N$^{O}$ d'ordre : 2015.

# THÈSE

présentée à

**L'UNIVERSITÉ BORDEAUX I**

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

PAR **Denis SIMON**

POUR OBTENIR LE GRADE DE

**DOCTEUR**

SPÉCIALITÉ : MATHÉMATIQUES PURES

---

## Équations dans les Corps de Nombres et Discriminants Minimaux

---

Soutenue le 21 décembre 1998

Après avis de :

| | | | | |
|---|---|---|---|---|
| MM | A. LEUTBECHER | Professeur | Technische Universität München | Rapporteurs |
| | M. POHST | Professeur | Technische Universität Berlin | |

Devant la commission d'examen formée de :

| | | | | |
|---|---|---|---|---|
| MM | Ph. CASSOU-NOGUÈS | Professeur | Université Bordeaux I | Président |
| | F. DIAZ Y DIAZ | Professeur | Université Bordeaux I | Rapporteur |
| | H. COHEN | Professeur | Université Bordeaux I | Examinateurs |
| | J. CREMONA | Professeur | University of Exeter | |
| | A. LEUTBECHER | Professeur | Technische Universität München | |
| | G. NIKLASCH | Docteur | Technische Universität München | |
| | E. REYSSAT | Professeur | Université de Caen | |

– 1998 –

C'est peu de choses que d'adresser mes remerciements à mon directeur de thèse Henri Cohen, qui ne m'a pas consacré seulement du temps mais tout son temps, à m'initier à la recherche en Mathématiques. Il m'a convaincu que cette recherche est un jeu des plus passionnants.

Après m'être largement inspiré du travail de John Cremona sur les courbes elliptiques, j'ai eu la chance de travailler personnellement avec lui. Je le remercie pour l'interêt qu'il m'a porté.

J'adresse ma gratitude aux professeurs allemands Armin Leutbecher et Michael Pohst qui ont accepté de rapporter ma thèse malgré sa rédaction en français.

Je suis reconnaissant envers Gerhard Niklasch pour son travail admirable de relecture.

Je remercie Philippe Cassou-Noguès, Francisco Diaz y Diaz et Eric Reyssat pour leur participation au jury.

Par l'intermédiaire de Michel Olivier, je remercie tous ceux qui ont consacré du temps à répondre à mes nombreuses questions, et plus généralement tous les membres de l'A2X, qui m'ont proposé un accueil et une ambiance de travail remarquables.

Je remercie Véronique Saint-Martin et Joëlle Pargade pour leur efficacité sans faille.

Je remercie mes collègues de bureau Karim, Christophe et Sami pour tout le temps que nous avons passé ensemble, ainsi que mes autres camarades, doctorants ou déjà docteurs.

Je n'oublie pas de citer Pari et Muscida avec qui j'ai passé tant d'heures, et qui ont travaillé pour moi nuit et jour, y compris le week-end.

Je remercie ma femme Carine et mes deux filles Doriane et Margot, pour tout le soutien qu'elles m'ont apporté dans ce long travail, et l'énergie qu'elles ont dépensée à essayer de comprendre toutes ces choses compliquées. Je les remercie d'autant plus pour la curieuse propriété que leurs âges $C$, $D$ et $M$ vérifient : $C$ divise $M|C$, qui divise lui-même $D|M|C$, qui divise lui-même $p^p$, où $p$ est un nombre premier, et où le signe $|$ désigne l'opération de juxtaposition des chiffres.

Je remercie aussi tous ceux qui ont participé à cette thèse, en particulier à la soutenance, et je présente mes excuses à tous ceux que cette thèse aura dérangés.

Je tiens enfin à remercier tous ceux qui m'ont donné le goût des Mathématiques et ceux qui m'ont encouragé dans cette voie, particulièrement ma famille. Plus généralement, je remercie tous ceux qui, au moins une fois, n'ont pas fui quand je leur ai avoué que je faisais une thèse de Mathématiques Pures.

*"Et concrètement, ça sert à quoi ?"*

# Table des matières

**Remerciements** **3**

**Table des Matières** **3**

**Introduction** **9**

**Mots-Clés et Notations** **13**

**I $S$-Unités et Groupes de Classes Relatifs** **15**
Qu'est-ce qu'un $S$-Entier ou une $S$-Unité ? . . . . . 15
I.1 $S$-Unités . . . . . 16
I.1.1 Définitions, Notations et Propriétés . . . . . 16
I.1.2 Algorithmes . . . . . 17
I.2 Groupes de Classes Relatifs . . . . . 20
I.2.1 Définitions . . . . . 21
I.2.2 Relations Entre les Différents Groupes de Classes Relatifs . . . . . 22
I.2.3 Algorithmes pour les Groupes de Classes Relatifs . . . . . 23

**II Équations de Legendre et Courbes Elliptiques** **25**
II.1 Propriétés de l'Équation de Legendre . . . . . 26
II.2 Symboles de Hilbert et Symboles de Legendre . . . . . 27
II.2.1 Définitions et Propriétés . . . . . 27
II.2.2 Places Au-Dessus de 2 . . . . . 30
II.3 Résolution de l'Équation de Legendre . . . . . 32
II.3.1 Résolution dans le Corps $\mathbb{Q}$ des Rationnels . . . . . 32
II.3.2 Résolution dans les Corps de Nombres . . . . . 36
1 Cas Terminaux . . . . . 37
2 Descente . . . . . 38
3 Corps non Principaux . . . . . 38
II.4 Applications aux Courbes Elliptiques . . . . . 38
II.4.1 Le Groupe $K(S, 2)$ . . . . . 39
II.4.2 Quartiques . . . . . 41
II.4.3 Descente par 2-Isogénie : Courbes avec 2-Torsion . . . . . 42

II.4.4 Exemple du Calcul du Rang d'une Courbe avec 2-Torsion . . . . . 45
II.4.5 Algorithme pour les Courbes sans 2-Torsion . . . . . 46
II.4.6 Exemple du Calcul du Rang d'une Courbe Sans 2-Torsion . . . . . 49

**III Équations aux Normes** **53**
Introduction . . . . . 53
III.1 Équations aux Normes dans les Extensions Galoisiennes . . . . . 55
III.1.1 Preuve du Théorème Principal pour les Extensions Galoisiennes . . . 55
III.1.2 Structure dans le Cas Galoisien . . . . . 58
III.1.3 Cas Particulier des Extensions Cycliques . . . . . 61
III.2 Équations aux Normes dans les Extensions Non Galoisiennes . . . . . 62
III.2.1 Préliminaires . . . . . 62
III.2.2 Preuve du Théorème Principal pour les Extensions Non Galoisiennes 64
III.2.3 Cas Particulier des Extensions de $\mathbb{Q}$ . . . . . 70
III.2.4 Existence de Solutions Entières . . . . . 72
III.3 Équations aux Normes : l'Algorithme . . . . . 74
III.3.1 Déterminer les Ensembles $S_0$ et $S$ . . . . . 74
III.3.2 Recherche de Solutions en $S$-unités . . . . . 75
III.3.3 Recherche de Solutions Entières ou $S$-Entières . . . . . 76

**IV Discriminants Minimaux** **79**
Qu'est-ce qu'un Discriminant ? . . . . . 79
IV.1 Quelques Propriétés des Résultants et des Discriminants . . . . . 81
IV.2 Discriminants Minimaux pour les Petits Degrés . . . . . 84
IV.2.1 Polynômes Irréductibles . . . . . 84
1 Petits Coefficients . . . . . 85
2 Petites Variations des Coefficients . . . . . 88
3 Petites Variations des Racines . . . . . 89
4 Extensions Relatives . . . . . 90
5 Semi-Extensions Relatives . . . . . 93
6 Polynômes de Résultant 1 . . . . . 95
IV.2.2 Polynômes Factorisables . . . . . 99
IV.3 Comportement Asymptotique des Petits Discriminants . . . . . 105
IV.3.1 Polynômes Cyclotomiques . . . . . 106
IV.3.2 Familles de Polynômes Irréductibles . . . . . 106
IV.3.3 Polynômes Fortement Premiers Entre Eux . . . . . 109
IV.3.4 Familles de Polynômes Factorisables . . . . . 113

**Annexes** **116**

**A Tables de Discriminants Minimaux** **117**

**B Corps Primitifs et Imprimitifs** **125**

**C Polynômes de Discriminants Minimaux** **133**

**Bibliographie** **147**

**Résumé** **150**

# Introduction Générale

Dans cette thèse, je propose des réponses à plusieurs problèmes différents. Ces problèmes sont essentiellement la résolution explicite de certaines équations diophantiennes dans les corps de nombres, puis la détermination de polynômes satisfaisant certaines conditions de minimalité. J'apporte à la fois des réponses théoriques, et des algorithmes qui résolvent complètement les équations proposées en s'appuyant sur les théorèmes que je démontre.

Je commence par un premier chapitre (chapitre I) contenant la description de certains outils nécessaires aux chapitres suivants : les $S$-unités et les groupes de classes.

Le premier problème que je me suis posé est la détermination algorithmique du rang d'une courbe elliptique (chapitre II). Un tel algorithme existait déjà pour les courbes elliptiques définies sur $\mathbb{Q}$ (voir [Cre a]), et mon but était de le généraliser aux corps de nombres. Plus précisément, une courbe elliptique est donnée par une équation de la forme

$$y^2 = x^3 + ax^2 + bx + c.$$

Les solutions rationnelles de cette équation forment un groupe abélien de type

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/mZ) \times \mathbb{Z}^r.$$

L'algorithme que je décris détermine le rang $r$ et exhibe un système de points de rang maximal sur cette courbe. Je décris en fait deux algorithmes qui correspondent aux cas où la courbe possède de la 2-torsion ou non, c'est-à-dire aux cas où le polynôme $x^3+ax^2+bx+c$ possède une racine ou non. Dans le premier cas (avec 2-torsion), un tel algorithme, dit de *descente par 2-isogénie*, est déjà connu (voir [Sil]), identique à la situation dans $\mathbb{Q}$, et je l'ai implanté dans le cas des corps de nombres. Pour le deuxième cas (sans 2-torsion), je propose un algorithme, issu d'un travail d'une année en commun avec J. Cremona. Ce nouvel algorithme m'a permis de calculer le rang de certaines courbes elliptiques dans des corps de nombres jusque là inaccessibles. Une des étapes de cette résolution consiste à trouver des solutions à l'équation de Legendre

$$x^2 - ay^2 = bz^2.$$

Je consacre donc une importante partie à la résolution complète de cette équation dans un corps de nombres $K$, aussi bien pour l'existence de solutions que pour la construction d'une solution particulière. La première idée que j'ai eue était de considérer cette équation comme une norme dans l'extension $K(\sqrt{a})/K$. Cette idée n'était pas la meilleure pour résoudre l'équation de Legendre et je décris un algorithme qui ne repose pas sur cette idée. Cet algorithme est tout à fait efficace et ne nécessite pas de calculer dans d'autre corps que $K$. Toutefois, cette idée est à l'origine du thème du chapitre suivant.

Le deuxième problème (chapitre III) est celui de la résolution de l'équation aux normes

$$\mathcal{N}_{L/K}(x) = a$$

où $L/K$ est une extension relative de corps de nombres fixée, et $a$ un élément de $K$. À partir de plusieurs exemples de résolution en degré 2, j'ai pu déduire la nature des solutions d'une telle équation dans le cas des extensions galoisiennes : l'expérience suggérait que les solutions exprimées en termes de $S$-unités se décrivent à partir du groupe de classes relatif de $L/K$, il ne restait plus qu'à démontrer précisément ce résultat. Toujours à partir d'expériences, ainsi que d'un article de H.J. Bartels (voir [Bar]), j'ai pu généraliser ce résultat aux extensions relatives quelconques. Je montre que sous certaines conditions décrites par des groupes de classes, les $S$-unités qui sont des normes sont identiques aux normes de $S$-unités. Lorsque ces conditions ne sont pas vérifiées, je décris, à l'aide des groupes de classes relatifs, le groupe qui mesure l'obstruction à une telle identité. Ces théorèmes, dont les preuves sont assez techniques, décrivent effectivement les solutions et permettent de donner des algorithmes pour résoudre de manière complète et satisfaisante ces équations. Bien que la rédaction de cette partie suive l'enchainement classique "énoncé du théorème – preuve – exemple", il faut souvent y voir l'inversion de l'ordre chronologique "expérience – énoncé probable du théorème – preuve". Je tiens ici à insister sur l'aide indispensable de ces expériences numériques, autant pour l'ébauche d'énoncés corrects de théorèmes, que pour la suggestion des méthodes à utiliser pour les démontrer.

Tous les calculs que l'on fait dans un corps de nombres sont limités par la taille de ce corps de nombres, et plus précisément par la taille du polynôme qui le définit. Cette taille est mesurée d'abord par le degré du polynôme, mais aussi par son discriminant. Il existe actuellement d'importantes listes de polynômes de petits discriminants jusqu'au degré 9 (voir [Nik]). Le troisième problème que j'ai envisagé (chapitre IV) est donc l'énumération des polynômes ayant les discriminants minimaux pour les degrés supérieurs. À partir du degré 9, on dispose de peu de résultats sur ces discriminants. Les différentes méthodes que je propose généralisent la méthode de recherche par simple majoration des coefficients, chacune de ces méthodes construisant des polynômes de type particulier (degré, signature, primitivité ...). Ainsi, j'ai pu dresser de longues listes de polynômes de petits discriminants (voir les annexes). En degré 9, j'ai pu confirmer, à quelques exceptions près, les listes proposées par G.

Niklasch (dans [Nik]) : plus de 1200 discriminants identiques ont été trouvés, une vingtaine n'ont pas pu être retrouvés, et 6 nouveaux ont été découverts. Pour les degrés supérieurs, j'obtiens de nombreux discriminants inférieurs à ceux qui étaient connus jusqu'à présent, en particulier pour les degrés qui sont des nombres premiers. Jusqu'au degré 14, les discriminants obtenus sont de sérieux candidats pour être minimaux, au delà, je trouve encore de nombreux petits discriminants mais qui ne sont probablement pas les plus petits. Si les polynômes qui définissent des corps de nombres sont irréductibles, il est encore intéressant d'étudier le comportement des discriminants des polynômes non nécessairement irréductibles. Pour ces polynômes, j'ai pu démontrer tous les discriminants minimaux jusqu'au degré 7, pour chaque signature. Cette recherche de polynômes factorisables de petits discriminants m'a naturellement amené à considérer des familles de polynômes dont les résultants deux à deux sont petits (égaux à $\pm 1$), et j'ai constaté que ces familles ont la curieuse propriété de contenir les polynômes de discriminants minimaux pour diverses signatures. Cette partie contient de nombreux résultats numériques, mais pose aussi de nouvelles questions (théoriques), et ouvre la voie à des investigations futures.

# Mots-Clés et Notations

## Mots-Clés

Algorithme
Corps de Nombres
Courbe Elliptique
Discriminant
Équation de Legendre
Groupe de Classes
Nombre Algébrique
Norme
Polynôme
Résultant
Unité / $S$-Unité

## Notations Générales

| | |
|---|---|
| $C_n$ | groupe cyclique d'ordre $n$ |
| $\|G\|$ | cardinal du groupe fini $G$ |
| $\langle x \rangle$ | sous-groupe engendré par $x$ |
| $p$ | un nombre premier |
| $\mathfrak{p}, \mathfrak{P}$ | un idéal premier |
| $v_\mathfrak{p}(x)$ | valuation de l'élément $x$ en $\mathfrak{p}$ |
| $\mathbb{Z}_K$ | anneau des entiers du corps $K$ |
| $\mathbb{U}_K$ | groupe des unités de $K$ |
| $(a, b)$ | *pgcd* des deux entiers $a$ et $b$ |
| $(a, b)_K$ | symbole de Hilbert global dans le corps $K$ |
| $(a, b)_\mathfrak{p}$ | symbole de Hilbert local en la place $\mathfrak{p}$ |

# Chapitre I

# $S$-Unités et Groupes de Classes Relatifs

Nous décrivons dans ce chapitre deux outils mathématiques qui nous servirons dans les chapitres suivants. Les $S$-entiers se révèlent être un outil tout à fait utile car ce sont des fractions qui possèdent les mêmes propriétés que les nombres entiers ordinaires. De plus, leur dénominateur est particulièrement simple. Lorsque l'on veut contrôler à la fois le dénominateur et le numérateur des nombres rationnels, on utilise les $S$-unités.

## Qu'est-ce qu'un $S$-Entier ou une $S$-Unité ?

La notion de $S$-entier est une notion tout à fait simple que l'on utilise couramment sans le dire, et l'on parle plus volontiers de *nombres décimaux*, mais c'est finalement le même objet.

Entre l'ensemble $\mathbb{Z}$ des entiers et l'ensemble $\mathbb{Q}$ des fractions, on peut intercaler l'ensemble $\mathcal{D}$ des nombres décimaux, qui peuvent s'écrire avec un nombre fini de chiffres après la virgule. Ces nombres décimaux se comportent de la même manière que les nombres entiers habituels : on peut les additionner, les soustraire, les multiplier...On peut aussi les définir comme les fractions qui n'ont que des puissances de 10 au dénominateur, c'est-à-dire que des puissances de 2 et de 5. Les nombres décimaux sont les *$S$-entiers* lorsque l'ensemble $S$ contient exactement 2 et 5. Plus généralement, les $S$-entiers sont les nombres qui peuvent s'écrire comme des fractions, dont les dénominateurs ne contiennent que des puissances des nombres premiers qui sont dans l'ensemble $S$.

Parmi les nombres décimaux, certains ont la propriété supplémentaire que leur inverse est aussi un nombre décimal, comme 2, 5, 0.1, 2.5,...Ces nombres sont ceux qui peuvent s'écrire comme une fraction où le numérateur et le dénominateur sont tous les deux des puissances de 2 ou 5. Ces nombres sont les *$S$-unités* lorsque l'ensemble $S$ contient 2 et 5. Plus généralement les $S$-unités sont les fractions dont les numérateurs et les dénominateurs ne contiennent que des puissances des nombres premiers qui sont dans l'ensemble $S$.

Dans le cas des nombres décimaux, on constate que les $S$-unités peuvent toutes s'écrire

en fonction de $-1$, 2 et 5, sous la forme

$$u = (-1)^{\varepsilon} 2^{\alpha} 5^{\beta},$$

où $\varepsilon \in \{0, 1\}$ et $\alpha, \beta \in \mathbb{Z}$. Les unités 2 et 5 sont dans ce cas des *unités fondamentales*. De telles unités sont particulièrement utiles quand on manipule les $S$-unités en général.

# I.1 $S$-Unités

Dans cette partie nous rappelons les notions fondamentales sur les $S$-unités d'un corps de nombres $K$, et nous donnons les algorithmes qui permettent de les utiliser.

## I.1.1 Définitions, Notations et Propriétés

Soit $S$ un ensemble fini d'idéaux premiers de $K$. On dit que $x \in K$ est un *$S$-entier* si $v_{\mathfrak{p}}(x) \geqslant 0$ pour tout $\mathfrak{p} \notin S$. On dit que $x \in K^*$ est une *$S$-unité* si $v_{\mathfrak{p}}(x) = 0$ pour tout $\mathfrak{p} \notin S$. On note $\mathbb{Z}_{K,S}$ l'anneau des $S$-entiers de $K$, et $\mathbb{U}_{K,S}$ le groupe multiplicatif des $S$-unités de $K^*$. Les éléments inversibles de $\mathbb{Z}_{K,S}$ sont exactement les $S$-unités. Notons $\mathcal{I}_S(K)$ le groupe des idéaux fractionnaires de $\mathbb{Z}_{K,S}$ et $\mathcal{P}_S(K)$ le sous-groupe des idéaux principaux (on dira aussi $S$-principaux). On note $\langle S \rangle$ le sous-groupe de $\mathcal{I}(K)$ des idéaux $I$ tels que $v_{\mathfrak{p}}(I) = 0$ pour tout $\mathfrak{p} \notin S$, et on dit qu'un idéal $I$ est $S$-entier si $v_{\mathfrak{p}}(I) \geqslant 0$ pour tout $\mathfrak{p} \notin S$.

Si $L/K$ est une extension de $K$, et $S$ est encore un ensemble fini d'idéaux premiers du corps de base $K$, on dit que $x \in L$ est une $S$-unité si $v_{\mathfrak{P}}(x) = 0$ pour tous les premiers $\mathfrak{P}$ de $L$ sauf peut-être pour les premiers au-dessus de $S$. On peut définir de la même manière les $S$-entiers de $L$. On note $\mathbb{U}_{L,S}$ (resp. $\mathbb{Z}_{L,S}$) le groupe des $S$-unités (resp. l'anneau des $S$-entiers) de $L$.

Le groupe de classes ordinaire $Cl(K)$ est défini comme le quotient fini $\mathcal{I}(K)/\mathcal{P}(K)$. On peut s'inspirer de cette définition et définir le *$S$-groupe de classes* $Cl_S(K)$ comme le quotient $\mathcal{I}_S(K)/\mathcal{P}_S(K)$. La proposition suivante permet de relier les différentes notions :

**Proposition I.1.1** *Le diagramme suivant est exact :*

$$\begin{array}{ccccccccccc}
 & & & & & & (A) & & (B) & & \\
 & & & & & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{U}_K & \to & \mathbb{U}_{K,S} & \to & \langle S \rangle & \to & Cl(\langle S \rangle) & \to & 1 \\
 & & & & & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{U}_K & \to & K^* & \to & \mathcal{I}(K) & \to & Cl(K) & \to & 1 \\
 & & & & & & \downarrow \phi & & \downarrow \bar{\phi} & & \\
1 & \to & \mathbb{U}_{K,S} & \to & K^* & \to & \mathcal{I}_S(K) & \to & Cl_S(K) & \to & 1 \\
 & & & & & & \downarrow & & \downarrow & & \\
 & & & & & & 1 & & 1 & &
\end{array}$$

*Preuve :* L'exactitude des suites horizontales n'est rien d'autre que la traduction des définitions des groupes de classes. Le morphisme $\phi$ est défini sur les idéaux entiers par $I \mapsto I\mathbb{Z}_{K,S}$, puis prolongé aux idéaux fractionnaires. Le morphisme $\bar{\phi}$ est défini de la même manière sur les classes d'idéaux.

*Exactitude de* (A) : L'exactitude en $\langle S \rangle$ est claire. Pour montrer l'exactitude en $\mathcal{I}_S(K)$, il suffit de montrer que tous les idéaux entiers de $\mathcal{I}_S(K)$ peuvent être écrits sous la forme $\phi(I)$. Soit $I_S$ un idéal entier de $\mathcal{I}_S(K)$, et soit $I = I_S \cap \mathbb{Z}_K$ : c'est un idéal entier de $\mathcal{I}(K)$. Il reste à prouver que $\phi(I) = I_S$, ce qui équivaut à $(I_S \cap \mathbb{Z}_K)\mathbb{Z}_{K,S} = I_S$. On sait déjà que $(I_S \cap \mathbb{Z}_K)\mathbb{Z}_{K,S} \subset I_S\mathbb{Z}_{K,S} = I_S$. Soit maintenant $x \in I_S$. Dans $I(K)$, on a la factorisation en idéaux premiers suivante :

$$x\mathbb{Z}_K = \mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_n^{x_n} \mathfrak{q}_1^{y_1} \cdots \mathfrak{q}_m^{y_m}$$

avec $\mathfrak{p}_i \in S$, $x_i \in \mathbb{Z}$, $\mathfrak{q}_i \notin S$ et $y_i \geqslant 0$. On peut ordonner les $\mathfrak{p}_i$ de sorte que $x_1, \ldots, x_k \leqslant 0$ et $x_{k+1}, \ldots, x_n \geqslant 0$. Soit $h$ le cardinal de $Cl(K)$. L'idéal entier $(\mathfrak{p}_1^{-x_1} \ldots \mathfrak{p}_k^{-x_k})^h$ est principal, engendré par une $S$ unité entière $\alpha$. On a alors

$$\alpha x\mathbb{Z}_K = \mathfrak{p}_1^{x'_1} \cdots \mathfrak{p}_n^{x'_n} \mathfrak{q}_1^{y_1} \cdots \mathfrak{q}_m^{y_m}$$

où tous les exposants sont positifs ou nuls. On déduit alors que $\alpha x \in \mathbb{Z}_K$, et $\alpha x \in \mathbb{Z}_K \cap I_S$. Mais on a $\frac{1}{\alpha} \in \mathbb{Z}_{K,S}$, donc on a aussi $x = \alpha x \cdot \frac{1}{\alpha} \in (I_S \cap \mathbb{Z}_K)\mathbb{Z}_{K,S}$. Ceci prouve la surjectivité de $\phi$. Pour (A), il n'y a plus qu'à prouver l'exactitude en $\mathcal{I}(K)$ : on a clairement $\langle S \rangle \subset \mathrm{Ker}(\phi)$. Maintenant, soit $I \in \mathrm{Ker}(\phi)$, on a alors $I\mathbb{Z}_{K,S} = \mathbb{Z}_{K,S}$, d'où $v_{\mathfrak{p}}(I) = 0$ pour tout $\mathfrak{p} \notin S$, ce qui prouve que $I \in \langle S \rangle$.

*Exactitude de* (B) : L'exactitude en $Cl(\langle S \rangle)$ est claire, et la surjectivité de $\bar{\phi}$ provient directement de celle de $\phi$. Il n'y a plus qu'à prouver l'exactitude en $Cl(K)$. Comme $\langle S \rangle$ est le noyau de $\phi$, $Cl(\langle S \rangle)$ est dans le noyau de $\bar{\phi}$. Soit maintenant $\bar{I} \in \mathrm{Ker}(\bar{\phi})$. On a $\phi(I) = \alpha\mathbb{Z}_{K,S}$ avec $\alpha \in K^*$. Ceci implique que $\frac{1}{\alpha} I \in \mathrm{Ker}(\phi)$, et que $\frac{1}{\alpha} I \in \langle S \rangle$, et donc $\bar{I} \in Cl(\langle S \rangle)$. ■

Cette proposition montre en particulier que $\mathbb{U}_{K,S}/\mathbb{U}_K$ est un $\mathbb{Z}$-module libre de rang égal au cardinal de $S$, et que le groupe $Cl_S(K)$ est le quotient du groupe $Cl(K)$ par le sous-groupe engendré par $S$. En particulier, ce groupe est fini, et son cardinal divise celui de $Cl(K)$.

### I.1.2 Algorithmes

Nous donnons maintenant l'algorithme qui permet de calculer un système fondamental de $S$-unités (modulo les unités de $K$), et qui donne en même temps le groupe $Cl_S(K)$ (à partir du groupe $Cl(K)$). Si l'on garde quelques matrices intermédiaires de cet algorithme, il est possible de résoudre le problème du "logarithme discret" dans $\mathbb{U}_{K,S}$, et celui de "l'idéal principal" dans $Cl_S(K)$. Ceci signifie que si l'on nous donne une $S$-unité, on peut l'écrire comme le produit des $S$-unités fondamentales à certaines puissances, et que si l'on nous donne un idéal de $K$, on peut calculer sa classe dans le groupe $Cl_S(K)$, et si sa classe est la classe triviale, on peut trouver un générateur de cet idéal.

Les algorithmes décrits dans cette partie ont fait l'objet d'une implantation dans le système PARI/GP, sous les noms bnfsunit (pour le calcul des $S$-unités fondamentales et du groupe $Cl_S(K)$) et bnfissunit (pour le logarithme discret et l'idéal principal dans $Cl_S(K)$).
**Notation** : Posons $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$, et soient $d_1, \dots, d_r$ les diviseurs élémentaires du groupe $Cl(K)$, et $\mathfrak{g}_1, \dots, \mathfrak{g}_r$ les générateurs correspondants. On utilise la notation $(A|B)$ pour la concaténation de deux matrices $A$ et $B$ dans cet ordre. Si $V$ est un vecteur avec $k$ composantes, et si $U$ est une matrice $k \times l$, $W = V^U$ est le vecteur à $l$ composantes défini par $W_j = \prod_i V_i^{U_{i,j}}$. On peut remarquer que $(V^A)^B = V^{AB}$.

**Algorithme I.1.2** (*Calcul de $Cl_S(K)$ et d'un système d'unités fondamentales de $\mathbb{U}_{K,S}/\mathbb{U}_K$*).
*1– Soit*

$$M = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \end{pmatrix}$$

*et $V = (\beta_1, \dots, \beta_r)$ tels que $\mathfrak{g}_i^{d_i} = \beta_i \mathbb{Z}_K$, avec $\beta_i \in K^*$.*
*2– Soit $M' = -(e_{i,j})$ et $V' = (\alpha_1, \dots, \alpha_s)$ tels que $e_{i,j} \in \mathbb{Z}$, $\alpha_j \in K^*$ et*

$$\mathfrak{p}_j = \Big(\prod_i \mathfrak{g}_i^{e_{i,j}}\Big)\alpha_j.$$

*3– Déterminer la matrice unimodulaire $U = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ telle que $(M|M')U = (0|H)$ est sous la forme HNF (Forme Normale d'Hermite).*
*4– Calculer $(W|W') = (V|V')^U$*
*Résultats :*

$$Cl_S(K) = \prod_i (\mathbb{Z}/H_{i,i}\mathbb{Z})\mathfrak{g}_i,$$

*et $W$ est un système fondamental de générateurs de $\mathbb{U}_{K,S}/\mathbb{U}_K$.*

*Preuve :* Soit $\mathfrak{M}$ la matrice carrée $\mathfrak{M} = \left(\begin{smallmatrix} M & M' \\ 0 & Id \end{smallmatrix}\right)$. Les différentes matrices sont reliées par la relation

$$(\mathfrak{g}_1, \dots, \mathfrak{g}_r, \mathfrak{p}_1, \dots, \mathfrak{p}_s)^{\mathfrak{M}} = (\beta_1\mathbb{Z}_K, \dots, \beta_r\mathbb{Z}_K, \alpha_1\mathbb{Z}_K, \dots, \alpha_s\mathbb{Z}_K) = (V|V')\mathbb{Z}_K$$

On a $\mathfrak{M}U = \left(\begin{smallmatrix} 0 & H \\ C & D \end{smallmatrix}\right)$. On peut remarquer que cette relation prouve que la matrice $C$ est de déterminant non nul. On a alors la nouvelle relation

$$(\mathfrak{g}_1, \dots, \mathfrak{g}_r, \mathfrak{p}_1, \dots, \mathfrak{p}_s)^{\mathfrak{M}U} = (W|W')\mathbb{Z}_K$$

de sorte que, pour chaque composante, on peut écrire

$$W_j\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{C_{i,j}}.$$

On voit que toutes les composantes de $W$ sont des $S$-unités.

Soit maintenant $w$ une $S$-unité. Il faut montrer que $w$ peut s'écrire comme un produit de $W_j$. L'idéal principal $w\mathbb{Z}_K$ se factorise sous la forme $\prod \mathfrak{p}_i^{F_i}$, et le vecteur $F$ ainsi défini est à coefficients entiers. On peut écrire

$$(\mathfrak{g}_1, \dots, \mathfrak{g}_r, \mathfrak{p}_1, \dots, \mathfrak{p}_s)^{\left(\begin{smallmatrix} M' \\ Id \end{smallmatrix}\right)} = V'\mathbb{Z}_K,$$

et si l'on élève cette relation à la puissance $F$, on obtient

$$(\mathfrak{g}_1, \ldots, \mathfrak{g}_r, \mathfrak{p}_1, \ldots, \mathfrak{p}_s)^{\binom{M'F}{F}} = {V'}^F \mathbb{Z}_K,$$

mais les idéaux $w\mathbb{Z}_K = (\mathfrak{p}_1, \ldots, \mathfrak{p}_s)^F$ et ${V'}^F\mathbb{Z}_K$ sont principaux, donc $(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)^{M'F}$ est principal, et on peut donc écrire $M'F = MZ$, où $Z$ a des coefficients entiers. Ceci équivaut à dire que $MZ - M'F = 0$, ou que $\binom{-Z}{F}$ est dans le noyau de $(M|M')$. Mais le noyau de $(M|M')$ est engendré par les colonnes $\binom{A}{C}$ de la matrice $U$ (pour une explication de ce fait, on peut consulter par exemple [Coh-Dia-Oli c]), et ainsi $\binom{-Z}{F} = \binom{A}{C} Y$. On a en particulier $F = CY$. Tout ceci nous donne la relation désirée

$$w = u \cdot \prod W_j^{y_j}$$

où $u$ est une unité de $\mathbb{U}_K$.

Il faut maintenant prouver que l'algorithme donne bien le groupe $Cl_S(K)$. Il est clair que les $\mathfrak{g}_i$ engendrent le groupe de classes $Cl_S(K)$ puisqu'ils engendrent déjà $Cl(K)$ dont le premier est un quotient. Il faut montrer que les relations données par $(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)^H \mathbb{Z}_{K,S} = W'\mathbb{Z}_{K,S}$ sont les seules. Soit $(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)^E \mathbb{Z}_{K,S} = w\mathbb{Z}_{K,S}$ une relation. On peut l'écrire

$$(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)^E (\mathfrak{p}_1, \ldots, \mathfrak{p}_s)^F = w\mathbb{Z}_K.$$

Dans le groupe $Cl(K)$, on a ainsi une nouvelle relation

$$(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)^{E - M'F} = w'\mathbb{Z}_K.$$

Ceci n'est possible que si $E - M'F$ est de la forme $MZ$ puisque $M$ engendre toutes les relations de $Cl(K)$. Mais alors $E = MZ + M'F$ est dans l'image de $(M|M')$, qui est elle-même donnée par la matrice $H$, donc $E$ est de la forme $E = HZ'$. Ceci prouve que $Cl_S(K)$ ne contient pas d'autre relation que celles données par la matrice $H$. ■

**Remarques** :

– Si l'on veut les diviseurs élémentaires de $Cl_S(K)$, il suffit de prendre la SNF (Forme Normale de Smith) de $H$, et pas seulement la HNF (Forme Normale d'Hermite). Ceci signifie que l'on s'autorise la multiplication à gauche par une matrice inversible, c'est-à-dire que l'on s'autorise un changement de base sur les $\mathfrak{g}_i$.

– La matrice $C$ de l'étape 3 contient les valuations des $S$-unités fondamentales sur les $\mathfrak{p}_i$ de $S$. On a prouvé que son déterminant est non nul. Cette matrice n'est définie qu'à la multiplication à droite par une matrice unimodulaire près. Pour la même raison, la matrice $D$ n'est définie que modulo $C$. En effet, on a la relation :

$$\begin{pmatrix} M & M' \\ 0 & Id \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} U' & X \\ 0 & Id \end{pmatrix} = \begin{pmatrix} 0 & H \\ CU' & D+CX \end{pmatrix}$$

Pour cette raison, on peut choisir un système fondamental de $S$-unités qui possède des propriétés supplémentaires. Par exemple, on peut obtenir des $S$-unités qui sont des entiers algébriques : il suffit pour cela de prendre la HNF de $C$. Si l'on veut des petites $S$-unités on peut réduire la matrice $C$ avec l'Algorithme LLL, qui assure que la nouvelle matrice $C$ a des petits coefficients entiers. Il faut remarquer que la multiplication à gauche de $C$ par une matrice de permutation équivaut à changer l'ordre des $\mathfrak{p}_i$ dans $S$. Cette remarque nous permet d'appliquer l'Algorithme LLL avec permutations qui est souvent plus efficace.

**Corollaire I.1.3** *Il existe un système fondamental de $S$-unités formé d'entiers algébriques de $K$.*

Si l'on garde la matrice $C$ de l'Algorithme I.1.2, il est très simple d'exprimer une $S$-unité comme produit des $S$-unités fondamentales, autrement dit, le logarithme discret dans $\mathbb{U}_{K,S}$ est algorithmiquement simple. De même, si l'on garde les matrices $H$ et $D$, et les vecteurs $W$ et $W'$, on peut calculer la classe d'un idéal dans le groupe $Cl_S(K)$ et trouver un générateur d'un idéal $S$-principal, c'est-à-dire résoudre algorithmiquement le problème de l'idéal principal.

Les deux algorithmes sont les suivants :

**Algorithme I.1.4** (*Logarithme Discret dans $\mathbb{U}_{K,S}/\mathbb{U}_K$*).
*Donnée : $u \in \mathbb{U}_{K,S}$.*
*1– Déterminer le vecteur $F = (F_i)$ tel que $u\mathbb{Z}_K = \prod \mathfrak{p}_i^{F_i}$.*
*2– Calculer $Z = C^{-1}F$ qui a des coefficients entiers.*
*Résultat : On obtient $u = \prod W_j^{Z_j} \cdot u'$ avec $u' \in \mathbb{U}_K$.*

**Algorithme I.1.5** (*Idéal Principal dans $Cl_S(K)$*).
*Donnée : $I$ idéal de $K$.*
*1– Déterminer $F = (F_i)$ et $\alpha \in K^*$ tels que $I = \prod \mathfrak{g}_i^{F_i} \cdot \alpha$ (c'est l'algorithme de l'idéal principal dans $Cl(K)$).*
*2– Réduire $F$ modulo $H$ : $F' = F - HZ$*
*Résultat : On trouve $I$ sous la forme*

$$I = (\prod \mathfrak{g}_i^{F'_i})(\prod \mathfrak{p}_i^{(-DZ)_i})(\prod W_i^{Z_i} \cdot \alpha)$$

**Remarque** : À l'étape 2, la réduction modulo $H$ signifie que l'on réduit $F_i$ modulo $H_{i,i}$. Pour faire cela, il faut effectuer les différentes divisions euclidiennes successivement en commençant par les plus grands indices.

## I.2 Groupes de Classes Relatifs

Si $L/K$ est une extension relative de corps de nombres, il existe au moins deux morphismes canoniques entre les groupes de classes $Cl(L)$ et $Cl(K)$. En effet, si $I_L$ est un idéal de $L$, on peut prendre sa norme dans $K$. Ce morphisme passe sans difficulté au quotient et permet de définir un morphisme $\mathcal{N}_{L/K}$ de $Cl(L)$ dans $Cl(K)$. Si $I_K$ est un idéal (entier) de $K$, on peut former l'idéal (entier) $I_K\mathbb{Z}_L$ de $L$. Ceci s'étend aux idéaux fractionnaires de $K$, et définit un morphisme sur les idéaux. Comme le précédent morphisme, on peut passer au quotient, et l'on obtient ainsi un morphisme $i$ de $Cl(K)$ dans $Cl(L)$. À partir de chacun de ces deux morphismes, on peut définir une notion différente de groupe de classes relatif pour l'extension $L/K$.

### I.2.1 Définitions

L'application $I_K \mapsto I_K\mathbb{Z}_L$ induit un morphisme $i$ de $Cl(K)$ vers $Cl(L)$, et suggère la définition suivante :

**Définition I.2.1** *Un idéal $I_L$ de $L$ est* pseudo-principal *s'il existe $\alpha \in L$ et un idéal $I_K$ de $K$ tel que $I_L = \alpha I_K\mathbb{Z}_L$. Si $\mathcal{I}$ est le groupe des idéaux fractionnaires de $L$, on note $\mathcal{PP}$ le sous-groupe des idéaux pseudo-principaux. On définit alors le* groupe de classes relatif *(pour l'inclusion) $Cl_i(L/K)$ par*

$$Cl_i(L/K) = \mathcal{I}/\mathcal{PP},$$

*et l'on note $h_i(L/K) = |Cl_i(L/K)|$ son ordre.*

**Remarque** : Comme $\mathcal{PP}$ est un sous-groupe de $\mathcal{I}$ contenant le sous-groupe des idéaux principaux de $L$, $Cl_i(L/K)$ est un quotient du groupe $Cl(L)$. En particulier, $Cl_i(L/K)$ est un groupe fini, et son ordre divise celui de $Cl(L)$. On a

$$Cl_i(L/K) = Cl(L)/i(Cl(K)) = \mathrm{Coker}(i).$$

Remarquons par exemple que si $Cl(K) = 1$, alors $Cl_i(L/K) = Cl(L)$.

On définit aussi le *groupe de capitulation* $Cl_i(K)$ comme le noyau de l'application $i$ : $Cl_i(K) = \mathrm{Ker}(i)$. La suite exacte suivante traduit les définitions :

$$1 \;\to\; Cl_i(K) \;\to\; Cl(K) \;\stackrel{i}{\to}\; Cl(L) \;\to\; Cl_i(L/K) \;\to\; 1$$

L'application $I_L \mapsto \mathcal{N}_{L/K}(I_L)$ sur les idéaux induit un morphisme $\mathcal{N}_{L/K}$ de $Cl(L)$ dans $Cl(K)$, et suggère la définition suivante :

**Définition I.2.2** *Le* groupe de classes relatif *(pour la norme) $Cl_{\mathcal{N}}(L/K)$ est le sous-groupe de $Cl(L)$ défini par*

$$Cl_{\mathcal{N}}(L/K) = \mathrm{Ker}(\mathcal{N}_{L/K})$$

*et l'on note $h_{\mathcal{N}}(L/K) = |Cl_{\mathcal{N}}(L/K)|$ son ordre.*

**Remarque** : Comme $Cl_{\mathcal{N}}(L/K)$ est un sous-groupe de $Cl(L)$, ce groupe est nécessairement fini. Si $Cl(K) = 1$, alors $Cl_{\mathcal{N}}(L/K) = Cl(L) = Cl_i(L/K)$.

On définit aussi le groupe $Cl_{\mathcal{N}}(K) = \mathrm{Coker}(\mathcal{N}_{L/K}) = Cl(K)/\mathcal{N}_{L/K}(Cl(L))$, de sorte que l'on a la suite exacte suivante :

$$1 \;\to\; Cl_{\mathcal{N}}(L/K) \;\to\; Cl(L) \;\stackrel{\mathcal{N}_{L/K}}{\to}\; Cl(K) \;\to\; Cl_{\mathcal{N}}(K) \;\to\; 1$$

De même que l'on a défini au paragraphe précédent le $S$-groupe de classes pour un ensemble $S$ arbitraire d'idéaux premiers, on peut définir le $S$-groupe de classes relatif (pour l'inclusion ou pour la norme) par

$$Cl_{i,S}(L/K) = Cl_S(L)/i(Cl_S(K)) = Cl_i(L/K)/\langle S\rangle$$

$$Cl_{\mathcal{N},S}(L/K) = \mathrm{Ker}(Cl_S(L) \stackrel{\mathcal{N}_{L/K}}{\to} Cl_S(K)) = Cl_{\mathcal{N}}(L/K)/\langle S\rangle\,.$$

### I.2.2 Relations Entre les Différents Groupes de Classes Relatifs

On a déjà vu que si $Cl(K) = 1$ alors les deux notions de groupes de classes relatifs coïncident avec $Cl(L)$. Dans le cas général, ces deux notions ne sont pas équivalentes, mais on peut donner quelques relations entre les deux.

On rappelle les suites exactes qui proviennent directement des définitions :

$$\begin{array}{ccccccccccc} 1 & \to & Cl_i(K) & \to & Cl(K) & \stackrel{i}{\to} & Cl(L) & \to & Cl_i(L/K) & \to & 1 \\ 1 & \to & Cl_{\mathcal{N}}(L/K) & \to & Cl(L) & \stackrel{\mathcal{N}_{L/K}}{\to} & Cl(K) & \to & Cl_{\mathcal{N}}(K) & \to & 1 \end{array}$$

Si $G$ est un groupe abélien, et si $p$ est un nombre premier, on note $G_p$ son $p$-sous-groupe de Sylow (ou sa $p$-partie), et l'application d'élévation à la puissance $m$ dans $G$ est notée $[m]$. Les deux suites exactes précédentes restent exactes si l'on prend les $p$-Sylow de chaque groupe. Notons $d = [L : K]$ le degré de l'extension $L/K$. On a

$$\mathcal{N}_{L/K} \circ i = [d].$$

**Proposition I.2.3** *Si $p \nmid h(K)$, alors $Cl(K)_p = Cl_i(K)_p = Cl_{\mathcal{N}}(K)_p = 1$ et $Cl(L)_p \sim Cl_i(L/K)_p \sim Cl_{\mathcal{N}}(L/K)_p$. Ces trois groupes sont engendrés par les classes des mêmes idéaux.*

*Preuve :* C'est évident à partir des suites exactes car dans ce cas $Cl(K)_p = 1$. ■

**Proposition I.2.4** *Si $p \nmid d$, alors $Cl_i(K)_p = Cl_{\mathcal{N}}(K)_p = 1$ et $Cl_i(L/K)_p \sim Cl_{\mathcal{N}}(L/K)_p$. Ces deux groupes sont engendrés par les classes des mêmes idéaux.*

*Preuve :* Puisque $d$ est premier à $p$, $\mathcal{N}_{L/K} \circ i = [d]$ est un automorphisme de $Cl(K)_p$. En particulier, l'application $i$ est injective et l'application $\mathcal{N}_{L/K}$ est surjective. Ceci prouve que $Cl_i(K)_p = Cl_{\mathcal{N}}(K)_p = 1$. Soit $\psi$ et $\phi$ les applications naturelles dans les diagrammes exacts suivants :

$$\begin{array}{ccccccccc} 1 & \to & Cl(K)_p & \stackrel{i}{\to} & Cl(L)_p & \stackrel{\psi}{\to} & Cl_i(L/K)_p & \to & 1 \\ 1 & \to & Cl_{\mathcal{N}}(L/K)_p & \stackrel{\phi}{\to} & Cl(L)_p & \stackrel{\mathcal{N}_{L/K}}{\to} & Cl(K)_p & \to & 1 \end{array}$$

Il faut prouver que $\psi \circ \phi$ est un isomorphisme. Soit $\psi \circ \phi(\bar{I}_L) = 1$, alors $\phi(\bar{I}_L) = i(\bar{I}_K)$, et $\mathcal{N}_{L/K}(\phi(\bar{I}_L)) = 1 = \mathcal{N}_{L/K}(i(\bar{I}_K)) = \bar{I}_K^d$. Mais $[d]$ est un isomorphisme de $Cl(K)_p$, donc $\bar{I}_K = 1$ et $\phi(\bar{I}_L) = 1$. Puisque $\phi$ est injective, on a $\bar{I}_L = 1$, et ceci prouve que $\psi \circ \phi$ est injective.

Pour prouver que $\psi \circ \phi$ est un isomorphisme, il suffit de prouver que les deux groupes $Cl_{\mathcal{N}}(L/K)_p$ et $Cl_i(L/K)_p$ ont le même cardinal. Or, la première suite exacte donne $|Cl_i(L/K)_p| = |Cl(L)_p|/|Cl(K)_p|$ et la seconde donne $|Cl(L)_p|/|Cl(K)_p| = |Cl_{\mathcal{N}}(L/K)_p|$. Ainsi, $\psi \circ \phi$ est un isomorphisme.

Il est clair que $\psi$ et $\phi$ préservent tous les deux la classe d'un idéal, et que l'isomorphisme $\psi \circ \phi$ préserve aussi la classe d'un idéal. Ainsi, les groupes $Cl_i(L/K)_p$ et $Cl_{\mathcal{N}}(L/K)_p$ sont engendrés par les classes des mêmes idéaux, et ceci achève la preuve de la proposition. ■

On peut déduire le corollaire suivant :

**Corollaire I.2.5** *Si* $(d, h(K)) = 1$ *alors* $Cl_i(K) = Cl_{\mathcal{N}}(K) = 1$ *et* $Cl_i(L/K) = Cl_{\mathcal{N}}(L/K)$.

La proposition suivante peut être vue comme une reformulation des précédentes dans un langage différent :

**Proposition I.2.6** *Les exposants des groupes* $Cl_i(K)$ *et* $Cl_{\mathcal{N}}(K)$ *divisent tous les deux le pgcd* $(d, h(K))$.

D'après ce que nous avons vu, les deux notions de groupes de classes relatifs ne diffèrent que pour les premiers qui divisent $(d, h(K))$.
**Remarque** : Le fait que l'isomorphisme entre $Cl_i(L/K)$ et $Cl_{\mathcal{N}}(L/K)$ respecte les classes d'idéaux montre qu'il ne s'agit pas seulement d'un isomorphisme de groupes abstraits, mais réellement d'une égalité de deux groupes.

On donne maintenant un exemple pour lequel les deux groupes ne sont pas égaux :
**Exemple** : Soit $K = \mathbb{Q}(y)$ avec $y^2 + 30 = 0$. Le groupe de classes de $K$ est de type $C_2 \times C_2$ engendré par les idéaux premiers ramifiés $\mathfrak{p}_3$ et $\mathfrak{p}_5$ au-dessus de 3 et 5.

Soit $L = K(x)$ avec $x^2 - y = 0$. Dans ce cas, on a $(d, h(K)) = 2$. Le groupe de classes de $L$ est de type $C_4 \times C_2$ engendré par l'idéal premier (totalement ramifié) $\mathfrak{P}_3$ (d'ordre 4) au-dessus de 3, et $\mathfrak{P}_5$ (d'ordre 2) au-dessus de 5. Les relations $\mathcal{N}_{L/K}(\mathfrak{P}_3) = \mathfrak{p}_3$ et $\mathcal{N}_{L/K}(\mathfrak{P}_5) = \mathfrak{p}_5$ montrent que $Cl_{\mathcal{N}}(L/K) \sim C_2$ est engendré par $\mathfrak{P}_3^2$. D'autre part, les relations $\mathfrak{p}_3\mathbb{Z}_L = \mathfrak{P}_3^2$ et $\mathfrak{p}_5\mathbb{Z}_L = \mathfrak{P}_5^2$ montrent que $Cl_i(L/K) \sim C_2 \times C_2$ est engendré par $\mathfrak{P}_3$ et $\mathfrak{P}_5$.

### I.2.3 Algorithmes pour les Groupes de Classes Relatifs

On ne donnera pas ici un algorithme pour calculer directement les deux groupes de classes relatifs, car cela est assez difficile. Pour le cas d'une extension relative quadratique, H. Cohen, F. Diaz Y Diaz et M. Olivier dans [Coh-Dia-Oli b] décrivent un algorithme explicite pour cela. Cet algorithme peut être étendu au cas d'une extension relative quelconque. Il est préférable d'utiliser un tel algorithme dès que cela est possible. Tel qu'il est décrit, cet algorithme donne le groupe $Cl_i(L/K)$. À partir de celui-ci, on peut retrouver le groupe $Cl(L)$, ainsi que le groupe $Cl_{\mathcal{N}}(L/K)$. Le groupe $Cl_i(L/K)$ semble donc plus naturel que le groupe $Cl_{\mathcal{N}}(L/K)$.

Une méthode plus simple consiste à utiliser les définitions. En effet, $Cl_i(L/K)$ est un quotient de $Cl(L)$, et l'article [Coh-Dia-Oli c] explique comment le déterminer à partir des groupes $Cl(L)$ et $Cl(K)$, lorsque l'on connaît l'application $i$. Le même article [Coh-Dia-Oli c] explique comment déterminer $Cl_{\mathcal{N}}(L/K)$ comme le noyau de l'application $\mathcal{N}_{L/K}$ de $Cl(L)$ dans $Cl(K)$.

Nous verrons au chapitre III que le groupe $Cl_i(L/K)$ est plus adapté aux problèmes que nous considérons que le groupe $Cl_{\mathcal{N}}(L/K)$.

# Chapitre II

# Équations de Legendre et Courbes Elliptiques

On s'intéresse particulièrement aux équations quadratiques de Legendre de la forme

$$X^2 - aY^2 = b$$

où $a$ et $b$ sont deux éléments d'un corps de nombres $K$.

Le but de ce chapitre est de résoudre explicitement cette équation, dans le corps $K$, et de trouver une solution rationnelle, ce qui est équivalent à paramétrer l'ensemble de toutes les solutions. La résolution de cette équation est une étape essentielle dans la détermination du rang d'une courbe elliptique.

La première partie décrit le symbole de Hilbert quadratique qui permet de décider l'existence d'une solution. Ceci est intimement lié à l'extension quadratique $K(\sqrt{a})$. Plus précisément, il existe une solution si et seulement si $b$ est une norme pour l'extension $K(\sqrt{a})$. Nous n'approfondirons pas ici cette approche, que nous gardons pour le chapitre suivant, où nous nous intéressons d'une manière générale aux équations $\mathcal{N}_{L/K}(x) = b$ où $L/K$ est une extension de corps de nombres fixée.

La deuxième partie décrit un algorithme pour résoudre l'équation de Legendre dans le cas de $K = \mathbb{Q}$, et une généralisation possible de cet algorithme dans un corps de nombres. Ce que nous donnons ici est plus une méthode qui donne souvent une solution, qu'un véritable algorithme qui marcherait dans tous les cas.

Enfin dans la troisième partie, qui est la motivation des parties précédentes, nous nous intéressons aux courbes elliptiques. Cette partie est le résultat d'un travail en collaboration avec J. Cremona. En effet, celui-ci a proposé un algorithme pour déterminer le rang d'une courbe elliptique, et cet algorithme semblait s'adapter au cas des corps de nombres, contrairement aux algorithmes précédemment connus. La première étape de cet algorithme a nécessité l'utilisation des $S$-unités : nous leur avons déjà consacré le chapitre précédent. L'étape suivante exige la résolution d'équations de Legendre, et c'est pourquoi il a fallu adapter aux corps de nombres les algorithmes déjà connus pour résoudre cette équation dans le corps des rationnels. La dernière étape enfin consiste à chercher des points sur des

quartiques, or il n'existe aujourd'hui aucun algorithme pour montrer que certaines quartiques n'ont pas de point, même lorsque le corps de base est $\mathbb{Q}$. Le résultat est qu'il faut souvent se contenter d'encadrements pour le rang d'une courbe elliptique. Grâce à cet algorithme nous avons réussi à calculer le rang de certaines courbes elliptiques sur un corps cubique ou même quintique.

L'originalité de ce chapitre ne réside pas dans les preuves des propositions (qui sont dans l'ensemble assez classiques), mais dans leur utilisation. Ainsi, nous rassemblons les propositions sur lesquelles reposent les algorithmes, sans les démontrer. Nous donnons en référence les articles ou les livres qui développent ces preuves. Nos deux principales références sont [Ser] pour les équations de Legendre et les symboles de Hilbert, et [Cre a] pour les courbes elliptiques.

## II.1 Propriétés de l'Équation de Legendre

Sous sa forme homogène l'équation de Legendre peut s'écrire

$$X^2 - aY^2 = bZ^2.$$

Dans ce paragraphe, nous noterons $L(a, b)$ cette équation. Les coefficients $a$ et $b$ jouent des rôles symétriques et les équations $L(a, b)$ et $L(b, a)$ sont tout à fait équivalentes.

Nous dirons que l'équation $L(a, b)$ est dégénérée si $a$ ou $b$ est nul, ou plus généralement si $a$ ou $b$ est un carré. En effet, si $a = \alpha^2 \neq 0$, on a

$$X^2 - aY^2 = (X - \alpha Y)(X + \alpha Y)$$

et on trouve une solution si l'on résout par exemple le système

$$X - \alpha Y = 1$$

$$X + \alpha Y = b$$

dont le déterminant est $2\alpha \neq 0$. Lorsque $a$ est nul, alors $(a, b)$ a une solution si et seulement si $b$ est un carré.

On voit sans peine que l'équation $L(a, b)$ équivaut à l'équation $L(ac^2, bd^2)$ où $c$ et $d$ sont deux éléments non nuls de $K$. Cette dernière remarque signifie que pour résoudre l'équation de Legendre, on peut se ramener au cas où $a$ et $b$ sont des entiers (en les multipliant par leur dénominateur au carré), et que l'on peut les supposer sans facteur carré (on ne peut pas toujours supposer que les idéaux principaux $a\mathbb{Z}_K$ et $b\mathbb{Z}_K$ sont sans facteur carré).

Supposons maintenant que ni $a$ ni $b$ ne sont des carrés. Comme nous l'avons vu dans l'introduction, l'équation de Legendre équivaut à l'équation

$$\mathcal{N}_{L/K}(x) = b$$

où $L = K(\sqrt{a})$. Mais on sait que la norme est une fonction multiplicative, ce qui nous suggère que l'équation de Legendre est elle-même multiplicative. En effet, on dispose de la relation :

$$(X_1^2 - aY_1^2)(X_2^2 - aY_2^2) = (X_1X_2 + aY_1Y_2)^2 - a(X_1Y_2 + X_2Y_1)^2$$

Cette propriété essentielle de l'équation de Legendre nous permet d'utiliser une méthode de descente pour la résoudre, c'est-à-dire que pour résoudre $L(a,b)$, on se ramène à résoudre $L(c,d)$ où $c$ et $d$ sont plus petits que $a$ et $b$.

L'équation de Legendre (non dégénérée) définit une courbe algébrique de degré 2 et de genre 0. Ceci implique en particulier deux choses fondamentales :

– l'existence de solutions dans $K$ est équivalente à l'existence de solutions locales pour toutes les places, d'après le Principe de Hasse : cette condition locale est le symbole de Hilbert $(a,b)_K$ de l'équation $L(a,b)$.

– l'ensemble des solutions, s'il est non vide, est paramétré par une variable. En effet, ceci peut se faire de la manière suivante :

Soit $P_0(x_0,y_0)$ une solution particulière. On trace à partir de $P_0$ une droite de pente $\lambda$. Cette droite rencontre la courbe donnée par l'équation de Legendre $x^2-ay^2=b$ au point $P_0$. Comme cette équation est de degré 2, la droite doit rencontrer la courbe en un autre point $P_\lambda$ (éventuellement confondu avec $P_0$ si la droite est tangente à la courbe). On peut calculer les coordonnées de $P_\lambda$ en fonction de $P_0$ et de $\lambda$. Ceci donne la formule :

$$P_\lambda\left(\frac{2y_0a\lambda-x_0(a\lambda^2+1)}{1-a\lambda^2},\frac{2x_0\lambda-y_0(a\lambda^2+1)}{1-a\lambda^2}\right)$$

Si $P_0$ et $P_\lambda$ ont pour coordonnées homogènes $(x_0,y_0,z_0)$ et $(x,y,z)$, on a

$$\begin{aligned}x&=2y_0a\lambda-x_0(a\lambda^2+1)\\y&=2x_0\lambda-y_0(a\lambda^2+1)\\z&=z_0(1-a\lambda^2)\end{aligned}$$

Dans le cas particulier de l'équation de Pythagore $x^2+y^2=z^2$, en partant de la solution triviale $1^2+0^2=1^2$, on retrouve la solution générale bien connue :

$$\begin{aligned}x&=\lambda^2-1\\y&=2\lambda\\z&=\lambda^2+1\end{aligned}$$

Ces remarques montrent que la résolution de l'équation de Legendre se ramène à la preuve de l'existence de solutions (ou la non existence), et la construction d'une solution particulière.

## II.2 Symboles de Hilbert et Symboles de Legendre

### II.2.1 Définitions et Propriétés

D'après le Principe de Hasse, l'équation $x^2-ay^2-bz^2=0$ (avec $ab\neq 0$) a une solution dans un corps de nombres $K$ si et seulement si elle admet une solution locale en toutes les places finies et infinies. On se propose donc de donner un algorithme répondant à cette question pour chaque place de $K$, et globalement sur $K$.

On définit le symbole de Hilbert local de la manière suivante :

**Définition II.2.1 (Symbole de Hilbert)** *Soit $\mathfrak{p}$ une place (finie ou infinie) de $K$. Le symbole de Hilbert local $(a,b)_\mathfrak{p}$ est défini par*

$$(a,b)_\mathfrak{p} = \begin{cases} 1 & \text{s'il existe } (x,y,z) \neq (0,0,0) \in K_\mathfrak{p}^3 \text{ tel que } x^2 - ay^2 - bz^2 = 0 \\ -1 & \text{sinon.} \end{cases}$$

*Le symbole de Hilbert global $(a,b)_K$ est défini par*

$$(a,b)_K = \begin{cases} 1 & \text{s'il existe } (x,y,z) \neq (0,0,0) \in K^3 \text{ tel que } x^2 - ay^2 - bz^2 = 0 \\ -1 & \text{sinon.} \end{cases}$$

Le Principe de Hasse s'écrit donc de la manière suivante :

**Proposition II.2.2 (Principe de Hasse)**

$$(a,b)_K = 1 \Leftrightarrow (a,b)_\mathfrak{p} = 1 \quad \forall\, \mathfrak{p}.$$

Le symbole de Hilbert (local ou global) jouit de nombreuses propriétés : pour tout $a$,$b$,$c \neq 0$ on a :

$$\begin{aligned} (a,b) &= (b,a) \\ (a,c^2) &= 1 \\ (a,-a) &= (a,1-a) = 1 \\ (a,bc)_\mathfrak{p} &= (a,b)_\mathfrak{p}(a,c)_\mathfrak{p} \quad \text{(seulement pour le symbole local)} \end{aligned}$$

La première propriété traduit simplement la symétrie de l'équation de Legendre en $a$ et $b$. Les deux suivantes se montrent en exhibant une solution particulière. Enfin la dernière propriété vient de la multiplicativité des équations de Legendre. Elle n'est pas vraie globalement comme le montre l'exemple suivant :

**Exemple** : Dans $\mathbb{Q}$, si l'on choisit $a = 3$, $b = 5$ et $c = 7$ on a les égalités

$$(3,5)_\mathbb{Q} = (3,7)_\mathbb{Q} = (3,35)_\mathbb{Q} = -1$$

qui proviennent des symboles locaux

$$(3,5)_5 = (3,7)_7 = (3,35)_3 = -1.$$

**Définition II.2.3 (Symbole de Legendre)** *Soit $\mathfrak{p}$ une place finie de $K$ et $0 \neq x \in \mathbb{Z}_{K,\mathfrak{p}}$ tel que $v_\mathfrak{p}(x) = 0$. On définit le symbole de Legendre $\left(\frac{x}{\mathfrak{p}}\right)$ par*

$$\left(\frac{x}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{si } x = y^2 \text{ dans } \mathbb{Z}_{K,\mathfrak{p}} \\ -1 & \text{sinon.} \end{cases}$$

**Remarque** : Malgré son nom, c'est bien le symbole de Hilbert qui détermine si l'équation de Legendre possède une solution, et non pas le symbole de Legendre.

