + 39)X + 9$
$X^3 - 25X - 1$	62473	$X^2 + (-\theta - 7)$
$X^3 - X^2 - 47X - 100$	62501	$X^3 + (-\theta - 9)X + (-2\theta - 11)$
$X^3 - X^2 - 29X - 28$	62501	$X^3 + \theta X^2 + (\theta + 1)X + (-\theta - 1)$
$X^3 - 26X - 17$	62501	$X^3 - X^2 + (-\theta - 9)X + (\theta + 10)$
$X^3 - X^2 - 41X + 104$	62501	$X^9 + 2X^8 + (-\theta - 12)X^7 + (-2\theta - 25)X^6 + (\theta^2 + 9\theta + 22)X^5 + (\theta^2 + 17\theta + 91)X^4 + (-7\theta^2 - 28\theta + 143)X^3 + (-8\theta^2 - 50\theta + 26)X^2 + (10\theta^2 + 26\theta - 308)X + (12\theta^2 + 45\theta - 269)$
$X^3 - 30X - 41$	62613	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 37X - 61$	62644	$X^3 + (-\theta - 6)X + (\theta + 4)$
$X^3 - 46X - 110$	62644	$X^3 - X^2 + (-\theta - 6)X + (\theta + 5)$
$X^3 - X^2 - 25X - 1$	62644	$X^3 + X^2 - 6X + (\theta - 2)$
$X^3 - X^2 - 43X + 113$	63028	$X^3 + X^2 + (\theta - 7)X - 2$
$X^3 - 76X - 236$	63028	$X^3 + X^2 + (\frac{1}{2}\theta^2 - 2\theta - 32)X + (\theta^2 - 4\theta - 62)$
$X^3 - 40X - 12$	63028	$X^3 - 7X + \theta$
$X^3 - X^2 - 64X + 214$	63564	$X^5 + 2X^4 - 9X^3 + (\theta - 14)X^2 + (-\theta^2 - 2\theta + 52)X - 1$
$X^3 - X^2 - 71X - 203$	63796	$X^2 + (-\theta^2 + 6\theta + 39)$
$X^3 - X^2 - 28X + 41$	64033	$X^2 + (\theta - 5)$
$X^3 - X^2 - 56X + 90$	64220	$X^3 + (\theta - 1)X^2 + (\frac{1}{3}\theta^2 - \frac{2}{3}\theta - 6)X - 5$
$X^3 - X^2 - 32X + 62$	64268	$X^2 - \theta X + (-\theta + 3)$
$X^3 - 35X - 63$	64337	$X^3 - \theta X^2 + (5\theta + 9)$
$X^3 - X^2 - 28X - 22$	64348	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 53X - 124$	64373	$X^2 + (-\theta - 5)$

$X^3 - X^2 - 69X - 144$	64389	$X^3 + (-\theta - 9)X + (2\theta + 11)$
$X^3 - X^2 - 31X + 57$	64436	$X^2 + X + (\theta - 5)$
$X^3 - 39X - 80$	64476	$X^3 + (\theta + 1)X^2 + \theta X + (-4\theta - 9)$
$X^3 - X^2 - 74X - 217$	65057	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 51X + 119$	65144	$X^5 - X^4 + (\theta - 9)X^3 + (-\theta + 6)X^2 + (-2\theta + 13)X + (\theta - 6)$
$X^3 - 43X - 46$	65224	$X^2 + (-\theta - 6)$
$X^3 - X^2 - 54X + 63$	65233	$X^4 + (-\theta + 1)X^3 + (\frac{1}{3}\theta^2 - \frac{1}{3}\theta - 4)X^2 + (-\theta + 1)X + 1$
$X^3 - 44X - 101$	65309	$X^2 + X + (-\theta - 6)$
$X^3 - 75X - 154$	65448	$X^3 + (\frac{-1}{4}\theta^2 + \frac{5}{4}\theta + \frac{25}{2})X^2 + (-2\theta + 19)X + (\frac{-3}{4}\theta^2 + \frac{15}{4}\theta + \frac{65}{2})$
$X^3 - 26X - 13$	65741	$X^3 + \theta X^2 + (-2\theta - 1)$
$X^3 - X^2 - 53X - 95$	65908	$X^3 + (-\theta - 8)X + 1$
$X^3 - X^2 - 59X - 75$	65908	$X^3 + X^2 + (\frac{1}{3}\theta^2 - \frac{2}{3}\theta - 21)X + (\frac{2}{3}\theta^2 - \frac{4}{3}\theta - 39)$
$X^3 - X^2 - 73X + 245$	65908	$X^3 - X^2 - 8X + (-\theta + 2)$
$X^3 - X^2 - 42X - 24$	66081	$X^2 + X + (\theta - 7)$
$X^3 - X^2 - 27X + 33$	66228	$X^2 + X + (\theta - 7)$
$X^3 - 29X - 34$	66344	$X^2 + X + (\theta - 6)$
$X^3 - X^2 - 64X + 32$	66376	$X^5 - 2X^4 - 10X^3 + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta + 7)X^2 + (\frac{-1}{4}\theta^2 + \frac{1}{4}\theta + 10)X - 3$
$X^3 - X^2 - 30X + 51$	66417	$X^3 + (\theta - 1)X^2 - \theta X + (-2\theta + 4)$
$X^3 - 48X - 118$	66420	$X^3 + X^2 + (\theta^2 - 3\theta - 44)X + (-2\theta^2 + 6\theta + 79)$
$X^3 - 74X - 224$	66536	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 37X - 60$	66581	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 39X + 94$	66589	$X^5 - X^4 - 9X^3 + (-\theta^2 - 2\theta + 33)X^2 + (\theta^2 + \theta - 24)X + 3$
$X^3 - X^2 - 32X + 61$	67009	$X^2 + (\theta - 5)$
$X^3 - 26X - 11$	67037	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 86X + 211$	67081	$X^3 + (\theta - 15)X + (-2\theta + 16)$
$X^3 - X^2 - 86X - 48$	67081	$X^3 + (\theta - 15)X + (\frac{-1}{3}\theta^2 + \frac{8}{3}\theta + 3)$
$X^3 - X^2 - 41X + 103$	67348	$X^2 + (\theta^2 + 2\theta - 36)$
$X^3 - X^2 - 57X - 54$	67741	$X^2 + X + (-\theta - 7)$
$X^3 - X^2 - 63X - 145$	67868	$X^3 + (-\theta - 8)X + 1$
$X^3 - 26X - 9$	68117	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 26X + 22$	68296	$X^2 + X + (\theta - 5)$
$X^3 - 46X - 109$	68557	$X^2 + (-\theta - 5)$
$X^3 - 42X - 28$	68796	$X^3 + (\frac{1}{2}\theta^2 - \theta - 28)X + (\frac{-3}{2}\theta^2 + 54)$
$X^3 - 59X - 142$	69272	$X^2 + (-\theta - 6)$
$X^3 - 57X - 65$	69633	$X^2 + (-\theta - 7)$
$X^3 - X^2 - 37X + 84$	69749	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 31X - 34$	69805	$X^2 + (-\theta - 6)$
$X^3 - 49X - 84$	70021	$X^3 - 16X + (\frac{-1}{2}\theta^2 + \frac{5}{2}\theta + 26)$
$X^3 - 63X - 117$	70065	$X^3 - \theta X^2 + (\frac{1}{3}\theta^2 - 1)X + (-2\theta - 4)$
$X^3 - X^2 - 39X - 67$	70292	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 42X + 107$	70313	$X^2 + X + (\theta^2 + 2\theta - 37)$
$X^3 - X^2 - 30X + 49$	70729	$X^2 + (\theta - 6)$
$X^3 - X^2 - 67X - 184$	70789	$X^2 + X + (-\theta - 5)$
$X^3 - 30X - 37$	71037	$X^3 + (-\theta + 1)X^2 - \theta X + (3\theta + 4)$
$X^3 - X^2 - 76X + 26$	71164	$X^2 + X + (\frac{1}{5}\theta^2 - \frac{81}{5})$
$X^3 - X^2 - 83X + 316$	71293	$X^2 + (\theta - 8)$
$X^3 - X^2 - 58X + 183$	71393	$X^3 + (-\theta^2 - 5\theta + 29)X + (-3\theta^2 - 13\theta + 104)$
$X^3 - X^2 - 65X + 197$	71540	$X^6 - X^5 - 10X^4 + (\frac{1}{2}\theta^2 + 2\theta - \frac{23}{2})X^3 + (-\theta^2 - 5\theta + 58)X^2 + (\frac{-1}{2}\theta^2 + \frac{45}{2})X + (\theta - 6)$
$X^3 - X^2 - 47X + 130$	71701	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 35X + 74$	71789	$X^2 - \theta X + (-\theta + 3)$
$X^3 - 65X - 195$	71825	$X^3 + (-\theta - 12)X + (2\theta + 6)$

$X^3-X^2-27X-10$	71861	$X^2+(-\theta-6)$
$X^3-X^2-33X-42$	72093	$X^2+X+(\theta-7)$
$X^3-44X-44$	72116	$X^2+X+(-\theta-6)$
$X^3-X^2-32X+59$	72329	$X^3-X^2+(\theta-7)X+(\theta-3)$
$X^3-X^2-34X+69$	72329	$X^3-X^2+(\theta-7)X+2$
$X^3-X^2-80X+299$	72329	$X^6+X^5+(\theta-12)X^4+(\theta-8)X^3+(-2\theta+21)X^2$ $+(-2\theta+11)X-2$
$X^3-X^2-46X-48$	72329	$X^3-7X+(-\theta+1)$
$X^3-X^2-43X+51$	72332	$X^3+(-\theta-10)X+(-2\theta-11)$
$X^3-36X-65$	72549	$X^2+(-\theta-8)$
$X^3-77X-21$	72569	$X^3+\theta X^2+(\frac{3}{5}\theta^2-\frac{1}{5}\theta-\frac{114}{5})X+(\frac{-3}{5}\theta^2+\frac{11}{5}\theta+\frac{219}{5})$
$X^3-42X-91$	72765	$X^3-\theta X^2+(6\theta+13)$
$X^3-X^2-29X+42$	72861	$X^2+X+(\theta-5)$
$X^3-X^2-80X+122$	73148	$X^2+X+(\theta-9)$
$X^3-X^2-56X-27$	73177	$X^3+(\theta-9)X+(\frac{1}{3}\theta^2-\frac{5}{3}\theta-9)$
$X^3-X^2-27X+26$	73949	$X^2+X+(-\theta-5)$
$X^3-X^2-72X-153$	74137	$X^3+(\frac{1}{3}\theta^2-\frac{7}{3}\theta-32)X+(\frac{2}{3}\theta^2-\frac{14}{3}\theta-60)$
$X^3-X^2-69X+180$	74253	$X^2+X+(\theta-7)$
$X^3-X^2-81X-235$	74420	$X^3+(-\theta-11)X+(-2\theta-8)$
$X^3-X^2-27X-7$	74708	$X^2+X+(-\theta-5)$
$X^3-X^2-68X-32$	74713	$X^2+X+(\frac{1}{4}\theta^2-\frac{1}{4}\theta-18)$
$X^3-X^2-27X+25$	74836	$X^2+X+(\theta-5)$
$X^3-29X-29$	74849	$X^2+(-\theta-7)$
$X^3-X^2-72X-188$	74872	$X^3+(\theta^2-5\theta-63)X+(\frac{-5}{2}\theta^2+\frac{19}{2}\theta+140)$
$X^3-30X-35$	74925	$X^3+(-\theta-1)X^2+\theta X+(3\theta+4)$
$X^3-X^2-55X+28$	75021	$X^2+(\theta-8)$
$X^3-49X-121$	75289	$X^2+(-\theta-7)$
$X^3-X^2-42X+106$	75304	$X^2+X+(\theta-5)$
$X^3-X^2-58X+85$	75313	$X^3+(-\theta+1)X^2+(\frac{2}{3}\theta^2-\theta-\frac{71}{3})X+(\theta^2-39)$
$X^3-X^2-65X+218$	75509	$X^3+(-\theta-9)X+(-2\theta^2-8\theta+89)$
$X^3-X^2-53X+158$	75653	$X^4-2X^3+(\theta-6)X^2+(-\theta+7)X+(-\theta+5)$
$X^3-X^2-27X+24$	75669	$X^2+(\theta-8)$
$X^3-28X-21$	75901	$X^3+\theta X^2+(-4\theta-3)$
$X^3-X^2-70X+224$	76321	$X^5-X^4+(\frac{-1}{2}\theta^2-\frac{5}{2}\theta+13)X^3+(\frac{1}{2}\theta^2+\frac{5}{2}\theta-14)X^2+3X-1$
$X^3-X^2-92X-236$	76729	$X^4-2X^3-11X^2+12X+(-\theta+13)$
$X^3-X^2-30X+46$	76792	$X^2+X+(\theta-5)$
$X^3-X^2-68X+64$	76897	$X^2+(\theta-9)$
$X^3-X^2-27X-4$	77069	$X^2+X+(-\theta-5)$
$X^3-75X-226$	77112	$X^3+(\frac{1}{2}\theta^2-\frac{5}{2}\theta-25)X^2+(-2\theta+19)X+(\frac{3}{2}\theta^2-\frac{15}{2}\theta-72)$
$X^3-X^2-56X-9$	77145	$X^2+(-\theta-7)$
$X^3-X^2-58X-41$	77273	$X^3+(\theta-12)X+(\frac{2}{3}\theta^2-3\theta-\frac{59}{3})$
$X^3-X^2-33X-40$	77717	$X^2+(-\theta-5)$
$X^3-93X-217$	77841	$X^3+X^2+(\frac{1}{5}\theta^2-\frac{1}{5}\theta-\frac{127}{5})X+(\theta-8)$
$X^3-93X-341$	77841	$X^3+X^2+(\theta^2-6\theta-75)X+(-\theta^2+3\theta+54)$
$X^3-X^2-27X+21$	77844	$X^3-7X+(-\theta+2)$
$X^3-X^2-29X+39$	77844	$X^3+X^2+(\theta-7)X+(-\theta+4)$
$X^3-X^2-47X+129$	77844	$X^3+X^2+(\theta-7)X+(2\theta-11)$
$X^3-57X-38$	77976	$X^3+(-\theta-10)X+(\theta+6)$
$X^3-31X-39$	78097	$X^2+X+(\theta-6)$
$X^3-X^2-51X+148$	78253	$X^3+(-\theta-16)X+(-3\theta^2-11\theta+108)$
$X^3-X^2-52X-118$	78268	$X^2+X+(\theta^2-4\theta-41)$
$X^3-X^2-62X-78$	78392	$X^2+(\frac{1}{3}\theta^2-\frac{2}{3}\theta-21)$

