N° d'ordre :04 /2014 – M /MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE-ALGER
Faculté de Mathématiques

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En: MATHÉMATIQUES

Spécialité : Arithmétique, Codage et Combinatoire : Théorie des Nombres

Par : DIBES Abdelkader

Thème

Les Coïncidences de Discriminants

Soutenu publiquement, **le 26 /11/2014**, devant le jury composé de :

Mr Farid BENCHERIF	Professeur à l'USTHB	Président
Mme Schehrazad SELMANE	Maître de Conférences /A à L'USTHB	Directrice de Mémoire
Mme Leila BENFERHAT	Maître de Conférences /A à L'USTHB	Examinatrice
Mr Boualem BENSEBA	Maître de Conférences /A à L'USTHB	Examinateur

Remerciement

Nous remercions tout d'abord et avant tout le tout puissant ALLAH qui nous a aidés à mener à terme ce travail.

Je tiens à remercier Mon Professeur et ma Directrice de mémoire, Madame Schehrazad SELMANE, qui a accepté de diriger mon travail et de me suivre patiemment dans toutes les étapes de cette étude. Je lui suis reconnaissant de ses nombreuses remarques, sa gentillesse et sa patience.

Mes sincères remerciements vont à Monsieur Farid BENCHERIF pour m'avoir fait l'honneur de présider le jury et à Monsieur Boualem BENSEBA, Madame Leila BENFERHAT d'avoir accepté d'examiner ce travail.

Je remercie aussi l'ensemble de mes camarades de Magister, mes amis, ma famille qui m'ont soutenue durant ce travail.

Enfin merci à tous ceux qui m'ont aidée de près ou de loin.

Table des matières

Chapitre (1)

Minorations de discriminants

Chapitre (2)

Corps de nombres

Chapitre (3)

Construction explicite des corps de nombres

Chapitre (4)

Coïncidence de discriminant

Résumé

Le discriminant d_K d'un corps de nombres K de degré n dépend de plusieurs éléments de K telle que :

- r Le nombre de place réelles et s le nombre de places complexes.
- Son signe est $(-1)^s$.
- À degré égal, les discriminants ont des tendances à croître avec le nombre de places réelles.
- Pour chaque nombre premier p, la valuation de p dans d_K ne peut prendre un nombre fini de valeurs.
- Il vérifie la congruence de la Stickelberger :

$$d_K \equiv\ 0\ ou\ 1\ mod 4$$

  .
- On dispose de minorations pour $|d_K|$ ne dépendant que de r et s.
- Enfin, il est bien connu que l'ensemble des classes d'isomorphismes des corps de nombres de discriminant donné est fini (Hermite). Il est donc naturel d'essayer de trier les corps de nombres par leurs discriminants.

Dans ce mémoire on étudie les méthodes de construction explicite des corps de nombres de degré n, de signature (r,s), et de discriminant plus petit, en valeur absolue, qu'une constante B à l'aide de la géométrie des nombres et nous appliquons ces méthodes dans la recherche du nombre maximum de coïncidences de discriminants dans le cas des corps de nombres de degré 10.

INTRODUCTION

Le discriminant d_K d'un corps de nombres K de degré n dépend de plusieurs éléments de K telle que :

- r Le nombre de place réelles et s le nombre de places complexes.
- Son signe est $(-1)^s$.
- À degré égal, les discriminants ont des tendances à croître avec le nombre de places réelles.
- Pour chaque nombre premier p, la valuation de p dans d_K ne peut prendre qu'un nombre fini de valeurs.
- Il vérifie la congruence de la Stickelberger :

$$d_K \equiv \ 0 \ ou 1 \mod 4$$

.

- On dispose de minorations pour $|d_K|$ ne dépendant que de r et s.
- Enfin, il est bien connu que l'ensemble des classes d'isomorphisme des corps de nombres de discriminant donné est fini (Hermite). Il est donc naturel d'essayer de trier les corps de nombres par leurs discriminants.

Dans ce mémoire on étudie les méthodes de construction explicite des corps de nombres de degré n, de signature (r,s), et de discriminant plus petit, en valeur absolue, qu'une constante B à l'aide de la géométrie des nombres et nous appliquons ces méthodes dans la recherche du nombre maximum de coïncidences de discriminants dans le cas des corps de nombres de degré 10.

Cette thèse est organisé comme suit :

Dans le premier chapitre on rappelle les théorèmes qui conduisent aux minorations de discriminants. Dans [15], A. M. Odlyzko évoque le problème de savoir l'ordre de grandeur du premier zéro de la fonction zêta de Dedekind. Dans cette direction, une conjecture a été énoncée dans [21] qui dit que la hauteur du premier zéro est majorée par $C/ln(|d_K|)$ ou C est une constante positive qui ne dépend que de n. Nous donnons une amélioration de cette inégalité sous l'hypothèse de Riemann généralisée (GRH) qui permet d'aboutir à une meilleure majoration de $C/lnln(|d_K|)$.

Dans le second chapitre nous rappelons quelques notions fondamentales de la théorie des nombres. Il s'agit de rappels sur les extensions des corps nombre algébriques, polynôme minimale, extension normal et séparable, élément primitif, la trace et la norme d'un entier, discriminant relatif.

Dans le troisième chapitre nous rappelons les résultats important dans la construction explicite des corps de nombres de degré n, de signature (r, s) et de discriminant plus petit qu'une constante donnée. Nous distinguons le cas des extensions primitifs et des extension non primitifs.

Dans le dernier chapitre, nous avons repris les travaux de S. Selmane sur la détermination d'un nombre maximal de corps de nombres de degré 10, ayant un discriminant donné, qui contiennent un sous-corps de degré 5 ayant un nombre de classes et un groupe de Galois donnés. Les listes construites des premières coïncidences de 52 (resp. 50, 40, 48, 22, 6) corps de nombres non isomorphes de même discriminant de degré 10 de signature (6,2) (resp. (4,3), (8, 1), (2,4), (0,5), (10,0)) qui contient un corps quantique sont données.

Chapitre 1

minoration de discriminant

Introduction et notations

Soit K un corps de nombres de degré n, de signature $(r1, r2)$ et de discriminant d_K. Dans [23], A. M. Odlyzko évoque le problème de savoir l'ordre de grandeur du premier zéro de la fonction zêta de Dedekind. Dans cette direction, une conjecture a été énoncée dans [23] qui dit que la hauteur du premier zéro est majorée par $C/ln(|d_K|)$ ou C est une constante positive qui ne dépend que de n. L'idée de cette dernière inégalité provient d'un théorème de densité (sous GRH) [21]. Malgré les progrès numériques sur la question [22] et [23], nous ne sommes toujours pas en mesure de confirmer expérimentalement cette conjecture. Cependant nous disposons d'un résultat théorique dû à A. Neugebauer, qui montre que la hauteur du premier zéro est majorée par $C/lnlnln(|d_K|)$.
Dans ce qui suit nous donnerons une amélioration de cette inégalité qui sous (GRH) aboutit à la majoration $C/lnln(|d_K|)$. L'outil crucial de la preuve, comme nous le verrons, sont les formules explicites de Weil.
Dans la suite, la notation $\ll$ réfère à une constante absolue alors que la notation $\ll_n$ réfère à une constante qui dépend uniquement de n.

Formules Explicites de Weil [21]

Soit F une fonction réelle d'une variable réelle qu'on peut supposer paire et qui vérifie les conditions (A) et (B) suivantes :
(A) F est continue et continument dérivable sur R sauf en un nombre fini de points a_i ou $F(x)$ et sa dérivée $F^{'}(x)$ n'ont que des discontinuités de première espèce pour lesquelles F vérifie la condition de la moyenne $(i.e)$

$$F(a_i) = \frac{1}{2}\Big(F(a_i + 0) + F(a_i - 0)\Big)$$

(B) Il existe $b > 0$ tel que $F(x)$ et $F'(x)$ sont des $O(e^{-(1/2+b)|x|})$ au voisinage de ∞
La transformée de Mellin de F :

$$\Phi(s) = \int_{\infty}^{\infty} F(x)e^{(s-1/2)x}dx$$

est alors holomorphe dans toute bande $-a \leq \sigma \leq 1 + a$ ou $0 < a < b,\ \ a < 1$ et on a le résultat dû à Weil.

Théorème (1) (Weil) [21]

Soit F vérifiant les conditions (A) et (B) ci-dessus avec $F(0) = 1$. Alors la somme étendue sur les zéros $\varrho = \beta + i\gamma$ non triviaux de $\zeta_K(s)$ avec $|\gamma| < T$ a une limite quand T tend vers l'infini et sa somme est donnée par la formule :

$$\sum_{\varrho} \Phi(\varrho) = \Phi(0) + \Phi(1) - 2\sum_{\rho,m} \frac{\ln\Big(N(\rho)\Big)}{N(\rho)^{m/2}} F\Big(m\ln\Big(N(\rho)\Big)\Big)$$

$$+ln\Big(|d_K|\Big) - n\Big[\ln(2\pi) + \gamma + 2ln(2)\Big] - r_1 J(F) + nI(F)$$

Avec

$$J(F) = \int_0^\infty \frac{F(x)}{2ch(x/2)}dx$$

$$I(F) = \int_0^\infty \frac{1 - F(x)}{2sh(x/2)}dx$$

et $\gamma = 0.57721566...$ désigne la constante d'Euler.

Remarque

On a :

$$\Phi(0) + \Phi(1) = 4\int_0^\infty F(x)ch(x/2)dx.$$

Si $\widehat{F}$ désigne la transformée de Fourier de F alors sous l'hypothèse de Riemann généralisée on a $\Phi(\varrho) = \widehat{F}(t)$ ou $\varrho = 1/2 + it$.

Estimation du premier zéro de la fonction zêta de Dedekind [21]

Dans un premier temps on cherche à majorer la multiplicité d'un éventuel zéro de la fonction zêta de Dedekind au point 1/2

Proposition (1) [21]

Soit r la multiplicité d'un éventuel zéro de la fonction $\zeta_K(s)$ au point 1/2. Alors on a la majoration

$$r \ll \frac{\ln(|d_K|)}{\ln\ln(|d_K|)}$$

Si on accepte la validité de la conjecture d'Artin sur la simplicité des zéros des séries L [21], on voit que r est majoré par le nombre de caractères et ne dépend que de n.

Dans la preuve de la proposition 1, on suit une démarche similaire 'a celle de Ram Murty[21] qui donne une majoration de la multiplicité de 1/2 comme zéro d'une série L de Dirichlet.

Preuve (de la proposition 1)

Soit F définie par

$$F(x) = \begin{cases} 1-|x| & si\ |x| \leq 1 \\ 0 & sinon \end{cases}$$

Alors F vérifie les conditions du théorème 1 et on a

$$\widehat{F}(u) = \Big(\frac{2\sin(u/2)}{u}\Big)^2$$

Si on pose $F_T(x) = F(x/T)$ alors $\widehat{F}(u) = T\widehat{F}(Tu)$.