Les propositions suivantes montrent que ces deux symboles sont intimement liés. Nous ne donnons pas leur preuve que l'on peut trouver dans [Ser].

**Proposition II.2.4** *Soit $\mathfrak{p}$ une place finie de $K$, première à 2, et $ab \neq 0$. Soit $\pi$ une uniformisante de $\mathfrak{p}$, et $u$ et $v$ définis par $a = \pi^\alpha u$ et $b = \pi^\beta v$ avec $v_\mathfrak{p}(u) = v_\mathfrak{p}(v) = 0$. On a la relation*

$$(a,b)_\mathfrak{p} = (-1)^{\alpha\beta\frac{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})-1}{2}} \left(\frac{u}{\mathfrak{p}}\right)^\beta \left(\frac{v}{\mathfrak{p}}\right)^\alpha$$

**Proposition II.2.5** *Soit $\mathfrak{p}$ une place finie de $K$, première à 2, et $x$ inversible dans $\mathbb{Z}_{K,\mathfrak{p}}$. On a l'équivalence*

$$\left(\frac{x}{\mathfrak{p}}\right) = 1 \Leftrightarrow v_\mathfrak{p}\left(x^{\frac{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})-1}{2}} - 1\right) \geqslant 1.$$

**Proposition II.2.6** *Dans les mêmes conditions que la Proposition II.2.4, on a les équivalences*

$$(a,b)_\mathfrak{p} = 1 \Leftrightarrow \left(\frac{a^\beta/b^\alpha}{\mathfrak{p}}\right) = 1 \Leftrightarrow v_\mathfrak{p}\left(\left(a^\beta/b^\alpha\right)^{\frac{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})-1}{2}} - 1\right) \geqslant 1.$$

**Proposition II.2.7** *Soient $a, b \in \mathbb{R}$. Alors*

$$(a,b)_\mathbb{R} = -1 \Leftrightarrow a < 0 \text{ et } b < 0.$$

Si l'on applique la Proposition II.2.6 avec $\alpha = \beta = 0$, on trouve le corollaire suivant :

**Corollaire II.2.8** *Soit $\mathfrak{p}$ une place finie de $K$. Si $\mathfrak{p} \nmid 2ab$, alors $(a,b)_\mathfrak{p} = 1$.*

Ce corollaire nous permet donc de ne tester qu'un nombre fini de places de $K$ pour connaître le symbole $(a,b)_K$ global. Il y a donc trois sortes de places à étudier :

– les places réelles (pour les places complexes le symbole de Hilbert est toujours trivial) : elles se calculent simplement à l'aide de la Proposition II.2.7 ;

– les places finies (les idéaux premiers) qui divisent $ab$ mais qui ne divisent pas 2 : elles se calculent à l'aide de la formule de la Proposition II.2.6 ;

– les places finies (les idéaux premiers) qui divisent 2.

La seule difficulté restante pour le calcul du symbole de Hilbert global est le calcul du symbole local en les places qui divisent 2. Dans le cas particulier où le corps de nombres est le corps $\mathbb{Q}$ des rationnels, on dispose d'une formule simple (voir par exemple [Ser]). Dans le cas général, et malgré l'abondante littérature sur les "formules explicites" (voir par exemple [Fes-Vos]), je ne connais pas de formule qui permette de calculer simplement ce symbole. Malgré cet obstacle théorique, il existe un algorithme simple qui résout cela.

Grâce à la proposition suivante (que l'on trouve dans [Ser]), on sait que les différents symboles de Hilbert locaux sont liés entre eux. En particulier, si l'on veut seulement savoir si l'équation a une solution, c'est-à-dire si elle a des solutions en toutes les places de $K$, on peut choisir une place en laquelle le calcul est inutile. On omettra par exemple le calcul du symbole de Hilbert en une place où le calcul est plus difficile, comme une place au-dessus de 2, ou une place au-dessus d'un grand nombre premier.

**Proposition II.2.9 (Formule du Produit)** *Lorsque $\mathfrak{p}$ parcourt l'ensemble des places (finies et infinies) de $K$, on a*

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}} = 1.$$

## II.2.2 Places Au-Dessus de 2

Pour les places $\mathfrak{p}$ au-dessus de 2, je ne connais pas de formule simple pour calculer le symbole de Hilbert local $(a,b)_{\mathfrak{p}}$. Bien que la théorie ne résolve pas cette question de manière satisfaisante, on peut écrire un algorithme relativement simple pour calculer ce symbole. Cet algorithme est une application directe du Lemme de Hensel (II.2.10).

**Proposition II.2.10 (Lemme de Hensel)** *Soit $f(x)$ un polynôme de $\mathbb{Z}_{K,\mathfrak{p}}[x]$ et $x_0 \in \mathbb{Z}_{K,\mathfrak{p}}$ tel que $v_{\mathfrak{p}}(f(x_0)) = \lambda$, $v_{\mathfrak{p}}(f'(x_0)) = \mu$ avec $\lambda \geqslant 2\mu + 1$, alors il existe $x \in \mathbb{Z}_{K,\mathfrak{p}}$ tel que $x \equiv x_0 \mod \mathfrak{p}^{\lambda-\mu}$ et $f(x) = 0$.*

*Ceci est vrai en particulier lorsque $v_{\mathfrak{p}}(f(x_0)) > 0$ et $v_{\mathfrak{p}}(f'(x_0)) = 0$.*

*Preuve :* voir [Lang][p. 42]. ■

L'algorithme que nous décrivons montre l'existence (ou la non existence) de solutions dans $\mathbb{Z}_{K,\mathfrak{p}}$ pour une équation de la forme $y^2 = g(x)$ où $g$ est un polynôme de degré quelconque. Nous aurons besoin de cet algorithme pour déterminer si une quartique est localement soluble. Si l'on s'intéresse aux solutions dans $K_{\mathfrak{p}}$, et que $g$ est de degré pair, il suffit de regarder simultanément les deux équations $y^2 = g(x)$ et $y^2 = \hat{g}(x)$ dans $\mathbb{Z}_{K,\mathfrak{p}}$ où $\hat{g}$ est le polynôme réciproque de $g$. Pour se convaincre de cela, il suffit de se rappeler que dans $K_{\mathfrak{p}}^*$, si un élément n'est pas entier, alors son inverse est entier.

L'algorithme repose sur le lemme suivant dont une démonstration a été proposée par S. Siksek (voir [Sik] ou [Serf]) : c'est une application du Lemme de Hensel II.2.10, qui généralise au cas des corps de nombres un lemme de [Bir-SwD].

**Lemme II.2.11** *Soient $e = v_{\mathfrak{p}}(2)$, $g(x) \in \mathbb{Z}_{K,\mathfrak{p}}[x]$ et $x_0 \in \mathbb{Z}_{K,\mathfrak{p}}$, et soit $\pi$ une uniformisante de $\mathfrak{p}$ dans $\mathbb{Z}_{K,\mathfrak{p}}$. On note $\lambda = v_{\mathfrak{p}}(g(x_0))$ et $\mu = v_{\mathfrak{p}}(g'(x_0))$. Soit $\nu \geqslant 0$. On peut résoudre $y^2 = g(x)$ avec $v_{\mathfrak{p}}(x - x_0) \geqslant \nu$ si l'on est dans l'un des cas suivants :*

*1- $g(x_0)$ est un carré dans $\mathbb{Z}_{K,\mathfrak{p}}$ ;*

*2- $\lambda - \mu \geqslant \nu > \mu$ ;*

*3- $\nu > \mu$ et $\lambda = \mu + \nu - i$ est pair avec $1 \leqslant i \leqslant 2e$, et $g(x_0)\pi^{-\lambda}$ est un carré modulo $\mathfrak{p}^i$ ;*

*La précision n'est pas suffisante pour conclure si l'on est dans l'un des cas suivants :*

*4- $\mu \geqslant \nu$ et $\lambda \geqslant 2\nu$ ;*

*5- $\mu \geqslant \nu$ et $\lambda = 2\nu - 2i$ avec $1 \leqslant i \leqslant e$, et $g(x_0)\pi^{-\lambda}$ est un carré modulo $\mathfrak{p}^{2i}$ ;*

*Il n'existe pas de telle solution si l'on est dans les autres cas.*

**Remarque** : Si l'on veut seulement savoir s'il existe une solution entière, sans savoir comment elle se réduit modulo $\mathfrak{p}^{\nu}$, on peut remplacer la condition 2 par la condition plus faible

$$\lambda > 2\mu.$$

De ce lemme, on déduit l'algorithme récursif suivant pour déterminer la solubilité de l'équation $y^2 = g(x)$ dans $\mathbb{Z}_{K,\mathfrak{p}}$.

Cet algorithme suppose que l'on dispose d'un système $\mathcal{R}$ de représentants de $\mathbb{Z}_{K,\mathfrak{p}}/\mathfrak{p}$, et d'une uniformisante $\pi$ de l'idéal $\mathfrak{p}$.

**Algorithme II.2.12** (*Étant donnés $x_0 \in \mathbb{Z}_{K,\mathfrak{p}}$ et $\nu \geqslant 0$, cet algorithme prouve l'existence d'une solution de l'équation $y^2 = g(x)$ dans $\mathbb{Z}_{K,\mathfrak{p}}$ telle que $v_{\mathfrak{p}}(x - x_0) \geqslant \nu$).*

*1– Si le Lemme II.2.11 permet de construire une solution, alors arrêter l'algorithme et renvoyer "Soluble". Si le Lemme II.2.11 montre qu'il n'existe pas de solution, alors arrêter l'algorithme et renvoyer "Non Soluble".*

*2– Pour chaque $r \in \mathcal{R}$, appliquer l'Algorithme II.2.12 avec $x_0' = x_0 + r\pi^\nu$ et $\nu' = \nu + 1$.*

*3– Si l'une au moins des réponses de l'étape 2 est positive, alors renvoyer "Soluble", sinon renvoyer "Non Soluble".*

Pour calculer le symbole de Hilbert local $(a, b)_{\mathfrak{p}}$, il suffit d'appliquer l'Algorithme II.2.12 avec le polynôme $g(x) = ax^2 + b$ puis avec $bx^2 + a$.

Le principe de cet algorithme est de construire une solution jusqu'à une précision telle que le Lemme de Hensel permet de relever cette solution dans $\mathbb{Z}_{K,\mathfrak{p}}$. Cet algorithme se termine toujours, car lorsque $\nu$ est grand, les conditions 4 et 5 du Lemme II.2.11 ne peuvent plus être vérifiées à cause de l'inégalité $\min(\lambda, \mu) \leqslant v_{\mathfrak{p}}(\operatorname{disc} g)$.

Pour pouvoir appliquer le Lemme II.2.11, il faut être capable de reconnaître les carrés modulo $\mathfrak{p}^\alpha$ (étapes 3 et 5). Pour cela, nous proposons deux méthodes. La plus simple consiste à calculer tous les carrés de $\mathbb{Z}_{K,\mathfrak{p}}/\mathfrak{p}^\alpha$, et à les stocker dans un long vecteur. Cette méthode est utilisable lorsque $\mathfrak{p}^\alpha$ n'est pas trop grand. La deuxième méthode consiste à déterminer le groupe $(\mathbb{Z}_{K,\mathfrak{p}}/\mathfrak{p}^\alpha)^*$, c'est-à-dire le décomposer sous sa forme canonique

$$(\mathbb{Z}_{K,\mathfrak{p}}/\mathfrak{p}^\alpha)^* = \prod_i (\mathbb{Z}/d_i\mathbb{Z})\,\omega_i$$

où les $d_i$ sont les diviseurs élémentaires, et les $\omega_i$ sont des générateurs de chaque facteur. Dans ce groupe tout élément se factorise de manière unique sous la forme

$$x = \prod_i \omega_i^{x_i}.$$

Avec ces notations $x$ est un carré dans $(\mathbb{Z}_{K,\mathfrak{p}}/\mathfrak{p}^\alpha)^*$ si et seulement si les $x_i$ correspondant aux $d_i$ pairs sont eux-mêmes pairs.

Enfin, pour appliquer le Lemme II.2.11, il faut savoir reconnaître les carrés de $\mathbb{Z}_{K,\mathfrak{p}}$ (étape 1). Ceci se fait grâce à la proposition suivante, qui est encore une conséquence du Lemme de Hensel II.2.10 :

**Proposition II.2.13 (Carrés $\mathfrak{p}$-adiques)** *Soit $e = 1 + 2v_{\mathfrak{p}}(2)$. Soit $a$ un élément non nul de $K_{\mathfrak{p}}$, que l'on représente sous la forme $a = \pi^\alpha q$ avec $v_{\mathfrak{p}}(q) = 0$. On a l'équivalence*

$$a = y^2, \quad y \in K_{\mathfrak{p}} \Leftrightarrow q = z^2 \mod \mathfrak{p}^e \text{ et } \alpha \in 2\mathbb{N}.$$

**Remarque** : Tout ce que nous avons dit dans ce paragraphe est vrai si l'on prend un idéal premier $\mathfrak{p}$ qui ne divise pas 2. Toutefois, si $\mathfrak{p}$ ne divise pas 2, nous avons vu qu'il

n'est pas nécessaire d'utiliser l'Algorithme II.2.12 pour calculer le symbole de Hilbert, mais simplement la Proposition II.2.6.

Nous utiliserons plus loin les résultats de ce paragraphe pour étudier la solubilité locale des quartiques de la forme $y^2 = g(x)$ où $g(x)$ est un polynôme de degré 4.

# II.3 Résolution de l'Équation de Legendre

## II.3.1 Résolution dans le Corps $\mathbb{Q}$ des Rationnels

Maintenant que nous avons résolu le problème de l'existence de solutions à l'équation de Legendre, nous proposons de résoudre explicitement cette équation. Cette résolution a été l'objet de nombreuses discussions avec D. Rusin et J. Cremona. On pourra consulter [Cre d] pour plus de détails, ou pour une approche légèrement différente.

Nous donnons ici deux versions de l'algorithme de résolution de l'équation $x^2 - ay^2 = bz^2$. La première version est simple, mais n'est pas très efficace (ni en temps de calcul, ni pour la taille des solutions). La deuxième version utilise une étape de réduction supplémentaire qui permet de diminuer considérablement le nombre d'étapes, et donc de factorisations de grands nombres. Un judicieux choix de signes dans l'algorithme permet de réduire d'une manière surprenante la taille des solutions.

La première version de l'algorithme est probablement connue depuis Lagrange. La deuxième version et ses raffinements sont moins connus, bien qu'ils aient été découverts depuis plusieurs années. On trouve par exemple des idées analogues dans [Pol-Sch].

On suppose dans cet algorithme qu'il existe des solutions non triviales à l'équation $x^2 - ay^2 = bz^2$. Cette existence peut être vérifiée par les algorithmes du paragraphe précédent. L'existence d'une solution garantit la possibilité de résoudre chaque étape dans ce calcul.

Cet algorithme est présenté sous sa version récursive.

**Algorithme II.3.1 (Leg(a,b))** (*Cet algorithme trouve une solution non triviale de l'équation* $x^2 - ay^2 = bz^2$) .

*1–* (*Élimination des Facteurs Carrés*) .

*Factoriser les nombres* $a$ *et* $b$ *sous la forme* $a = a' \cdot \alpha^2$ *et* $b = b' \cdot \beta^2$ *avec* $a'$ *et* $b'$ *sans facteur carré. Si* $\alpha$ *ou* $\beta$ *n'est pas trivial, calculer une solution* $(x, y, z)$ *de* $Leg(a', b')$, *et renvoyer* $(x, y/\alpha, z/\beta)$.

*2–* (*Échange*) .

*Si* $|b| < |a|$, *calculer une solution* $(x, y, z)$ *de* $Leg(b, a)$, *et renvoyer* $(x, z, y)$.

*3–* (*Cas Triviaux*) .

*Si* $b = 1$, *renvoyer* $(1, 0, 1)$.

*Si* $b = -1$ (*dans ce cas on a* $a = 1$) , *renvoyer* $(0, 1, 1)$.

*Si* $a = 0$, *alors* $b$ *est nécessairement un carré. Renvoyer* $(\sqrt{b}, 0, 1)$.

*Si* $a = 1$, *alors renvoyer* $(1, 1, 0)$.

*4–* (*Solution modulo* $b$) .

*Factoriser $b$ en produit de nombres premiers $p_i$ (ici $b$ est sans facteur carré), et calculer $x_i$ tel que $x_i^2 \equiv a \mod p_i$ (par exemple par l'Algorithme de Shanks). À l'aide de l'Algorithme des Restes Chinois, trouver $X \in \mathbb{Z}$ tel que $X^2 \equiv a \mod b$.*

*5– (Réduction).*

*Réduire $X$ modulo $b$ tel que $-\frac{|b|}{2} \leqslant X \leqslant \frac{|b|}{2}$, et poser $k = (X^2 - a)/b$.*

*6– (Récursivité).*

*Calculer une solution $(x, y, z)$ de $Leg(a, k)$ et renvoyer $(Xx - ay, Xy - x, kz)$.*

*Preuve :* Pour voir que l'algorithme se termine, il suffit de voir que la quantité $|ab|$ diminue à chaque passage. Ceci est clair pour l'étape 1. Pour l'étape 5, le choix de $X$ dans l'intervalle $-\frac{|b|}{2} \leqslant X \leqslant \frac{|b|}{2}$, entraîne que $|bk| = |X^2 - a| < \frac{|b|^2}{4} + |b|$ et donc que $k \leqslant \frac{|b|}{4} + 1$. Les cas terminaux sont réglés par l'étape 3.

Pour montrer que cet algorithme donne une solution correcte, on vérifie qu'à l'étape 6, les équations $x^2 - ay^2 = kz^2$ et $X^2 - a = bk$ entraînent bien que $(Xx - ay)^2 - a(Xy - x)^2 = b(kz)^2$. Ceci est dû à la multiplicativité des équations de Legendre (c'est-à-dire à la multiplicativité de la norme pour le corps de nombres $\mathbb{Q}(\sqrt{a})$). ■

**Exemple** : Essayons de résoudre l'équation

$$x^2 - 123452853y^2 = 375556542871687561z^2.$$

Cette équation nous a été proposée par D. Rusin au cours de fructueux échanges au sujet de cet algorithme. Les valeurs successives du couple $(a, b)$ pour cet algorithme sont :

$$\begin{aligned}
&(123452853, 375556542871687561)\\
&(123452853, 5400769724919127)\\
&(123452853, 620370967013929)\\
&(123452853, 3142852309164)\\
&(123452853, 785713077291)\\
&(123452853, 30919053556)\\
&(123452853, 7729763389)\\
&(123452853, 208158484)\\
&(52039621, 123452853)\\
&(18231075, 52039621)\\
&(5586406, 18231075)\\
&(9003, 5586406)\\
&(9003, 32401)\\
&(553, 9003)\\
&(176, 553)\\
&(1, 176)
\end{aligned}$$

et après avoir simplifié par un grand contenu, la solution trouvée est

$$x = 29924927279480074513107553205157561176029471 37$$
$$y = 13475573249145124472197351692569670848867 5$$
$$z = 42279295754022424752939785259874811 02$$

**Remarque** : Dans cet algorithme, on calcule des racines carrées modulo des nombres premiers. Comme il existe deux telles racines modulo $p$ (de signes opposés), il y a $2^k$ racines carrées différentes modulo $b$ si $b$ a $k$ facteurs premiers. Chaque choix est aussi valide, et cela mène à des solutions différentes à la fin de l'algorithme. Pour cette raison, on trouve rarement deux fois le même résultat si l'on utilise cet algorithme deux fois consécutives.

La principale difficulté de cet algorithme est le grand nombre de factorisations que l'on doit effectuer (à l'étape 4), qui est de l'ordre de $\log b / \log 4$. Comme on sait que résoudre une telle équation de Legendre est équivalent à factoriser le nombre $b$, il ne faut pas s'attendre à trouver un algorithme rapide (i.e. polynomial) qui puisse résoudre ce problème sans factorisation. Toutefois, on peut réduire considérablement le nombre total de factorisations à effectuer, en réduisant le nombre de passages dans l'algorithme. L'algorithme ne nécessitera plus alors que la factorisation de quelques nombres, dont inévitablement $a$ et $b$.

La réduction se fait en remarquant qu'après un passage dans l'algorithme, l'équation à résoudre à l'étape suivante est $x^2 - ay^2 \equiv 0 \mod k$. Or, l'étape précédente a précisément produit une solution telle que $X^2 - aY^2 = bk$ (avec $Y = 1$). On peut donc se servir de cette solution pour construire la solution suivante. On peut opérer cette réduction tant que le nouveau $k$ est inférieur au précédent. On peut effectuer cette réduction (sans le moindre coût) jusqu'à $k \leqslant 2\sqrt{|b|}$. Le gain est considérable par rapport au $\frac{|b|}{4}$ de l'algorithme précédent, et il n'y a plus que $\log\log b / \log 2$ passages dans l'algorithme. Les seules factorisations à effectuer sont celles de $a$ et $b$ et de nombres inférieurs à $\min(\sqrt{|a|}, \sqrt{|b|})$. Récemment, D. Rusin a décrit une version de cet algorithme qui utilise la factorisation des nombres $a$ et $b$, mais d'aucun autre nombre (voir [Cre d]).

Nous donnons une forme non récursive de l'algorithme, où nous utilisons la notation suivante : si $M$ est une matrice $3 \times 3$, $M(i)$ est sa $i$-ième ligne.

**Algorithme II.3.2** (*Cet algorithme trouve une solution non triviale de l'équation* $x^2 - ay^2 = bz^2$) .

*0–* (*Initialisation*)

$M = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ *et* $Y = 1$.

*1–* (*Élimination des Facteurs Carrés*)

*Si* $a$ *et* $b$ *sont divisibles par* $\alpha^2$ *et* $\beta^2$, *alors diviser* $a$ *par* $\alpha^2$, $b$ *par* $\beta^2$, $M(2)$ *par* $\alpha$ *et* $M(3)$ *par* $\beta$.

*2–* (*Échange*)

*Si* $|b| < |a|$, *alors échanger* $a$ *et* $b$, *puis échanger* $M(2)$ *et* $M(3)$.

*3–* (*Cas Triviaux*)

*Si* $b = 1$, *poser* $S = \left(\begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix}\right)$, *et aller à l'étape 7.*

*Si* $b = -1$ *(dans ce cas on a* $a = 1$*), poser* $S = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$*, et aller à l'étape 7.*

*Si* $a = 1$*, alors poser* $S = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$*, et aller à l'étape 7.*

*4– (Solution modulo b).*

*Factoriser b en produit de nombres premiers* $p_i$ *(ici b est sans facteur carré), et calculer* $x_i$ *tel que* $x_i^2 \equiv a \mod p_i$ *(par exemple par l'Algorithme de Shanks). À l'aide de l'Algorithme des Restes Chinois, trouver* $X \in \mathbb{Z}$ *tel que* $X^2 \equiv a \mod b$.

*5– (Réduction).*

*Réduire X modulo b tel que* $-\frac{|b|}{2} \leqslant X \leqslant \frac{|b|}{2}$*. Poser* $k = (X^2 - a)/b$.

*6– (Boucle).*

$Y = -Y$ *;* $M = M \cdot \begin{pmatrix} X & aY & 0 \\ Y & X & 0 \\ 0 & 0 & k \end{pmatrix}$*. Réduire X modulo k tel que* $-\frac{|k|}{2} \leqslant X \leqslant \frac{|k|}{2}$*. Poser* $b = k$ *puis* $k = (X^2 - a)/b$*. Si* $k \neq 0$ *et* $|k| < |b|$*, recommencer l'étape 6, sinon aller à l'étape 1.*

*7– (Fin).*

*Calculer* $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = M \cdot S$ *et renvoyer* $(x, y, z)$.

**Exemple** : Partons toujours de l'équation précédente. Les valeurs successives du couple $(a, b)$ sont :

$$(123452853, 375556542871687561)$$
$$(4, 123452853)$$

et après avoir simplifié par un grand contenu (d'une centaine de chiffres), la solution trouvée est

$$x = 1256429287$$
$$y = 24875$$
$$z = 2$$

Le nombre d'étapes de l'algorithme a considérablement diminué, et les solutions sont de taille satisfaisante, une fois qu'on les a simplifiées par un grand contenu. Si l'on omet l'instruction $Y = -Y$ au début de l'étape 6, l'algorithme est encore valide, et les étapes du calcul sont inchangées. Toutefois les solutions trouvées sont de taille désastreuse, car elles sont sans contenu :

$x =$
360010515657942682762404806233687713954865411498575732630848357345655792305828249

$y =$
712777294435460827070458262226448182858472058520241756667130820236610525095 5

$z =$573068368810995988359128945355518783035208945533383041688857142296479154

La raison d'un tel phénomène, est que dans l'algorithme que nous avons décrit, la multiplication de la matrice $M$ par la matrice $\begin{pmatrix} X & aY & 0 \\ Y & X & 0 \\ 0 & 0 & k \end{pmatrix}$ correspond en réalité à la multipication d'une solution de $x^2 - ay^2 = bk$ par une solution de l'équation $x^2 - ay^2 = k$. Faire ici une multiplication ou une division est sans importance car on travaille modulo les carrés. Toutefois, on peut s'attendre à obtenir des simplifications de fractions lorsque l'on effectue

des divisions, alors qu'en faisant des multiplications, les termes vont toujours s'accumuler. Lorsque l'on ajoute un signe "$-$" dans l'expression, cela revient à faire une division et non pas une multiplication. Il est alors concevable que deux solutions consécutives se compensent (ou se simplifient si l'on pense en termes de fractions non irréductibles). Ceci se traduit par un énorme contenu dans l'expression finale de la solution.

Nous avons tenu à obtenir des solutions de petite taille pour deux raisons. La première est que ces solutions servent à paramétrer les quartiques qu'il faut ensuite résoudre dans l'Algorithme II.4.9. Ainsi, plus les solutions de l'équation de Legendre sont petites, plus les solutions des quartiques seront faciles à trouver. La deuxième raison est que de telles solutions existent, comme le prouve le Théorème de Holzer :

**Théorème (Holzer)** *Soient $a$, $b$ et $c$ trois entiers (de $\mathbb{Z}$) premiers entre eux et sans facteur carré. Si l'équation $ax^2 + by^2 = cz^2$ admet une solution non triviale dans $\mathbb{Z}^3$, alors on peut trouver une solution $(x_0, y_0, z_0) \in \mathbb{Z}^3$ non triviale telle que*

$$|x_0| \leqslant \sqrt{bc}, \quad |y_0| \leqslant \sqrt{ac}, \quad |z_0| \leqslant \sqrt{ab}.$$

*Preuve :* Voir [Hol] ou [Coc-Mit]. ■

On peut enfin remarquer que si l'on dispose d'une solution qui ne vérifie pas ces inégalités, il existe un algorithme (simple) dû à Mordell pour réduire cette solution (voir [Mor] ou [Cre d]).

### II.3.2 Résolution dans les Corps de Nombres

Dans cette partie, nous essayons de résoudre l'équation de Legendre $x^2 - ay^2 = bz^2$ dans un corps de nombres $K$. Comme nous avons déjà décrit le calcul du symbole de Hilbert global $(a, b)_K$, nous supposerons désormais que cette équation possède des solutions non triviales.

La généralisation de l'Algorithme II.3.2 aux corps de nombres se heurte à trois principales difficultés :

1– Les cas terminaux (essentiellement les cas où $a$ et $b$ sont des unités) ne sont pas triviaux si $K$ possède beaucoup d'unités ;

2– Si le corps $K$ n'est pas euclidien, on ne peut pas nécessairement se ramener à une équation avec des coefficients plus petits, c'est-à-dire que la méthode de descente n'est plus possible ;

3– Si le corps $K$ n'est pas principal, on peut être amené à manipuler des carrés (au moins localement) là où l'on avait supposé que les nombres étaient sans facteur carré, dans le cas de $\mathbb{Q}$ .

Le calcul des racines carrées modulo les idéaux premiers $\mathfrak{p}$ de $K$ est connu, de même que l'algorithme des Restes Chinois dans ce cadre. La manipulation des solutions intermédiaires se fait de manière identique à l'Algorithme II.3.2.

Nous allons maintenant indiquer comment lever ces difficultés. Les méthodes proposées ne sont pas toujours efficaces quant au nombre d'étapes de calcul, ni quant à la taille des solutions. Elles ont en revanche l'intérêt de résoudre l'équation de Legendre dans de

nombreux cas. Si toutefois aucune de ces méthodes ne donne de résultat, on peut utiliser les méthodes du chapitre III.

## 1 Cas Terminaux

Si nous devons résoudre l'équation $L(a,b)$ : $x^2 - ay^2 = bz^2$ où $a$ et $b$ sont des unités, nous pouvons d'abord réduire $a$ et $b$ modulo les carrés des unités. Ainsi, il n'y a qu'un nombre fini de telles équations à résoudre.

Deux cas triviaux peuvent être immédiatement testés :

– Si $a = 1$ ou $b = 1$, alors une solution est donnée par $(x,y,z) = (1,1,0)$ ou $(1,0,1)$ ;

– Si $a = -b$, alors une solution est donnée par $(0,1,1)$.

À cette liste, on peut ajouter les solutions données par les éventuelles unités exceptionnelles. Les équations qui restent peuvent se regrouper par équivalence, par exemple en utilisant les équivalences $L(b,a) \sim L(a,b) \sim L(-ab,b)$. Enfin, si le corps $K$ possède des plongements réels, les tests locaux aux places réelles montrent que plusieurs d'entre elles ne sont pas solubles (c'est précisément le cas où $K$ possède beaucoup d'unités, et où $a$ et $b$ peuvent prendre de nombreuses valeurs).

**Exemple** : Soit $K = \mathbb{Q}(\sqrt{D})$ un corps quadratique réel. Notons $u$ une unité fondamentale de $K$, de sorte que $a$ et $b$ peuvent prendre leurs valeurs dans $\{1,-1,u,-u\}$. L'équation $L(-1,-1)$ (i.e. $x^2 + y^2 = -z^2$) n'a pas de solution. Si $a$ ou $b$ vaut 1, ou si $a = -b$ alors l'équation est triviale. En permutant $x$,$y$ et $z$, on voit que l'équation $L(a,a)$ est équivalente à $L(a,-1)$. Ainsi, à équivalence près, il n'y a qu'à considérer les équations $L(-1,u)$ et $L(-1,-u)$. Lorsque les conjugués de $u$ sont de signes opposés (c'est-à-dire lorsque $u$ est de norme $-1$), alors les deux équations ne sont pas solubles (en une place réelle). Lorsque les conjugués de $u$ sont de même signe (c'est-à-dire lorsque $u$ est de norme $+1$), alors une et une seule de ces équations est soluble aux places réelles : dans ce cas, il ne reste plus qu'à regarder les places au-dessus de 2, en particulier, s'il n'y a qu'un seul idéal au-dessus de 2, la Proposition II.2.9 implique qu'une et une seule de ces deux équations est soluble.

Pour trouver les solutions des quelques équations qui restent à résoudre, on peut essayer plusieurs méthodes. On peut d'abord chercher des petites solutions en $(x,y,z)$. Cette méthode simple permet de résoudre un certain nombre de cas. Bien que la version du Théorème de Holzer que nous avons donnée ne soit valable que dans $\mathbb{Z}$, il en existe une version démontrée par C.L. Siegel dans [Sie], tout à fait analogue et valable dans les corps de nombres. Ceci suggère que si les coefficients $a$ et $b$ sont petits, alors il existe une solution $(x,y,z)$ formée de petits nombres. Comme dans les cas terminaux les coefficients $a$ et $b$ sont petits, il est raisonnable de chercher des petites solutions $(x,y,z)$, par une recherche naïve en faisant varier les $y$ et $z$ dans des petits intervalles.

Une autre méthode consiste à choisir $x$ et $y$ au hasard, à calculer $b' = x^2 - ay^2$, puis à multiplier l'équation $L(a,b)$ par $L(a,b')$ en utilisant la formule du produit des équations de Legendre. Cette nouvelle équation $L(a,c)$ est soluble si et seulement si $L(a,b)$ est soluble. En appliquant la méthode de descente, on aboutit de nouveau à un cas terminal. En répétant plusieurs fois cette opération, on peut s'attendre à arriver à un cas facile.

### 2 Descente

Si le corps n'est pas euclidien, on ne peut pas prouver que l'Algorithme II.3.2 se termine. De plus, même lorsqu'il est euclidien, on ne dispose pas en général d'algorithme simple pour la division euclidienne de deux entiers, à moins de travailler dans un corps particulier.

Pour contourner ce problème, on s'appuiera sur la remarque suivante : à l'étape 4 de l'Algorithme II.3.2, on construit deux racines carrées (de signes opposés) pour chaque premier $\mathfrak{p}$, ce qui construit $2^k$ solutions modulo $b$ si $b$ a $k$ facteurs premiers. Parmi ces nombreuses solutions, nous avons presque toujours constaté que l'une au moins donnait lieu à un $k$ dont la norme est inférieure à celle de $b$. Lorsque ce n'était pas le cas, l'étape 5 de réduction donnait alors une valeur de $k$ convenable. Ceci signifie que la norme de $b$ ne diminue pas nécessairement à chaque étape, mais expérimentalement elle diminue après deux étapes.

### 3 Corps non Principaux

Dans l'Algorithme II.3.2, nous réduisons à chaque étape les nombres $a$ et $b$ pour éliminer leurs facteurs carrés. Cette réduction nous permet de ne travailler que modulo des nombres premiers à l'étape 4. Lorsque le corps $K$ n'est pas principal, on ne peut pas toujours assurer que les idéaux principaux $a\mathbb{Z}_K$ et $b\mathbb{Z}_K$ sont sans facteur carré. Cela nous oblige à travailler non pas modulo $\mathfrak{p}$ mais modulo $\mathfrak{p}^e$. Les calculs ne sont guère différents.

## II.4 Applications aux Courbes Elliptiques

L'application que nous donnons ici est le calcul du rang d'une courbe elliptique, et la recherche d'une famille de points de rang maximal sur cette courbe. On peut toujours trouver une équation de la courbe sous la forme de Weierstrass

$$y^2 = x^3 + ax^2 + bx + c \qquad (E).$$

Il est habituel de distinguer deux (éventuellement trois) familles de courbes elliptiques, pour lesquelles la difficulté du calcul du rang n'est pas la même. Nous distinguons les courbes qui ont de la 2-torsion (éventuellement de la 2-torsion complète), et celles qui n'en ont pas. La 2-torsion se mesure en fait par le nombre de racines du polynôme $P(x) = x^3 + ax^2 + bx + c$ dans le corps $K$. Si le polynôme $P$ a une racine multiple, l'équation $(E)$ ne définit plus une courbe elliptique, et cette équation ne nous intéresse plus. Nous pouvons donc distinguer trois cas :

– $E$ est sans 2-torsion si $P$ n'a pas de racine dans $K$ ;

– $E$ a de la 2-torsion si $P$ a au moins une racine dans $K$, et une simple translation de $x$ permet d'écrire la courbe sous la forme

$$y^2 = x^3 + ax^2 + bx \qquad (E) ;$$

– $E$ a de la 2-torsion complète si $P$ a trois racines distinctes dans $K$. En notant $e_1$, $e_2$ et $e_3$ ces racines, on a

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad (E).$$

Lorsque la courbe $E$ a de la 2-torsion, le calcul du rang est plus simple que si elle n'en a pas. Si $E$ n'a pas de 2-torsion, on peut toujours se placer dans une extension cubique $K(\theta)$ du corps de base $K$ qui contient une racine $\theta$ du polynôme $P$, et dans ce nouveau corps la courbe elliptique a de la 2-torsion. Une fois dans cette extension, on peut utiliser les algorithmes de détermination d'un système de points de rang maximal, puis calculer leur trace (au sens de l'addition sur la courbe elliptique) pour redescendre dans le corps de base. Il n'est pas clair que cette méthode par extension du corps de base soit préférable à la méthode générale pour les courbes sans 2-torsion en restant dans le corps de base. Même la méthode qui reste dans le corps de base utilise un certain nombre de calculs dans l'extension $K(\theta)$, et on n'évitera pas en particulier la construction du groupe de classes et des unités de cette extension.

Dans son livre [Cre a], J. Cremona donne une description détaillée des algorithmes qui calculent le rang d'une courbe elliptique, en restant dans le corps de base, dans le cas particulier où ce corps est $\mathbb{Q}$. L'algorithme de descente par 2-isogénie décrit dans ce livre se généralise sans trop de difficulté au cas des corps de nombres. En revanche, celui de la 2-descente générale (pour les courbes sans 2-torsion) est beaucoup plus difficile. En effet, une des étapes consiste à choisir des invariants $I$ et $J$, ce qui se fait par des considérations locales déjà délicates. Une fois que ces invariants sont choisis, il faut trouver les quartiques ayant ces invariants, et cela se fait par exemple par la majoration des valeurs absolues des coefficients. Dans le cas des corps quadratiques réels, P. Serf (dans [Serf] et [Cre-Ser]) trouve des inégalités suffisantes pour en déduire un algorithme. Dans le cas d'un corps de nombres quelconque, ces majorations ne sont plus valables, ou alors elles ne permettent pas de choisir un nombre fini de telles quartiques. En utilisant plus extensivement la théorie des invariants, J. Cremona a donné dans [Cre c] une description plus algébrique de l'algorithme, qui se généralise beaucoup plus aisément au cas d'un corps de nombres.

### II.4.1 Le Groupe $K(S, 2)$

Dans les algorithmes que nous décrivons par la suite, nous utilisons à plusieurs reprises le groupe $K(S, 2)$, dont nous donnons ici la définition et quelques propriétés. Nous nous appuyons sur les $S$-unités décrites au chapitre précédent.

**Définition II.4.1** *Soit $S$ un ensemble fini d'idéaux premiers de $K$. On définit le groupe $K(S, 2)$ par*

$$K(S, 2) = \{\delta \in K^*/K^{*2} \text{ tel que } v_{\mathfrak{p}}(\delta) \equiv 0 \mod 2 \text{ pour tout } \mathfrak{p} \notin S\}.$$

Lorsque $K = \mathbb{Q}$, $S$ peut se représenter comme l'ensemble des nombres premiers qui divisent un certain entier $s$ non nul. L'ensemble $K(S, 2)$ peut alors se voir comme les

diviseurs sans facteur carré de $s$. La proposition que nous indiquons donne une description du groupe $K(S,2)$ comme groupe d'exposant 2, ou, ce qui est équivalent comme $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.

**Proposition II.4.2** *On a un isomorphisme*

$$K(S,2) \sim \frac{\mathbb{U}_{K,S}}{\mathbb{U}_{K,S}^2} \times \frac{Cl_S(K)}{Cl_S(K)^2}$$

*Preuve :* Notons $d_i$ les diviseurs élémentaires de $Cl_S(K)$ et $\mathfrak{g}_i$ les générateurs correspondants. Notons aussi $\alpha_i$ des générateurs des idéaux $S$-principaux $\mathfrak{g}_i^{d_i}$. On note $Cl'_S(K)$ le sous-groupe de $Cl_S(K)$ engendré par les $\mathfrak{g}_i$ dont les ordres $d_i$ sont pairs. Définissons le morphisme $\phi$ de la manière suivante :

$$\begin{aligned} \phi \ :&\mathbb{U}_{K,S} \times Cl'_S(K) \to K(S,2) \\ &(u, \prod \mathfrak{g}_i^{\varepsilon_i}) \qquad \mapsto u \prod \alpha_i^{\varepsilon_i} \end{aligned}$$

Il est clair qu'une $S$-unité a des valuations paires (car nulles) en tous les idéaux premiers qui ne sont pas dans $S$. De même, $\alpha_i$ a des valuations paires en dehors de $S$ car l'idéal principal $\alpha_i \mathbb{Z}_{K,S}$ se factorise en $\alpha_i \mathbb{Z}_{K,S} = \mathfrak{g}_i^{d_i}$ et $d_i$ est pair. Ainsi, le morphisme $\phi$ est bien défini. On peut remarquer que cette construction dépend du choix des générateurs $\alpha_i$ qui n'est possible qu'à une $S$-unité près.

Montrons que $\phi$ est surjectif. Soit $\delta \in K^*/K^{*2}$ tel que $v_\mathfrak{p}(\delta) \equiv 0 \mod 2$ pour tout $\mathfrak{p} \notin S$. L'idéal principal $\delta \mathbb{Z}_{K,S}$ est un carré, que l'on note $I^2$. Soit $I = \beta \prod \mathfrak{g}_i^{\beta_i}$ avec $\beta \in K^*$ et $0 \leqslant \beta_i < d_i$. Comme $I^2$ est principal, on a nécessairement $d_i \mid 2\beta_i$. Lorsque $d_i$ est impair, cela implique que $d_i \mid \beta_i$ et donc que $\beta_i = 0$. Pour les autres $d_i$, on a $\beta_i = \varepsilon_i \cdot d_i/2$ où $\varepsilon_i = 0$ ou 1. On a alors $\delta = \beta^2 \prod \alpha_i^{\varepsilon_i} \cdot u_s$ où $u_S$ est une $S$-unité. Ceci prouve la surjectivité de $\phi$.

Montrons que le noyau de $\phi$ est $\mathbb{U}_{K,S}^2 \times Cl'_S(K)^2$. Comme les carrés ont une image triviale dans $K(S,2)$, il est clair que ce sous-groupe est dans le noyau. Montrons que c'est exactement le noyau. Soit $(u_S, \prod \mathfrak{g}_i^{\varepsilon_i})$ un élément du noyau. On a $u_S \prod \alpha_i^{\varepsilon_i} = \beta^2$. En termes de $S$-idéaux, cela s'écrit $\prod \mathfrak{g}_i^{\varepsilon_i d_i} = \beta^2 \mathbb{Z}_{K,S}$. Comme les $d_i$ sont pairs, on peut diviser les exposants par 2 et affirmer que l'idéal $\prod \mathfrak{g}_i^{\varepsilon_i d_i/2}$ est $S$-principal. Mais la définition des entiers $d_i$ implique alors que chaque $d_i$ divise $\varepsilon_i \frac{d_i}{2}$ et donc que 2 divise chaque $\varepsilon_i$. Ainsi, $\mathfrak{g}_i^{\varepsilon_i}$ est bien dans $Cl'_S(K)^2$. Comme les $\varepsilon_i$ sont pairs, la relation $u_S \prod \alpha_i^{\varepsilon_i} = \beta^2$ montre que $u_S$ est un carré, et donc que $u_S \in \mathbb{U}_{K,S}^2$. Ceci montre que $\phi$ est $\mathbb{U}_{K,S}^2 \times Cl'_S(K)^2$ est bien le noyau de $\phi$.

Pour conclure la preuve, il suffit d'utiliser l'isomorphisme

$$\frac{Cl'_S(K)}{Cl'_S(K)^2} \sim \frac{Cl_S(K)}{Cl_S(K)^2}.$$

■

De cette proposition, on déduit les corollaires suivants :

**Corollaire II.4.3** *Le groupe $K(S,2)$ est un groupe fini d'exposant 2. De plus, si $h_2$ désigne le 2-rang du groupe de classes $Cl_S(K)$, alors l'ordre du groupe $K(S,2)$ est donné par*

$$|K(S,2)| = 2^{r_1+r_2+|S|+h_2}.$$

**Corollaire II.4.4** *Soit $S$ un ensemble fini d'idéaux premiers de $K$, et $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ des générateurs premiers de la 2-partie du groupe de classes $Cl_S(K)$. Si l'on pose $S' = S \cup \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$, alors on a*

$$K(S,2) \sim K(S',2) \sim \mathbb{U}_{K,S'}/\mathbb{U}_{K,S'}^2.$$

Grâce à ces corollaires, le calcul de $K(S,2)$ se ramène à un calcul de $S$-unités, et le groupe $K(S,2)$ est décrit exactement par un système fondamental de $S$-unités de $K$, donné par exemple par l'Algorithme I.1.2.

## II.4.2 Quartiques

Pour l'algorithme général du calcul du rang d'une courbe elliptique, nous avons besoin de manipuler des quartiques, plus précisément des courbes données par une équation de la forme $y^2 = g(x)$, où $g$ est un polynôme de degré 4. Nous avons besoin en particulier de savoir s'il existe des points sur ces courbes, aussi bien localement que globalement dans $K$. Nous utilisons parfois les quartiques sous leur forme semi-homogène, c'est-à-dire sous la forme $Y^2 = G(X,Z)$, où $G$ est un polynôme homogène de degré 4 : ceci correspond au changement de variables $x = X/Z$ et $y = Y/X^2$. Nous ne nous intéressons qu'aux solutions non triviales, c'est-à-dire $(X,Y,Z) \neq (0,0,0)$.

Nous montrons d'abord que l'étude locale se ramène à un nombre fini de places (les places infinies et celles qui divisent $2\operatorname{disc} g$), puis nous indiquons comment traiter chacune de ces places.

**Proposition II.4.5** *Soit $g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \in \mathbb{Z}_K[x,z]$ et soit $\mathfrak{p}$ un idéal premier de $K$. Si $\mathfrak{p}$ ne divise pas $2\operatorname{disc} g(x,1)$, alors l'équation $y^2 = g(x,z)$ admet localement une solution non triviale dans $\mathbb{Z}_{K,\mathfrak{p}}$.*

*Preuve :* La première partie de cette preuve vient de [Serf].

Commençons par montrer que l'on peut construire une solution modulo $\mathfrak{p}$. Ensuite nous utiliserons le Lemme de Hensel pour construire une solution dans $\mathbb{Z}_{K,\mathfrak{p}}$.

Si $a \equiv 0 \mod \mathfrak{p}$, alors $(x,y,z) = (1,0,0)$ est une solution modulo $\mathfrak{p}$. Si $a$ n'est pas nul modulo $\mathfrak{p}$, alors $g(x,1) \mod \mathfrak{p}$ est de degré 4 et sans facteur carré puisque $\mathfrak{p}$ ne divise pas son discriminant (ni son degré). Ainsi, l'équation $y^2 = g(x,1)$ définit une courbe de genre 1 sur le corps fini $K/\mathfrak{p} \sim \mathbb{F}_q$. L'inégalité de Hasse montre alors que le nombre de points sur cette courbe est au moins égal à $q + 1 - 2\sqrt{q}$ et donc au moins égal à 1 (ce point pouvant éventuellement être à l'infini).

Maintenant, nous savons que l'équation $y^2 = g(x,z)$ admet une solution non triviale $(x_0,y_0,z_0)$ modulo $\mathfrak{p}$. Si $y_0$ est non nul modulo $\mathfrak{p}$, alors on choisit des relèvements quelconques $x$ et $z$ de $x_0$ et $z_0$, et l'on applique le Lemme de Hensel (II.2.10) à la fonction $f(y) = y^2 - g(x,z)$. En effet, on a $v_{\mathfrak{p}}(f(y_0)) > 0$ par construction, et $v_{\mathfrak{p}}(f'(y_0)) = v_{\mathfrak{p}}(2y_0) = 0$. On a ainsi une solution de $y^2 = g(x,z)$.

Si $y_0$ est nul modulo $\mathfrak{p}$, alors on pose $y = 0$. On peut trouver des polynômes $\alpha_1(x)$ et $\beta_1(x)$ tels que

$$\alpha_1 g(x,z_0) + \beta_1 g'_x(x,z_0) = z_0^6 \operatorname{disc} g.$$

Comme le discriminant de $g(x,1)$ est égal au discriminant de $g(1,z)$, on peut aussi trouver $\alpha_2(x)$ et $\beta_2(x)$ tels que $\alpha_2 g(x_0,z) + \beta_2 g'_z(x_0,z) = x_0^6 \operatorname{disc} g$. Comme $x_0$ et $z_0$ ne sont pas tous les deux nuls en même temps, les égalités précédentes montrent que l'une au moins des quantités $g'_x(x_0,z_0)$ ou $g'_z(x_0,z_0)$ est non nulle modulo $\mathfrak{p}$. On peut alors appliquer le Lemme de Hensel (II.2.10) avec la fonction $f(x) = g(x,z_0)$ (ou avec $f(z) = g(x_0,z)$) et obtenir une solution de $g(x,z) = 0$ dans $\mathbb{Z}_{K,\mathfrak{p}}$. ■

Lorsque l'on regarde une quartique en une place réelle, on peut utiliser la proposition suivante (valable en réalité quel que soit le degré de $g$) :

**Proposition II.4.6** *Soit $g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \in \mathbb{R}[x,z]$ avec $a \neq 0$, et tel que* $\operatorname{disc} g(x,1) \neq 0$. *Notons $r_1$ le nombre de racines réelles de $g(x,1)$. L'équation $y^2 = g(x,z)$ admet toujours une solution non triviale dans $\mathbb{R}$ à moins que l'on ait simultanément*

$$r_1 = 0 \text{ et } a < 0.$$

Il reste donc à étudier ce qui se passe pour les places finies qui divisent 2 ou $\operatorname{disc} g$. Comme nous l'avions déjà annoncé précédemment, ceci peut se faire à l'aide de l'Algorithme II.2.12, que l'on applique à $y^2 = g(x,1)$, puis à $y^2 = g(1,z)$.

Une fois que l'on sait qu'une quartique est localement soluble en toutes les places de $K$, on peut chercher des points sur cette courbe. Malheureusement, il n'est pas suffisant pour une quartique d'être localement soluble pour l'être globalement. Dans l'algorithme des courbes elliptiques, cette obstruction est mesurée par le groupe de Tate-Shafarevich $Ш(E/K)$, sur lequel nous manquons de renseignements.

Pour chercher un point sur une quartique, on peut se contenter de tester toutes les valeurs de $x$ comprises entre deux bornes. Cette méthode naïve permet de trouver les points les plus simples. On peut raffiner en criblant sur quelques nombres premiers, et trouver ainsi des points un peu moins triviaux. Ces méthodes sont décrites dans [Cre a] et dans [Serf]. Récemment, J. Cremona ([Cre b]) a utilisé une méthode de descente pour trouver des points de grande hauteur sur certaines quartiques, ou montrer dans certains cas, qu'elles n'ont pas de solution. Malgré cela, il faut savoir qu'aucun algorithme n'est aujourd'hui connu pour résoudre en général cette question.

### II.4.3 Descente par 2-Isogénie : Courbes avec 2-Torsion

Nous ne donnons pas la preuve de l'algorithme, et nous ne voulons pas non plus rentrer dans les explications des différents groupes. Cet algorithme est décrit à la fois dans [Sil] (sous son aspect théorique) et dans [Cre a] (sous son aspect algorithmique lorsque $K = \mathbb{Q}$), ainsi que dans [Serf] (lorsque $K$ est un corps quadratique réel de nombre de classes 1).

On suppose ici que la courbe elliptique $E$ définie sur le corps de nombres $K$ est donnée par une équation de la forme

$$y^2 = x^3 + ax^2 + bx \qquad (E)$$

où $a, b \in \mathbb{Z}_K$. On peut toujours se ramener à cette situation, et un point de 2-torsion est alors donné par $(0,0)$. Le principe de l'algorithme est d'utiliser une isogénie $\phi$ de degré 2

avec la courbe

$$y^2 = x^3 + a'x^2 + b'x \qquad (E')$$

où $a' = -2a$ et $b' = a^2 - 4b$. Cette isogénie est définie par

$$\begin{aligned} \phi \ : E \quad &\to E' \\ (x,y) &\mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \end{aligned}$$

L'isogénie duale $\phi'$ est définie par

$$\begin{aligned} \phi' \ : E' \quad &\to E \\ (x,y) &\mapsto \left(\frac{y^2}{4x^2}, \frac{y(x^2-b')}{8x^2}\right) \end{aligned}$$

Lorsque l'on compose ces isogénies, on trouve un morphisme de $E$ dans $E$ (ou de $E'$ dans $E'$) qui n'est autre que la multiplication par 2 sur ces courbes elliptiques. Cela se note $\phi' \circ \phi = [2]_E$ et $\phi \circ \phi' = [2]_{E'}$. L'isogénie est dite de degré 2, car on obtient précisément la multiplication par 2 quand on la compose avec son isogénie duale. Les mauvais premiers (ceux pour lesquels les courbes ont mauvaise réduction) sont ceux qui divisent les discriminants de $E$ et de $E'$, c'est-à-dire ceux qui divisent $2bb'$. On note alors $S$, l'ensemble des idéaux premiers qui divisent $2bb'$ :

$$S = \{\mathfrak{p} \mid 2bb'\}.$$

Comme nous avons voulu suivre l'algorithme décrit dans [Sil], nous avons laissé cette définition de $S$. Nous verrons ensuite comment réduire significativement la taille de $S$.

**Algorithme II.4.7 (Descente par 2-isogénie)** (*Cet algorithme calcule un système de représentants de* $E'(K)/\phi(E(K))$ ) .

*1– Déterminer l'ensemble* $K(S,2)$.

*2– À chaque élément* $\delta \in K(S,2)$, *on associe la courbe* $(C_\delta)$ *(l'espace homogène) d'équation*

$$\delta y^2 = \delta^2 x^4 + a'\delta x^2 z^2 + b'z^4 \qquad (C_\delta).$$

*Déterminer le sous-groupe* $S^{(\phi)}(E/K) \subset K(S,2)$ *des éléments* $\delta$ *tels que la courbe* $(C_\delta)$ *est localement soluble en toutes les places (finies et infinies) de* $K$.

*3– Déterminer le sous-groupe* $\mathcal{E}'$ *de* $S^{(\phi)}(E/K)$ *des éléments* $\delta$ *tels que* $(C_\delta)$ *a un point* $(x,y,z)$ *non trivial dans* $K$.

*4– Pour chaque* $\delta \in \mathcal{E}'$, *construire le point* $P_\delta \in E'(K)$ *de coordonnées* $(\frac{\delta x^2}{z^2}, \frac{\delta yx}{z^3})$.

**Remarque** : Le groupe $S^{(\phi)}(E/K)$ est le groupe de Selmer de l'isogénie $\phi$. Il est construit essentiellement à partir de conditions locales, et sa détermination est certaine. Toutefois, il est essentiel de savoir qu'il n'existe aujourd'hui aucun algorithme qui sache résoudre l'étape 3. Plus précisément, on sait montrer qu'une quartique a des points localement, ou montrer qu'elle n'en a pas localement (c'est l'étape 2). Lorsqu'une quartique est soluble en

toutes les places (finies et infinies) de $K$, on peut chercher des points dessus en utilisant des méthodes plus ou moins perfectionnées. Dans certains cas, un algorithme de seconde-descente (voir [Cre b]) permet de prouver qu'il n'y a pas de point sur la quartique, ou bien de trouver des points difficilement accesibles aux méthodes naïves. Malheureusement, lorsque ces méthodes ne donnent aucun point, on ne peut en général pas montrer qu'il n'y a pas de point du tout, et l'on doit rester dans l'incertitude. Ainsi, l'algorithme de descente par 2-isogénie ne peut donner que des inégalités concernant le rang de la courbe elliptique. Ce phénomène d'existence de solutions locales et d'absence de solution globale est mesuré par le groupe de Tate-Shafarevich, et ainsi le Principe de Hasse n'est pas toujours vérifé dans le contexte des quartiques.

Avec les notations de l'algorithme précédent, on peut sensiblement améliorer l'ensemble de recherche $K(S,2)$. Sans que cela conduise à une confusion, nous notons $K(b',2)$ au lieu de $K(\{\mathfrak{p} \mid b'\},2)$.

**Proposition II.4.8** *Si la quartique $(C_\delta)$ est localement soluble en toutes les places de $K$, alors $\delta \in K(b',2)$.*

*Dans l'Algorithme II.4.7, on peut remplacer le groupe $K(S,2)$ par le sous-groupe $K(b',2)$.*

*Preuve :* La deuxième assertion est une conséquence immédiate de la première.

Soit $\mathfrak{p} \nmid b'$, et supposons que $(x,y,z)$ est une solution non triviale de $(C_\delta)$ localement en $\mathfrak{p}$. Remarquons d'abord que $v_\mathfrak{p}(b') = 0$ $v_\mathfrak{p}(a') \geqslant 0$. Notons $e_1 = v_\mathfrak{p}(\delta x^2)$ et $e_2 = v_\mathfrak{p}(z)$. Regardons successivement les trois cas correspondants aux valeurs relatives de $e_1$ et $2e_2$.

– 1$^{\text{er}}$cas : $e_1 < 2e_2$. On a les valuations suivantes : $v_\mathfrak{p}(\delta^2x^4) = 2e_1$, $v_\mathfrak{p}(a'\delta x^2z^2) = v_\mathfrak{p}(a') + e_1 + 2e_2 > 2e_1$, et $v_\mathfrak{p}(b'z^4) = 4e_2 > 2e_1$. Ainsi, $\delta^2x^4$ est le terme qui a la plus petite valuation et l'on a $2e_1 = v_\mathfrak{p}(\delta^2x^4) = v_\mathfrak{p}(\delta y^2)$, ce qui implique que $v_\mathfrak{p}(\delta)$ est pair.

– 2$^{\text{e}}$cas : $e_1 = 2e_2$. Comme on a $v_\mathfrak{p}(\delta x^2) = e_1 = 2e_2$, $v_\mathfrak{p}(\delta)$ est nécessairement pair.

– 3$^{\text{e}}$cas : $e_1 > 2e_2$. On a les valuations suivantes : $v_\mathfrak{p}(\delta^2x^4) = 2e_1 > 4e_2$, $v_\mathfrak{p}(a'\delta x^2z^2) = v_\mathfrak{p}(a') + e_1 + 2e_2 > 4e_2$, et $v_\mathfrak{p}(b'z^4) = 4e_2$. Ainsi, $b'z^4$ est le terme qui a la plus petite valuation et l'on a $4e_2 = v_\mathfrak{p}(b'z^4) = v_\mathfrak{p}(\delta y^2)$, ce qui implique que $v_\mathfrak{p}(\delta)$ est pair.

On a donc montré que dans tous les cas, $v_\mathfrak{p}(\delta)$ est pair. Comme cela est vrai pour tous les $\mathfrak{p} \nmid b'$, cela signifie exactement que $\delta \in K(b',2)$. ■

Pour retrouver le groupe $E(K)/2E(K)$ à partir des renseignements donnés par l'algorithme, on utilise les suites exactes

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0$$

et

$$0 \to E(K)/\phi'(E'(K)) \to S^{(\phi')}(E'/K) \to Ш(E'/K)[\phi'] \to 0$$

À partir des deux quotients $E'(K)/\phi(E(K))$ et $E(K)/\phi'(E'(K))$, et de l'expression explicite des isogénies $\phi$ et $\phi'$, il n'est pas difficile de retrouver les groupes $E(K)/2E(K)$ et $E'(K)/2E'(K)$, et en particulier le rang de ces courbes elliptiques. On remarquera que les deux courbes $E$ et $E'$ sont isogènes sur $K$ et donc elles ont le même rang.

### II.4.4 Exemple du Calcul du Rang d'une Courbe avec 2-Torsion

On se place dans le corps $K = \mathbb{Q}(\zeta)$ avec $\zeta^5 - \zeta^3 - \zeta^2 + \zeta + 1 = 0$. Ce corps est de discriminant 1609, et son groupe de classes est trivial. Dans ce corps, on veut étudier la courbe elliptique

$$y^2 = x^3 + x^2 - \zeta x \quad (E).$$

On va appliquer l'Algorithme II.4.7 avec $a = 1$ et $b = -\zeta$. On utilise l'isogénie avec la courbe

$$y^2 = x^3 - 2x^2 + (1 + 4\zeta)x \quad (E'),$$

c'est-à-dire que l'on a $a' = -2$ et $b' = 1 + 4\zeta$. Ces deux courbes admettent le point $(0, 0)$ comme unique point de 2-torsion.

• Détermination de $E'(K)/\phi(E(K))$.

L'élément $b' = 1 - 4\zeta$ est de norme $-719$. Le groupe $K(b', 2)$ est d'ordre $2^4$ et est engendré par

$$K(b', 2) = \left\langle -1, \zeta, \zeta^4 - \zeta, -3\zeta^4 - \zeta^3 + 3\zeta^2 + 4\zeta - 2 \right\rangle,$$

où les $\langle\rangle$ signifient que l'on ne donne que les générateurs de ce 2-groupe. Les normes de ces générateurs valent $-1$, $-1$, $1$, $-719$. L'examen successif des valeurs de $\delta \in K(b', 2)$ donne des quartiques non solubles en 2 pour $\delta$ valant $-1$, $\zeta$, $-\zeta$, $\zeta^4 - \zeta$, $-\zeta^4 + \zeta$. Pour $\delta = \zeta(\zeta^4 - \zeta)$, on trouve la quartique

$$y^2 = (\zeta^3 - \zeta - 1)x^4 - 2x^2z^2 + (3\zeta^4 - 3\zeta^3 - 4\zeta^2 + 3)z^4,$$

qui possède le point $(\zeta^4 - \zeta^2, 2\zeta^3 - 2\zeta^2, 1)$. Ce point permet de construire le point de $E'$ :

$$P'_1 = (2\zeta^2 - 1, -2\zeta^4 + 2\zeta^3 - 2\zeta).$$

Pour $\delta = -3\zeta^4 - \zeta^3 + 3\zeta^2 + 4\zeta - 2$, on trouve la quartique

$$y^2 = (-3\zeta^4 - \zeta^3 + 3\zeta^2 + 4\zeta - 2)x^4 - 2x^2z^2 + y^2z^4,$$

qui possède la solution triviale $(0, \zeta, 1)$, qui donne le point $(0, 0)$ sur $E'$.