$X^3 - X^2 - 34X + 67$	78441	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 44X - 20$	78988	$X^3 + (\theta + 1)X^2 + \theta X + (-6\theta - 3)$
$X^3 - X^2 - 68X + 36$	79473	$X^4 - 2X^3 + (-\theta - 8)X^2 + (\theta + 9)X + (\frac{1}{2}\theta^2 + \frac{7}{2}\theta - 4)$
$X^3 - X^2 - 28X + 30$	79532	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 53X - 122$	79573	$X^5 + (\theta + 2)X^4 + (\theta^2 - \theta - 26)X^3 + (-\theta^2 + 9\theta + 67)X^2 + (\theta^2 - 24)X + (\theta + 5)$
$X^3 - X^2 - 68X + 16$	79693	$X^2 + (-\theta - 8)$
$X^3 - X^2 - 68X + 20$	79757	$X^5 + 2X^4 + (\theta - 10)X^3 + (\frac{-1}{4}\theta^2 + \frac{11}{4}\theta - \frac{13}{2})X^2 + (\frac{-1}{4}\theta^2 - \frac{1}{4}\theta + \frac{41}{2})X + (\frac{1}{4}\theta^2 - \frac{7}{4}\theta - \frac{7}{2})$
$X^3 - X^2 - 43X - 1$	79768	$X^3 + (-2\theta - 13)X + (3\theta + 18)$
$X^3 - 75X - 244$	80028	$X^3 + (\theta^2 - 5\theta - 50)X^2 + (-2\theta + 19)X + (3\theta^2 - 15\theta - 149)$
$X^3 - X^2 - 46X - 93$	80561	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 75X + 216$	80653	$X^2 + X + (\frac{1}{3}\theta^2 + \frac{2}{3}\theta - 23)$
$X^3 - 29X - 25$	80681	$X^2 + X + (-\theta - 6)$
$X^3 - 66X - 199$	80757	$X^3 + (-\theta^2 + 5\theta + 44)X^2 + (\theta^2 - 7\theta - 19)X + (-4\theta^2 + 20\theta + 163)$
$X^3 - X^2 - 65X - 174$	80997	$X^3 - 16X + (-2\theta^2 + 9\theta + 82)$
$X^3 - 79X - 158$	81133	$X^3 + X^2 + (-\theta - 10)X + (\frac{1}{4}\theta^2 + \frac{3}{4}\theta - \frac{21}{2})$
$X^3 - 51X - 129$	81297	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 34X + 66$	81416	$X^2 - \theta X + (-\theta + 3)$
$X^3 - X^2 - 41X + 100$	81565	$X^2 + X + (\theta - 5)$
$X^3 - 63X - 99$	81729	$X^3 - \theta X^2 + (\frac{1}{3}\theta^2 - 1)X + (-2\theta - 4)$
$X^3 - X^2 - 67X - 183$	81908	$X^2 + X + (-\theta - 5)$
$X^3 - 83X - 190$	82028	$X^5 - 2X^4 + (\frac{1}{4}\theta^2 - \frac{3}{4}\theta - \frac{45}{2})X^3 + 5X^2 + (-\theta^2 + 3\theta + 80)X + (\frac{-1}{4}\theta^2 + \frac{3}{4}\theta + \frac{39}{2})$
$X^3 - X^2 - 69X + 171$	82484	$X^3 + (\frac{1}{3}\theta^2 + \frac{2}{3}\theta - 25)X + (\frac{-2}{3}\theta^2 - \frac{4}{3}\theta + 44)$
$X^3 - X^2 - 59X - 39$	82484	$X^3 - X^2 + (\frac{1}{3}\theta^2 - \frac{2}{3}\theta - 22)X + (\frac{1}{3}\theta^2 - \frac{2}{3}\theta - 18)$
$X^3 - 44X - 20$	82484	$X^3 + X^2 + (-\theta - 9)X + (-\theta - 7)$
$X^3 - 42X - 89$	82485	$X^2 + (-\theta - 5)$
$X^3 - 28X - 14$	82516	$X^3 - \theta X^2 + (4\theta + 2)$
$X^3 - X^2 - 61X - 156$	82661	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 68X + 233$	82673	$X^2 + X + (-\theta - 9)$
$X^3 - X^2 - 31X - 28$	83221	$X^4 - 2X^3 + (\theta - 8)X^2 + (-\theta + 9)X + 1$
$X^3 - 52X - 92$	83476	$X^2 + (\theta - 8)$
$X^3 - X^2 - 50X - 64$	83513	$X^2 + X + (-\theta - 7)$
$X^3 - 60X - 170$	83700	$X^3 - X^2 - 10X + (-\theta^2 + 5\theta + 47)$
$X^3 - 30X - 30$	83700	$X^3 + (-\theta - 1)X^2 + (\theta^2 - 20)X + (-\theta^2 + 25)$
$X^3 - X^2 - 43X + 109$	83892	$X^2 + X + (\theta - 5)$
$X^3 - 81X - 225$	84321	$X^2 + X + (\frac{1}{3}\theta^2 - \theta - 24)$
$X^3 - 28X - 11$	84541	$X^2 + X + (\theta - 6)$
$X^3 - X^2 - 91X + 216$	84701	$X^2 + X + (\frac{1}{5}\theta^2 - \frac{101}{5})$
$X^3 - X^2 - 34X - 42$	84872	$X^3 + (-\theta - 7)X + (-\theta - 3)$
$X^3 - X^2 - 51X - 69$	85260	$X^3 + (\theta + 1)X^2 + \theta X + (-7\theta - 10)$
$X^3 - X^2 - 46X + 123$	85313	$X^2 + X + (-\theta - 9)$
$X^3 - X^2 - 82X + 292$	85557	$X^3 + \theta X^2 + (\frac{1}{2}\theta^2 + \frac{1}{2}\theta - 15)X + (2\theta - 9)$
$X^3 - X^2 - 63X + 179$	85688	$X^2 + X + (\theta - 7)$
$X^3 - X^2 - 72X - 48$	85848	$X^3 + (-2\theta - 19)X + (\frac{1}{4}\theta^2 - \frac{5}{4}\theta - 26)$
$X^3 - X^2 - 44X + 28$	85948	$X^4 + (-\theta + 1)X^3 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 10)X^2 + (-\theta + 1)X + 1$
$X^3 - X^2 - 69X + 238$	85957	$X^2 + (\theta - 7)$
$X^3 - X^2 - 76X - 225$	86105	$X^2 + X + (\theta^2 - 5\theta - 56)$
$X^3 - X^2 - 64X - 169$	86161	$X^2 + (-\theta^2 + 6\theta + 31)$
$X^3 - X^2 - 72X - 184$	86216	$X^2 + X + (\frac{-1}{2}\theta^2 + \frac{7}{2}\theta + 15)$
$X^3 - 63X - 91$	86289	$X^3 + (-\theta - 18)X + (\frac{-1}{3}\theta^2 - \frac{1}{3}\theta + \frac{77}{3})$

$X^3 - X^2 - 76X - 96$	86321	$X^2 + (-\theta - 8)$
$X^3 - X^2 - 35X - 46$	86429	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 50X + 142$	86440	$X^2 + (-\theta^2 - 4\theta + 25)$
$X^3 - X^2 - 65X - 90$	86485	$X^3 - 16X + (\frac{1}{3}\theta^2 - \frac{8}{3}\theta - 28)$
$X^3 - X^2 - 86X + 316$	86485	$X^3 + (\frac{1}{2}\theta^2 + \frac{5}{2}\theta - 31)X^2 + (2\theta + 12)X + (\theta^2 + 3\theta - 45)$
$X^3 - 28X - 7$	86485	$X^3 - \theta X^2 + (4\theta + 1)$
$X^3 - X^2 - 88X - 196$	86572	$X^5 - X^4 + (-\theta - 11)X^3 + (\theta + 10)X^2 + 3X - 1$
$X^3 - X^2 - 72X + 232$	86632	$X^3 - X^2 + (\frac{1}{2}\theta^2 + \frac{5}{2}\theta - 44)X + (\theta^2 + 3\theta - 67)$
$X^3 - X^2 - 65X - 147$	86676	$X^2 + (-\theta - 6)$
$X^3 - 35X - 56$	86828	$X^3 + \theta X^2 + (-5\theta - 8)$
$X^3 - X^2 - 44X + 8$	86828	$X^3 + (-\theta - 1)X^2 + \theta X + (6\theta - 1)$
$X^3 - X^2 - 72X + 92$	86828	$X^3 + (2\theta - 17)X + (\frac{3}{4}\theta^2 - \frac{17}{4}\theta - \frac{33}{2})$
$X^3 - X^2 - 29X - 13$	86996	$X^2 + X + (-\theta - 7)$
$X^3 - 61X - 144$	87013	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 53X - 121$	87092	$X^2 + X + (-\theta - 5)$
$X^3 + X^2 - 81X + 198$	87149	$X^2 + (\frac{1}{3}\theta^2 + \frac{4}{3}\theta - 24)$
$X^3 - 79X - 146$	87289	$X^2 + (\frac{1}{4}\theta^2 - \frac{3}{4}\theta - \frac{43}{2})$
$X^3 - X^2 - 57X - 138$	87693	$X^2 + X + (\theta^2 - 4\theta - 45)$
$X^3 - 28X - 1$	87781	$X^2 + X + (-\theta - 6)$
$X^3 - 66X - 172$	87804	$X^3 - X^2 - 14X + (-\theta^2 + 3\theta + 41)$
$X^3 - 29X - 19$	87809	$X^2 + X + (\theta - 6)$
$X^3 - X^2 - 44X + 113$	87857	$X^3 + (-\theta - 1)X^2 + \theta X + (6\theta - 16)$
$X^3 + X^2 - 76X + 92$	87933	$X^7 - 2X^6 + (\theta - 11)X^5 + (\frac{1}{4}\theta^2 - \frac{9}{4}\theta + \frac{21}{2})X^4 + (\frac{-1}{4}\theta^2 - \frac{11}{4}\theta + \frac{67}{2})X^3$ $+(-\theta^2 + 9\theta - 12)X^2 + (\frac{5}{4}\theta^2 - \frac{25}{4}\theta - \frac{47}{2})X + (2\theta - 15)$
$X^3 - X^2 - 28X - 1$	88057	$X^2 + X + (-\theta - 5)$
$X^3 - 76X - 228$	88084	$X^3 + X^2 + (\theta - 11)X + (\theta^2 - 5\theta - 49)$
$X^3 - 49X - 119$	88249	$X^3 - \theta X^2 + (7\theta + 17)$
$X^3 - X^2 - 60X - 151$	88289	$X^2 + X + (-\theta - 5)$
$X^3 - 71X - 26$	88337	$X^2 + X + (\frac{1}{4}\theta^2 + \frac{1}{4}\theta - \frac{41}{2})$
$X^3 - X^2 - 37X + 79$	88404	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 31X + 46$	88845	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 57X + 176$	88949	$X^2 + (-\theta - 9)$
$X^3 - X^2 - 81X + 285$	88980	$X^2 + X + (\theta - 7)$
$X^3 - X^2 - 86X + 285$	88985	$X^3 - X^2 + (\theta - 12)X + (\frac{1}{3}\theta^2 - \frac{2}{3}\theta - 9)$
$X^3 - 45X - 101$	89073	$X^3 - X^2 + (-\theta - 8)X + (2\theta + 10)$
$X^3 - 81X - 256$	89073	$X^3 - X^2 - 8X + \theta$
$X^3 - 69X - 213$	89073	$X^3 - X^2 + (\theta^2 - 4\theta - 54)X + (-2\theta^2 + 8\theta + 106)$
$X^3 - 87X - 307$	89289	$X^2 + (-\theta - 6)$
$X^3 - X^2 - 49X - 51$	89396	$X^2 + (-\theta - 6)$
$X^3 - 30X - 26$	89748	$X^3 + (-\theta - 1)X^2 + \theta X + (3\theta + 3)$
$X^3 - X^2 - 29X + 30$	89877	$X^2 + (\theta - 7)$
$X^3 - X^2 - 43X - 79$	89908	$X^3 + (-\theta^2 + 6\theta + 14)X + (2\theta^2 - 11\theta - 36)$
$X^3 - 49X - 64$	90001	$X^2 + X + (-\theta - 6)$
$X^3 - 94X - 346$	90004	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 84X - 160$	90257	$X^2 - X + (-\theta - 9)$
$X^3 - 74X - 216$	90296	$X^5 - X^4 - 9X^3 + (\theta + 8)X^2 + (-\theta + 5)X - 5$
$X^3 - X^2 - 29X - 10$	90437	$X^2 + (\theta - 7)$
$X^3 - 90X - 279$	90477	$X^3 + \theta X^2 + (\frac{1}{3}\theta^2 - 1)X + (3\theta + 10)$
$X^3 - X^2 - 58X - 142$	90568	$X^2 + X + (-\theta - 5)$
$X^3 - X^2 - 30X + 38$	90584	$X^3 + (\theta - 1)X^2 - \theta X + (-2\theta + 3)$
$X^3 - X^2 - 100X - 223$	90601	$X^3 + (\frac{-1}{5}\theta^2 + \frac{2}{5}\theta - \frac{17}{5})X + (-3\theta - 12)$
$X^3 - X^2 - 100X + 379$	90601	$X^3 + (\theta - 17)X + (\frac{1}{3}\theta^2 + 3\theta - \frac{109}{3})$