En appliquant maintenant les Formules Explicites à la fonction F_T , on obtient les inégalités

$$rT \leq 4\int_0^T ch(x/2)dx + \ln(|\ d_K\ |) + n\int_0^T \frac{x}{2Tsh(x/2)}dx,$$

$$rT \leq e^{T/2} + \ln(|\ d_K\ |) + n$$

Si on pose $T = 2\ln\ln(|d_K|)$, il s'ensuit que

$$r \leq \frac{\ln(|d_K|)}{\ln\ln(|d_K|)} + \frac{n}{2\ln\ln(|d_K|)}$$

Comme $n \ll \ln(|d_K|)$ (inégalité d'Odlyzko), on a

$$r \ll \frac{\ln(|d_K|)}{\ln\ln(|d_K|)}$$

Théorème (2) [21]

Soit h la hauteur du premier zéro différent de $1/2$ de la fonction zêta de Dedekind d'un corps de nombres K de discriminant d_K. Alors on a l'estimation

$$h \ll_n \frac{1}{\ln\ln(|d_K|)}$$

Corollaire 1

Si on prend une suite de corps de nombres pour lesquels n est fixe et d_K tend vers ∞ alors le premier zéro tend vers $1/2$.

Pour démontrer le théorème 2, on a besoin de trois lemmes :

Lemme 1

Soit F la fonction paire à support compact définie sur $[0,\infty[$ par

$$F(x) = \begin{cases} (1-x)\cos(\pi x) + \frac{3}{\pi}\sin(\pi x) & si\ 0 \le x \le 1 \\ 0 & sinon \end{cases}$$

Alors F vérifie les conditions du théorème 1 et

$$\widehat{F}(u) = \Big(2 - \frac{u^2}{\pi^2}\Big)\Big[\frac{2\pi}{\pi^2 - u^2}\cos(u/2)\Big]^2$$

Preuve

On pourra vérifier que $F(x)$ s'écrit en termes de la fonction d'Odlyzko.G [21] et de sa dérivée seconde. En effet $F(x) = 2G(x) + \frac{1}{\pi^2}G''(x)$

Lemme 2

Si on pose $F_T(x) = F(x/T)$ avec F comme au lemme 1 alors on a l'estimation suivante de la somme sur les idéaux premiers :

$$\Big|\sum_{\rho,m}\frac{\ln(N(\rho))}{N(\rho)^{m/2}}F_T\Big(m\ln\Big(N(\rho)\Big)\Big)\Big| \ll n^2 e^{T/2} \qquad (1)$$

Lemme 3

Soient A, B, C trois constantes réelles positives vérifiant $C > 2B$. Si $T > 0$ vérifie $AT + Be^{T/2} \ge C$, alors

$$T \ge \varepsilon\ln(C), \quad ou \quad \varepsilon = \min\Big(\frac{C}{2A\ln(C)}, \frac{2\ln(C/(2B))}{\ln(C)}\Big)$$

Preuve du théorème 2

On applique cette fois-ci les Formules Explicites à la fonction $F_T(x) = F(x/T)$ ou F est la fonction définie dans le **lemme 1** :

et on pose $T = \sqrt{2\pi}/h$ ou h est la hauteur du premier zéro différent de $1/2$ de la fonction $\zeta_K(s)$. On obtient alors l'inégalité

$$\frac{8}{\pi^2} rT \geq \Phi_T(0) + \Phi_T(1) - 2\sum_{\rho,m} \frac{\ln(N(\rho))}{N(\rho)^{m/2}} F_T\Big(m \ln\Big(N(\rho)\Big)\Big)$$

$$+ \ln(|d_K|) - n\Big[\ln(2\pi) + \gamma + 2\ln(2)\Big] - r_1 J(F_T) + nI(F_T) \qquad (2)$$

il est facile de vérifier que

$$\Big|\Phi_T(0) + \Phi_T(1)\Big| \ll e^{T/2}$$

et que les intégrales $J(F_T)$ et $I(F_T)$ sont bornées quand T est grand. En se servant maintenant du **lemme 2**, l'inégalité (2) donne alors une inégalité comme celle du **lemme 3** avec

$$A = c_1 \frac{\ln(|d_K|)}{\ln\ln(|d_K|)}, \quad C = \ln(|d_K|),$$

ou c_1 est tel que

$$r > c_1 \frac{8}{\pi^2} . \frac{\ln(|d_K|)}{\ln\ln(|d_K|)}$$

Ceci est assuré grâce à la p**proposition 1**.

Finalement avec les constantes ci-dessus, on obtient

$$\varepsilon = \min\Big(\frac{C}{2c_1}, 1 - \frac{\ln(2B)}{\ln\ln(d_K)}\Big)$$

et le résultat du **théorème 2** découle facilement du **lemme 3.**

Chapitre 2

Corps de nombres

Soient$K$ et F deux corps tels que $F \subset K$. On dit alors que K est une extension de F.
Notations : K/F ou $K \longrightarrow F$

Si on considère K comme un $F-$ espace vectoriel, la dimension de K sur F ($dim_F K$) est appelée le degré de l'extension K/F et est notée $[K : F]$.
Toute base de l'espace vectoriel K sur F est appelée une base de l'extension K/F.
Etant donné deux corps K et $K^{'}$ contenant un corps F, on appelle $F-$ isomorphisme de K sur $K^{'}$ tout isomorphisme de corps $\varphi : K \longrightarrow K^{'}$ tel que $\varphi(a) = a$ pour tout $a \in F$, dans ces conditions, on dit que Ket $K^{'}$ sont isomorphes.
soit

$$A(x) = a_0 x^n + a_1 x^{n-1} + ...a_{n-1}x + a_n$$

un polynôme de degré $deg(A) = n$ et de coefficient dominant $l(A) = a_0 \neq 0$. Par convention, on pose $deg(0) = -\infty$ et $l(0) = 0$, où 0 désigne le polynôme nul dont les coefficients sont tous nuls. Pour tout corps F, on note l'anneau des polynômes de la variable x à coefficients dans F par $F[x]$.

Un élément $\alpha \in F$ est appelé un nombre algébrique sur F s'il existe un polynôme $A(x) \in F[x]$, non identiquement nul, tel que $A(\alpha) = 0$. Si tout élément de K est algébrique sur F, on dit que K est algébrique sur F. Supposons que le polynôme A soit choisi pour avoir le plus petit degré, à coefficient dominant égal 1, un tel polynôme est déterminé de manière unique. Il est appelé le polynôme minimal ou irréductible de α sur le corps F, généralement notée $Min(\alpha, F)$. Le nombre α est appelé un entier algébrique si $A(x) \in \mathbb{Z}[x]$ et $l(A) = 1$.
Par le corps de décomposition d'un polynôme $A(x) \in F[X]$, on entend une extension Ω de F telle que$f$ se décompose en facteurs linéaires sur Ω, c'est-à-dire :

$$f(x) = a_0(x - a_1)...(x - a_n)$$

avec $\alpha_i \in \Omega$, $(0 \leq i \leq n))$ telle que $\Omega = F(\alpha_0...\alpha_1)$ soit engendré par toutes les racines de f.
Une extension algébrique K de F est dite Galoisienne si elle est normale et séparable, l'extension (K/F) est normale si tout polynôme irréductible de $F[x]$, qui a une racine dans K se décompose en facteurs linéaires dans K et K/F est séparable si tout élément α de K est séparable,

c'est-à-dire le polynôme irréductible $Min(\alpha, F)$ n'a pas de racines multiples. Le groupe des $F-$ automorphismes de K est appelé le groupe de Galois de K sur F, et est notée $G(K/F)$, ou simplement G. Une extension finie est dite abélienne (resp. cyclique) si elle est galoisienne et son groupe de Galois G est abélien (resp. cyclique).

Soit F un corps et $f(x)$ un polynôme de degré$\geq$ 1 dans $F[x]$. Soit sa factorisation dans un corps décomposition $\overline{F}$ sur F. Le groupe de Galois de K sur $\overline{F}$ est nommé le groupe de Galois de f sur F.

Les corps des nombres

Soit K un corps de nombres, à savoir, une extension finie des nombres rationnels $\mathbb{Q}$. Le corps des nombres de degré 2 (resp. 4, 5, 8) est appelé corps quadratique (resp. quartique, quintique, octique). Par $n - ieme$ corps cyclotomique on désigne le corps des nombres $\mathbb{Q}(\zeta)$, ou ζ désigne une racine primitive $n - ieme$ de l'unité, c'est-à-dire, $\zeta = e^{2k\pi i/n}$.

Soit K_1, K_2 deux corps des nombres, nous définissons le corps de composition K_1K_2 comme le plus petit sous-corps de $\mathbb{C}$ contenant K_1 et K_2.

soit K un corps de nombres de degré $[K : \mathbb{Q}] = n$, alors

1) Il existe un élément $\theta \in K$, appelé élément primitif de K, tel que $K = \mathbb{Q}(\theta)$.

2) Il existe exactement n plongements de K dans $\mathbb{C}$, donnés par $\sigma_i : \theta \longrightarrow \theta^{(i)}$, ou les $\theta^{(i)}$ sont les racines du polynôme minimal de θ. Ces plongements sont $\mathbb{Q}-$ invariant, leur K_i images dans $\mathbb{C}$ sont appelés les corps conjugués de K et K_i sont isomorphes à K.

3) La signature d'un corps de nombre est le couple (r, s), ou r est le nombre de plongements réels de K et s est le nombre de plongements complexes non réels de K, telle que $r + 2s = n$. Si f désigne le polynôme minimal de θ , alors r (resp. $2s$) est le nombre de racines réelles (resp. non réelles) de f dans $\mathbb{C}$.

Remarque

Pour déterminer la signature d'un corps de nombre K on peut soit calculer les racines du polynôme soit utiliser le théorème de ***Sturm***.

Pour $\alpha \in K$, on note $\alpha^{(1)} = \sigma_1(\alpha)$, ..., $\alpha^{(r)} = \sigma_r(\alpha)$ ses conjugués réels, par
$\alpha^{(r+1)} = \sigma_{r+1}(\alpha)$,..., $\alpha^{r+s} = \sigma_{r+s}(\alpha)$, $\alpha^{(r+s+1)} = \overline{\alpha^{(r+1)}} = \sigma_{r+s+1}(\alpha)$, ... ,$\alpha^{(n)} = \overline{\alpha^{(r+s)}} = \sigma_{r+s+1}(\alpha)$ ses conjugués complexes, σ_i sont les n plongements distincts de K dans $\mathbb{C}$.

Soit α entier algébrique de K , la trace de α dans K est :

$$Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

et la norme de α dans K est :

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Le polynôme caractéristique $\alpha \in K$ est le polynôme :

$$f_\alpha(x) = \prod_{i=1}^{n} \Big(x - \sigma_i(\alpha)\Big) = x^n + \sum_{i=1}^{n} a_i x^{n-i} = x^n + \sum_{i=1}^{n} (-1)^i \delta_i(\alpha) x^{n-i}$$

$\delta_i(\alpha)$ est la $i-$ ième fonction symétrique de α dans K définie comme suit :

$$\delta_1(\alpha) = \sum_{i \leq n} \sigma_i(\alpha) = -\alpha_1$$

$$\delta_2(\alpha) = \sum_{1 \leq i \leq j \leq n} \sigma_i(\alpha)\sigma_j(\alpha) = \alpha_2$$

$$\delta_3(\alpha) = \sum_{1 \leq i \leq j \leq k \leq n} \sigma_i(\alpha)\sigma_j(\alpha)\sigma_k(\alpha) = -\alpha_3$$

.....

$$\delta_n(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)...\sigma_n(\alpha) = (-1)^n a_n$$

Le polynôme caractéristique de $f_\alpha(x)$ est à coefficients entiers et est soit irréductible ou une puissance du polynôme minimal $Min(\alpha, \mathbb{Q})$.