En utilisant la structure de 2-groupe de $S^{(\phi)}(E/K)$ et de $E'(K)/\phi(E(K))$, on voit que les résultats pour les autres éléments de $K(b', 2)$ peuvent se déduire des précédents, et en particulier que les points éventuels que l'on trouvera sur la courbe elliptique sont des combinaisons linéaires des précédents.

On a donc les résultats partiels :

$$\begin{aligned} |E'(K)/\phi(E(K))| &= 4 \\ |S^{(\phi)}(E/K)| &= 4 \\ |Ш(E/K)[\phi]| &= 1 \end{aligned}$$

• Détermination de $E(K)/\phi'(E'(K))$.

L'élément $b = -\zeta$ est une unité. Le groupe $K(b,2)$ est d'ordre $2^3$ et est engendré par

$$K(b,2) = \left\langle -1, \zeta, \zeta^4 - \zeta \right\rangle .$$

L'examen successif des valeurs de $\delta \in K(b,2)$ donne des quartiques non solubles en l'unique place réelle de $K$ pour $\delta$ valant $-1$ et $\zeta$. Pour $\delta = -\zeta$, on trouve la quartique

$$y^2 = -\zeta x^4 + x^2 z^2 + z^4,$$

qui admet comme solution triviale $(0,1,1)$, et qui donne le point trivial $(0,0)$ sur $E$. Pour $\delta = \zeta^4 - \zeta$, on trouve la quartique

$$y^2 = (\zeta^4 - \zeta)x^4 + x^2 z^2 + (\zeta^4 - \zeta^2 + 1)z^4,$$

qui possède le point $(\zeta^2 - 1, -\zeta^4 + \zeta^3 - \zeta^2, 1)$. Ce point permet de construire le point de $E$ :

$$P_1 = (-\zeta^4 + \zeta^2, -2\zeta^4 + 2\zeta^2 - 1).$$

On utilise la structure de groupe pour obtenir directement les résultats partiels :

$$\begin{aligned} |E(K)/\phi'(E'(K))| &= 4 \\ |S^{(\phi')}(E'/K)| &= 4 \\ |Ш(E'/K)[\phi']| &= 1 \end{aligned}$$

En combinant les différents résultats, on trouve

$$\begin{aligned} |Ш(E/K)[2]| &= 1 \\ |E(K)[2]| &= 2 \\ |E(K)/2E(K)| &= 8 \\ \text{rang } (E/K) &= 2 \end{aligned}$$

Enfin, en utilisant l'isogénie $\phi'$, on trouve les points

$$\begin{aligned} \phi'(P_1') &= (5\zeta^4 - 4\zeta^3 - 2\zeta^2 - 3\zeta + 7, 17\zeta^4 - 12\zeta^3 - 9\zeta^2 - 11\zeta + 25) \\ P_1 &= (-\zeta^4 + \zeta^2, -2\zeta^4 + 2\zeta^2 - 1) \end{aligned}$$

qui engendrent un sous-groupe de rang maximal sur la courbe elliptique $E$.

### II.4.5 Algorithme pour les Courbes sans 2-Torsion

Nous nous donnons une courbe elliptique définie sur un corps de nombres $K$ sans 2-torsion et de la forme

$$y^2 = x^3 - 27Ix - 27J \qquad (E)$$

avec $I, J \in \mathbb{Z}_K$. On peut toujours se ramener à cette situation en posant $I = c_4$ et $J = 2c_6$, où $c_4$ et $c_6$ sont les invariants classiques de la courbe $E$ (voir par exemple [Sil]).

Posons $\Delta = 4I^3 - J^2$ et notons $\theta$ une racine de

$$\theta^3 = 3I\theta - J.$$

Avec cette définition, $K(\theta)$ est le plus petit corps dans lequel $(E)$ possède de la 2-torsion (en effet, $(0, -3\theta) \in E[2]$). À partir de l'article [Cre c], on peut déduire l'algorithme suivant :

**Algorithme II.4.9** (*Cet algorithme calcule le rang de la courbe $E(K)$ d'équation $y^2 = x^3 - 27Ix - 27J$ (sans 2-torsion) et trouve un système de représentants de $E(K)/2E(K)$).*

*1– Déterminer le groupe $K(\theta)(S, 2)$ où $S$ contient les idéaux premiers de $K(\theta)$ qui divisent $3\Delta$, ainsi que les idéaux premiers qui engendrent la 2-partie du groupe de classes $Cl(K(\theta))$. Déterminer également le groupe $K(S', 2)$ où $S'$ contient les normes des idéaux de $S$ (voir le paragraphe II.4.1).*

*2– Déterminer le noyau $K(\theta)(S, 2)_1$ de l'application norme*

$$\mathcal{N}_{K(\theta)/K} : K(\theta)(S, 2) \to K(S', 2).$$

*3– Déterminer le sous-ensemble $H$ de $K(\theta)(S, 2)_1$ des éléments $\delta$ qui peuvent s'écrire sous la forme $\delta = a' + b'\theta$ (d'après l'Algorithme II.4.10).*

*4– Pour chaque élément $\delta = a' + b'\theta \in H$ de norme $\mathcal{N}_{K(\theta)/K} = r^2$, poser*

$$p = 3a',\ a = \frac{3b'}{4},\ b = 0,\ c = -\frac{p}{8a},\ d = \frac{r}{8a^2},\ e = \frac{I - c^2}{12a}$$

*puis associer à $\delta$ la quartique (ou espace homogène) $(C_\delta)$ d'équation*

$$y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \qquad (C_\delta)$$

*dont les invariants $I$,$J$ et $\Delta$ sont les mêmes que ceux de la courbe $E$.*

*5– Déterminer le sous-groupe $S^{(2)}(E/K) \subset H \subset K(\theta)(S, 2)_1$ des éléments $\delta$ tels que la quartique $(C_\delta)$ est localement soluble en toutes les places de $K$.*

*6– Déterminer le sous-groupe $\mathcal{E}$ de $S^{(2)}(E/K)$ des éléments $\delta$ tels que la courbe $(C_\delta)$ a un point $(x, y, z)$ non trivial dans $K$.*

*7– Pour chaque $\delta \in \mathcal{E}$, construire le point $P_\delta \in E(K)$ défini par ses coordonnées $(x_P, y_P)$ :*

$$x_P = \frac{3g_4(x, z)}{(2y)^2}$$
$$y_P = \frac{27g_6(x, z)}{(2y)^3}$$

*où $g_4$ et $g_6$ sont définis par les formules suivantes en fonction des coefficients $a, b, c, d, e$ de*

*la quartique $C_\delta$ :*

$$\begin{aligned} g_4(x,z) =& (3b^2 - 8ac)x^4 + 4(bc - 6ad)x^3z + 2(2c^2 - 24ae - 3bd)x^2z^2 \\ &+ 4(cd - 6be)xz^3 + (3d^2 - 8ce)z^4 \\ g_6(x,z) =& (b^3 + 8a^2d - 4abc)x^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)x^5z \\ &+ 5(8abe + b^2d - 4acd)x^4z^2 + 20(b^2e - ad^2)x^3z^3 \\ &- 5(8ade + bd^2 - 4bce)x^2z^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)xz^5 \\ &- (d^3 + 8be^2 - 4cde)z^6 \end{aligned}$$

**Remarque** : Nous avons voulu suivre de près les notations de [Cre c], ce qui nous fait laisser $b$ dans toutes les expressions. Comme $b$ est toujours nul, les formules se simplifient significativement. On peut aussi les simplifier en faisant apparaître les différents invariants $I$, $J$, $p$, $r\ldots$

Faisons quelques remarques sur les divers ensembles qui interviennent dans cet algorithme. L'ensemble $H$ défini à l'étape 3 n'est en général pas un sous-groupe de $K(\theta)(S,2)_1$. Le groupe $S^{(2)}(E/K)$ défini à l'étape 5 est le groupe de Selmer de la courbe $(E)$ pour la multiplication par 2. Il mesure l'existence de points locaux sur la courbe. Le groupe $\mathcal{E}$ est isomorphe à $E(K)/2E(K)$. Le quotient $S^{(2)}(E/K)/\mathcal{E} = Ш(E/K)[2]$ est la 2-torsion du groupe de Tate-Shafarevich $Ш(E/K)$. Ce groupe mesure l'obstruction pour les quartiques localement solubles en toutes les places de $K$ a être globalement solubles. Pour les équations de Legendre, le principe de Hasse signifie qu'il suffit d'être localement soluble pour l'être globalement, et donc une telle obstruction n'existerait pas dans ce cas. Il existe des courbes elliptiques pour lesquelles on sait montrer que le groupe $Ш(E/K)[2]$ n'est pas trivial.

Ces différents groupes sont liés par la suite exacte suivante :

$$0 \to E(K)/2E(K) \to S^{(2)}(E/K) \to Ш(E/K)[2] \to 0$$

Une conjecture classique affirme que le groupe $Ш(E/K)$ est fini, ce qui implique que son ordre est un carré parfait, et en particulier que l'ordre du sous-groupe $Ш(E/K)[2]$ est aussi un carré parfait. Comme ce sous-groupe est un 2-groupe, son ordre est alors de la forme $2^e$ où $e$ est pair. Ce renseignement peut parfois servir à montrer (conjecturalement) qu'il existe des points sur la courbe, même si on n'en a pas trouvé.

Comme dans le cas de l'algorithme de descente par 2-isogénie, il est souvent impossible de montrer qu'une quartique n'a pas de point global alors qu'elle est localement soluble en toutes les places de $K$ : on ne sait en général pas montrer qu'une quartique provient d'un élément non nul du groupe $Ш(E/K)$, ou d'un point non trivial de la courbe elliptique.

**Remarque** : Si l'on dispose par avance de points sur la courbe, on peut retrouver les éléments de $K(\theta)(S,2)$ dont ils proviennent, et éviter ainsi de faire inutilement des calculs pour les retrouver. En effet, si l'on connait un point $(x,y)$ sur la courbe, alors il vérifie

$$y^2 = x^3 - 27Ix - 27J = \mathcal{N}_{K(\theta)/K}(x + 3\theta),$$

ce qui signifie que $\delta = x + 3\theta$ (à un carré près). À partir de cette expression de $\delta$, on voit que si la valuation de $\delta$ en un idéal premier $\mathfrak{p}$ est impaire, alors $\mathfrak{p}$ doit aussi diviser $\mathcal{N}_{K(\theta)/K}(\delta)/\delta = 9\theta^2 - 3x\theta + x^2 - 27I$, et donc $\mathfrak{p}$ doit diviser le résultant $\mathrm{Res}_x(x + 3\theta, 9\theta^2 - 3x\theta + x^2 - 27I) = 27(\theta^2 - I)$ dont la norme vaut $3^{12}\Delta$. Cela justifie donc le choix de $S$ à l'étape 1 de l'Algorithme II.4.9.

**Sous-algorithme II.4.10 (Linéarisation)** (*Cet algorithme représente un élément* $\delta = a + b\theta + c\theta^2 \in K(\theta)(S,2)_1$ *sous la forme* $\delta = a' + b'\theta$, *ou prouve que cela est impossible*)

*1– Poser* $\alpha = 3c^2I + ac - b^2$, $\beta = ab + c^2J$ *et* $\mathcal{N}_{K(\theta)/K}(\delta) = r^2$.

*2– Si* $c = 0$, *renvoyer* $\delta$. *Si* $\alpha = 0$, *renvoyer* $1/\delta$.

*3– À l'aide des Propositions II.2.6 et II.2.7, ainsi que de l'Algorithme II.2.12, déterminer si l'équation*

$$\alpha u_1^2 + v_1^2 - cw_1^2 = 0$$

*admet une solution. S'il n'y a pas de solution, alors* $\delta$ *n'a pas de représentation linéaire en* $\theta$, *et s'arrêter.*

*4– À l'aide de l'Algorithme II.3.2, trouver une solution* $(u_1, v_1, w_1)$ *de l'équation précédente, et poser*

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} c & b & 3cI + a \\ & \alpha & -\beta \\ & & r \end{pmatrix}^{-1} \begin{pmatrix} u_1 \\ v_1 \\ w_1 \end{pmatrix}$$

*5– Renvoyer* $\delta = \delta \cdot (u + v\theta + w\theta^2)^2$.

Dans cet algorithme, on cherche à résoudre $\delta z^2 = a' + b'\theta$. En posant $z = u + v\theta + w\theta^2$, la composante suivant $\theta^2$ de $\delta z^2$ est donnée par une forme quadratique $Q(u,v,w)$. On peut diagonaliser cette forme quadratique à l'aide d'un changement de variables (explicité à l'étape 4). On est alors amené à résoudre la forme quadratique diagonale $\alpha u_1^2 + v_1^2 - cw_1^2 = 0$.

## II.4.6 Exemple du Calcul du Rang d'une Courbe Sans 2-Torsion

Plaçons nous dans le corps cubique $K = \mathbb{Q}(\zeta)$ où $\zeta^3 + \zeta^2 - 1 = 0$. Nous voulons déterminer le rang de la courbe elliptique définie par l'équation

$$y^2 = x^3 + \zeta.$$

Si l'on fait une homothétie sur $x$ et $y$, on voit que cette courbe est isomorphe sur $K$ à la courbe d'équation

$$y^2 = x^3 + 729\zeta \quad (E).$$

Ainsi, on peut appliquer l'Algorithme II.4.9 avec $I = 0$ et $J = -27\zeta$ et $\Delta = -3^9\zeta^2$. Notons $\theta$ une racine de $\theta^3 - 27\zeta = 0$, et $\theta' = \frac{\theta}{3}$. Les corps $K$ et $K(\theta)$ sont principaux, et le seul premier qui interviendra est 3 (inerte dans $K$). Ainsi, pour $S = \{3\}$, on détermine les ensembles $K(S,2)$ et $K(\theta)(S,2)$ :

$$\begin{aligned} K(S,2) &= \langle \zeta, -1, 3 \rangle \\ K(\theta)(S,2) &= \langle \theta', (\zeta^2 + \zeta)(\theta'^2 - 1), \theta'^2 + \zeta, \zeta\theta'^2 + \theta'), -1, \\ &\qquad (\zeta^2 + \zeta + 1)\theta'^2 + (\zeta^2 + \zeta)\theta' + (\zeta^2 + \zeta + 1) \rangle. \end{aligned}$$

Les éléments de norme carrée forment le groupe $K(\theta)(S,2)_1$ donné par

$$\begin{aligned} K(\theta)(S,2)_1 = \langle \delta_1 &= \theta'^2 + \zeta, \\ \delta_2 &= \zeta\theta'^2 + \theta', \\ \delta_3 &= -(\zeta^2+\zeta)\theta'^2 + \zeta^2 + \zeta \rangle. \end{aligned}$$

Les normes valent toutes 1.

Nous utilisons la structure de 2-groupe de $S^{(2)}(E/K)$ et $E(K)/2E(K)$ pour économiser un grand nombre d'étapes (3 au lieu de $2^3$).

• Pour $\delta = \delta_1$

On a $\delta = \theta'^2 + \zeta$, c'est-à-dire $a = 1/9$, $b = 0$, $c = \zeta$ et $r = 1$. On pose $\alpha = \zeta/9$. Pour linéariser $\delta$, il faut résoudre l'équation de Legendre

$$\frac{\zeta}{9}u_1^2 + v_1^2 - \zeta w_1^2 = 0.$$

On trouve la solution (triviale) $(u_1, v_1, w_1) = (3, 0, 1)$, ce qui donne $z = -9\zeta + (3\zeta^2 + 3\zeta - 3)\theta + \theta^2$. Si l'on remplace $\delta$ par $\delta \cdot z^2/9^2$, on obtient

$$\delta = 1 + (2\zeta^2 - 2)\theta'.$$

La quartique $C_\delta$ a pour équation

$$y^2 = \frac{1}{2}(\zeta^2-1)x^4 + \frac{3}{4}(\zeta^2+\zeta+1)x^2z^2 + \frac{1}{2}(2\zeta^2+\zeta+1)xz^3 + \frac{1}{32}(4y^2+21y+15)z^4.$$

Cette quartique admet comme solution le point $\left(\frac{\zeta^2+\zeta+1}{2}, \zeta^2+\zeta+1, 1\right)$, ce qui donne le point de $(E)$ :

$$P_1 = \left(9, 27(\zeta^2+\zeta)\right).$$

• Pour $\delta = \delta_2$

On a $\delta = \zeta\theta'^2 + \theta'$, c'est-à-dire $a = 0$, $b = 1/3$, $c = \zeta/9$ et $r = 1$. On pose $\alpha = -1/9$. Pour linéariser $\delta$, il faut résoudre l'équation de Legendre

$$-\frac{1}{9}u_1^2 + v_1^2 - \frac{1}{3}(\zeta^2-1)w_1^2 = 0.$$

Comme $-\alpha$ est un carré, on trouve la solution triviale $(u_1, v_1, w_1) = (3, -1, 0)$, ce qui donne $z = 9\theta$. Si l'on remplace $\delta$ par $\delta \cdot z^2/27^2$, on obtient

$$\delta = \zeta + \zeta^2\theta'.$$

La quartique $C_\delta$ a pour équation

$$y^2 = \frac{1}{4}\zeta^2x^4 - \frac{3}{8}(\zeta^2+1)x^2z^2 + \frac{1}{8}(\zeta^2+\zeta+1)xz^3 - \frac{3}{256}(\zeta+1)^2z^4.$$

Cette quartique admet comme solution le point $\left(1, \frac{\zeta}{2}, 0\right)$, ce qui donne le point de $(E)$ :

$$P_2 = (9\zeta(\zeta+1), 27(\zeta+1)).$$

• Pour $\delta = \delta_3$

On a $\delta = -(\zeta^2+\zeta)\theta'^2 + \zeta^2 + \zeta$, c'est-à-dire $a = \zeta^2+\zeta$, $b = 0$, $c = -(\zeta^2+\zeta)/9$ et $r = 1$. On pose $\alpha = -(\zeta+1)/9$. Pour linéariser $\delta$, il faut résoudre l'équation de Legendre

$$-\frac{1}{9}(\zeta+1)u_1^2 + v_1^2 + \frac{1}{9}(\zeta^2+\zeta)w_1^2 = 0.$$

On trouve la solution (encore une fois triviale) $(u_1, v_1, w_1) = (1, (\zeta^2+\zeta)/3, 0)$, ce qui donne $z = -9\zeta(1+\theta')$. Si l'on remplace $\delta$ par $\delta \cdot z^2/(9\zeta)^2$, on obtient

$$\delta = (2\zeta^2 + 2\zeta - 1)\theta' + \zeta^2 + \zeta - 2.$$

La quartique $C_\delta$ a pour équation

$$y^2 = \frac{1}{4}(2\zeta^2+2\zeta-1)x^4 + \frac{3}{22}(3\zeta^2+9\zeta-4)x^2z^2 + \frac{2}{121}(16\zeta^2+37\zeta+41)xz^3$$
$$+\frac{3}{5324}(166\zeta^2 - 327\zeta + 17)z^4.$$

Cette quartique admet comme solution le point $\left(\frac{7\zeta^2+10\zeta+9}{11}, \zeta^2+2\zeta+1, 1\right)$, ce qui donne le point de $(E)$ :

$$P_3 = (-9\zeta, 27\zeta^2).$$

Les résultats que nous avons trouvés permettent de déduire les informations suivantes :

$$\begin{aligned} |S^{(2)}(E/K)| &= 8 \\ |E(K)/2E(K)| &= 8 \\ |Ш(E/K)[2]| &= 1 \\ \text{rang } (E/K) &= 3, \end{aligned}$$

un système de points de $E$ de rang maximal étant donné par

$$\begin{aligned} P_1 &= (9, 27(\zeta^2+\zeta)) \\ P_2 &= (9(\zeta^2+\zeta), 27(\zeta+1)) \\ P_3 &= (-9\zeta, 27\zeta^2) \end{aligned}$$

On retrouve les points suivants sur la courbe $y^2 = x^3 + \zeta$ à partir de ceux de $E$ :

$$\begin{aligned} Q_1 &= (1, \zeta^2+\zeta) \\ Q_2 &= (\zeta^2+\zeta, \zeta+1) \\ Q_3 &= (-\zeta, \zeta^2) \end{aligned}$$

# Chapitre III

# Équations aux Normes

## Introduction

Le but de ce chapitre est de résoudre explicitement une équation du type

$$\mathcal{N}_{L/K}(x) = a,$$

où $L/K$ est une extension relative de corps de nombres arbitraire fixée, et $a$ est un élément non nul du corps de nombres $K$. Nous voulons aussi être capable de décider si une équation a une solution ou si elle n'en a pas. Nous ne nous limitons pas aux solutions entières de cette équation, mais à n'importe quelle solution rationnelle.

Si l'on écrit $a$ sous la forme $a = \alpha/d$ avec $d \in \mathbb{Z}$, et $\alpha$ entier algébrique dans $K$, alors nous voyons que l'équation est équivalente à $\mathcal{N}_{L/K}(x) = d^{n-1}\alpha$ où $n = [L : K]$ est le degré de l'extension, à cause de la relation $\mathcal{N}_{L/K}(d) = d^n$. Ainsi, on peut toujours faire l'hypothèse non restrictive que $a$ est un entier algébrique.

La première idée pour résoudre cette équation est de chercher des solutions entières lorsque $a$ est lui-même entier, et ceci peut se faire par exemple en majorant la (ou les) valeur absolue des solutions. Cette idée que nous n'utiliserons pas est développée par C.L. Siegel dans [Sie] pour le cas des extensions galoisiennes, par U. Fincke et M. Pohst dans [Fin-Poh] pour le cas d'une extension quelconque de $\mathbb{Q}$, ou par C. Fieker, A. Jurk et M. Pohst dans [Fie-Jur-Poh] pour le cas relatif. Une solution plus algébrique de ce problème est donnée par D. Garbanati dans [Gar] pour le cas d'une extension abélienne. Récemment, C. Fieker (dans [Fie]) a décrit un algorithme résolvant cette équation dans le cas des extensions galoisiennes en utilisant, comme nous allons le faire, les $S$-unités. Notre but dans ce chapitre est de donner une description algébrique des solutions pour le cas général, et d'en déduire un algorithme efficace. À notre connaissance, c'est la première fois qu'un tel algorithme est décrit. En particulier, jusqu'à présent aucun algorithme ne pouvait décider si une équation aux normes tout à fait générale admet une solution ou n'en admet pas.

Nous démontrons d'abord quelques théorèmes donnant une description précise de la factorisation en idéaux premiers des solutions, qui donnent une borne sur les premiers qui interviennent dans les solutions. Ensuite nous déduisons de ces théorèmes un algorithme

qui construit une solution, ou prouve qu'il n'y a pas de solution. Cet algorithme suppose que nous avons une bonne connaissance du corps $L$, par exemple que nous disposons d'un système fondamental d'unités de $L$, et que nous savons résoudre le problème de "l'idéal principal". Nous illustrons chaque proposition par un exemple.

Si l'on peut prouver qu'il n'y a pas de solution entière, cela ne prouve malheureusement pas qu'il n'y a pas de solution du tout. En effet, considérons l'exemple suivant :
**Exemple** : Soit $L/K = \mathbb{Q}(\sqrt{34})/\mathbb{Q}$, et $a = -1$. L'unité fondamentale de $L$ est $u = 6\sqrt{34}+35$ dont la norme est $+1$, ce qui prouve que $a$ n'est pas la norme d'un entier algébrique de $L$. Toutefois, nous avons $\mathcal{N}_{L/K}((\sqrt{34}+5)/3) = -1$.

L'existence de solutions rationnelles (et non entières) pour l'équation $\mathcal{N}_{L/K}(x) = a$ pourrait nous laisser penser qu'on ne peut pas réduire ce problème à un nombre fini de tests. Notre but est de démontrer au contraire comment cela est possible, en donnant une borne sur le dénominateur, ou plus précisément en donnant la liste finie des idéaux premiers qui peuvent intervenir au numérateur et au dénominateur. Ainsi, il devient algorithmiquement possible de décider de l'existence d'une solution rationnelle, et de trouver une solution lorsqu'il y en a.

Nous allons utiliser les résultats du chapitre I et décrire les solutions en termes de $S$-unités. Soit $S$ un ensemble fini d'idéaux premiers du corps de base $K$. Nous notons $\mathbb{U}_{K,S}$ le groupe des $S$-unités de $K$ et $\mathbb{U}_{L,S}$ le groupe des $S$-unités de $L$. Tous les idéaux premiers qui divisent $a$ doivent avoir une contribution dans les solutions $x$, c'est-à-dire que nous pouvons faire l'hypothèse que $S$ contient tous les idéaux premiers qui divisent $a$, de sorte que $a$ est une $S$-unité.

Il est clair que la norme d'une $S$-unité de $L$ est une $S$-unité de $K$, en d'autres termes que $\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) \subset \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$. L'exemple précédent nous montre que l'inclusion réciproque n'est pas vraie en général (ici avec $S = \varnothing$) : une $S$-unité qui est une norme n'est pas toujours la norme d'une $S$-unité.

Le théorème que nous allons démontrer affirme que l'on a égalité dès que $S$ est assez grand, c'est-à-dire dès que $S$ contient un certain sous-ensemble $S_0$ qui ne dépend que de l'extension $L/K$. Ainsi, pour résoudre l'équation $\mathcal{N}_{L/K}(x) = a$, il suffit de considérer les idéaux premiers qui divisent $a$, ainsi que les idéaux premiers exceptionnels de $S_0$.

**Théorème (Théorème Principal)** *Soit $L/K$ une extension de corps de nombres. Il existe un ensemble fini $S_0$ d'idéaux premiers de $K$, ne dépendant que de $L$ et $K$, tel que*

$$\textit{si } S \supset S_0 \textit{ alors } \mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

Un tel $S_0$ est donné explicitement en termes de générateurs de groupes de classes. Il est intéressant de remarquer que la preuve de ce théorème repose essentiellement sur la construction d'éléments de norme 1, grâce auxquels on peut translater une solution qui ne serait pas une $S$-unité. Quand $S$ ne contient pas $S_0$, il est tout de même possible de donner quelques renseignements concernant le groupe quotient $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$, d'autant plus précis que l'extension est galoisienne, ou mieux abélienne : ces renseignements sont donnés par des "théorèmes de structure".

**Définition** : On dit qu'un groupe $G$ est un *$n$-groupe* si tous les premiers qui divisent $|G|$ divisent aussi $n$. Si $G$ est abélien, on dit que $G$ est d'*exposant $d$* si $g^d = 1$ pour tout $g \in G$, et si $d$ est minimal pour cette propriété. Dans ce cas, $d$ est toujours un diviseur de $|G|$.

**Notation** : Lorsque nous ferons agir un groupe de Galois $G$ sur des éléments ou des idéaux, nous utiliserons la notation $I^\sigma$ et $x^\sigma$ pour $\sigma(I)$ et $\sigma(x)$. Cette notation exponentielle nous permettra de faire des calculs dans l'anneau de groupe $\mathbb{Z}[G]$, de sorte que l'on aura $I^{\alpha+\beta} = I^\alpha \cdot I^\beta$ et $I^{\alpha\beta} = (I^\beta)^\alpha$.

# III.1 Équations aux Normes dans les Extensions Galoisiennes

Dans le cas où l'extension $L/K$ est galoisienne, la situation est considérablement simplifiée, et pour cette raison nous commençons par étudier ce cas. On trouve déjà ces résultats dans [Fie].

## III.1.1 Preuve du Théorème Principal pour les Extensions Galoisiennes

Avant de montrer le Théorème Principal, nous étudions un peu plus en détail l'exemple de l'introduction pour nous donner une idée du résultat général.
**Exemple** : L'extension $L/K$ est l'extension quadratique réelle $\mathbb{Q}(\sqrt{34})/\mathbb{Q}$ de discriminant 136. L'unité fondamentale est $6\sqrt{34} + 35$ de norme $+1$. On a les relations suivantes :

$$\mathcal{N}_{L/K}((\sqrt{34}+5)/3) = -1,$$

$$\mathcal{N}_{L/K}((\sqrt{34}+3)/5) = -1,$$

$$\mathcal{N}_{L/K}((5\sqrt{34}+27)/11) = -1,$$

$$\mathcal{N}_{L/K}((5\sqrt{34}+3)/29) = -1,$$

$$\mathcal{N}_{L/K}((25\sqrt{34}+141)/37) = -1, \ldots$$

Ainsi, $-1$ est la norme d'une $S$-unité dès que $S$ contient l'un des premiers 3, 5, 11, 29, 37, ... Or, il se trouve que le corps $L = \mathbb{Q}(\sqrt{34})$ a un groupe de classes non trivial d'ordre 2 qui peut être engendré par des idéaux premiers au-dessus de 3, 5, 11, 29, 37,...Dans cet exemple, la condition pour que $-1$ soit la norme d'une $S$-unité semble être que $S$ engendre le groupe de classes de $L$ : c'est exactement ce que nous allons démontrer.

Nous noterons toujours $S$ pour un ensemble d'idéaux premiers du corps de base $K$, et par un abus de notation, justifié par la définition des $S$-unités donnée dans I.1, $S$ sera aussi l'ensemble des idéaux premiers de $L$ au-dessus des premiers de $K$ pour toute extension finie $L$ de $K$.

**Lemme III.1.1** *Soit $L/K$ une extension galoisienne, $S$ un ensemble fini d'idéaux premiers de $K$. Soit $A$ un idéal $S$-entier de $K$, et $X$,$Y$ deux idéaux $S$-entiers de $L$. Supposons qu'ils satisfont la relation $\mathcal{N}_{L/K}(X) = A \cdot \mathcal{N}_{L/K}(Y)$ et qu'il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ de $L$, qui ne sont pas dans $S$, tels que leur produit divise $Y$.*

*Alors, il existe des conjugués $\sigma_1(\mathfrak{p}_1), \ldots, \sigma_k(\mathfrak{p}_k)$ de $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ dont le produit divise $X$.*

*Preuve :* Montrons cela par récurrence sur $k$. Soit $H_k$ la propriété pour $k$ fixé. Pour $k = 0$, il n'y a rien à démontrer.

Pour $k = 1$ : Soit $\mathfrak{p}$ un idéal premier divisant $Y$ et qui n'est pas dans $S$. Alors $\mathcal{N}_{L/K}(\mathfrak{p})$ divise $\mathcal{N}_{L/K}(Y)$ et comme $A$ est $S$-entier, $\mathcal{N}_{L/K}(\mathfrak{p})$ doit aussi diviser $\mathcal{N}_{L/K}(X) = A \cdot \mathcal{N}_{L/K}(Y)$. Mais l'extension est galoisienne, donc il existe nécessairement un conjugué $\sigma(\mathfrak{p})$ de $\mathfrak{p}$ qui divise $X$, et ceci prouve $H_1$.

Supposons maintenant que $H_k$ est vraie pour un certain $k \geqslant 1$. Soit $\prod_{1 \leqslant i \leqslant k+1} \mathfrak{p}_i$ divisant $Y$. On a en particulier $\prod_{1 \leqslant i \leqslant k} \mathfrak{p}_i$ qui divise $Y$, et $H_k$ implique que $\prod_{1 \leqslant i \leqslant k} \sigma_i(\mathfrak{p}_i)$ divise $X$. On peut encore appliquer $H_1$ à l'égalité

$$\mathcal{N}_{L/K}\left(X / \prod_{1 \leqslant i \leqslant k} \sigma_i(\mathfrak{p}_i)\right) = A \cdot \mathcal{N}_{L/K}\left(Y / \prod_{1 \leqslant i \leqslant k} \mathfrak{p}_i\right)$$

et ceci prouve $H_{k+1}$. ■

**Théorème I (Cas Galoisien)** *Si $L/K$ est une extension galoisienne, et si $S_0$ engendre le groupe de classes relatif $Cl_i(L/K)$, alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

$$\text{et } \mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S}.$$

*Preuve :* Soit $S \supset S_0$. Les deux inclusions $\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) \subset (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})$ et $\mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) \subset (\mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S})$ sont évidentes.

Réciproquement, soit $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$ (resp. $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S}$) et $x, y \in \mathbb{Z}_{L,S}$ tels que $\mathcal{N}_{L/K}(\frac{x}{y}) = a$. On peut écrire

$$\mathcal{N}_{L/K}(x) = a\mathcal{N}_{L/K}(y).$$

Soit $\prod \mathfrak{p}_i$ la factorisation en idéaux premiers de l'idéal principal $y\mathbb{Z}_L$. D'après le Lemme III.1.1 il existe des conjugués $\sigma_i(\mathfrak{p}_i)$ des $\mathfrak{p}_i$ tels que $\prod \sigma_i(\mathfrak{p}_i)$ divise l'idéal principal $x\mathbb{Z}_L$. Soit $X$ l'idéal $S$-entier de $L$ tel que

$$x\mathbb{Z}_L = \prod \sigma_i(\mathfrak{p}_i) \cdot X$$

On utilise maintenant le fait que $S_0$ engendre le groupe de classes relatif $Cl_i(L/K)$. Chaque idéal $\mathfrak{p}_i$ est $S_0$-pseudo-principal et peut donc être écrit sous la forme

$$\mathfrak{p}_i = \alpha_i \cdot \mathfrak{s}_i \cdot \mathfrak{q}_i\mathbb{Z}_L$$

où $\alpha_i$ est un élément de $L^*$, $\mathfrak{s}_i$ est un produit d'idéaux de $S$ dans $L$, et $\mathfrak{q}_i$ est un idéal de $K$. En termes de $S$-idéaux, cette relation peut encore s'écrire

$$\mathfrak{p}_i\mathbb{Z}_{L,S} = \alpha_i \cdot \mathfrak{q}_i\mathbb{Z}_{L,S}.$$

Ceci donne

$$y\mathbb{Z}_{L,S} = \prod \alpha_i \prod \mathfrak{q}_i\mathbb{Z}_{L,S}$$

et puisque $\mathfrak{q}_i\mathbb{Z}_L$ est fixé par $\sigma_i$, on a aussi

$$x\mathbb{Z}_{L,S} = \prod \sigma_i(\alpha_i) \prod \mathfrak{q}_i\mathbb{Z}_{L,S} \cdot X$$

Maintenant, si l'on pose

$$u = \left(x/\prod \sigma_i(\alpha_i)\right) / \left(y/\prod \alpha_i\right),$$

on a $\mathcal{N}_{L/K}(u) = a$. Les relations précédentes impliquent que

$$u\mathbb{Z}_{L,S} = \frac{X\prod \mathfrak{q}_i\mathbb{Z}_{L,S}}{\prod \mathfrak{q}_i\mathbb{Z}_{L,S}} = X\mathbb{Z}_{L,S},$$

et donc que $u$ est un $S$-entier. La deuxième égalité du théorème est ainsi démontrée. Pour prouver la première, il suffit de remarquer que si une $S$-unité $a$ est la norme d'un $S$-entier $u$, alors $u$ est une $S$-unité. ■

**Corollaire III.1.2** *Soit $L/K$ une extension galoisienne telle que le groupe de classes $Cl_i(L/K)$ soit trivial, et $a$ un entier de $K$, alors :*

*L'équation $\mathcal{N}_{L/K}(x) = a$ admet une solution rationnelle si et seulement si elle a une solution entière.*

*Plus généralement, si $S$ est un ensemble arbitraire d'idéaux premiers dont les classes engendrent $Cl_i(L/K)$, et si $a$ est un $S$-entier, alors :*

*L'équation $\mathcal{N}_{L/K}(x) = a$ admet une solution rationnelle si et seulement si elle a une solution $S$-entière.*

*Preuve :* C'est une conséquence immédiate du théorème précédent. ■

**Exemple** : On peut illustrer ce corollaire par les exemples suivants : les équations $x^2+y^2 = n$, $x^2+2y^2 = n$, $x^2+xy+y^2 = n$, $x^3+y^3+9z^3-3xy^2-9xz^2-9yz^2+9xyz = n$,...admettent une solution rationelle si et seulement si elles ont une solution entière (ces équations correspondent à des normes pour des extensions galoisiennes de nombre de classes 1). Ceci est encore vrai pour les équations $x^2 - 34y^2 = 9n$, $x^2 + 34y^2 = 25n$,...(qui correspondent à des normes pour des extensions galoisiennes de nombre de classes $> 1$).

### III.1.2 Structure dans le Cas Galoisien

**Notation** : (valable jusqu'à la fin du chapitre) : Si $G$ est le groupe de Galois $\mathrm{Gal}(L/K)$, on note $R$ un ensemble de générateurs de $G$ et on note $r$ son cardinal : $R = \{\sigma_1, \cdots, \sigma_r\}$. Notons $Cl_S(L)^r$ le produit direct de $r$ copies de $Cl_S(L)$.

Montrons tout d'abord deux lemmes sur les idéaux de norme 1 :

**Lemme III.1.3** *Soit $L/K$ une extension galoisienne de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_n\}$. Tout idéal $I$ de $L$ de norme 1 peut s'écrire sous la forme*

$$I = \prod_{i=1}^{n} I_i^{\sigma_i - 1}$$

*Preuve :* À cause de la multiplicativité de la norme et des automorphismes $\sigma_i - 1$, on peut supposer que $I$ est le produit d'idéaux premiers $\mathfrak{p}_i$, tous au-dessus d'un même premier de $K$. Si $I$ est de norme 1, alors $I = \prod \mathfrak{p}_i^{\alpha_i}$ avec $\sum \alpha_i = 0$. On a donc

$$I = \prod \mathfrak{p}_i^{\alpha_i} \cdot \prod \mathfrak{p}_1^{-\alpha_i} = \prod (\mathfrak{p}_i/\mathfrak{p}_1)^{\alpha_i}.$$

Mais l'extension est galoisienne, de sorte que $\mathfrak{p}_i = \sigma_i(\mathfrak{p}_1)$, et donc $I = \prod (\mathfrak{p}_1^{\alpha_i})^{\sigma_i - 1}$. ■

**Lemme III.1.4** *Soit $L/K$ une extension galoisienne de groupe de Galois engendré par $R = \{\sigma_1, \cdots, \sigma_r\}$. Tout idéal $I$ de $L$ de norme 1 peut s'écrire sous la forme*

$$I = \prod_{i=1}^{r} I_i^{\sigma_i - 1}$$

*Preuve :* Grâce au Lemme III.1.3, il suffit de le prouver pour les idéaux de la forme $I^{\sigma-1}$. Soit $\sigma \in G$ que l'on écrit en fonction des générateurs $\sigma = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_k}$, $\sigma_{i_j} \in R$, on a :

$$\begin{aligned} \sigma - 1 &= (\sigma_{i_1}\cdots\sigma_{i_k} - \sigma_{i_2}\cdots\sigma_{i_k}) + (\sigma_{i_2}\cdots\sigma_{i_k} - \sigma_{i_3}\cdots\sigma_{i_k}) + \ldots + (\sigma_{i_k} - 1) \\ &= (\sigma_{i_1} - 1)\alpha_1 + (\sigma_{i_2} - 1)\alpha_2 + \ldots + (\sigma_{i_k} - 1)\alpha_k \\ &= (\sigma_1 - 1)\beta_1 + (\sigma_2 - 1)\beta_2 + \ldots + (\sigma_r - 1)\beta_r. \end{aligned}$$

On peut alors écrire

$$I^{\sigma-1} = \prod_{i=1}^{r} (I^{\beta_i})^{\sigma_i - 1}.$$

■

**Théorème II** *Soit $L/K$ une extension galoisienne. Pour tout $S$, il existe un sous-groupe $Cl_S(L)^{r,0}$ de $Cl_S(L)^r$ et un morphisme surjectif*

$$\phi : Cl_S(L)^{r,0} \to (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

*Preuve : Construction de $\phi$ :* Soit $\psi$ l'application définie de la manière suivante :

$$\begin{array}{rccl} \psi & : & \mathcal{I}_S(L)^r & \to & \mathcal{I}_S(L) \\ & & (I_1, \ldots, I_r) & \mapsto & \displaystyle\prod_{i=1}^{r} \frac{\sigma_i(I_i)}{I_i} = \prod_{i=1}^{r} I_i^{\sigma_i - 1} \end{array}$$

où $\mathcal{I}_S(L)^r$ est le produit de $r$ copies de $\mathcal{I}_S(L)$. Notons $\mathcal{I}_S(L)^{r,0}$ le sous-groupe de $\mathcal{I}_S(L)^r$ dont les éléments ont une image $S$-principale par le morphisme $\psi$. On a donc un morphisme (toujours noté $\psi$) :

$$\begin{array}{rccl} \psi & : & \mathcal{I}_S(L)^{r,0} & \to & \mathcal{P}_S(L) \\ & & (I_1, \ldots, I_r) & \mapsto & \displaystyle\prod_{i=1}^{r} I_i^{\sigma_i - 1} = x\mathbb{Z}_{L,S}. \end{array}$$

Ceci est tel que $\psi(I_1, \ldots, I_r) = x\mathbb{Z}_{L,S}$ est $S$-principal de norme 1. À chaque $x \in L^*$, on peut lui associer sa norme sur $K$. Comme $x$ n'est défini qu'à une $S$-unité près, $\mathcal{N}_{L/K}(x)$ n'est défini qu'à la norme d'une $S$-unité près. Mais l'idéal $x\mathbb{Z}_{L,S}$ est de norme 1, donc $\mathcal{N}_{L/K}(x)$ est une $S$-unité. On a donc défini un morphisme :

$$\overline{\psi} \ : \mathcal{I}_S(L)^{r,0} \to (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

Ce morphisme peut se définir sur le groupe de classes de $L$. En effet, si $I_i$ est principal, disons par exemple $I_i = x_i\mathbb{Z}_{L,S}$, alors $\psi(I_i) = I_i^{\sigma_i - 1} = x_i^{\sigma_i - 1}\mathbb{Z}_{L,S}$, et alors $\overline{\psi}(I_i) = \mathcal{N}_{L/K}(x_i^{\sigma_i - 1}) = 1$. Ainsi, on peut définir $\phi$ comme la restriction de $\overline{\psi}$ au quotient $Cl_S(L)^{r,0}$ :

$$\phi \ : Cl_S(L)^{r,0} \to (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

*Surjectivité de $\phi$ :* Soit $a \in (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})$, et $x$ tel que $a = \mathcal{N}_{L/K}(x)$. Puisque $a \in \mathbb{U}_{K,S}$, on a $\mathcal{N}_{L/K}(x\mathbb{Z}_{L,S}) = a\mathbb{Z}_{K,S} = \mathbb{Z}_{K,S}$. D'après le Lemme III.1.4, on peut exprimer $x\mathbb{Z}_{L,S}$ sous la forme

$$x\mathbb{Z}_{L,S} = \prod_{i=1}^{r} I_i^{\sigma_i - 1}$$

On vérifie alors aisément que $\phi(I_1, \ldots, I_r) = a$. ■

**Corollaire III.1.5** *Pour tout $S$ il existe un sous-groupe $Cl_{i,S}(L/K)^{r,0}$ de $Cl_{i,S}(L/K)^r$ et un morphisme surjectif*

$$\phi \ : Cl_{i,S}(L/K)^{r,0} \to (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

*Preuve :* Puisque $Cl_{i,S}(L/K) = Cl_S(L)/i(Cl_S(K))$, il est suffisant de montrer que le sous-groupe $i(Cl_S(K))$ de $Cl_S(L)$ est contenu dans le noyau du morphisme $\phi$ du Théorème II. Or, si $I$ est un idéal de $K$, alors $I^{\sigma - 1} = 1$ et $\phi(\bar{I}) = \mathcal{N}_{L/K}(1) = 1$. ■

**Remarque** : Ceci prouve non seulement que $i(Cl_S(K))$ est dans le noyau de $\phi$ mais aussi que le sous-groupe plus grand $Cl_S(I^G)$ de $Cl_S(L)$ engendré par les idéaux de $L$ fixés par $G$ est également dans ce noyau.

Si $u$ est une $S$-unité de $K$, alors on a la relation $\mathcal{N}_{L/K}(u) = u^{[L:K]}$, qui montre que le groupe quotient $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$ a un exposant qui divise $[L : K]$. Cette simple remarque montre que dans le Théorème II (ou dans le Corollaire III.1.5), il est suffisant de considérer les $[L : K]$-parties des groupes de classes. Par exemple, on a le corollaire suivant :

**Corollaire III.1.6** *Soit $L/K$ une extension galoisienne, et $S_0$ un ensemble fini d'idéaux premiers de $K$ qui engendre la $[L : K]$-partie du groupe de classes relatif $Cl_i(L/K)$, alors pour tout $S \supset S_0$ on a*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S},$$

*c'est-à-dire que le Théorème Principal est vrai avec ce $S_0$.*

*Preuve :* Pour cela, il suffit de remarquer que le groupe

$$(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

est d'exposant divisant $[L : K]$. ■

**Remarque** : Il n'est pas suffisant de faire l'hypothèse que $[L : K]$ soit premier à $h$ pour prouver comme dans le Théorème I que les entiers qui sont des normes sont des normes d'entiers. Nous illustrons cela par un exemple :

**Exemple** : Soit $L/K = \mathbb{Q}(\sqrt{229})/\mathbb{Q}$. Le groupe $Cl(L)$ est d'ordre 3 (premier à 2), et est engendré par un idéal $\mathfrak{p}$ au-dessus de 3. L'entier 3 est une norme puisque

$$\mathcal{N}_{L/K}(\frac{16 - \sqrt{229}}{3}) = 3.$$

Mais il ne peut pas être la norme d'un entier $x$, sinon cet $x$ engendrerait l'un des deux idéaux au-dessus de 3 qui ne sont pas principaux.

Nous avons vu dans la partie I.2.1 qu'il existe deux notions différentes de groupes de classes relatifs. L'exemple suivant montre que le Corollaire III.1.6 est faux si l'on remplace $Cl_i(L/K)$ par $Cl_{\mathcal{N}}(L/K)$. La notion de groupe de classes relatif adaptée à notre situation est celle liée à l'inclusion et non pas celle liée à la norme.

**Exemple** : Soit $K = \mathbb{Q}(y)$ avec $y^2 - y - 26 = 0$. Le discriminant de $K$ est 105, et son groupe de classes est d'ordre 2, engendré par l'idéal premier $\mathfrak{p}_2 = 2\mathbb{Z}_K + (y + 1)\mathbb{Z}_K$ au-dessus de 2. Considérons l'extension de $K$ définie par $L = K(x)$ avec $x^2 + (-2y + 1)x - 158 = 0$. On a alors $x^4 - 421x^2 + 24964 = 0$. Ce corps $L$ n'est autre que le corps $\mathbb{Q}(\sqrt{105}, \sqrt{737})$, de discriminant $105^2 737^2$. Dans l'extension relative $L/K$, $-1$ est une norme puisque

$$\mathcal{N}_{L/K}\left(\frac{(18808y + 87240)x + (-352680y - 1625419)}{((44y - 330)x + (1124y - 4777))^3}\right) = -1$$

Le groupe de classes $Cl(L)$ est de type $C_6 \times C_2$, engendré par un idéal premier $\mathfrak{P}_2$ au-dessus de $\mathfrak{p}_2$ (au-dessus de 2) d'ordre 6, et un idéal premier $\mathfrak{P}_{59}$ au-dessus de 59 d'ordre 2. On a

$$\mathcal{N}_{L/K}(\mathfrak{P}_2) = \mathfrak{p}_2 \text{ et } \mathcal{N}_{L/K}(\mathfrak{P}_{59}) = (4y - 21)\mathbb{Z}_K,$$

Ainsi, le groupe $Cl_{\mathcal{N}}(L/K) = \mathrm{Ker}(\mathcal{N}_{L/K})$ est d'ordre 6, et son 2-Sylow est engendré par $\mathfrak{P}_{59}$. Si le Corollaire III.1.6 était vrai avec $Cl_{\mathcal{N}}(L/K)$ à la place de $Cl_i(L/K)$, alors $-1$ serait la norme d'une 59-unité. Montrons que ce n'est pas le cas :

Les unités fondamentales de $L$ sont

$$\begin{aligned} u_1 &= 8y + 37 \\ u_2 &= (17952y - 8976)x + 777239 \\ u_3 &= -18636936x + (18636936y + 243656915) \end{aligned}$$

dont les normes sont $(8y + 37)^2$, 1 et 1, où $8y + 37$ est l'unité fondamentale de $K$. Ceci prouve que les unités ont des normes triviales. Les 59-unités supplémentaires sont données par

$$\begin{aligned} s_1 &= 4x + (26y - 221) \\ s_2 &= 230x + (-230y + 3237) \\ s_3 &= 4y - 21 \\ s_4 &= 59 \end{aligned}$$

On remarque que $s_3$ et $s_4$ (ajoutées à $8y+37$) forment un système fondamental de 59-unités de $K$. Pour cette raison, leur contribution aux normes est triviale. Les normes de $s_1$ et $s_2$ sont $(8y+37)^{-1}(4y-21)^2$ et $-59(4y-21)$. Ceci prouve que la seule unité de $K$ qui est une norme non triviale de 59-unité est $(8y + 37)$, et que $-1$ n'est pas la norme d'une 59-unité.

Nous pouvons reformuler cet exemple en un autre langage. L'équation $\mathcal{N}_{L/K}(x) = -1$ équivaut à l'équation

$$a^2 + \sqrt{105}ab - 158b^2 = -1.$$

Cette équation admet une solution dans $\mathbb{Q}(\sqrt{105})$ donnée par exemple par

$$\begin{aligned} a &= \frac{-13389802194\sqrt{105} + 137206113757}{13^3} \\ b &= \frac{1584534586\sqrt{105} - 16236473944}{13^3} \end{aligned}$$

Nous avons montré qu'il n'existe pas de solution entière, ni de solution dont le dénominateur soit une puissance de 59.

### III.1.3 Cas Particulier des Extensions Cycliques

Considérons ici le cas particulier des extensions cycliques. Dans ce cas nous pouvons déterminer explicitement le noyau du morphisme du Théorème II, et donc faire apparaître un isomorphisme. Ce résultat, dû à Chevalley dans [Che], est connu sous le nom de "Formule des Classes Ambiges".

Soit $Cl_S(L)^G$ le sous-groupe de $Cl_S(L)$ des classes fixes par l'action de $G$ (c'est le groupe des classes ambiges), et $Cl_S(\mathcal{I}_S(L)^G)$ le sous-groupe de $Cl_S(L)^G$ engendré par les idéaux qui sont eux-même invariants. Le théorème est le suivant :

**Théorème (des Classes Ambiges)** *Si $G = Gal(L/K)$ est cyclique, alors pour tout $S$, il existe un isomorphisme*

$$\frac{Cl_S(L)^G}{Cl_S(\mathcal{I}_S(L)^G)} \sim \frac{\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}}{\mathcal{N}_{L/K}(\mathbb{U}_{L,S})}.$$

*Preuve :* Partons du morphisme surjectif $\phi$ du Théorème II. Comme $G = Gal(L/K)$ est cyclique, on a $Cl_S(L)^{r,0} = Cl_S(L)^0 = Cl_S(L)^G$.

Soit $I$ un idéal invariant par l'action de $G$, et $\sigma$ un générateur de $G$. On a $I^{\sigma-1} = 1$ et $\phi(\bar{I}) = \mathcal{N}_{L/K}(1) = 1$. Ceci prouve que $Cl_S(\mathcal{I}_S(L)^G)$ est inclus dans le noyau.

Réciproquement, montrons que $Cl_S(\mathcal{I}_S(L)^G)$ est exactement le noyau. Soit $I$ un idéal de $L$, dont la classe est dans $Cl_S(L)^G$ et dans le noyau de $\phi$. On a $I^{\sigma-1} = x\mathbb{Z}_{L,S}$ avec $\mathcal{N}_{L/K}(x) = 1$. Mais le Théorème 90 de Hilbert affirme que $x$ est de la forme $x = \alpha^{1-\sigma}$, où $\alpha$ est un élément non trivial de $L$. Ainsi, on a $(\alpha I)^{\sigma-1} = 1$, ce qui prouve que $\alpha I$ est un idéal fixe par $G$, et ainsi on a $\bar{I} \in Cl_S(\mathcal{I}_S(L)^G)$, comme il fallait le démontrer. ■

Dans ce théorème, le groupe de classes relatif est en fait implicite. En effet, l'inclusion $i(Cl_S(K)) \subset Cl_S(\mathcal{I}_S(L)^G)$ montre que $Cl_S(L)^G/Cl_S(\mathcal{I}_S(L)^G$ peut être vu comme un quotient d'un sous-groupe du groupe de classes relatif $Cl_{i,S}(L/K)$.

**Remarque** : Dans le cas particulier où $S$ engendre le groupe $Cl(L)$ tout entier, le groupe $Cl_S(L)$ est trivial, et l'on a $\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$, comme l'affirme le Théorème Principal. Toutefois, il n'est pas nécessaire d'engendrer le groupe de classes tout entier, mais seulement le sous-groupe $Cl(L)^G$ qui est le groupe des classes ambiges.

## III.2 Équations aux Normes dans les Extensions Non Galoisiennes

Dans cette partie nous considérons le cas général où l'extension $L/K$ n'est plus nécessairement galoisienne.

**Notation** : Nous noterons désormais $\mathfrak{L}/K$ sa clôture galoisienne, et $G$ son groupe de Galois. Le sous-groupe $H$ de $G$ est le sous-groupe de $G$ qui correspond à l'extension $\mathfrak{L}/L$ par la correspondance de Galois. Nous noterons $d = [L : K]$ et $|H| = [\mathfrak{L} : L]$, de sorte que l'on a $|G| = d \cdot |H|$.

### III.2.1 Préliminaires

Avant de prouver le Théorème Principal dans le cas général, nous prouvons une proposition préliminaire qui résout déjà quelques questions. Avec les notations précédentes nous avons :

**Proposition III.2.1** *Si $S$ est un ensemble fini d'idéaux premiers de $K$, alors le groupe*

$$(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

*est d'exposant divisant à la fois $d$ et $|H| \cdot |Cl_{i,S}(\mathfrak{L}/K)|$.*

*Preuve :* Lorsque $a \in K^*$, la relation

$$a^d = \mathcal{N}_{L/K}(a)$$

justifie la première affirmation. Pour la seconde, on pose $h = |Cl_{i,S}(\mathfrak{L}/K)|$. Choisissons $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$. Si l'on écrit $a = \mathcal{N}_{L/K}(x)$ avec $x \in L$, alors

$$a^{|H|} = \mathcal{N}_{L/K}(x^{|H|}) = \mathcal{N}_{\mathfrak{L}/K}(x),$$

et $a^{|H|}$ est une norme pour l'extension galoisienne $\mathfrak{L}/K$. Comme l'affirme le Corollaire III.1.5 pour le cas galoisien, l'exposant du groupe $(\mathcal{N}_{\mathfrak{L}/K}(\mathfrak{L}^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{\mathfrak{L}/K}(\mathbb{U}_{\mathfrak{L},S})$ divise $h$, donc $(a^{|H|})^h$ est la norme d'une $S$-unité $s$ de $\mathbb{U}_{\mathfrak{L},S}$. On a alors

$$a^{|H|h} = \mathcal{N}_{\mathfrak{L}/K}(s) = \mathcal{N}_{L/K}(\mathcal{N}_{\mathfrak{L}/L}(s)),$$

ce qui prouve que $a^{|H|h}$ est la norme d'une $S$-unité pour l'extension $L/K$. ■

**Corollaire III.2.2** *Soit $L/K$ une extension telle que $d$ est premier à $|H|$, et $S_0$ un ensemble fini d'idéaux premiers de $K$. Si $S_0$ est tel que $h = |Cl_{i,S_0}(\mathfrak{L}/K)|$ est premier à $d$, alors pour tout $S \supset S_0$,*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S},$$

*c'est-à-dire que le Théorème Principal est vrai avec ce $S_0$.*

Ce corollaire s'applique par exemple aux extensions galoisiennes (dans ce cas $|H|$=1, et c'est exactement le Corollaire III.1.6). Dans le cas particulier où $d$ est premier, le degré $|H| = [\mathfrak{L} : L]$ doit diviser $(d-1)!$, et donc $d$ et $|H|$ sont toujours premiers entre eux, et l'on peut appliquer le Corollaire III.2.2. Pour les petits degrés ($d \leqslant 5$), les seules extensions qui ne peuvent pas être traitées par ce théorème sont celles dont le groupe de Galois est de type $D_4$ (le groupe diédral d'ordre 8) ou $S_4$ (le groupe complet des permutations de 4 lettres). Nous reviendrons plus tard sur ces deux cas particuliers.

Donnons un exemple qui montre qu'il est nécessaire de considérer le groupe $Cl(\mathfrak{L})$ (et pas seulement le groupe $Cl(L)$).

**Exemple** : Soit $L/K = \mathbb{Q}(x)/\mathbb{Q}$ avec $x^4 - x^3 - 27x^2 + 3x + 149 = 0$. Ce corps est de type $D_4$, et son discriminant est $62525 = 5^2 \cdot 41 \cdot 61$. Son groupe de classes est trivial, alors que le groupe de classes de sa clôture galoisienne $\mathfrak{L}$ est de type $C_4 \times C_2$ engendré par deux premiers au-dessus de 11 (ou de manière équivalente 79,151,181,191...). Toutes les unités de $L$ sont de norme $+1$, et donc $-1$ ne peut pas être la norme d'une unité. Pourtant, on a la relation :

$$\mathcal{N}_{L/K}((x^3 - 2x^2 - 14x + 6)/11) = -1$$

qui prouve que $-1$ est une norme, et plus précisément que c'est la norme d'une 11-unité. On a aussi les relations suivantes :

$$\mathcal{N}_{L/K}((28x^3 + 5x^2 - 341x + 63)/395) = -1$$

$$\mathcal{N}_{L/K}((29x^3 - 102x^2 - 244x + 1156)/151) = -1$$
$$\mathcal{N}_{L/K}((68x^3 - 135x^2 - 971x - 77)/905) = -1$$
$$\mathcal{N}_{L/K}((20x^3 - 32x^2 - 177x + 510)/191) = -1$$

qui prouvent que $-1$ est la norme d'une 79-unité, d'une 151-unité, d'une 181-unité, d'une 191-unité...

### III.2.2 Preuve du Théorème Principal pour les Extensions Non Galoisiennes

Dans le cas où l'extension n'est plus galoisienne, les conditions sur $S_0$ sont plus nombreuses, et la preuve est assez technique et utilise de nombreuses notations. Nous nous inspirons en grande partie d'une démonstration de à H.J. Bartels (dans [Bar]).

En plus des notations précédentes, introduisons-en quelques nouvelles :
**Notations** : Si $C$ est un sous-groupe de $G$, $\mathfrak{L}^C$ est le sous-corps de $\mathfrak{L}$ dont les éléments sont fixes par l'action de $C$ (par exemple $\mathfrak{L}^H = L$). Le groupe $\mathbb{Z}[G/C]$ est le groupe abélien libre engendré par les éléments du quotient $G/C$, $\mathbb{Z}[G/C]^H$ est le sous-groupe de $\mathbb{Z}[G/C]$ dont les éléments sont fixes par $H$ (pour la multiplication à gauche), et $\mathbb{Z}[G/C]^{0,H}$ est le sous-groupe de $\mathbb{Z}[G/C]$ des éléments $\sum \alpha_i \sigma_i C$ fixes par $H$, et tels que $\sum \alpha_i = 0$.

**Lemme III.2.3** *Si $\sum \alpha_i \sigma_i C \in \mathbb{Z}[G/C]^{0,H}$, alors l'application $x \mapsto x^{\Sigma \alpha_i \sigma_i}$ envoit $\mathfrak{L}^C$ dans le noyau de la norme $\mathcal{N}_{L/K}$.*

**Remarque** : Nous noterons ${}^{\mathcal{N}}L^*$ le noyau de la norme $\mathcal{N}_{L/K}$.

*Preuve :* Il est clair que cette application est bien définie sur $\mathfrak{L}^C$, et comme $\sum \alpha_i \sigma_i C$ est fixe par $H$, l'image est nécessairement dans $L^*$. Si $\{t_1, \cdots, t_r\}$ est un système de représentants de $G/H$, on a $\mathcal{N}_{L/K}(x) = x^{\Sigma t_j}$. Dans $\mathbb{Z}[G/C]$, les égalités suivantes sont vérifiées :

$$\begin{aligned} |H| \sum t_j \sum \alpha_i \sigma_i &= \sum_{g \in G} \sum \alpha_i g \sigma_i \\ &= (\sum \alpha_i)(\sum g) \\ &= 0 \end{aligned}$$

et l'on a $\sum t_j \sum \alpha_i \sigma_i C = 0$, c'est-à-dire que $\sum \alpha_i \sigma_i C$ envoit bien $\mathfrak{L}^C$ dans ${}^{\mathcal{N}}L^*$ comme cela était annoncé. ■

On peut énoncer un lemme équivalent pour les idéaux :

**Lemme III.2.4** *Si $\sum \alpha_i \sigma_i C \in \mathbb{Z}[G/C]^{0,H}$, alors l'application $I \mapsto I^{\Sigma \alpha_i \sigma_i}$ envoit les idéaux de $\mathfrak{L}^C$ sur les idéaux de $L$ de norme 1.*

*Preuve :* La preuve est identique à celle du Lemme III.2.3. ■

**Notations** : Dans la proposition suivante, $C$ parcourt tous les sous-groupes cycliques de $G$. Soit $n_C$ le rang du $\mathbb{Z}$-module libre $\mathbb{Z}[G/C]^{0,H}$. Dans ce paragraphe, $ClI(\mathfrak{L}^C)$ est le sous-groupe du groupe de classes de $\mathfrak{L}^C$ engendré par les idéaux premiers qui restent inertes

(donc non ramifiés) dans l'extension $\mathfrak{L}/\mathfrak{L}^C$. Par exemple on a $ClI(\mathfrak{L}) = Cl(\mathfrak{L})$. Le groupe $ClI_S(\mathfrak{L}^C)$ est l'analogue pour les $S$-idéaux, et $ClI_S(\mathfrak{L}^C)^{n_C}$ est le produit direct de $n_C$ copies de $ClI_S(\mathfrak{L}^C)$.