$X^3 - 38X - 69$	90941	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 45X + 33$	90996	$X^2 + (\theta - 8)$
$X^3 - X^2 - 83X + 62$	91325	$X^2 + X + (\theta - 9)$
$X^3 - X^2 - 63X - 164$	91333	$X^3 + (-\theta^2 + 5\theta + 28)X + (-\theta^2 + 7\theta + 36)$
$X^3 - X^2 - 72X - 20$	91336	$X^3 + (\theta - 12)X + (\frac{1}{2}\theta^2 - \frac{5}{2}\theta - 17)$
$X^3 - X^2 - 40X + 93$	91409	$X^2 + X + (\theta - 5)$
$X^3 - 66X - 110$	91476	$X^3 + X^2 - 10X + (\theta - 9)$
$X^3 - 91X - 329$	91777	$X^3 + \theta X^2 + (\theta^2 - 3\theta - 50)X + (-3\theta^2 + 17\theta + 215)$
$X^3 - X^2 - 94X + 76$	91781	$X^2 + X + (\frac{1}{6}\theta^2 + \frac{1}{2}\theta - \frac{62}{3})$
$X^3 - X^2 - 39X + 88$	91837	$X^2 + X + (\theta - 5)$
$X^3 - X^2 - 37X + 78$	91973	$X^3 + (-\theta - 1)X^2 + \theta X + (5\theta - 11)$
$X^3 - X^2 - 76X + 132$	92021	$X^2 + (\frac{1}{4}\theta^2 + \frac{1}{4}\theta - \frac{39}{2})$
$X^3 - 34X - 49$	92389	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 73X - 187$	92692	$X^2 + (-\theta - 6)$
$X^3 - X^2 - 64X - 71$	92721	$X^4 + (-\theta - 1)X^3 + (\frac{1}{3}\theta^2 + \theta - \frac{10}{3})X^2 + (\frac{-1}{3}\theta^2 - \theta + \frac{1}{3})X + 2$
$X^3 - 65X + 164$	93077	$X^2 + X + (\theta - 6)$
$X^3 - 60X - 31$	93117	$X^2 + (\theta - 8)$
$X^3 - 31X - 31$	93217	$X^3 + (\theta^2 - \theta - 31)X + (2\theta^2 - 2\theta - 60)$
$X^3 - 39X - 73$	93393	$X^3 + (\theta - 1)X^2 - \theta X + (-4\theta - 8)$
$X^3 - 46X - 24$	93448	$X^5 - \theta X^4 + (\frac{1}{2}\theta^2 - 11)X^3 - 5X^2 + (\frac{-1}{2}\theta^2 + \theta + 9)X + (\theta - 1)$
$X^3 - 80X - 269$	94253	$X^2 + X + (-\theta - 6)$
$X^3 - X^2 - 85X + 326$	94357	$X^2 + (\theta - 7)$
$X^3 - 57X - 116$	94365	$X^3 - X^2 + (\theta - 14)X + (\frac{-1}{2}\theta^2 + \frac{1}{2}\theta + 35)$
$X^3 - 43X - 91$	94441	$X^2 + (-\theta - 6)$
$X^3 + X^2 - 72X - 16$	94504	$X^2 + (-\theta - 9)$
$X^3 - X^2 - 80X - 186$	94636	$X^3 - X^2 + (\frac{-1}{3}\theta^2 + \frac{8}{3}\theta + 7)X + (\frac{2}{3}\theta^2 - \frac{16}{3}\theta - 17)$
$X^3 - 46X - 20$	94636	$X^3 + X^2 + (-\theta - 10)X + 1$
$X^3 - X^2 - 60X - 116$	94636	$X^3 - \theta X^2 + (\frac{1}{2}\theta^2 - \frac{1}{2}\theta - 10)X + (-2\theta - 7)$
$X^3 - X^2 - 75X - 197$	94636	$X^3 + (-\theta - 10)X + (-2\theta - 11)$
$X^3 - X^2 - 79X + 232$	95109	$X^3 + (-\theta - 17)X + (-2\theta - 13)$
$X^3 - 51X - 127$	95121	$X^2 + (\theta^2 - 3\theta - 44)$
$X^3 - X^2 - 84X + 208$	95317	$X^2 + (\theta - 9)$
$X^3 - 63X - 72$	95580	$X^3 - \theta X^2 + (\frac{1}{3}\theta^2 - 1)X + (-2\theta - 3)$
$X^3 + X^2 - 86X - 111$	95649	$X^2 + X + (-\theta - 9)$
$X^3 - X^2 - 29X - 4$	95861	$X^2 + (-\theta - 5)$
$X^3 - X^2 - 56X - 92$	95992	$X^3 + (\theta - 9)X + (\frac{-1}{2}\theta^2 + \frac{5}{2}\theta + 16)$
$X^3 - 91X - 234$	95992	$X^6 - 2X^5 + (-\theta - 11)X^4 + (\frac{1}{4}\theta^2 + \frac{11}{4}\theta + \frac{27}{2})X^3$ $+(\frac{-1}{4}\theta^2 - \frac{3}{4}\theta + \frac{17}{2})X^2 + (\frac{-1}{4}\theta^2 - \frac{15}{4}\theta - \frac{31}{2})X + (\frac{1}{4}\theta^2 + \frac{11}{4}\theta + \frac{13}{2})$
$X^3 - X^2 - 30X - 14$	95992	$X^3 + (-\theta + 1)X^2 - \theta X + (2\theta + 1)$
$X^3 - X^2 - 37X - 52$	96133	$X^2 + X + (\theta - 7)$
$X^3 - X^2 - 57X - 137$	96148	$X^3 - \theta X^2 + (2\theta + 8)X + (-\theta^2 + 4\theta + 21)$
$X^3 - 31X - 29$	96457	$X^2 + (\theta - 6)$
$X^3 - 79X - 126$	96469	$X^2 + X + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta - \frac{41}{2})$
$X^3 - 49X - 56$	96481	$X^3 - \theta X^2 + (7\theta + 8)$
$X^3 - X^2 - 46X + 36$	96605	$X^3 - X^2 + (\theta - 8)X + 1$
$X^3 - X^2 - 77X - 207$	96852	$X^2 + (-\theta - 9)$
$X^3 - X^2 - 30X - 13$	97265	$X^3 + (-\theta - 1)X^2 + \theta X + (4\theta + 2)$
$X^3 - X^2 - 76X + 116$	97345	$X^2 + X + (\frac{1}{4}\theta^2 + \frac{1}{4}\theta - \frac{39}{2})$
$X^3 - 99X - 118$	97368	$X^7 + X^6 + (\frac{-1}{6}\theta^2 + \frac{5}{6}\theta - \frac{11}{3})X^5 + (\frac{-1}{6}\theta^2 + \frac{11}{6}\theta - \frac{8}{3})X^4$ $+(\frac{4}{3}\theta^2 - \frac{26}{3}\theta - \frac{26}{3})X^3 + (\frac{3}{2}\theta^2 - \frac{33}{2}\theta - 19)X^2$ $+(\frac{-5}{2}\theta^2 + \frac{45}{2}\theta + 30)X + (\frac{-7}{2}\theta^2 + \frac{65}{2}\theta + 44)$
$X^3 - X^2 - 66X - 177$	97473	$X^2 + (-\theta - 8)$

$X^3-48X-44$	97524	$X^3+X^2+(\frac{1}{2}\theta^2-32)X+(\frac{3}{2}\theta^2-81)$
$X^3-X^2-45X+116$	97637	$X^2+X+(\theta-7)$
$X^3-75X-173$	97713	$X^2+(\frac{1}{3}\theta^2-\frac{4}{3}\theta-\frac{80}{3})$
$X^3-X^2-72X+228$	97752	$X^2+X+(\theta-7)$
$X^3-X^2-29X-1$	97844	$X^3+(\theta+1)X^2+(\theta^2-20)X+(\theta+4)$
$X^3-62X-178$	97844	$X^3+(\theta-11)X+(-2\theta^2+9\theta+81)$
$X^3-X^2-77X-229$	97844	$X^3+X^2+(\theta-11)X+(2\theta^2-11\theta-104)$
$X^3-58X-159$	97861	$X^2+X+(-\theta-6)$
$X^3-64X-156$	97876	$X^2+X+(-\theta-6)$
$X^3-X^2-104X-371$	97969	$X^7-2X^6-15X^5+(3\theta^2-20\theta-182)X^4+(-3\theta^2+24\theta+227)X^3$ $+(-3\theta^2+19\theta+198)X^2+(-8\theta-36)X+(-4\theta-20)$
$X^3-86X-301$	97997	$X^6-X^5-12X^4+(\theta^2-5\theta-51)X^3+12X^2-X-1$
$X^3-X^2-29X+20$	98117	$X^2+X+(-\theta-5)$
$X^3-X^2-53X+155$	98132	$X^3-X^2+(\theta-7)X+(\theta-4)$
$X^3-50X-122$	98132	$X^3-7X+(\theta-1)$
$X^3-X^2-59X+185$	98132	$X^3-X^2+(\theta-7)X+(-2\theta+11)$
$X^3-63X-150$	98172	$X^2+X+(-\theta-6)$
$X^3-X^2-51X-111$	98196	$X^3+(-\theta-1)X^2+\theta X+(7\theta+16)$
$X^3-30X-19$	98253	$X^3+(\theta-1)X^2-\theta X+(-3\theta-2)$
$X^3-41X-81$	98537	$X^2+X+(-2\theta-10)$
$X^3-X^2-72X+253$	98833	$X^3+(\theta^2+3\theta-61)X+(-3\theta^2-11\theta+164)$
$X^3-X^2-76X-60$	98885	$X^2+(\frac{1}{4}\theta^2-\frac{3}{4}\theta-\frac{43}{2})$
$X^3-X^2-32X+47$	99713	$X^2+(-\theta-7)$
$X^3-X^2-29X+3$	99732	$X^2+X+(-\theta-5)$
$X^3-X^2-68X-186$	99852	$X^2+X+(-\theta-5)$
$X^3-32X-34$	99860	$X^3-7X+(\theta+1)$
$X^3-X^2-35X+65$	99860	$X^3+X^2+(\theta-7)X+(-\theta+4)$
$X^3-X^2-61X+195$	99860	$X^3+X^2+(\theta-7)X-1$

A.3. Corps quartiques

La table suivante donne le corps de classes de Hilbert des 406 corps quartiques totalement réels non principaux de discriminant ≤ 500000. Parmi ces corps, il y en a 378 de nombre de classes 2, 20 de nombre de classes 3 et 8 de nombre de classes 4.