Si on pose

$$S_k(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)^k$$

alors pour $0 < k \leq n$

$$S_k(\alpha) = (-1)^{k+1} k\delta_k(\alpha) - \sum_{i=1}^{k-1} (-1)^i \delta_i(\alpha) S_{k-i}(\alpha) = -ka_k - \sum_{i=1}^{k-1} a_i S_{k-i}(\alpha)$$

et pour $k > n$

$$S_k(\alpha) = -\sum_{i=1}^{n} (-1)^i \delta_i(\alpha) S_{k-i}(\alpha) = -\sum_{i=1}^{n} a_i S_{k-i}(\alpha)$$

base intégral de K est une $Z-$base de l'anneau des entiers ϑ_K de K. Le discriminant d'une base intégrale $w_1, ..., w_n$ est définie par $det\Big(Tr_{K/\mathbb{Q}}(w_i w_j)\Big)$, il est indépendant du choix de cette base, et est appelé le discriminant de corps K ou tout simplement le discriminant de K, et on le note par d_K.

Le discriminant du corps de composition K_1K_2 de deux corps du nombres K_1 et K_2 tel que $K_1 \cap K_2 = \mathbb{Q}$, est égale à

$$d_{K_1K_2} = d_{K_1}^{[K_2:\mathbb{Q}]} \cdot d_{K_2}^{[K_1:\mathbb{Q}]}$$

Soit f un polynôme irréductible unitaire de $\mathbb{Z}[x]$.

Le discriminant de f est définie par :

$$d_f = \prod_{1 \leq i < j \leq n} \Big(\theta_i - \theta_j\Big)^2 = det(s_j^i)$$

ou $\theta_1, ..., \theta_n$ sont les racines de f et

$$s_j^i = \sum_{k=1}^{n} \theta_k^{i+j-2}$$

(avec $1 \leq i, j \leq n$)

posons $\theta = \theta_1$ et considérons $K = \mathbb{Q}(\theta)$.

le discriminant d_K du corps K et le discriminant d_f de f sont liés par le relation suivante :

$$d_f = i_K^2 \cdot d_K$$

où $i_K = \left[\vartheta_K : \mathbb{Z}[\theta]\right]$ est l'indice de θ à K.

Extensions relatives

Soit K un corps des nombres de degré $[K : \mathbb{Q}] = n$, extension de degré $[F : K] = m$ d'un sous-corps de F degré $[\mathbb{Q} : F] = n^{'}$

$$\begin{array}{ll} K & \\ | & m \\ F & \\ | & n' \\ \mathbb{Q} & \end{array}$$

Soit $J(F)$ (resp. $J(K)$) l'ensemble des $Q-$ isomorphismes distincts de F (resp. K) dans $\mathbb{C}$. Pour $\sigma \in J(F)$, on pose

$$J_\sigma(K) = \left\{\tau \in J(K) : \tau_{/F} = \sigma\right\}$$

De toute évidence,

$$J(K) = \bigcup_{\sigma \in J(F)} J_\sigma(K)$$

Pour $\sigma \in J(F)$, on définit le $\sigma-$ trace d'un élément $\theta \in K$ par

$$Tr_{\sigma,K/F}(\theta) = \sum_{\tau \in J_\sigma(K)} \tau(\theta)$$

Nous avons $Tr_{\sigma,K/F}(\theta) \in F$ et

$$\sum_{\sigma \in J(F)} Tr_{\sigma,K/F}(\theta) = Tr_{K/\mathbb{Q}}(\theta)$$

Si nous supposons que $K = F(\theta)$, alors θ est une racine d'un polynôme irréductible $P(x)$ de degré $m = n/n^{'}$

$$P(x) = x^m + a_1 x^{m-1} + ... + a_m \in \vartheta_F[x]$$

Pour $\sigma \in J(F)$, P_σ désigne le polynôme conjugué de P

$$P_\sigma(x) = x^m + \sigma(a_1)x^{m-1} + ... + \sigma(a_m)$$

et f désigne le produit de tous les conjugués

$$f(x) = \prod_{\sigma \in J(F)} P_\sigma(x) = \sum_{i=1}^{n} t_i x^{n-i}$$

ce polynôme est à coefficients entiers et est soit irréductible ou une puissance d'un polynôme irréductible. soient $\theta_1, .., \theta_n$ les racines de f ordonnées de sorte que $\theta_1, .., \theta_m$ soient les racines de P. Pour chaque entier naturel j on considère les sommes de puissances

$$s_j = s_j(\theta) = \sum_{i=1}^{m} \theta_i^j$$

$$S_j = S_j(\theta) = \sum_{i=1}^{n} \theta_i^j$$

et

$$T_j(\theta) = \sum_{i}^{n} \left|\theta^{(i)}\right|^j$$

De toute évidence, pour $2 \leq j \leq m$

$$S_j = \sum_{i=1}^{n^{'}} s_j^{(i)}$$

et

$$\left|S_j\right| \leq \sum_{i=1}^{n^{'}} \left|s_j^{(i)}\right| \leq T_j(\theta)$$

Discriminant relatif.

Soit $\delta_{K/F}$ le discriminant relatif de K sur F, les discriminants de K et F sont liés par la relation

$$d_K = (-1)^c \cdot \Big|d_F\Big|^m \cdot N_{F/\mathbb{Q}} \cdot \Big(\delta_{K/F}\Big),$$

ou c désigne le nombre de places complexes de K dont la restriction à une place de F est réelle. Un résultat de **J. Martinet** [18] affirme que

$$N_{F/\mathbb{Q}}(\delta_{K/F}) \equiv 0 \;\; ou \;\; (-1)^c \; mod 4$$

Nous rappelons qu'un discriminant généralisé est le produit de l'idéal entier $\delta_{K/F}$ de F par un ensemble infini de places ramifiées dans K/F : $d_{K/F} = \delta_{K/F} \;\; \infty_1 ... \infty_c$

Certaines inégalités utilisées :

1) Le théorème bien connu de la moyenne arithmétique et géométrique

$$x_1 ... x_n \leq \Big(\frac{x_1 + ... + x_n}{n}\Big)^n$$

pour tous nombres réels positifs $x_1, ..., x_n$

2)L'inégalité de **Cauchy Schwartz :**

$$\prod_{1\leq i\leq n} x_i y_i \leq \Big(\sum_{1\leq i\leq n} x_i^2\Big)^{1/2} \Big(\sum_{1\leq i\leq n} y_i^2\Big)^{1/2}$$

pour tous nombres réels positifs $x_1, ..., x_n, y_1, ..., y_n$

3) Soit $x_1, ..., x_n$ n nombres complexes($n \geq 1$). alors

$$\Big|(n-1)\Big(\sum_{1\leq i\leq n} x_i^2\Big)^2 - 2n \sum_{1\leq i\leq j\leq n} x_i x_j\Big| + \Big|\sum_{1\leq i\leq n} x_i\Big|^2 \leq n \sum_{1\leq i\leq n} \Big|x_i\Big|^2$$

si tous les x_i sont réels, alors l'inégalité précédente devient une égalité et dans ce cas nous avons

$$(n-1)\Big(\sum_{1\leq i\leq n} x_i^2\Big)^2 - 2n \sum_{1\leq i\leq j\leq n} x_i y_j \geq 0$$

4) Si z et z' sont deux nombres complexes, alors nous avons

$$| \, z + z^{'} \, |^2 + | \, z - z^{'} \, |^2 = 2(| \, z \, |^2 + | \, z \, |^2)$$

Chapitre 3

Construction explicite des corps de nombres

Le but de ce chapitre est la description des méthodes de construction explicites des corps de nombres qui nous permettent d'énumérer tous les corps de nombre,du degré n et la signature (r, s), dont les discriminants sont délimitées par des limites données. Les outils de base utilisées pour compter le nombre de ces domaines sont un théorème en raison de Hunter-Pohst [20] pour la détermination des extensions primitives et sa généralisation proposée par J.Martinet qui permettent possible l'étude de la extensions non-primitifs. Nous allons décrire les techniques et les simplifications ayant été utilisées pour les calculs.

La Méthode

Soit B une constante réelle, nous allons montrer comment énumérer tous les corps de nombres de degré n, de signature (r, s) et de discriminant inférieur en valeur absolue à B.

Le choix de B dépend de plusieurs éléments tels que :

1) Le degré n

2) La signature (r, s)

3) La connaissance de petit discriminants (déterminés pour d'autres causes, par exemple parce qu'ils sont corps euclidiens)

4) Le temps de calcul nécessaire

Remarque.

Si nous nous contentons de chercher les petits discriminants proches du minimum, on peut utiliser les bornes inférieures **d'Odlyzko [15]** avec des corrections locales afin de raccourcir la recherche.

Pour définir un corps de nombres il suffit de donner un polynôme irréductible dont une racine est un élément primitif du corps. Nous allons montrer comment construire de tels polynômes faisant appel aux méthodes la géométrie des nombres qui nous a permis de trouver des bornes pour les coefficients des polynômes recherchés. On distingue le cas des extensions primitives, des extensions non primitives, à savoir, les extensions qui contiennent des sous-corps non triviaux.

Extensions primitives

Nous allons décrire les méthodes de calculs qui conduisent à la construction explicite des corps de nombres de degré n, de signature (r, s) et de discriminant majoré , en valeur absolue, par une constante donnée.

Théorème 1(HUNTER-POHST) [11]

Soit K un corps de nombres de degré n, de signature (r, s) et de discriminant d_K. Il existe un entier $\theta \in K$, $\theta \in \mathbb{Z}$ tel que :

$$0 \leq Tr_{K/\mathbb{Q}}(\theta) \leq \left[\frac{n}{2}\right] \tag{3.1}$$

$$\sum_{i=1}^{n} \left|\theta^{(i)}\right|^2 \leq \frac{1}{n}\Big(Tr_{K/\mathbb{Q}}(\theta)\Big)^2 + \gamma_{n-1}\Big(\frac{\mid d_K \mid}{n}\Big)^{\frac{1}{1-n}} \tag{3.2}$$

où $[x]$ désigne la partie entier de x et γ_{n-1} la constante d'**Hermite** pour la dimension $(n-1)$.