**Proposition III.2.5 (Cas Non-Galoisien)** *Pour tout ensemble fini $S$ contenant les premiers de $K$ qui se ramifient dans $L$, il existe un sous-groupe $\left(\prod_C ClI_S(\mathfrak{L}^C)^{n_C}\right)^0$ du produit $\prod_C ClI_S(\mathfrak{L}^C)^{n_C}$ et une application surjective*

$$\phi_0 \ : \ \left(\prod_C ClI_S(\mathfrak{L}^C)^{n_C}\right)^0 \ \rightarrow \ (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

*Preuve :*

*Construction de $\phi_0$* : Soit $\{\sigma_{C,i}\}_{1 \leqslant i \leqslant n_C}$ une $\mathbb{Z}$-base de $\mathbb{Z}[G/C]^{0,H}$. Nous allons définir $\phi_0$ comme la composée des applications suivantes :

$$(I_{C,i}) \ \mapsto \ \prod (I_{C,i})^{\sigma_{C,i}} = \alpha \mathbb{Z}_{L,S} \ \mapsto \ \mathcal{N}_{L/K}(\alpha)$$

Détaillons un peu ces notations : si $I_{C,i}$ est un idéal de $\mathfrak{L}^C$ (inerte dans l'extension $\mathfrak{L}/\mathfrak{L}^C$), alors le Lemme III.2.4 affirme que $I_{C,i}^{\sigma_{C,i}}$ est de norme 1 sur $L$. La première flèche est le produit portant sur toutes les paires $(C,i)$ de tels idéaux : c'est encore un idéal de $L$ de norme 1 sur $K$. Le sous-groupe $\left(\prod ClI_S(\mathfrak{L}^C)^{n_C}\right)^0$ sur lequel est défini $\phi_0$ est le plus grand sous-groupe dont l'image par cette flèche est $S$-principale dans $L$. On peut donc engendrer chaque image par un élément $\alpha$ de $L$.

Pour la seconde flèche, on voit que l'idéal $\prod (I_{C,i})^{\sigma_{C,i}}$ est de norme 1 sur $K$, ce qui implique que $\mathcal{N}_{L/K}(\alpha)$ est une $S$-unité de $K$, et donc que $\mathcal{N}_{L/K}(\alpha)$ est dans $\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$. Le générateur $\alpha$ n'est défini qu'à une $S$-unité près, mais justement toutes les normes de $S$-unités sont triviales dans le quotient $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$, de sorte que la deuxième flèche est bien définie.

Pour montrer que $\phi_0$ est bien défini, il suffit de vérifier que l'image d'un idéal $I_{C,i}$ est triviale dès que cet idéal est $S$-principal dans $\mathfrak{L}^C$. Or, si $I_{C,i} = \beta \mathbb{Z}_{\mathfrak{L}^C,S}$, alors $I_{C,i}^{\sigma_{C,i}} = \beta^{\sigma_{C,i}} \mathbb{Z}_{L,S}$, et le Lemme III.2.3 implique que $\mathcal{N}_{L/K}(\beta^{\sigma_{C,i}}) = 1$.

*Surjectivité de $\phi_0$* : Soit $a \in (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})$, et $x$ tels que $a = \mathcal{N}_{L/K}(x)$. La construction que nous allons faire revient à factoriser l'idéal principal $x\mathbb{Z}_{L,S}$ en produit d'idéaux premiers $\mathfrak{P}_k$, ces idéaux premiers pouvant être dans des corps $\mathfrak{L}^C$ différents. Soit $p$ un idéal de $K$ et $p \notin S$. Choisissons un idéal premier $\mathfrak{P}$ de $\mathfrak{L}$ au-dessus de $p$ dans $K$. Soit $C$ son groupe de décomposition. Puisque $p$ n'est pas dans $S$, alors $p$ est non ramifié, et $C$ est cyclique. Soient $\mathfrak{P}_k$ les conjugués de $\mathfrak{P}$, et $\sigma_k$ un système de représentants de $G/C$ indicés de telle manière que $\sigma_k(\mathfrak{P}) = \mathfrak{P}_k$. Les idéaux $\mathfrak{P}_k$ peuvent être vu à la fois comme idéaux de $\mathfrak{L}$, ou comme idéaux de $\mathfrak{L}^C$, ces deux interprétations étant en bijection.

L'élément

$$\tau = \sum v_{\mathfrak{P}_k}(x)\sigma_k,$$

où $v_{\mathfrak{P}}(x)$ est la valuation de $x$ en $\mathfrak{P}$, est dans $\mathbb{Z}[G/C]$. Le fait que $x$ soit dans $L$ implique que $\tau \in \mathbb{Z}[G/C]^H$. De plus, $a$ est une $S$-unité, alors $\mathcal{N}_{L/K}(x\mathbb{Z}_{L,S}) = a\mathbb{Z}_{K,S} = 1$, et donc

$$\tau \in \mathbb{Z}[G/C]^{0,H}.$$

On peut exprimer $\tau$ sur la base $\sigma_{C,i}$ de $\mathbb{Z}[G/C]^{0,H}$ : $\tau = \sum \alpha_i \sigma_i$ et on construit le $n_C$-uplet $(I_{C,i}) = (\mathfrak{P}^{\alpha_i})$.

Si on construit ainsi tous les $\tau_p$ et $(I_{C,i})_p$ pour tous les premiers $p$ de $K$ qui ne sont pas dans $S$, on peut les multiplier entre eux (seul un nombre fini de $\tau_p$ sont non nuls), et l'image par $\phi_0$ de ce produit est exactement $a$. Pour s'assurer de cela, remarquons que l'on a

$$\begin{aligned} v_{\mathfrak{P}}(\prod (I_{C,i})^{\sigma_{C,i}}) &= v_{\mathfrak{P}}((I_{C,i})_p^{\tau_p}) \\ &= v_{\mathfrak{P}}(x) \end{aligned}$$

pour tout $\mathfrak{P}$, et donc $\prod (I_{C,i})^{\sigma_{C,i}} = x\mathbb{Z}_{L,S}$, de sorte que $a$ est dans l'image de $\phi_0$. ■

**Notation** : Les notations restent identiques, et maintenant $D$ parcourt l'ensemble des sous-groupes cycliques de $G$ d'ordre $p^\alpha$ où $p \mid (d, |H|h)$, avec comme d'habitude $d = [L : K]$, $|H| = [\mathfrak{L} : L]$ et $h = |Cl_{i,S}(\mathfrak{L}/K)|$.

**Théorème III (Cas Non Galoisien)** *Pour tout ensemble fini $S$ contenant les premiers de $K$ ramifiés dans $L$, il existe un sous-groupe $\left(\prod_D ClI_S(\mathfrak{L}^D)^{n_D}\right)^0$ du produit $\prod_D ClI_S(\mathfrak{L}^D)^{n_D}$ et un morphisme surjectif*

$$\phi \; : \; \left(\prod_D ClI_S(\mathfrak{L}^D)^{n_D}\right)^0 \; \to \; (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

*Preuve :* La définition de $\phi$ est la même que la définition de $\phi_0$ dans la Proposition III.2.5, sauf que l'on se restreint à un ensemble de départ plus petit. Il suffit donc de prouver que $\phi$ est surjectif. Nous allons montrer que $\mathrm{Im}\,\phi \supset \mathrm{Im}\,\phi_0$ et la conclusion viendra de la surjectivité de $\phi_0$.

Pour chaque sous-groupe cyclique $C$ de $G$, on définit deux entiers $a(C)$ et $b(C)$ premiers entre eux, tels que $|C| = ab$ et tels que $(p \mid (d, |H|h)$ et $p \mid |C|) \Leftrightarrow p \mid b$. Puisque $C$ est cyclique, on peut trouver deux sous-groupes cycliques $A$ et $B$ de $C$, d'ordre exactement $a$ et $b$, tels que $C = A \cdot B$. Nous considérerons la quantité $\pi_a = \prod_C a(C)$, qui est certainement première à $(d, |H|h)$.

Soit $((\bar{I}_{C,i})) \in \left(\prod_C ClI_S(\mathfrak{L}^C)^{n_C}\right)^0$, avec $I_{C,i}$ inerte (non ramifié) dans $\mathfrak{L}/\mathfrak{L}^C$. On a $\prod {I_{C,i}}^{\sigma_{C,i}} = x\mathbb{Z}_{L,S}$. Considérons maintenant l'idéal principal $x^{\pi_a}\mathbb{Z}_{L,S}$. Il se factorise sous la forme

$$x^{\pi_a}\mathbb{Z}_{L,S} = \prod (I_{C,i})^{\pi_a \sigma_{C,i}}$$

Puisque $I_{C,i}$ est fixe par $C$, il est aussi fixé par $B \subset C$. On obtient alors

$$I_{C,i}^{\pi_a \sigma_{C,i}} = I_{C,i}^{\tau_{C,i}}$$

avec $\tau_{C,i} = \frac{\pi_a}{a} \cdot \sigma_{C,i} \cdot \sum_{\alpha \in A} \alpha$ et $\tau_{C,i} \in \mathbb{Z}[G/B]^{0,H}$. Une fois de plus, la factorisation en puissances d'idéaux premiers $b = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$ implique que $B = D_1 \cdots D_k$ avec $|D_l| = p_l^{\varepsilon_l}$. Notons $D_l'$ le produit $\prod_{i \neq l} D_i$ et $\delta_l' = |B|/p_l^{\varepsilon_l}$ son ordre. Comme les $p_l$ sont premiers entre eux, les $\delta_l'$ sont aussi premiers entre eux, et l'on peut trouver des entiers $\gamma_l$ tels que $\sum \gamma_l \delta_l' = 1$. On écrit alors

$$\begin{aligned} I_{C,i}^{\tau_{C,i}} &= I_{C,i}^{\sum \gamma_l \delta_l' \tau_{C,i}} \\ &= \prod_l (I_{C,i}^{\gamma_l})^{\tau_{C,i} \sum_{d' \in D_l'} d'} \end{aligned}$$

On peut remarquer que $I_{C,i}^{\gamma_l}$ est fixe par $D_l \subset B \subset C$ et que $\tau_{C,i} \sum_{d' \in D_l'} d' \in \mathbb{Z}[G/D_l]^{0,H}$. En l'écrivant sur la base $\sigma_{D_l,j}$ de $\mathbb{Z}[G/D_l]^{0,H}$ sous la forme $\tau_{C,i} = \sum \alpha_{D_l,j} \sigma_{D_l,j}$, on construit l'idéal $J_{D_l,j} = I_{C,i}^{\alpha_{D_l,j}}$. En multipliant tous les $J_{D_l,j}$ composante par composante, on obtient un élément $(J)$ de $\left(\prod_D ClI_S(\mathfrak{L}^D)^{n_D}\right)^0$ dont l'image par $\phi$ est

$$\phi((J)) = \phi_0((I^{\pi_a})) = \mathcal{N}_{L/K}(x^{\pi_a}).$$

On peut conclure en se rappelant que $\pi_a$ est premier à $(d, |H|h)$, donc qu'il existe un entier $\pi'$ tel que $\pi_a \pi' = 1 \mod (d, |H|h)$, et la Proposition III.2.1 affirme que

$$\phi((J^{\pi'})) = \phi_0((I^{\pi_a \pi'})) = \phi_0((I)).$$

Ceci prouve que $\operatorname{Im}\phi \supset \operatorname{Im}\phi_0$, et comme $\phi_0$ est surjective, $\phi$ est également surjective. ■

**Remarque** : Comme il est probablement plus habituel de considérer les groupes $Cl_S(\mathfrak{L}^D)$ plutôt que les groupes $ClI_S(\mathfrak{L}^D)$, il faut étendre le morphisme $\phi$ à $\left(\prod Cl_S(\mathfrak{L}^D)^{n_D}\right)^0$, ce qui se fait de manière naturelle. Comme dans le cas galoisien, il est facile de montrer qu'un idéal fixe par $G$ a une image triviale par $\phi$, c'est-à-dire $i(Cl_S(K)) \subset Cl_S(\mathcal{I}(\mathfrak{L}^D)^G) \subset \operatorname{Ker}(\phi)$. On peut en déduire immédiatement le corollaire suivant :

**Corollaire III.2.6** *Pour tout ensemble fini $S$ contenant les premiers de $K$ ramifiés dans $L$, il existe un sous-groupe $\left(\prod Cl_{i,S}(\mathfrak{L}^D/K)^{n_D}\right)^0$ du produit $\prod Cl_{i,S}(\mathfrak{L}^D/K)^{n_D}$ et un morphisme surjectif*

$$\phi \ : \ \left(\prod_D Cl_{i,S}(\mathfrak{L}^D/K)^{n_D}\right)^0 \ \rightarrow \ (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

**Corollaire III.2.7** *Soit $S_0$ un ensemble fini d'idéaux premiers de $K$ contenant les premiers ramifiés de $L/K$. Si $h = |Cl_{i,S_0}(\mathfrak{L}/K)|$ est premier à $d$, et si pour tout sous-groupe cyclique $D$ de $G = Gal(L/K)$ d'ordre $p^\alpha$ avec $p \mid (d, |H|)$ le groupe de classes $Cl_{i,S_0}(\mathfrak{L}^D/K)$ est d'ordre premier à $(d, |H|)$, alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S},$$

*c'est-à-dire que le Théorème Principal est vrai avec ce $S_0$.*

Pour rendre le Théorème III plus précis, il est nécessaire de connaitre la structure de tous les groupes $\mathbb{Z}[G/C]^{0,H}$ (par exemple leur rang comme $\mathbb{Z}$-modules). Dans [Bar], Bartels prouve quelques résultats dans cette direction. Nous ne gardons ici qu'un seul critère, qui permet de montrer que le morphisme $\phi$ est trivial sur certains groupes de classes.

**Proposition III.2.8** *Soit $S$ un ensemble fini d'idéaux premiers de $K$ contenant les premiers ramifiés de $L/K$, et tel que $h = |Cl_{i,S}(\mathfrak{L}/K)|$ soit premier à $(d, |H|)$. Si $C$ est un sous-groupe cyclique de $G$ tel que $H \cap \sigma C \sigma^{-1} = 1$ pour tout $\sigma \in G$, alors $\phi$ est trivial sur $ClI_S(\mathfrak{L}^C)$.*

*Preuve :* Soit $\{g_i\}$ un système de représentants de $G/C$. Si deux éléments $h \in H$ et $c \in C$ sont tels que $hg_i = g_i c$ pour un certain $g_i$, alors $h = g_i c g_i^{-1}$, mais l'hypothèse implique que $h = c = 1$. Ceci signifie que l'on peut choisir $\{g_i\}$ et $F$ tels que $\{g_i\}$ soit égal à $H \cdot F$, et ceci implique en particulier que

$$|F| = \frac{|G|}{|C||H|},$$

donc que le produit $|C||H|$ divise $|G|$.

Soit $\tau \in \mathbb{Z}[G/C]^{0,H} = \sum \alpha_i g_i = \sum \alpha_{i,j} h_i f_j$. Comme $\tau$ est invariant par multiplication à gauche par $H$, $\alpha_{i,j}$ ne dépend que de $j$, et l'on a :

$$\tau = \left( \sum_H h \right) \left( \sum \alpha_j f_j \right).$$

De plus, on a $\sum \alpha_{i,j} = 0 = |H| \sum \alpha_j$, d'où

$$\tau = \left( \sum_H h \right) \left( \sum \alpha_j (f_j - 1) \right).$$

Soit maintenant $I$ un idéal premier de $\mathfrak{L}^C$ inerte dans $\mathfrak{L}/\mathfrak{L}^C$ et non ramifié dans $\mathfrak{L}/K$ (comme précédemment $I$ peut être vu aussi bien comme un idéal de $\mathfrak{L}$ que comme un idéal de $\mathfrak{L}^C$). L'idéal $I^h$ est $S$-pseudo-principal dans $\mathfrak{L}$, donc on peut trouver $x \in \mathfrak{L}$ et un idéal $I_K$ de $K$ tels que $I^h = x I_K \mathbb{Z}_{\mathfrak{L},S}$. Comme $I_K^\tau = 1$ on a

$$I^{h\tau} = \mathcal{N}_{\mathfrak{L}/L}((x\mathbb{Z}_{\mathfrak{L},S})^{\sum \alpha_j (f_j - 1)}) = \mathcal{N}_{\mathfrak{L}/L}(x^{\sum \alpha_j (f_j - 1)}) \mathbb{Z}_{L,S},$$

et

$$\phi(I^h) = \mathcal{N}_{L/K}(\mathcal{N}_{\mathfrak{L}/L}(x^{\sum \alpha_j (f_j - 1)})) = 1.$$

Mais $\phi(I^h) = \phi(I)^h$, et $h$ est premier à $(d, |H|)$, donc $a \mapsto a^h$ est un automorphisme de $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$, et donc $\phi(I) = 1$. ■

Donnons immédiatement deux corollaires de cette proposition.

**Corollaire III.2.9 (Extensions type $D_4$)** *Soit $L/K$ une extension de degré 4 de type $D_4$. Si $S_0$ contient tous les premiers ramifiés de $L/K$ et si $S_0$ est tel que $Cl_{i,S_0}(\mathfrak{L}/K)$ et $Cl_{i,S_0}(L/K)$ sont d'ordre impair, alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

*c'est-à-dire que le Théorème Principal est vrai avec ce $S_0$.*

*Preuve :* Dans le cas présent, le groupe $G = \mathrm{Gal}(\mathfrak{L}/K)$ est isomorphe au groupe $D_4$. On peut écrire $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ avec la relation $\tau\sigma\tau^{-1} = \sigma^3$. Le groupe $H = \mathrm{Gal}(\mathfrak{L}/L)$ peut être choisi égal à $\{1, \tau\}$. À conjugaison près, tous les sous-groupes cycliques de $G$ sont $H = \{1, \tau\}$, $C_1 = \{1, \tau\sigma^2\}$, $C_2 = \{1, \sigma^2\}$ et $C_4 = \{1, \sigma, \sigma^2, \sigma^3\}$. Dans cette liste, seul $H$ a une intersection non triviale avec $H$ (ou son conjugué). Le résultat suit directement grâce au Corollaire III.2.6 et à la Proposition III.2.8. ■

**Corollaire III.2.10 (Extensions de type $S_4$)** *Soit $L/K$ une extension de degré 4 de type $S_4$. Soit $\mathfrak{L}^{C_2}$ le sous-corps cyclique de $\mathfrak{L}$ d'indice 2 et contenant $L$. Si $S_0$ contient tous les premiers ramifiés de $L/K$ et si $S_0$ est tel que $Cl_{i,S_0}(\mathfrak{L}/K)$ et $Cl_{i,S_0}(\mathfrak{L}^{C_2}/K)$ sont d'ordre impair, alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

*c'est-à-dire que le Théorème Principal est vrai avec ce $S_0$.*

*Preuve :* Commençons par faire une remarque sur la définition de $\mathfrak{L}^{C_2}$. Il n'existe pas qu'un seul sous-corps d'indice 2 de $\mathfrak{L}$ contenant $L$, mais en fait trois. En effet, $\mathfrak{L}/L$ est une extension galoisienne d'ordre 6, de type $S_3$, et $S_3$ contient trois sous-groupes d'ordre 2. Mais ces trois sous-groupes sont conjugués, et donc les trois corps correspondants sont isomorphes. Cet isomorphisme nous permet donc de faire cet abus de notation. En particulier, leurs trois groupes de classes sont engendrés par les mêmes idéaux.

Le groupe $G$ est le groupe des permutations de quatre lettres $a, b, c$ et $d$. Le groupe $H = \mathrm{Gal}(\mathfrak{L}/L)$ est isomorphe au groupe $S_3$, et on peut décider de le représenter par les permutations des trois lettres $a, b$ et $c$. Les 2-sous-groupes de $S_4$ sont d'ordre 1,2 ou 4. Examinons successivement ces différentes possibilités.

Si $C$ est un sous-groupe cyclique d'ordre 2, alors il est conjugué soit à $C_1 = \{1, (ab)(cd)\}$ soit à $C_2 = \{1, (ab)\}$. Si $C$ est conjugué à $C_2$, alors le sous-corps de $\mathfrak{L}$ correspondant est $\mathfrak{L}^{C_2}$, et l'hypothèse faite sur $S_0$ rend $\phi$ trivial sur le groupe de classes correspondant. Si $C$ est conjugué à $C_1$, alors il ne peut pas intersecter $H$, car deux permutations de type $(ab)$ et $(ab)(cd)$ ne sont jamais conjuguées. La Proposition III.2.8 montre alors que $\phi$ est trivial sur le groupe de classes de $\mathfrak{L}^C$.

Si $C$ est un sous-groupe cyclique d'ordre 4, alors $C$ est conjugué à $C_4 = \{1, (acbd), (ab)(cd), (adbc)\}$. Or, tous les conjugués de $C$ rencontrent $H$ trivialement. Comme dans le cas précédent, la Proposition III.2.8 montre que $\phi$ est trivial sur le groupe de classes de $\mathfrak{L}^C$.

On a donc montré que le morphisme surjectif du Corollaire III.2.6 est trivial, ce qui implique que

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

■

Donnons maintenant un exemple qui montre la nécessité de la condition sur les premiers ramifiés :

**Exemple** : Soit $L/K = \mathbb{Q}(x)/\mathbb{Q}$ avec $x^4 - x^3 - 8x^2 + 9x + 3 = 0$. Ce corps de discriminant $25857 = 3^2 \cdot 13^2 \cdot 17$ est de type $D_4$ (groupe diédral d'ordre 8), et son groupe de classes est trivial. Sa clôture galoisienne a également un groupe de classes trivial. Les unités fondamentales sont de norme $+1$. Si l'on oublie la condition sur les premiers ramifiés dans le Corollaire III.2.9, ceci devrait impliquer que l'équation $\mathcal{N}_{L/K}(x) = -1$ n'a pas de solution. Toutefois, on trouve que

$$\mathcal{N}_{L/K}((x^3 + 2x^2 - 8x + 3)/6) = -1.$$

Cette solution se factorise sous la forme $\mathfrak{p}_1\mathfrak{p}_2^{-1}$ avec $\mathfrak{p}_1^2\mathfrak{p}_2^2 = 3$, et donc c'est une 3-unité. Le nombre premier 3 est ramifié puisqu'il divise le discriminant du corps $L$.

On remarque dans cet exemple qu'il ne suffit pas de considérer le discriminant de $\mathfrak{L}/L$ (c'est-à-dire les premiers qui se ramifient dans l'extension relative $\mathfrak{L}/L$), mais réellement le discriminant de $L/K$ ou de manière équivalente le discriminant de $\mathfrak{L}/K$ (c'est-à-dire les premiers qui se ramifient dans l'extension $L/K$). En effet, seuls les premiers au-dessus de 17 se ramifient dans l'extension $\mathfrak{L}/L$, alors que 3,13 et 17 se ramifient dans $L/K$.

### III.2.3 Cas Particulier des Extensions de $\mathbb{Q}$

Dans le Théorème Principal, et dans la plupart des autres propositions, nous affirmons l'existence d'un certain ensemble $S_0$ tel que les groupes $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0})$ et $\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S_0}$ sont égaux, et tel que cette égalité reste vraie pour tous les $S$ contenant $S_0$. Il existe des cas où l'égalité est vraie pour un certain $S_0$ mais pas pour un $S$ contenant ce $S_0$. Nous donnons ici une condition suffisante pour que l'égalité reste vraie, et nous donnons un exemple où ceci est faux.

Cette condition nous permettra de considérer les cas particuliers des extensions de $\mathbb{Q}$ de degrés impairs, ou encore de degrés pairs totalement complexes, car dans ces deux cas les unités qui sont des normes sont particulièrement simples à décrire.

**Proposition III.2.11** *Si $Cl_{S_0}(L)$ est d'ordre $h$ premier à $d = [L : K]$ et si $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S_0}$ alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

*Preuve :* Soit $S \supset S_0$ satisfaisant les conditions de la proposition, et $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$. Choisissons un élément $x$ de $L^*$ tel que $a = \mathcal{N}_{L/K}(x)$, où $x$ n'est pas nécessairement une $S$-unité. Factorisons l'idéal principal $x\mathbb{Z}_L$ dans $L$ :

$$x\mathbb{Z}_L = \left(\prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{\alpha_i}\right)\left(\prod_{\mathfrak{p}_i \notin S} \mathfrak{p}_i^{\alpha_i}\right) = I_S \cdot I_{\hat{S}}$$

La définition de $h$ rend les idéaux $(I_S)^h$ et $(I_{\hat{S}})^h$ $S_0$-principaux. On a alors $(I_S)^h = x_S\mathbb{Z}_{L,S_0}$ où $x_S$ est une $S$-unité, et $(I_{\hat{S}})^h = x_{\hat{S}}\mathbb{Z}_{L,S_0}$, tels que

$$x^h = x_S \cdot x_{\hat{S}}.$$

Mais on a aussi $\mathcal{N}_{L/K}((I_S)^h) = a^h\mathbb{Z}_{K,S_0}$ et $\mathcal{N}_{L/K}((I_{\hat{S}})^h) = 1$, donc $v = \mathcal{N}_{L/K}(x_{\hat{S}})$ est une $S_0$-unité. Cet élément $v$ est à la fois une norme et une $S_0$-unité, et l'hypothèse sur $S_0$ force $v$ à être la norme d'une $S_0$-unité, disons $v = \mathcal{N}_{L/K}(y)$. On a les relations suivantes :

$$a^h = \mathcal{N}_{L/K}(x^h) = \mathcal{N}_{L/K}(x_S \cdot x_{\hat{S}}) = \mathcal{N}_{L/K}(x_S \cdot y),$$

qui prouvent que $a^h$ est la norme d'une $S$-unité. Enfin, on a aussi la relation

$$a^d = \mathcal{N}_{L/K}(a),$$

et comme $h$ et $d$ sont premiers entre eux, on conclut que $a$ est la norme d'une $S$-unité. ■

**Corollaire III.2.12** *Soit $L/\mathbb{Q}$ une extension de degré impair $d$. Si l'ordre $h$ de $Cl(L)$ est premier à $d$, alors pout tout $S$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

*Preuve :* Dans ce cas particulier, on prend $S_0 = \varnothing$ et $\mathbb{U}_{\mathbb{Q}} = \{\pm 1\} = \mathcal{N}_{L/\mathbb{Q}}(\mathbb{U}_L)$ car $\mathcal{N}_{L/\mathbb{Q}}(-1) = -1$. On peut appliquer la Proposition III.2.11 avec $S_0 = \varnothing \subset S$. ■

**Corollaire III.2.13** *Soit $L/\mathbb{Q}$ une extension totalement complexe de degré pair $d$. Si $Cl(L)$ est d'ordre $h$ premier à $d$, alors pour tout $S$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

*Preuve :* Dans ce cas particulier, $-1$ ne peut pas être une norme car toutes les normes doivent être positives. Ainsi, on a $\mathcal{N}_{L/\mathbb{Q}}(\mathbb{U}_L) = \mathcal{N}_{L/\mathbb{Q}}(L^*) \cap \mathbb{U}_{\mathbb{Q}} = \{1\}$. On peut alors appliquer la Proposition III.2.11 avec $S_0 = \varnothing \subset S$. ■

Donnons maintenant un exemple pour lequel l'égalité est vraie pour $S_0 = \varnothing$, mais ne l'est plus pour un certain $S$ plus grand :
**Exemple** : Soit $L/K = \mathbb{Q}(x)/\mathbb{Q}$, avec $x^3 - x^2 - 41x + 93 = 0$. Cette extension totalement réelle de degré 3 est de discriminant $28212 = 2^2 \cdot 3 \cdot 2351$ et son groupe de Galois est $S_3$ (donc ce n'est pas une extension galoisienne). Pour être précis, il y a trois corps de nombres ayant ces propriétés, et curieusement le même phénomène arrive dans les deux autres corps cubiques de discriminant 28212, avec toutefois des valeurs numériques différentes. Il est clair que $\mathcal{N}_{L/\mathbb{Q}}(\mathbb{U}_L) = \mathbb{U}_{\mathbb{Q}}$. Considérons maintenant $S = \{3\}$. On a

$$\mathcal{N}_{L/\mathbb{Q}}((-3x^2 + 7x + 31)/31) = 3.$$

Ceci prouve que 3 est une norme. Remarquons qu'il y a 31 au dénominateur, et que notre solution n'est pas une 3-unité. Montrons qu'il n'y a pas de 3-unité de norme 3. Supposons

au contraire que 3 est la norme d'une 3-unité $s$. On a $3\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2$ avec $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{p}_1) = 3\mathbb{Z}$ et $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{p}_2) = 3\mathbb{Z}$, on peut donc écrire

$$s\mathbb{Z}_L = \mathfrak{p}_1^{v_1}\mathfrak{p}_2^{v_2}$$

avec $v_1 + v_2 = 1$. Mais le groupe de classes de $L$ est cyclique d'ordre 3 engendré par $\mathfrak{p}_1$, et la principalité de l'idéal $s\mathbb{Z}_L$ implique la relation $v_1 + v_2 \equiv 0 \mod 3$. Ces deux relations ne peuvent pas être satisfaites en même temps, ce qui prouve que 3 ne peut pas être la norme d'une 3-unité.

### III.2.4 Existence de Solutions Entières

Dans ce paragraphe, nous voulons trouver des solutions entières $x$ lorsque le paramètre $a$ est lui-même un entier algébrique. Nous allons chercher à généraliser le Théorème I pour les entiers et les $S$-entiers.

**Remarque** : Si l'on veut que les entiers qui sont des normes soient des normes d'entiers, il faut que cela soit déjà vrai pour les unités. Pour cela, il est nécessaire de supposer que l'on a déjà l'égalité des groupes $\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$ et $\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$. Celle-ci peut être obtenue par exemple grâce aux Corollaires III.2.2 ou III.2.7.

Il est également nécessaire que les idéaux entiers qui sont des normes soient des normes d'idéaux entiers. Cette dernière condition est plus faible que celle pour les nombres entiers algébriques, et fait l'objet du lemme suivant :

**Lemme III.2.14** *Soit $L/K$ une extension (non nécessairement galoisienne) de degré 3,4 ou 6, $I_K$ un idéal de $K$ et $I_K = \prod \mathfrak{p}^{\alpha_\mathfrak{p}}$ sa décomposition en idéaux premiers dans $K$. Supposons que $I_K$ est la norme d'un idéal $I_L$ de $L$, alors pour tout idéal premier $\mathfrak{p}$ de $K$ il existe un idéal premier $\mathfrak{P}$ de $L$ au-dessus de $\mathfrak{p}$ dont l'indice résiduel $f_{\mathfrak{P}/\mathfrak{p}}$ divise $\alpha_\mathfrak{p}$.*

*Preuve :* Soit $I_L = \prod \mathfrak{P}^{\beta_\mathfrak{P}}$ la factorisation en idéaux premiers de $I_L$. On a

$$\sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}\beta_\mathfrak{P} = \alpha_\mathfrak{p},$$

donc $\alpha_\mathfrak{p}$ est un multiple du *pgcd* des $f_{\mathfrak{P}/\mathfrak{p}}$. Mais si l'on écrit la relation $[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}$, celle-ci doit être l'une des partitions suivantes :

$$3 = 1 + 1 + 1 = 1 + 2 = 3,$$

$$4 = 1 + 1 + 1 + 1 = 1 + 1 + 2 = 1 + 3 = 2 + 2 = 4,$$

$$6 = 1 + 1 + 1 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 2 = 1 + 1 + 1 + 3 = 1 + 1 + 2 + 2$$

$$6 = 1 + 1 + 4 = 1 + 2 + 3 = 2 + 2 + 2 = 1 + 5 = 2 + 4 = 3 + 3 = 6.$$

Dans chacun des cas, le *pgcd* des termes est toujours égal à l'un des termes, ce qui implique qu'au moins l'un des $f_{\mathfrak{P}/\mathfrak{p}}$ divise $\alpha_\mathfrak{p}$. ■

**Théorème IV** *Soit $L/K$ une extension (non nécessairement galoisienne) de degré 3,4 ou 6 et $S_0$ satisfaisant $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S_0}$ . Si $S_0$ engendre aussi le groupe $Cl(L)$, alors pour tout $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S}.$$

*Preuve :* Remarquons d'abord que la Proposition III.2.11 implique que

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

L'inclusion directe $\mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) \subset (\mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S})$ est triviale. Montrons l'inclusion réciproque. Soit $a \in (\mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S})$, et $a = \mathcal{N}_{L/K}(x)$. Factorisons l'idéal principal $a\mathbb{Z}_{L,S}$ dans $L$ :

$$a\mathbb{Z}_{L,S} = \prod \mathfrak{p}^{\alpha_\mathfrak{p}}$$

Le Lemme III.2.14 nous permet de constuire un idéal entier

$$I_L = \prod \mathfrak{P}^{\alpha_\mathfrak{p}/f_{\mathfrak{P}/\mathfrak{p}}}$$

de norme $a\mathbb{Z}_{K,S}$. Mais le groupe de classes $Cl_S(L)$ est trivial, donc l'idéal $I_L$ doit être $S$-principal, et on peut trouver un $S$-entier $z$ de $L$ qui engendre $I_L$. Ainsi, il existe une $S$-unité $u$ de $K$ telle que

$$\mathcal{N}_{L/K}(z) = a \cdot u.$$

On a aussi la relation $a = \mathcal{N}_{L/K}(x)$, qui montre que $u$ est une norme. Comme on l'a remarqué au début de cette preuve, une $S$-unité qui est une norme est une norme de $S$-unité, on peut donc écrire $u = \mathcal{N}_{L/K}(w)$. Finalement on a

$$\mathcal{N}_{L/K}(z \cdot w^{-1}) = a$$

où $z \cdot w^{-1}$ est un $S$-entier. ■

**Remarque** : Quand le degré est différent de 3, 4 ou 6, alors le Lemme III.2.14 ne s'applique plus. En degré 5, on peut regarder l'exemple suivant :

**Exemple** : Soit $L/K = \mathbb{Q}(x)/\mathbb{Q}$ avec $x^5 + 3x - 2 = 0$. L'entier 7 est une norme puisque

$$\mathcal{N}_{L/K}((90x^4 + 8x^3 + 34x^2 + 24x + 281)/7) = 7.$$

Le premier 7 se décompose en deux idéaux premiers $\mathfrak{P}_1$ et $\mathfrak{P}_2$ d'indices résiduels 3 et 2. Si 7 était la norme d'un entier $z$, alors $z$ aurait des valuations $v_1$ et $v_2$ en $\mathfrak{P}_1$ et $\mathfrak{P}_2$, avec la relation impliquée par la norme $3v_1 + 2v_2 = 1$, qui impose que $v_1$ ou $v_2$ est négatif, et donc que $z$ ne peut pas être entier.

On peut remarquer qu'il existe une infinité de premiers qui possèdent cette même propriété, et donc qu'il n'existe aucun ensemble fini $S$ satisfaisant le Théorème IV dans ce cas.

Il existe un grand nombre d'extensions de degrés différents de 3, 4 ou 6 qui satisfont le Lemme III.2.14. C'est certainement le cas pour toutes les extensions galoisiennes, mais aussi pour les extensions de type $D_p$ (groupe diédral d'ordre $2p$ avec $p$ premier). Il serait intéressant de donner une caractérisation de ces extensions, peut-être en fonction des valeurs relatives de $d = [L : K]$ et $|H| = [\mathfrak{L} : L]$.

## III.3 Équations aux Normes : l'Algorithme

L'algorithme que nous décrivons maintenant a été implanté sur le système de théorie des nombres PARI, qui est développé à Bordeaux. Ce système contient déjà un grand nombre d'algorithmes que nous utilisons. Par exemple, nous supposons que les corps $K$ et $L$ sont complètement connus, c'est-à-dire que nous avons leurs discriminants, bases d'entiers, groupes de classes, unités fondamentales et les logarithmes discrets correspondants (pour une description de ces algorithmes voir [Coh]).

Les paragraphes précédents donnent des conditions sur $S$ qui assurent que toutes les $S$-unités qui sont des normes sont des normes de $S$-unités. La stratégie générale de notre algorithme pour trouver une solution à l'équation $\mathcal{N}_{L/K}(x) = a$ est de dire que $a$ est une $S$-unité pour un ensemble $S$ bien choisi, puis de chercher une $S$-unité dont c'est la norme. Le reste de l'algorithme consiste à utiliser le logarithme discret sur les $S$-unités, et à faire un peu d'algèbre linéaire sur $\mathbb{Z}$.

L'algorithme peut se décrire brièvement de la manière suivante :

**Algorithme III.3.1** (*Recherche d'une solution à l'équation $\mathcal{N}_{L/K}(x) = a$ dans $L$*).
*Données : $K, L$ et $a \in K^*$.*
*1– Déterminer l'ensemble $S$ avec l'Algorithme III.3.4.*
*2– Trouver une $S$-unité $x$ telle que $\mathcal{N}_{L/K}(x) = a$ avec l'Algorithme III.3.5.*
*Résultat : Si l'étape 2 trouve un $x$ alors c'est une solution, sinon l'équation n'a pas de solution du tout dans $L$.*

Dans les paragraphes suivants, nous décrivons cela plus en détail. Remarquons que si l'on veut une solution entière (ou $S$-entière pour $S$ fixé), alors on peut utiliser directement l'algorithme III.3.6.

### III.3.1 Déterminer les Ensembles $S_0$ et $S$

Si l'on veut trouver une solution entière à l'équation $\mathcal{N}_{L/K}(x) = a$ lorsque $a$ est un entier de $K$, alors tous les idéaux premiers qui divisent une solution $x$ divisent aussi $a$, et donc dans ce cas, on construit simplement $S$ comme l'ensemble des idéaux premiers qui divisent $a$, c'est-à-dire que l'on prend $S_0 = \varnothing$.

Si l'on veut une solution rationnelle, il faut ajouter à l'ensemble des idéaux premiers qui divisent $a$ un ensemble $S_0$ d'idéaux premiers exceptionnels satisfaisant le Théorème Principal. On prend alors $S = S_0 \cup \{\mathfrak{p} \mid a\}$. Le choix de $S_0$ se fait de la manière suivante :

– si $L/K$ est galoisienne, alors le Corollaire III.1.6 montre qu'il est suffisant de prendre des idéaux premiers qui engendrent la $[L : K]$-partie du groupe de classes relatif $Cl_i(L/K)$ de sorte que $Cl_{i,S_0}(L/K) = Cl_i(L/K)/\langle S_0 \rangle$ soit d'ordre premier au degré $[L : K]$.

– si l'extension n'est pas galoisienne, alors le Corollaire III.2.7 montre qu'il est suffisant de prendre les premiers ramifiés, et les idéaux premiers qui engendrent la $[L : K]$-partie des groupes de classes relatifs $Cl_i(\mathfrak{L}^D/K)$ de sorte que les groupes $Cl_{i,S_0}(\mathfrak{L}^D/K)$ soient d'ordre premier au degré $[L : K]$, où l'on rappelle que $\mathfrak{L}$ est la clôture galoisienne de $L/K$ et que les $\mathfrak{L}^D$ sont les sous-corps de $\mathfrak{L}$ tels que $\mathfrak{L}/\mathfrak{L}^D$ soit cyclique de degré $p^\alpha$ avec $p \mid [L : K]$. En

particulier, le groupe de classes $Cl_{i,S_0}(\mathfrak{L}/K)$ lui-même doit être d'ordre premier à $[L:K]$. Si l'on ne dispose pas explicitement des générateurs de ces groupes de classes, ceci peut se faire par exemple en prenant tout les premiers dont la norme est inférieure à la borne de Minkowski pour le corps $L/K$ (ou à une borne inférieure si l'on suppose que l'Hypothèse de Riemann Généralisée est vraie). Si l'on fait cela, on est certain d'annuler tous les groupes de classes $Cl_{i,S_0}(\mathfrak{L}^D/K)$, mais alors $S_0$ est certainement trop grand. Il est préférable de n'utiliser que le Corollaire III.2.7, qui ne requiert que d'engendrer les $[L:K]$-parties des différents groupes de classes.

Remarquons que l'ensemble $S_0$ ne dépend que de l'extension relative $L/K$, et absolument pas de la valeur de $a$ dans l'équation $\mathcal{N}_{L/K}(x) = a$. Lorsque l'on doit résoudre plusieurs équations aux normes pour la même extension, il suffit de calculer une seule fois $S_0$. Pour cette raison il est préférable d'écrire deux algorithmes différents :

**Algorithme III.3.2** (*Détermination de l'ensemble $S_0$ pour une extension galoisienne $L/K$*).
*1– Calculer le groupe de classes relatif $Cl_i(L/K)$ en utilisant le paragraphe I.2.3, et noter $\mathfrak{g}_i$ les générateurs de la $[L:K]$-partie de ce groupe.*
*2– Prendre tous les facteurs premiers des idéaux $\mathcal{N}_{L/K}(\mathfrak{g}_i)$.*

**Algorithme III.3.3** (*Détermination de l'ensemble $S_0$ pour une extension non galoisienne $L/K$*).
*1– Déterminer $G = Gal(\mathfrak{L}/K)$ et tous les sous-groupes cycliques $D$ de $G$ d'ordre $p^\alpha$ avec $p \mid [L:K]$.*
*2– Calculer les groupes de classes relatifs $Cl_i(\mathfrak{L}^D/K)$, et noter $\mathfrak{g}_i$ les générateurs des $[L:K]$-parties de ces groupes.*
*3– Prendre tous les facteurs premiers $\mathfrak{p}_j$ des idéaux $\mathcal{N}_{\mathfrak{L}^D/K}(\mathfrak{g}_i)$.*

**Algorithme III.3.4** (*Détermination de l'ensemble $S$ pour l'équation $\mathcal{N}_{L/K}(x) = a$*).
*1– Déterminer l'ensemble $S_0$ avec l'Algorithme III.3.2 ou III.3.3.*
*2– Factoriser $a$ en idéaux premiers $\mathfrak{p}_i$ de $K$, et poser $S = S_0 \cup \{\mathfrak{p}_i\}$.*

**Remarque** : Dans les Algorithmes III.3.2 et III.3.3, les étapes 2 et 3 peuvent être remplacées par une seule étape si l'on est capable de trouver des générateurs premiers, ce qui est toujours possible en théorie.

## III.3.2 Recherche de Solutions en $S$-unités

Dans ce paragraphe, nous donnons un algorithme qui résout l'équation aux normes

$$\mathcal{N}_{L/K}(x) = a$$

lorsque $a$ est une $S$-unité, et que l'on cherche une solution $x$ qui est aussi une $S$-unité. Dès que l'on a écrit $x$ et $a$ comme un produit de $S$-unités, le problème se réduit à un système linéaire. L'algorithme est le suivant :

**Algorithme III.3.5** (*Recherche d'une solution de $\mathcal{N}_{L/K}(x) = a$ dans $\mathbb{U}_{L,S}$*).
*Données : $L, K, S$ et $a \in \mathbb{U}_{L,S}$.*

*1– À l'aide de l'Algorithme I.1.2, déterminer un système fondamental* $\{s_0, \ldots, s_n\}$ *de* $S$*-unités de* $K$*, et* $\{\sigma_0, \ldots, \sigma_m\}$ *de* $L$*, où* $s_0$ *et* $\sigma_0$ *sont les unités de torsion d'ordre* $w_K$ *et* $w_L$*, avec* $w_K \mid w_L$*.*

*2– À l'aide de l'Algorithme I.1.4 calcluer* $\alpha_i$ *et* $\beta_{i,j}$ *tels que*

$$a = \prod s_i^{\alpha_i} \text{ et } \mathcal{N}_{L/K}(\sigma_j) = \prod s_i^{\beta_{i,j}}.$$

*3– Résoudre le système linéaire :*

$$\text{pour tout} \quad i > 0 \quad \sum_{j>0} \beta_{i,j} x_j = \alpha_i$$

$$\sum_{j \geqslant 0} \beta_{0,j} x_j \equiv \alpha_0 \mod w_K.$$

*Résultat : L'équation* $\mathcal{N}_{L/K}(x) = a$ *admet une solution avec* $x$ $S$*-unité si et seulement si le système linéaire de l'étape 3 a une solution* $(x_j)$ *dans* $\mathbb{Z}$*. Une solution est alors donnée par*

$$\mathcal{N}_{L/K}(\prod \sigma_j^{x_j}) = a.$$

**Remarques** : – À l'étape 2, $\alpha_0$ n'est défini que modulo $w_K$. Puisque la norme d'une unité de torsion est encore une unité de torsion, on a $\beta_{i,0} = 0$ pour tout $i > 0$.

– À l'étape 3, le système linéaire de congruences $\beta_1 x_1 + \ldots + \beta_n x_n \equiv \alpha_0 \mod w$ avec $n$ variables est équivalent au système linéaire sur $\mathbb{Z}$ avec $n+1$ variables $\beta_1 x_1 + \ldots + \beta_n x_n + w x_0 = 0$.

### III.3.3 Recherche de Solutions Entières ou $S$-Entières

Supposons maintenant que nous voulons résoudre $\mathcal{N}_{L/K}(x) = a$ où $a$ est un $S$-entier, et que nous voulions une solution également $S$-entière. L'algorithme utilise le fait que les facteurs premiers de $x$ sont au-dessus des facteurs premiers de $a$, exceptés peut-être quelques idéaux premiers de $S$.

Si l'on écrit $x$ et $a$ comme produit d'idéaux premiers, l'équation $\mathcal{N}_{L/K}(x\mathbb{Z}_{L,S}) = a\mathbb{Z}_{K,S}$ se réduit à un système linéaire (étape 2). Le fait que $x\mathbb{Z}_{L,S}$ soit un idéal principal nous donne des conditions linéaires supplémentaires qui doivent être satisfaites simultanément avec le premier système (étape 2). Comme nous cherchons une solution entière $x$, cela implique que les solutions du système linéaire (qui correspondent aux valuations sur les idéaux premiers) soient positives ou nulles. Le nombre de telles solutions est alors fini (étape 3).

Pour chaque solution du système, on déduit une égalité de la forme :

$$\mathcal{N}_{L/K}(b) = a \cdot u,$$

où $u$ est une $S$-unité, et $b$ un $S$-entier. Il ne reste plus alors qu'à écrire la $S$-unité $u$ comme la norme d'une $S$-unité pour obtenir une solution à notre problème (étape 4).

L'algorithme est donc le suivant :

**Algorithme III.3.6** (*Recherche d'une solution de $\mathcal{N}_{L/K}(x) = a$ dans $\mathbb{Z}_{L,S}$*) .

*Données : $K, L, S$ et $a \in \mathbb{Z}_{L,S}$.*

*1– (Factorisation) .*

*Déterminer les idéaux premiers $\mathfrak{p}_i$ (qui ne sont pas dans $S$) et les entiers $\alpha_i$ tels que $a\mathbb{Z}_{K,S} = \prod \mathfrak{p}_i^{\alpha_i}$. Déterminer également les idéaux premiers $\mathfrak{P}_{i,j}$ de $L$ et les entiers $e_{i,j}$ et $f_{i,j}$ tels que*

$$\mathfrak{p}_i = \prod \mathfrak{P}_{i,j}^{e_{i,j}} \text{ et } \mathcal{N}_{L/K}(\mathfrak{P}_{i,j}) = \mathfrak{p}_i^{f_{i,j}}.$$

*2– (Calcul des $m_{i,j,k}$) .*

*À l'aide de l'Algorithme I.1.2, calculer un système de générateurs $\{\mathfrak{g}_k\}$ du groupe de classes $Cl_S(L)$, et $d_k$ leurs ordres dans ce groupe. En utilisant l'Algorithme I.1.5, calculer les composantes $m_{i,j,k}$ des classes des idéaux $\mathfrak{P}_{i,j}$ sur les générateurs $\mathfrak{g}_k$.*

*3– (Résolution d'un système linéaire) .*

*Trouver tous les n-uplets d'entiers $(\beta_{i,j})$ satisfaisant simultanément les conditions :*

$$\begin{cases} \forall i & \sum_j f_{i,j}\beta_{i,j} = \alpha_i \\ \forall k & \sum_{i,j} m_{i,j,k}\beta_{i,j} \equiv 0 \mod d_k \\ \forall i & 0 \leqslant \beta_{i,j} \leqslant \alpha_i \end{cases}$$

*4– (Élimination de l'unité restante ) .*

*Pour chaque solution $(\beta_{i,j})$ du système trouver un $S$-entier $b$ de $L$ tel que $b\mathbb{Z}_{L,S} = \prod \mathfrak{P}_{i,j}^{\beta_{i,j}}$, et noter $u$ la $S$-unité définie par $u = \mathcal{N}_{L/K}(b)/a$. À l'aide de l'Algorithme III.3.4, trouver une $S$-unité $v$ telle que $u = \mathcal{N}_{L/K}(v)$.*

*Résultat : Si l'étape 3 ou l'étape 4 n'a pas de solution, alors l'équation n'est pas soluble en $S$-entiers. Sinon, le $S$-entier $bv^{-1}$ est une solution.*

**Remarque** : Il est facile d'adapter cet algorithme pour obtenir toutes les solutions (à $S$-unité près). De même, si l'on n'est intéressé que par l'équation $\mathcal{N}_{L/K}(x) = a \cdot u$, alors il est également possible d'adapter cet algorithme.

# Chapitre IV

# Discriminants Minimaux

Dans les chapitres précédents, nous avons fait de nombreux calculs dans des corps de nombres. Or, de tels calculs sont toujours limités par la taille de ces corps de nombres, et plus précisément par les polyômes irréductibles choisis pour les définir. Cette taille se mesure à l'aide de plusieurs grandeurs. Ne retenons que deux d'entre elles : le degré du polynôme et son discriminant. On pourrait aussi regarder d'autres grandeurs comme par exemple le groupe de Galois, ou la norme $T_2$ associée aux racines du polynôme, mais nous ne les évoquerons même pas. Nous essayons dans ce chapitre de déterminer les plus petites valeurs possibles des discriminants des polynômes pour les différentes signatures. Jusqu'au degré 9, de nombreux résultats sont connus, ou au moins conjecturés. Au delà de ce degré, on ne sait pas grand chose, et l'on ne dispose pratiquement pas d'exemples. Les méthodes proposées ici permettent de construire des petits discriminants pour les degrés supérieurs à 9, dont une grande partie améliorent les bornes précédemment connues. En particulier, les discriminants obtenus jusqu'au degré 14 sont tout à fait proches des bornes inférieures proposées par Odlyzko pour les discriminants de corps de nombres.

Dès lors que l'on s'intéresse aux discriminants de polynômes et non plus de corps de nombres (le lien est étroit entre les deux), il est naturel de se poser les mêmes questions pour les polynômes non nécessairement irréductibles. Ce domaine semble généralement peu étudié, et nous avons dû démontrer (probablement pour la première fois) tous les discriminants minimaux pour les degrés allant jusqu'à 7. Comme nous le verrons, cette étude nécessite l'examen attentif du comportement des résultants de certaines familles de polynômes.

## Qu'est-ce qu'un Discriminant ?

Le discriminant d'un polynôme a d'abord été introduit pour détecter les polynômes qui ont des racines multiples. À un facteur de normalisation près, le discriminant est égal au produit des carrés des différences des racines du polynôme :

$$\mathrm{disc}(P) = l(P)^{2d-2} \prod_{1 \leqslant i < j \leqslant d} (\alpha_i - \alpha_j)^2$$

où $d$ est le degré de $P$, où les $\alpha_i$ sont les racines de $P$, et $l(P)$ est le coefficient dominant de $P$. Ainsi, un polynôme $P$ a une racine multiple si et seulement si son discriminant est nul. Quand il n'est pas nul, le discriminant mesure d'une certaine manière la distance entre les racines. Un polynôme ayant un petit discriminant a donc des racines rapprochées, contenues dans un petit domaine (du plan complexe).

Il y a plusieurs manières équivalentes de définir le discriminant. Par exemple, on peut le définir comme le déterminant de la matrice de Sylvester des deux polynômes $P$ et $P'$, divisé par $l(P)$. Cette expression montre en particulier que le discriminant s'exprime comme un polynôme en les coefficients de $P$. Tout le monde se souvient de la formule du discriminant $\Delta$ d'un polynôme du second degré :

$$\Delta = b^2 - 4ac.$$

Le discriminant peut également s'écrire en fonction du résultant de $P$ et de sa dérivée $P'$ grâce à la formule suivante :

$$(-1)^{\frac{d(d-1)}{2}} \operatorname{disc}(P) = \frac{1}{l(P)} \operatorname{Res}(P, P').$$

Cette dernière expression peut encore s'écrire :

$$(-1)^{\frac{d(d-1)}{2}} \operatorname{disc}(P) = l(P)^{d-2} \prod_i P'(\alpha_i) = d^d l(P)^{d-1} \prod_j P(\beta_j).$$

où les $\beta_j$ sont les racines de $P'$. Si le discriminant de $P$ est petit, alors le produit des $P'(\alpha_i)$ est petit aussi, et on peut même penser que chaque $P'(\alpha_i)$ doit être petit, ou encore que chaque $P(\beta_j)$ doit être petit. Ceci montre que les extrema locaux de $P$ doivent être petits, ou encore que $P$ doit avoir un graphe relativement plat, avec seulement de petites variations. En quelque sorte, le discriminant mesure les variations de $P$.

Lorsque l'on élève cette dernière formule à la puissance $\frac{1}{d}$, on voit que le discriminant représente la moyenne des variations de $P$ en ses racines, ou alors la moyenne des extrema locaux. Enfin, sans donner davantage de détail, signalons que le discriminant peut également s'interpréter comme le volume d'un réseau de dimension $d$, et pour cette raison la seule grandeur vraiment comparable lorsque le degré varie est le discriminant élevé à la puissance $\frac{1}{d}$.

Parmi les polynômes de $\mathbb{Z}[x]$, on peut s'intéresser à plusieurs sous-familles, et la question de trouver les plus petits discriminants est différente selon chaque famille. Les méthodes varieront suivant les polynômes considérés. On peut d'abord distinguer les polynômes irréductibles des polynômes factorisables. On peut ensuite distinguer les polynômes unitaires ou non unitaires. Nous allons essentiellement nous intéresser aux polynômes irréductibles (unitaires), puis aux polynômes factorisables (non nécessairement unitaires).

Lorsque l'on s'intéresse aux discriminants de polynômes factorisables, on utilise en tout premier lieu la formule du discriminant d'un produit :

$$\operatorname{disc}(AB) = \operatorname{disc}(A) \operatorname{disc}(B) \operatorname{Res}^2(A, B).$$

Ainsi, pour obtenir des polynômes factorisables de petits discriminants, il est naturel de chercher des familles de polynômes dont les résultants deux à deux soient petits. Nous chercherons donc des familles de polynômes dont les résultants deux à deux sont tous égaux à $\pm 1$.

**Notations** : Si $P$ est un polynôme, on note $\operatorname{disc} P$ son discriminant. Son degré sera généralement noté $d$, $r_1$ est le nombre de racines réelles du polynôme $P$, et $2r_2$ le nombre de ses racines complexes, de sorte que l'on a $r_1 + 2r_2 = d$. On appelle alors $d.r_1$ la signature de $P$. La notation $l(P)$ désignera le coefficient dominant de $P$, et $\operatorname{Res}(P, Q)$ est le résultant des deux polynômes $P$ et $Q$. Enfin, lorsque nous utiliserons des polynômes à plusieurs variables, nous ajouterons en indice la variable sur laquelle nous travaillerons.

Si $P_1, \ldots, P_n$ sont des polynômes dont les coefficients $a_{i,j}$ sont indéterminés, on note $\mathbb{Z}[P_1, \ldots, P_n]$ l'anneau des polynômes à coefficients dans $\mathbb{Z}$ en les variables $a_{i,j}$. Par exemple, on a $\operatorname{disc}_x P \in \mathbb{Z}[P]$, et $\operatorname{Res}_x(P_1, P_2) \in \mathbb{Z}[P_1, P_2]$.

## IV.1 Quelques Propriétés des Résultants et des Discriminants

Commençons par rappeler la proposition suivante qui donne le signe du discriminant d'un polynôme en fonction de sa signature :

**Proposition IV.1.1** *Le signe du discriminant d'un polynôme de $\mathbb{Z}[x]$ est donné par la parité de l'entier $r_2 = \frac{d-r_1}{2}$ :*

$$\operatorname{disc} P = (-1)^{r_2} |\operatorname{disc} P|.$$

La proposition qui suit nous sera particulièrement utile pour déterminer le résultant de deux polynômes quadratiques dont on ne connaît que les discriminants. Sa démonstration est élémentaire.

**Proposition IV.1.2** *Soient $P_1 = a_1x^2 + b_1x + c_1$ et $P_2 = a_2x^2 + b_2x + c_2$ deux polynômes de degré 2 à coefficients indéterminés, et de discriminants respectifs $\Delta_1$ et $\Delta_2$. Soit $\delta = 2a_1c_2 - b_1b_2 + 2a_2c_1 \in \mathbb{Z}[P_1, P_2]$. On a la relation*

$$4 \operatorname{Res}(P_1, P_2) = \delta^2 - \Delta_1\Delta_2.$$

**Remarque** : Lorsque l'on est sous les mêmes hypothèses, on peut aussi noter la formule suivante :

$$4 \operatorname{Res}(P_1, P_2) = \operatorname{disc}(P_1 * P_2)$$

où $P_1 * P_2 = P_1'P_2 - P_2'P_1$ est encore un polynôme de degré 2. Plus généralement, lorsque $P_1$ et $P_2$ sont deux polynômes quelconques, on a toujours la relation

$$\operatorname{Res}(P_1, P_2) \mid \operatorname{disc}(P_1 * P_2)$$

où $P_1 * P_2$ est défini de la même manière que pour le degré 2. Cette dernière relation est vraie dans $\mathbb{Z}[P_1, P_2]$.

Cette proposition permet de montrer que certains résultants ne sont pas égaux à $\pm 1$. On peut aussi remarquer qu'il n'est pas du tout nécessaire que les polynômes soient irréductibles, ni même sans facteur carré. Nous ne retenons que le corollaire suivant :

**Corollaire IV.1.3** *Soient $P_1$ et $P_2$ deux polynômes de degré 2 de $\mathbb{Z}[x]$, ayant le même discriminant $\Delta$. Si $\mathrm{Res}(P_1, P_2)$ est non nul, alors on a l'inégalité*

$$|\mathrm{Res}(P_1, P_2) - 1| \geqslant |\Delta|.$$

*Si $\Delta < 0$, alors on a même l'inégalité*

$$\mathrm{Res}(P_1, P_2) \geqslant |\Delta| + 1 \geqslant 4.$$

*Preuve :* Notons $r$ le résultant de $P_1$ et $P_2$. La Proposition IV.1.2 montre qu'il existe un entier $\delta$ tel que $4r = \delta^2 - \Delta^2$. Ceci implique en tout premier lieu que $\delta$ et $\Delta$ ont la même parité.

Si $|\delta| > |\Delta|$, alors $|\delta| \geqslant |\Delta| + 2$. Ceci implique que $4r \geqslant 4(|\Delta| + 1)$.

Si $|\delta| < |\Delta|$, alors $|\delta| \leqslant |\Delta| - 2$. Ceci implique que $4r \leqslant -4(|\Delta| - 1)$.

De là, on tire l'inégalité annoncée.

Lorsque $\Delta$ est négatif, le résultant est une norme pour l'extension quadratique imaginaire $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$, donc il est positif, et on peut enlever la valeur absolue de l'inégalité précédente. ■

Ce corollaire montre que le résultant de deux polynômes irréductibles de degré 2 et de mêmes discriminants est soit nul soit supérieur ou égal à 4. En particulier, il ne peut pas être égal à $\pm 1$. Pour les degrés différents de 2, ceci n'est plus vrai comme l'indiquent les exemples suivants :

$$\begin{aligned}
&\mathrm{Res}(x, x+1) = \mathrm{Res}(x, 2x+1) = \mathrm{Res}(2x+1, x+1) = 1 && \mathrm{disc} = 1\\
&\mathrm{Res}(x^3 + 3x^2 - 4x + 1, x^3 - 6x^2 + 5x - 1) = 1 && \mathrm{disc} = 49\\
&\mathrm{Res}(x^4 - 4x^3 + 3x - 1, x^4 + 3x^3 - 2x^2 - 2x + 1) = 1 && \mathrm{disc} = 725
\end{aligned}$$

Quand on applique la Proposition IV.1.2 avec le polynôme $P_2 = x(x-1)$ de discriminant $\Delta_2 = 1$, la formule montre que le discriminant $\Delta_1$ est un carré modulo 4, c'est-à-dire qu'il est congru à 0 ou 1 modulo 4. Pour le cas du degré 2, il n'est pas nécessaire d'utiliser une grande théorie pour déduire cela, car le discriminant est de la forme $\Delta = b^2 - 4ac$, et il est clair que c'est un carré modulo 4. La proposition suivante montre que quel que soit le degré, un discriminant est toujours un carré modulo 4. Le résultat est dû à Stickelberger, mais nous proposons une nouvelle démonstration.