X^4-17X^2+36	21025	$X^2+(\frac{-1}{12}\theta^3+\frac{11}{12}\theta+\frac{1}{2})X+(\frac{-1}{6}\theta^3+\frac{1}{2}\theta^2+\frac{7}{3}\theta-7)$
$X^4-X^3-19X^2+4X+76$	32625	$X^2+(-\theta-3)$
X^4-22X^2+116	46400	$X^2-\theta X+2$
X^4-9X^2-5X+9	56025	$X^2+X+(-\theta-2)$
X^4-20X^2+50	51200	$X^2+\theta X+\frac{1}{5}\theta^2$
X^4-20X^2+25	57600	X^2-X-1
X^4-16X^2+49	57600	$X^2+\theta X+1$
X^4-8X^2+1	57600	$X^2+\theta X-1$
X^4-25X^2+145	58000	$X^2-\theta X+(\frac{1}{3}\theta^2-\frac{5}{3})$
$X^4-X^3-27X^2+23X+149$	64525	$X^2+(\theta-4)$
$X^4-2X^3-24X^2+25X+155$	64525	$X^2+X+(\theta-4)$
$X^4-2X^3-17X^2+8X+56$	65600	$X^2+(\frac{-1}{2}\theta^3+2\theta^2+\frac{7}{2}\theta-10)X+(-\theta-2)$
$X^4-2X^3-7X^2+3X+1$	71425	$X^2+(\theta^3-2\theta^2-6\theta+2)X+1$
X^4-30X^2+180	72000	$X^2+(\frac{-1}{6}\theta^2+3)X+(\frac{-1}{6}\theta^2-\theta-1)$
$X^4-X^3-28X^2+21X+171$	73225	$X^2+(\frac{-2}{3}\theta^3-\frac{7}{3}\theta^2+\frac{32}{3}\theta+30)$
$X^4-2X^3-27X^2+28X+176$	73225	$X^2+(\frac{1}{4}\theta^2-\frac{1}{4}\theta-3)X+(\frac{1}{4}\theta^3-\frac{17}{4}\theta-7)$

$X^4 - 11X^2 - 13X + 1$	79937	$X^2 + X + (-\theta - 2)$
$X^4 - 10X^2 - 8X + 7$	80896	$X^2 + X + (-\theta - 2)$
$X^4 - 20X^2 + 82$	83968	$X^2 - \theta X + (\frac{1}{3}\theta^2 - \frac{4}{3})$
$X^4 - 22X^2 - 12X + 82$	94464	$X^2 + X + (-\theta - 3)$
$X^4 - 2X^3 - 7X^2 + 3X + 6$	96825	$X^2 + (-\theta - 2)$
$X^4 - X^3 - 32X^2 + 23X + 229$	97025	$X^3 - \theta X^2 + (\frac{-1}{8}\theta^3 - \frac{1}{4}\theta^2 + \frac{9}{4}\theta + \frac{63}{8})X + (\frac{1}{8}\theta^3 + \frac{1}{4}\theta^2 - \frac{9}{4}\theta - \frac{39}{8})$
$X^4 - X^3 - 10X^2 + 12X + 4$	97300	$X^2 + (\theta - 3)$
$X^4 - X^3 - 34X^2 + 4X + 241$	100125	$X^2 + (-\theta - 4)$
$X^4 - 33X^2 + 261$	104400	$X^2 + (\frac{-1}{3}\theta^2 + 5)X + (-\theta - 4)$
$X^4 - X^3 - 11X^2 + 20X - 5$	104825	$X^2 + (\theta^3 + \theta^2 - 9\theta + 3)X + (-\theta^3 - \theta^2 + 9\theta - 3)$
$X^4 - 2X^3 - 23X^2 + 24X + 62$	107584	$X^2 - X + (\frac{1}{33}\theta^3 + \frac{5}{11}\theta^2 - \frac{32}{33}\theta - \frac{355}{33})$
$X^4 - 26X^2 - 20X + 94$	108800	$X^2 + (\frac{1}{13}\theta^3 - \frac{5}{13}\theta^2 - \frac{14}{13}\theta + \frac{63}{13})X + (\frac{1}{13}\theta^3 - \frac{5}{13}\theta^2 - \frac{27}{13}\theta + \frac{11}{13})$
$X^4 - 28X^2 + 49$	112896	$X^2 + (\frac{-1}{7}\theta^3 + 4\theta)X + (\frac{-2}{7}\theta^2 + 7)$
$X^4 - 24X^2 + 81$	112896	$X^2 + (\frac{1}{9}\theta^3 - \frac{8}{3}\theta)X + (\frac{-1}{3}\theta^2 + 6)$
$X^4 - X^3 - 13X^2 + 4X + 37$	113337	$X^2 - \theta X + 1$
$X^4 - X^3 - 34X^2 + 19X + 271$	113625	$X^2 + (\theta - 5)$
$X^4 - 2X^3 - 21X^2 + 22X + 46$	118800	$X^2 + (\frac{-1}{5}\theta^2 + \frac{6}{5}\theta - \frac{9}{5})$
$X^4 - X^3 - 36X^2 + 10X + 295$	122525	$X^2 + (\frac{1}{7}\theta^3 - \frac{4}{7}\theta^2 - \frac{17}{7}\theta + \frac{54}{7})X + (-\theta - 4)$
$X^4 - X^3 - 23X^2 + X + 86$	122825	$X^2 + (\theta^3 - 2\theta^2 - 13\theta - 7)$
$X^4 - 39X^2 + 319$	127600	$X^2 + (\frac{1}{7}\theta^2 - \frac{23}{7})X + (\frac{-1}{7}\theta^3 + \frac{1}{7}\theta^2 + \frac{23}{7}\theta - \frac{51}{7})$
$X^4 - 36X^2 + 319$	127600	$X^2 + (\frac{1}{2}\theta^2 - \frac{19}{2})X + (\frac{-1}{2}\theta^2 + \theta + \frac{9}{2})$
$X^4 - 2X^3 - 11X^2 - 6X + 1$	129344	$X^2 - X + (\theta^3 - 2\theta^2 - 11\theta - 7)$
$X^4 - X^3 - 17X^2 - 7X + 34$	130100	$X^2 + (-\theta^3 + 3\theta^2 + 10\theta - 10)X + (\theta^3 - 4\theta^2 - 8\theta + 20)$
$X^4 - 2X^3 - 35X^2 + 36X + 319$	131225	$X^2 - X + (\theta - 5)$
$X^4 - X^3 - 38X^2 + 31X + 311$	131225	$X^2 + (\theta - 5)$
$X^4 - 18X^2 + 57$	131328	$X^2 + \theta X + 1$
$X^4 - 2X^3 - 9X^2 + 5X + 15$	132025	$X^2 + (-\theta - 2)$
$X^4 - 2X^3 - 7X^2 + 6X + 1$	134464	$X^2 + X + (-\theta - 2)$
$X^4 - 2X^3 - 23X^2 + 24X + 126$	135232	$X^3 + (\theta - 2)X^2 + (\frac{1}{3}\theta^2 - \frac{4}{3}\theta - 1)X + (\frac{-1}{3}\theta^2 + \frac{1}{3}\theta + 3)$
$X^4 - 16X^2 - 20X + 4$	139600	$X^2 + (-\theta - 3)$
$X^4 - 38X^2 + 356$	142400	$X^2 + (\frac{1}{2}\theta^2 - 9)X + (\theta - 4)$
$X^4 - 2X^3 - 41X^2 + 42X + 361$	148625	$X^2 + (\theta - 6)$
$X^4 - X^3 - 39X^2 + 24X + 356$	148625	$X^2 + (\frac{1}{16}\theta^3 + \frac{1}{16}\theta^2 - \frac{21}{16}\theta - \frac{17}{8})X + (\theta - 5)$
$X^4 - X^3 - 42X^2 + 38X + 359$	151525	$X^2 + (\frac{-1}{5}\theta^3 - \frac{1}{5}\theta^2 + 5\theta - \frac{8}{5})$
$X^4 - 2X^3 - 38X^2 + 39X + 369$	151525	$X^2 - X + (\frac{-1}{3}\theta^2 - \frac{2}{3}\theta + 2)$
$X^4 - 2X^3 - 10X^2 + 11X + 9$	151725	$X^2 - \theta X + (\frac{1}{3}\theta^3 - \frac{10}{3}\theta - 2)$
$X^4 - 2X^3 - 8X^2 + 9X - 1$	151725	$X^2 + (\theta^3 - 3\theta^2 - 2\theta)$
$X^4 - 8X^2 + 6$	153600	$X^2 + \theta X + (\theta^2 - 6)$
$X^4 - 16X^2 + 54$	153600	$X^2 + (\frac{1}{3}\theta^3 - \frac{7}{3}\theta)X + (\theta^2 - 6)$
$X^4 - X^3 - 9X^2 + 4X + 1$	154625	$X^2 + (-\theta - 3)$
$X^4 - 17X^2 + 34$	157216	$X^2 + \theta X + (\frac{1}{3}\theta^2 - \frac{4}{3})$
$X^4 - X^3 - 8X^2 + X + 6$	157225	$X^2 + X + (\theta^2 - \theta - 7)$
$X^4 - 44X^2 + 404$	161600	$X^2 + X + (\frac{-1}{8}\theta^2 + \theta - \frac{7}{4})$
$X^4 - 2X^3 - 11X^2 + 6X + 15$	165696	$X^2 + (\frac{1}{3}\theta^3 - \frac{1}{3}\theta^2 - 3\theta - 2)X + (\frac{-1}{3}\theta^3 + \frac{1}{3}\theta^2 + 4\theta + 3)$
$X^4 - 2X^3 - 43X^2 + 44X + 404$	166025	$X^2 - X + (\frac{-1}{8}\theta^2 - \frac{7}{8}\theta - \frac{7}{4})$
$X^4 - X^3 - 41X^2 + 20X + 400$	166025	$X^2 + (-\theta - 5)$
$X^4 - 20X^2 + 73$	168192	$X^2 + \theta X + (\frac{1}{3}\theta^2 - \frac{4}{3})$
$X^4 - 16X^2 - 24X + 1$	168192	$X^2 + (\theta - 1)X + (\theta^3 - 2\theta^2 - 11\theta - 2)$
$X^4 - 11X^2 - 10X - 1$	170800	$X^2 + (\theta^2 - 2\theta - 13)$
$X^4 - 19X^2 + 64$	176400	$X^2 + \theta X + 1$

X^4-25X^2+25	176400	$X^2+\theta X+\frac{1}{5}\theta^2$
X^4-11X^2+4	176400	$X^2+\theta X-1$
$X^4-X^3-8X^2+6X+6$	177300	$X^2+(\theta-1)X-1$
$X^4-X^3-44X^2+9X+431$	177625	$X^2+(\frac{1}{6}\theta^3-\theta^2-\frac{13}{3}\theta+\frac{79}{6})$
X^4-45X^2+445	178000	$X^2+(\frac{-1}{7}\theta^2+\frac{26}{7})X+(\frac{1}{7}\theta^3+\frac{1}{7}\theta^2-\frac{26}{7}\theta-\frac{54}{7})$
$X^4-34X^2-28X+158$	178432	$X^2-X+(\frac{5}{33}\theta^3-\frac{2}{33}\theta^2-\frac{41}{11}\theta-\frac{203}{33})$
$X^4-28X^2-8X+161$	178432	$X^2+X+(-\theta-4)$
X^4-30X^2+175	179200	$X^2-X+(\frac{-1}{5}\theta^2+\theta-1)$
$X^4-2X^3-27X^2+18X+161$	180800	$X^2+(\frac{1}{7}\theta^3-\frac{4}{7}\theta^2-\frac{12}{7}\theta+5)X+(-\theta-3)$
$X^4-2X^3-17X^2-8X+16$	183872	$X^2+(\frac{1}{4}\theta^3-\frac{1}{2}\theta^2-\frac{13}{4}\theta-1)X+(\theta+2)$
$X^4-2X^3-13X^2+14X+23$	183872	$X^2+X+(\frac{1}{5}\theta^3+\frac{1}{5}\theta^2-3\theta-\frac{26}{5})$
$X^4-X^3-15X^2-18X-1$	187025	$X^2+(\theta^3-2\theta^2-12\theta-10)$
$X^4-2X^3-20X^2+6X+69$	187200	$X^2+(\frac{-1}{3}\theta^3+\frac{4}{3}\theta^2+3\theta-7)X+(-\theta-2)$
$X^4-X^3-49X^2+49X+451$	190125	$X^2+(\frac{1}{71}\theta^3+\frac{3}{71}\theta^2-\frac{30}{71}\theta-\frac{180}{71})X+(\theta-5)$
$X^4-X^3-14X^2+9X+36$	191625	$X^2+(\frac{-1}{3}\theta^3+\frac{1}{3}\theta^2+\frac{11}{3}\theta-2)X+(-\theta^2+9)$
$X^4-X^3-11X^2+18X-1$	191769	$X^3+X^2+(-\theta^3-\theta^2+8\theta-5)X+(-\theta^3-2\theta^2+6\theta+2)$
$X^4-X^3-45X^2+32X+464$	193225	$X^3+X^2+(\theta-5)X+(\frac{1}{8}\theta^3-\frac{5}{8}\theta^2-\frac{17}{8}\theta+\frac{21}{2})$
$X^4-2X^3-11X^2-3X+1$	193625	$X^2+(\theta^3-2\theta^2-11\theta-5)$
$X^4-2X^3-43X^2+44X+479$	196025	$X^3+(\frac{1}{2}\theta^2-\frac{1}{2}\theta-\frac{23}{2})X^2+(\frac{-1}{2}\theta^2+\frac{3}{2}\theta+\frac{11}{2})X$ $+(\frac{1}{2}\theta^3-3\theta^2-9\theta+\frac{115}{2})$
X^4-9X^2-5X+4	196825	$X^2+(-\theta^3+\theta^2+8\theta-4)$
X^4-45X^2+495	198000	$X^2+(\frac{1}{3}\theta^2-8)X+(\theta-5)$
X^4-47X^2+441	198025	$X^2+(\frac{1}{14}\theta^3+\frac{1}{2}\theta^2-\frac{33}{14}\theta-18)$
X^4-45X^2+505	202000	$X^2+X+(-\theta^3+2\theta^2+23\theta-50)$
X^4-25X^2+75	202800	$X^2+\theta X+\frac{1}{5}\theta^2$
$X^4-14X^2-8X+12$	203072	$X^2-\frac{1}{2}\theta^2$
$X^4-X^3-49X^2+4X+496$	203625	$X^2+(-\theta-5)$
$X^4-22X^2-40X-4$	206400	$X^2-\frac{1}{2}\theta^2$
$X^4-2X^3-7X^2+8X+6$	206400	$X^2+(2\theta-1)X+(\theta^2-\theta-1)$
$X^4-X^3-47X^2+13X+509$	209525	$X^2+(\theta^3-6\theta^2-21\theta+116)$
X^4-15X^2+5	210125	$X^2+\theta X-1$
$X^4-2X^3-12X^2-7X+1$	214925	$X^2+(-\theta^3+3\theta^2+9\theta)X+(\theta^3-3\theta^2-9\theta+1)$
$X^4-2X^3-10X^2+6X+4$	217300	$X^2+(\frac{1}{2}\theta^3-\theta^2-4\theta+2)X+1$
$X^4-2X^3-31X^2+32X+206$	219200	$X^2+(\frac{-1}{5}\theta^2-\frac{4}{5}\theta-\frac{4}{5})$
X^4-52X^2+551	220400	$X^2+(\frac{-1}{10}\theta^2+\frac{21}{10})X+(\frac{-1}{10}\theta^2+\theta-\frac{29}{10})$
X^4-47X^2+551	220400	$X^2+(\theta^2-24)X+(-\theta^2+\theta+18)$
$X^4-X^3-49X^2+39X+531$	221125	$X^2+(\theta-6)$
$X^4-2X^3-46X^2+47X+541$	221125	$X^2+X+(\theta-6)$
$X^4-2X^3-12X^2+8X+31$	222800	$X^2+X+(-\theta-2)$
X^4-20X^2+97	223488	$X^2+\theta X+2$
$X^4-14X^2-12X+10$	223488	$X^2+(\frac{-2}{3}\theta^3+\frac{2}{3}\theta^2+\frac{20}{3}\theta-\frac{11}{3})$
$X^4-X^3-20X^2+2X+69$	223925	$X^2+(\frac{-1}{7}\theta^3+\frac{2}{7}\theta^2+\frac{11}{7}\theta-\frac{6}{7})X+(-\theta-2)$
$X^4-X^3-50X^2+42X+539$	224725	$X^2+(\frac{-5}{21}\theta^3-\frac{3}{7}\theta^2+\frac{145}{21}\theta+\frac{16}{3})$
$X^4-2X^3-50X^2+51X+549$	224725	$X^2+X+(\frac{-1}{9}\theta^2-\frac{8}{9}\theta-\frac{5}{3})$
X^4-18X^2+18	225792	$X^2+\theta X+(\frac{1}{3}\theta^2-2)$
$X^4-X^3-13X^2+26X-9$	226825	$X^2-\theta X-\theta$
$X^4-X^3-29X^2+52X+52$	230009	$X^3+(\frac{1}{20}\theta^3+\frac{1}{4}\theta^2-\frac{39}{20}\theta-\frac{31}{10})X^2$ $+(\frac{-1}{5}\theta^3+\frac{19}{5}\theta+\frac{7}{5})X+(\frac{1}{20}\theta^3+\frac{1}{4}\theta^2-\frac{39}{20}\theta-\frac{1}{10})$
X^4-25X^2+50	231200	$X^2+\theta X+\frac{1}{5}\theta^2$
X^4-36X^2+226	231424	$X^2+\theta X+(\frac{2}{7}\theta^2-\frac{8}{7})$
$X^4-X^3-18X^2-4X+16$	231525	$X^2+(\frac{1}{4}\theta^3-\frac{3}{4}\theta^2-2\theta-1)$
X^4-50X^2+580	232000	$X^2+(\frac{1}{6}\theta^2-\frac{14}{3})X+(\frac{-1}{3}\theta^2+\theta+\frac{7}{3})$