Dans le tableau suivant, on donne les valeur de γ_n pour $2 \leq n \leq 8$.

j	2	3	4	5	6	7	8
γ_j^j	$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	256
les résultats sont dû à	Lagrange	Gauss	Korkorine & Zolotareff		Blichfeldt		

Pour $j \geq 9$ plusieurs bornes supérieures ont été données. Nous indiquons ici une borne supérieure donnée par **Blichfeldt**

$$\gamma_j^j \leq \Big(\frac{2}{\pi}\Big)^j \Gamma\Big(1 + (j+1)/2\Big)^2,$$

qui peut être calculée à partir du logiciel **KANT** : ou la fonction gamma est définie par

$$\Gamma(z) = \int_o^\infty e^{-y} y^{z-1} dy \quad pour \quad z_1 \geq 0 \quad z = z_1 + iz_2$$

Soit

$$f(x) = \prod_i^n \left(x - \theta^{(i)}\right) = x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

le polynôme caractéristique de l'entier dont l'existence est affirmée dans le théorème (1).

On fixe a_1 avec :

$$a_1 \in \left\{ -\left[\frac{n}{2}\right], ..., 0 \right\}$$

à partir de l'inégalité (2) et en utilisant l'inégalité entre moyennes arithmétique et géométrique on déduit :

$$1 \leq \mid a_n \mid = \left| \prod_i^n \left(x - \theta^{(i)}\right) \right| \leq \left[\frac{T_2(\theta)}{n}\right]^{n/2}.$$

Pour pouvoir caractériser les autres coefficients de $P(x)$ d'autres inégalités sont nécessaires.

Considérons, pour cela, les fonctions symétriques S_m tel que :

$$S_m = S_m(\theta) = \sum_{i=1}^n \sigma_i(\theta)^m,$$

pour $m \in \mathbb{Z}$ ainsi que les fonctions T_m tel que :

$$T_m(\theta) = \sum_{i=1}^n \left|\sigma_i(\theta)\right|^m.$$

On a les inégalités suivantes :

$$|S_m| \leq T_m(\theta) \qquad pour \qquad m \in \mathbb{Z} - \{0\}.$$

A partir de ces inégalités et des relations de **NEWTON** :

$$S_m = -ma_m - \sum_{i=1}^{m-1} a_i S_{m-i} \qquad pour \qquad 2 \leq m \leq n.$$

on déduit des inégalités pour les coefficients $a_2, ..., a_{n-1}$.

Les fonctions symétriques S_m pour $2 \leq m \leq n$ doivent vérifier la congruence :

$$S_m = -\sum_{i=1}^{m-1} a_i S_{m-i} \mod m \qquad pour \qquad 2 \leq m \leq n.$$

L'égalité $a_{n-1} = -a_n S_{-1}$ donne dans la pratique une meilleure borne pour a_{n-1} dans le cas ou $|a_n|$ est petit que celle déduite de S_{n-1}.

De même l'inégalité

$$\Big|(n-1)\Big(\sum_{i=1}^{n}\sigma_i(\theta)\Big)^2 - 2n\sum_{1\le i<j\le n}\sigma_i(\theta)\sigma_j(\theta)\Big| + \Big|\sum_{i=1}^{n}\sigma_i(\theta)\Big|^2 \le n\sum_{i=1}^{n}\Big|\sigma_i(\theta)\Big|^2$$

fournit une meilleure majoration pour le deuxième coefficient.

En effet

$$\frac{1}{2}\Big(a_1^2 - T_2(\theta)\Big) \le a_2 \le \frac{1}{2}\Big(T_2(\theta) + \frac{n-2}{n}a_1^2\Big).$$

il nous reste cependant à chercher des majoration pour les fonctions $T_m(\theta)$.

Le théorème suivant, dû à **POHST**, indique une manière de trouver ces majorations.

Théorème 2 (POHST) [20]

si T et N sont deux constantes positives telle que $(T/n)^{n/2} \ge N$, alors les fonctions

$$T_m(x_1,...,x_n) = \sum_{i=1}^{n} x_i^m \qquad pour \qquad m \in \mathbb{Z}, m \ne 0 \;\; et \;\; m \ne 2$$

atteint un maximum absolu sur le compact

$$S = \Big\{x = (x_1,...,x_n) \in \mathbb{R}_+^n : \sum_{i=1}^{n} x_i^2 \le T, \prod_{i=1}^{n} x_i = N\Big\}$$

Ce maximum est atteint en un point $y \in S$ ayant deux coordonnées différentes au plus .

Remarque.

La condition $(T/n)^{n/2} \ge N$ est nécessaire car sinon S est vide.

Nous allons décrire la manière de calculer effectivement ces majorations. On fixe T, N et m $\Big(T = \frac{a_1^2}{n} + \gamma_{n-1}\Big(\frac{|\ d_K\ |}{n}\Big)^{1/n-1},\ N = |\ a_n\ |\ \Big)$. Le maximum de la fonction $T_m(\theta)$ est atteint en un point $y = (y_1,...,y_n) \in S$ ayant deux coordonnées différentes au plus, soit y_1 et y_2. Notons t le nombre de coordonnée de y égal à y_1 , et le reste $(n-t)$ égal à y_2.

$y = (y_1,...,y_n) \in S$ signifie que :

$$N = y_1^t \cdot y_2^{n-t}$$

et

$$T = t \cdot y_1^2 + (n-t) \cdot y_2^2$$

ceci entraine

$$T = t\Big(N \cdot y_2^{t-n}\Big)^{2/t} + (n-t) \cdot y_2^2 \qquad (\star)$$

En résolvant cette équation on détermine y_2 par suite y_1 et donc y comme il s'agit d'une majoration on est amené à déterminer y_2 racine de l'équation $(\star)$ et qui soit la plus petite racine positive.
Pour chaque $m \in Z - \{0, 2\}$ on a :

$$\max_{\theta \in S} T_m(\theta) = T_m(y_1, ..., y_n) = t \cdot y_1^m + (n-t) \cdot y_2^m = t\Big(N \cdot y_2^{t-n}\Big)^{m/t} + (n-t) \cdot y_2^m$$

D'ou :

$$T_m(\theta) \leq \max_{1 \leq t \leq n} \Big\{ t\Big(N y_2^{t-n}\Big)^{m/t} + (n-t) y_2^m \Big\} \qquad pour \qquad m \in Z - \{0, 2\}$$

Remarque

1) Etant donné que les constantes T_m correspondant à $N = 1$ sont plus grandes que celles correspondant à $N > 1$, on peut choisir, pour simplifier, N=1.
2) Si la signature de K est $(0, n/2)$ on ne prend en considération que les valeurs de t paires dans l'intervalle $1 < t < n$.

Afin de compléter la liste des corps de nombres K de degré n et de la signature (r, s) dont le discriminant est majoré, en valeur absolu, par une constante d, on aura besoin , lorsque n n'est pas premier, d'étudier l'existence possible d'extensions relatives K/F qui ne sont pas obtenues à partir des calculs décrit précédemment.
Plaçons nous dans cette situation c'est-à-dire dans le cas ou le corps K contient un sous corps F de degré $[F : \mathbb{Q}] = n'$, de discriminant d_F et de signature (r', s'). On commencera cette étude par l'énoncé d'une proposition qui montre quels sont les corps F à prendre en considération.

$$K$$

$$| \qquad m$$

$$F$$

$$| \qquad n'$$

$$\mathbb{Q}$$

Proposition [17] :

pour qu'il existe une extension relative K/F avec $\mid d_K \mid \leq d$ il faut que les conditions suivantes soient vérifiées :

1) $n = mn^{'}$

2) $s \geq ms^{'}$

3) $\left|d_F\right| \leq \left[\frac{2\gamma_{n-1}}{m(n'-1)}\left(\frac{d}{n}\right)^{\frac{1}{(n-1)}}\right]^{\frac{n'(n'-1)}{2}}$

où $m = [K : F]$ est le degré relative de l'extension relative K/F,et γ_{n-1} le constante d'Hermite en dimension $n-1$.

Remarque :

Dans la pratique l'inégalité $|d_F| \leq d^{1/m}$, déduite de la formule de composition des discriminants, semble donner une meilleure majoration de d_F pour $n' \geq 3$

Supposons donc que le corps F existe, que sont connus son discriminant d_F et une base d'entiers $W = \left\{w_1 = 1, w_2, ...w_{n'}\right\}$, par contre K désignera le corps cherché, contenant le corps F ou l'un de ces conjugués. Le corps K peut ne pas exister .

Nous allons voir maintenant une génération du théorème de **HUNTER-POHST** donnée par **J.MARTINET** qui nous permettra de compléter la liste des corps de nombres K de ce type. Auparavant nous devons introduire les fonction traces relatives.

Soit $J(K)$ (resp. $J(F)$) l'ensemble des $\mathbb{Q}$ – isomorphismes distincts de K (resp. F) dans $\mathbb{C}$.
Pour $\sigma_i \in J(F)$, soit $J_{\sigma_i}(K)$ tel que :

$$J_{\sigma_i}(K) = \Big\{\tau \in J(K) : \tau/F = \sigma_i\Big\} \qquad pour \qquad i = 1, ..., n'$$

Si θ est un entier de K on pose :

$$Tr_{\sigma,K/F}(\theta) = \sum_{\tau \in J_{\sigma_i}(K)} \tau(\theta)$$

C'est la trace relative d'un conjugué de K par rapport à un conjugué de F qu'il contient .

Théorème 3 (J.MARTINET) [17]

soit K un corps de nombres de degré n, extension de degré m d'un sous corps F de degré $[F : \mathbb{Q}]$. Il existe un entier $\theta \in K$, $\theta \notin F$ vérifiant l'inégalité :

$$\sum_{i=1}^{n} \Big|\theta^{(i)}\Big|^2 \leq \frac{1}{m} \sum_{\sigma \in J(F)} \Big(Tr_{\sigma,K/F}(\theta)\Big)^2 + \gamma_{n-n'} \Big(\frac{\mid d_K \mid}{m^{n'} \cdot \mid d_F \mid}\Big)^{\frac{1}{n-n'}}$$

Cette inégalité reste valable pour tout élément de K de la forme $\theta + \lambda$ où $\varepsilon\theta$, avec λ est un entier de F et ε une racine de l'unité de F.

Remarque (1)

L'inégalité précédente reste valable pour tout entier de la forme $\theta - \alpha$ avec $\alpha \in \vartheta_F$, ou encore pour $\varepsilon\theta$ si ε est une racine de l'unité de F.

Remarque (2)

le corps $F(\theta)$ est une extension non triviale de K, et de ce fait un corps intermédiaire entre K et F. Puisque l'étude d'existence possible d'extensions relatives K/F est faite pour chaque diviseur $n' > 1$ de n on peut supposer $K = F(\theta)$.
soit $P(x) = x^m + a_1 x^{m-1} + ... + a_m \in \vartheta_F[x]$ le polynôme minimal de l'entier θ dont l'existence est affirmée dans le théorème précédent .
Nous allons décrire une méthode permettant de construire tous les polynômes relatifs .

Construction des polynômes relatifs [3]

Choix de a_1

Étant donnée que l'inégalité du théorème 3 reste invariante par translation de θ par un entier de $\vartheta_F[x]$, on peut choisir a_1 dans $\vartheta_F[x]$ modulo $m\vartheta_F[x]$, c'est-à-dire de la forme $a_1 = a_1, 1+a_1, 2w_2+...+a_1, n'w_n$ avec $a_{1,i} \in \left\{ -[\frac{n}{2}], ..., [\frac{n-1}{2}] \right\}$ pour $i = 1, ..., n'$ et donc on se limite à $m^{n'}$ valeurs de a_1, nombre qui peut encore diminuer par multiplication ou par translation des racines de l'unité du corps F.