**Proposition IV.1.4** *Soit $P$ un polynôme à coefficients indéterminés. Si l'on écrit $P$ sous la forme $P(x) = A(x^2) + xB(x^2)$, alors on a*

$$\mathrm{disc}\, P - \mathrm{Res}^2(A, B) \in 4\mathbb{Z}[P].$$

*En particulier si $P \in \mathbb{Z}[x]$,*

$$\mathrm{disc}\, P \equiv 0 \text{ ou } 1 \mod 4.$$

*Preuve :* Soit $P$ un polynôme dont les coefficients sont indéterminés. Notons $d$ le degré de $P$, $l$ son coefficient dominant, et $c \neq 0$ son coefficient constant.

Tout polynôme $P$ peut s'écrire sous la forme $P(x) = A(x^2) + xB(x^2)$. Nous allons utiliser le polynôme auxiliaire suivant

$$\Delta_P(y) = \mathrm{Res}_x(P(x), P(xy))$$

Ce polynôme est dans $\mathbb{Z}[P][y]$, et on peut le factoriser en utilisant les racines (formelles) $\alpha_i$ de $P$ :

$$\Delta_P(y) = l^{2d} \prod_{i,j} (y\alpha_i - \alpha_j)$$

C'est donc un polynôme de degré $d^2$, qui est divisible par $(y-1)^d$. Notons $Q(y)$ le polynôme $\Delta_P(y)/(y-1)^d$. Ce polynôme de $\mathbb{Z}[P][y]$ est de degré $d(d-1)$. Comme ce degré est pair, nous le noterons $2m$, c'est-à-dire que nous avons $m = d(d-1)/2$. À partir de l'expression de $\Delta_P$ comme produit de facteurs linéaires, on voit que les racines de $Q$ sont les quotients $\alpha_i/\alpha_j$ pour $i \neq j$. Ainsi, les racines de $Q$ sont stables par inversion, ce qui signifie que $Q$ est un polynôme réciproque. Comme les racines de $P$ ne sont écrites que formellement, il n'est pas nécessaire de considérer séparément le cas où $\alpha_i = 0$, ce qui n'a d'ailleurs pas de sens formellement. Nous allons évaluer $Q$ pour $y = 1$ et pour $y = -1$.

Si l'on écrit $Q$ sous la forme

$$Q(y) = \alpha y^{2m} + \beta y^{2m-1} + \ldots + \gamma y^m + \ldots + \beta y + \alpha$$

avec $\alpha, \beta, \ldots \gamma \in \mathbb{Z}[P]$, on a

$$\begin{aligned} Q(1) &= \alpha + \beta + \ldots \quad +\gamma + \ldots + \beta + \alpha = 2(\alpha + \beta + \ldots) + \gamma \\ Q(-1) &= \alpha - \beta + \ldots + (-1)^m\gamma + \ldots - \beta + \alpha = 2(\alpha - \beta + \ldots) + (-1)^m\gamma \end{aligned}$$

De là, on déduit que $Q(1) - (-1)^m Q(-1) \in 4\mathbb{Z}[P]$

Pour $y = 1$, on a

$$\begin{aligned} Q(1) &= l^{2d} \prod_{i=j} \alpha_i \prod_{i \neq j} (\alpha_i - \alpha_j) \\ &= (-1)^m lc \,\mathrm{disc}\, P \end{aligned}$$

Pour $y = -1$, on a

$$\begin{aligned} Q(-1) &= \frac{\mathrm{Res}(P(x), P(-x))}{(-2)^d} \\ &= (-2)^{-d} \,\mathrm{Res}(A(x^2) + xB(x^2), A(x^2) - xB(x^2)) \\ &= (-2)^{-d} l \,\mathrm{Res}(A(x^2) + xB(x^2), -2xB(x^2)) \\ &= lc \,\mathrm{Res}(A(x^2), B(x^2)) \\ &= lc \,\mathrm{Res}^2(A, B) \end{aligned}$$

Des deux expressions de $Q(1)$ et $Q(-1)$, nous déduisons que

$$lc \operatorname{disc} P - lc \operatorname{Res}^2(A, B) \in 4\mathbb{Z}[P].$$

Il n'y a plus qu'à simplifier par $lc$ pour obtenir le résultat annoncé. ■

En général, lorsque $n$ est un entier quelconque, si les polynômes $P$ et $Q$ ont des coefficients entiers, on a la relation

$$\operatorname{disc}(P + nQ) \equiv \operatorname{disc} P \mod n,$$

qui provient du simple fait que le discriminant est une fonction polynomiale en les coefficients du polynôme. Lorsque $n$ est pair, on peut déduire de la proposition précédente une information un peu plus précise :

$$\operatorname{disc}(P + nQ) \equiv \operatorname{disc} P \mod 2n,$$

comme l'exprime le corollaire suivant :

**Corollaire IV.1.5** *Quels que soient les polynômes $P$ et $Q$ à coefficients indéterminés, et $n \in \mathbb{Z}$ on a*

$$\operatorname{disc}(P + 2nQ) - \operatorname{disc} P \in 4n\mathbb{Z}[P, Q].$$

*Preuve :* Si l'on écrit $P$ et $Q$ sous la forme $P(x) = A(x^2) + xB(x^2)$ et $Q = C(x^2) + xD(x^2)$, et si l'on note $F(P)$ le polynôme de $\mathbb{Z}[P]$ tel que $\operatorname{disc} P - \operatorname{Res}^2(A, B) = 4F(P)$, on a

$$\operatorname{disc}(P + 2nQ) = \operatorname{Res}^2(A + 2nC, B + 2nD) + 4F(P + 2nQ).$$

De là, on déduit l'existence de polynômes $G, H, I \in \mathbb{Z}[P, Q]$ tels que

$$\begin{aligned} \operatorname{disc}(P + 2nQ) &= (\operatorname{Res}^2(A, B) + 4nG) + 4(F(P) + 2nH) \\ &= \operatorname{Res}^2(A, B) + 4F(P) + 4nI \\ &= \operatorname{disc} P + 4nI \end{aligned}$$

■

# IV.2 Discriminants Minimaux pour les Petits Degrés

## IV.2.1 Polynômes Irréductibles

### Les Bornes d'Odlyzko

Un polynôme irréductible $P$ définit un corps de nombres $K = \mathbb{Q}(\alpha)$, en adjoignant une racine $\alpha$ de $P$ au corps de base $\mathbb{Q}$. Les discriminants $\operatorname{disc} P$ et $\operatorname{disc} K$ sont reliés par une relation simple du type :

$$\operatorname{disc} P = f^2 \operatorname{disc} K,$$

où l'entier $f$ est appelé l'indice de $P$. À partir de cette formule, il est clair que l'on a toujours l'inégalité suivante lorsque l'on prend les valeurs absolues des discriminants :

$$|\operatorname{disc} P| \geqslant |\operatorname{disc} K|.$$

Grâce à cela, toute minoration pour les discriminants de corps de nombres donnera immédiatement une minoration pour les discriminants de polynômes irréductibles. En particulier, nous disposons des bornes d'Odlyzko (voir [Odl]) qui donnent des minorations particulièrement précises des discriminants des corps de nombres pour chaque signature sous la forme :

$$|\operatorname{disc} P| \geqslant |\operatorname{disc} K| \geqslant Odl(d, r_1, r_2).$$

Ces minorations qui dépendent de la validité de l'hypothèse de Riemann pour les fonctions $L$ de Dirichlet seront toujours notre référence pour décider si un discriminant est petit ou grand, selon qu'il est proche ou éloigné de ces bornes. Nous comparerons tous nos discriminants aux bornes d'Odlyzko. Il existe d'autres minorations qui ne dépendent d'aucune hypothèse, mais elles sont moins précises.

Certains polynômes irréductibles définissent des corps de nombres $K$ qui ne contiennent pas d'autre sous-corps que $\mathbb{Q}$ et $K$ lui-même : de tels polynômes sont dits *primitifs*. Les polynômes primitifs sont généralement plus difficiles à trouver, puisque l'on s'interdit d'utiliser les méthodes par extensions relatives. On peut sans doute comparer cette difficulté à celle de trouver des polynômes de degrés premiers. Comme le degré d'un sous-corps divise toujours le degré du corps, un corps de degré premier ne peut pas contenir de sous-corps non trivial. Ainsi, les polynômes irréductibles dont le degré est un nombre premier sont automatiquement primitifs.

Nous indiquons maintenant les différentes méthodes qui nous ont permis de construire nos tables de petits discriminants. Dans plusieurs de ces méthodes, nous décrivons des constructions à partir de listes de polynômes déjà trouvés. Dans chacune de ces méthodes, on peut souvent remplacer les polynômes par d'autres polynômes de même discriminant. Pour cela, on peut changer un polynôme $P(x)$ en $P(x+1)$, ou en $P(-x)$, ou enfin prendre son réciproque. Ces trois transformations qui fixent le discriminant engendrent un groupe isomorphe à $GL_2(\mathbb{Z})$. Remarquons enfin que le choix d'un générateur d'un corps de nombres n'est pas du tout canonique, ce qui signifie qu'un même corps peut être défini par plusieurs polynômes de mêmes discriminants mais qui ne se déduisent pas l'un de l'autre par une simple transformation de $GL_2(\mathbb{Z})$.

## 1 Petits Coefficients

Il est tentant de dire qu'un polynôme $P = \sum a_i x^i$ qui a des petits coefficients entiers $a_i$ est un petit polynôme. Notre mesure de la taille d'un polynôme est son discriminant. Mais celui-ci est une fonction polynomiale en les coefficients de $P$. Si les $a_i$ sont petits, on s'attend alors à ce que le discriminant soit également petit.

**Méthode** : Après avoir choisi une borne $M$, on peut parcourir tous les polynômes de degré $d$ fixé dont les coefficients $a_i$ sont dans l'intervalle $[-M, M]$, et calculer chaque discriminant.

**Exemples** :

– Il a été démontré ([Diaz a]) que le polynôme $x^7 - x^6 - x^5 + x^4 - x^2 + x + 1$ est celui qui a le plus petit discriminant ($-184607$) pour le degré 7 dont la signature est $r_1 = 1$. Ses coefficients satisfont l'inégalité : $|a_i| \leqslant 1$.

– Le polynôme $x^d - 1$ a des coefficients particulièrement petits (presque tous nuls), et son discriminant vaut $d^d$, ce qui est encore de taille raisonnable lorsque $d$ n'est pas trop grand. Ce polynôme n'est pas irréductible, et se factorise en un produit de polynômes cyclotomiques, dont les discriminants sont nécessairement plus petits que $d^d$. Il se trouve que les coefficients des polynômes cyclotomiques sont très petits (bien qu'ils croissent quand même exponentiellement, voir par exemple [Erd-Vau]). En particulier, le premier polynôme cyclotomique dont un coefficient est au moins égal à 2 est $\Phi_{105}$ (de degré 48), et le premier dont un coefficient est au moins égal à 3 est $\Phi_{385}$ (de degré 240).

**Domaine d'Utilisation de la Méthode** : Le nombre de polynômes à tester est de l'ordre de $(2M+1)^d$. Lorsque l'on se place sous la condition très restrictive $M = 2$, le nombre de polynômes est déjà de l'ordre de $5 \cdot 10^7$ pour le degré $d = 11$. Cette méthode donne des listes relativement complètes de petits discriminants jusqu'à $d = 9$, mais donne presque toujours des polynômes de signature complexe ($r_1 \leqslant 4$). La grande majorité des polynômes trouvés sont primitifs. Jusqu'au degré 9, il faut certainement commencer par cette méthode avant d'en utiliser une autre plus compliquée. Au delà, elle ne donne presque rien.

Le recours à la majoration des coefficients a pour principal intérêt de pouvoir démontrer la minimalité de certains discriminants. Ceci peut se faire par exemple à l'aide du théorème suivant de Hunter (dans [Hun]) issu de la géométrie des nombres.

**Théorème (Hunter)** *Soit $K$ un corps de nombres de degré $d$ sur $\mathbb{Q}$ de discriminant* $\operatorname{disc} K$ *satisfaisant* $|\operatorname{disc} K| \leqslant M$. *Il existe $\theta \in \mathbb{Z}_K \setminus \mathbb{Z}$, dont on note $\theta_i$ les conjugués, tel que* $0 \leqslant Tr(\theta) = \sum \theta_i \leqslant \frac{d}{2}$ *et tel que*

$$\sum |\theta_i|^2 \leqslant \frac{1}{d} Tr(\theta)^2 + \gamma_{d-1} \left(\frac{M}{d}\right)^{\frac{1}{d-1}}$$

*où $\gamma_{d-1}$ est la constante d'Hermite en dimension $d-1$.*

Pour plus de précision sur la constante d'Hermite $\gamma_{d-1}$, on peut consulter [Con-Slo]. Ainsi, pour démontrer la minimalité de certains discriminants, on utilise ce théorème pour majorer les coefficients des polynômes, et obtenir des listes complètes contenant tous les minimaux successifs. Ces bornes sont suffisantes pour traiter les degrés jusqu'à 6 (voir [Poh]), et des raffinements permettent de traiter jusqu'au degré 8 (voir [Poh-Mar-Dia]). Au delà, ces bornes ne sont plus utilisables. Il faut toutefois remarquer que dans ce théorème, l'élément $\theta$ peut appartenir à un sous corps propre de $K$.

Une petite variation de cette méthode consiste à ne regarder que les polynômes réciproques, c'est-à-dire satisfaisant la relation $P(x) = x^d P(\frac{1}{x})$. Dans ce cas, le nombre de variables est divisé par 2, et pour un temps de calcul équivalent, on peut considérer des polynômes dont le degré est multiplié par 2. Ainsi, on trouve de bons résultats jusqu'au degré 18. Comme dans le cas précédent, on ne trouve que des signatures complexes. En revanche, dès

que $d > 2$ la proposition suivante montre que la réciprocité impose à tous les polynômes d'être de degré pair et imprimitifs.

**Proposition IV.2.1** *Soit $P \in \mathbb{Z}[x]$ un polynôme réciproque irréductible de degré $d$. Si $d > 2$, alors $d$ est pair et $P$ est imprimitif.*

*Preuve :* La réciprocité montre que $P(-1) = (-1)^d P(-1)$. Si $d$ est impair, cela implique que $-1$ est une racine de $P$, ce qui est impossible puisque $P$ est irréductible de degré $d > 2$.

Soit $\alpha$ une racine de $P$. Montrons que le corps $L = \mathbb{Q}(\alpha)$ contient un sous-corps d'indice 2. Soit $\beta = \alpha + \frac{1}{\alpha}$ et $K = \mathbb{Q}(\beta)$. Comme $\beta = \alpha + \frac{1}{\alpha}$, $K$ est un sous-corps de $L$. Le nombre algébrique $\beta$ est racine du polynôme

$$Q(x) = P(0)^d \prod_{P(\alpha)=0} \left( x - \alpha - \frac{1}{\alpha} \right)$$

Ce polynôme est à coefficients rationnels puisque c'est simplement le résultant

$$Q(x) = \mathrm{Res}_y \left( P(y), y \left( x - y - \frac{1}{y} \right) \right)$$

Mais ce polynôme est un carré puisqu'il est aussi égal à

$$Q(x) = P(0)^{2\frac{d}{2}} \prod{}^{*} \left( x - \alpha - \frac{1}{\alpha} \right)^2$$

où le produit est fait sur toutes les racines de $P$ modulo l'équivalence $\alpha \sim \frac{1}{\alpha}$. Comme $P$ est irréductible de degré supérieur à 2, on ne peut pas avoir $\alpha = \frac{1}{\alpha}$, et $Q$ est bien un carré. Comme c'est un carré dans $\mathbb{C}[x]$, c'est en réalité un carré dans $\mathbb{Q}[x]$. Ainsi, on a $Q = R^2$, ce qui prouve que $\beta$ est une racine du polynôme $R$ à coefficients rationnels de degré $d/2$. L'extension $L/K$ est donc de degré au moins 2, et même exactement 2 à cause de l'équation relative $\alpha^2 - \beta\alpha + 1 = 0$. Comme $d > 2$, le sous-corps $K$ est un sous-corps non-trivial de degré $\frac{d}{2}$ de $L$, ce qui prouve que $P$ est imprimitif. ■

**Remarque** : Nous venons de montrer que le sous-corps de degré $\frac{d}{2}$ est engendré par $\alpha + \frac{1}{\alpha}$. Ainsi, pour retrouver le sous-corps, il suffit de calculer le polynôme caractéristique $\chi$ de $\alpha + \frac{1}{\alpha}$ dont le carré est donné par

$$\chi(y)^2 = \mathrm{Res}_x(P(x), x^2 - xy + 1)$$

On a alors

$$P(x) = \mathrm{Res}_y(\chi(y), x^2 - xy + 1).$$

Ceci est un cas particulier d'une "formule d'inversion" que nous montrerons plus loin (Proposition IV.2.4).

**Exemple** : Le plus petit discriminant que nous avons trouvé pour un polynôme de signature $d.r_1 = 16.0$ est donné par le polynôme réciproque $P = x^{16} - x^{14} + x^{13} - 2x^{11} + x^{10} + x^9 - x^8 + x^7 + x^6 - 2x^5 + x^3 - x^2 + 1$ qui a des petits coefficients. Son discriminant vaut

$\mathrm{disc}(P) = 2773873245710329$. Il n'est qu'à 1.73% au-dessus de la borne d'Odlyzko. D'après la remarque précédente, le polynôme $P$ est de la forme

$$P = \mathrm{Res}_y(y^8 - 9y^6 + y^5 + 26y^4 - 7y^3 - 24y^2 + 12y + 1, x^2 - xy + 1)$$

Les tables de [Coh-Dia-Oli a], contiennent un polynôme réciproque pour la même signature qui engendre un corps dont le discriminant est inférieur au nôtre. Toutefois, ce polynôme a un indice $7^2$, ce qui rend son discriminant supérieur au nôtre.

## 2 Petites Variations des Coefficients

**Méthode** : Le discriminant d'un polynôme est une fonction polynomiale en les coefficients, et donc c'est une fonction continue. Ainsi, on s'attend à ce que le discriminant varie peu si l'on fait une petite variation des coefficients. Si l'on note $P$ le polynôme de départ dont le discriminant est déjà petit, et $\varepsilon$ un polynôme comme $1, -1, x, -x, \ldots$, alors le polynôme $Q = P + \varepsilon$ devrait avoir aussi un petit discriminant. Le polynôme $P$ peut être soit irréductible soit factorisable. Nous avons observé que les polynômes factorisables ont des discriminants inférieurs à ceux des polynômes irréductibles, il est alors souvent préférable de choisir $P$ factorisable. Toutefois, si $P$ est trop factorisable, en particulier si son discriminant est nul, alors l'expérience montre que le discriminant de $Q$ explose facilement. Les meilleurs résultats ont été obtenus pour des polynômes $Q$ de la forme $Q = xP + \varepsilon$ ou $Q = (x-1)P + \varepsilon$, où $P$ est irréductible de petit discriminant. Dans ce cas, le discriminant de $Q$ est voisin du discriminant de $xP$ ou de $(x-1)P$, qui est donné par $P(0)^2 \cdot \mathrm{disc}(P)$ ou $P(1)^2 \cdot \mathrm{disc}(P)$. Une méthode voisine de celle-ci est décrite plus loin (Polynômes de résultant 1).

Remarquons que choisir pour $\varepsilon$ un polynôme qui a des petits coefficients n'est pas nécessairement le meilleur choix possible. Un polynôme ayant un petit discriminant est parfois meilleur. En effet, nous avons expliqué dans l'introduction qu'un petit discriminant équivaut à un graphe relativement plat, sans fortes variations. Ainsi, si l'on ajoute à $P$, qui a un graphe plat, un polynôme $\varepsilon$ qui est également plat, le graphe de $Q$ devrait garder cette propriété, et donc avoir un petit discriminant.

**Exemple** : À partir du polynôme $P = x^9 + 4x^8 + 7x^7 + 10x^6 + 12x^5 + 11x^4 + 8x^3 + 5x^2 + 2x + 1$ ($\mathrm{disc} = 30453593$, $d.r_1 = 9.1$), en faisant varier les coefficients de $\pm 1$, on trouve vingt autres polynômes de signature $d.r_1 = 9.1$ en dessous de 10% et trois polynômes de signature $d.r_1 = 9.3$ en dessous de 10%. Nous donnons ici la signature et le discriminant de $Q$, ainsi que la différence $Q - P$.

| $r_1$ | disc | $Q - P$ |
|---|---|---|
| 3 | $-198348791$ | $-x^8 - x^7 + x^6 - x^5 + x^3 + x$ |
| 3 | $-192165947$ | $-x^7 - x^5 + x^3 + x$ |
| 3 | $-149039567$ | $-x^7 + x^5 - x^4 + x^3$ |

| $r_1$ | disc | $Q - P$ |
|---|---|---|
| 1 | 32344469 | $x^7 + x^6 - x^4 - x^3$ |
| 1 | 32923873 | $x^7 + x^6 + x^5 + x^4 + x^3 + x^2$ |
| 1 | 33121433 | $x^5 - x^4 - x^3 - x$ |
| 1 | 33626161 | $x^7 + x^6 + x^4 + x^3 + x^2 + x$ |
| 1 | 34590113 | $-x^8 - x^4$ |
| 1 | 35028793 | $x^7 + x^6 - x^5 - x^4 - x^3 - x^2$ |
| 1 | 35050633 | $-x^8 - x^7$ |
| 1 | 38118173 | $-x^8 + x$ |
| 1 | 38525297 | $-x^8 - x^7 - x^6 - x^5 + x^3 + x$ |
| 1 | 39067993 | $-x^8 + x^6$ |
| 1 | 40466809 | $-x^5 - x^4$ |
| 1 | 41995553 | $-x^8 + x^7$ |
| 1 | 44573353 | $x^7 + x^6 + x^5 + x^4 + x^3 + x$ |
| 1 | 46094281 | $-x^8 - x^7 - x^5 + x^3 + x^2 + x$ |
| 1 | 46382993 | $x^7 + x^6 - x^3 - x^2$ |
| 1 | 47138401 | $-x^8 - x^7 - x^6 + x^3 + x^2 + x$ |
| 1 | 48487609 | $x^7 - x^5 - x^4 - x^3$ |
| 1 | 50644288 | $x^6 - x^5 - x^4 + x$ |
| 1 | 53814641 | $-x^8 - x^5$ |
| 1 | 60095296 | $-x^8 + x^3$ |

De tels exemples se reproduisent très fréquemment en degré 9.

**Domaine d'Utilisation de la Méthode** : Cette méthode suppose que l'on dispose déjà d'une liste suffisante de polynômes de petits discriminants. Son principal avantage est que l'on peut faire augmenter le degré d'une unité à chaque étape, et ainsi arriver à des degrés premiers. La signature du polynôme $Q = xP + \varepsilon$ est en général voisine de celle de $xP$, et l'on peut ainsi prévoir la signature des polynômes que l'on trouve, bien que les polynômes totalement réels soient rarement trouvés par cette méthode. Enfin, il faut noter que lorsque le degré devient trop grand (de l'ordre de 17), la moindre variation des coefficients d'un polynôme entraîne l'explosion de son discriminant.

## 3 Petites Variations des Racines

**Méthode** : Si $\varepsilon$ est un (petit) nombre réel, alors les racines du polynôme $P(x + \varepsilon)$ sont les $\alpha_i - \varepsilon$ où les $\alpha_i$ sont les racines de $P$. Pour cette raison, l'application $P(x) \to Q(x) = P(x + \varepsilon)$ préserve le discriminant et la signature du polynôme. Toutefois, même si $P$ a des coefficients entiers, $Q$ n'a pas de coefficients entiers lorsque $\varepsilon$ n'est pas lui-même un entier. Pour retrouver cette propriété, on peut arrondir ses coefficients à l'entier le plus proche. Dans ce cas, le discriminant et la signature de $Q$ sont différents de ceux de $P$. Si le discriminant de $P$ est petit, alors il est probable que le discriminant de $Q$ soit également petit, et sa signature voisine de celle de $P$. Plus généralement, on peut appliquer à $P$ la transformation $x \to \alpha x + \varepsilon$ où $\varepsilon$ est proche de 0 et $\alpha$ est proche de 1.

**Exemple** : En appliquant au polynôme $P = x^{11} - x^{10} + 4x^9 - 6x^8 + 8x^7 - 11x^6 + 11x^5 - 11x^4 + 8x^3 - 6x^2 + 3x - 1$ ($d.r_1 = 11.1$ et disc $= -6004248839$) la transformation $x \to \alpha x + \varepsilon$ et en arrondissant les coefficients aux entiers les plus proches, on trouve les polynômes suivants qui sont distants de la borne d'Odlyzko de moins de 10%.

| $\alpha$ | $\varepsilon$ | $d.r_1$ | disc |
|---|---|---|---|
| 0.950 | 0.035 | 11.1 | −8095166839 |
| 0.980 | 0.120 | 11.1 | −6046447999 |
| 0.984 | 0.015 | 11.1 | −13908165539 |
| 0.992 | 0.030 | 11.1 | −11025730003 |
| 0.992 | 0.045 | 11.1 | −11914617343 |
| 0.993 | −0.074 | 11.1 | −11941490767 |
| 0.993 | 0.070 | 11.1 | −8168279567 |
| 1.000 | −0.085 | 11.1 | −9716055647 |
| 1.020 | −0.023 | 11.1 | −6580722667 |
| 1.020 | −0.123 | 11.1 | −11588314931 |
| 1.027 | −0.058 | 11.1 | −13714009931 |
| 1.033 | −0.115 | 11.3 | 50760160601 |

**Domaine d'Utilisation de la Méthode** : Cette méthode permet de trouver de nombreux polynômes de petits discriminants pour n'importe quelle signature, y compris pour les signatures réelles ($r_2 \leqslant 3$). Il semble que pour la plupart des polynômes de degré inférieur à 15 (un peu moins pour les signatures réelles), cette méthode permette de construire des nouveaux polynômes. Toutefois, il est difficile de prévoir les bonnes valeurs de $\alpha$ et $\varepsilon$, d'autant qu'il faut les connaître avec une certaine précision (inférieure à 0.005), et un balayage de toutes les valeurs possibles pour $\alpha$ et $\varepsilon$ est vite très fastidieux.

Nous avons constaté expérimentalement que les "bonnes" valeurs de $\varepsilon$ et de $\alpha - 1$ sont de l'ordre de $\pm\frac{1}{d}$.

## 4 Extensions Relatives

Quand on fait une extension de corps de nombres $L/K$ de degré $r$, le discriminant absolu de $L$ est relié au discriminant relatif de $L/K$ par la formule

$$|\operatorname{disc}(L/\mathbb{Q})| = |\operatorname{disc}(K/\mathbb{Q})|^r \cdot \mathcal{N}_{K/\mathbb{Q}}(\operatorname{disc}(L/K)),$$

où le discriminant relatif $\operatorname{disc} L/K$ est un idéal de $K$.

Si une équation absolue de $K = \mathbb{Q}(\alpha)$ est donnée par $P(\alpha) = 0$, si une équation relative de $L = K(\beta)$ est donnée par $R(\alpha, \beta) = 0$ avec $R \in \mathbb{Z}[x, y]$, et si $\beta$ est un élément primitif pour l'extension $L/\mathbb{Q}$, alors une équation absolue de $L/\mathbb{Q}$ est donnée par le résultant suivant :

$$Q(y) = \operatorname{Res}_x(P(x), R(x, y)).$$

La proposition suivante donne le discriminant du polynôme $Q$ en fonction de $P$ et $R$, et doit être vue comme l'analogue de la formule précédente du discriminant relatif adaptée au

cas des polynômes. Il faut constater qu'il y a un facteur parasite, que l'on peut enlever dans certains cas, mais qui impose parfois de gros indices entre les discriminants de polynômes et les discriminants de corps. C'est probablement à cause de cet indice que les méthodes d'extensions relatives n'ont pas la même efficacité suivant que l'on s'intéresse aux polynômes ou aux corps de nombres.

**Proposition IV.2.2** *Soient $P \in \mathbb{Z}[x]$ et $R \in \mathbb{Z}[x,y]$. Si l'on pose $Q(y) = \mathrm{Res}_x(P(x), R(x,y))$ et $r = \deg_y R$, on a*

$$\begin{aligned}\operatorname{disc} Q = &(\operatorname{disc} P)^r \cdot \mathrm{Res}_x(P, \operatorname{disc}_y R)\\ &\times \mathrm{Res}_x\left(P(x), \mathrm{Res}_w\left(\frac{P(w)-P(x)}{w-x}, \mathrm{Res}_y\left(R(x,y), \frac{R(w,y)-R(x,y)}{w-x}\right)\right)\right).\end{aligned}$$

Pour démontrer ce résultat, nous utilisons une formule sur le discriminant que nous commençons par redémontrer :

**Lemme IV.2.3** *Soit $P$ un polynôme de degré $d$. On a*

$$(-1)^{\frac{d(d-1)}{2}} \operatorname{disc} P = l(P)^{-2} \lim_{y\to 0} y^{-d} \mathrm{Res}_x(P(x), P(x+y)).$$

*Preuve :* Notons $\alpha_i$ les racines de $P$. On a

$$\begin{aligned}\mathrm{Res}_x(P(x), P(x+y)) =& l(P)^{2d} \prod_{i,j}(y + \alpha_i - \alpha_j)\\ =& l(P)^{2d} y^d \prod_{i\neq j}(y + \alpha_i - \alpha_j)\end{aligned}$$

De là on déduit le lemme souhaité. ■

*Preuve de la Proposition IV.2.2 :* Notons $q = \deg Q$. Nous partons de la formule précédente, qui donne le discriminant de $Q$ :

$$\begin{aligned}&(-1)^{\frac{d(d-1)}{2}} l(Q)^2 \operatorname{disc} Q\\ &= \lim_{z\to 0} z^{-q} \mathrm{Res}_y(Q(y), Q(y+z))\\ &= \lim_{z\to 0} z^{-q} \mathrm{Res}_y(\mathrm{Res}_x(P(x), R(x,y)), \mathrm{Res}_w(P(w), R(w, y+z)))\\ &= \lim_{z\to 0} z^{-q} \mathrm{Res}_x(P(x), \mathrm{Res}_w(P(w), \mathrm{Res}_y(R(x,y), R(w,y+z))))\\ &= \lim_{z\to 0} z^{-q} \mathrm{Res}_x\left(P(x), \mathrm{Res}_w\left(\frac{P(w)-P(x)}{w-x}\cdot(w-x), \mathrm{Res}_y(R(x,y), R(w,y+z))\right)\right)\\ &= \lim_{z\to 0} z^{-q} \mathrm{Res}_x(P(x), \mathrm{Res}_y(R(x,y), R(x,y+z)))\\ &\quad \times \mathrm{Res}_x\left(P(x), \mathrm{Res}_w\left(\frac{P(w)-P(x)}{w-x}, \mathrm{Res}_y(R(x,y), R(w,y+z))\right)\right)\end{aligned}$$

$$= \mathrm{Res}_x(P(x), l_y(R)^2 \operatorname{disc}_y R(x,y))$$
$$\times \mathrm{Res}_x\left(P(x), \mathrm{Res}_w\left(\frac{P(w)-P(x)}{w-x}, \mathrm{Res}_y\left(R(x,y), \frac{R(w,y)-R(x,y)}{w-x}\cdot(w-x)\right)\right)\right)$$
$$= \mathrm{Res}_x(P(x), l_y(R(x,y)))^2 \,\mathrm{Res}_x(P(x), \operatorname{disc}_y R(x,y)) \times \operatorname{disc}^r P$$
$$\times \mathrm{Res}_x\left(P(x), \mathrm{Res}_w\left(\frac{P(w)-P(x)}{w-x}, \mathrm{Res}_y\left(R(x,y), \frac{R(w,y)-R(x,y)}{w-x}\right)\right)\right).$$

La preuve s'achève lorsque l'on a remarqué que $l(Q) = \mathrm{Res}_x(P(x), l_y(R(x,y)))$. ■

**Remarque** : Dans le cas particulier où $R(x,y)$ est de la forme $A(y)x+B(y)$ avec $\mathrm{Res}(A,B) = \pm 1$, alors on retrouve la formule classique du discriminant d'une extension relative :

$$\operatorname{disc} Q = (\operatorname{disc} P)^r \cdot \mathrm{Res}_x(P(x), \operatorname{disc}_y R(x,y)).$$

**Méthode** : À partir d'une liste de polynômes de base $P_i$, et d'une liste de polynômes relatifs $R_j$, on construit les polynômes $\mathrm{Res}(P_i, R_j)$.

**Exemple** : Dans les tables de polynômes de discriminants minimaux données en annexe, la plupart des polynômes de degré pair supérieur ou égal à 18 sont de la forme $Q(y) = \mathrm{Res}(P(x), R(x,y))$ avec $R$ de degré 2 parmi la liste suivante (certains polynômes $R$ se déduisent les uns des autres par une transformation de $GL_2(\mathbb{Z})$ sur $x$ mais donnent des résultats différents) :

| $R$ | $\mathrm{Res}(A,B)$ | $\operatorname{disc} Q / \operatorname{disc}^2 P$ |
|---|---|---|
| $y^2+y\pm x$ | 1 | $4^d P(\mp\frac{1}{4})$ |
| $y^2+xy+1$ | $-1$ | $P(2)P(-2)$ |
| $y^2+xy-1$ | 1 | $P(2i)P(-2i)$ |
| $(y^2-y+1)x\pm 1$ | 1 | $3^d P(\mp\frac{4}{3})P(0)$ |

Signalons ici le polynôme de signature $d.r_1 = 26.0$ qui a été construit par cette méthode à partir d'un polynôme de degré 13 :
$Q = y^{26} - y^{25} + 3y^{24} - 4y^{23} + 6y^{22} - 19y^{21} + 9y^{20} - 100y^{19} + 12y^{18} - 322y^{17} + 14y^{16} - 630y^{15} + 15y^{14} - 783y^{13} + 15y^{12} - 630y^{11} + 14y^{10} - 322y^9 + 12y^8 - 100y^7 + 9y^6 - 19y^5 + 6y^4 - 4y^3 + 3y^2 - y + 1 =$
$\mathrm{Res}(x^{13} + x^{12} - 10x^{11} - 8x^{10} + 38x^9 + 22x^8 - 69x^7 - 24x^6 + 62x^5 + 7x^4 - 26x^3 + 2x^2 + 4x - 1, y^2 + xy + 1)$
Ce polynôme de discriminant $-(1535761 \cdot 7036903)^2 239$ n'est qu'à 5.79% de la borne d'Odlyzko. Son discriminant est inférieur à ceux trouvés par H. Cohen-F. Diaz Y Diaz-M. Olivier dans [Coh-Dia-Oli a]. Dans cet article, les auteurs sont partis des corps connus jusqu'au degré 6, et ont réalisé des extensions abéliennes. Ainsi, aucune extension cyclique de degré 13 d'un corps quadratique n'a donné de discriminant inférieur à notre exemple.

**Domaine d'Utilisation de la Méthode** : Par définition, cette méthode ne permet de construire que des polynômes imprimitifs. Cette méthode est particulièrement efficace pour les degrés pairs élevés (nous avons obtenu des polynômes jusqu'au degré 48 pour les signatures complexes, et 24 pour les signatures réelles) comme le montrent les tables données en annexe. Quelques exemples d'extensions relatives cubiques ont été trouvés (par exemple

pour les degrés 27 et 33). Si les extensions relatives quadratiques ont donné de bons résultats, les extensions cubiques, quartiques ou même quintiques n'ont quasiment rien donné. Par exemple, pour les degré 18, 24 ou 30, les discriminants obtenus par extensions quadratiques sont meilleurs que ceux obtenus par extensions cubiques. Cette remarque s'éclaircit peut-être en disant que les polynômes relatifs cubiques étaient mal choisis. On peut plus sérieusement se demander s'il n'y a pas de raison à cela, et essayer d'expliquer par la même occasion pourquoi les minimaux connus pour chaque signature en degré 9 sont tous primitifs (y compris lorsque l'on regarde les discriminants des corps de nombres et non pas ceux des polynômes). Certains auteurs (par exemple dans [Coh-Dia-Oli c]), n'hésitent pas à dire que les corps imprimitifs n'ont aucune raison de donner les discriminants minimaux (au moins pour les grands degrés), et que ces discriminants devraient même être atteints par des corps dont le groupe de Galois est le groupe symétrique $S_n$, ce qui impliquerait en particulier que ces corps sont primitifs.

La proposition suivante est utile pour retrouver le polynôme $P$ à partir du polynôme $Q$. C'est une sorte de "formule d'inversion" pour les extensions relatives.

**Proposition IV.2.4** *Soit $P \in \mathbb{Z}[x]$ et $R \in \mathbb{Z}[x,y]$. Si l'on pose $Q = \mathrm{Res}_x(P,R)$ et $r = \deg_y R$, alors on a*

$$P^r \mid \mathrm{Res}_y(Q,R).$$

*De plus si $R$ est de la forme $R = A(y)x + B(y)$, et si $d = \deg P$, alors on a*

$$\mathrm{Res}_y(Q,R) = \mathrm{Res}(A,B)^d P^r.$$

*Preuve :* C'est un calcul sur les résultants :

$$\begin{aligned}
\mathrm{Res}_y(Q, R(z,y)) &= \mathrm{Res}_y(\mathrm{Res}_x(P(x), R(x,y)), R(z,y)) \\
&= \mathrm{Res}_y(\mathrm{Res}_x(P(x), R(x,y) - R(z,y)), R(z,y)) \\
&= P(z)^r \,\mathrm{Res}_y\left(\mathrm{Res}_x\left(P(x), \frac{R(x,y) - R(z,y)}{x - z}\right), R(z,y)\right)
\end{aligned}$$

Ceci prouve la première assertion. Dans le cas où $R(x,y) = A(y)x + B(y)$, on peut poursuivre le calcul :

$$\begin{aligned}
\mathrm{Res}_y(Q, R(z,y)) &= P(z)^r \,\mathrm{Res}_y(\mathrm{Res}_x(P(x), A(y)), A(y)z + B(y)) \\
&= P(z)^r \,\mathrm{Res}_y(A(y)^d, A(y)z + B(y)) \\
&= P(z)^r \,\mathrm{Res}(A,B)^d
\end{aligned}$$

■

## 5 Semi-Extensions Relatives

**Méthode** : Le principe qui a déjà conduit à plusieurs méthodes est de déformer légèrement les polynômes qui ont des petits discriminants. Nous appliquons ce principe à la méthode des extensions relatives. Une extension relative se fait à partir de la formule

$Q(y) = \mathrm{Res}(P(x), R(x,y))$, où $P$ est le polynôme de base, et $R$ le polynôme relatif. Une modification sur le polynôme $R$, donnera toujours une extension relative, et donc n'est pas une vraie modification. En revanche, une modification sur le polynôme $P$ conduit à considérer les polynômes $Q$ de la forme $Q(y) = \mathrm{Res}_x(P(x,y), R(x,y))$. Il ne s'agit plus du tout d'extensions relatives, et l'on ne peut plus rien prédire sur le polynôme $Q$. En particulier, on ne peut pas simplement dire s'il est primitif, ni calculer son discriminant ou sa signature, ni même parfois son degré.

Nous nous sommes restreints aux polynômes de la forme $Q(y) = \mathrm{Res}_x(\alpha(x,y)P(x) + \beta(x,y), R(x,y))$, où $\alpha$ et $\beta$ sont des petits polynômes comme par exemple $y$, $-y$, $xy$, $y-1$... et où $P$ et $R$ engendrent déjà une extension relative de petit discriminant. Nous avons constaté expérimentalement que cette méthode de "semi-extensions relatives" permet de construire de nombreux polynômes primitifs, y compris en degrés premiers. De plus, nous avons constaté que les différents invariants des polynômes $Q$ ainsi obtenus (degré, signature, discriminant...) sont souvent proches de ceux obtenus par de vraies extensions relatives ($\alpha = 1$ et $\beta = 0$).

**Exemple** : Nous illustrons cette méthode en donnant des polynômes pour certaines signatures en degré impair assez élevé. Ces polynômes donnent les plus petits discriminants que nous ayons trouvés pour leurs signatures. Ils sont tous primitifs et sont à moins de 10% de la borne d'Odlyzko.

$d.r_1 = 19.5$ avec $Q = \mathrm{Res}_x(y(x^9-x^8+2x^7-5x^6+3x^5-5x^4+5x^3-2x^2+3x-1)+1, xy^2+y-x)$

$d.r_1 = 21.3$ avec $Q = \mathrm{Res}_x(x^{10} - 2x^8 + 2x^7 - 3x^5 + 3x^4 - x^2 + 2x - 1 + y, (x-1)y^2 - x)$

$d.r_1 = 23.3$ avec $Q = \mathrm{Res}_x(x^{11} - 3x^{10} + 8x^9 - 12x^8 + 15x^7 - 12x^6 + 6x^5 - 4x^3 + 3x^2 - 2x + 1 - y(x-1), xy^2 + (x+1)y + x)$.

**Domaine d'Utilisation de la Méthode** : Bien que cette méthode ne nous ait pas permis d'obtenir des polynômes de degrés aussi élevés que les vraies extensions relatives (27 au lieu de 48), elle nous a permis de trouver de très nombreux polynômes primitifs pour tous les degrés jusqu'à 27, dont en particulier les degrés impairs, et surtout les degrés premiers. La principale limite de cette méthode est le nombre considérable de polynômes à tester. En effet, il faut considérer simultanément les polynômes $P, R, \alpha$ et $\beta$.

Comme dans le cas des extensions relatives, on dispose d'une "formule d'inversion", c'est-à-dire d'un moyen de retrouver le polynôme $P$ à partir du polynôme $Q$ :

**Proposition IV.2.5** *Soit $P \in \mathbb{Z}[x]$. Soit $R \in \mathbb{Z}[x,y]$ de la forme $R(x,y) = A(y)x + B(y)$ et $\alpha,\ \beta \in \mathbb{Z}[x,y]$. Notons $d = \deg P$ et $r = \deg_y R$. Si l'on pose $Q = \mathrm{Res}_x(\alpha P + \beta, R)$, alors dans $\mathbb{Z}[A,B][x]$ on a*

$$\mathrm{Res}(A,B)^d P^r \mid \mathrm{Res}_y(Q - (-A)^d \beta, R)$$

*Preuve :* Comme pour le cas des extensions relatives, ceci est un calcul sur les résultants.

$$\begin{aligned}
&\mathrm{Res}_y(Q(y) - (-A(y))^d\beta(z,y), R(z,y)) \\
&\quad = \mathrm{Res}_y(\mathrm{Res}_x(\alpha(x,y)P(x) + \beta(x,y), R(x,y)) - (-A(y))^d\beta(z,y), R(z,y)) \\
&\quad = \mathrm{Res}_y(\mathrm{Res}_x(\alpha(x,y)P(x) + \beta(x,y), R(x,y) - R(z,y)) - (-A(y))^d\beta(z,y), R(z,y)) \\
&\quad = \mathrm{Res}_y(\mathrm{Res}_x(\alpha(x,y)P(x) + \beta(a,y), A(y)(x-z)) - (-A(y))^d\beta(z,y), R(z,y)) \\
&\quad = \mathrm{Res}_y(\mathrm{Res}_x((-A(y))^d \cdot (\alpha(z,y)P(z) + \beta(z,y)) - (-A(y))^d\beta(z,y), R(z,y)) \\
&\quad = (-1)^{rd}\,\mathrm{Res}(A,B)^d P(z)^r\,\mathrm{Res}_y(\alpha(z,y), R(z,y))
\end{aligned}$$

■

## 6 Polynômes de Résultant 1

Nous avons observé que les polynômes qui ont un résultant égal à $\pm 1$ avec de nombreux autres "petits" polynômes ont très souvent des discriminants voisins des discriminants minimaux. Cette observation, qui peut par exemple se justifier par la proposition suivante, est à l'origine de cette méthode.

**Proposition IV.2.6** *Soit $P \in \mathbb{R}[x]$ un polynôme de degré $d$, dont toutes les racines sont réelles. On a l'inégalité :*

$$\mathrm{disc}\, P \leqslant \left|\mathrm{Res}\left(P, \frac{x^{2d}-1}{x^2-1}\right)\right|.$$

*Preuve :* Commençons par montrer l'inégalité pour un polynôme $P \in \mathbb{R}[x]$ unitaire de degré $d$. Notons $x_1,\ldots,x_d$ les racines de $P$. Soit $V$ la matrice de Vandermonde associée aux $x_i$ :

$$V = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{d-1} \\ & \vdots & & \\ 1 & x_d & \cdots & x_d^{d-1} \end{pmatrix}.$$

Le déterminant de cette matrice vérifie $\det^2 V = \mathrm{disc}\, P$. Si l'on applique l'inégalité de Hadamard à $V$, on trouve

$$\det{}^2 V \leqslant \prod_i (1 + x_i^2 + \ldots + x_i^{2d-2}).$$

Or, ce produit est (au signe près) le résultant $\mathrm{Res}\left(P, \frac{x^{2d}-1}{x^2-1}\right)$, on a donc l'inégalité annoncée.

Si $P$ est un polynôme non-unitaire, de coefficient dominant $l$, on applique l'inégalité précédente avec $\frac{1}{l}P$. On peut simplifier les deux termes par le même facteur $l^{2d-2}$, et l'on obtient l'inégalité annoncée. ■

D'après cette proposition, un polynôme totalement réel dont les résultants avec les polynômes cyclotomiques sont petits doit avoir un petit discriminant. Les coefficients de la matrice de Vandermonde sont les valeurs $Q_j(x_i)$ des polynômes $Q_j = x^{j-1}$ aux racines de $P$. Si on prend d'autres polynômes $Q_j$, on trouve l'inégalité $m^2\,\mathrm{disc}\, P \leqslant |\,\mathrm{Res}(P, \sum Q_j^2)|$,

où $m$ est le déterminant de la matrice $M$ contenant les coefficients des polynômes $Q_j$ (il suffit de multiplier $V$ par $M$). Ainsi, en faisant varier les polynômes $Q_j$, on peut obtenir des inégalités plus ou moins précises. Dans tous les cas, le polynôme $\sum Q_j^2$ est totalement complexe.

**Méthode** : La méthode que nous décrivons ici consiste à fabriquer des polynômes en leur imposant d'avoir un résultant égal à $\pm 1$ avec un ou plusieurs autres polynômes. En termes de corps de nombres, cela revient à construire un corps à partir de ses unités. On peut en fait distinguer deux méthodes.

**A**– Dans la première méthode, on considère toute une famille de polynômes $P_i$ de petits degrés et l'on cherche les polynômes de grands degrés satisfaisant le système

$$\forall i,\ \mathrm{Res}(P, P_i) = \pm 1.$$

On peut par exemple se contenter de prendre $P = \prod P_i \pm 1$, et cela donne déjà de bons résultats, mais on peut aussi chercher des solutions moins triviales, et les résultats sont alors encore meilleurs. Expérimentalement, nous avons constaté qu'un bon choix pour les polynômes $P_i$ était de prendre des polynômes totalement réels (contrairement à la situation de la Proposition IV.2.6 où les polynômes cyclotomiques sont totalement complexes), de petits discriminants et si possible tels que leurs résultants soient aussi égaux à $\pm 1$.

**Exemple** : Le plus petit discriminant trouvé pour la signature $d.r_1 = 19.15$ ($(|\operatorname{disc} P|)^{\frac{1}{19}} = 22.880$) a été obtenu pour le polynôme
$P = x^{19} + 9x^{18} + 21x^{17} - 35x^{16} - 195x^{15} - 62x^{14} + 628x^{13} + 552x^{12} - 1004x^{11} - 1173x^{10} + 865x^9 + 1145x^8 - 395x^7 - 528x^6 + 86x^5 + 98x^4 - 7x^3 - 6x^2 + 1$
$= 1 + x^2(x-1)^2(x+1)^2(x+2)(x^2+2x-1)^2(x^2+x-3)(x^3+x^2-3x-1)(x^3+x^2-2x-1).$

D'après sa dernière expression, il est clair que $P$ a un résultant $\pm 1$ avec tous les polynômes $x$, $x-1$, $x+1$, $x+2$, $x^2+2x-1$, $x^2+x-3$, $x^3+x^2-3x-1$ et $x^3+x^2-2x-1$. Tous ces polynômes sont totalement réels et ont des discriminants voisins des minimaux pour leurs signatures. Le grand nombre de racines réelles de ces polynômes a forcé le polynôme $P$ à avoir aussi de nombreuses racines réelles (ici $r_1 = 15$).

La même remarque peut se faire avec le polynôme suivant qui donne le meilleur discriminant ($|\operatorname{disc} P|^{\frac{1}{23}} = 20.400$) pour la signature $d.r_1 = 23.13$ :
$P = x^{23} + 2x^{22} - 21x^{21} - 41x^{20} + 194x^{19} + 366x^{18} - 1038x^{17} - 1866x^{16} + 3564x^{15} + 5988x^{14} - 8220x^{13} - 12564x^{12} + 12951x^{11} + 17334x^{10} - 13887x^9 - 15399x^8 + 9890x^7 + 8350x^6 - 4434x^5 - 2470x^4 + 1120x^3 + 300x^2 - 120x - 1$
$= -1 + x(x-1)(x+1)(x+2)(x^2-x-1)(x^2+x-1)(x^2-2)(x^2-3)(x^3-3x+1)(x^4-4x^2+2)(x^4-5x^2+5)$

**Exemple** : Le polynôme totalement réel $P_0 = x^{14} - 3x^{13} - 9x^{12} + 31x^{11} + 28x^{10} - 122x^9 - 31x^8 + 228x^7 - 6x^6 - 205x^5 + 32x^4 + 78x^3 - 16x^2 - 8x + 1$ (tel que $|\operatorname{disc} P_0|^{\frac{1}{14}} = 22.994$) a un résultant égal à $\pm 1$ avec les polynômes totalement réels suivants (et d'autres encore...) :

| disc | $P_i$ |
|---|---|
| 1 | $x$ |
| 1 | $x-1$ |
| 1 | $x+1$ |
| 1 | $x-2$ |
| 5 | $x^2-x-1$ |
| 5 | $x^2+x-1$ |
| 8 | $x^2-2$ |
| 12 | $x^2-3$ |
| 49 | $x^3-x^2-2x+1$ |
| 49 | $x^3+x^2-2x-1$ |
| 49 | $x^3-2x^2-x+1$ |
| 81 | $x^3-3x-1$ |
| 257 | $x^3-x^2-4x+3$ |
| 725 | $x^4-x^3-3x^2+x+1$ |
| 725 | $x^4-2x^3-2x^2+3x+1$ |
| 2048 | $x^4-4x^2+2$ |
| 2777 | $x^4-5x^2+x+4$ |
| 3981 | $x^4-x^3-5x^2+3x+5$ |
| 14641 | $x^5-x^4-4x^3+3x^2+3x-1$ |
| 24217 | $x^5-5x^3-x^2+5x+1$ |
| 24217 | $x^5-2x^4-3x^3+6x^2-1$ |
| 24217 | $x^5-2x^4-4x^3+7x^2+4x-5$ |
| 36497 | $x^5-x^4-5x^3+3x^2+6x-1$ |
| 65657 | $x^5-x^4-5x^3+4x^2+5x-3$ |
| 81509 | $x^5-x^4-5x^3+3x^2+5x-2$ |
| 371293 | $x^6-x^5-5x^4+4x^3+6x^2-3x-1$ |
| 485125 | $x^6-2x^5-4x^4+8x^3+2x^2-5x+1$ |
| 592661 | $x^6-x^5-5x^4+4x^3+5x^2-2x-1$ |
| 20134393 | $x^7-x^6-6x^5+4x^4+10x^3-4x^2-4x+1$ |
| 32354821 | $x^7-2x^6-5x^5+9x^4+6x^3-8x^2-x+1$ |
| | ... |

On peut remarquer que cette liste contient les discriminants minimaux pour les corps totalement réels de degrés 1, 2, 3, 4, 5 et 7.

**B**– La deuxième méthode consiste à ne considérer qu'un seul polynôme $P_0$ (de grand degré) et à construire d'autres polynômes de même degré (ou de degré voisin) ayant un résultant égal à $\pm 1$ avec $P_0$. Cela peut se faire en construisant les unités du corps de nombres engendré par une racine $\theta$ de $P_0$. On exprime alors ces unités en fonction de $\theta$, ce qui nous donne un polynôme $U$ de degré inférieur au degré de $P_0$, et en général non-unitaire. On peut alors étudier le polynôme $P_0 \pm U$.

**Exemple** : À partir du polynôme $P_0$ de l'exemple précédent, on construit les polynômes suivants de degré 14 et totalement réels :

| $\text{disc}^{\frac{1}{14}}$ | $P_0 + U$ |
|---|---|
| 21.946 | $x^{14} - 3x^{13} - 10x^{12} + 34x^{11} + 36x^{10} - 150x^9 - 52x^8 + 324x^7$ $+11x^6 - 351x^5 + 38x^4 + 170x^3 - 25x^2 - 23x + 1$ |
| 22.902 | $x^{14} - 3x^{13} - 10x^{12} + 32x^{11} + 39x^{10} - 132x^9 - 74x^8 + 262x^7$ $+67x^6 - 251x^5 - 19x^4 + 99x^3 - 6x^2 - 9x + 1$ |
| 23.074 | $x^{14} - 4x^{13} - 6x^{12} + 38x^{11} + 3x^{10} - 137x^9 + 44x^8 + 234x^7$ $-103x^6 - 193x^5 + 82x^4 + 69x^3 - 22x^2 - 8x + 1$ |
| 23.301 | $x^{14} - 4x^{13} - 7x^{12} + 41x^{11} + 10x^{10} - 164x^9 + 33x^8 + 321x^7$ $-120x^6 - 311x^5 + 134x^4 + 126x^3 - 52x^2 - 8x + 1$ |
| 23.426 | $x^{14} - x^{13} - 13x^{12} + 10x^{11} + 67x^{10} - 36x^9 - 172x^8 + 55x^7$ $+226x^6 - 30x^5 - 140x^4 - x^3 + 33x^2 + 3x - 1$ |
| 23.489 | $x^{14} - 4x^{13} - 6x^{12} + 38x^{11} + 3x^{10} - 138x^9 + 47x^8 + 238x^7$ $-120x^6 - 193x^5 + 110x^4 + 58x^3 - 36x^2 + 1$ |
| 23.865 | $x^{14} - 3x^{13} - 9x^{12} + 30x^{11} + 30x^{10} - 114x^9 - 47x^8 + 206x^7$ $+38x^6 - 179x^5 - 19x^4 + 65x^3 + 7x^2 - 6x - 1$ |
| 23.869 | $x^{14} - 3x^{13} - 11x^{12} + 35x^{11} + 49x^{10} - 162x^9 - 114x^8 + 375x^7$ $+147x^6 - 448x^5 - 99x^4 + 253x^3 + 26x^2 - 49x + 1$ |
| 23.938 | $x^{14} - 3x^{13} - 9x^{12} + 31x^{11} + 27x^{10} - 120x^9 - 24x^8 + 214x^7$ $-21x^6 - 173x^5 + 40x^4 + 53x^3 - 14x^2 - 4x + 1$ |

Ce même exemple a permis de construire des centaines d'autres polynômes en toutes signatures (avec toujours $r_1$ grand).

**Domaine d'Utilisation de la Méthode** : Ces méthodes permettent de trouver des polynômes ayant de nombreuses racines réelles dès lors que les polynômes utilisés dans la construction ont eux-mêmes de nombreuses racines réelles. Les exemples précédents montrent que l'on peut trouver ainsi quelques polynômes dont le degré atteint 23 (et même 25). Pour des degrés inférieurs, on peut obtenir de nombreux polynômes, et cette méthode s'avère donc particulièrement adaptée aux signatures réelles pour les degrés de l'ordre de 14.

La principale difficulté de la méthode A est la résolution du système algébrique $\text{Res}(P, P_i) = \pm 1$, et les degrés des polynômes ainsi construits sont au plus de l'ordre d'une dizaine. Si l'on se contente d'une construction de la forme $\prod P_i \pm 1$, on peut doubler les degrés obtenus.

La difficulté de la seconde méthode est la recherche des unités fondamentales du corps de nombres défini par $P_0$, puis le grand nombre d'unités à regarder. On peut ainsi atteindre le degré 15. En ce qui concerne les unités fondamentales, on peut peut-être se contenter d'avoir beaucoup d'unités, quel que soit le moyen de les obtenir. Un premier moyen consiste à factoriser le polynôme $P_0 \pm U$ où $U(\theta)$ est déjà une unité, et en commençant par exemple à partir de $U = 1$. Un deuxième moyen consiste simplement à regarder parmi les polynômes de petits discriminants déjà trouvés si certains ont un résultant 1 avec $P_0$. Ce dernier moyen est efficace si l'on admet le principe qui gouverne toute cette méthode, à savoir que les

polynômes de petits discriminants ont souvent des résultants égaux à $\pm 1$.

### IV.2.2 Polynômes Factorisables

Dans cette partie, nous donnons les plus petits discriminants pour les polynômes factorisables.

**Proposition IV.2.7** *Soient $P_1,\ldots,P_n$ des polynômes de degré 1, et $p \leqslant n-2$ un nombre premier. Le discriminant de $\prod P_i$ est divisible par $p^{2(n-p-1)}$.*

*En particulier, si $n \geqslant 4$ le discriminant est divisible par $4^{n-3}$, et si $n \geqslant 5$ le discriminant est divisible par $9^{n-4}$.*

*Preuve :* On commence par le montrer pour $n = p+2$. Dans ce cas, lorsque l'on réduit modulo $p$, il n'y a que $p+1$ réductions possibles à une constante inversible près : $1, x, x+1, \ldots, x+p-1$. Ainsi, parmi les $n = p+2$ polynômes, il en existe au moins deux qui ont la même réduction modulo $p$, et leur résultant est divisible par $p$.

Lorsque l'on a $n \geqslant p+2$ polynômes, une simple récurrence (sur $n$) permet de montrer qu'il y a au moins $n-p-1$ résultants qui sont divisibles par $p$. Comme les résultants interviennent au carré dans le discriminant du produit, on a le résultat annoncé. ■

Comme application immédiate de cette proposition, on montre que les discriminants minimaux de produits de facteurs linéaires sont donnés jusqu'au degré 5 par

| $d$ | disc | polynôme |
|---|---|---|
| 1 | 1 | $x$ |
| 2 | 1 | $x(x-1)$ |
| 3 | 1 | $x(x-1)(2x-1)$ |
| 4 | 4 | $x(x-1)(2x-1)(3x-1)$ |
| 5 | 144 | $x(x-1)(2x-1)(3x-1)(4x-1)$ |

Contrairement à ce que pourrait laisser croire ce tableau, le polynôme $P = x(x-1)(2x-1)(3x-1)(4x-1)(5x-1)$ ne donne pas le discriminant minimum pour le degré 6. En effet, le discriminant de $P$ vaut 82944, alors que le discriminant de $Q = x(x-1)(2x-1)(3x-1)(4x-1)(5x-2)$ ne vaut que 46656.

Bien que cela ne soit pas complètement nécessaire, nous introduisons ici la notion d'*unité exceptionnelle*, qui nous permet de traduire dans un autre langage la propriété qu'ont certains polynômes d'avoir des résultants égaux à $\pm 1$. Nous reviendrons sur cette traduction à propos des polynômes fortement premiers entre eux. Dans ce paragraphe, nous utilisons cette notion uniquement pour montrer que certains résultants ne sont pas triviaux.

**Définition** : On dit qu'une unité $\theta$ d'un corps de nombres $K$ est une *unité exceptionnelle* si $1-\theta$ est aussi une unité de $K$.

**Proposition IV.2.8** *Soient $P_1$,$P_2$ et $P_3$ trois polynômes linéaires, et $Q$ un polynôme irréductible de degré au moins 2. Si les quatre polynômes sont fortement premiers entre eux (i.e. si tous les résultants deux à deux sont égaux à $\pm 1$), alors le corps $K = \mathbb{Q}(\alpha)$ engendré par une racine $\alpha$ de $Q$ contient une unité exceptionnelle.*

*Les seules unités exceptionnelles de degré 2 sont les racines des polynômes* $x^2 \pm x - 1$, *et* $x^2 - (2 \pm 1)x + 1$, *dont les discriminants sont* $-3$ *et* $5$.