$X^4-33X^2-42X+78$	232848	$X^2+X+(\frac{-7}{34}\theta^3+\frac{15}{34}\theta^2+\frac{80}{17}\theta-\frac{90}{17})$
$X^4-X^3-49X^2+19X+571$	235125	$X^2+(\theta-6)$
$X^4-X^3-13X^2+X+21$	235325	$X^2+(-\theta-3)$
$X^4-2X^3-16X^2+12X+16$	236500	$X^2+(\frac{1}{4}\theta^3-\frac{1}{2}\theta^2-3\theta+2)X+1$
$X^4-X^3-12X^2-2X+4$	236600	$X^2+(\frac{1}{2}\theta^3-\frac{1}{2}\theta^2-5\theta-1)X+1$
X^4-11X^2+14	236600	$X^2+(\frac{1}{2}\theta^3+\frac{1}{2}\theta^2-5\theta-6)$
$X^4-14X^2-20X-1$	236800	$X^2-\theta X+\theta$
$X^4-X^3-9X^2+9X+1$	239125	$X^2+(-\theta-3)$
$X^4-2X^3-37X^2+8X+226$	244800	$X^2+(\frac{8}{19}\theta^3+\frac{4}{19}\theta^2-\frac{286}{19}\theta-\frac{689}{19})$
$X^4-2X^3-24X^2+4X+94$	247104	$X^2+(-\theta+1)X+(-\theta^3+5\theta^2+10\theta-33)$
$X^4-2X^3-36X^2-14X+97$	247104	$X^2+(\frac{276}{55}\theta^3-\frac{35}{11}\theta^2-\frac{936}{5}\theta-\frac{18736}{55})$
$X^4-X^3-55X^2+2X+604$	247225	$X^2+(\frac{-5}{39}\theta^3+\frac{16}{39}\theta^2+\frac{154}{39}\theta-\frac{536}{39})$
$X^4-X^3-50X^2+27X+599$	247225	$X^2+(\frac{-1}{24}\theta^3+\frac{13}{12}\theta+\frac{23}{24})X+(\theta-6)$
$X^4-X^3-53X^2+46X+596$	248225	$X^3-X^2+(\frac{-3}{17}\theta^3-\frac{4}{17}\theta^2+\frac{93}{17}\theta+\frac{11}{17})X$ $+(\frac{1}{34}\theta^3-\frac{27}{34}\theta^2-\frac{65}{34}\theta+\frac{443}{17})$
$X^4-X^3-56X^2+55X+605$	253025	$X^2+(\frac{3}{22}\theta^3+\frac{4}{11}\theta^2-\frac{51}{11}\theta-\frac{31}{2})$
$X^4-2X^3-49X^2+50X+620$	253025	$X^2+X+(\frac{-1}{2}\theta^2+\frac{3}{2}\theta+6)$
X^4-53X^2+576	255025	$X^2+(\frac{-7}{48}\theta^3-2\theta^2+\frac{107}{48}\theta+\frac{61}{2})$
X^4-20X^2+10	256000	$X^2+\theta X+(\frac{1}{3}\theta^2-\frac{10}{3})$
X^4-20X^2+90	256000	$X^2+\theta X+(\theta^2-10)$
$X^4-X^3-9X^2+9X+6$	256500	$X^2+\theta X+(\theta-2)$
$X^4-2X^3-12X^2+8X+1$	257300	$X^2+(\theta-1)X+(\frac{1}{2}\theta^3-\frac{1}{2}\theta^2-\frac{13}{2}\theta-\frac{1}{2})$
$X^4-2X^3-41X^2+42X+241$	257600	$X^2+(\frac{-1}{5}\theta^2+\frac{6}{5}\theta-\frac{9}{5})$
$X^4-2X^3-51X^2+52X+631$	257625	$X^2+(\frac{1}{6}\theta^3-5\theta-\frac{59}{6})$
$X^4-X^3-25X^2+37X+69$	257725	$X^2+(\frac{1}{3}\theta^3+\theta^2-\frac{16}{3}\theta-8)X+(\theta-3)$
$X^4-34X^2-12X+238$	260352	$X^2+X+(-\theta-4)$
$X^4-2X^3-24X^2+25X+50$	260389	$X^2-\theta X+(\frac{1}{5}\theta^2-\frac{1}{5}\theta-1)$
X^4-13X^2+37	261072	$X^2-\theta X+1$
$X^4-2X^3-14X^2+15X-1$	262205	$X^3+(\frac{2}{3}\theta^3-\theta^2-\frac{28}{3}\theta+\frac{13}{3})X^2+(\frac{-1}{3}\theta^3+\frac{17}{3}\theta+\frac{4}{3})X-2$
X^4-18X^2+41	262400	$X^2+(\frac{-1}{2}\theta^2+\theta-\frac{1}{2})$
$X^4-14X^2-20X-6$	262400	$X^2+(\theta^3-\theta^2-14\theta-8)X+(\theta^3-\theta^2-12\theta-4)$
$X^4-X^3-52X^2+18X+639$	262525	$X^3+X^2+(\frac{1}{3}\theta^3-\frac{7}{3}\theta^2-\frac{22}{3}\theta+49)X$ $+(\frac{3}{5}\theta^3-\frac{17}{5}\theta^2-13\theta+\frac{359}{5})$
$X^4-29X^2-30X+94$	262800	$X^2+(28\theta^3+6\theta^2-988\theta-2291)$
$X^4-2X^3-11X^2+2X+6$	263500	$X^2+(-2\theta^2+1)$
$X^4-2X^3-54X^2+55X+655$	267525	$X^2-X+(\frac{-1}{9}\theta^2-\frac{8}{9}\theta-\frac{22}{9})$
$X^4-X^3-52X^2+28X+649$	267525	$X^2+(-\theta-6)$
X^4-14X^2+20	269120	$X^2+(\frac{1}{2}\theta^2-3)X+(\theta-1)$
$X^4-2X^3-53X^2+54X+599$	270400	$X^4+(\frac{4}{99}\theta^3-\frac{2}{33}\theta^2-\frac{116}{99}\theta+\frac{158}{99})X^3$ $+(\frac{1}{11}\theta^3+\frac{4}{11}\theta^2-\frac{40}{11}\theta-\frac{175}{11})X^2$ $+(\frac{-10}{99}\theta^3+\frac{5}{33}\theta^2+\frac{389}{99}\theta-\frac{98}{99})X$ $+(\frac{-2}{9}\theta^3-\frac{2}{3}\theta^2+\frac{85}{9}\theta+\frac{308}{9})$
$X^4-2X^3-35X^2+36X+194$	270400	$X^4+X^3+(\frac{1}{19}\theta^3-\frac{11}{19}\theta^2+\frac{7}{19}\theta+\frac{49}{19})X^2$ $+(\frac{1}{19}\theta^3-\frac{11}{19}\theta^2+\frac{7}{19}\theta+\frac{49}{19})X$ $+(\frac{-5}{19}\theta^3+\frac{36}{19}\theta^2+\frac{3}{19}\theta-\frac{207}{19})$
$X^4-2X^3-25X^2+26X+39$	270400	$X^4-X^3+(\frac{1}{9}\theta^3+\frac{1}{3}\theta^2-\frac{28}{9}\theta-\frac{35}{3})X^2$ $+(\frac{-1}{3}\theta^3+\frac{25}{3}\theta+9)X+(\frac{1}{9}\theta^3-\frac{2}{3}\theta^2-\frac{19}{9}\theta+\frac{40}{3})$
X^4-18X^2+16	270400	$X^4-X^3+(\frac{-1}{2}\theta^2+\theta-2)X^2+(\frac{1}{2}\theta^2-3\theta+2)X+(\theta-1)$
$X^4-2X^3-10X^2+6X+19$	270400	$X^2+X+(-\theta-2)$
$X^4-X^3-24X^2+4X+16$	274625	$X^2+\theta X+(\frac{1}{8}\theta^3+\frac{1}{8}\theta^2-\frac{11}{4}\theta-2)$
$X^4-X^3-24X^2+69X-49$	274625	$X^2-\theta X+(-\theta+1)$
X^4-34X^2+25	278784	$X^2+(\frac{3}{10}\theta^3-\frac{117}{10}\theta-10)$