Choix de $a_1 (i = 2, ..., m)$

On fixe a_1 on évalue les autres coefficients en procédant par récurrence à l'aide des formules de NEWTON :

$$S_q = -qa_q - \sum_{i=1}^{q-1} a_q S_{q-i} \qquad pour \qquad 2 \leq q \leq m.$$

où

$$S_q = \sum_{i=1}^{m} \theta_i^q$$

avec $\theta_1, ..., \theta_m$ racines de $P(x)$.

Pour évaluer les S_q possibles, $S_q = x_1 + x_1 w_1 + ... + x_{n'} w_{n'}$, et $x_i \in \mathbb{Z} (i = 1, ..., n')$.

On sait que

$$\sum_{i=1}^{n'} \left| \sigma_i S_q \right| \leq T_q(\theta) \qquad (*)$$

(les $\sigma_i \;\; i = 1, ..., n'$ sont les différents $\mathbb{Q}$-isomorphismes de F dans $\mathbb{C}$) inégalité déduite, en utilisant l'inégalité de **Cauchy Schwartz**, de l'inégalité

$$\sum_{i=1}^{n'} \left| \sigma_i S_q \right|^2 \leq \Big(T_q(\theta) \Big)^2 \qquad q = 2, ..., m \qquad (**)$$

D'autre part

$$\sum_{i=1}^{n'} \left| \sigma_i S_q \right|^2 = {}^t x \cdot A \cdot {}^t \bar{A} \cdot x \qquad avec \qquad x = (x_1, ..., x_{n'})$$

$B = A.{}^t\overline{A}$ n'est autre la matrice de la forme quadratique définie positive associée au réseau des entiers de ϑ_F.

Ainsi déterminer tous les entiers S_q qui satisfont à $(*)$ revient à trouver tous les $x \in \mathbb{Z}^{n'}$ tel que ${}^t x.B.x \leq \Big(T_q(\theta)\Big)^2$.

Soit

$$q(x_1, ..., x_{n'}) = a_{11}\Big(x_1 + a_{12}x_2 + ... + a_{1n'}\Big)^2 + ... + a_{n'-1}\Big(x_{n'-1} + a_{n'-1}x_{n'}\Big)^2 + a_{n'.n'}x_{n'}^2$$

la décomposition de la forme quadratique de matrice B en somme de carrés par la méthode de Gauss.
Alors si on pose $\Im_{n'} = \Big(T_q(\theta)\Big)^2$

$$\Big|y_{n'}\Big| \leq \Big[\sqrt{\frac{\Im_{n'}}{m_{n'n'}}}\Big]$$

Si $\Im_{n'-1} = T_q^2 - m_{n'n'}y_{n'}^2 \geq 0$ alors

$$\Big[-\sqrt{\frac{\Im_{n'-1}}{m_{n'-1\ n'-1}}} - m_{n'-1\ n'-1}y_{n'}\Big] \leq y_{n'-1} \leq \Big[\sqrt{\frac{\Im_{n'-1}}{m_{n'-1\ n'-1}}} - m_{n'-1\ n'-1}y_{n'}\Big]$$

sinon on prend une nouvelle valeur de $x_{n'}$.

supposons avoir déterminé $x_{n'}, ..., x_{k+1}$

si

$$\Im_k = \Im_{k+1} - m_{k+1\ k+1}\Big(y_{k+1} + \sum_{j=k+1}^{n'} m_{k+1\ j}\ y_j\Big)^2 \geq 0,$$

alors on obtient un encadrement de y_k

$$\Big[-\sqrt{\frac{\Im_k}{m_{k\ k}}} - \sum_{j=k+1}^{n'} m_{k\ j}\ y_j\Big] \leq y_k \leq \Big[\sqrt{\frac{\Im_k}{m_{k\ k}}} - \sum_{j=k+1}^{n'} m_{k\ j}\ y_j\Big]$$

Une fois déterminées toutes les coordonnées x_i de s_q, on exprime l'entier $s_q + \sum_{i=1}^{q-1} a_i s_{q-i}$ dans la base W de F. quand toutes les coordonnées de cet entier sont divisibles par q, on obtient alors

$$a_q = -\Big(s_q + \sum_{i=1}^{q-1} a_i s_{q-i}\Big)/q \qquad pour \qquad 1 < q \leq n'$$

et donc un polynôme $P(x)$, on forme alors le polynôme $P(x)$ produit de tous les conjugués de $P(x)$.
les calculs décrits précédemment peuvent être considérablement simplifiés lorsque le corps F est une extension quadratique.

En effet on peut exclure par translation ou multiplication par les racines de l'unité de F, d'autres

valeurs de a_1. D'autre part si F est imaginaire, on a $|s_q| = |\sigma s_q|$ pour $q \in \mathbb{N}$ et par suite l'inégalité $(**)$ devient :

$$\left|s_q\right| \leq \frac{T_q}{2}.$$

Si F est réel, en écrivant les entiers de F sous la forme suivant :

$$\frac{a + b\sqrt{d_F}}{2}$$

où $a \equiv b \mod 2$, on a

$$|s_q| + |\sigma s_q| = \max\left(|a_q|, |b_q|\sqrt{d_F}\right)$$

$$s_q = \frac{a_q + b_q\sqrt{d_F}}{2} \qquad avec \qquad a_q \equiv b_q \mod 2$$

et par suite

$$|a_q| \leq T_q(\theta) \qquad et \qquad b_q \leq \frac{T_q(\theta)}{\sqrt{d_F}}$$

Nous terminerons ce chapitre par l'étude de cas particuliers.

(I) Cas où F est un corps quadratique

Supposons que F est le corps quadratique alors $F = \mathbb{Q}(\sqrt{d})$, où d est sans facteur carré et différent de 1. Soit $(1, w)$ une base intégrale et d_F le discriminant de F. Alors

• si $d \equiv 1\ mod 4$

$$d_F = d \qquad et\ nous\ pouvons\ prendre \qquad w = (1 + \sqrt{d})/2$$

• si $d \equiv 2 \ \ ou \ \ 3\ mod 4$

$$d_F = 4d \qquad et\ nous\ pouvons\ prendre \qquad w = \sqrt{d}$$

de plus, tout entier ν dans F peut s'écrire comme $\nu = (\alpha + \beta\sqrt{d_F})$ avec $\alpha \equiv \beta \mod 2$ pour $d \equiv 1 \mod 4$ et α pour $d \equiv 2 \ \ ou \ \ 3 \mod 4$. On note cet entier par le couple (α, β).

Rappelons que lorsque F est un corps quadratique imaginaire alors

(i) si $d_F = -4$, F contient 4 unités : $\pm 1, \pm i$

(ii) si $d_F = -3$, F contient 6 unités : $\pm 1, \dfrac{\pm 1 \pm i\sqrt{3}}{2}$

(iii) si $d_F < -4$, F contient 2 unités : ± 1

sinon, il contient une infinité d'unités.

Selon le théorème de **J. Martinet**, le coefficient a_1 est choisi dans $\vartheta_F \mod (m\vartheta_F)$. Alors m^2 valeurs possibles pour a_1, un nombre qui peut être considérablement réduit, par la translation ou la multiplication par les racines de l'unité de F, de $m^2/2$ valeurs et plus encore. Par exemple pour les extensions quartiques de corps quadratiques le coefficient a_1 peut être choisi dans l'ensemble

$$\{(0,0),(0,1),(0,2),(2,0),(2,1),(2,2),(4,0),(4,1),(4,2)\}$$

pour $d \equiv 1 \mod 4$ et dans l'ensemble

$$\{(0,0),(1,1),(2,0),(2,2),(3,1),(4,0),(4,2)\}$$

pour $d \equiv 2 \ ou \ 3 \mod 4$.

Notons que les bornes pour les s_i sont meilleures que ceux mis en place dans le cas général. En effet

• si F est imaginaire, alors nous avons $\mid s_i \mid + \mid \sigma(s_i) \mid$ et l'inégalité (4) devient

$$\mid s_i \mid \leq T_i/2$$

• si F est réel où $s_i = (\alpha + \beta\sqrt{d_F})/2$ alors

$$\mid s_i \mid + \mid \sigma(s_i) \mid = \max\Big(\mid \alpha \mid, \mid \beta \mid \sqrt{d_F} \Big) \leq T_i$$

(II) **Cas où K est une extension quadratique de F.**

Dans ce cas, nous avons $K = F(\theta)$ où θ est une racine du polynôme du second degré

$$p(x) = x^2 + ax + b \in \vartheta_K[x]$$

$$b = \theta\theta^{'}$$

$$a = -(\theta + \theta^{'})$$

$$\Delta = b^2 - 4b = (\theta + \theta^{'})^2$$

et

$$\mid \theta \mid^2 + \mid \theta^{'} \mid^2 = \begin{cases} 1/2(\mid \Delta \mid + \mid a \mid^2) & a, b \in \mathbb{C} \\ \Delta + 2b & a, b \in \mathbb{R}, \Delta > 0 \\ 2b & a, b \in \mathbb{R}, \Delta < 0 \end{cases}$$

Proposition

$$\sum_{i=1}^{n} \left|\theta^{(i)}\right|^2 \leq 1/2 \sum_{i=1}^{n^{'}} \left|a^{(i)}\right|^2 + M \Longleftrightarrow \sum_{i=1}^{n^{'}} \left|\Delta^{(i)}\right| \leq 2M$$

Preuve

L'inégalité précédente est une conséquence immédiate de ces égalités

$$\sum_{i=1}^{n} \left|\theta^{(i)}\right|^2 = \sum_{i=1}^{n^{'}} \left(\left|\theta^{(i)}\right|^2 + \left|\theta^{'(i)}\right|^2\right) = 1/2 \sum_{i=1}^{n^{'}} \left(\left|\theta^{(i)} + \theta^{'(i)}\right|^2 + \left|\theta^{(i)} - \theta^{'(i)}\right|^2\right) = 1/2 \sum_{i=1}^{n^{'}} \left|a^{(i)}\right|^2 + \left|\Delta^{(i)}\right|$$

Remarque

Pour l'élimination des polynômes ayant des valeurs trop grandes de $T_2(\theta)$ nous n'avons pas besoin de calculer les racines de chaque conjugué de P, il suffit de vérifier si l'inégalité $\sum_{i=1}^{n^{'}} \left|\Delta^{(i)}\right| \leq 2M$ est remplie.