*Preuve :* Quitte à faire une transformation de $GL_2(\mathbb{Z})$ (qui ne change pas les résultants, ni le corps $K$), on peut toujours supposer que $P_1 = x$. Les autres polynômes sont alors de la forme

$$\begin{aligned} P_2 &= ax + 1 \\ P_3 &= (a+1)x + 1 \\ Q(0) &= 1 \end{aligned}$$

Si on prend les polynômes réciproques, (ce qui est une transformation de $GL_2(\mathbb{Z})$), les nouveaux polynômes sont de la forme

$$\begin{aligned} P_2' &= x + a \\ P_3' &= x + a + 1 \end{aligned}$$

et $Q'$ est un polynôme unitaire. On peut faire le changement de variables $y = x + a + 1$ (qui est encore une transformation de $GL_2(\mathbb{Z})$), et on trouve les polynômes $x$, $x - 1$ et $Q''$ dont les résultants sont $\pm 1$. Si $\beta$ est une racine de $Q''$ (qui est dans le corps $K$), c'est une unité car $Q''$ est unitaire et son résultant avec $x$ est 1. Enfin $1 - \beta$ est aussi une unité puisque sa norme est $\mathrm{Res}(x - 1, Q'') = \pm 1$.

Si $P = x^2 + ax + b$, les relations $\mathrm{Res}(P, x) = \pm 1$ et $\mathrm{Res}(P, x - 1) = \pm 1$ forment un système linéraire à deux inconnues et deux équations, dont les solutions donnent les polynômes annoncés. ■

Le théorème que nous démontrons maintenant donne les discriminants minimaux pour chaque signature jusqu'au degré 7. Nous remarquons que tous les discriminants minimaux sont atteints par des polynômes non irréductibles (sauf pour la signature $d.r_1 = 2.0$ pour une raison évidente). Remarquons aussi que pour chaque degré, le plus petit discriminant est atteint lorsque $r_1 = 2$ ou 3, contrairement au cas des polynômes irréductibles où le plus petit discriminant est atteint pour $r_1 = 0$ ou 1.

La preuve utilise essentiellement les Propositions IV.1.2 et IV.2.7, ainsi que la connaissance des discriminants minimaux des polynômes irréductibles jusqu'au degré 7.

**Théorème V** *Les discriminants donnés dans le tableau suivant sont les discriminants minimaux pour chaque signature.*

| $d.r_1$ | disc | $\sqrt[d]{\lvert\text{disc}\rvert}$ | polynôme |
|---|---|---|---|
| 1.1 | 1 | 1.000 | $x$ |
| 2.0 | $-3$ | 1.732 | $x^2+x+1$ |
| 2.2 | 1 | 1.000 | $x(x-1)$ |
| 3.1 | $-3$ | 1.442 | $x(x^2+x+1)$ |
| 3.3 | 1 | 1.000 | $x(x-1)(2x-1)$ |
| 4.0 | 12 | 1.861 | $(x^2+1)(x^2-x+1)$ |
| 4.2 | $-3$ | 1.316 | $x(x-1)(x^2-x+1)$ |
| 4.4 | 4 | 1.414 | $x(x-1)(2x-1)(3x-1)$ |
| 5.1 | 12 | 1.644 | $x(x^2+1)(x^2-x+1)$ |
| 5.3 | $-3$ | 1.246 | $x(x-1)(2x-1)(3x^2-3x+1)$ |
| 5.5 | 5 | 1.380 | $x(x-1)(2x-1)(x^2+x-1)$ |
| 6.0 | $-180$ | 2.376 | $(x^2+1)(x^2+x+1)(2x^2+x+2)$ |
| 6.2 | 12 | 1.513 | $x(x-1)(x^2-x+1)(2x^2-2x+1)$ |
| 6.4 | $-23$ | 1.686 | $x(x-1)(2x-1)(x^3-x^2+2x-1)$ |
| 6.6 | 20 | 1.647 | $x(x-1)(2x-1)(3x-1)(x^2-3x+1)$ |
| 7.1 | $-276$ | 2.232 | $(x^2+1)(x^2-x+1)(x^3-x^2+2x-1)$ |
| 7.3 | 48 | 1.738 | $x(x-1)(2x-1)(2x^2-2x+1)(3x^2-3x+1)$ |
| 7.5 | $-92$ | 1.908 | $x(x-1)(2x-1)(3x-1)(7x^3-11x^2+6x-1)$ |
| 7.7 | 160 | 2.065 | $x(x-1)(x+1)(2x^2-1)(x^2+x-1)$ |

*Preuve :* Dans cette preuve, nous regardons chaque signature séparément.

Comme le discriminant est entier non nul, il est toujours supérieur ou égal à 1 en valeur absolue. Pour les signatures $\mathbf{d.r_1} = \mathbf{1.1},\ \mathbf{2.2},\ \mathbf{3.3}$, on a donc le minimum.

Pour les signatures $\mathbf{d.r_1} = \mathbf{2.0},\ \mathbf{3.1},\ \mathbf{4.2},\ \mathbf{5.3}$, on a toujours $r_2 = 1$, et les discriminants sont donc négatifs d'après la Proposition IV.1.1. Comme ils sont congrus à 0 ou 1 modulo 4, il est clair que $-3$ est la meilleure valeur possible.

Dorénavant, et jusqu'à la fin de cette démonstration, par discriminant, nous entendrons toujours la valeur absolue du discriminant du polynôme.

Un polynôme de signature $\mathbf{d.r_1} = \mathbf{4.0}$ est soit irréductible, soit le produit de deux irréductibles de signature 2.0. Dans le premier cas, le discriminant est au moins égal à 117. Dans le deuxième cas, notons $P = P_1P_2$. Le discriminant de $P$ est égal à $\text{disc}(P_1)\,\text{disc}(P_2)\,\text{Res}^2(P_1,P_2)$. Le produit des deux discriminants est au moins égal à $3{\cdot}3 = 9$. La seule possibilité pour obtenir un discriminant strictement plus petit que 12 est d'avoir $\text{Res}(P_1,P_2) = \pm 1$ et $|\,\text{disc}(P_1)| = |\,\text{disc}(P_2)| = 3$, on aurait alors $\text{disc}(P) = 9$. Or, d'après le Corollaire IV.1.3, ceci est impossible. De là, on déduit que 12 est le discriminant minimal pour cette signature.

Si un polynôme de signature $\mathbf{d.r_1} = \mathbf{4.4}$ est divisible par un polynôme irréductible de degré au moins 2, alors son discriminant est divisible par un entier au moins égal à 5 (qui est le discriminant minimal pour un polynôme irréductible de signature 2.2). Tout polynôme de discriminant inférieur est donc le produit de quatre facteurs linéaires. Or, d'après la Proposition IV.2.7 le discriminant d'un tel produit est au moins égal à 4, ce qui est le cas de notre polynôme.

Soit $P$ un polynôme de signature $\mathbf{d.r_1 = 5.1}$ et de discriminant inférieur à 12. Il ne peut avoir de facteur irréductible de degré 3, 4 ou 5, sinon ce facteur imposerait que le discriminant soit au moins égal à 23. Les facteurs irréductibles de $P$ sont donc de degré au plus 2. Comme 5 est impair, au moins un des facteurs est de degré 1. En fait, il n'y a qu'un seul facteur linéaire, car $P$ n'a qu'une seule racine réelle. Le polynôme $P$ est donc de la forme $P_1P_2P_3$ où $P_1$ est de degré 1, et $P_2$ et $P_3$ de signature 2.0. Le résultat pour la signature 4.0 montre que $P_1P_2$ est de discriminant au moins 12. L'exemple donné montre alors que 12 est le minimum.

Soit $P$ un polynôme de signature $\mathbf{d.r_1 = 5.5}$ de discriminant plus petit que 5. $P$ ne peut pas avoir cinq facteurs linéaires à cause de la Proposition IV.2.7. Ainsi, $P$ possède au moins un facteur irréductible de degré 2, et donc son discriminant est au moins 5.

Montrons que le discriminant 180 est le minimum pour la signature $\mathbf{d.r_1 = 6.0}$. Soit $P$ un polynôme de cette signature dont le discriminant est plus petit. Comme toutes ses racines sont complexes, tous ses facteurs irréductibles sont de degré pair. Si $P$ est irréductible, alors son discriminant vaut au moins 9747. Si $P$ a un facteur irréductible de degré 4, alors ce facteur a un discriminant au moins égal à 117, mais le facteur de degré 2 restant a un discriminant au moins égal à 3, et donc le discriminant de $P$ est supérieur à 351. Il ne nous reste plus qu'à regarder le cas où $P$ a trois facteurs $P_1$,$P_2$ et $P_3$ de signature 2.0. Supposons que $D_1 = |\operatorname{disc} P_1|$ soit le plus petit discriminant, et que $D_3 = |\operatorname{disc} P_3|$ soit le plus grand. Comme le discriminant de $P$ est inférieur à 180, alors $D_1$ vaut 3 ou 4. Si $D_1 = 4$ alors les résultants des trois polynômes sont tous égaux à 1, sinon le discriminant de $P$ serait plus grand que 256. Mais le Corollaire IV.1.3 montre que les discriminants ne peuvent pas être égaux, et donc le discriminant de $P$ vaut au moins $4 \cdot 7 \cdot 8 = 224$. Il nous reste à regarder le cas où $D_1 = 3$. Si deux facteurs ont le même discriminant (négatif), alors leur résultant vaut au moins 4 d'après le Corollaire IV.1.3, et le discriminant de $P$ vaut au moins $3^2 \cdot 4^2 = 432$. Cela prouve que les trois polynômes ont des discriminants différents, qui valent au moins 3, 4 et 7. Comme le discriminant de $P$ est inférieur à 180, alors les résultants des trois polynômes sont égaux à 1, et $D_3$ est inférieur à 15. Comme $P_1$ et $P_2$ ont un résultant égal à 1, alors le Corollaire IV.1.3 montre que $D_2$ vaut 4 ou 15. Cela est également vrai pour $D_3$. Ainsi, le meilleur discriminant possible est 180, atteint par notre exemple avec $D_1 = 3$, $D_2 = 4$ et $D_3 = 15$.

Soit $P$ un polynôme de signature $\mathbf{d.r_1 = 6.2}$. Si $P$ a un facteur irréductible de degré au moins 3, alors son discriminant vaut au moins 23. Si $P$ n'a que des facteurs de degré égal à 2, alors son discriminant vaut au moins $3 \cdot 3 \cdot 5 = 45$. Dans le dernier cas, $P$ a deux facteurs irréductibles $P_1$ et $P_2$ de signature 2.0, et deux facteurs linéaires. Le résultat pour la signature 4.0 montre que le discriminant de $P_1P_2$ est au moins 12. Ceci prouve que notre exemple donne le plus petit discriminant possible.

Pour la signature $\mathbf{d.r_1 = 6.4}$, supposons qu'il existe un polynôme $P$ de discriminant inférieur à 23. Ce polynôme ne peut avoir de facteur irréductible de degré 3 ou plus, sinon son discriminant serait supérieur à 23. Si tous les facteurs irréductibles de $P$ étaient de degré 2, alors son discriminant serait supérieur à $3 \cdot 5 \cdot 5 = 75$. S'il y a deux facteurs irréductibles $P_1$ et $P_2$ de degré 2, alors ils sont de signature 2.0 et 2.2 et de discriminant $|D_1| \geqslant 3$ et $D_2 \geqslant 5$. Or, le Corollaire IV.1.3 montre que le résultant de ces deux polynômes vérifie l'inégalité

$4\,\mathrm{Res}(P_1,P_2) \geqslant D_1D_2 \geqslant 15$. Dans ce cas, le résultant vaut au moins 4, et le discriminant de $P$ vaut au moins $3\cdot 5\cdot 4^2 = 240$. Il ne reste plus qu'à regarder le cas où $P$ a quatre facteurs linéaires $P_1,\ldots,P_4$ et un facteur irréductible $P_5$ de signature 2.0. S'il y a $r$ résultants supérieurs ou égaux à 2 entre les $P_i$, alors on a l'inégalité $3\cdot 4^r < 23$, ce qui implique $r = 0$ ou 1. Mais il y a au moins un résultant supérieur à 2 entre les facteurs linéaires. On a donc $r = 1$. Supposons que $\mathrm{Res}(P_1,P_2) > 1$, alors en posant $Q = P_1P_2$, on a $\mathrm{disc}\,Q = \mathrm{Res}^2(P_1,P_2) \geqslant 4$. La Proposition IV.1.2 affirme alors que $4\,\mathrm{Res}(P_5,Q) = \delta^2 + |\,\mathrm{disc}(Q)\,\mathrm{disc}(P_5)| \geqslant 12$. Ceci implique que $P_5$ a un résultant au moins égal à 3 avec $Q$, et donc au moins égal à 2 avec l'un des $P_i$. Comme ceci est en contradiction avec le fait que $r = 1$, on déduit que le discriminant minimal pour la signature $d.r_1 = 6.4$ est 23.

Pour la signature $\mathbf{d.r_1 = 6.6}$, supposons qu'il existe un polynôme $P$ de discriminant inférieur à 20. Ce polynôme ne peut avoir de facteur irréductible de degré 3 ou plus, sinon son discriminant serait supérieur à 23. Donc, tous les facteurs irréductibles de $P$ sont de degré au plus 2. Si $P$ a au moins un facteur irréductible de degré 2, alors il est de signature 2.2, et son discriminant est au moins 5. La facteur restant est de signature 4.4, non nécessairement irréductible. Le résultat pour cette signature montre que son discriminant est au moins 4. Dans ce cas, le discriminant de $P$ est donc au moins égal à $4\cdot 5 = 20$. Il ne reste plus que le cas où $P$ n'a que des facteurs linéaires. Dans ce dernier cas, la Proposition IV.2.7 montre que le discriminant de $P$ est au moins $4^3 = 64$. Ceci prouve que 20 est bien le discriminant minimal pour cette signature.

Pour la signature $\mathbf{d.r_1 = 7.1}$, supposons qu'il existe un polynôme $P$ de discriminant inférieur à 276. Ce polynôme ne peut avoir de facteur irréductible de degré 5 ou plus, sinon son discriminant serait supérieur à 1609. S'il contient un facteur irréductible de degré 4, alors le discriminant de ce facteur est au moins 117, et le facteur restant (non nécessairement irréductible) est de signature 3.1, donc de discriminant au moins 3, ainsi, le polynôme $P$ a un discriminant au moins $117\cdot 3 = 351$. Nous sommes maintenant dans le cas où les facteurs irréductibles de $P$ sont de degré au plus 3. Si $P$ a un tel facteur de degré 3, alors le facteur restant est de signature 4.0, et le résultat pour cette signature impose que le discriminant de $P$ soit au moins égal à $23\cdot 12 = 276$. Il ne reste plus qu'à regarder le cas où tous les facteurs irréductibles de $P$ sont de degré au plus 2. Dans ce cas, les racines complexes forcent $P$ à être le produit de trois polynômes irréductibles $P_1,\ldots,P_3$ de signature 2.0 et d'un polynôme linéaire $P_4$. Le Corollaire IV.1.3 montre que si deux des trois polynômes $P_1$, $P_2$, $P_3$ ont le même discriminant, alors leur résultant est supérieur à 4, et le discriminant de $P$ est au moins égal à $3^3\cdot 4^2 > 276$. Il faut encore regarder le cas où les trois polynômes $P_1$, $P_2$ et $P_3$ ont des discriminants différents. Notons $r$ le nombre de résultants non égaux à 1 entre les $P_i$. On a la majoration $3\cdot 4\cdot 7\cdot 4^r < 276$, ce qui implique que $r = 0$. Les relations alors imposées par la Proposition IV.1.2 montrent que ces discriminants ne peuvent prendre que les valeurs 3, 4 et 15. Quitte à faire une transformation de $SL_2(\mathbb{Z})$ (qui laisse invariants les discriminants et les résultants), on peut supposer que $P_4 = x$. Ainsi, les autres polynômes sont de la forme $P_i = a_ix^2 + b_ix + 1$. On a les relations $b_1^2 - 4a_1 = -3$, $b_2^2 - 4a_2 = -4$, et $b_3^2 - 4a_3 = -15$. Si l'on remplace $a_i$ par son expression en fonction de $b_i$ dans le résultant de $P_2$ et $P_3$, on trouve la relation $(b_2 - b_3)^2 + 19 = \pm 16$, qui est impossible. Nous devons donc conclure que le plus petit discriminant possible pour la signature $d.r_1 = 7.1$ est 276.

Étudions le cas de la signature $\mathbf{d.r_1 = 7.3}$, et supposons qu'il existe un polynôme de discriminant inférieur à 48. S'il a un facteur irréductible de degré au moins 4, alors son discriminant est au supérieur à 117. S'il contient un facteur irréductible de degré 3, alors le discriminant de ce facteur est au moins égal à 23, mais parmi les facteurs restants, il y en au moins un qui a deux racines complexes, et dont le discriminant est supérieur ou égal à 3, ce qui montre que le discriminant de $P$ est au moins égal à $23 \cdot 3 = 69$. Regardons maintenant le dernier cas où tous les facteurs irréductibles de $P$ sont de degré inférieur ou égal à 2. Il y a au moins deux facteurs irréductibles de signature 2.0, et le discriminant de leur produit est au moins égal à 12. S'il y a un autre facteur de degré 2, alors il est de signature 2.2, et son discriminant est au moins 5, ce qui rend le discriminant de $P$ supérieur ou égal à $12 \cdot 5 = 60$. Nous avons donc trois facteurs $P_1$,$P_2$ et $P_3$ de degré 1, et deux facteurs $P_4$ et $P_5$ de signature 2.0. Si $P_4$ et $P_5$ ont le même discriminant, alors leur résultant est supérieur à 4, et le discriminant de $P$ est supérieur à $3^3 \cdot 4^2 = 144$, mais ceci est contraire à l'hypothèse, donc ces deux discriminants sont différents. Notons $r$ le nombre de résultants supérieurs à 2 entre les $P_i$. On a la majoration $12 \cdot 4^r < 48$, qui implique que $r = 0$. La Proposition IV.2.8 montre alors que les discriminants de $P_4$ et $P_5$ devraient être égaux, ce qui n'est pas le cas. Ainsi, 48 est le discriminant minimal pour la signature $d.r_1 = 7.3$.

Pour la signature $\mathbf{d.r_1 = 7.5}$, supposons que $P$ est un polynôme de discriminant inférieur à 92. Il ne peut pas avoir de facteur irréductible de degré supérieur à 4, sinon son discriminant serait supérieur à 117. Si $P$ avait un facteur irréductible de signature 3.3, alors il aurait aussi un facteur de signature 2.0, et donc son discriminant serait au moins égal à $49 \cdot 3 = 147$. De même, si $P$ avait un facteur de signature 3.1, alors le facteur restant serait de signature 4.4, et le résultat pour cette signature montrerait que le discriminant de $P$ serait au moins égal à $23 \cdot 4 = 92$. Ainsi, tous les facteurs irréductibles de $P$ sont de degré au plus 2. Il existe exactement un facteur $P_1$ de signature 2.0. Le discriminant de $P_1$ est au moins 3. Notons $P = P_1P_2$. Le polynôme $P_2$ est de signature 5.5. Si $P_2$ est un produit de cinq facteurs linéaires, alors la Proposition IV.2.7 montre que son discriminant est divisible par $4^2 \cdot 9 = 144$, ce qui est supérieur à 92. Si $P_2$ a un facteur irréductible $P_3$ de degré 2, et de signature 2.2, alors la Proposition IV.1.2 montre que le résultant de $P_1$ et $P_3$ est au moins égal à 4, et comme le discriminant de $P_3$ est au moins 5, le discriminant de $P$ est supérieur ou égal à $3 \cdot 5 \cdot 4^2 = 240$. Il ne reste plus qu'à regarder le cas où $P_2$ possède deux facteurs irréductibles $P_3$ et $P_4$ de degré 2 et un facteur linéaire. Si $P_3$ et $P_4$ ont le même discriminant, alors leur résultant est au moins égal à 4, et le discriminant de $P$ est supérieur à $3 \cdot 5^2 \cdot 4^2 = 1200$. Si enfin les discriminants de $P_3$ et $P_4$ sont distincts, alors le discriminant de $P$ est au moins égal à $3 \cdot 5 \cdot 8 = 120$. Dans tous les cas, nous avons montré que le discriminant de $P$ est au moins égal à 92.

Il ne reste plus qu'à étudier le cas de la signature $\mathbf{d.r_1 = 7.7}$. Supposons que $P$ a un discriminant inférieur à 160. Il ne peut pas avoir de facteur irréductible de degré supérieur à 4, sinon son discriminant serait supérieur à 725. Si $P$ avait un facteur irréductible de degré 3, alors le facteur restant serait de signature 4.4, et le résultat pour cette signature montrerait que le discriminant de $P$ serait au moins égal à $49 \cdot 4 = 196$. Il nous reste à regarder les cas où les facteurs irrductibles de $P$ sont de degré au plus 2. Notons $n$ le nombre de facteurs linéaires de $P$. Si $n = 7$, alors la Proposition IV.2.7 montre que le discriminant

de $P$ est divisible par $4^4 \cdot 9^3 \cdot 25 > 160$. Si $n = 5$, alors la même proposition montre que le discriminant de $P$ est au moins égal à $5 \cdot 4^2 \cdot 9 = 720$. Si $n = 1$, alors chaque facteur irréductible a un discriminant au moins égal à 5. Si l'un de ces discriminants est plus grand que 5, alors il vaut au moins 8, et alors le discriminant de $P$ est au moins égal à $5^2 \cdot 8 = 200$. Si en revanche, tous les discriminants sont égaux à 5, alors les résultants sont au moins égaux à 4, et le discriminant de $P$ est bien supérieur à 160. Regardons enfin le cas $n = 3$. Si les trois facteurs linéaires sont de résultants 1 entre eux, alors on est dans la situation de la Proposition IV.2.8, qui montre que les discriminants des deux facteurs de degré 2 sont égaux à 5. Dans ce cas, ces deux facteurs ont un résultant au moins égal à 4, et le discriminant de $P$ est au moins égal à $5^2 \cdot 4^2 = 400$. Si les trois facteurs linéaires ont un résultant supérieur à 2, alors le discriminant de leur produit est au moins 4. Le discriminant du produit des deux facteurs de degré 2 est au moins égal à $5^2 \cdot 4^2 = 200$ lorsque leurs discriminants sont égaux, et au moins égal à $5 \cdot 840$ lorsqu'ils sont différents. Dans tous les cas, on trouve que le discriminant de $P$ est au moins égal à $40 \cdot 4 = 160$. ■

## IV.3 Comportement Asymptotique des Petits Discriminants

Dans cette partie, nous essayons de trouver des familles infinies de polynômes $\{P_n\}$ ayant des petits discriminants $D_n = |\operatorname{disc} P_n|$. Nous nous plaçons dans le cas où $d_n = \deg P_n$ tend vers $+\infty$, et nous regardons l'expression $D_n^{1/d_n}$ lorsque $n$ tend vers $+\infty$.

Un exemple particulièrement simple de famille infinie de polynômes est la famille $P_n = x^n - 1$. Pour cette famille, on a $d_n = n$, et $D_n = n^n$. Cela s'exprime sous la forme :

$$D_n^{1/d_n} = d_n.$$

Le polynôme $P_n = x^n - 1$ est en général très factorisable. Les polynômes cyclotomiques $\Phi_p$ où $p$ est un nombre premier donnent des discriminants du même ordre de grandeur pour des polynômes irréductibles. En effet, on a $\operatorname{disc}(\Phi_p) = p^{p-2}$, et $d_p = p - 1$ ce qui donne

$$D_p^{1/d_p} = (d_p + 1)^{1-1/d_p} \sim d_p.$$

On atteint le même ordre de grandeur à partir du polynôme irréductible $x^n - 2$.

Évidemment, ces deux familles de polynômes donnent des discriminants bien supérieurs aux bornes d'Odlyzko, car celles-ci n'impliquent seulement que

$$D_n^{1/d_n} \geqslant Cte.$$

Toutefois, nous estimerons qu'une famille de polynômes donne des petits discriminants si l'on a

$$D_n^{1/d_n} < d_n.$$

**Notation** : Dans toute cette partie, $p$ désignera toujours un nombre premier $\geqslant 2$.

Dans ce qui suit, presque tous nos exemples sont construits à partir des polynômes cyclotomiques. Pour cette raison, nous leur consacrons un paragraphe.

### IV.3.1 Polynômes Cyclotomiques

Nous utiliserons le résultat suivant sur les discriminants des polynômes cyclotomiques :

**Proposition IV.3.1** *Le discriminant du polynôme cyclotomique $\Phi_n$ de degré $\phi(n)$ est donné par*

$$|\operatorname{disc}\Phi_n|^{1/\phi(n)} = n\prod_{p|n} p^{-\frac{1}{p-1}} = \phi(n)\prod_{p|n}\left(\frac{p^{1-\frac{1}{p-1}}}{p-1}\right)$$

*où $\phi(n)$ est l'indicateur d'Euler.*

*Preuve :* Voir [Was][p.12]. ■

**Proposition IV.3.2** *Soient $m$ et $n$ deux entiers tels que $1 < m < n$ et $m \nmid n$. Alors, on a*

$$\operatorname{Res}(\Phi_m, \Phi_n) = \pm 1.$$

*Preuve :* Soit $a = (m,n)$ le *pgcd* de $m$ et $n$, et notons $m = am'$ et $n = an'$. Les relations $\Phi_m(x) \mid \Phi_{m'}(x^a)$ et $\Phi_n(x) \mid \Phi_{n'}(x^a)$ montrent que $\operatorname{Res}(\Phi_m, \Phi_n) \mid \operatorname{Res}(\Phi_{m'}(x^a), \Phi_{n'}(x^a))$. Mais on a aussi $\operatorname{Res}(\Phi_{m'}(x^a), \Phi_{n'}(x^a)) \mid \operatorname{Res}(\Phi_{m'}(x), \Phi_{n'}(x))^a$. Comme $m \nmid n$ alors on a l'inégalité $1 < m' < n'$, ce qui prouve que l'on s'est ramené au cas où $m$ et $n$ sont premiers entre eux.

Supposons donc maintenant que $m$ et $n$ sont premiers entre eux. On sait déjà que $\operatorname{Res}(\Phi_m, \Phi_n)$ divise $\operatorname{Res}(x^m - 1, \Phi_n)/\operatorname{Res}(x-1, \Phi_n)$. Or, le résultant $\operatorname{Res}(x^m - 1, \Phi_n)$ est, au signe près, la norme de l'élément $\zeta_n^m - 1$ dans l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Comme $m$ est premier à $n$, $\zeta_n^m$ est un conjugué de $\zeta_n$, et $\zeta_n^m - 1$ est un conjugué de $\zeta_n - 1$. En particulier, ces deux éléments ont la même norme. En termes de résultants, ceci signifie que $\operatorname{Res}(x^m - 1, \Phi_n) = \operatorname{Res}(x-1, \Phi_n)$. Nous avons donc montré que $\operatorname{Res}(\Phi_m, \Phi_n) = \pm 1$. ■

**Proposition IV.3.3** *Soient $m$ et $n$ deux entiers tels que $1 \leqslant m < n$. Si $|\operatorname{Res}(\Phi_m, \Phi_n)| > 1$ alors $m \mid n$ et $\frac{m}{n}$ est la puissance d'un nombre premier.*

*Preuve :* D'après la Proposition IV.3.2 on a déjà $m \mid n$. Notons $n = mq$. On a alors

$$\operatorname{Res}(\Phi_m, \Phi_n) \mid \operatorname{Res}(\Phi_1(x^m), \Phi_q(x^m)) \mid \operatorname{Res}(x-1, \Phi_q)^m$$

Rappelons maintenant que si $p$ est un nombre premier, alors $\operatorname{Res}(x-1, \Phi_p) = p$. Ceci montre que si $q = pq'$, alors $\operatorname{Res}(x-1, \Phi_q) \mid \operatorname{Res}(x-1, \Phi_p(x^{q'})) = p$. Ainsi, si $q$ est divisible par deux nombres premiers distincts, le résultant de $x-1$ et $\Phi_q$ est nécessairement trivial. Nous avons donc prouvé la proposition. ■

### IV.3.2 Familles de Polynômes Irréductibles

Nous cherchons ici à étudier la plus petite valeur possible du discriminant d'un polynôme à coefficients entiers de degré $d$ irréductible, et en particulier d'en regarder le comportement lorsque $d$ tend vers $+\infty$.

**Notation** : Nous noterons $M_{irr}(d)$ la valeur minimale de $|\operatorname{disc}(P)|^{1/d}$ lorsque $P$ parcourt l'ensemble des polynômes de $\mathbb{Z}[x]$ irréductibles de degré $d$.

Les bornes de Minkowski (ou d'Odlyzko) montrent qu'il existe une constante $c > 1$ telle que pour tout $d > 1$, on ait l'inégalité $1 < c < M_{irr}(d)$. Cette constante peut être choisie relativement grande si on la remplace par $c+o(1)$. Si l'on regarde les discriminants des corps de nombres, cette inégalité est optimale car il existe des familles de corps de nombres $K_d$ de degré $d$ tendant vers $+\infty$ pour lesquels la suite $|\operatorname{disc}(K)|^{1/d}$ est constante. De telles familles ont été décrites par exemple par J. Martinet dans [Mar a] en exhibant des tours de Hilbert infinies. Pour les polynômes, l'inégalité reste vraie, mais elle n'est peut-être pas optimale, car les indices peuvent rendre les discriminants des polynômes démesurés, y compris lorsque les discriminants des corps de nombres qu'ils définissent restent petits.

Nous proposons des exemples qui donnent des majorations de $M_{irr}(d)$ pour certaines valeurs de $d$. Commençons par donner le résultat simple suivant :

**Proposition IV.3.4** *Soit $P$ un polynôme unitaire à coefficients entiers de degré $d$ et de discriminant $|\operatorname{disc}(P)| = D$. Supposons de plus que $P(0) = \pm 1$. Posons $P_n = P(x^n)$. On a*

$$D_n^{1/d_n} = \frac{D^{1/d}}{d} d_n$$

*De plus, si $P$ est irréductible de degré $d \geqslant 2$, alors il existe une infinité de $n$ pour lesquels $P_n$ est irréductible.*

*Preuve :* Comme $P$ est unitaire, $P_n$ est aussi unitaire, et on a

$$|\operatorname{disc} P_n| = |\operatorname{Res}(P(x^n), nx^{n-1}P'(x^n))|$$

D'où

$$\begin{aligned} |\operatorname{disc} P_n| &= n^{dn}|P(0)|^{n-1}|\operatorname{Res}(P(x^n), P'(x^n))| \\ &= n^{dn}|\operatorname{disc}(P)|^n \end{aligned}$$

Comme on a $d_n = dn$, on obtient l'expression annoncée pour le discriminant.

Si $P$ est un polynôme cyclotomique (différent de $x-1$), alors le choix $n = 2^m$ donne le polynôme $P(x^{2^m})$ qui est irréductible.

Supposons maintenant que $n$ soit un nombre premier assez grand, et que $P$ ne soit pas cyclotomique. Comme $P$ est irréductible de degré $d \geqslant 2$, une racine $\alpha$ de $P$ engendre un corps de nombres $K$ de degré $d$ sur $\mathbb{Q}$. Comme $P(0) = \pm 1$, $\alpha$ est une unité non triviale dans ce corps. Si $n$ est assez grand, alors $\alpha$ ne peut pas être une puissance $n$-ième dans $K$ (car $\alpha$ n'est pas une racine de l'unité) et l'extension $L$ de $K$ engendrée par une racine $\beta$ de $x^n - \alpha = 0$ est non triviale de degré $n$. Le corps $L$ est donc de degré $pd$ sur $\mathbb{Q}$ engendré par l'élément primitif $\beta$. Comme $\beta$ est une racine du polynôme $P(x^n)$, ce polynôme est irréductible. ■

**Remarque** : Dans cet exemple, on exhibe une famille de polynômes $P_n$ telle que le rapport $D_n^{1/d_n}/d_n$ soit constant. Cela montre que si l'on peut trouver un polynôme pour lequel le rapport $D^{1/d}/d$ est plus petit que 1, alors on peut en trouver une infinité ayant le même rapport.

Nous donnons maintenant un exemple pour lequel la suite des rapports $D_n^{1/d_n}/d_n$ tend vers 0. Nous considérons ici certains polynômes cyclotomiques dont les indices bien choisis permettent de montrer que leurs discriminants sont petits.

**Proposition IV.3.5** *Soit* $n = \prod_{p \leqslant x} p$, *et* $P_n = \Phi_n$. *Posons* $d_n = \deg P_n$ *et* $D_n = |\operatorname{disc} P_n|$. *Lorsque* $x$ *tend vers* $+\infty$, *on a*

$$D_n^{1/d_n} \sim e^{2\gamma} d_n \frac{\log\log d_n}{\log d_n}$$

*Preuve :* Nous partons de la Proposition IV.3.1 qui nous donne :

$$D_n^{1/d_n} = n \prod_{p \leqslant x} p^{-\frac{1}{p-1}}.$$

On a

$$\log \prod_{p \leqslant x} p^{-\frac{1}{p-1}} = -\sum_{p \leqslant x} \frac{\log p}{p-1}.$$

Une des multiples formes du Théorème des Nombres Premiers affirme que $\sum_{n \leqslant x} \frac{\Lambda(n)}{n} = \log x - \gamma + \mathrm{o}(1)$, où la fonction $\Lambda$ est la fonction de Von Mangoldt, et $\gamma$ la constante d'Euler. On déduit de cette égalité le développement suivant :

$$\sum_{p \leqslant x} \frac{\log p}{p-1} = \log x - \gamma + \mathrm{o}(1).$$

Le Deuxième Théorème de Mertens, plus connu sous le nom de "Formule de Mertens" (voir [Ten][p.17]) donne

$$\frac{\phi(n)}{n} \sim \frac{e^{-\gamma}}{\log x}.$$

Remarquons en particulier que cela implique que $\log n \sim \log \phi(n)$. Nous avons donc

$$D_n^{1/d_n} \sim \phi(n) \exp(-\log x + \gamma + \mathrm{o}(1)) e^{\gamma} \log x \sim e^{2\gamma} \phi(n) \cdot \frac{\log x}{x}.$$

Une autre forme du Théorème des Nombres Premiers est

$$\sum_{p \leqslant x} \log p \sim x,$$

ce qui nous donne $\log \phi(n) \sim \log n \sim x$. De l'égalité précédente, on déduit alors

$$D_n^{1/d_n} \sim e^{2\gamma} \phi(n) \frac{\log\log \phi(n)}{\log \phi(n)}.$$

Il ne reste plus qu'à remplacer $\phi(n)$ par $d_n$ pour obtenir le résultat annoncé. ■

L'exemple que nous venons de donner implique directement le corollaire suivant :

**Corollaire IV.3.6** *Il existe une suite* $d_n$ *tendant vers* $+\infty$ *telle que*

$$M_{irr}(d_n) \leqslant d_n \frac{\log\log d_n}{\log d_n} \cdot (e^{2\gamma} + \mathrm{o}(1)).$$

Il est intéressant de remarquer que dans l'exemple que nous avons construit pour montrer cette inégalité, les degrés $d_n$ sont très factorisables. De même, dans l'exemple de J. Martinet d'une tour de Hilbert infinie, les degrés sont tous très factorisables (essentiellement des puissances de 2). Dans le cas extrême, pour les degrés premiers, presque rien n'est connu, y compris pour les corps de nombres. En particulier, on ne sait pas si le minimum $M_{irr}(d_n)$ pour les corps de nombres est borné pour les degrés premiers. Aucune conjecture n'est aujourd'hui raisonnable sur cette question. D'autres questions sur le même sujet sont posées par Odlyzko dans [Odl].

### IV.3.3 Polynômes Fortement Premiers Entre Eux

**Définition** : Nous dirons que les polynômes $P_1,\ldots,P_n$ sont *fortement premiers entre eux* si tous les résultants $\mathrm{Res}(P_i,P_j)$ sont égaux à $\pm 1$ pour $i \neq j$.

Si le calcul du résultant de deux polynômes de $\mathbb{Z}[x]$ est une opération algorithmiquement facile (par exemple par l'Algorithme du Sous-Résultant), il est en revanche beaucoup plus difficile de déterminer le résultant par la théorie. Les polynômes cyclotomiques (dont les résultants sont donnés par la Proposition IV.3.3) sont l'un des rares cas où cela est possible.

Il semble difficile de trouver des grandes familles de polynômes fortement premiers entre eux. Ces familles se sont pourtant avérées très utiles dans la recherche de petits discriminants. Nous nous sommes donc intéressés plus particulièrement à décrire de telles familles. Ce problème se pose probablement dans n'importe quel anneau de polynômes (à coefficients dans $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{C}$, ou même dans un corps fini).

Les polynômes fortement premiers entre eux sont liés à la théorie des unités exceptionnelles. Rappelons qu'une unité exceptionnelle d'un corps est un entier algébrique $u$ qui est une unité, et tel que $1-u$ soit encore une unité. Ceci se traduit sur le polynôme minimal $P$ de $u$ par la relation

$$|\,\mathrm{Res}(P,x)| = |\,\mathrm{Res}(P,1-x)| = |\,\mathrm{Res}(x,1-x)| = 1$$

Ainsi, toute unité exceptionnelle définit un triplet de polynômes fortement premiers entre eux. De même, si nous avons $n$ polynômes $P_1,\ldots,P_n$ fortement premiers entre eux tels que $P_1 = x$, alors les racines $u_i$ des polynômes $P_i$ sont des unités à cause de la relation $\mathrm{Res}(P_i,x) = \pm 1$, et forment une suite exceptionnelle car la relation $\mathrm{Res}(P_i,P_j) = \pm 1$ implique que $u_i - u_j$ est encore une unité. On remarque que la condition qui définit les suites exceptionnelles ("$u_i - u_j$ est une unité") est plus faible que la condition $\mathrm{Res}(P_i,P_j) = \pm 1$, qui implique que les $u_i - u_j$ sont des unités, ainsi que toutes les expressions obtenues par conjugaison des $u_i$ et des $u_j$. En utilisant la théorie des unités exceptionnelles et des suites exceptionnelles, H. Lenstra montre que que certains corps sont euclidiens (voir [Len]). Il montre que les corps qui ont des suites exceptionnelles suffisamment longues sont euclidiens. Il se trouve que ces mêmes corps ont toujours des discriminants voisins des minimaux, sans que l'on sache démontrer le lien entre ces deux propriétés.

**Notation** : Notons $R1(d)$ le nombre maximum de polynômes à coefficients entiers de degré au plus $d$ fortement premiers entre eux.

La proposition suivante montre que $R1(d)$ est majoré :

**Proposition IV.3.7** *On a* $R1(d) < 2^{d+1}$.

*Preuve :* Soient $P_1,\ldots,P_n$ des polynômes à coefficients entiers de degré au plus $d$ fortement premiers entre eux. Lorsque l'on réduit ces polynômes modulo 2, ils restent fortement premiers entre eux. En particulier, les réductions des polynômes doivent toutes être distinctes. Or, il n'existe que $2^{d+1}-1$ polynômes de degré au plus $d$ dans $\mathbb{F}_2[x]$, ce qui prouve notre assertion. ■

D'après une suggestion de J-P. Serre, on peut améliorer cette majoration en regardant les facteurs irréductibles des polynômes dans $\mathbb{F}_2[x]$.

**Proposition IV.3.8** *On a*

$$R1(d) \leqslant 1 + \sum_{k\leqslant d} \frac{2^k}{k} \sum_{l\leqslant \frac{d}{k}} \frac{\mu(l)}{l} = \frac{2^{d+1}}{d}\left(1 + \mathrm{O}\left(\frac{1}{d}\right)\right)$$

*où* $\mu(l)$ *désigne la fonction de Moebius.*

*Preuve :* Une application classique de la formule d'inversion de Moebius montre que le nombre de polynômes irréductibles de degré au plus $d$ dans $\mathbb{F}_2[x]$ est donné par

$$\sum_{k\leqslant d} \frac{2^k}{k} \sum_{l\leqslant \frac{d}{k}} \frac{\mu(l)}{l}.$$

Or, si l'on réduit une famille $P_1,\ldots,P_n$ de polynômes fortement premiers entre eux, ils ne peuvent pas avoir de facteurs irréductibles communs. Comme il est possible qu'un polynôme soit congru à 1 modulo 2, on obtient la majoration annoncée.

Il reste à donner un équivalent de cette somme. Posons

$$f(d) = \sum_{k\leqslant d} \frac{2^k}{k} \sum_{l\leqslant \frac{d}{k}} \frac{\mu(l)}{l}$$

et

$$F(d) = \sum_{k\leqslant d} \frac{2^k}{k}.$$

Si l'on sépare dans $f$ les termes pour $\frac{d}{2} < k \leqslant d$, on trouve

$$f(d) = F(d) - F\left(\frac{d}{2}\right) + \sum_{k\leqslant \frac{d}{2}} \frac{2^k}{k} \cdot \sum_{l\leqslant \frac{d}{k}} \frac{\mu(l)}{l}$$

On utilise la majoration $|\sum_{l\leqslant \frac{d}{k}} \frac{\mu(l)}{l}| \leqslant 1$ (on aurait pu se contenter de majorer par $\log d+1$) pour déduire que l'on a

$$f(d) = F(d) - F\left(\frac{d}{2}\right) + \mathrm{O}\left(F\left(\frac{d}{2}\right)\right) = F(d) + \mathrm{O}\left(F\left(\frac{d}{2}\right)\right).$$

Il n'y a plus qu'à donner un équivalent de la fonction $F$. Une sommation par parties donne

$$\begin{aligned} F(d) =& \sum_{k \leqslant d} \frac{2^k}{k} \\ =& \frac{2^{d+1}}{d} - \sum_{1 \leqslant k \leqslant d} \left( \frac{1}{k} - \frac{1}{k+1} \right) 2^{k+1} + \mathrm{O}(1) \end{aligned}$$

Or, le terme à l'intérieur de la somme est majoré par $\frac{2^{k+1}}{k^2}$, et donc la somme est $\mathrm{O}\left(\frac{2^d}{d^2}\right)$. On déduit alors que

$$F(d) = \frac{2^{d+1}}{d} + \mathrm{O}\left(\frac{2^d}{d^2}\right),$$

et que

$$f(d) = F(d) + \mathrm{O}\left(\frac{2^{\frac{d}{2}}}{d}\right) = \frac{2^{d+1}}{d} + \mathrm{O}\left(\frac{2^d}{d^2}\right),$$

ce qui donne l'équivalent annoncé dans la proposition. ■

Une lecture attentive de la démonstration fait apparaître que l'on a seulement majoré le nombre de polynômes dont les résultants deux à deux sont impairs. Comme la condition d'être fortement premiers entre eux est beaucoup plus restrictive, il est probable que cette majoration puisse être améliorée. Toutefois, lorsque l'on prend $d = 1$, 2, 3 ou 4 on trouve les inégalités $R1(1) \leqslant 3$, $R1(2) \leqslant 4$, $R1(3) \leqslant 6$ et $R1(4) \leqslant 9$, qui sont optimales comme le montre la famille de polynômes fortement premiers entre eux donnée dans le tableau suivant :

| $d.r_1$ | disc | polynôme |
|---|---|---|
| 1.1 | 1 | $x$ |
| 1.1 | 1 | $x-1$ |
| 1.1 | 1 | $2x-1$ |
| 2.2 | 5 | $x^2+x-1$ |
| 3.3 | 49 | $x^3+3x^2-4x+1$ |
| 3.3 | 49 | $x^3-6x^2+5x-1$ |
| 4.4 | 725 | $x^4-6x^2+5x-1$ |
| 4.2 | $-283$ | $7x^4-5x^3-5x^2+5x-1$ |
| 4.2 | $-507$ | $3x^4+3x^3-10x^2+6x-1$ |

Ainsi, on a

$$R1(1) = 3 \qquad R1(2) = 4$$
$$R1(3) = 6 \qquad R1(4) = 9$$

Les polynômes cyclotomiques fournissent une minoration non constante de $R1(d)$ :

**Proposition IV.3.9** *On a l'inégalité suivante :*

$$\frac{d+1}{2} + 1 \leqslant R1(d).$$

*Preuve :* Si l'on considère les polynômes cyclotomiques $\Phi_n$ pour $\frac{d+1}{2} < n \leqslant d+1$, on a une famille de $N$ polynômes de degré au plus $d$ avec $N \geqslant \frac{d+1}{2}$. Si $\frac{d+1}{2} < n < n' \leqslant d+1$ alors $n$ ne peut pas diviser $n'$ et la Proposition IV.3.2 implique que ces polynômes sont fortement premiers entre eux. On peut ajouter à cette liste le polynôme $x$, car $\mathrm{Res}(x, \Phi_n) \mid \mathrm{Res}(x, x^n - 1) = \pm 1$. Comme on a $N + 1 \geqslant \frac{d+1}{2} + 1$ polynômes fortement premiers entre eux, on a l'inégalité voulue. ■

Si l'on note $\zeta(s) = \sum \frac{1}{n^s}$ la fonction de Riemann habituelle, on peut raffiner cette minoration par la proposition suivante :

**Proposition IV.3.10** *On a l'inégalité*

$$0.6478d \leqslant \frac{\zeta(2)\zeta(3)}{3\zeta(6)}d \leqslant R1(d) + \mathrm{o}(d).$$

*Preuve :* Considérons l'ensemble

$$A(x) = \{n \text{ tel que } \phi(n) \leqslant x \text{ et } n \text{ pair }\}.$$

Les résultats de Erdös et Turán (dans [Erd]) montrent que si l'on enlève la condition *n pair* dans la définition de $A(x)$, le cardinal de $A(x)$ est équivalent à $Cx$ où $C = \zeta(2)\zeta(3)/\zeta(6)$. Cette constante est le résidu en $s = 1$ de la fonction $F(s) = \sum \frac{1}{\phi(n)^s}$. Si l'on ajoute la condition *n pair*, on voit que cela revient à étudier la fonction $G(s) = \left(2 - \frac{1}{2^s}\right)^{-1} F(s)$. Nous avons donc

$$|A(x)| \sim \frac{2}{3}Cx.$$

Considérons maintenant l'ensemble

$$A_1(x) = A(x) \smallsetminus A\left(\frac{x}{2}\right).$$

Le cardinal de cet ensemble est équivalent à $\frac{C}{3}x$. Soit $n \in A_1(x)$ et $k$ un entier (supérieur ou égal à 2). On a l'inégalité $\phi(kn) \geqslant 2\phi(n)$. Ceci prouve que dans $A_1(x)$, on ne peut pas trouver deux entiers distincts dont le rapport soit entier. Ainsi, les polynômes cyclotomiques $\Phi_n$ (avec $n \in A_1(x)$ ont des résultants égaux à $\pm 1$, et leurs degrés sont tous inférieurs à $x$. Ceci prouve la proposition. ■

Dans ces propositions, nous avons une minoration de $R1(d)$ linéaire en $d$. Un argument heuristique donne une majoration également linéaire de $R1(d)$. En effet, si nous avons une famille $P_1, \ldots, P_n$ de polynômes fortement premiers entre eux de degrés au plus $d$, alors ceux-ci restent fortement premiers entre eux lorsqu'on les regarde modulo un nombre premier $p$. Dans $\mathbb{F}_p[x]$ il y a $p^{d+1}$ polynômes de degré au plus $d$. Les résultants des polynômes prennent leurs valeurs parmi les $p$ valeurs de $\mathbb{F}_p$. Si l'on suppose que les valeurs des résultants $\mathrm{Res}(P_i, P_j)$ sont indépendantes, alors la probabilité qu'un résultant soit égal à $\pm 1$ est $2/(p+1)$. La probabilité que tous les résultants soient $\pm 1$ est $(2/(p+1))^{n(n-1)/2}$. Pour qu'il y ait une solution il faudrait donc que l'on ait

$$p^{n(d+1)} \geqslant \left(\frac{p+1}{2}\right)^{\frac{n(n-1)}{2}}$$

Lorsque $p$ tend vers $+\infty$ cette inégalité donne

$$n \leqslant 2d + 3.$$

Un autre argument de nature un peu différente donne la même majoration : en effet, si l'on considère les coefficients des polynômes $P_1,\ldots,P_n$ comme des variables, alors il y a $n(d+1)$ variables. Les équations $\mathrm{Res}(P_i, P_j) = \pm 1$ sont au nombre de $n(n-1)/2$. Si l'on estime qu'il est nécessaire d'avoir plus de variables que d'équations pour qu'il existe une solution, on a alors l'inégalité

$$n(d+1) \geqslant \frac{n(n-1)}{2}.$$

Cette inégalité implique alors

$$n \leqslant 2d + 3.$$

Ces deux arguments semblent indiquer que l'on doit avoir l'inégalité

$$R1(d) \leqslant 2d + 3.$$

Sans être aussi précis que les arguments précédents, nous posons la question suivante :

**Question IV.3.11** *Peut-on trouver une constante* $\lambda \geqslant 0.6478$ *telle que*

$$R1(d) \leqslant \lambda d + \mathrm{o}(d) \quad ?$$

### IV.3.4 Familles de Polynômes Factorisables

Comme dans le cas des polynômes irréductibles, nous proposons une construction à partir des polynômes cyclotomiques. À l'aide de la Proposition IV.3.2, nous pouvons déterminer le discriminant d'un produit particulier de polynômes cyclotomiques.

**Proposition IV.3.12** *Soit* $P_n = \prod_{n<m\leqslant 2n} \Phi_m$ *et* $D_n = |\operatorname{disc} P_n|$. *Lorsque* $n$ *tend vers* $+\infty$, *on a* $d_n = \deg P_n = \frac{9}{\pi^2} n^2 + \mathrm{O}(n \log n)$, *et*

$$D_n^{1/d_n} = \frac{\pi}{3} 2^{\frac{4}{3}} e^{-C-1} \sqrt{d_n} + \mathrm{O}(\log^2 d_n)$$

*avec* $C = -\frac{\zeta'(2)}{\zeta(2)} = \sum_{p<+\infty} \frac{\log p}{p^2-1} \sim 0.570$.

*Preuve :* Le degré de $P_n$ est simplement la somme de degrés des polynômes $\Phi_m$ :

$$d_n = \sum_{n<m\leqslant 2n} \phi(m).$$

Intéressons nous d'abord à la série $A(x) = \sum_{m\leqslant x} \phi(m)$. Dans [Ten][p.41], l'auteur évalue cette série en utilisant le principe de l'hyperbole de Dirichlet :

$$A(x) = \frac{3}{\pi^2} x^2 + \mathrm{O}(x \log x),$$

ce qui nous donne

$$d_n = A(2n) - A(n) = \frac{9}{\pi^2}n^2 + \mathrm{O}(n \log n).$$

Lorsque $n < m < m' \leqslant 2n$, il est impossible d'avoir $m \mid m'$. Ainsi, la Proposition IV.3.2 prouve que les résultants deux à deux des polynômes $\Phi_m$ sont tous triviaux. La formule du discriminant d'un produit nous dit que le discriminant de $P_n$ est le produit des discriminants des $\Phi_m$ :

$$D_n = \prod_{n<m\leqslant 2n} \operatorname{disc} \Phi_m.$$

D'après la Proposition IV.3.1, nous devons donc évaluer la somme :

$$\frac{1}{d_n} \log D_n = \frac{1}{d_n} \sum_{n<m\leqslant 2n} \phi(m) \sum_{p\mid m} (v_p(m) - \frac{1}{p-1}) \log p.$$

Posons

$$B(x) = \sum_{m\leqslant x} \phi(m) \sum_{p\mid m} v_p(m) \log p$$

et

$$C(x) = \sum_{m\leqslant x} \phi(m) \sum_{p\mid m} \frac{\log p}{p-1}$$

Lorsque nous aurons évalué les séries $B$ et $C$, il ne restera plus qu'à écrire $\frac{1}{d_n}\log(D_n) = (B(2n) - C(2n) - B(n) + C(n))/d_n$. Pour $B(x)$ nous avons

$$\begin{aligned} B(x) &= \sum_{m\leqslant x} \phi(m) \sum_{p\mid m} v_p(m) \log p \\ &= \sum_{m\leqslant x} \phi(m) \log m \\ &= A(x) \log x - \int_1^x \frac{1}{t} A(t) dt \\ &= (\frac{3}{\pi^2}x^2 + \mathrm{O}(x \log x)) \log x - \int_1^x \frac{3}{\pi^2} t + \mathrm{O}(\log t) dt \\ &= \frac{3}{\pi^2} x^2 \log x - \frac{3}{2\pi^2} x^2 + \mathrm{O}(x \log^2 x) \end{aligned}$$

Il reste à évaluer $C(x)$ :

$$C(x) = \sum_{m\leqslant x} \phi(m) \sum_{p\mid m} \frac{\log p}{p-1} = \sum_{p\leqslant x} \frac{\log p}{p-1} \sum_{m\leqslant x/p} \phi(mp).$$

Mais $\phi(mp) = \phi(m)\phi(p)$ lorsque $p \nmid m$ et $\phi(mp) = \phi(m)\phi(p) + \phi(m)$ sinon. On a alors

$$C(x) = \sum_{p\leqslant x} \frac{\log p}{p-1} \sum_{m\leqslant x/p} \phi(m)\phi(p) + \ldots + \sum_{m\leqslant x/p^k} \phi(m)\phi(p),$$

où $k = [\frac{\log x}{\log p}]$. D'où

$$\begin{aligned}
C(x) &= \sum_{p\leqslant x} \log p \sum_{1\leqslant q\leqslant k} A\left(\frac{x}{p^q}\right) \\
&= \sum_{p\leqslant x} \log p \left(\sum_{1\leqslant q\leqslant k} \frac{3}{\pi^2}\frac{x^2}{p^{2q}} + \mathrm{O}\left(\frac{x}{p^q}\log\frac{x}{p^q}\right)\right) \\
&= \frac{3}{\pi^2}x^2 \sum_{p\leqslant x} \log p \frac{1-p^{-2k}}{p^2-1} + \mathrm{O}\left(x\log x \sum_{p\leqslant x}\log p \sum_{1\leqslant q\leqslant k}\frac{1}{p^q}\right) \\
&= \frac{3}{\pi^2}x^2\left(\sum_{p\leqslant x}\frac{\log p}{p^2-1} + \mathrm{O}\left(\frac{1}{x^2}\sum_{p\leqslant x}\log p\right)\right) + \mathrm{O}\left(x\log x\sum_{p\leqslant x}\log p\frac{1}{p-1}\right) \\
&= \frac{3}{\pi^2}x^2 \sum_{p<+\infty}\frac{\log p}{p^2-1} + \mathrm{O}(x\log^2 x)
\end{aligned}$$

En notant $C = \sum_{p<+\infty}\frac{\log p}{p^2-1} = -\frac{\zeta'(2)}{\zeta(2)}$ on a

$$C(x) = \frac{3}{\pi^2}Cx^2 + \mathrm{O}(x\log^2 x).$$

On peut maintenant revenir à l'expression de départ :

$$\begin{aligned}
\frac{1}{d_n}\log D_n &= \frac{(B(2n)-C(2n))-(B(n)+C(n))}{d_n} \\
&= \frac{\frac{9}{\pi^2}n^2\log n + (\frac{12}{\pi^2}\log 2 - \frac{9}{\pi^2} + \frac{9}{\pi^2}C)n^2 + \mathrm{O}(n\log^2 n)}{\frac{9}{\pi^2}n^2 + \mathrm{O}(n\log n)} \\
&= \log n + (\frac{4}{3}\log 2 - C - 1) + \mathrm{O}\left(\frac{\log^2 n}{n}\right) \\
&= \frac{1}{2}\log d_n - \log\frac{3}{\pi} + (\frac{4}{3}\log 2 - C - 1) + \mathrm{O}\left(\frac{\log^2 d_n}{\sqrt{d_n}}\right)
\end{aligned}$$

ce qui nous donne

$$D_n^{1/d_n} = \frac{\pi}{3}2^{\frac{4}{3}}e^{-C-1}\sqrt{d_n} + \mathrm{O}(\log^2 d_n)$$

■

**Remarque** : Si l'on évalue la constante, on trouve $D_n^{1/d_n} \sim 0.549\sqrt{d_n}$.

Les Théorèmes de Minkowski et d'Odlyzko montrent qu'il existe une constante $c > 1$ ayant la propriété suivante : pour tout corps de nombres de degré $d > 1$ et de discriminant $D$, on a $|D|^{1/d} > c$. Cette propriété se transmet immédiatement aux polynômes irréductibles. Montrons qu'elle est encore vraie pour les polynômes factorisables de degré $d \geqslant 4$ :

**Proposition IV.3.13** *Il existe une constante $c > 1$ telle que, pour tout polynôme $P \in \mathbb{Z}[x]$ de degré $d \geqslant 4$ sans facteur carré, on ait l'inégalité :*

$$|\operatorname{disc}(P)|^{1/d} > c.$$

*Preuve :* Soit $\alpha > 1$ une constante donnée par le Théorème de Minkowski telle que pour tout polynôme irréductible $P$ de degré $d \geqslant 2$, on ait $|\operatorname{disc}(P)|^{1/d} > \alpha$. Soit maintenant un polynôme $P$ de degré $d \geqslant 2$ sans facteur carré dont la factorisation en polynômes irréductibles de $\mathbb{Z}[x]$ est donnée par

$$P = \prod_{\deg A_i = 1} A_i \prod_{\deg B_j > 1} B_j$$

où les $A_i$ sont de degré 1 et les $B_j$ de degré $> 1$. On note $A$ le produit des $A_i$ et $n$ son degré. On note aussi $B$ le produit des $B_j$ et $b_j$ le degré de chaque $B_j$. On a donc $d = n + \sum b_j$. La formule du discriminant d'un produit nous dit que

$$\operatorname{disc} P = \operatorname{disc} A \operatorname{disc} B \operatorname{Res}^2(A, B)$$

La minoration $\operatorname{Res}^2(A, B) \geqslant 1$ est toujours vraie puisque $A$ et $B$ sont sans facteurs communs à coefficients entiers. La formule du discriminant d'un produit nous dit encore que

$$|\operatorname{disc} B| \geqslant \prod_j |\operatorname{disc} B_j| \geqslant \alpha^{\sum b_j}$$

$$|\operatorname{disc} B| \geqslant \alpha^{d-n}.$$

Pour $A$, on a

$$\operatorname{disc} A = \prod_{i \neq j} \operatorname{Res}^2(A_i, A_j).$$

D'après la Proposition IV.2.7, on a

$$\operatorname{disc} A \geqslant \max(1, 4^{n-3}).$$

Pour le discriminant de $P$, on trouve

$$|\operatorname{disc} P| \geqslant \alpha^{d-n} \max(1, 4^{n-3}).$$

Posons $\beta = \min(\alpha, 4) > 1$. On a alors

$$|\operatorname{disc} P| \geqslant \beta^{d-3}.$$

En posant enfin $c = \beta^{\frac{1}{4}}$, on a la proposition annoncée. ■

**Remarque** : En ce qui concerne les degrés 1, 2 et 3, la proposition n'est plus vraie comme le montrent les exemples suivants :

$$\operatorname{disc} x = 1$$
$$\operatorname{disc} x(x-1) = 1$$
$$\operatorname{disc} x(x-1)(2x-1) = 1.$$

# Annexe A

# Tables de Discriminants Minimaux

Dans cette table nous indiquons pour chaque signature $d.r_1$ le plus petit discriminant que nous avons trouvé (disc), sa racine $d$-ième ($\sqrt[d]{|\,\mathrm{disc}\,|}$), et la distance qui le sépare de la borne d'Odlyzko exprimée en pourcentage (%). Nous indiquons aussi le nombre ($n$) de discriminants trouvés pour chaque signature, sachant que l'on a gardé les 50 discriminants les plus petits en dessous de 30%, ainsi que tous ceux en dessous de 10%.

Pour le degré 9, nous avons redécouvert tous les discriminants minimaux connus :
$d.r_1 = 9.1$ et $d.r_1 = 9.3$ dans [Leu-Mar],
$d.r_1 = 9.5$ et $d.r_1 = 9.7$ dans [Leu a],
$d.r_1 = 9.9$ dans [Leu b].

À quelques rares exceptions près, les listes de petits discriminants que nous trouvons pour le degré 9 coïncident avec celles de G. Niklasch ([Nik]), ce qui donne une certaine assurance sur leur exhaustivité. Les tables de G. Niklasch vont bien au delà des 10% ou 30% auxquels nous nous sommes limités. Nous indiquons ici les valeurs des discriminants qui manquent dans nos listes par rapport aux listes de G. Niklasch, ainsi que ceux qui sont nouveaux. Nous indiquons aussi entre parenthèses leurs places dans les listes.

| $d.r_1$ | Manquants | | Nouveaux | |
|---|---|---|---|---|
| 9.1 | – | | – | |
| 9.3 | $-114479303$ ($10^{\mathrm{e}}$) | $-129079703$ | | |
| | $-133731799$ | $-157505216$ | | |
| | $-195458751$ | $-197369219$ | – | |
| | $-203221591$ | $-206640119$ | | |
| | $-215222063$ | | | |
| 9.5 | 858645521 ($223^{\mathrm{e}}$) | 912438613 | 729659521 ($120^{\mathrm{e}}$) | 821790577 |
| | | | 835481369 | 895086761 |
| 9.7 | $-2964637151$ ($13^{\mathrm{e}}$) | | $-4076715319$($50^{\mathrm{e}}$) | |
| 9.9 | 39783402073 ($34^{\mathrm{e}}$) | 41649746033 | 34800272761 ($25^{\mathrm{e}}$) | |
| | 45472867937 | 46527002977 | | |
| | 48259276753 | 49553865017 | | |

Ainsi, sur les 1277 discriminants trouvés pour le degré 9, il en manque seulement 18, et 6

nouveaux ont été trouvés. En particulier, il est tout à fait remarquable que pour la signature $d.r_1 = 9.1$, les deux listes sont identiques et contiennent près de 300 polynômes. De même, la première centaine de discriminants pour la signature $d.r_1 = 9.5$ est identique dans les deux listes.