$X^4 - 44X^2 + 121$	278784	$X^2 - \frac{1}{11}\theta^2$
$X^4 - 12X^2 - 10X + 11$	280400	$X^2 + (\theta^3 - 2\theta^2 - 8\theta + 4)X + (\theta^3 - 2\theta^2 - 8\theta + 6)$
$X^4 - 36X^2 + 274$	280576	$X^2 + \theta X + (\frac{1}{5}\theta^2 + \frac{2}{5})$
$X^4 - X^3 - 10X^2 + 12X - 1$	282325	$X^2 + (-\theta^3 + 9\theta - 4)X + (\theta + 2)$
$X^4 - X^3 - 15X^2 + 32X - 11$	282825	$X^2 + (-\theta^3 - \theta^2 + 12\theta - 7)X + 1$
$X^4 - X^3 - 55X^2 + 42X + 684$	283225	$X^3 - X^2 + (\theta - 6)X + (\theta - 5)$
$X^4 - 20X^2 - 12X + 47$	286784	$X^2 + (\frac{3}{2}\theta^3 - \frac{11}{2}\theta^2 - \frac{21}{2}\theta + \frac{39}{2})$
$X^4 - 2X^3 - 14X^2 + 4X + 20$	289552	$X^2 + (\frac{-1}{2}\theta^2 + \theta + 4)X + 1$
$X^4 - 15X^2 - 2X + 49$	289552	$X^2 + \theta X + 1$
$X^4 - 54X^2 + 724$	289600	$X^2 + (\frac{1}{2}\theta^2 - 13)X + (\theta - 5)$
$X^4 - X^3 - 13X^2 + 11X + 26$	290200	$X^2 - \theta X + (\theta^2 - 8)$
$X^4 - X^3 - 58X^2 + 6X + 711$	290725	$X^2 + (\frac{40}{19}\theta^3 + \frac{113}{19}\theta^2 - \frac{1836}{19}\theta - \frac{6948}{19})$
$X^4 - X^3 - 55X^2 + 17X + 709$	290725	$X^2 + (\frac{-1}{9}\theta^3 + \frac{5}{9}\theta^2 + \frac{17}{9}\theta - \frac{175}{9})$
$X^4 - 2X^3 - 26X^2 + 27X + 101$	291525	$X^2 + (\frac{-1}{5}\theta^2 - \frac{4}{5}\theta - \frac{4}{5})$
$X^4 - 46X^2 + 287$	293888	$X^2 + (\frac{1}{11}\theta^2 - \frac{12}{11})X + (\frac{1}{11}\theta^3 + \frac{2}{11}\theta^2 - \frac{34}{11}\theta - \frac{90}{11})$
$X^4 - 34X^2 + 287$	293888	$X^2 + (-\theta^2 + 16)X + (-\theta - 4)$
$X^4 - X^3 - 20X^2 + 12X + 9$	293925	$X^2 + (\frac{-1}{3}\theta^3 + \frac{1}{3}\theta^2 + \frac{20}{3}\theta - 7)$
$X^4 - 2X^3 - 11X^2 + 2X + 1$	296000	$X^2 + (\theta^3 - 2\theta^2 - 12\theta + 1)X + (\theta + 3)$
$X^4 - 20X^2 - 20X + 15$	296000	$X^2 - X + (-\theta - 4)$
$X^4 - 2X^3 - 41X^2 + 42X + 279$	296512	$X^2 + (\frac{-1}{9}\theta^2 - \frac{8}{9}\theta - \frac{5}{3})$
$X^4 - 2X^3 - 33X^2 + 34X + 281$	296512	$X^2 + (\theta - 5)$
$X^4 - 30X^2 - 60X - 6$	297216	$X^2 + (\frac{2}{13}\theta^3 - \frac{10}{13}\theta^2 - \frac{36}{13}\theta - \frac{5}{13})$
$X^4 - 10X^2 - 5X + 10$	299125	$X^2 + (-\theta - 3)$
$X^4 - 2X^3 - 12X^2 - 2X + 1$	302400	$X^2 + (-\theta^3 + 2\theta^2 + 11\theta + 1)X + (\theta + 2)$
$X^4 - 18X^2 + 21$	302400	$X^2 + (\frac{1}{2}\theta^3 + \frac{1}{2}\theta^2 - \frac{17}{2}\theta - \frac{19}{2})$
$X^4 - 2X^3 - 16X^2 + 8X + 49$	304596	$X^2 - \theta X + 1$
$X^4 - X^3 - 16X^2 + 4X + 52$	304596	$X^2 + \theta X + 1$
$X^4 - X^3 - 18X^2 + 16X + 16$	304700	$X^2 + (\frac{1}{4}\theta^3 - \frac{1}{4}\theta^2 - \frac{7}{2}\theta + 2)X + (-\theta + 2)$
$X^4 - 36X^2 + 306$	313344	$X^2 + \theta X + (\frac{1}{3}\theta^2 - 2)$
$X^4 - 36X^2 + 289$	313600	$X^2 + (\frac{-1}{17}\theta^3 + \frac{19}{17}\theta - 1)X + (\theta - 4)$
$X^4 - 34X^2 + 9$	313600	$X^2 - X + (\frac{1}{12}\theta^3 - \frac{1}{4}\theta^2 - \frac{25}{12}\theta - \frac{3}{4})$
$X^4 - 12X^2 + 1$	313600	$X^2 + (\theta^3 - 13\theta - 1)X + (\theta + 2)$
$X^4 - X^3 - 10X^2 - 3X + 4$	314425	$X^2 + (-2\theta^2 + 3\theta - 1)$
$X^4 - 34X^2 + 272$	314432	$X^2 + (\frac{-1}{2}\theta^2 + 8)X + (\theta - 3)$
$X^4 - 40X^2 - 24X + 289$	315648	$X^2 + (-\theta^2 - 4\theta)$
$X^4 - X^3 - 14X^2 + 24X - 4$	316500	$X^2 + \theta X - \theta$
$X^4 - 11X^2 - 6X + 1$	318672	$X^2 + (\theta - 1)X + (-\theta - 1)$
$X^4 - X^3 - 11X^2 + 5X + 10$	319700	$X^2 + (-\theta - 3)$
$X^4 - X^3 - 58X^2 + 16X + 781$	319725	$X^2 + (6\theta^3 - 37\theta^2 - 161\theta + 925)$
$X^4 - 57X^2 + 801$	320400	$X^2 + (\frac{1}{3}\theta^2 - 9)X + (\theta - 5)$
$X^4 - 2X^3 - 14X^2 - 11X + 1$	321269	$X^2 + (-\theta^2 - \theta)$
$X^4 - 2X^3 - 13X^2 + 14X + 9$	321600	$X^2 + \theta X + (\frac{1}{2}\theta^2 + \frac{1}{2}\theta - \frac{13}{2})$
$X^4 - 2X^3 - 25X^2 + 16X + 64$	321600	$X^2 + (\frac{7}{6}\theta^3 - \frac{23}{3}\theta^2 + \frac{25}{6}\theta + \frac{37}{3})$
$X^4 - X^3 - 64X^2 + 64X + 781$	325125	$X^2 + (\frac{-193}{131}\theta^3 + \frac{828}{131}\theta^2 + \frac{9623}{131}\theta - \frac{44715}{131})$
$X^4 - X^3 - 15X^2 - 13X + 4$	326700	$X^2 + (\frac{1}{2}\theta^3 - \theta^2 - \frac{11}{2}\theta - 2)X - \theta$
$X^4 - 60X^2 + 820$	328000	$X^2 - X + (\frac{-1}{8}\theta^2 + \theta - \frac{7}{4})$
$X^4 - 2X^3 - 13X^2 + 9X - 1$	328825	$X^2 - \theta X + (-\theta^3 + 2\theta^2 + 13\theta - 7)$
$X^4 - 36X^2 + 322$	329728	$X^2 + \theta X + 4$
$X^4 - 26X^2 + 145$	334080	$X^2 + (-\theta^2 + 8)$
$X^4 - 22X^2 - 36X + 10$	334080	$X^2 - X + (2\theta^3 - 6\theta^2 - 27\theta + 7)$
$X^4 - 2X^3 - 57X^2 + 58X + 821$	334225	$X^2 + X + (\theta - 7)$
$X^4 - X^3 - 60X^2 + 47X + 809$	334225	$X^2 + (\theta - 7)$

$X^4 - 62X^2 + 836$	334400	$X^2 + (\frac{-1}{10}\theta^2 + \frac{13}{5})X + (\frac{-1}{10}\theta^2 + \theta - \frac{12}{5})$
$X^4 - X^3 - 21X^2 - 15X + 20$	336200	$X^2 - X + (\frac{1}{4}\theta^3 - \frac{21}{4}\theta - 10)$
$X^4 - 2X^3 - 9X^2 + 2X + 7$	336704	$X^2 + X + (-\theta - 2)$
$X^4 - X^3 - 15X^2 + 22X - 1$	336825	$X^2 + (\frac{-1}{3}\theta^3 - \frac{1}{3}\theta^2 + \frac{13}{3}\theta - \frac{2}{3})X + \theta$
$X^4 - 65X^2 + 845$	338000	$X^2 + X + (\frac{-1}{13}\theta^2 + \theta - 3)$
$X^4 - 17X^2 - 6X + 28$	340008	$X^3 + (\frac{-1}{6}\theta^3 - \frac{1}{3}\theta^2 + \frac{19}{6}\theta + \frac{10}{3})X^2$ $+(\frac{-1}{2}\theta^3 + \frac{13}{2}\theta + 6)X + (\frac{-1}{6}\theta^3 - \frac{1}{3}\theta^2 + \frac{19}{6}\theta + \frac{16}{3})$
$X^4 - 60X^2 + 855$	342000	$X^2 + (\frac{-1}{6}\theta^2 + \frac{11}{2})X + (\theta - 6)$
$X^4 - 14X^2 - 10X + 19$	343700	$X^2 + (-2\theta^2 - 2\theta + 3)$
$X^4 - 30X^2 + 150$	345600	$X^2 + X + (\frac{-1}{5}\theta^2 + \theta - 1)$
$X^4 - 52X^2 + 338$	346112	$X^2 - X + (\frac{-1}{13}\theta^2 + \theta - 3)$
$X^4 - 2X^3 - 33X^2 + 34X + 142$	346896	$X^2 + (\frac{-2}{7}\theta^2 - \frac{12}{7}\theta - \frac{15}{7})$
$X^4 - 27X^2 - 12X + 132$	346896	$X^2 + (\frac{3}{2}\theta^3 - 7\theta^2 - \frac{37}{2}\theta + 58)$
$X^4 - 2X^3 - 37X^2 + 28X + 316$	347200	$X^2 + (\frac{11}{2}\theta^3 - 34\theta^2 - \frac{131}{2}\theta + 428)$
$X^4 - 2X^3 - 16X^2 - 16X - 2$	348480	$X^2 + X + (-\theta - 2)$
$X^4 - 2X^3 - 41X^2 + 42X + 141$	349200	$X^2 + (\frac{-1}{5}\theta^2 + \frac{6}{5}\theta - \frac{9}{5})$
$X^4 - 18X^2 - 20X + 1$	350800	$X^2 + (-\theta - 4)$
$X^4 - 2X^3 - 58X^2 + 59X + 869$	353525	$X^3 - X^2 + (\theta - 6)X + (\theta^3 - 7\theta^2 - 24\theta + 180)$
$X^4 - X^3 - 40X^2 + 52X + 256$	353736	$X^2 + (\theta - 5)$
$X^4 - 19X^2 - 10X + 24$	357400	$X^2 + (\frac{-1}{4}\theta^3 + \frac{1}{4}\theta^2 + \frac{7}{2}\theta - 1)X + 1$
$X^4 - 40X^2 + 350$	358400	$X^2 + X + (\frac{-1}{5}\theta^2 + \theta - 1)$
$X^4 - X^3 - 14X^2 - 6X + 16$	359000	$X^2 - \theta X + (\frac{-1}{2}\theta^3 + \frac{3}{2}\theta^2 + 5\theta - 5)$
$X^4 - 2X^3 - 13X^2 + 4X + 24$	359200	$X^2 + (\theta^2 - 2\theta - 11)$
$X^4 - 2X^3 - 51X^2 + 52X + 338$	359488	$X^2 + (\frac{4}{13}\theta^3 + \frac{2}{13}\theta^2 - \frac{214}{13}\theta - 35)$
$X^4 - 2X^3 - 37X^2 + 36X + 324$	359488	$X^2 + (-6\theta^3 - 36\theta^2 + 112\theta + 531)$
$X^4 - 64X^2 + 899$	359600	$X^2 + (\frac{1}{5}\theta^3 - \frac{7}{10}\theta^2 - \frac{27}{5}\theta + \frac{89}{10})$
$X^4 - 61X^2 + 899$	359600	$X^2 + (\frac{1}{5}\theta^2 - \frac{33}{5})X + (\frac{-2}{5}\theta^2 + \theta + \frac{26}{5})$
$X^4 - 65X^2 + 905$	362000	$X^2 + (\frac{30}{11}\theta^3 - 18\theta^2 - \frac{612}{11}\theta + 361)$
$X^4 - 66X^2 + 909$	363600	$X^2 - X + (\frac{-1}{12}\theta^2 + \theta - \frac{11}{4})$
$X^4 - 62X^2 + 916$	366400	$X^2 + (\frac{-1}{6}\theta^2 + \frac{17}{3})X + (\frac{-1}{6}\theta^2 + \theta - \frac{1}{3})$
$X^4 - 2X^3 - 12X^2 + 3X + 21$	366525	$X^2 + (-\theta^3 + 4\theta^2 + 5\theta - 17)$
$X^4 - 2X^3 - 28X^2 + 8X + 142$	366912	$X^2 + X + (-\theta - 3)$
$X^4 - 2X^3 - 13X^2 + 7X + 33$	368449	$X^2 + (\theta^3 - 4\theta^2 - 4\theta + 12)$
$X^4 - X^3 - 66X^2 + 5X + 905$	369025	$X^2 + (\frac{2}{47}\theta^3 - \frac{24}{47}\theta^2 - \frac{432}{47}\theta - \frac{1301}{47})$
$X^4 - X^3 - 61X^2 + 30X + 900$	369025	$X^2 + (\frac{1}{30}\theta^3 - \frac{1}{30}\theta^2 - \frac{31}{30}\theta)X + (\theta - 7)$
$X^4 - 2X^3 - 20X^2 - 4X + 24$	370900	$X^2 + (\frac{-1}{2}\theta^3 - 2\theta^2 - \theta + 1)$
$X^4 - 52X^2 - 48X + 337$	370944	$X^2 + (\frac{-58}{119}\theta^3 - \frac{375}{119}\theta^2 + \frac{138}{119}\theta + \frac{2080}{119})$
$X^4 - X^3 - 20X^2 + 12X + 64$	371900	$X^2 + (-\theta - 4)$
$X^4 - 2X^3 - 13X^2 + 6X + 31$	372544	$X^2 + X + (-\theta - 2)$
$X^4 - X^3 - 23X^2 + 35X + 52$	373388	$X^2 + (\frac{-1}{2}\theta^3 - \theta^2 + \frac{17}{2}\theta + 6)X + (-\theta^3 - 2\theta^2 + 16\theta + 12)$
$X^4 - 20X^2 - 20X + 35$	376000	$X^2 + X + (-\theta - 3)$
$X^4 - X^3 - 62X^2 + 23X + 919$	376025	$X^2 + (\frac{1}{20}\theta^3 - \frac{1}{5}\theta^2 - \frac{3}{2}\theta + \frac{93}{20})X + (-\theta - 5)$
$X^4 - 16X^2 - 12X + 15$	377664	$X^2 + (\frac{-1}{2}\theta^2 + \frac{7}{2})X + (\theta + 2)$
$X^4 - 2X^3 - 60X^2 + 61X + 929$	377725	$X^2 - X + (-\theta^2 + 24)$
$X^4 - X^3 - 68X^2 + 66X + 911$	377725	$X^2 + (\frac{-2}{129}\theta^3 - \frac{8}{43}\theta^2 - \frac{47}{129}\theta - \frac{98}{129})$
$X^4 - 2X^3 - 26X^2 + 27X + 76$	382925	$X^2 + (\frac{-1}{5}\theta^2 + \frac{6}{5}\theta - \frac{9}{5})$
$X^4 - X^3 - 64X^2 + 49X + 931$	383625	$X^2 + (\frac{-1}{14}\theta^3 - \frac{3}{7}\theta^2 + \frac{18}{7}\theta + \frac{27}{2})X + (-\theta - 6)$
$X^4 - 20X^2 + 60$	384000	$X^2 + X + (\frac{-1}{4}\theta^3 - \frac{1}{2}\theta^2 + \frac{5}{2}\theta - 1)$
$X^4 - 10X^2 + 15$	384000	$X^2 + (2\theta + 1)X + (\theta^2 + \theta - 1)$
$X^4 - 2X^3 - 19X^2 + 20X + 10$	385600	$X^2 + (\theta - 1)X + (\frac{1}{3}\theta^2 - \frac{4}{3}\theta - \frac{13}{3})$
$X^4 - 2X^3 - 25X^2 + 26X + 129$	385600	$X^2 + (\theta - 1)X + (\frac{1}{6}\theta^3 + \frac{1}{2}\theta^2 - \frac{25}{6}\theta - 8)$
$X^4 - X^3 - 20X^2 - 8X + 24$	387925	$X^2 + (\frac{1}{4}\theta^3 - \frac{1}{4}\theta^2 - 4\theta - 6)$