Remarque

Pour les corps de nombres totalement réel $\sum_{i=1}^{n^{'}} \left|\Delta^{(i)}\right|$ est un entier positif. Plus précisément, nous avons $\sum_{i=1}^{n^{'}} \left|\Delta^{(i)}\right| = T_{K/\mathbb{Q}}(\theta)^2 - 2T_{F/\mathbb{Q}}(b)$.

irréductibilité de test

• Lorsque le sous-corps F est totalement réel ($n^{'} = r^{'}$) et le choix avec signature (r, s) de K est telle que $s \neq 0$, le polynôme $P(x)$ est irréductible dans $\vartheta_F[x]$. En effet, si nous supposer que θ est un nombre entier de F alors $\sigma(\theta) \in \vartheta_F[x]$ avec $\sigma \in J(F)$, comme $s \neq 0$, alors au moins l'un des $\sigma(\theta)$ est non réel. Or ceci, il est impossible puisque $\vartheta_F \subset \mathbb{R}$

• Lorsque le sous-corps F est de signature $(r^{'}, s^{'})$ avec $s^{'}$ impair le polynôme $P(x)$ est irréductible dans $\vartheta_F[x]$. En effet, si nous supposons que θ est un entier de F alors $\sigma(\theta) \in \vartheta_F[x]$ avec $\sigma \in J(F)$, donc $\sum_{\sigma \in J(F)} \sigma(\theta) \in \mathbb{Z}$.

Chapitre 4

Coïncidence de discriminant

Résultats connus

Pour un degré fixe n ($2 \leq n \leq 10$) d'un corps de nombres nous mentionnons, pour toutes les signatures possibles (r, s) tels que $r + 2s = n$, le plus petit discriminant d_K connu, un polynôme f qui engendre le corps K ayant pour d_K discriminant.
Notons que le plus petit discriminant, dans la plupart des cas, a été donné avant l'année mentionnée ; découvert pour d'autres causes, par exemple dans la recherche de corps euclidiens, à la recherche d'extensions non-primitives.

Notation

$rd(K)$ est le racine n^{eme} de d_K, c'est-a-dire $rd(K) = |D|^{\frac{1}{n}}$
$grd(K)$ est la racine discriminante Galois du corps K c'est-a-dire discriminant de la racine de la fermeture de Galois K.

- S_n c'est le groupe symétrique d'ordre $n!$

- A_n c'est le groupe alterné de dégrée $\frac{n!}{2}$

Définition

A_n est l'ensemble des permutation paire de S_n.
pour $n = 1$, on a $A_1 = \{e\}$.
pour $n > 2$ $A_n = \left\{\sigma \in S_n, \varepsilon(\sigma) = 1\right\}$ est le noyan d'isomorphisme $\varepsilon : S_n \longrightarrow \{-1, 1\}$
donc A_n est sous-groupe de S_n de dégrée $\frac{n!}{2}$

- D_n c'est le groupe diédral d'ordre $2n$ avec $n \geq 3$
- C_n c'est le groupe cyclique

Définition

Un groupe infini est dit monogène si il est engendré par un de ses éléments. Cet élément est appelé générateur de ce groupe. Un groupe fini est dit cyclique si il est engendré par un de ses éléments. Cet élément est appelé générateur de ce groupe.

- Gal le groupe de Galois

Degré 2

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(2,0)	5	1	2.24	2.24	x^2+x-1	S_2
(0,1)	-3	1	1.73	1.73	x^2+x+1	S_2

Des tables complètes avec des propriétés arithmétiques pour les corps de nombres quadratiques peuvent être calculé en utilisant KANT-Kash.

Degré 3

Les discriminants minimaux pour le troisième degré ont été donné d'abord par Furtwangler en 1896.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(3,0)	49	1	3.66	3.66	x^3+x^2-2x-1	A_3
(1,1)	-23	1	4.80	2.84	x^3-x-1	S_3

Degré 4

Pour $n=4$; le discriminant minimal pour chaque signature ont été découverts par Mayer en 1929.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(4,0)	725	1	12.04	5.19	$x^4-x^3-3x^2+x+1$	D_4
(2,1)	-275	1	7.42	4.07	x^4-2x^3+x-1	D_4
(0,2)	117	1	6.24	3.29	$x^4-x^3-x^2+x+1$	V_4

Degré 5

Pour les trois signatures possibles de degré 5, discriminants minimaux ont été découverts par Hunter en 1956 et 1957,des listes détaillées y ont été établi par F.Diaz Diaz, M. Pohst et A. Schwarz avec $d_K \leq 2.10^7$ pour $(r;s) = (5;0)$ en 1988 ; $d_K \leq 10^6$ pour $(r;s) = (3;1)$ en 1988 ; et $d_K \leq 10^6$ pour $(r;s) = (1;2)$ en 1988.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(5,0)	14641	1	6.81	6.81	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$	C_5
(3,1)	-4511	1	67.16	5.38	$x^5 - x^3 - 2x^2 + 1$	S_5
(1,2)	1609	1	40.11	3.38	$x^5 - 2x^4 + 3x^3 - 3x^2 + 3x - 1$	S_5

Degré 6

Le discriminant minimal a été découvert par Liang et Zassenhauss en 1976,par M. phost en 1982 pour les signatures restantes. Des tables complètes pour toutes les signatures de degré 6 ont été donnés par M. Olivier (1988) avec $d_K \leq 2.10^5$ $(resp 4.10^5, 10^6, 10^7)$ pour $(r;s) = (0;3)(resp : (2;2);(4;1);(6;0))$.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(6,0)	300125	1	8.18	8.18	$x^6 + x^5 - 7x^4 - 2x^3 + 7x^2 + 2x - 1$	C_6
(4,1)	-92779	1	304.60	6.43	$x^6 + x^5 - 2x^4 - 3x^3 - x^2 + 2x + 1$	S_6
(2,2)	28037	1	34.91	5.51	$x^6 + 2x^5 - 3x^3 + 2x - 1$	S_4C_2
(0,3)	-9747	1	12.33	4.62	$x^6 + x^4 + x^3 - 2x^2 - x + 1$	S_3C_3

Degré 7

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal	résultat dû à
(7,0)	20134393	1	4487.14	11.05	$x^7+x^6-6x^5-5x^4+8x^3+5x^2-2x-1$	S_7	M. Pohst (1977)
(5,1)	-2306599	1	1518.75	8.11	$x^7-3x^5+x^4+x^3-3x^2+x+1$	S_7	F. D. y D. (1988)
(3,2)	612233	1	782.45	6.71	$x^7-x^6-x^5-x^4+x^2+x+1$	S_7	F. D. y D. (1983)
(1,3)	-184607	1	429.66	5.65	$x^7-3x^6+5x^5-7x^4+6x^3-4x^2+2x-1$	S_7	F. D. y D. (1982)

P. Létard donne des listes pour les corps de nombre de degré 7 de discriminant $d_K \leq 6.10^5$ (resp : 18.10^5, 12.10^6, 15.10^7) pour $(r;s) = (1;3)(resp : (3;2);(5;1);(7;0))$

Degré 8

Le minimum pour le discriminant dans le degré de huit ne sont connus que pour deux signatures ;$(8;0)$ par F. Diaz y Diaz, J. Martinet, M. Pohst (1990)$et(0,4)$ par F ; Diaz y Diaz (1987). Pour les autres signatures, nous donnons la plus petite discriminants connue. Les listes restreintes pour les extensions non-primitives pour la signature $(2,3),(4,2)et(6;1)$ a été donné par Sc. Selmane.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(8,0)	282300416	1	45.83	11.39	$x^8+2x^7-7x^6-8x^5+15x^4+8x^3-9x^2-2x+1$	T_{17}
(6,1)	-65106259	1	30.79	22.81	$x^8-2x^7-4x^6+4x^5+7x^4-x^3-5x^2+1$	T_{31}
(4,2)	15243125	1	27.64	7.90	$x^8+x^7-3x^6-3x^5+3x^4+6x^3-2x^2-3x+1$	T_{17}
(2,3)	-4286875	1	9.75	6.75	$x^8-3x^7+4x^6-3x^5+3x^4-6x^3+6x^2-4x+1$	D_8
(0,4)	1257728	1	16.74	5.79	$x^8-4x^7+7x^6-8x^5+8x^4-6x^3+4x^2-2x+1$	T_{17}

Degré 9

Les premiers listes pour les corps de nombre non-primitifs de degré 9 ont été donnés par F. Diaz y Diaz et M.Olivier Nous citons ici les discriminant minimaux.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$	Gal
(9,0)	16240385609	1	1359.57	13.63	$x^9+2x^8-14x^7-32x^6+16x^5+61x^4+15x^3-18x^2-5x+1$	T_{28}
(7,1)	-1904081383	1	765.61	13.98	$x^9+x^8-5x^7-6x^6+5x^5+11x^4+5x^3-6x^2-6x-1$	T_{28}
(5,2)	453771377	1	342.93	11.59	$x^9+x^8-3x^7-3x^6+2x^5+x^4+3x^2-1$	T_{28}
(3,3)	-109880167	1	12.33	10.27	$x^9-5x^8+10x^7-12x^6+9x^5-3x^4-3x^3+4x^2-3x+1$	S_3C_3
(1,4)	29510281	1	17.49	9.87	$x^9-x^8+x^7-3x^6+5x^5-8x^4+8x^3-6x^2+3x-1$	T_{10}

Degré 10

Les premiers liste etablie pour le degré 10 ont été construite par SELMANE pour $r=10$, $r=8$, $r=6$, $r=4$, et $r=2$ et à Leutbecher et Martinet pour $r=0$ (corps euclidienne). nous trouvons des tableaux complets pour chaque signature en degré 10 contenant des corps quintiques.

(r,s)	d_k	h	$grd(K)$	$rd(K)$	$f(x)$
(10,0)	443952558373	1	4281.62	14.61	$x^{10}-11x^8-3x^7+37x^6+14x^5-48x^4-22x^3+20x^2+12x+1$
(8,1)	-70952789611	1	123.89	12.16	$x^{10}+x^9-7x^8-x^7+16x^6-6x^5-14x^4+8x^3+6x^2-2x-1$
(6,2)	15417264029	1	1632.78	10.44	$x^{10}-5x^9+6x^8+7x^7-21x^6+10x^5+17x^4-18x^3-2x^2+5x-1$
(4,3)	-3120654523	1	605.24	8.90	$x^{10}+2x^9+2x^8+7x^7+8x^6+3x^5+8x^4+7x^3+2x^2+2x+1$
(2,4)	799905449	1	425.55	7.77	$x^{10}-x^9+2x^8-5x^6-x^5+3x^4+4x^3+x^2-2x-1$
(0,5)	-209352647	1	263.42	6.79	$x^{10}-3x^9+8x^8-14x^7+20x^6-22x^5+19x^4-13x^3+6x^2-2x+1$

Coïncidence de discriminant

Dans le tableau I, pour chaque degré n ($n \leq 6$) et la signature (r, s) résultats connus, concernant coïncidences de discriminants dans les limites de tables disponibles de corps de nombres sont présentés [11]. La valeur d_1 du discriminant de la première coïncidence de discriminant de 2 corps non isomorphes et la valeur d_2 de le nombre maximum β ($\beta > 2$) des corps de nombres non isomorphes de même discriminant de discriminant inférieure à celle du B lié sont donnés. Nous indiquons le nombre η (resp ; η_1, η_2) des corps de discriminant plus petit que B (resp ; d_1, d_2)
Enfin, signifie qu'il n'y a pas de coïncidences de discriminants dans de tels cas.
Parmi les 121 (resp. 162, 201, 154) corps de nombres de degré 7 ayant un degré (resp. 3, 5,7) réel lieu de discriminant plus petit que, en valeur absolue, 6.10^5 (resp. 18.10^5, 12.10^6, 15.10^7) il existe pas de coïncidences de discriminant.