Nous avons aussi redécouvert les autres minimums connus pour les signatures suivantes :
$d.r_1 = 10.0$ dans [Leu a],
$d.r_1 = 10.4$ dans [Zie],
$d.r_1 = 11.5$ dans [Zie],
$d.r_1 = 12.0$ dans [Coh-Dia-Oli a].

Les polynômes qui nous donnent les meilleurs résultats pour les signatures $d.r_1 = 12.12$,18.18,20.20 et 24.24 sont les polynômes de Tchebycheff.

On remarquera que la première signature manquante est $d.r_1 = 17.17$ et que le premier degré manquant est $d = 29$. Il faut se rappeler que les degrés premiers sont plus difficiles à trouver que les autres, et que les signatures réelles ($r_1$ proche de $d$) sont plus rares que les signatures complexes ($r_1$ proche de 0).

À notre connaissance, tous les minimums connus de discriminants de polynômes (inférieurs à 30%) sont inscrits dans cette table.

Pour les signatures totalement complexes ($r_1 = 0$), H. Cohen, F. Diaz Y Diaz et M. Olivier donnent dans [Coh-Dia-Oli a] des discriminants inférieurs à ceux que nous indiquons ici pour les degrés 14, 16, 18, 20, 22, 24, 28, 30, 32, 36, 40, 44 et 48. Toutefois, ils donnent des discriminants de corps de nombres et non de polynômes. Les polynômes qui définissent ces corps ont la particularité d'avoir d'assez gros indices, ce qui rend leurs discriminants largement supérieurs à ceux de cette table. Il semble particulièrement difficile d'éliminer ces indices et de trouver des bases d'entiers monogènes pour ces corps. Nous reviendrons à ces corps dans la table suivante.

| $d.r_1$ | disc | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | n |
|---|---|---|---|---|
| 9.1 | 29510281 | 0.85% | 6.761 | 287 |
| 9.3 | −109880167 | 0.96% | 7.824 | 603 |
| 9.5 | 453771377 | 1.58% | 9.159 | 285 |
| 9.7 | −1904081383 | 1.78% | 10.742 | 50 |
| 9.9 | 9685993193 | 3.63% | 12.870 | 50 |
| 10.0 | −209352647 | 0.94% | 6.793 | 239 |
| 10.2 | 799905449 | 1.07% | 7.768 | 1675 |
| 10.4 | −3191230411 | 1.09% | 8.921 | 1456 |
| 10.6 | 14002335917 | 1.57% | 10.342 | 414 |
| 10.8 | −74596123648 | 3.56% | 12.226 | 50 |
| 10.10 | 513087549389 | 7.86% | 14.826 | 50 |
| 11.1 | −5781612911 | 1.04% | 7.717 | 2099 |
| 11.3 | 23653561333 | 1.13% | 8.772 | 2769 |
| 11.5 | −104044407583 | 1.44% | 10.036 | 1009 |
| 11.7 | 487871635289 | 1.94% | 11.550 | 197 |
| 11.9 | −2413345112407 | 2.55% | 13.356 | 50 |
| 11.11 | 30733206894581 | 12.05% | 16.832 | 50 |
| 12.0 | 41223887921 | 0.84% | 7.666 | 940 |
| 12.2 | −172922533711 | 1.00% | 8.639 | 2883 |
| 12.4 | 779600892073 | 1.37% | 9.795 | 1195 |
| 12.6 | −3732622477247 | 1.90% | 11.160 | 327 |
| 12.8 | 17497403356237 | 1.92% | 12.693 | 90 |
| 12.10 | −110034817788739 | 4.14% | 14.795 | 50 |
| 12.12 | 551709470703125 | 4.14% | 16.923 | 50 |
| 13.1 | 1296443603821 | 1.05% | 8.546 | 2097 |
| 13.3 | −6004259398927 | 1.50% | 9.615 | 974 |
| 13.5 | 30572565095101 | 2.38% | 10.898 | 260 |
| 13.7 | −158547669654323 | 3.11% | 12.368 | 103 |
| 13.9 | 922071522770617 | 4.49% | 14.162 | 50 |
| 13.11 | −4768959849003391 | 4.67% | 16.070 | 50 |
| 13.13 | 62557040066579369 | 12.37% | 19.589 | 30 |
| 14.0 | −9866941650479 | 1.17% | 8.475 | 605 |
| 14.2 | 44856176930933 | 1.36% | 9.443 | 860 |
| 14.4 | −230312802348199 | 2.16% | 10.614 | 213 |
| 14.6 | 1066457629922633 | 1.94% | 11.842 | 102 |
| 14.8 | −5221080604842703 | 1.87% | 13.264 | 50 |
| 14.10 | 38213434345183981 | 4.54% | 15.291 | 50 |
| 14.12 | −375594908253322939 | 9.33% | 18.003 | 50 |
| 14.14 | 1776478047975643577 | 8.32% | 20.115 | 24 |

| $d.r_1$ | disc | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | n |
|---|---|---|---|---|
| 15.1 | −405022595697311 | 2.51% | 9.415 | 133 |
| 15.3 | 1932098331869129 | 2.68% | 10.449 | 78 |
| 15.5 | −12557469881316011 | 4.75% | 11.837 | 50 |
| 15.7 | 49954118550260597 | 3.19% | 12.979 | 50 |
| 15.9 | −259445842195368391 | 3.27% | 14.485 | 50 |
| 15.11 | 1809208205586432929 | 5.20% | 16.487 | 50 |
| 15.13 | −34014660913686708907 | 14.29% | 20.050 | 43 |
| 15.15 | 363145034778499996657 | 19.37% | 23.479 | 3 |
| 16.0 | 2773873245710329 | 1.73% | 9.230 | 127 |
| 16.2 | −11705685949886767 | 1.05% | 10.099 | 121 |
| 16.4 | 60447330360817889 | 1.43% | 11.190 | 94 |
| 16.6 | −488576402290603343 | 4.49% | 12.751 | 50 |
| 16.8 | 2065633544167346897 | 3.19% | 13.954 | 50 |
| 16.10 | −14027767668189833431 | 4.78% | 15.728 | 50 |
| 16.12 | 911049751926122949 89 | 5.92% | 17.679 | 50 |
| 16.14 | −2166599664000000000000 | 15.96% | 21.552 | 26 |
| 16.16 | 4151600163965461328125 | 8.30% | 22.446 | 13 |
| 17.1 | 152386181912827249 | 4.20% | 10.251 | 50 |
| 17.3 | −974785446871123751 | 5.84% | 11.433 | 50 |
| 17.5 | 3462565393841824229 | 3.66% | 12.318 | 50 |
| 17.7 | −30383869816887350663 | 6.89% | 13.997 | 50 |
| 17.9 | 279117834864985945753 | 10.34% | 15.947 | 50 |
| 17.11 | −1205448451307144937223 | 8.80% | 17.381 | 50 |
| 17.13 | 25522065986492999399417 | 17.63% | 20.799 | 14 |
| 17.15 | −754424650732128851556379 | 29.53% | 25.384 | 1 |
| 17.17 | – | >30% | | 0 |
| 18.0 | −813353263818459731 | 1.89% | 9.886 | 63 |
| 18.2 | 3882675302999984089 | 1.69% | 10.783 | 193 |
| 18.4 | −21960508005098221571 | 2.28% | 11.872 | 63 |
| 18.6 | 136294362264505730221 | 3.24% | 13.139 | 50 |
| 18.8 | −1047999309957441092791 | 5.31% | 14.716 | 50 |
| 18.10 | 5386481861613431603329 | 4.89% | 16.117 | 50 |
| 18.12 | −37644290208944611459163 | 6.14% | 17.955 | 50 |
| 18.14 | 214547097427475246206649 | 6.07% | 19.778 | 50 |
| 18.16 | −10806948883692488597332 31 | 5.15% | 21.637 | 22 |
| 18.18 | 36202993110042424993725741 | 15.68% | 26.298 | 7 |
| 19.1 | −72973572770787219191 | 6.45% | 11.103 | 50 |
| 19.3 | 883343924143089981757 | 11.37% | 12.660 | 50 |
| 19.5 | −1640783267216919594863 | 5.42% | 13.079 | 50 |
| 19.7 | 24349879441828030184441 | 11.16% | 15.074 | 50 |
| 19.9 | −81172345477394712921043 | 8.22% | 16.060 | 42 |
| 19.11 | 677712175493888590645321 | 10.44% | 17.958 | 26 |
| 19.13 | −50453737927337005621445 63 | 11.90% | 19.960 | 14 |
| 19.15 | 67570981671365062021501753 | 16.82% | 22.880 | 4 |
| 19.17 | – | >30% | | 0 |
| 19.19 | – | >30% | | 0 |

| $d.r_1$ | disc | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | n |
|---|---|---|---|---|
| 20.0 | 294179066004120138473 | 2.70% | 10.554 | 50 |
| 20.2 | −1240514077961238536107 | 1.66% | 11.342 | 50 |
| 20.4 | 8248827519028002239989 | 2.81% | 12.468 | 77 |
| 20.6 | −59553360765360541453819 | 4.27% | 13.764 | 50 |
| 20.8 | 336605885845914288243389 | 4.34% | 15.009 | 50 |
| 20.10 | −29497691355358383016689 11 | 6.61% | 16.730 | 50 |
| 20.12 | 29001517818595120504239517 | 9.44% | 18.755 | 50 |
| 20.14 | −48819774148807723143118 4831 | 15.29% | 21.599 | 9 |
| 20.16 | 16720528329244063297416918 01 | 12.05% | 22.970 | 21 |
| 20.18 | – | >30% | | 0 |
| 20.20 | 16967521098303929080200195 3125 | 17.60% | 28.939 | 6 |
| 21.1 | 34482057615039759645721 | 7.90% | 11.836 | 50 |
| 21.3 | −15059036273258474306 3267 | 6.87% | 12.697 | 50 |
| 21.5 | 29989056537957029698821 53 | 13.65% | 14.641 | 50 |
| 21.7 | −19172891990497966004371039 | 14.36% | 15.993 | 47 |
| 21.9 | 72988832652439117027217237 | 12.16% | 17.044 | 38 |
| 21.11 | −29272102456618575600445 80707 | 22.93% | 20.320 | 8 |
| 21.13 | 63007729165400262135327683 21 | 17.10% | 21.076 | 6 |
| 21.15 | −10313820517799744843025 8698267 | 22.76% | 24.076 | 1 |
| 22.0 | −10799837824317129037616 3 | 3.14% | 11.142 | 50 |
| 22.2 | 536711831589389927080153 | 2.77% | 11.985 | 67 |
| 22.4 | −33986022539618285406514 39 | 3.43% | 13.033 | 50 |
| 22.6 | 24102052053683949980878777 | 4.52% | 14.247 | 50 |
| 22.8 | −35791288273914981689815 1203 | 9.12% | 16.106 | 50 |
| 22.10 | 16083663901102605883089 10001 | 7.80% | 17.245 | 50 |
| 22.12 | −30284695472228064975248 516279 | 13.56% | 19.706 | 17 |
| 22.14 | 28575970395704458829493 1170541 | 15.84% | 21.823 | 50 |
| 22.16 | −47434654305929672666106 06635579 | 21.14% | 24.795 | 2 |
| 22.18 | 13193141640994946075582 963010901 | 16.71% | 25.975 | 12 |
| 23.1 | −25796217911733551120365 987 | 11.04% | 12.731 | 50 |
| 23.3 | 79972758619041750666817 201 | 8.28% | 13.373 | 30 |
| 23.5 | −84900372018433387582727 5823 | 11.28% | 14.819 | 25 |
| 23.7 | 44529734950795704929254 97957 | 10.81% | 15.926 | 14 |
| 23.9 | −16656303582514502292550 218959 | 8.63% | 16.866 | 3 |
| 23.13 | −13232141550693790885913 59558775 | 12.33% | 20.400 | 1 |

| $d.r_1$ | disc | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | n |
|---|---|---|---|---|
| 24.0 | 37886087608691786498090597 | 3.07% | 11.635 | 50 |
| 24.2 | −33845803096068179255132407 1 | 5.12% | 12.747 | 50 |
| 24.4 | 17827554272258786941631520 49 | 4.79% | 13.660 | 50 |
| 24.6 | −23645390555295627946291692479 | 8.45% | 15.214 | 50 |
| 24.8 | 14337549835233758207336146534 4 | 8.56% | 16.400 | 50 |
| 24.10 | −11550589758414060470488353727 19 | 9.88% | 17.890 | 31 |
| 24.12 | 31892423120801508936152820466241 | 16.98% | 20.542 | 50 |
| 24.14 | −26188264830335824818333785973571 1 | 18.32% | 22.426 | 6 |
| 24.16 | 40133904805188804668817776562024 01 | 22.75% | 25.127 | 4 |
| 24.20 | 39315400730219687394625467906103 7056 | 27.15% | 30.416 | 1 |
| 24.24 | 16176178662669837731720352172851 5625 | 4.62% | 29.311 | 5 |
| 25.1 | 12909960050986308081521496163 7 | 22.48% | 14.603 | 17 |
| 25.3 | −60753031355745860055784174675 9 | 21.53% | 15.536 | 6 |
| 25.5 | 16218456845860618892315431258 37 | 17.79% | 16.158 | 3 |
| 25.7 | −16693453533590270424331126316771 | 20.40% | 17.738 | 1 |
| 25.9 | 40983482256514369073292413695360 9 | 27.34% | 20.161 | 1 |
| 25.11 | −61588198552268971277820012818181 1 | 20.35% | 20.492 | 1 |
| 26.0 | −27913114648851916933143115871 | 5.79% | 12.418 | 50 |
| 26.2 | 11813828024462296964864827494 1 | 4.56% | 13.127 | 50 |
| 26.4 | −10402799416813522506500262336 19 | 6.21% | 14.273 | 50 |
| 26.6 | 22211163076419026499081519461737 | 11.54% | 16.056 | 50 |
| 26.8 | −29037019659171227244987157672558 3 | 14.88% | 17.725 | 21 |
| 26.10 | 15990473960454567982337371350587 29 | 14.37% | 18.926 | 25 |
| 26.12 | −13194862011946140635898140466419 3099 | 26.28% | 22.428 | 3 |
| 26.14 | 27960608912656265954654338935703 2709 | 21.04% | 23.085 | 4 |
| 26.16 | −10766283169612606806299902061193086311 | 29.63% | 26.565 | 1 |
| 26.18 | 53448263818690604995573656846143768261 | 28.24% | 28.254 | 2 |
| 27.1 | −77302478433842264174513534351387 | 22.87% | 15.172 | 9 |
| 27.3 | 13367209867355057360362599283060 33 | 27.88% | 16.861 | 3 |
| 27.5 | −41420863585404557602466435793432 43 | 24.80% | 17.582 | 4 |
| 27.7 | 45897876644806433587356777982144 13 | 17.16% | 17.649 | 5 |
| 27.9 | −16319133446993098389962188178518 6675 | 24.99% | 20.145 | 2 |
| 27.11 | 14377584446384360726628765470211075 89 | 26.55% | 21.836 | 1 |
| 27.13 | −47478628645972427043965033010914 48543 | 23.48% | 22.823 | 2 |
| 28.0 | 41234698411531193629362341046937 | 10.72% | 13.462 | 50 |
| 28.2 | −24464615659456396994224127047475 9 | 10.74% | 13.364 | 50 |
| 28.4 | 73127764305805923915667988154966 1 | 8.01% | 14.918 | 50 |
| 28.6 | −27285880065980294660266071926117387 | 15.22% | 16.977 | 36 |
| 28.8 | 85488507795008896063798242261533161 | 12.43% | 17.683 | 24 |
| 28.10 | −63561011282166523273909587888868569 59 | 22.77% | 20.625 | 6 |
| 28.12 | 67245637166563131176177356582442788 01 | 15.12% | 20.667 | 4 |
| 28.16 | 61732452161611456807758538885447746779 41 | 28.42% | 26.369 | 1 |
| 28.20 | 25752553270939408379207658486742180196 0869 | 28.05% | 30.127 | 1 |

| $d.r_1$ | disc | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | n |
|---|---|---|---|---|
| 29 | | | | 0 |
| 30.0 | −2186952635858070103612819069946695 1 | 11.17% | 13.953 | 50 |
| 30.2 | 428531372884769714814286148803842 01 | 7.07% | 14.269 | 50 |
| 30.4 | −130551576155318938552085942458597 4519 | 12.93% | 15.990 | 32 |
| 30.6 | 112604583668729660455860098121799401 13 | 14.14% | 17.181 | 21 |
| 30.8 | −515584148385453483936313858153425911563 | 21.90% | 19.517 | 8 |
| 30.10 | 342031385709540977362789293642665765928 1 | 22.02% | 20.787 | 2 |
| 32.0 | 643321282795296933060532468731358576 9 | 9.41% | 14.134 | 50 |
| 32.2 | −253020852401144453476677514790390875439 | 15.91% | 15.852 | 18 |
| 32.4 | 466190950302947822847621954878202984769 | 11.54% | 16.158 | 34 |
| 32.6 | −383344313436513713518821789553142592962 56 | 20.81% | 18.545 | 6 |
| 32.8 | 199620256088427301025642985967051774955977 | 19.98% | 19.527 | 11 |
| 32.10 | −144037173174480100058360390608179825971 6231 | 20.33% | 20.771 | 1 |
| 32.12 | 110826505720388984870650129881431456675309841 | 29.89% | 23.790 | 1 |
| 32.18 | −216076908558611115428951745930656671594640836 31 | 27.92% | 28.051 | 1 |
| 33.3 | −221677751601922737558815703039602963731127 | 25.75% | 17.902 | 2 |
| 34.0 | −111579601551108952840143572397363101014 79 | 13.55% | 15.061 | 20 |
| 34.2 | 532549558813612581528295561237086863375 77 | 12.61% | 15.770 | 23 |
| 34.4 | −465321185391452958381128884316269708301946 7 | 21.59% | 17.985 | 4 |
| 34.6 | 271006106965629231645708436503798888006702 25 | 21.18% | 18.943 | 11 |
| 34.10 | 697681911911492469072811775176582291750556 2009 | 27.63% | 22.302 | 2 |
| 34.14 | 106593531400763215090519510113261054779870746121 | 23.52% | 24.164 | 1 |
| 36.0 | 612051511177055859392372686793473809607863 77 | 21.07% | 16.455 | 10 |
| 36.2 | −612553954675865342801021833909968265549568 51 | 14.96% | 16.455 | 17 |
| 36.4 | 540689038410768530807788391343880870009800 1393 | 23.57% | 18.636 | 11 |
| 36.6 | −927821611545371973420757169962164779455980 2587 | 19.01% | 18.918 | 3 |
| 36.8 | 119368564538133737477789259791500718910481000 0384 | 29.18% | 21.651 | 1 |
| 38.0 | −341518335239120846688126191179782076850932636 31 | 20.66% | 16.771 | 4 |
| 38.2 | 389787070544597190551402472840699143242653335161 | 22.41% | 17.881 | 8 |
| 38.4 | −215181949791432635155756500487618686870577047916 99 | 29.41% | 19.871 | 1 |
| 38.6 | 249507802131743786332309151178005273754139049624 89 | 23.55% | 19.949 | 1 |
| 40.0 | 232139752287223841447145061268685055410875229840 1 | 14.04% | 16.186 | 10 |
| 40.2 | −198814311768183336609441508721676925804810491359639 | 21.54% | 18.091 | 4 |
| 40.4 | 594462143202882896306537802656516268602493273864792 1 | 26.13% | 19.695 | 2 |
| 40.8 | 267745374983004418305988272298054896652984776746310001 | 25.96% | 21.662 | 1 |
| 42.2 | 669544256360610626065632756682074671788232633221933 21 | 19.51% | 18.103 | 3 |
| 44.0 | 272331422002629200050217775956750929288554489127728340 81 | 23.45% | 18.192 | 3 |
| 44.2 | −177977487259514521989317073793000809662691913630872930 2587 | 29.91% | 20.005 | 1 |
| 48.0 | 387639244281837478990692173059434206488028427365121373773636 49 | 25.99% | 19.191 | 5 |

# Annexe B

# Corps Primitifs et Imprimitifs

Dans le tableau suivant, nous donnons les plus petits discriminants des corps de nombres connus de degrés inférieurs à 48, en distinguant entre les corps primitifs et les imprimitifs, et en ne retenant que ceux qui sont inférieurs à 30%.

À part pour les degrés inférieurs ou égaux à 9 et pour quelques signatures isolées, tous les résultats viennent des travaux de cette thèse, et de ceux de H. Cohen, F. Diaz Y Diaz et Olivier sur les extensions abéliennes (dans [Coh-Dia-Oli a] et [Coh-Dia-Oli d]). Ces derniers trouvent des corps jusqu'au degré 100, mais leur construction par des extensions abéliennes ne leur permet pas d'obtenir des corps primitifs (à part quelques extensions abéliennes de $\mathbb{Q}$ de degré premier mais dont les discriminants sont largement au-dessus des bornes d'Odlyzko).

Les corps marqués d'un ▲ sont dûs à H.Cohen, F. Diaz Y Diaz et Olivier ([Coh-Dia-Oli a], [Coh-Dia-Oli d]), et ceux marqués d'un ♦ proviennent d'ailleurs (ils sont déjà cités dans la table précédente). Tous les autres corps font partie des résultats nouveaux de cette thèse.

Pour qu'apparaissent clairement les corps (primitifs ou imprimitifs) qui donnent les plus petits discriminants, nous avons indiqué en gras le minimum sur chaque ligne.

Comme il n'existe pas de corps imprimitifs de degré premier, nous avons volontairement omis d'indiquer les degrés premiers dans cette table.

Pour les corps imprimitifs de degré 15, nos méthodes ont permis de trouver quelques discriminants compris entre 10% et 30%. Toutefois ces discriminants n'étaient pas parmi les 50 minimaux, et donc nous ne les avons pas conservés car nous n'avons fait la distinction entre primitifs et imprimitifs qu'une fois la liste dressée. Ainsi, ils n'apparaissent pas dans ce tableau. Ce phénomène se produit aussi peut-être pour quelques autres signatures.

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ |
| 4.0 | ⧫19.09% | 3.890 | ⧫0.68% | **3.289** |
| 4.2 | ⧫1.56% | 4.102 | ⧫0.83% | **4.072** |
| 4.4 | ⧫29.72% | 6.651 | ⧫1.20% | **5.189** |
| 6.0 | ⧫7.74% | 4.951 | ⧫0.58% | **4.622** |
| 6.2 | ⧫1.06% | 5.545 | ⧫0.45% | **5.512** |
| 6.4 | ⧫1.28% | **6.728** | ⧫3.10% | 6.849 |
| 6.6 | ⧫12.48% | 9.165 | ⧫0.42% | **8.182** |
| 8.0 | ⧫1.10% | 5.801 | ⧫0.86% | **5.787** |
| 8.2 | ⧫1.03% | 6.747 | ⧫1.00% | **6.746** |
| 8.4 | ⧫1.383% | 7.947 | ⧫0.84% | **7.905** |
| 8.6 | ⧫2.23% | **9.478** | ⧫2.95% | 9.544 |
| 8.8 | ⧫10.27% | 12.176 | ⧫3.10% | **11.385** |
| 9.1 | ⧫0.85% | **6.761** | ⧫1.84% | 6.827 |
| 9.3 | ⧫0.96% | **7.824** | ⧫1.06% | 7.832 |
| 9.5 | ⧫1.58% | **9.159** | ⧫1.93% | 9.191 |
| 9.7 | ⧫1.78% | **10.742** | ⧫5.67% | 11.152 |
| 9.9 | ⧫3.63% | **12.870** | ⧫9.76% | 13.630 |
| 10.0 | 1.21% | 6.812 | ⧫0.94% | **6.793** |
| 10.2 | 1.09% | 7.769 | 1.07% | **7.768** |
| 10.4 | ⧫1.09% | **8.921** | 1.13% | 8.924 |
| 10.6 | 1.57% | **10.342** | 1.81% | 10.367 |
| 10.8 | 3.56% | **12.225** | 5.71% | 12.479 |
| 10.10 | 7.86% | **14.825** | ⧫9.06% | 14.990 |
| 12.0 | 1.04% | 7.681 | ▲0.84% | **7.666** |
| 12.2 | 1.00% | **8.639** | 1.52% | 8.684 |
| 12.4 | 1.37% | 9.795 | ▲0.70% | **9.729** |
| 12.6 | 1.90% | 11.160 | ▲1.87% | **11.157** |
| 12.8 | 2.22% | 12.731 | 1.92% | **12.693** |
| 12.10 | 4.14% | **14.795** | 9.52% | 15.559 |
| 12.12 | 11.65% | 18.143 | ⧫4.14% | **16.923** |
| 14.0 | 1.46% | 8.500 | ⧫0.58% | **8.426** |
| 14.2 | 2.06% | 9.508 | 1.36% | **9.443** |
| 14.4 | 2.16% | **10.614** | 2.23% | 10.621 |
| 14.6 | 2.39% | 11.894 | 1.94% | **11.842** |
| 14.8 | 3.67% | 13.499 | 1.87% | **13.264** |
| 14.10 | 7.51% | 15.725 | 4.54% | **15.291** |
| 14.12 | 9.33% | **18.003** | 13.54% | 18.694 |
| 14.14 | 18.17% | 21.946 | 8.32% | **20.115** |

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ |
| 15.1 | 2.51% | **9.415** | – | – |
| 15.3 | 2.68% | **10.449** | – | – |
| 15.5 | 4.75% | 11.837 | ▲2.00% | **11.527** |
| 15.7 | 3.19% | **12.979** | – | – |
| 15.9 | 3.27% | **14.485** | – | – |
| 15.11 | 5.20% | **16.487** | – | – |
| 15.13 | 14.29% | **20.050** | – | – |
| 15.15 | 19.37% | 23.479 | ▲12.63% | **22.153** |
| 16.0 | 4.46% | 9.478 | ▲1.16% | **9.179** |
| 16.2 | 4.42% | 10.435 | 1.05% | **10.099** |
| 16.4 | 4.22% | 11.498 | ▲1.42% | **11.189** |
| 16.6 | 4.49% | **12.751** | 5.03% | 12.816 |
| 16.8 | 4.49% | 14.130 | 3.19% | **13.954** |
| 16.10 | 4.78% | **15.728** | 11.72% | 16.770 |
| 16.12 | 5.92% | **17.679** | 10.57% | 18.456 |
| 16.14 | 21.95% | 22.665 | 15.96% | **21.552** |
| 16.16 | 29.80% | 26.903 | ▲5.08% | **21.779** |
| 18.0 | 6.14% | 10.298 | ▲1.37% | **9.836** |
| 18.2 | 4.82% | 11.114 | 1.69% | **10.783** |
| 18.4 | 8.83% | 12.633 | 2.28% | **11.872** |
| 18.6 | 5.91% | 13.479 | ▲1.09% | **12.865** |
| 18.8 | 9.65% | 15.323 | 5.31% | **14.716** |
| 18.10 | 9.54% | 16.831 | 4.89% | **16.117** |
| 18.12 | 13.09% | 19.131 | 6.14% | **17.955** |
| 18.14 | 20.68% | 22.503 | 6.07% | **19.778** |
| 18.16 | 29.73% | 26.696 | 5.15% | **21.637** |
| 18.18 | – | – | ▲5.12% | **23.896** |
| 20.0 | 8.05% | 11.103 | ▲1.57% | **10.438** |
| 20.2 | 9.86% | 12.256 | 1.66% | **11.342** |
| 20.4 | 9.40% | 13.267 | 2.81% | **12.468** |
| 20.6 | 10.87% | 14.635 | 4.27% | **13.764** |
| 20.8 | 11.53% | 16.043 | 4.34% | **15.009** |
| 20.10 | 13.94% | 17.880 | ▲3.33% | **16.214** |
| 20.12 | 18.71% | 20.344 | 9.44% | **18.755** |
| 20.14 | 29.74% | 24.307 | 15.29% | **21.599** |
| 20.16 | 25.51% | 25.728 | 12.05% | **22.970** |
| 20.18 | – | – | – | – |
| 20.20 | – | – | ▲13.38% | **27.900** |

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ |
| 21.1 | 7.90% | **11.836** | 12.68% | 12.360 |
| 21.3 | 6.87% | **12.697** | 15.65% | 13.739 |
| 21.5 | 13.65% | **14.641** | 18.13% | 15.218 |
| 21.7 | 14.36% | 15.993 | ▲1.45% | **14.187** |
| 21.9 | 12.16% | **17.044** | 13.97% | 17.319 |
| 21.11 | 23.11% | 20.350 | 22.93% | **20.320** |
| 21.13 | 17.10% | **21.076** | – | – |
| 21.15 | 22.76% | **24.076** | – | – |
| 21.21 | – | – | ▲8.55% | **27.681** |
| 22.0 | 9.21% | 11.797 | ▲1.85% | **11.003** |
| 22.2 | – | – | 2.77% | **11.985** |
| 22.4 | – | – | 3.43% | **13.033** |
| 22.6 | – | – | 4.52% | **14.247** |
| 22.8 | 9.12% | **16.106** | 10.30% | 16.281 |
| 22.10 | 18.50% | 18.956 | 7.80% | **17.245** |
| 22.12 | – | – | 13.56% | **19.706** |
| 22.14 | 17.10% | 22.061 | 15.84% | **21.823** |
| 22.16 | – | – | 21.14% | **24.795** |
| 22.18 | – | – | 16.71% | **25.975** |
| 22.22 | – | – | ▲5.74% | **27.877** |
| 24.0 | – | – | ▲1.35% | **11.441** |
| 24.2 | – | – | 5.12% | **12.747** |
| 24.4 | – | – | 4.79% | **13.660** |
| 24.6 | 16.12% | 16.289 | ▲3.31% | **14.492** |
| 24.8 | 15.03% | 17.377 | ▲2.31% | **15.456** |
| 24.10 | 14.11% | 18.580 | 9.88% | **17.890** |
| 24.12 | 18.78% | 20.858 | ▲3.55% | **18.183** |
| 24.14 | 26.38% | 23.952 | 18.32% | **22.426** |
| 24.16 | – | – | ▲7.24% | **21.950** |
| 24.20 | – | – | 27.15% | **30.416** |
| 24.24 | – | – | ▲4.08% | **29.159** |
| 25.1 | 22.48% | **14.603** | – | – |
| 25.3 | 21.53% | **15.536** | – | – |
| 25.5 | 17.79% | **16.158** | – | – |
| 25.7 | 20.40% | **17.738** | – | – |
| 25.9 | 27.34% | **20.161** | – | – |
| 25.11 | 20.35% | **20.492** | – | – |

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ |
| 26.0 | – | – | 5.79% | **12.418** |
| 26.2 | – | – | 4.56% | **13.127** |
| 26.4 | – | – | 6.21% | **14.273** |
| 26.6 | 17.60% | 16.927 | 11.54% | **16.056** |
| 26.8 | 14.88% | **17.725** | 16.52% | 17.978 |
| 26.10 | – | – | 14.37% | **18.926** |
| 26.12 | 29.66% | 23.028 | 26.28% | **22.428** |
| 26.14 | – | – | 21.04% | **23.085** |
| 26.16 | 29.63% | **26.565** | – | – |
| 26.18 | – | – | 28.24% | **28.254** |
| 27.1 | 22.87% | **15.172** | 22.98% | 15.184 |
| 27.3 | 28.90% | 16.995 | 27.88% | **16.861** |
| 27.5 | 25.60% | 17.696 | 24.80% | **17.582** |
| 27.7 | 25.56% | 18.915 | 17.16% | **17.649** |
| 27.9 | – | – | ▲2.38% | **16.501** |
| 27.11 | – | – | 26.55% | **21.836** |
| 27.11 | – | – | 23.48% | **22.823** |
| 27.27 | – | – | ▲2.82% | **31.176** |
| 28.0 | – | – | ▲1.13% | **12.296** |
| 28.2 | – | – | 10.74% | **13.364** |
| 28.4 | – | – | 8.01% | **14.918** |
| 28.6 | – | – | 15.22% | **16.977** |
| 28.8 | – | – | 12.43% | **17.683** |
| 28.10 | – | – | 22.77% | **20.625** |
| 28.12 | – | – | 15.12% | **20.667** |
| 28.14 | – | – | ▲5.12% | **20.177** |
| 28.16 | – | – | 28.42% | **26.369** |
| 28.20 | – | – | 28.42% | **30.127** |
| 28.28 | – | – | ▲9.81% | **34.094** |
| 30.0 | – | – | ▲1.72% | **12.766** |
| 30.2 | – | – | 7.07% | **14.269** |
| 30.4 | – | – | 12.93% | **15.990** |
| 30.6 | – | – | 14.14% | **17.181** |
| 30.8 | – | – | 21.90% | **19.517** |
| 30.10 | – | – | ▲2.24% | **17.417** |
| 30.20 | – | – | ▲11.59% | **26.111** |
| 30.30 | – | – | ▲9.49% | **35.523** |

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ | % | $\sqrt[d]{\lvert\text{disc}\rvert}$ |
| 32.0 | – | – | ▲1.13% | **13.065** |
| 32.2 | – | – | 15.91% | **15.852** |
| 32.4 | – | – | 11.54% | **16.158** |
| 32.6 | – | – | 20.81% | **18.545** |
| 32.8 | – | – | ▲5.35% | **17.144** |
| 32.10 | – | – | 20.33% | **20.771** |
| 32.12 | – | – | 29.89% | **23.790** |
| 32.16 | – | – | ▲4.27% | **21.526** |
| 32.18 | – | – | 27.92% | **28.051** |
| 32.32 | – | – | ▲10.97% | **37.474** |
| 33.3 | – | – | 25.75% | **17.902** |
| 33.11 | – | – | ▲6.39% | **19.019** |
| 33.33 | – | – | ▲10.54% | **38.036** |
| 34.0 | – | – | 13.55% | **15.061** |
| 34.2 | – | – | 12.61% | **15.770** |
| 34.4 | – | – | 21.59% | **17.985** |
| 34.6 | – | – | 21.18% | **18.943** |
| 34.10 | – | – | 27.63% | **22.302** |
| 34.14 | – | – | 23.52% | **24.164** |
| 36.0 | – | – | ▲1.71% | **13.823** |
| 36.2 | – | – | 14.96% | **16.455** |
| 36.4 | – | – | 23.57% | **18.636** |
| 36.6 | – | – | 19.01% | **18.918** |
| 36.8 | – | – | 29.18% | **21.651** |
| 36.12 | – | – | ▲2.37% | **19.093** |
| 36.18 | – | – | ▲4.31% | **22.888** |
| 36.24 | – | – | ▲6.67% | **27.608** |
| 36.36 | – | – | ▲5.54% | **38.246** |
| 38.0 | – | – | 20.66% | **16.771** |
| 38.2 | – | – | 22.41% | **17.881** |
| 38.4 | – | – | 29.41% | **19.871** |
| 38.6 | – | – | 23.55% | **19.949** |
| 39.13 | – | – | ▲4.29% | **20.197** |
| 39.39 | – | – | ▲25.49% | **47.618** |

| | Primitifs | | Imprimitifs | |
|---|---|---|---|---|
| $d.r_1$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ | % | $\sqrt[d]{\lvert \text{disc} \rvert}$ |
| 40.0 | – | – | ▲1.54% | **14.412** |
| 40.2 | – | – | 21.54% | **18.091** |
| 40.4 | – | – | 26.13% | **19.695** |
| 40.8 | – | – | 25.96% | **21.662** |
| 40.10 | – | – | ▲3.02% | **18.601** |
| 40.20 | – | – | ▲2.71% | **23.745** |
| 40.40 | – | – | ▲2.51% | **39.457** |
| 42.0 | – | – | ▲6.33% | **15.387** |
| 42.2 | – | – | 19.51% | **18.103** |
| 42.14 | – | – | ▲2.59% | **20.550** |
| 42.28 | – | – | ▲9.46% | **30.677** |
| 42.42 | – | – | ▲8.61% | **42.954** |
| 44.0 | – | – | ▲1.51% | **14.960** |
| 44.2 | – | – | 29.91% | **20.005** |
| 44.22 | – | – | ▲9.03% | **26.374** |
| 44.44 | – | – | ▲6.94% | **43.378** |
| 45.15 | – | – | ▲2.71% | **21.213** |
| 45.45 | – | – | ▲20.92% | **49.646** |
| 46.0 | – | – | ▲22.37% | **18.343** |
| 48.0 | – | – | ▲1.01% | **15.386** |
| 48.12 | – | – | ▲4.26% | **20.353** |
| 48.16 | – | – | ▲3.92% | **22.067** |
| 48.24 | – | – | ▲4.39% | **26.279** |
| 48.32 | – | – | ▲17.35% | **35.102** |
| 48.48 | – | – | ▲6.80% | **45.367** |

# Annexe C

# Polynômes de Discriminants Minimaux

Dans cette table, nous donnons la liste des polynômes qui donnent pour chaque signature le discriminant minimal indiqué dans la table précédente : ce n'est donc pas une table de corps de nombres, mais de polynômes. Nous rappelons la distance de la borne d'Odlyzko (en %) et nous donnons également la factorisation du discriminant. Cette factorisation donne une indication sur la primitivité des polynômes, et sur le discriminant des sous-corps éventuels du corps de nombres défini par le polynôme. En effet, la formule du discriminant relatif montre que le discriminant d'un sous-corps d'indice $r$ doit apparaître à la puissance $r$ dans le discriminant du polynôme, ce qui assure par exemple qu'un polynôme dont le discriminant est sans facteur carré est primitif.

Dans de nombreux cas, nous avons donné les polynômes sous la forme d'un résultant $P = \mathrm{Res}(\chi, R(x,y))$, c'est-à-dire sous la forme d'extension relative, en indiquant le polynôme de base $\chi$, et le polynôme relatif $R(x,y)$. À moins que cela soit explicitement indiqué, tous les résultants sont relatifs à la variable $x$. Dans la factorisation du discriminant de $P$, nous indiquons entre parenthèses la factorisation du discriminant de $\chi$, ainsi que son signe, y compris lorsque celui-ci intervient au carré.

**d = 9 r$_1$= 1,** disc $= 101 \cdot 292181$**, % = 0.85**
$x^9 - 2x^8 - x^7 + x^6 + 3x^5 + x^4 - 2x^3 - x^2 + 1$
**d = 9, r$_1$= 3,** disc $= -367 \cdot 299401$**, % = 0.96**
$x^9 - 2x^8 + x^7 + x^6 - 3x^5 + x^4 + 3x^3 - 2x - 1$
**d = 9, r$_1$= 5,** disc $= 453771377$**, % = 1.58**
$x^9 + 2x^8 - x^7 - 2x^6 - x^5 - 5x^4 + x^3 + 5x^2 - 1$
**d = 9, r$_1$= 7,** disc $= -37 \cdot 51461659$**, % = 1.78**
$x^9 + x^8 - 6x^7 - 8x^6 + 10x^5 + 19x^4 - 2x^3 - 13x^2 - 2x + 1$
**d = 9, r$_1$= 9,** disc $= 9685993193$**, % = 3.63**
$x^9 + 2x^8 - 7x^7 - 14x^6 + 15x^5 + 30x^4 - 10x^3 - 19x^2 + 2x + 1$

**d = 10, r$_1$= 0,** disc $= -7^2 431^2 23$**, % = 0.94**

$x^{10} - 3x^9 + 7x^8 - 11x^7 + 13x^6 - 12x^5 + 9x^4 - 5x^3 + 3x^2 - 2x + 1$
**d = 10, r₁= 2,** disc = $7^2631^241$, **% = 1.07**
$x^{10} - x^9 + x^7 + x^6 - x^5 - x^4 + x^3 - x - 1$
**d = 10, r₁= 4,** disc = $-3191230411$, **% = 1.09**
$x^{10} - x^9 - 3x^8 + 5x^6 + 4x^5 - 4x^4 - 2x^3 - x^2 - x + 1$
**d = 10, r₁= 6,** disc = $43 \cdot 325635719$, **% = 1.57**
$x^{10} - x^9 - x^8 + 4x^7 - 4x^6 + 8x^4 - 3x^3 - 5x^2 + x + 1$
**d = 10, r₁= 8,** disc = $-2^{10}2389 \cdot 30493$, **% = 3.56**
$x^{10} - 2x^9 - 6x^8 + 10x^7 + 15x^6 - 16x^5 - 19x^4 + 10x^3 + 9x^2 - 2x - 1$
**d = 10, r₁= 10,** disc = $460181 \cdot 1114969$, **% = 7.86**
$x^{10} + 4x^9 - 2x^8 - 23x^7 - 11x^6 + 40x^5 + 30x^4 - 21x^3 - 18x^2 + 1$

**d = 11, r₁= 1,** disc = $-239 \cdot 24190849$, **% = 1.04**
$x^{11} - 2x^{10} + 2x^9 - 3x^8 + 6x^7 - 8x^6 + 7x^5 - 7x^4 + 7x^3 - 6x^2 + 3x - 1$
**d = 11, r₁= 3,** disc = $3989 \cdot 5929697$, **% = 1.13**
$x^{11} - 2x^{10} - 2x^9 + 6x^8 + 2x^7 - 9x^6 + 8x^4 - x^3 - 5x^2 + 1$
**d = 11, r₁= 5,** disc = $-104044407583$, **% = 1.44**
$x^{11} + x^{10} - x^9 - 2x^8 - 4x^7 + 2x^5 + 3x^4 + 3x^3 - x^2 - 1$
**d = 11, r₁= 7,** disc = $587 \cdot 831127147$, **% = 1.94**
$x^{11} - 2x^{10} - 3x^9 + 9x^8 - 3x^7 - 10x^6 + 12x^5 - 7x^3 + 4x^2 + x - 1$
**d = 11, r₁= 9,** disc = $-681589 \cdot 3540763$, **% = 2.55**
$x^{11} - x^{10} - 8x^9 + 6x^8 + 23x^7 - 10x^6 - 29x^5 + x^4 + 16x^3 + 6x^2 - 3x - 1$
**d = 11, r₁= 11,** disc = $649087 \cdot 47348363$, **% = 12.05**
$x^{11} - 2x^{10} - 10x^9 + 19x^8 + 37x^7 - 65x^6 - 61x^5 + 94x^4 + 42x^3 - 48x^2 - 9x + 1$

**d = 12, r₁= 0,** disc = $37^2857^241$, **% = 0.84**
$x^{12} - 2x^{11} + 2x^{10} - x^9 + 2x^8 - 5x^7 + 8x^6 - 7x^5 + 4x^4 - 3x^3 + 4x^2 - 3x + 1$
**d = 12, r₁= 2,** disc = $-743 \cdot 3407 \cdot 68311$, **% = 1.00**
$x^{12} - x^{11} - 2x^9 + x^7 + x^6 + 3x^5 - 2x^2 - x - 1$
**d = 12, r₁= 4,** disc = $61 \cdot 12780342493$, **% = 1.37**
$x^{12} - 4x^{11} + 10x^{10} - 21x^9 + 30x^8 - 37x^7 + 32x^6 - 20x^5 + 7x^4 + 3x^3 - 4x^2 + 3x - 1$
**d = 12, r₁= 6,** disc = $-3732622477247$, **% = 1.90**
$x^{12} - 3x^{11} - 4x^{10} + 16x^9 + 6x^8 - 31x^7 - 9x^6 + 27x^5 + 13x^4 - 11x^3 - 7x^2 + 2x + 1$
**d = 12, r₁= 8,** disc = $7^230941^2373$, **% = 1.92**
$x^{12} - 5x^{11} + 5x^{10} + 11x^9 - 24x^8 + 11x^7 + 12x^6 - 35x^5 + 25x^4 + 21x^3 - 20x^2 - 4x + 1$
**d = 12, r₁= 10,** disc = $-2377 \cdot 46291467307$, **% = 4.14**
$x^{12} - 10x^{10} - x^9 + 35x^8 + 6x^7 - 51x^6 - 13x^5 + 27x^4 + 12x^3 - 2x^2 - 4x - 1$
**d = 12, r₁= 12,** disc = $5^97^{10}$, **% = 4.14**
$x^{12} - x^{11} - 12x^{10} + 11x^9 + 54x^8 - 43x^7 - 113x^6 + 71x^5 + 110x^4 - 46x^3 - 40x^2 + 8x + 1$

**d = 13, r₁= 1,** disc = $199 \cdot 2797 \cdot 2329207$, **% = 1.05**
$x^{13} - 7x^{12} + 19x^{11} - 39x^{10} + 63x^9 - 83x^8 + 92x^7 - 88x^6 + 72x^5 - 50x^4 + 29x^3 - 14x^2 + 5x - 1$
**d = 13, r₁= 3,** disc = $-250361 \cdot 23982407$, **% = 1.50**

$x^{13} - 3x^{12} + 6x^{10} - x^9 - 8x^8 + 6x^7 + 3x^6 - 8x^5 + x^4 + 3x^3 + 1$
**d = 13, $r_1$= 5,** disc = $457 \cdot 66898391893$, **% = 2.38**
$x^{13} - 7x^{11} + x^{10} + 19x^9 - 6x^8 - 26x^7 + 13x^6 + 18x^5 - 12x^4 - 4x^3 + 5x^2 - 1$
**d = 13, $r_1$= 7,** disc = $-67 \cdot 1913 \cdot 2297 \cdot 538529$, **% = 3.11**
$x^{13} - 2x^{12} - 12x^{11} + 22x^{10} + 59x^9 - 93x^8 - 153x^7 + 187x^6 + 222x^5 - 177x^4 - 171x^3 + 62x^2 + 55x + 1$
**d = 13, $r_1$= 9,** disc = $61 \cdot 15115926602797$, **% = 4.49**
$x^{13} + x^{12} - 11x^{11} - 8x^{10} + 47x^9 + 19x^8 - 97x^7 - 5x^6 + 95x^5 - 27x^4 - 32x^3 + 18x^2 - 3x + 1$
**d = 13, $r_1$= 11,** disc = $-521 \cdot 1049 \cdot 7703 \cdot 1132793$, **% = 4.67**
$x^{13} + 2x^{12} - 10x^{11} - 19x^{10} + 39x^9 + 67x^8 - 75x^7 - 106x^6 + 73x^5 + 71x^4 - 31x^3 - 16x^2 + 4x + 1$
**d = 13, $r_1$= 13,** disc = $103 \cdot 4271 \cdot 142203208513$, **% = 12.37**
$x^{13} + 3x^{12} - 8x^{11} - 27x^{10} + 23x^9 + 91x^8 - 28x^7 - 141x^6 + 12x^5 + 98x^4 - 24x^2 + 1$

**d = 14, $r_1$= 0,** disc = $-167^2 1361^2 191$, **% = 1.17**
$x^{14} - 3x^{13} + 6x^{12} - 11x^{11} + 16x^{10} - 21x^9 + 25x^8 - 25x^7 + 25x^6 - 21x^5 + 16x^4 - 11x^3 + 6x^2 - 3x + 1$
**d = 14, $r_1$= 2,** disc = $919969^2 53$, **% = 1.36**
$x^{14} + 2x^{13} + 4x^{12} + 6x^{11} + 6x^{10} + 5x^9 + 2x^8 + x^7 + 2x^6 + 5x^5 + 6x^4 + 6x^3 + 4x^2 + 2x + 1$
**d = 14, $r_1$= 4,** disc = $-59 \cdot 1997 \cdot 1954735513$, **% = 2.16**
$x^{14} - 11x^{12} - x^{11} + 47x^{10} + 8x^9 - 98x^8 - 23x^7 + 103x^6 + 28x^5 - 51x^4 - 12x^3 + 10x^2 + x - 1$
**d = 14, $r_1$= 6,** disc = $13^2 157^2 1367^2 137$, **% = 1.94**
$x^{14} + 7x^{13} + 18x^{12} + 20x^{11} - 32x^9 - 53x^8 - 59x^7 - 53x^6 - 32x^5 + 20x^3 + 18x^2 + 7x + 1$
**d = 14, $r_1$= 8,** disc = $-17^2 172519^2 607$, **% = 1.87**
$x^{14} - 3x^{13} - 15x^{12} + 68x^{11} + 4x^{10} - 413x^9 + 674x^8 + 208x^7 - 1905x^6 + 2671x^5 - 1911x^4 + 784x^3 - 183x^2 + 22x - 1$
**d = 14, $r_1$= 10,** disc = $13^2 157^2 1367^2 4909$, **% = 4.54**
$x^{14} - 7x^{13} + 10x^{12} + 31x^{11} - 86x^{10} - 21x^9 + 201x^8 - 51x^7 - 213x^6 + 88x^5 + 104x^4 - 50x^3 - 17x^2 + 10x - 1$
**d = 14, $r_1$= 12,** disc = $-470040281 \cdot 799069619$, **% = 9.33**
$x^{14} + x^{13} - 13x^{12} - 12x^{11} + 65x^{10} + 53x^9 - 159x^8 - 109x^7 + 197x^6 + 107x^5 - 114x^4 - 45x^3 + 25x^2 + 5x - 1$
**d = 14, $r_1$= 14,** disc = $32354821^2 1697$, **% = 8.32**
$x^{14} + 2x^{13} - 15x^{12} - 19x^{11} + 90x^{10} + 56x^9 - 255x^8 - 46x^7 + 338x^6 - 30x^5 - 184x^4 + 47x^3 + 23x^2 - 10x + 1$

**d = 15, $r_1$= 1,** disc = $-47 \cdot 163 \cdot 52868110651$, **% = 2.51**
$x^{15} + x^{14} + 3x^{13} + 2x^{12} + 4x^{11} + 4x^{10} + 5x^9 + 5x^8 + 4x^7 + 4x^6 + 3x^5 + 3x^4 + x^3 + 2x^2 + 1$
**d = 15, $r_1$= 3,** disc = $238859 \cdot 8088865531$, **% = 2.68**
$x^{15} + x^{14} - 3x^{13} + x^{12} + 4x^{11} - 7x^{10} + 3x^9 + 3x^8 - 9x^7 + 8x^6 - 2x^5 - 3x^4 + 4x^3 - 3x^2 + 2x - 1$
**d = 15, $r_1$= 5,** disc = $-12557469881316011$, **% = 4.75**
$x^{15} + 2x^{14} - 11x^{13} - 22x^{12} + 47x^{11} + 94x^{10} - 99x^9 - 197x^8 + 109x^7 + 210x^6 - 63x^5 - 106x^4 + 18x^3 + 19x^2 - 2x - 1$
**d = 15, $r_1$= 7,** disc = $101 \cdot 298153 \cdot 1658863849$, **% = 3.19**
$x^{15} - x^{14} - 11x^{13} + 11x^{12} + 47x^{11} - 47x^{10} - 98x^9 + 99x^8 + 101x^7 - 107x^6 - 43x^5 + 55x^4 + x^3 - 10x^2 + 2x + 1$

**d = 15, r$_1$= 9,** disc = $-227274217 \cdot 1141554223$, **% = 3.27**
$x^{15} - x^{14} - 12x^{13} + 11x^{12} + 56x^{11} - 47x^{10} - 128x^9 + 99x^8 + 148x^7 - 108x^6 - 80x^5 + 59x^4 + 17x^3 - 14x^2 - x + 1$
**d = 15, r$_1$= 11,** disc = $4999 \cdot 361914023922071$, **% = 5.20**
$x^{15} - 2x^{14} - 12x^{13} + 23x^{12} + 57x^{11} - 102x^{10} - 136x^9 + 219x^8 + 169x^7 - 234x^6 - 100x^5 + 114x^4 + 21x^3 - 18x^2 - 1$
**d = 15, r$_1$= 13,** disc = $-37 \cdot 1423 \cdot 3413 \cdot 189288065789$, **% = 14.29**
$x^{15} - 10x^{14} + 32x^{13} - 9x^{12} - 142x^{11} + 190x^{10} + 207x^9 - 446x^8 - 128x^7 + 441x^6 + 46x^5 - 190x^4 - 17x^3 + 26x^2 + x - 1$
**d = 15, r$_1$= 15,** disc = $251 \cdot 1446792967245019907$, **% = 19.37**
$x^{15} + 2x^{14} - 14x^{13} - 22x^{12} + 78x^{11} + 82x^{10} - 214x^9 - 116x^8 + 289x^7 + 40x^6 - 172x^5 + 12x^4 + 44x^3 - 8x^2 - 4x + 1$

**d = 16, r$_1$= 0,** disc = $7^2 7523939^2$, **% = 1.73**
$x^{16} - x^{14} + x^{13} - 2x^{11} + x^{10} + x^9 - x^8 + x^7 + x^6 - 2x^5 + x^3 - x^2 + 1$
**d = 16, r$_1$= 2,** disc = $-7245127^2 223$, **% = 1.05**
$x^{16} + 3x^{15} + 2x^{14} - 5x^{13} - 11x^{12} - 2x^{11} + 16x^{10} + 15x^9 - 7x^8 - 18x^7 - 6x^6 + 10x^5 + 8x^4 - 2x^3 - 3x^2 - x + 1$
**d = 16, r$_1$= 4,** disc = $26061149^2 89$, **% = 1.43**
$x^{16} + 8x^{15} + 34x^{14} + 98x^{13} + 207x^{12} + 332x^{11} + 400x^{10} + 339x^9 + 137x^8 - 122x^7 - 316x^6 - 365x^5 - 285x^4 - 158x^3 - 58x^2 - 12x - 1$
**d = 16, r$_1$= 6,** disc = $-488576402290603343$, **% = 4.49**
$x^{16} - 2x^{15} - 9x^{14} + 18x^{13} + 31x^{12} - 62x^{11} - 50x^{10} + 101x^9 + 36x^8 - 77x^7 - 8x^6 + 23x^5 - 2x^3 - 1$
**d = 16, r$_1$= 8,** disc = $94156147^2 233$, **% = 3.19**
$x^{16} - 3x^{15} - 13x^{14} + 53x^{13} + 28x^{12} - 319x^{11} + 262x^{10} + 656x^9 - 1343x^8 + 366x^7 + 1420x^6 - 2084x^5 + 1431x^4 - 574x^3 + 137x^2 - 18x + 1$
**d = 16, r$_1$= 10,** disc = $-140277676681898334 31$, **% = 4.78**
$x^{16} + x^{15} - 14x^{14} - 13x^{13} + 78x^{12} + 67x^{11} - 221x^{10} - 174x^9 + 338x^8 + 241x^7 - 273x^6 - 176x^5 + 103x^4 + 63x^3 - 11x^2 - 8x - 1$
**d = 16, r$_1$= 12,** disc = $31 \cdot 2938870167503622419$, **% = 5.92**
$x^{16} - 6x^{15} + 3x^{14} + 44x^{13} - 68x^{12} - 112x^{11} + 264x^{10} + 100x^9 - 446x^8 + 26x^7 + 364x^6 - 88x^5 - 137x^4 + 41x^3 + 20x^2 - 4x - 1$
**d = 16, r$_1$= 14,** disc = $-2^{16} 3^8 5^1 220639$, **% = 15.96**
$x^{16} - 8x^{15} + 20x^{14} - 78x^{12} + 104x^{11} + 40x^{10} - 200x^9 + 129x^8 + 112x^7 - 188x^6 + 8x^5 + 93x^4 - 18x^3 - 17x^2 + 2x + 1$
**d = 16, r$_1$= 16,** disc = $5^8 19^2 94439^2 3301$, **% = 8.30**
$x^{16} - 8x^{15} + 15x^{14} + 35x^{13} - 140x^{12} + 21x^{11} + 375x^{10} - 280x^9 - 418x^8 + 437x^7 + 216x^6 - 263x^5 - 59x^4 + 62x^3 + 11x^2 - 5x - 1$

**d = 17, r$_1$= 1,** disc = $26183 \cdot 1017307 \cdot 5721029$, **% = 4.20**
$x^{17} + 3x^{16} + 5x^{15} + 7x^{14} + 9x^{13} + 11x^{12} + 13x^{11} + 16x^{10} + 18x^9 + 18x^8 + 16x^7 + 14x^6 + 12x^5 + 11x^4 + 9x^3 + 6x^2 + 3x + 1$
**d = 17, r$_1$= 3,** disc = $-53717 \cdot 18146684417803$, **% = 5.84**

$x^{17}-3x^{16}+5x^{15}-6x^{14}+3x^{13}+2x^{12}-7x^{11}+9x^{10}-7x^9+4x^8+x^7-2x^6+3x^5-2x^4-x^2-1$
**d = 17, $r_1$= 5,** disc $= 211 \cdot 16410262530056039$, % = **3.66**
$x^{17}+6x^{16}+8x^{15}-16x^{14}-39x^{13}+21x^{12}+91x^{11}-5x^{10}-123x^9-16x^8+105x^7+15x^6-61x^5-3x^4+22x^3-2x^2-4x+1$
**d = 17, $r_1$= 7,** disc $= -4439838149 \cdot 6843463387$, % = **6.89**
$x^{17}-15x^{15}+x^{14}+92x^{13}-11x^{12}-297x^{11}+47x^{10}+541x^9-99x^8-552x^7+107x^6+292x^5-55x^4-66x^3+10x^2+4x-1$
**d = 17, $r_1$= 9,** disc $= 83 \cdot 787678603 \cdot 4269337097$, % = **10.34**
$x^{17}-4x^{16}-6x^{15}+39x^{14}+2x^{13}-149x^{12}+55x^{11}+286x^{10}-144x^9-293x^8+142x^7+155x^6-53x^5-36x^4+3x^3+2x^2+1$
**d = 17, $r_1$= 11,** disc $= -449309717 \cdot 2682889787819$, % = **8.80**
$x^{17}+x^{16}-14x^{15}-12x^{14}+81x^{13}+57x^{12}-250x^{11}-136x^{10}+442x^9+170x^8-444x^7-104x^6+232x^5+24x^4-49x^3-x^2+2x+1$
**d = 17, $r_1$= 13,** disc $= 457 \cdot 55846971524054703281$, % = **17.63**
$x^{17}-x^{16}-16x^{15}+15x^{14}+105x^{13}-92x^{12}-362x^{11}+296x^{10}+695x^9-531x^8-720x^7+517x^6+351x^5-240x^4-54x^3+36x^2-1$
**d = 17, $r_1$= 15,** disc $= -754424650732128851556379$, % = **29.53**
$x^{17}+x^{16}-16x^{15}-15x^{14}+104x^{13}+90x^{12}-353x^{11}-276x^{10}+670x^9+459x^8-708x^7-406x^6+392x^5+174x^4-100x^3-28x^2+9x+1$

**d = 18, $r_1$= 0,** disc $= -(44058793)^2 419$, % = **1.89**
$\mathrm{Res}(x^9-5x^8+15x^7-30x^6+45x^5-50x^4+42x^3-24x^2+8x-1, y^2-y+x)$
**d = 18, $r_1$= 2,** disc $= (43 \cdot 1693 \cdot 27067)^2$, % = **1.69**
$\mathrm{Res}(x^9+8x^8+26x^7+46x^6+50x^5+30x^4-3x^3-18x^2-8x-1, y^2+y-x)$
**d = 18, $r_1$= 4,** disc $= -(-228936047)^2 419$, % = **2.28**
$\mathrm{Res}(x^9+2x^8+5x^7+2x^6+x^5-7x^4-3x^3-3x^2+2x+1, (y^2+y+1)x+y)$
**d = 18, $r_1$= 6,** disc $= (-107 \cdot 1791541)^2 3709$, % = **3.24**
$\mathrm{Res}(x^9-2x^8+x^7+3x^6-6x^5+3x^4+x^3-4x^2+3x-1, -x+(y^2+y-1))$
**d = 18, $r_1$= 8,** disc $= -(41 \cdot 11221481)^2 4951$, % = **5.31**
$\mathrm{Res}(x^9-7x^7+x^6+14x^5+x^4-13x^3-2x^2+5x-1, yx^2+(y^2-1)x+(-y+1))$
**d = 18, $r_1$= 10,** disc $= (-757 \cdot 3052187)^2 1009$, % = **4.89**
$\mathrm{Res}(x^9-12x^8+56x^7-129x^6+148x^5-63x^4-19x^3+18x^2-1, y^2+y-x)$
**d = 18, $r_1$= 12,** disc $= -(13 \cdot 11743 \cdot 122867)^2 107$, % = **6.14**
$\mathrm{Res}(x^9-2x^8-14x^7+12x^6+76x^5+17x^4-125x^3-110x^2-21x-1, y^2+(x-1)y+1)$
**d = 18, $r_1$= 14,** disc $= (-337 \cdot 6396703)^2 337 \cdot 137$, % = **6.07**
$\mathrm{Res}(x^9-14x^8+74x^7-186x^6+217x^5-70x^4-51x^3+17x^2+10x+1, y^2+y-x)$
**d = 18, $r_1$= 16,** disc $= -(9685993193)^2 11519$, % = **5.15**
$\mathrm{Res}(x^9-16x^8+104x^7-349x^6+629x^5-556x^4+149x^3+52x^2-12x-1, y^2+y-x)$
**d = 18, $r_1$= 18,** disc $= 3^{27}7^{15}$, % = **15.68**
$\chi(2\cos(\frac{2\pi}{63}))$

**d = 19, $r_1$= 1,** disc $= -67 \cdot 1283 \cdot 9339373 \cdot 90896347$, % = **6.45**
$x^{19}+9x^{18}+44x^{17}+152x^{16}+405x^{15}+876x^{14}+1584x^{13}+2437x^{12}+3232x^{11}+3714x^{10}+$