$X^4-17X^2-27X-1$	388409	$X^3+(-\theta-4)X+(\theta+2)$
X^4-52X^2+169	389376	$X^2-X+(\frac{-1}{13}\theta^2+\theta-3)$
X^4-40X^2+361	389376	$X^2+(-4\theta^2+55)$
X^4-16X^2+25	389376	$X^2+(-4\theta^2+7)$
$X^4-X^3-23X^2+X+6$	389800	$X^2+(\frac{1}{4}\theta^3-\frac{23}{4}\theta-\frac{13}{2})$
X^4-64X^2+979	391600	$X^2+(\frac{-1}{6}\theta^2+\frac{35}{6})X+(\frac{-1}{6}\theta^2-\theta-\frac{1}{6})$
X^4-69X^2+979	391600	$X^2+(\frac{-1}{13}\theta^2+\frac{28}{13})X+(\frac{-1}{13}\theta^2-\theta-\frac{37}{13})$
X^4-70X^2+980	392000	$X^2+(\frac{-1}{14}\theta^2+3)X+(\frac{-1}{7}\theta^2-\theta-1)$
$X^4-2X^3-65X^2+66X+964$	392225	$X^2+X+(\frac{-1}{10}\theta^2-\frac{9}{10}\theta-\frac{16}{5})$
$X^4-X^3-63X^2+36X+956$	392225	$X^2+(-\theta-7)$
$X^4-X^3-64X^2+19X+961$	392625	$X^2+(\theta-7)$
$X^4-16X^2-5X+49$	392725	$X^2+(-\theta-3)$
$X^4-2X^3-66X^2+67X+971$	395125	$X^2+(\frac{1}{11}\theta^2-\frac{12}{11}\theta-\frac{116}{11})$
$X^4-X^3-64X^2+44X+961$	395125	$X^2+(\frac{-2}{9}\theta^3-\frac{17}{9}\theta^2+\frac{79}{9}\theta+\frac{487}{9})$
$X^4-X^3-9X^2+4X+6$	395500	$X^2+\theta X-2$
$X^4-2X^3-63X^2+64X+979$	398025	$X^2+X+(\frac{-1}{3}\theta^2+\frac{4}{3}\theta+\frac{8}{3})$
$X^4-X^3-67X^2+58X+964$	398025	$X^2+(\frac{-7}{62}\theta^3-\frac{1}{62}\theta^2+\frac{273}{62}\theta-\frac{233}{31})$
$X^4-2X^3-25X^2+26X+9$	398400	$X^2+\theta X+(\frac{1}{4}\theta^2+\frac{3}{4}\theta-\frac{17}{4})$
$X^4-2X^3-23X^2+24X+134$	398400	$X^2+\theta X+(\frac{-1}{3}\theta^3+2\theta^2+\frac{11}{3}\theta-\frac{65}{3})$
$X^4-2X^3-69X^2+70X+980$	399025	$X^3+(\frac{1}{14}\theta^3-\frac{43}{14}\theta-9)X+(\frac{1}{14}\theta^3+\frac{5}{14}\theta^2-\frac{31}{7}\theta-19)$
$X^4-X^3-15X^2-13X+9$	400325	$X^2+(-\theta^3-3\theta^2-\theta+1)$
$X^4-2X^3-49X^2+8X+376$	401472	$X^2+(\frac{4}{43}\theta^3-\frac{5}{43}\theta^2-\frac{146}{43}\theta-\frac{314}{43})$
$X^4-2X^3-39X^2+40X+382$	401472	$X^2+(\frac{-1}{3}\theta^2+\frac{4}{3}\theta+\frac{2}{3})$
$X^4-X^3-65X^2+47X+979$	402725	$X^2+(\theta-6)$
$X^4-2X^3-62X^2+63X+991$	402725	$X^2-X+(\theta-6)$
$X^4-X^3-14X^2+4X+36$	404500	$X^2+(\theta^2-\theta-11)$
X^4-36X^2+177	407808	$X^2+\theta X+(\frac{2}{7}\theta^2-\frac{8}{7})$
$X^4-2X^3-26X^2+27X+51$	407925	$X^2+(\frac{-1}{5}\theta^2+\frac{6}{5}\theta-\frac{9}{5})$
$X^4-2X^3-41X^2+42X+391$	411200	$X^2+(\frac{-1}{5}\theta^2-\frac{4}{5}\theta-\frac{4}{5})$
$X^4-2X^3-10X^2+X+9$	411925	$X^2+(-\theta^2-\theta)$
$X^4-2X^3-17X^2-17X+1$	413825	$X^2+(\theta^3-4\theta^2-9\theta+2)X+(-\theta^3+4\theta^2+8\theta)$
$X^4-20X^2-40X-15$	416000	$X^4+2X^3+(\theta^2-3\theta-14)X^2+(\theta^2-3\theta-15)X$ $+(-\theta^3+21\theta+37)$
$X^4-30X^2-20X+90$	416000	$X^4-2X^3+(-\theta-4)X^2+(\theta+5)X$ $+(\frac{-1}{9}\theta^3-\frac{2}{9}\theta^2+\frac{26}{9}\theta+7)$
X^4-66X^2+1044	417600	$X^2+(\frac{1}{6}\theta^2-5)X+(\theta-7)$
X^4-65X^2+1045	418000	$X^2+(\frac{1}{3}\theta^2-\frac{34}{3})X+(\frac{1}{3}\theta^3+\frac{2}{3}\theta^2-\frac{34}{3}\theta-\frac{83}{3})$
$X^4-X^3-19X^2-16X+16$	421500	$X^2+(-\theta-3)$
$X^4-2X^3-45X^2+46X+401$	422464	$X^2+(\frac{1}{4}\theta^3-\frac{3}{2}\theta^2-\frac{5}{2}\theta+\frac{47}{4})$
$X^4-2X^3-43X^2+22X+391$	422464	$X^2+(\frac{-2}{9}\theta^3+\frac{5}{9}\theta^2+\frac{34}{9}\theta-\frac{97}{9})$
X^4-12X^2-5X+1	426325	$X^2+(\theta^3-12\theta-7)$
$X^4-19X^2-3X+80$	426497	$X^3+(-\theta^2+10)X^2+(\theta+1)X-1$
$X^4-2X^3-8X^2+9X+4$	426725	$X^2+(2\theta-1)X+(\theta^2-\theta-1)$
$X^4-X^3-35X^2-23X+139$	426725	$X^2+(\frac{-4}{23}\theta^3+\frac{5}{23}\theta^2+\frac{64}{23}\theta-\frac{108}{23})$
$X^4-X^3-18X^2+X+1$	426725	$X^2+(\frac{1}{2}\theta^3-\theta^2-7\theta-\frac{3}{2})$
$X^4-2X^3-70X^2+71X+1049$	426725	$X^2+(\frac{-1}{13}\theta^2-\frac{12}{13}\theta-\frac{36}{13})$
$X^4-X^3-72X^2+3X+1049$	427025	$X^2+X+(\frac{-3}{28}\theta^3+\frac{1}{2}\theta^2+\frac{59}{14}\theta-\frac{591}{28})$
$X^4-X^3-66X^2+25X+1045$	427025	$X^4+2X^3+(\frac{-1}{22}\theta^3+\frac{13}{11}\theta^2+\frac{5}{11}\theta-\frac{87}{2})X^2$ $+(\frac{-1}{22}\theta^3+\frac{13}{11}\theta^2+\frac{5}{11}\theta-\frac{89}{2})X$ $+(\frac{-9}{22}\theta^3-\frac{15}{11}\theta^2+\frac{199}{11}\theta+\frac{143}{2})$
X^4-44X^2+159	429936	$X^2+(\frac{-1}{10}\theta^2+\frac{17}{10})X+(\frac{-1}{10}\theta^2+\theta-\frac{13}{10})$
X^4-31X^2+159	429936	$X^2+(\frac{1}{5}\theta^2-\frac{18}{5})X+(\frac{-1}{5}\theta^2+\theta-\frac{2}{5})$