RÉSULTATS ET COMMENTAIRES

Ensuite, nous avons calculé le polynôme

$$f(x) = \prod_{i=1}^{n} \Big(x^2 + \sigma_i(a)x + \sigma_i(b)\Big) = \sum_{i=1}^{10} t_i x^{10-i} \quad t_0 = 1$$

Dans ce paragraphe nous reprenons les résultats obtenu par S. Selmane sur la détermination du résultat.
Pour un corps quintique fixe F de signature (r', s'), le nombre maximum η des corps non isomorphes de même discriminant $2^{10} \cdot p \cdot_F^2$ est obtenu avec la signature (r, s) de K tel que $|r - r'| = 1$. Pour la signature correspondant, c'est-à-dire, $(2r' - r, \frac{1}{2}r + 2s')$, on obtient $\beta(\beta \leq \eta)$ corps non isomorphe. De plus, il est pas nécessaire de faire le calcul pour la détermination de polynômes définissant le β corps non isomorphes de même discriminant pour la signature correspondante $(2r' - r, \frac{1}{2}r + 2s')$. En effet, si on désigne par

$$f_i(x) = x^{10} + a_1x^8 + a_2x^6 + a_3x^4 + a_4x^2 + a_5 \qquad i = 1, ..., \eta$$

Les η polynômes définissant les corps non isomorphes avec même discriminant de discriminant $|d_K| = 2^{10} \cdot p \cdot d_F^2$ sont, parmi les η polynômes g_i $(i = 1, ..., \eta)$

$$g_i(x) = x^{10} - a_1 x^8 + a_2 x^6 - a_3 x^4 + a_4 x^2 - a_5$$

β polynômes définissent les corps de nombres non isomorphes avec même discriminant de signature $(2r' - r, \frac{1}{2}r + 2s')$ et discriminant
$|d_K| = 2^{10} \cdot p \cdot d_F^2$, et $(\eta - \beta)$ polynômes définir des corps non isomorphes avec même discriminant de signature $(2r' - r, \frac{1}{2}r + 2s')$ et discriminant $d_K = p \cdot d_F^2$. Les polynômes $f_i(x)$ et $g_i(x)$ ne sont autre les polynômes définissant le corps quintique F.
Les notations pour le groupe de Galois Gal de F sont similaires à celles de G. Butler and J. McKay. h (resp. h^+) correspond au classe de nombre (resp. borne classe de nombre)de F, et nb est le nombre de corps pour toutes les signatures.
Nous listons pour chaque signature fixe du corps F, les polynômes définissant les corps non isomorphes dixième de degré construit de signature (r, s) et celles qui définissent le degré 10 corps non isomorphes pour la signature correspondante $(2r' - r, \frac{1}{2}r + 2s')$.

TABLE 1

(n, r)	$\mathfrak{B}$	η	d_1	η_1	β	d_2	η_2
$(3,1)$	10^6	182417	$-972 = -2^2 3^5$	120	9	$274347 = 3^5 1129$	48356
$(3,3)$	$2 \cdot 10^6$	112444	$3969 = 3^4 7^2$	133	4	32009 *prime*	1400
$(4,0)$	10^6	81322	$576 = 2^6 3^2$	18	19	$705600 = 2^6 3^2 5^2 7^2$	56296
$(4,2)$	10^6	90671	$-1472 = -2^6 23$	30	10	$-132800 = -2^6 5^2 83$	9517
$(4,4)$	10^6	13073	$16448 = 2^6 257$	96	7	$705600 = 2^6 3^2 5^2 7^2$	8801
$(5,1)$	10^6	28993	$16757 = 13 \times 1289$	137	5	$721872 = 2^4 3^4 557$	19630
$(5,3)$	10^6	10800	$-28976 = -2^4 1811$	63	3	$-428976 = -2^4 3^4 331$	3618
$(5,5)$	$2 \cdot 10^7$	22740	1810969 *prime*	928	✓	✓	✓
$(6,0)$	$2 \cdot 10^5$	442	$-33856 = -2^6 23^2$	36	3	$-64387 = -31^2 67$	98
$(6,2)$	$4 \cdot 10^5$	1179	111269 *prime*	161	3	$237521 = 23^2 449$	505
$(6,4)$	10^6	405	✓	✓	✓	✓	✓
$(6,6)$	10^7	398	$3195392 = 2^9 79^2$	72	✓	✓	✓

Parmi les 121 (resp. 162, 201, 154) corps de nombres de degré 7 ayant une (resp. 3, 5, 7) place réel de discriminant plus petit, en valeur absolu, $6 \cdot 10^5$ (resp. $18 \cdot 10^5$, $12 \cdot 10^6$, $15 \cdot 10^7$) il n'existe pas de coïncidence de discriminant.

TABLE 2

Number of Fields with same Discriminant : $d_{\mathcal{K}} = 2^{10} \cdot p \cdot d_{\mathcal{F}}^2$

(h, h^+)	r'	Gal	$d_{\mathcal{F}}$	p	$(0,5)$	$(2,4)$	$(4,3)$	$(6,2)$	$(8,1)$	$(10,0)$	nb
$(1,1)$	5	T_1	14641	23	1	5	9	10	5	1	31
	5	T_2	160801	83	5	25	47	50	23	5	155
	5	T_4	15784729	149	5	23	50	48	25	4	155
	5	T_5	24217	3329	5	24	50	46	25	5	155
	3	T_5	-7367	277	10	29	30	10	–	–	79
	1	T_2	2209	83	19	20	–	–	–	–	39
	1	T_3	44217	359	20	20	–	–	–	–	40
	1	T_4	42849	911	18	20	–	–	–	–	38
	1	T_5	1649	499	19	20	–	–	–	–	39
$(1,2)$	5	T_3	6725897	59	6	22	48	52	20	6	154
	5	T_4	11812969	769	6	24	48	48	26	6	158
	5	T_5	144209	227	6	22	48	52	20	6	154
	3	T_5	-39231	173	12	28	28	12	–	–	80
$(1,4)$	5	T_5	1476577	103	4	36	38	40	34	4	156
$(2,2)$	5	T_5	12284977	89	2	10	20	18	10	2	62
	3	T_5	-550151	709	12	36	36	12	–	–	96
	1	T_5	64665	269	8	8	–	–	–	–	16

Number of Fields with same Discriminant : $d_{\mathcal{K}} = 2^{10} \cdot p \cdot d_{\mathcal{F}}^2$

(h, h^+)	r'	Gal	$d_{\mathcal{F}}$	p	$(0,5)$	$(2,4)$	$(4,3)$	$(6,2)$	$(8,1)$	$(10,0)$	nb
$(2,4)$	5	T_5	7322417	191	0	16	14	16	14	0	60
	3	T_5	-936823	137	16	32	32	16	–	–	96
$(2,8)$	5	T_5	15216977	419	0	48	40	48	40	0	176
$(3,3)$	1	T_4	426409	631	19	20	–	–	–	–	39
	1	T_5	271785	701	20	18	–	–	–	–	38
$(4,4)$	1	T_5	791825	59	22	24	–	–	–	–	46
$(5,5)$	1	T_2	717409	149	20	19	–	–	–	–	39
	1	T_5	792425	937	20	20	–	–	–	–	40

Table 3

$(r\prime, s\prime) = (1, 2)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 531 \cdot 791825^2$	
$(0, 5)$	$(2, 4)$
$(1, 0, -2, 0, 9, 0, 65, 0, -119, 0, 531)$	$(1, 0, 2, 0, 9, 0, -65, 0, -119, 0, -531)$
$(1, 0, 2, 0, 32, 0, 217, 0, 392, 0, 531)$	$(1, 0, -2, 0, 32, 0, -217, 0, 392, 0, -531)$
$(1, 0, 6, 0, 65, 0, 234, 0, 968, 0, 531)$	$(1, 0, -6, 0, 65, 0, -234, 0, 968, 0, -531)$
$(1, 0, 8, 0, 46, 0, 177, 0, 304, 0, 531)$	$(1, 0, -8, 0, 46, 0, -177, 0, 304, 0, -531)$
$(1, 0, 8, 0, -31, 0, 334, 0, 838, 0, 531)$	$(1, 0, -8, 0, -31, 0, -334, 0, 838, 0, -531)$
$(1, 0, 15, 0, 69, 0, -14, 0, -397, 0, 531)$	$(1, 0, -15, 0, 69, 0, 14, 0, -397, 0, -531)$
$(1, 0, -27, 0, 266, 0, -1113, 0, 1559, 0, 531)$	$(1, 0, 27, 0, 266, 0, 1113, 0, 1559, 0, -531)$
$(1, 0, 28, 0, 251, 0, 767, 0, 1019, 0, 531)$	$(1, 0, -28, 0, 251, 0, -767, 0, 1019, 0, -531)$
$(1, 0, 30, 0, 49, 0, 6, 0, 278, 0, 531)$	$(1, 0, -30, 0, 49, 0, -6, 0, 278, 0, -531)$
$(1, 0, -1, 0, -78, 0, 505, 0, -1277, 0, 1475)$	$(1, 0, 1, 0, -78, 0, -505, 0, -1277, 0, -1475)$
$(1, 0, 4, 0, 21, 0, 254, 0, 736, 0, 1475)$	$(1, 0, -4, 0, 21, 0, -254, 0, 736, 0, -1475)$
$(1, 0, 8, 0, -5, 0, 237, 0, -321, 0, 1475)$	$(1, 0, -8, 0, -5, 0, -237, 0, -321, 0, -1475)$
$(1, 0, 11, 0, 70, 0, 306, 0, 729, 0, 1475)$	$(1, 0, -11, 0, 70, 0, -306, 0, 729, 0, -1475)$
$(1, 0, 20, 0, 169, 0, 568, 0, 1412, 0, 1475)$	$(1, 0, -20, 0, 169, 0, -568, 0, 1412, 0, -1475)$
$(1, 0, 21, 0, 201, 0, 761, 0, 1116, 0, 1475)$	$(1, 0, -21, 0, 201, 0, -761, 0, 1116, 0, -1475)$
$(1, 0, 22, 0, 193, 0, 835, 0, 1773, 0, 1475)$	$(1, 0, -22, 0, 193, 0, -835, 0, 1773, 0, -1475)$
$(1, 0, 23, 0, 208, 0, 895, 0, 1823, 0, 1475)$	$(1, 0, -23, 0, 208, 0, -895, 0, 1823, 0, -1475)$
$(1, 0, 28, 0, 273, 0, 1105, 0, 1503, 0, 1475)$	$(1, 0, -28, 0, 273, 0, -1105, 0, 1503, 0, -1475)$
$(1, 0, 9, 0, 28, 0, 595, 0, 5425, 0, 13275)$	$(1, 0, -9, 0, 28, 0, -595, 0, 5425, 0, -13275)$
$(1, 0, -44, 0, 723, 0, -5115, 0, 11525, 0, 13275)$	$(1, 0, 44, 0, 723, 0, 5115, 0, 11525, 0, -13275)$
$(1, 0, -26, 0, 175, 0, 700, 0, -12150, 0, 36875)$	$(1, 0, 26, 0, 175, 0, -700, 0, -12150, 0, -36875)$
$(1, 0, 49, 0, 885, 0, 7250, 0, 26925, 0, 36875)$	$(1, 0, -49, 0, 885, 0, -7250, 0, 26925, 0, -36875)$
	$(1, 0, -15, 0, 74, 0, 258, 0, -283, 0, -1475)$
	$(1, 0, -1, 0, -17, 0, 72, 0, 181, 0, -531)$