$3714x^9 + 3231x^8 + 2437x^7 + 1584x^6 + 876x^5 + 405x^4 + 152x^3 + 44x^2 + 9x + 1$
**d = 19, r₁= 3,** disc $= 23 \cdot 8693 \cdot 14327 \cdot 308373499769$, **% = 11.37**
$x^{19} + 3x^{18} - 4x^{17} - 16x^{16} + 13x^{15} + 47x^{14} - 32x^{13} - 84x^{12} + 59x^{11} + 97x^{10} - 74x^9 - 76x^8 + 65x^7 + 41x^6 - 42x^5 - 12x^4 + 18x^3 - 4x + 1$
**d = 19, r₁= 5,** disc $= -169319 \cdot 31967917 \cdot 303131581$, **% = 5.42**
$x^{19} + 2x^{18} - 7x^{17} - 10x^{16} + 27x^{15} + 21x^{14} - 62x^{13} - 19x^{12} + 92x^{11} - x^{10} - 92x^9 + 23x^8 + 62x^7 - 27x^6 - 27x^5 + 17x^4 + 7x^3 - 6x^2 - x + 1$
**d = 19, r₁= 7,** disc $= 461 \cdot 6263 \cdot 234203 \cdot 36009826129$, **% = 11.16**
$x^{19} + 9x^{18} + 23x^{17} - 11x^{16} - 108x^{15} - 24x^{14} + 264x^{13} + 75x^{12} - 441x^{11} - 77x^{10} + 510x^9 + 13x^8 - 386x^7 + 45x^6 + 172x^5 - 40x^4 - 37x^3 + 11x^2 + 3x - 1$
**d = 19, r₁= 9,** disc $= -37^2643 \cdot 1307909 \cdot 70504387781$, **% = 8.22**
$x^{19} + 2x^{18} - 16x^{17} - 31x^{16} + 110x^{15} + 203x^{14} - 425x^{13} - 729x^{12} + 1013x^{11} + 1558x^{10} - 1538x^9 - 2009x^8 + 1480x^7 + 1507x^6 - 865x^5 - 591x^4 + 276x^3 + 90x^2 - 36x + 1$
**d = 19, r₁= 11,** disc $= 677712175493888590645321$, **% = 10.44**
$x^{19} - 9x^{18} + 23x^{17} + 22x^{16} - 185x^{15} + 159x^{14} + 436x^{13} - 750x^{12} - 311x^{11} + 1201x^{10} - 188x^9 - 843x^8 + 367x^7 + 201x^6 - 176x^5 + 36x^4 + 42x^3 - 15x^2 - 9x - 1$
**d = 19, r₁= 13,** disc $= -163 \cdot 223 \cdot 5297 \cdot 922853 \cdot 28394771507$, **% = 11.90**
$x^{19} + 2x^{18} - 16x^{17} - 30x^{16} + 109x^{15} + 186x^{14} - 411x^{13} - 615x^{12} + 930x^{11} + 1168x^{10} - 1275x^9 - 1281x^8 + 1016x^7 + 775x^6 - 428x^5 - 226x^4 + 80x^3 + 21x^2 - 6x - 1$
**d = 19, r₁= 15,** disc $= 251 \cdot 22567 \cdot 34961 \cdot 341215563237469$, **% = 16.82**
$x^{19} + 9x^{18} + 21x^{17} - 35x^{16} - 195x^{15} - 62x^{14} + 628x^{13} + 552x^{12} - 1004x^{11} - 1173x^{10} + 865x^9 + 1145x^8 - 395x^7 - 528x^6 + 86x^5 + 98x^4 - 7x^3 - 6x^2 + 1$

**d = 20, r₁= 0,** disc $= (193 \cdot 7592561)^2137$, **% = 2.70**
$\mathrm{Res}(x^{10} + 10x^9 + 47x^8 + 133x^7 + 243x^6 + 297x^5 + 253x^4 + 152x^3 + 58x^2 + 12x + 1, y^2 + y - x)$
**d = 20, r₁= 2,** disc $= -(-673 \cdot 2281 \cdot 2803)^2 67$, **% = 1.66**
$\mathrm{Res}(x^{10} + 9x^9 + 34x^8 + 69x^7 + 79x^6 + 52x^5 + 33x^4 + 38x^3 + 28x^2 + 9x + 1, y^2 + y - x)$
**d = 20, r₁= 4,** disc $= (-83 \cdot 1181 \cdot 49597)^2 349$, **% = 2.81**
$\mathrm{Res}(x^{10} - 3x^9 - x^8 + 17x^7 - 28x^6 + 45x^4 - 56x^3 + 32x^2 - 9x + 1, y^2 + xy + 1)$
**d = 20, r₁= 6,** disc $= -(-29 \cdot 103 \cdot 181 \cdot 6229)^2 59 \cdot 89$, **% = 4.27**
$\mathrm{Res}(x^{10} - 2x^9 + 3x^8 - 3x^7 - x^6 + 3x^5 - 5x^4 + 3x^3 - x + 1, y^2x^2 + y - x)$
**d = 20, r₁= 8,** disc $= (-41 \cdot 197 \cdot 610823)^2 13829$, **% = 4.34**
$\mathrm{Res}(x^{10} - 4x^9 + 12x^8 - 27x^7 + 41x^6 - 49x^5 + 45x^4 - 34x^3 + 20x^2 - 7x + 1, y^2 + xy - 1)$
**d = 20, r₁= 10,** disc $= -(97259 \cdot 221447)^2 6359$, **% = 6.61**
$\mathrm{Res}(x^{10} - x^9 - 6x^8 + 4x^7 + 17x^6 - 7x^5 - 23x^4 + 5x^3 + 12x^2 - 1, y^2x - (x^2 + 1)y + 1)$
**d = 20, r₁= 12,** disc $= (21535538293)^2 62533$, **% = 9.44**
$\mathrm{Res}(x^{10} + 3x^9 - 6x^8 + 18x^7 - 30x^6 + 3x^5 + 44x^4 - 56x^3 + 32x^2 - 9x + 1, y^2 + xy - 1)$
**d = 20, r₁= 14,** disc $= -(-449 \cdot 288418411)^2 43 \cdot 677$, **% = 15.29**
$\mathrm{Res}(x^{10} - 14x^9 + 81x^8 - 248x^7 + 423x^6 - 377x^5 + 124x^4 + 32x^3 - 24x^2 + 1, y^2 + y - x)$
**d = 20, r₁= 16,** disc $= (-130833798211)^2 23 \cdot 31 \cdot 137$, **% = 12.05**
$\mathrm{Res}(x^{10} - 12x^9 + 62x^8 - 186x^7 + 355x^6 - 426x^5 + 292x^4 - 88x^3 - 3x^2 + 7x - 1, y^2 + y - x)$
**d = 20, r₁= 20,** disc $= 5^{15}11^{18}$, **% = 17.60**
$\chi(2\cos(\frac{2\pi}{55}))$

**d = 21, r$_1$= 1,** disc = 34482057615039759645721, **% = 7.90**
$x^{21}+2x^{20}-9x^{19}-21x^{18}+31x^{17}+90x^{16}-53x^{15}-214x^{14}+51x^{13}+333x^{12}-23x^{11}-361x^{10}-4x^9+277x^8+12x^7-149x^6-6x^5+53x^4+x^3-11x^2+1$
**d = 21, r$_1$= 3,** disc = $-42473\cdot 522703\cdot 6783116077093$, **% = 6.87**
$x^{21}+x^{20}-10x^{19}-5x^{18}+45x^{17}+18x^{16}-120x^{15}-24x^{14}+210x^{13}+2x^{12}-252x^{11}+41x^{10}+210x^9-67x^8-120x^7+56x^6+45x^5-28x^4-10x^3+8x^2+x-1$
**d = 21, r$_1$= 5,** disc = $31\cdot 73\cdot 25876054049\cdot 51212997919$, **% = 13.65**
$x^{21}+3x^{20}-13x^{19}-42x^{18}+72x^{17}+250x^{16}-223x^{15}-821x^{14}+428x^{13}+1613x^{12}-536x^{11}-1919x^{10}+451x^9+1328x^8-256x^7-476x^6+92x^5+64x^4-16x^3+1$
**d = 21, r$_1$= 7,** disc = $-3539\cdot 5417601579682951682501$, **% = 14.36**
$x^{21}-18x^{19}+139x^{17}-603x^{15}+x^{14}+1616x^{13}-11x^{12}-2770x^{11}+47x^{10}+3037x^9-99x^8-2064x^7+107x^6+807x^5-55x^4-155x^3+10x^2+10x-1$
**d = 21, r$_1$= 9,** disc = $239\cdot 2357\cdot 1468904243\cdot 88207486933$, **% = 12.16**
$x^{21}-3x^{20}-14x^{19}+46x^{18}+81x^{17}-301x^{16}-244x^{15}+1093x^{14}+378x^{13}-2397x^{12}-170x^{11}+3235x^{10}-367x^9-2618x^8+652x^7+1175x^6-415x^5-246x^4+106x^3+16x^2-8x-1$
**d = 21, r$_1$= 11,** disc = $(-13\cdot 157\cdot 1367)^3 29\cdot 4647521$, **% = 22.93**
$\mathrm{Res}(x^7-9x^6+39x^5-93x^4+105x^3-53x^2+12x-1,(y^3-y^2-1)x+(-y^2+y+1))$
**d = 21, r$_1$= 13,** disc = $1117\cdot 2432113\cdot 2319299879622756101$, **% = 17.10**
$x^{21}+2x^{20}-18x^{19}-35x^{18}+140x^{17}+262x^{16}-614x^{15}-1092x^{14}+1660x^{13}+2761x^{12}-2836x^{11}-4320x^{10}+3008x^9+4079x^8-1854x^7-2149x^6+567x^5+528x^4-54x^3-36x^2-1$
**d = 21, r$_1$= 15,** disc = $-45513355273\cdot 2266108586355582979$, **% = 22.76**
$x^{21}-20x^{19}+2x^{18}+162x^{17}-28x^{16}-691x^{15}+153x^{14}+1699x^{13}-427x^{12}-2489x^{11}+666x^{10}+2184x^9-607x^8-1130x^7+328x^6+331x^5-101x^4-50x^3+16x^2+3x-1$

**d = 22, r$_1$= 0,** disc = $-(509\cdot 62416433)^2 107$, **% = 3.14**
$\mathrm{Res}(x^{11}-5x^{10}+4x^9+18x^8-40x^7+20x^6+23x^5-46x^4+41x^3-21x^2+7x-1,y^2+xy+1)$
**d = 22, r$_1$= 2,** disc = $(2069\cdot 35952097)^2 97$, **% = 2.77**
$\mathrm{Res}(x^{11}-8x^9+22x^7+2x^6-25x^5-6x^4+10x^3+4x^2+1,y^2+xy+1)$
**d = 22, r$_1$= 4,** disc = $-(-1553\cdot 2011\cdot 66413)^2 79$, **% = 3.43**
$\mathrm{Res}(x^{11}+9x^{10}+30x^9+35x^8-46x^7-213x^6-327x^5-279x^4-138x^3-30x^2+4x+1,y^2+xy+1)$
**d = 22, r$_1$= 6,** disc = $(41\cdot 702937801)^2 29017$, **% = 4.52**
$\mathrm{Res}(x^{11}+10x^{10}+44x^9+109x^8+158x^7+117x^6-87x^4-92x^3-50x^2-12x-1,y^2+y-x)$
**d = 22, r$_1$= 8,** disc = $-521\cdot 1581193\cdot 11899067\cdot 36512520553$, **% = 9.12**
$x^{22}-18x^{20}-x^{19}+139x^{18}+16x^{17}-602x^{16}-108x^{15}+1604x^{14}+400x^{13}-2711x^{12}-885x^{11}+2882x^{10}+1192x^9-1827x^8-950x^7+594x^6+408x^5-50x^4-72x^3-12x^2+1$
**d = 22, r$_1$= 10,** disc = $(-53^2 50211527)^2 80849$, **% = 7.80**
$\mathrm{Res}(x^{11}-x^{10}+2x^9-3x^8-5x^7+5x^6+3x^5-2x^4-2x^3+2x+1,y^2+xy-1)$
**d = 22, r$_1$= 12,** disc = $-(61\cdot 449\cdot 2089\cdot 12613)^2 58151$, **% = 13.56**
$\mathrm{Res}(x^{11}-10x^{10}+43x^9-100x^8+121x^7-30x^6-111x^5+128x^4-27x^3-20x^2+3x+1,y^2+y-x)$
**d = 22, r$_1$= 14,** disc = $(727\cdot 1041646127)^2 498301$, **% = 15.84**
$\mathrm{Res}(x^{11}-11x^{10}+53x^9-148x^8+262x^7-299x^6+220x^5-112x^4+44x^3-7x^2-3x+1,y^2+y-x)$
**d = 22, r$_1$= 16,** disc = $-(-8147\cdot 9341\cdot 59809)^2 401\cdot 571$, **% = 21.14**

$\mathrm{Res}(x^{11}-9x^{10}+27x^9-19x^8-49x^7+77x^6+14x^5-64x^4+9x^3+15x^2-2x-1, y^2+y-x)$
**d = 22, $\mathbf{r_1}$= 18,** $\mathrm{disc} = (-739\cdot 2687\cdot 2800403)^2 426661$**, % = 16.71**
$\mathrm{Res}(x^{11}-2x^9-x^8-12x^7+2x^6+26x^5+3x^4-16x^3-4x^2+3x+1, y^2+xy-1)$

**d = 23, $\mathbf{r_1}$= 1,** $\mathrm{disc} = -947\cdot 967\cdot 28169528890267476263$**, % = 11.04**
$x^{23}+2x^{22}+6x^{21}+11x^{20}+20x^{19}+31x^{18}+45x^{17}+60x^{16}+75x^{15}+89x^{14}+99x^{13}+105x^{12}+106x^{11}+101x^{10}+92x^9+79x^8+64x^7+49x^6+35x^5+23x^4+13x^3+7x^2+3x+1$
**d = 23, $\mathbf{r_1}$= 3,** $\mathrm{disc} = 7829\cdot 549257\cdot 18597740496250117$**, % = 8.28**
$x^{23}+13x^{22}+89x^{21}+419x^{20}+1506x^{19}+4359x^{18}+10482x^{17}+21355x^{16}+37346x^{15}+56581x^{14}+74757x^{13}+86532x^{12}+87967x^{11}+78546x^{10}+61434x^9+41853x^8+24620x^7+12355x^6+5203x^5+1797x^4+492x^3+101x^2+14x+1$
**d = 23, $\mathbf{r_1}$= 5,** $\mathrm{disc} = -1591567\cdot 533438881419590803169$**, % = 11.28**
$x^{23}-14x^{21}+10x^{20}+58x^{19}-38x^{18}-160x^{17}+86x^{16}+304x^{15}-134x^{14}-404x^{13}+142x^{12}+387x^{11}-100x^{10}-272x^9+44x^8+139x^7-11x^6-50x^5+3x^4+14x^3-x^2-4x-1$
**d = 23, $\mathbf{r_1}$= 7,** $\mathrm{disc} = 1787\cdot 3221747\cdot 773453350035640613$**, % = 10.81**
$x^{23}+3x^{22}-14x^{21}-46x^{20}+82x^{19}+301x^{18}-262x^{17}-1097x^{16}+504x^{15}+2438x^{14}-622x^{13}-3401x^{12}+534x^{11}+2955x^{10}-345x^9-1535x^8+156x^7+440x^6-37x^5-61x^4+3x^3+3x^2+1$
**d = 23, $\mathbf{r_1}$= 9,** $\mathrm{disc} = -109\cdot 15281012461022479167477265 1$**, % = 8.63**
$x^{23}+3x^{22}-16x^{21}-51x^{20}+112x^{19}+379x^{18}-452x^{17}-1614x^{16}+1166x^{15}+4336x^{14}-2009x^{13}-7618x^{12}+2329x^{11}+8770x^{10}-1759x^9-6433x^8+784x^7+2808x^6-156x^5-628x^4+48x^2-1$
**d = 23, $\mathbf{r_1}$= 13,** $\mathrm{disc} = -5^2 3061\cdot 302297\cdot 2364287\cdot 24193169507669$**, % = 12.33**
$x^{23}+2x^{22}-21x^{21}-41x^{20}+194x^{19}+366x^{18}-1038x^{17}-1866x^{16}+3564x^{15}+5988x^{14}-8220x^{13}-12564x^{12}+12951x^{11}+17334x^{10}-13887x^9-15399x^8+9890x^7+8350x^6-4434x^5-2470x^4+1120x^3+300x^2-120x-1$

**d = 24, $\mathbf{r_1}$= 0,** $\mathrm{disc} = (-601\cdot 3943\cdot 185057)^2 197$**, % = 3.07**
$\mathrm{Res}(x^{12}-x^{11}-6x^{10}+10x^9+4x^8-29x^7+29x^6+6x^5-40x^4+42x^3-23x^2+7x-1, y^2+xy+1)$
**d = 24, $\mathbf{r_1}$= 2,** $\mathrm{disc} = -(-73\cdot 48563\cdot 75289)^2 4751$**, % = 5.12**
$\mathrm{Res}(x^{12}-3x^{11}-3x^{10}+11x^9+9x^8-17x^7-19x^6+9x^5+18x^4+4x^3-6x^2-4x-1, y^2+xy+1)$
**d = 24, $\mathbf{r_1}$= 4,** $\mathrm{disc} = (-1117\cdot 2749\cdot 137443)^2 10009$**, % = 4.79**
$\mathrm{Res}(x^{12}+6x^{11}+15x^{10}+15x^9-10x^8-49x^7-65x^6-46x^5-20x^4-11x^3-10x^2-6x-1, y^2+y-x)$
**d = 24, $\mathbf{r_1}$= 6,** $\mathrm{disc} = -(4951\cdot 235786027)^2 17351$**, % = 8.45**
$\mathrm{Res}(x^{12}-7x^{11}+13x^{10}+10x^9-47x^8+9x^7+60x^6-22x^5-36x^4+12x^3+9x^2-2x-1, y^2+xy+1)$
**d = 24, $\mathbf{r_1}$= 8,** $\mathrm{disc} = (2^{12}31^2 103\cdot 2309)^2 163601$**, % = 8.56**
$\mathrm{Res}(x^{12}-12x^{11}+62x^{10}-180x^9+318x^8-336x^7+173x^6+20x^5-74x^4+24x^3+10x^2-4x-1, y^2+y-x)$
**d = 24, $\mathbf{r_1}$= 10,** $\mathrm{disc} = -(-67\cdot 104864533273)^2 23399$**, % = 9.88**
$\mathrm{Res}(x^{12}-14x^{11}+86x^{10}-304x^9+679x^8-983x^7+893x^6-434x^5+21x^4+83x^3-24x^2-4x+1, y^2+y-x)$
**d = 24, $\mathbf{r_1}$= 12,** $\mathrm{disc} = (-73\cdot 73038811211)^2 463\cdot 2423$**, % = 16.98**
$\mathrm{Res}(x^{12}-10x^{11}+37x^{10}-55x^9+2x^8+73x^7-37x^6-38x^5+19x^4+10x^3+2x^2-4x-1, y^2+y-x)$
**d = 24, $\mathbf{r_1}$= 14,** $\mathrm{disc} = -(12781\cdot 2585448361)^2 239831$**, % = 18.32**
$\mathrm{Res}(x^{12}-10x^{11}+48x^{10}-136x^9+226x^8-184x^7-17x^6+174x^5-131x^4+14x^3+18x^2-$

$3x-1, y^2+y-x)$
**d = 24, r$_1$= 16,** disc = $(46454430474329)^2 1249 \cdot 1489$, **% = 22.75**
$\mathrm{Res}(x^{12}-8x^{11}+17x^{10}+14x^9-73x^8+5x^7+116x^6-14x^5-82x^4+3x^3+23x^2-1, y^2+y-x)$
**d = 24, r$_1$= 20,** disc = $(1091 \cdot 140312594369)^2 2^{24}$, **% = 27.15**
$\mathrm{Res}(x^{12}-21x^{11}+192x^{10}-1005x^9+3301x^8-7050x^7+9900x^6-9115x^5+5420x^4-2007x^3+427x^2-43x+1, y^2-x)$
**d = 24, r$_1$= 24,** disc = $3^{12}5^{18}7^{20}$, **% = 4.62**
$\chi(2\cos(\frac{2\pi}{105}))$

**d = 25, r$_1$= 1,** disc = $383 \cdot 213139 \cdot 71666561 \cdot 22067169745241$, **% = 22.48**
$x^{25}-2x^{24}+3x^{23}-4x^{22}+5x^{21}-6x^{20}+7x^{19}-8x^{18}+9x^{17}-9x^{16}+9x^{15}-8x^{14}+6x^{13}-5x^{12}+3x^{11}-x^{10}+x^8-2x^7+3x^6-3x^5+3x^4-3x^3+2x^2-x+1$
**d = 25, r$_1$= 3,** disc = $-41617 \cdot 145981284945445034615143 27$, **% = 21.53**
$x^{25}-11x^{24}+67x^{23}-284x^{22}+924x^{21}-2422x^{20}+5267x^{19}-9671x^{18}+15156x^{17}-20380x^{16}+23531x^{15}-23217x^{14}+19327x^{13}-13188x^{12}+6860x^{11}-2053x^{10}-569x^9+1353x^8-1118x^7+604x^6-211x^5+25x^4+22x^3-18x^2+7x-1$
**d = 25, r$_1$= 5,** disc = $197 \cdot 179805641 \cdot 45786768231018741281$, **% = 17.79**
$x^{25}-10x^{24}+54x^{23}-208x^{22}+628x^{21}-1568x^{20}+3345x^{19}-6226x^{18}+10268x^{17}-15159x^{16}+20187x^{15}-24371x^{14}+26756x^{13}-26756x^{12}+24370x^{11}-20187x^{10}+15159x^9-10268x^8+6226x^7-3345x^6+1568x^5-628x^4+208x^3-54x^2+10x-1$
**d = 25, r$_1$= 7,** disc = $-16693453533590270424331126316771$, **% = 20.40**
$x^{25}+12x^{24}+66x^{23}+220x^{22}+486x^{21}+702x^{20}+518x^{19}-297x^{18}-1400x^{17}-1884x^{16}-1075x^{15}+591x^{14}+1778x^{13}+1549x^{12}+312x^{11}-716x^{10}-824x^9-315x^8+125x^7+206x^6+86x^5-10x^4-24x^3-8x^2+x+1$
**d = 25, r$_1$= 9,** disc = $2079577 \cdot 19707605083396464316201 0417$, **% = 27.34**
$x^{25}+12x^{24}+46x^{23}+8x^{22}-353x^{21}-556x^{20}+1058x^{19}+2769x^{18}-1737x^{17}-7157x^{16}+2038x^{15}+11826x^{14}-2689x^{13}-13222x^{12}+4084x^{11}+9780x^{10}-4661x^9-4233x^8+3201x^7+626x^6-1128x^5+219x^4+126x^3-72x^2+14x-1$
**d = 25, r$_1$= 11,** disc = $-23^2 3203 \cdot 29390063 \cdot 38884243 \cdot 318061223317$, **% = 20.35**
$x^{25}-11x^{24}+41x^{23}-20x^{22}-264x^{21}+611x^{20}+237x^{19}-2355x^{18}+1587x^{17}+3945x^{16}-5115x^{15}-3518x^{14}+7264x^{13}+2117x^{12}-6353x^{11}-1456x^{10}+3812x^9+1151x^8-1463x^7-618x^6+224x^5+160x^4+36x^3-5x^2-6x-1$

**d = 26, r$_1$= 0,** disc = $-(1535761 \cdot 7036903)^2 239$, **% = 5.79**
$\mathrm{Res}(x^{13}+x^{12}-10x^{11}-8x^{10}+38x^9+22x^8-69x^7-24x^6+62x^5+7x^4-26x^3+2x^2+4x-1, y^2+xy+1)$
**d = 26, r$_1$= 2,** disc = $(199 \cdot 18025912231)^2 9181$, **% = 4.56**
$\mathrm{Res}(x^{13}-4x^{12}+3x^{11}+6x^{10}-7x^9-3x^8+2x^7+x^6+5x^5-x^4-4x^3+x^2-1, (y^2-y+1)x-1)$
**d = 26, r$_1$= 4,** disc = $-(-101 \cdot 7351 \cdot 15906221)^2 7459$, **% = 6.21**
$\mathrm{Res}(x^{13}+2x^{12}-4x^{10}-6x^9-x^8+6x^7+6x^6-3x^4+x^2-1, (y^2-y+1)x+1)$
**d = 26, r$_1$= 6,** disc = $(35751827796541)^2 17377$, **% = 11.54**
$\mathrm{Res}(x^{13}+x^{12}-9x^{11}-9x^{10}+29x^9+28x^8-40x^7-34x^6+22x^5+11x^4-3x^3+3x^2+1, y^2+(x^2-1)y+1)$

**d = 26, r$_1$= 8,** disc = $-48212963 \cdot 60226581923975979748407 41$, **% = 14.88**
$x^{26}+4x^{25}-15x^{24}-75x^{23}+85x^{22}+617x^{21}-171x^{20}-2923x^{19}-402x^{18}+8794x^{17}+3303x^{16}-17461x^{15}-9211x^{14}+23001x^{13}+14633x^{12}-19630x^{11}-14360x^{10}+10183x^9+8674x^8-2744x^7-3040x^6+187x^5+536x^4+53x^3-33x^2-6x+1$
**d = 26, r$_1$= 10,** disc = $(281 \cdot 135009882661)^2 31 \cdot 35839$, **% = 14.37**
$\mathrm{Res}(x^{13}+5x^{12}+2x^{11}-24x^{10}-27x^9+39x^8+54x^7-26x^6-31x^5+9x^4-4x^3-2x^2+4x-1, y^2+y-(1+x))$
**d = 26, r$_1$= 12,** disc = $-(-7^2 113 \cdot 57512297251)^2 1301171$, **% = 26.28**
$\mathrm{Res}(x^{13}-2x^{12}-5x^{11}-9x^{10}-12x^9+31x^8+43x^7-39x^6-40x^5+25x^4+15x^3-8x^2-2x+1, (y^2-y-1)x+1)$
**d = 26, r$_1$= 14,** disc = $(-31 \cdot 53 \cdot 242591 \cdot 421459)^2 443 \cdot 22367$, **% = 21.04**
$\mathrm{Res}(x^{13}-4x^{12}+5x^{11}+x^{10}-12x^9+14x^8-x^7-12x^6+12x^5-5x^3+3x^2-1, (y^2-y-1)x+1)$
**d = 26, r$_1$= 16,** disc = $-179 \cdot 6619 \cdot 18089 \cdot 81943 \cdot 6130472768243884285993$, **% = 29.63**
$x^{26}-13x^{24}-15x^{23}+78x^{22}+154x^{21}-286x^{20}-579x^{19}+715x^{18}+865x^{17}-1287x^{16}+124x^{15}+1716x^{14}-2229x^{13}-1716x^{12}+3421x^{11}+1287x^{10}-2709x^9-715x^8+1279x^7+286x^6-364x^5-78x^4+58x^3+13x^2-4x-1$
**d = 26, r$_1$= 18,** disc = $(1138094965960681)^2 1151 \cdot 35851$, **% = 28.24**
$\mathrm{Res}(x^{13}-2x^{12}-9x^{11}+17x^{10}+30x^9-51x^8-46x^7+64x^6+33x^5-30x^4-9x^3+2x^2+1, (y^2-y-1)x-1)$

**d = 27, r$_1$= 1,** disc = $-263 \cdot 58741 \cdot 10279807631 \cdot 486756036921719$, **% = 22.87**
$x^{27}-15x^{26}+121x^{25}-675x^{24}+2883x^{23}-9941x^{22}+28578x^{21}-69944x^{20}+147849x^{19}-272648x^{18}+441763x^{17}-632028x^{16}+801119x^{15}-901499x^{14}+901498x^{13}-801119x^{12}+632028x^{11}-441763x^{10}+272648x^9-147849x^8+69944x^7-28578x^6+9941x^5-2883x^4+675x^3-121x^2+15x-1$
**d = 27, r$_1$= 3,** disc = $(43 \cdot 311 \cdot 2621)^3 167 \cdot 185881727$, **% = 27.88**
$\mathrm{Res}(x^9-2x^8-2x^7+5x^6+x^5-6x^4+x^3+3x^2-x-1, y^3-xy-1)$
**d = 27, r$_1$= 5,** disc = $(-17 \cdot 10058599)^3 3833 \cdot 216133$, **% = 24.80**
$\mathrm{Res}(x^9-2x^8-x^7+4x^6+x^5-5x^4+3x^2-x-1, (y^3-y^2)x+(-y^2+y+1))$
**d = 27, r$_1$= 7,** disc = $-(-97 \cdot 229 \cdot 5179)^3 59 \cdot 1031 \cdot 49559$, **% = 17.16**
$\mathrm{Res}(x^9-5x^8+7x^7-5x^5+5x^4-7x^3+4x+1, y^3-y-x)$
**d = 27, r$_1$= 9,** disc = $(-2300611591)^3 5^2 239 \cdot 2243$, **% = 24.99**
$\mathrm{Res}(x^9+2x^8-5x^7-7x^6+9x^4+8x^3-2x^2-4x-1, (y^3-y^2-1)x+(-y^2+y+1))$
**d = 27, r$_1$= 11,** disc = $(7^6 41 \cdot 97)^3 491 \cdot 28587287$, **% = 26.55**
$\mathrm{Res}(x^9+9x^7-27x^6-x^5+27x^4+4x^3-19x^2+8x-1, y^3-y-x)$
**d = 27, r$_1$= 13,** disc = $(-2307632671)^3 386365313$, **% = 23.48**
$\mathrm{Res}(x^9-3x^8-70x^7+172x^6+389x^5+219x^4+10x^3-30x^2-10x-1, (y^3-y^2)x+(-y^2+y+1))$

**d = 28, r$_1$= 0,** disc = $(-499 \cdot 1031 \cdot 66047903)^2 71 \cdot 503$, **% = 10.72**
$\mathrm{Res}(x^{14}-3x^{13}+3x^{11}+3x^{10}+x^9-7x^8+3x^6+3x^5-4x^3+1, y^2+xy+1)$
**d = 28, r$_1$= 2,** disc = $-(97 \cdot 1627 \cdot 579204319)^2 19 \cdot 23 \cdot 67$, **% = 10.74**
$\mathrm{Res}(x^{14}-4x^{12}+4x^{10}+x^9+2x^8-4x^7-5x^6+4x^5+2x^4+x^3-2x+1, (y^2-y+1)x-1)$
**d = 28, r$_1$= 4,** disc = $(61 \cdot 489487 \cdot 1687087)^2 288181$, **% = 8.01**

$\mathrm{Res}(x^{14}-2x^{13}+4x^{12}-8x^{11}+12x^{10}-17x^9+20x^8-23x^7+23x^6-20x^5+16x^4-11x^3+6x^2-3x+1,(y^2-y+1)x-1)$
**d = 28, r$_1$= 6,** disc = $-(-37\cdot 73\cdot 757\cdot 4481\cdot 34963)^2 139\cdot 1913$, **% = 15.22**
$\mathrm{Res}(x^{14}-x^{12}+2x^{11}-x^9+x^7-4x^5+2x^4+x^3-2x^2+x+1,(y^2-y+1)x+1)$
**d = 28, r$_1$= 8,** disc = $(-390725608087363)^2 59\cdot 9491$, **% = 12.43**
$\mathrm{Res}(x^{14}-7x^{12}-6x^{11}+18x^{10}+49x^9-41x^8-110x^7+52x^6+110x^5-27x^4-49x^3+4x^2+6x-1,(y^2-y-1)x-1)$
**d = 28, r$_1$= 10,** disc = $-(139\cdot 727\cdot 29437\cdot 1162597)^2 37\cdot 53\cdot 271$, **% = 22.77**
$\mathrm{Res}(x^{14}+2x^{13}-53x^{12}-335x^{11}-752x^{10}-347x^9+1626x^8+3809x^7+4182x^6+2835x^5+1297x^4+418x^3+95x^2+14x+1,y^2+xy+1)$
**d = 28, r$_1$= 12,** disc = $(4567\cdot 325253082499)^2 3047609$, **% = 15.12**
$\mathrm{Res}(x^{14}-2x^{13}-12x^{12}+12x^{11}+53x^{10}-25x^9-107x^8+23x^7+104x^6-11x^5-49x^4+2x^3+11x^2-1,(y^2-y-1)x+1)$
**d = 28, r$_1$= 16,** disc = $(-467729\cdot 28189872859)^2 29\cdot 761\cdot 1609$, **% = 28.42**
$\mathrm{Res}(x^{14}+3x^{13}-9x^{12}-31x^{11}+29x^{10}+123x^9-40x^8-236x^7+21x^6+223x^5-2x^4-90x^3+8x+1,y^2+y-(1+x))$
**d = 28, r$_1$= 20,** disc = $(131\cdot 535543521479983)^2 2243\cdot 23327$, **% = 28.05**
$\mathrm{Res}(x^{14}+x^{13}-12x^{12}-11x^{11}+55x^{10}+46x^9-120x^8-91x^7+125x^6+86x^5-52x^4-34x^3+3x^2+3x+1,(y^2-y-1)x-1)$

**d = 30, r$_1$= 0,** disc = $-(191\cdot 349\cdot 36980260927)^2 59\cdot 61$, **% = 11.17**
$\mathrm{Res}(x^{15}-3x^{14}-8x^{13}+28x^{12}+24x^{11}-103x^{10}-35x^9+189x^8+32x^7-180x^6-28x^5+83x^4+18x^3-14x^2-4x+1,y^2+xy+1)$
**d = 30, r$_1$= 2,** disc = $(-1333468588569033 1)^2 241$, **% = 7.07**
$\mathrm{Res}(x^{15}-x^{14}-13x^{13}+12x^{12}+68x^{11}-57x^{10}-183x^9+135x^8+269x^7-164x^6-212x^5+93x^4+82x^3-18x^2-12x-1,y^2+xy+1)$
**d = 30, r$_1$= 4,** disc = $-(157\cdot 257\cdot 271\cdot 547\cdot 333757)^2 327599$, **% = 12.93**
$\mathrm{Res}(x^{15}+10x^{14}+35x^{13}+34x^{12}-79x^{11}-195x^{10}-20x^9+272x^8+158x^7-153x^6-131x^5+34x^4+40x^3-2x^2-4x-1,y^2+xy+1)$
**d = 30, r$_1$= 6,** disc = $(-5419\cdot 5745289124693)^2 11617$, **% = 14.14**
$\mathrm{Res}(x^{15}+11x^{14}+41x^{13}+15x^{12}-331x^{11}-994x^{10}-835x^9+1470x^8+4709x^7+5843x^6+4218x^5+1952x^4+602x^3+124x^2+16x+1,y^2+xy+1)$
**d = 30, r$_1$= 8,** disc = $-(-2399\cdot 75557\cdot 123980029)^2 1020907$, **% = 21.90**
$\mathrm{Res}(x^{15}+15x^{14}+113x^{13}+551x^{12}+1827x^{11}+4053x^{10}+5658x^9+4070x^8-331x^7-3343x^6-2723x^5-844x^4+11x^3+69x^2+15x+1,y^2+y-x)$
**d = 30, r$_1$= 10,** disc = $(-30464899\cdot 1504584469)^2 571\cdot 2851$, **% = 22.02**
$\mathrm{Res}(x^{15}+14x^{14}+78x^{13}+207x^{12}+199x^{11}-232x^{10}-655x^9-179x^8+615x^7+357x^6-292x^5-179x^4+84x^3+30x^2-12x+1,y^2+xy+1)$

**d = 32, r$_1$= 0,** disc = $(-149\cdot 218869829180759)^2 23\cdot 263$, **% = 9.41**
$\mathrm{Res}(x^{16}-3x^{15}-9x^{14}+31x^{13}+32x^{12}-132x^{11}-56x^{10}+297x^9+47x^8-375x^7-11x^6+258x^5-8x^4-84x^3+4x^2+8x+1,y^2+xy+1)$
**d = 32, r$_1$= 2,** disc = $-(-43\cdot 3010213\cdot 749559169)^2 26879$, **% = 15.91**

$\mathrm{Res}(x^{16}+4x^{15}-4x^{14}-30x^{13}+93x^{11}+20x^{10}-152x^9-31x^8+135x^7+14x^6-58x^5+8x^3-1, y^2+xy+1)$
**d = 32, r₁= 4,** $\mathrm{disc} = (-6932117\cdot 3700929283)^2 277\cdot 2557$**, % = 11.54**
$\mathrm{Res}(x^{16}+11x^{15}+43x^{14}+50x^{13}-106x^{12}-316x^{11}-50x^{10}+549x^9+356x^8-427x^7-373x^6+157x^5+141x^4-24x^3-12x^2+1, y^2+xy+1)$
**d = 32, r₁= 6,** $\mathrm{disc} = -((-2^{12}7^2 23)^2 5657)^2 2638039$**, % = 20.81**
$\mathrm{Res}_y(\mathrm{Res}_x(x^8+2x^7+5x^6+4x^5-3x^4-12x^3-13x^2-6x-1, y^2+xy-1), z^2+z+y-1)$
**d = 32, r₁= 8,** $\mathrm{disc} = (-137\cdot 16188577\cdot 640333051)^2 29\cdot 3413$**, % = 19.98**
$\mathrm{Res}(x^{16}+4x^{15}-12x^{14}-73x^{13}-11x^{12}+407x^{11}+513x^{10}-653x^9-1547x^8-33x^7+1642x^6+776x^5-534x^4-420x^3-52x^2-8x+1, y^2+xy+1)$
**d = 32, r₁= 10,** $\mathrm{disc} = -(-648223930401682619)^2 3427871$**, % = 20.33**
$\mathrm{Res}(x^{16}-12x^{15}+55x^{14}-105x^{13}+307x^{11}-330x^{10}-236x^9+530x^8-2x^7-351x^6+74x^5+106x^4-31x^3-12x^2+4x+1, y^2+y-x)$
**d = 32, r₁= 12,** $\mathrm{disc} = (-3^4 269\cdot 6187309\cdot 6321079)^2 1181\cdot 129221$**, % = 29.89**
$\mathrm{Res}(x^{16}+13x^{15}+68x^{14}+193x^{13}+337x^{12}+318x^{11}-221x^{10}-1376x^9-2135x^8-1367x^7+256x^6+1143x^5+944x^4+420x^3+110x^2+16x+1, y^2+xy-1)$
**d = 32, r₁= 18,** $\mathrm{disc} = -((-2593\cdot 52579)^2 17417)^2 17\cdot 67\cdot 181$**, % = 27.92**
$\mathrm{Res}_y(\mathrm{Res}_x(x^8-4x^7-6x^6-24x^5-49x^4-33x^3-3x^2+4x+1, y^2+yx-1), z^2+z+y-1)$

**d = 33, r₁= 3,** $\mathrm{disc} = (-6839578507)^3 812387\cdot 852847$**, % = 25.75**
$\mathrm{Res}(x^{11}-4x^{10}+5x^9-2x^8-2x^7+7x^6-6x^5+3x^4+x^3-3x^2+2x-1, (y^3-y^2+1)x+(-y^2+y-1))$

**d = 34, r₁= 0,** $\mathrm{disc} = -(509\cdot 4381747\cdot 577796627)^2 6719$**, % = 13.55**
$\mathrm{Res}(x^{17}-3x^{16}-10x^{15}+34x^{14}+39x^{13}-158x^{12}-72x^{11}+387x^{10}+52x^9-534x^8+25x^7+410x^6-69x^5-160x^4+42x^3+24x^2-8x+1, y^2+xy+1)$
**d = 34, r₁= 2,** $\mathrm{disc} = (-4531883700323658883)^2 2593$**, % = 12.61**
$\mathrm{Res}(x^{17}-3x^{16}-11x^{15}+38x^{14}+44x^{13}-194x^{12}-65x^{11}+505x^{10}-32x^9-693x^8+196x^7+459x^6-175x^5-112x^4+30x^3+12x^2-1, y^2+xy+1)$
**d = 34, r₁= 4,** $\mathrm{disc} = -(-1315674972302176747)^2 449\cdot 5987$**, % = 21.59**
$\mathrm{Res}(x^{17}+9x^{16}+28x^{15}+26x^{14}-33x^{13}-74x^{12}-31x^{11}+72x^{10}+531x^9+1565x^8+2407x^7+2268x^6+1473x^5+722x^4+275x^3+76x^2+13x+1, y^2+xy+1)$
**d = 34, r₁= 6,** $\mathrm{disc} = (-5\cdot 195047\cdot 30322223\cdot 176043187)^2$**, % = 21.18**
$\mathrm{Res}(x^{17}+2x^{16}-15x^{15}-30x^{14}+89x^{13}+176x^{12}-271x^{11}-516x^{10}+465x^9+803x^8-467x^7-646x^6+271x^5+240x^4-78x^3-32x^2+8x+1, y^2+xy+1)$
**d = 34, r₁= 10,** $\mathrm{disc} = (8039\cdot 5814690880682891)^2 241\cdot 13249$**, % = 27.63**
$\mathrm{Res}(x^{17}+13x^{16}+65x^{15}+138x^{14}+14x^{13}-458x^{12}-612x^{11}+308x^{10}+1111x^9+265x^8-798x^7-410x^6+240x^5+162x^4-21x^3-18x^2+1, y^2+xy+1)$
**d = 34, r₁= 14,** $\mathrm{disc} = (-5573\cdot 10117905880843931)^2 33525209$**, % = 23.52**
$\mathrm{Res}(x^{17}-18x^{16}+145x^{15}-674x^{14}+1932x^{13}-3312x^{12}+2665x^{11}+1004x^{10}-4060x^9+2415x^8+1219x^7-1798x^6+254x^5+317x^4-70x^3-26x^2+4x+1, y^2+y-x)$

**d = 36, r₁= 0,** $\mathrm{disc} = (269\cdot 188891\cdot 269507383919)^2 37\cdot 8821$**, % = 21.07**
$\mathrm{Res}(x^{18}-3x^{17}-10x^{16}+35x^{15}+37x^{14}-166x^{13}-57x^{12}+413x^{11}+10x^{10}-579x^9+80x^8+$

$453x^7 - 103x^6 - 180x^5 + 51x^4 + 27x^3 - 9x^2 + 1, y^2 + xy + 1)$
**d = 36, r$_1$= 2,** disc = $-((43 \cdot 1693 \cdot 27067)^2)^2 101 \cdot 40231$, **% = 14.96**
$\mathrm{Res}_y(\mathrm{Res}_x(x^9 + x^8 - 10x^7 - 17x^6 + 8x^5 + 51x^4 + 60x^3 + 33x^2 + 9x + 1, y^2 + y(x-1) + 1), z^2 + (y-1)z + 1)$
**d = 36, r$_1$= 4,** disc = $((37354501)^2 10321)^2 547 \cdot 47659$, **% = 23.57**
$\mathrm{Res}_y(\mathrm{Res}_x(x^9 - 6x^8 + 17x^7 - 37x^6 + 64x^5 - 72x^4 + 51x^3 - 26x^2 + 8x - 1, y^2 - yx + 1), z^2 + z - y + 1)$
**d = 36, r$_1$= 6,** disc = $-(-53 \cdot 11821 \cdot 107207932980079)^2 2056603$, **% = 19.01**
$\mathrm{Res}(x^{18} - 10x^{17} + 35x^{16} - 31x^{15} - 102x^{14} + 249x^{13} - 20x^{12} - 431x^{11} + 287x^{10} + 301x^9 - 294x^8 - 111x^7 + 110x^6 + 41x^5 - 11x^4 - 14x^3 - x^2 + x + 1, y^2 + xy + 1)$
**d = 36, r$_1$= 8,** disc = $(2^{18} 227 \cdot 121441 \cdot 100986877)^2 43 \cdot 47 \cdot 1109$, **% = 29.18**
$\mathrm{Res}(x^{18} + 18x^{17} + 121x^{16} + 336x^{15} - 100x^{14} - 3320x^{13} - 9128x^{12} - 7872x^{11} + 13600x^{10} + 47992x^9 + 64883x^8 + 49350x^7 + 21887x^6 + 5590x^5 + 1103x^4 + 372x^3 + 117x^2 + 18x + 1, y^2 + xy + 1)$

**d = 38, r$_1$= 0,** disc = $-(16068047209 \cdot 91386076897)^2 47 \cdot 337$, **% = 20.66**
$\mathrm{Res}(x^{19} - 3x^{18} - 12x^{17} + 39x^{16} + 62x^{15} - 215x^{14} - 186x^{13} + 653x^{12} + 374x^{11} - 1184x^{10} - 545x^9 + 1289x^8 + 568x^7 - 791x^6 - 374x^5 + 224x^4 + 120x^3 - 12x^2 - 8x + 1, y^2 + xy + 1)$
**d = 38, r$_1$= 2,** disc = $(31 \cdot 71 \cdot 73 \cdot 281 \cdot 525923 \cdot 286864519)^2 31 \cdot 271$, **% = 22.41**
$\mathrm{Res}(x^{19} - 3x^{18} - 12x^{17} + 41x^{16} + 56x^{15} - 234x^{14} - 120x^{13} + 722x^{12} + 78x^{11} - 1302x^{10} + 150x^9 + 1384x^8 - 341x^7 - 831x^6 + 270x^5 + 253x^4 - 94x^3 - 30x^2 + 12x - 1, y^2 + xy + 1)$
**d = 38, r$_1$= 4,** disc = $-(-59^2 20790017 \cdot 73335576527)^2 11 \cdot 37 \cdot 1877$, **% = 29.41**
$\mathrm{Res}(x^{19} - 2x^{18} - 14x^{17} + 27x^{16} + 80x^{15} - 147x^{14} - 242x^{13} + 417x^{12} + 422x^{11} - 669x^{10} - 434x^9 + 623x^8 + 262x^7 - 336x^6 - 88x^5 + 102x^4 + 15x^3 - 16x^2 - x + 1, y^2 + xy + 1)$
**d = 38, r$_1$= 6,** disc = $(229 \cdot 10259 \cdot 44579 \cdot 162671 \cdot 174467)^2 2824201$, **% = 23.55**
$\mathrm{Res}(x^{19} + 10x^{18} + 34x^{17} + 21x^{16} - 139x^{15} - 296x^{14} + 44x^{13} + 694x^{12} + 483x^{11} - 586x^{10} - 836x^9 + 39x^8 + 533x^7 + 204x^6 - 113x^5 - 99x^4 - 13x^3 + 13x^2 + 6x + 1, y^2 + xy + 1)$

**d = 40, r$_1$= 0,** disc = $((-353 \cdot 744659)^2 7321)^2 9071521$, **% = 14.04**
$\mathrm{Res}_y(\mathrm{Res}_x(x^10 - 10x^9 + 43x^8 - 103x^7 + 148x^6 - 127x^5 + 59x^4 - 7x^3 - 8x^2 + 4x + 1, y^2 - y - x), z^2 + yz + 1)$
**d = 40, r$_1$= 2,** disc = $-(-(1023379157)^2 43 \cdot 97)^2 41 \cdot 254119$, **% = 21.54**
$\mathrm{Res}_y(\mathrm{Res}_x(x^10 - 9x^9 + 33x^8 - 62x^7 + 58x^6 - 13x^5 - 21x^4 + 13x^3 + 4x^2 - 4x - 1, y^2 + y - x), z^2 + yz + 1)$
**d = 40, r$_1$= 4,** disc = $((17 \cdot 1657 \cdot 45341)^2 17581)^2 199 \cdot 36319$, **% = 26.13**
$\mathrm{Res}_y(\mathrm{Res}_x(x^10 - 11x^9 + 52x^8 - 137x^7 + 215x^6 - 194x^5 + 80x^4 + 7x^3 - 15x^2 + 2x + 1), z^2 + yz + 1)$
**d = 40, r$_1$= 8,** disc = $(647 \cdot 44129306144864118383)^2 7 \cdot 503 \cdot 93281$, **% = 25.96**
$\mathrm{Res}(x^{20} + 19x^{19} + 156x^{18} + 714x^{17} + 1930x^{16} + 2838x^{15} + 983x^{14} - 3809x^{13} - 5994x^{12} - 1298x^{11} + 4335x^{10} + 3387x^9 - 725x^8 - 1579x^7 - 235x^6 + 263x^5 + 78x^4 - 10x^3 - 4x^2 + 1, y^2 + xy + 1)$

**d = 42, r$_1$= 2,** disc = $(-197 \cdot 373 \cdot 1223 \cdot 3643 \cdot 3213804663031)^2 31 \cdot 1951$, **% = 19.51**
$\mathrm{Res}(x^{21} + 4x^{20} - 10x^{19} - 55x^{18} + 30x^{17} + 322x^{16} + 27x^{15} - 1045x^{14} - 396x^{13} + 2049x^{12} + 1105x^{11} - 2478x^{10} - 1570x^9 + 1805x^8 + 1254x^7 - 734x^6 - 547x^5 + 140x^4 + 114x^3 - 8x^2 - 8x + 1, y^2 + xy + 1)$

**d = 44, r$_1$= 0,** disc = $(-(-113 \cdot 3677 \cdot 17419)^2 61 \cdot 199)^2 5981 \cdot 11261$, **% = 23.45**

$\mathrm{Res}_y(\mathrm{Res}_x(x^{11}-9x^{10}+35x^9-77x^8+103x^7-77x^6+10x^5+38x^4-29x^3-x^2+6x+1, y^2+y-x), z^2+yz+1)$
**d = 44, $\mathbf{r_1}$= 2,** disc $= -((-6257\cdot 1327759)^2 113\cdot 257)^2 1997\cdot 221831$**, % = 29.91**
$\mathrm{Res}_y(\mathrm{Res}_x(x^{11}-9x^{10}+38x^9-109x^8+232x^7-371x^6+425x^5-339x^4+182x^3-62x^2+12x-1, y^2-xy-1), z^2+(y-1)z+1)$

**d = 48, $\mathbf{r_1}$= 0,** disc $= ((971\cdot 105075211)^2 3697)^2 2687\cdot 9740543$**, % = 25.99**
$\mathrm{Res}_y(\mathrm{Res}_x(x^{12}-2x^{11}+4x^9-3x^8-3x^7+7x^6-4x^5-x^4+2x^3+x^2-2x+1, (y^2-2y)x-y^2+y+1), z^2+yz+1)$

# Bibliographie


[Bar] H.J. Bartels :*Über Normen algebraischer Zahlen*, Math. Ann., 251 (1980), pp. 191–212 ;

[Bir-SwD] B.J. Birch and H.P.F. Swinnerton-Dyer : *Notes on Elliptic Curves.* J. Reine Angew. Math. 212 (1963), pp. 7–25 ;

[Che] C. Chevalley :*Sur la Théorie du Corps de Classes dans les Corps Finis et les Corps Locaux*, J. Fac. Sci Tokyo, 2 (1933), pp. 365–475 ;

[Coc-Mit] T. Cochrane and P. Mitchell : *Small Solutions of the Legendre Equation*, J. Number Theory, 70 (1998), pp. 62–66 ;

[Coh] H. Cohen :*A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., Vol. 138, Springer-Verlag (1993) ;

[Coh-Dia-Oli a] H. Cohen, F. Diaz Y Diaz and M. Olivier :*A Table of Totally Complex Number Fields of Small Discriminants*, ANTS III, Springer LN in Computer Science, 1423 (J. Buhler Ed. 1998), pp. 381–391 ;

[Coh-Dia-Oli b] H. Cohen, F. Diaz Y Diaz, M. Olivier :*Computation of Relative Quadratic Class Groups*, ANTS III, Springer LN in Computer Science, 1423 (J. Buhler Ed. 1998), pp. 433–440.

[Coh-Dia-Oli c] H. Cohen, F. Diaz Y Diaz and M. Olivier :*Computing Ray Class Groups, Conductors and Discriminants*, Math. Comp., 222 vol. 67 (1998), pp. 773–795 ;

[Coh-Dia-Oli d] H. Cohen, F. Diaz Y Diaz et M. Olivier :travail en cours sur les extensions abéliennes (1998) ;

[Con-Slo] J. Conway and N. Sloane :*Sphere Packings, Lattices and Groups*, Grundlehren der Math. Wiss. 290, Springer Verlag (1988) ;

[Cre a] J.E. Cremona :*Algorithms For Modular Elliptic Curves*, Cambridge University Press (1997), Second edition ;

[Cre b] J.E. Cremona : *Higher Descents on Elliptic Curves*, actes des "Huitièmes Rencontres Arithmétiques de Caen" J. Boxall ed., (1997), preprint ;

[Cre c] J.E. Cremona :*Classical Invariants and 2-Descent on Elliptic Curves*, J. Symb. Comp., à paraître (1998) ;

[Cre d] J.E. Cremona : *Efficient Solution of Rational Conics*, preprint (1998) ;

[Cre-Ser] J.E. Cremona and P. Serf : *Computing the rank of Elliptic Curves over Real Quadratic Fields of Class Number 1*, Math. Comp., à paraître (1998) ;

[Diaz a] F. Diaz Y Diaz :*Valeurs Minima du Discriminant des Corps de Degré 7 Ayant une Seule Place Réelle*, C.R.A.S. Paris, t.296 (1983), pp. 137–139 ;

[Diaz b] F. Diaz Y Diaz :*Valeurs Minima du Discriminant pour Certains Types de Corps de Degré 7*, Ann, Inst. Fourier. Grenoble, 33, 3 (1984), pp. 29–38 ;

[Erd] P. Erdös : *Some Remarks on Euler's $\phi$ Function and Some Other Related Problems*, Bull. Amer. Math. Soc. 51 (1945), pp. 540–544 ;

[Erd-Vau] P. Erdös and R.C. Vaughan :*Bounds for the r-th Coefficients of Cyclotomic Polynomials*, J. London Math. Soc. (2) 8 (1974), pp. 393–400 ;

[Fes-Vos] I.B. Fesenko and S.V. Vostokov : *Local Fields and Their Extensions : A Constructive Approach*, Trans. Math. Monographs, vol. 121, Amer. Math. Soc. (1993) ;

[Fie] C. Fieker : *Ueber Relative Normgleichungen in Algebraischen Zahlkörpern*, Dissertation, Technische Univertität Berlin (1997) ;

[Fie-Jur-Poh] C. Fieker, A. Jurk and M. Pohst :*On solving relative norm equations in algebraic number fields*, Math. Comp., 217 vol. 66 (1997), pp. 399–410 ;

[Fin-Poh] U. Fincke and M. Pohst :*A Procedure for Determining Algebraic Integers of Given Norm*, Proceedings EUROCAL 83, Springer LN in Computer Science, 162 (1983), pp. 194–202 ;

[Gar] D. Garbanati :*An Algorithm for Finding an Algebraic Number Whose Norm is a Given Rational Number*, J. Reine Angew. Math., 316 (1980), pp. 1–13 ;

[Hol] L. Holzer : *Minimal Solutions of Diophantine Equations*, Canad. J. Math, 2 (1950), pp. 238–244 ;

[Hun] J. Hunter :*The Minimum discriminants of Quintic Fields*, Proc. Glasgow Math. Ass, 3 (1957), pp. 57–67 ;

[Lang] S. Lang :*Algebraic Number Theory*, Graduate Texts in Math., Vol. 110, Springer-Verlag (1994), Second edition ;

[Len] H. Lenstra :*Euclidean Number Fields of Large Degree*, Inv. Math., 38 (1977), pp. 237–254 ;

[Leu a] A. Leutbecher :*Euclidean Fields Having a Large Lenstra Constant*, Ann. Inst. Fourier Grenoble, vol. 35 (1985), pp. 83–106 ;

[Leu b] A. Leutbecher :Résultats non publiés, cités dans [Odl] ;

[Leu-Mar] A. Leutbecher and J. Martinet :*Lenstra's Constant and Euclidean Number Fields*, Proceedings, Journées Arithmétiques 1981, Astérisque 94 (1982), pp. 87–131 ;

[Leu-Nik] A. Leutbecher and G. Niklasch :*On Cliques of Exceptional Units and Lenstra's Construction of Euclidean Fields*, Springer LNM 1380, *Number Theory Ulm 1987*, H.P. Schlickewei and E. Wirsing ed. (1989), pp. 150–178 ;

[Mar a] J. Martinet :*Tours de Corps de Classes et Estimations de Discriminants*, Inventiones math. 44 (1978), pp. 65–73 ;

[Mar b] J. Martinet :*Petits Discriminants des Corps de Nombres*, Journées Arithmétiques 1980, London Math. Soc. Lecture Note Ser. 56, Cambridge Univ. Press (1982), pp. 151–193 ;

[Mor] L.J. Mordell : *Diophantine Equations*, Pure and Applied Mathematics 30, Academic Press (1969) ;

[Nik] G. Niklasch : Number Field Data Base, http://hasse.mathematik.tu-muenchen.de/nfdb/hier/survey.html ;

[Odl] A. Odlyzko :*Bounds for Discriminants and Related Estimates for Class Numbers, Regulators and Zeros of Zeta Functions: a Survey of Recent Results*, Sém. Th. des Nombres Bordeaux (Série 2) 2 (1990), pp. 119–141 ;

[Poh] M. Pohst : *On the Computation of Number Fields of Small Discriminants Including the Minimum Discriminants of Sixth Degree Fields*, J. Number Theory, 14 (1982), pp. 99–117 ;

[Poh-Mar-Dia] M. Pohst, J. Martinet and F. Diaz Y Diaz : *The Minimum Discriminant of Totally Real Octic Fields*, J. Number Theory, 36 (1990), pp. 145–159 ;

[Pol-Sch] J. Pollard and C. Schnorr :*An Efficient Solution of the Congruence* $x^2 + ky^2 = m$ mod $n$, IEEE Transactions on Information Theory, Vol. it-33, 5 (Sept. 1987), pp. 702–709 ;

[Serf] P. Serf :*The Rank of Elliptic Curves Over Real Quadratic Number Fields of Class Number 1*, Doctoral Thesis, Universität des Saarlandes (1995) ;

[Ser] J.P. Serre :*Corps Locaux*, ch. XIV, Hermann, 3$^{e}$éd. (1968) ;

[Sie] C.L. Siegel :*Normen algebraischer Zahlen*, Nachr. Akad. Wiss. Göttingen (1973), pp. 197–215 ;

[Sik] S. Siksek : *Descent on Curves of Genus 1*, PhD thesis, University of Exeter, (1995) ;

[Sil] J. Silverman :*The Arithmetic of Elliptic Curves*, Graduate Texts in Math., Vol. 106, Springer-Verlag (1986) ;

[Ten] G. Tenenbaum :*Introduction à la Théorie Analytique et Probabiliste des Nombres*, Cours Spécialisés, Coll. SMF, no 1, (1995) ;

[Was] L.C. Washington :*Introduction to Cyclotomic Fields*, Graduate Texts in Math., Vol. 83, Springer-Verlag (1982) ;

[Zie] A. Ziegler :*Diskriminanten und Differenten*, unpublished diploma thesis, supervised by Prof. Dr. A. Leutbecher and Dr. G. Niklasch, Mathematisches Institut der Technischen Universität München (1995) .

Nombre de références bibliographiques : 48.

**Résumé** :

Cette thèse aborde trois problèmes différents. On propose en premier un algorithme pour déterminer le rang d'une courbe elliptique définie sur un corps de nombres. On rappelle l'algorithme de descente par 2-isogénie pour les courbes ayant de la 2-torsion, et pour les courbes sans 2-torsion, on décrit un nouvel algorithme. Cet algorithme conditionnel repose sur la résolution de l'équation de Legendre, et l'on expose en détail cette résolution. Le second problème est la résolution des équations aux normes dans les extensions relatives quelconques de corps de nombres. L'interprétation de ce problème en termes de $S$-unités permet de donner une description explicite des solutions, et de résoudre entièrement et de manière satisfaisante ces équations. Le troisième problème abordé est la détermination des discriminants minimaux des polynômes irréductibles pour les degrés supérieurs ou égaux à 9. Les méthodes proposées fournissent de longues listes de petits discriminants qui améliorent les bornes précédemment connues, en particulier jusqu'au degré 14. On donne également, en les démontrant, tous les discriminants minimaux des polynômes non irréductibles jusqu'au degré 7.

**Title : Equations in Number Fields and Minimal Discriminants**

**Abstract** :

This thesis deals with three different problems. We first propose an algorithm that computes the rank of an elliptic curve defined over a number field. A standard algorithm is known for curves with non-trivial 2-torsion (descent via 2-isogeny), and we describe a new algorithm for curves with no rational 2-torsion. This conditional algorithm relies on a solution method for Legendre's equation, and we give a detailed description for the solution of this equation. The second problem consists in solving norm equations in relative extensions of number fields. The reformulation of this in terms of $S$-units allows us to give an explicit description of the solutions, and to solve completely these equations in a quite efficient way. The third problem discussed consists in listing the minimal discriminants of irreducible polynomials of degree 9 and above. The proposed methods build large lists of small discriminants, and improve many known bounds, in particular up to degree 14. We also give all minimal discriminants of non-irreducible polynomials up to degree 7, and prove them.

---

Thèse de **MATHÉMATIQUES PURES**

**Mots-Clés** :

Algorithme, Corps de Nombres, Courbe Elliptique, Discriminant, Équation de Legendre, Groupe de Classes, Nombre Algébrique, Norme, Polynôme, Résultant, Unité / $S$-Unité.

---

Laboratoire A2X, Université Bordeaux I,
351, Cours de la Libération 33405 TALENCE Cedex.