$X^4 - X^3 - 18X^2 + 36X - 9$	431325	$X^2 + X + (\frac{1}{3}\theta^3 + \frac{2}{3}\theta^2 - 5\theta - 4)$
$X^4 - X^3 - 13X^2 - 11X + 1$	433557	$X^2 + (-\theta - 3)$
$X^4 - 10X^2 - 3X + 4$	433557	$X^2 - X + (\theta - 3)$
$X^4 - 35X^2 + 100$	435600	$X^2 - X + (\frac{-1}{5}\theta^2 + \theta - 1)$
$X^4 - 29X^2 + 169$	435600	$X^2 + (\frac{-1}{13}\theta^3 + \frac{16}{13}\theta - 1)X + (\theta - 3)$
$X^4 - 13X^2 + 1$	435600	$X^2 + (\theta^3 - 12\theta + 1)X + (\theta + 1)$
$X^4 - 2X^3 - 23X^2 + 9X + 54$	435825	$X^2 + X + (\frac{2}{15}\theta^3 - \frac{1}{15}\theta^2 - \frac{8}{3}\theta - \frac{29}{5})$
$X^4 - X^3 - 69X^2 + 14X + 1076$	438625	$X^2 + (\frac{1}{17}\theta^3 - \frac{9}{17}\theta^2 - \frac{48}{17}\theta + \frac{143}{17})$
$X^4 - 2X^3 - 14X^2 + 10X + 40$	442100	$X^2 + X + (-\theta - 3)$
$X^4 - X^3 - 10X^2 + 2X + 14$	442900	$X^2 + (\theta - 1)X + (-\theta - 1)$
$X^4 - 2X^3 - 45X^2 + 20X + 412$	443456	$X^2 + (-2\theta - 9)$
$X^4 - 68X^2 + 1111$	444400	$X^2 + X + (\frac{1}{6}\theta^3 + \frac{1}{3}\theta^2 - \frac{37}{6}\theta - \frac{52}{3})$
$X^4 - 67X^2 + 1111$	444400	$X^2 - X + (\theta - 6)$
$X^4 - X^3 - 25X^2 + 12X + 72$	444412	$X^2 + (\frac{4}{9}\theta^3 - \frac{34}{9}\theta^2 + \frac{2}{9}\theta + \frac{35}{3})$
$X^4 - X^3 - 22X^2 - 13X + 25$	444412	$X^2 + (\frac{1}{9}\theta^3 + \frac{1}{9}\theta^2 - \frac{29}{9}\theta - \frac{71}{9})$
$X^4 - X^3 - 19X^2 + 23X + 4$	444412	$X^2 + (\frac{1}{6}\theta^3 - \frac{1}{3}\theta^2 - \frac{11}{6}\theta - \frac{1}{3})$
$X^4 - 52X^2 + 434$	444416	$X^2 + (\frac{-1}{11}\theta^2 + \frac{15}{11})X + (\theta - 5)$
$X^4 - 28X^2 + 193$	444672	$X^2 + \theta X + 3$
$X^4 - 20X^2 - 24X + 25$	444672	$X^2 + (\frac{-1}{3}\theta^3 + \frac{2}{3}\theta^2 + \frac{13}{3}\theta - \frac{5}{3})X + (-\theta - 3)$
$X^4 - 2X^3 - 69X^2 + 70X + 1100$	447025	$X^3 + (\frac{-1}{10}\theta^2 + \frac{1}{10}\theta + 3)X^2 + (\frac{-1}{10}\theta^2 - \frac{9}{10}\theta - 2)X + (\frac{1}{10}\theta^2 + \frac{9}{10}\theta + 2)$
$X^4 - 2X^3 - 9X^2 + 10X + 15$	449600	$X^2 + (2\theta - 1)X + (\theta^2 - \theta - 1)$
$X^4 - 26X^2 - 40X + 24$	449600	$X^2 - \frac{1}{2}\theta^2$
$X^4 - 2X^3 - 66X^2 + 67X + 1111$	451125	$X^2 + (\frac{-1}{3}\theta^3 + \frac{4}{3}\theta^2 + \frac{32}{3}\theta - 41)$
$X^4 - X^3 - 74X^2 + 4X + 1121$	456125	$X^2 + (\frac{19}{139}\theta^3 - \frac{127}{139}\theta^2 - \frac{589}{139}\theta + \frac{2590}{139})$
$X^4 - X^3 - 69X^2 + 49X + 1111$	456125	$X^2 + (\theta^3 + 5\theta^2 - 38\theta - 180)X + (\theta - 6)$
$X^4 - 2X^3 - 9X^2 + 4X + 9$	456944	$X^2 + X + (-\theta - 2)$
$X^4 - 15X^2 - 10X - 1$	456944	$X^2 + X + (\theta^3 - 15\theta - 10)$
$X^4 - X^3 - 72X^2 + 63X + 1109$	457025	$X^4 + (\frac{-1}{80}\theta^3 - \frac{1}{8}\theta^2 + \frac{21}{40}\theta + \frac{399}{80})X^3 + (\frac{1}{80}\theta^3 + \frac{1}{8}\theta^2 - \frac{21}{40}\theta - \frac{799}{80})X^2 + (\frac{3}{20}\theta^3 + \frac{1}{2}\theta^2 - \frac{63}{10}\theta - \frac{377}{20})X - 1$
$X^4 - 2X^3 - 73X^2 + 74X + 1124$	457025	$X^2 + (\frac{1}{14}\theta^2 - \frac{1}{14}\theta - \frac{15}{7})X + (\frac{1}{14}\theta^3 - \frac{45}{14}\theta - \frac{57}{7})$
$X^4 - 2X^3 - 51X^2 + 52X + 434$	457792	$X^3 + (\frac{-1}{11}\theta^2 - \frac{10}{11}\theta - \frac{40}{11})X + (\frac{-1}{11}\theta^2 - \frac{10}{11}\theta - \frac{18}{11})$
$X^4 - 70X^2 + 1145$	458000	$X^2 + (\frac{-1}{8}\theta^2 + \frac{31}{8})X + (\frac{1}{8}\theta^3 + \frac{1}{4}\theta^2 - \frac{39}{8}\theta - \frac{59}{4})$
$X^4 - 12X^2 - 5X + 21$	458325	$X^2 + (-\theta - 3)$
$X^4 - X^3 - 15X^2 + 4X + 16$	458345	$X^2 + (-\theta + 1)X + (\frac{-1}{4}\theta^3 + \frac{1}{4}\theta^2 + \frac{7}{4}\theta - 2)$
$X^4 - 2X^3 - 23X^2 + 24X + 28$	458345	$X^2 + \theta X + (\frac{1}{4}\theta^2 - \frac{1}{4}\theta - \frac{3}{2})$
$X^4 - 60X^2 + 450$	460800	$X^2 - X + (\frac{-1}{5}\theta^2 - \theta - 1)$
$X^4 - 2X^3 - 27X^2 + 28X + 193$	460944	$X^2 - \theta X + 2$
$X^4 - 33X^2 - 24X + 177$	460944	$X^2 + (\theta^2 - 2\theta - 23)$
$X^4 - 2X^3 - 22X^2 + 23X + 94$	461533	$X^3 + \theta X^2 + (\frac{1}{3}\theta^2 - \frac{1}{3}\theta - \frac{10}{3})X + (-\theta - 2)$
$X^4 - 2X^3 - 69X^2 + 70X + 1055$	462400	$X^2 - X + (\frac{5}{131}\theta^3 + \frac{58}{131}\theta^2 - \frac{316}{131}\theta - \frac{3083}{131})$
$X^4 - 2X^3 - 45X^2 + 46X + 359$	462400	$X^2 + (\frac{-2}{7}\theta^3 - \frac{11}{7}\theta^2 + \frac{32}{7}\theta + \frac{127}{7})$
$X^4 - 2X^3 - 27X^2 + 28X + 26$	462400	$X^2 + (\frac{2}{23}\theta^3 - \frac{26}{23}\theta^2 + \frac{2}{23}\theta + \frac{11}{23})$
$X^4 - 22X^2 + 36$	462400	$X^2 + (\frac{-1}{6}\theta^3 + \frac{8}{3}\theta - 1)X + (\theta - 2)$
$X^4 - 18X^2 - 12X + 30$	463104	$X^2 - X + (-\theta - 4)$
$X^4 - 2X^3 - 18X^2 + 4X + 4$	464400	$X^2 + (\frac{1}{2}\theta^3 - \theta^2 - 10\theta + 1)X + (\theta + 5)$
$X^4 - 2X^3 - 15X^2 + 16X + 4$	464400	$X^2 - X + (\frac{1}{2}\theta^3 - \frac{1}{2}\theta^2 - 7\theta - 5)$
$X^4 - 2X^3 - 69X^2 + 70X + 1145$	465025	$X^2 - X + (\frac{-1}{8}\theta^2 - \frac{7}{8}\theta - \frac{9}{8})$
$X^4 - X^3 - 76X^2 + 75X + 1125$	465025	$X^2 + (\frac{4}{45}\theta^3 + \frac{11}{45}\theta^2 - \frac{184}{45}\theta - \frac{44}{3})$
$X^4 - 2X^3 - 16X^2 + 17X - 4$	465125	$X^2 + (\theta^3 - 2\theta^2 - 19\theta + 7)$
$X^4 - 46X^2 - 20X + 434$	467200	$X^2 + (\frac{-1}{3}\theta^3 + \frac{5}{3}\theta^2 + 8\theta - \frac{97}{3})X + (-\theta - 5)$

$X^4 - 2X^3 - 68X^2 + 69X + 1159$	470525	$X^2 + X + (\theta - 8)$
$X^4 - X^3 - 71X^2 + 55X + 1145$	470525	$X^2 + (\theta - 8)$
$X^4 - 16X^2 + 35$	470960	$X^2 + \theta X + (\frac{1}{2}\theta^2 - \frac{7}{2})$
$X^4 - 13X^2 + 35$	470960	$X^2 + \theta X + (\theta^2 - 7)$
$X^4 - 2X^3 - 12X^2 + 3X + 1$	471325	$X^2 + (-\theta^3 + 2\theta^2 + 12\theta - 6)$
$X^4 - 10X^2 - 4X + 6$	473344	$X^2 + (\theta - 1)X + (-\theta - 1)$
$X^4 - X^3 - 10X^2 + 7X + 14$	474425	$X^2 + (\theta - 1)X - 1$
$X^4 - 33X^2 + 100$	474721	$X^2 + (\frac{1}{10}\theta^3 - \frac{23}{10}\theta)X + (\frac{1}{20}\theta^3 - \frac{43}{20}\theta - \frac{1}{2})$
$X^4 - 74X^2 + 1189$	475600	$X^2 + (\frac{1}{12}\theta^2 - \frac{31}{12})X + (\frac{-1}{12}\theta^2 + \theta - \frac{53}{12})$
$X^4 - 69X^2 + 1189$	475600	$X^2 + (\theta^2 - 34)X + (\theta^2 + \theta - 42)$
$X^4 - 2X^3 - 13X^2 - 2X + 15$	476224	$X^2 + \theta X + (\theta^2 - 2\theta - 8)$
$X^4 - X^3 - 17X^2 + 4X + 61$	476249	$X^2 + (-\theta - 3)$
$X^4 - 17X^2 - 3X + 62$	476249	$X^2 - \theta X + 1$
$X^4 - X^3 - 12X^2 + 9X + 26$	476249	$X^2 + X + (-\theta^2 + \theta + 3)$
$X^4 - X^3 - 13X^2 - 4X + 1$	477825	$X^2 + (-\theta - 3)$
$X^4 - X^3 - 23X^2 - 19X + 26$	481300	$X^2 + X + (\frac{1}{4}\theta^3 - \frac{1}{2}\theta^2 - \frac{17}{4}\theta - \frac{9}{2})$
$X^4 - X^3 - 14X^2 + 19X + 16$	481625	$X^2 + (-\theta - 4)$
$X^4 - X^3 - 33X^2 + 95X - 50$	483516	$X^2 + (\frac{2}{5}\theta^3 + \frac{3}{5}\theta^2 - \frac{56}{5}\theta + 7)$
$X^4 - 24X^2 + 111$	483516	$X^2 + X + (\theta - 4)$
$X^4 - 16X^2 - 4X + 31$	484672	$X^2 + (\frac{-1}{2}\theta^2 + \frac{7}{2})X + 1$
$X^4 - 29X^2 + 36$	485809	$X^3 + (\theta + 1)X^2 + (\frac{1}{12}\theta^3 + \frac{1}{2}\theta^2 - \frac{17}{12}\theta - \frac{15}{2})X + 5$
$X^4 - 15X^2 - 10X + 15$	486000	$X^2 + (-\theta - 1)X + (\frac{-1}{3}\theta^3 + \frac{2}{3}\theta^2 + \frac{14}{3}\theta - 3)$
$X^4 - 70X^2 + 1220$	488000	$X^2 + (\frac{1}{2}\theta^2 - 17)X + (\theta - 6)$
$X^4 - X^3 - 15X^2 - 4X + 29$	489937	$X^3 + (-\theta^3 + 3\theta^2 + 8\theta - 10)X^2 + (-\theta + 2)X - 1$
$X^4 - 42X^2 + 424$	490144	$X^2 + X + (\frac{1}{4}\theta^3 + \theta^2 - \frac{13}{2}\theta - 26)$
$X^4 - 21X^2 + 106$	490144	$X^2 + \theta X + 2$
$X^4 - 2X^3 - 10X^2 + X + 4$	491325	$X^2 + (\theta - 1)X + (\theta^2 - 2\theta - 7)$
$X^4 - 62X^2 - 60X + 450$	491776	$X^2 + X + (\frac{1}{15}\theta^3 - \frac{47}{15}\theta - 8)$
$X^4 - 48X^2 - 24X + 457$	491776	$X^2 + X + (-\theta - 5)$
$X^4 - X^3 - 34X^2 - 59X + 1$	491985	$X^2 - X + (\frac{3}{14}\theta^3 - \frac{2}{7}\theta^2 - \frac{48}{7}\theta - \frac{173}{14})$
$X^4 - X^3 - 16X^2 + 19X + 13$	491985	$X^2 + (-\theta - 4)$
$X^4 - 2X^3 - 19X^2 + 19X + 19$	494209	$X^2 + \theta X + (\frac{1}{9}\theta^3 + \frac{2}{9}\theta^2 - \frac{20}{9}\theta - \frac{16}{9})$
$X^4 - X^3 - 50X^2 - 48X + 159$	494325	$X^2 + (\frac{17}{103}\theta^3 + \frac{2}{103}\theta^2 - \frac{872}{103}\theta - \frac{2039}{103})$
$X^4 - 28X^2 + 183$	494832	$X^2 + \theta X + (\frac{1}{2}\theta^2 - \frac{9}{2})$
$X^4 - 37X^2 + 183$	494832	$X^2 + \theta X + (\frac{2}{7}\theta^2 - \frac{9}{7})$
$X^4 - X^3 - 10X^2 + 9X + 10$	496129	$X^2 + (\theta - 3)$
$X^4 - X^3 - 17X^2 - 10X - 1$	496129	$X^2 + X + (\theta^3 - \theta^2 - 17\theta - 10)$
$X^4 - 2X^3 - 13X^2 - 5X + 9$	496129	$X^2 + X + (-\theta - 2)$
$X^4 - 11X^2 - 8X + 3$	496304	$X^2 + X + (-\theta - 3)$
$X^4 - 13X^2 - 12X - 1$	496304	$X^2 - \theta X + \theta$
$X^4 - 2X^3 - 16X^2 - 12X + 7$	497872	$X^2 + X + (-\theta - 2)$
$X^4 - X^3 - 15X^2 - 3X + 9$	498525	$X^2 + (\frac{1}{3}\theta^3 - \frac{1}{3}\theta^2 - 4\theta - 1)X + 1$
$X^4 - 2X^3 - 14X^2 + 15X + 35$	498525	$X^2 + (\frac{1}{3}\theta^3 - \frac{14}{3}\theta - \frac{16}{3})$
$X^4 - 46X^2 - 12X + 466$	499968	$X^2 - X + (-\theta - 5)$