Table 4

$(r\prime, s\prime) = (3,1)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 709 \cdot (-550151)^2$	
$(2,4)$	$(4,3)$
$(1,0,-10,0,-50,0,187,0,210,0,-709)$	$(1,0,10,0,-50,0,-187,0,210,0,709)$
$(1,0,-30,0,305,0,338,0,-686,0,-709)$	$(1,0,30,0,305,0,-338,0,-686,0,709)$
$(1,0,17,0,33,0,3,0,-212,0,-709)$	$(1,0,-17,0,33,0,-3,0,-212,0,709)$
$(1,0,17,0,9,0,-423,0,-188,0,-709)$	$(1,0,-17,0,9,0,423,0,-188,0,709)$
$(1,0,31,0,359,0,1684,0,2563,0,-709)$	$(1,0,-31,0,359,0,-1684,0,2563,0,709)$
$(1,0,11,0,-184,0,-917,0,-1405,0,-709)$	$(1,0,-11,0,-184,0,917,0,-1405,0,709)$
$(1,0,0,0,41,0,458,0,-1550,0,-709)$	$(1,0,0,0,41,0,-458,0,-1550,0,709)$
$(1,0,6,0,-173,0,-1933,0,-5481,0,-709)$	$(1,0,-6,0,-173,0,1933,0,-5481,0,709)$
$(1,0,-7,0,56,0,427,0,-17,0,-709)$	$(1,0,7,0,56,0,-427,0,-17,0,709)$
$(1,0,6,0,-37,0,-88,0,574,0,-709)$	$(1,0,-6,0,-37,0,88,0,574,0,709)$
$(1,0,33,0,145,0,104,0,-465,0,-709)$	$(1,0,-33,0,145,0,-104,0,-465,0,709)$
$(1,0,39,0,514,0,2750,0,5181,0,-709)$	$(1,0,-39,0,514,0,-2750,0,5181,0,709)$
$(1,0,-18,0,13,0,351,0,-751,0,-709)$	$(1,0,18,0,13,0,-351,0,-751,0,709)$
$(1,0,0,0,-136,0,-691,0,-1184,0,-709)$	$(1,0,0,0,-136,0,691,0,-1184,0,709)$
$(1,0,17,0,35,0,-254,0,719,0,-709)$	$(1,0,-17,0,35,0,254,0,719,0,709)$
$(1,0,17,0,-1213,0,15238,0,-58031,0,-709)$	$(1,0,-17,0,-1213,0,-15238,0,-58031,0,709)$
$(1,0,2,0,50,0,199,0,-2746,0,-709)$	$(1,0,-2,0,50,0,-199,0,-2746,0,709)$
$(1,0,-25,0,186,0,-207,0,-1205,0,-709)$	$(1,0,25,0,186,0,207,0,-1205,0,709)$
$(1,0,27,0,-126,0,-1077,0,4555,0,-6381)$	$(1,0,-27,0,-126,0,1077,0,4555,0,6381)$
$(1,0,12,0,-43,0,-1111,0,-4891,0,-6381)$	$(1,0,-12,0,-43,0,1111,0,-4891,0,6381)$
$(1,0,65,0,-133,0,-1655,0,6460,0,-6381)$	$(1,0,-65,0,-133,0,1655,0,6460,0,6381)$
$(1,0,48,0,893,0,7626,0,24562,0,-6381)$	$(1,0,-48,0,893,0,-7626,0,24562,0,6381)$
$(1,0,3,0,-82,0,10,0,977,0,-6381)$	$(1,0,-3,0,-82,0,-10,0,977,0,6381)$
$(1,0,37,0,381,0,1351,0,-46,0,-6381)$	$(1,0,-37,0,381,0,-1351,0,-46,0,6381)$
$(1,0,-1,0,-279,0,-2482,0,-8017,0,-6381)$	$(1,0,1,0,-279,0,2482,0,-8017,0,6381)$
$(1,0,40,0,353,0,644,0,-1844,0,-6381)$	$(1,0,-40,0,353,0,-644,0,-1844,0,6381)$
$(1,0,-9,0,-159,0,-800,0,-8743,0,-34741)$	$(1,0,9,0,-159,0,800,0,-8743,0,34741)$

$(r\prime, s\prime) = (3,1)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 709 \cdot (-550151)^2$	
$(2,4)$	$(4,3)$
$(1,0,38,0,-622,0,-683,0,26278,0,-34741)$	$(1,0,-38,0,-622,0,683,0,26278,0,34741)$
$(1,0,22,0,-100,0,-5427,0,-35886,0,-34741)$	$(1,0,-22,0,-100,0,5427,0,-35886,0,34741)$
$(1,0,16,0,-30,0,-2155,0,-15480,0,-34741)$	$(1,0,-16,0,-30,0,2155,0,-15480,0,34741)$
$(1,0,15,0,-95,0,-2929,0,-18114,0,-34741)$	$(1,0,-15,0,-95,0,2929,0,-18114,0,34741)$
$(1,0,24,0,187,0,348,0,-5416,0,-34741)$	$(1,0,-24,0,187,0,-348,0,-5416,0,34741)$
$(1,0,-1,0,-403,0,-488,0,22563,0,-57429)$	$(1,0,1,0,-403,0,488,0,22563,0,57429)$
$(1,0,38,0,-239,0,-4357,0,39559,0,-85789)$	$(1,0,-38,0,-239,0,4357,0,39559,0,85789)$
$(1,0,43,0,347,0,-6263,0,-83906,0,-85789)$	$(1,0,-43,0,347,0,6263,0,-83906,0,85789)$
$(1,0,52,0,581,0,-6840,0,-133974,0,-516861)$	$(1,0,-52,0,581,0,6840,0,-133974,0,516861)$

Table 5

$(r\prime, s\prime) = (5,0)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 277 \cdot 144209^2$	
$(6,2)$	$(4,3)$
$(1,0,-26,0,103,0,132,0,-222,0,-227)$	$(1,0,26,0,103,0,-132,0,-222,0,227)$
$(1,0,-12,0,-19,0,111,0,53,0,-227)$	$(1,0,12,0,-19,0,-111,0,53,0,227)$
$(1,0,-12,0,-29,0,117,0,69,0,-227)$	$(1,0,12,0,-29,0,-117,0,69,0,227)$
$(1,0,24,0,-63,0,-128,0,394,0,-227)$	$(1,0,-24,0,-63,0,128,0,394,0,227)$
$(1,0,-22,0,80,0,83,0,-346,0,-227)$	$(1,0,22,0,80,0,-83,0,-346,0,227)$
$(1,0,13,0,-15,0,-367,0,772,0,-227)$	$(1,0,-13,0,-15,0,367,0,772,0,227)$
$(1,0,1,0,-59,0,44,0,959,0,-2043)$	$(1,0,-1,0,-59,0,-44,0,959,0,2043)$
$(1,0,9,0,-103,0,91,0,242,0,-227)$	$(1,0,-9,0,-103,0,-91,0,242,0,227)$
$(1,0,2,0,-51,0,-23,0,595,0,-227)$	$(1,0,-2,0,-51,0,23,0,595,0,227)$
$(1,0,-39,0,42,0,298,0,-363,0,-227)$	$(1,0,39,0,42,0,-298,0,-363,0,227)$
$(1,0,8,0,-117,0,349,0,-215,0,-227)$	$(1,0,-8,0,-117,0,-349,0,-215,0,227)$
$(1,0,-33,0,313,0,-759,0,-1002,0,-227)$	$(1,0,33,0,313,0,759,0,-1002,0,227)$
$(1,0,11,0,-11,0,-202,0,459,0,-227)$	$(1,0,-11,0,-11,0,202,0,459,0,227)$
$(1,0,-47,0,-102,0,299,0,529,0,-227)$	$(1,0,47,0,-102,0,-299,0,529,0,227)$

$(r\prime, s\prime) = (5, 0)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 277 \cdot 144209^2$	
$(6, 2)$	$(4, 3)$
$(1, 0, -33, 0, 313, 0, -759, 0, -1002, 0, -227)$	$(1, 0, 33, 0, 313, 0, 759, 0, -1002, 0, 227)$
$(1, 0, 11, 0, -11, 0, -202, 0, 459, 0, -227)$	$(1, 0, -11, 0, -11, 0, 202, 0, 459, 0, 227)$
$(1, 0, -47, 0, -102, 0, 299, 0, 529, 0, -227)$	$(1, 0, 47, 0, -102, 0, -299, 0, 529, 0, 227)$
$(1, 0, -20, 0, 103, 0, 140, 0, -1540, 0, -227)$	$(1, 0, 20, 0, 103, 0, -140, 0, -1540, 0, 227)$
$(1, 0, 14, 0, -15, 0, -172, 0, 390, 0, -227)$	$(1, 0, -14, 0, -15, 0, 172, 0, 390, 0, 227)$
$(1, 0, 17, 0, -2, 0, -301, 0, 513, 0, -227)$	$(1, 0, -17, 0, -2, 0, 301, 0, 513, 0, 227)$
$(1, 0, 14, 0, -26, 0, -541, 0, 708, 0, -227)$	$(1, 0, -14, 0, -26, 0, 541, 0, 708, 0, 227)$
$(1, 0, -8, 0, -17, 0, 144, 0, 146, 0, -227)$	$(1, 0, 8, 0, -17, 0, -144, 0, 146, 0, 227)$
$(1, 0, -11, 0, 23, 0, 78, 0, -173, 0, -227)$	$(1, 0, 11, 0, 23, 0, -78, 0, -173, 0, 227)$
$(1, 0, 20, 0, -19, 0, -248, 0, 490, 0, -227)$	$(1, 0, -20, 0, -19, 0, 248, 0, 490, 0, 227)$
$(1, 0, -1, 0, -73, 0, 329, 0, -286, 0, -227)$	$(1, 0, 1, 0, -73, 0, -329, 0, -286, 0, 227)$
$(1, 0, 5, 0, -79, 0, -164, 0, 1145, 0, -227)$	$(1, 0, -5, 0, -79, 0, 164, 0, 1145, 0, 227)$
$(1, 0, -19, 0, 35, 0, 361, 0, 172, 0, -227)$	$(1, 0, 19, 0, 35, 0, -361, 0, 172, 0, 227)$
$(1, 0, 23, 0, 61, 0, -814, 0, 1323, 0, -227)$	$(1, 0, -23, 0, 61, 0, 814, 0, 1323, 0, 227)$
$(1, 0, 29, 0, 135, 0, -629, 0, 694, 0, -227)$	$(1, 0, -29, 0, 135, 0, 629, 0, 694, 0, 227)$
$(1, 0, -1, 0, -58, 0, 67, 0, 269, 0, -227)$	$(1, 0, 1, 0, -58, 0, -67, 0, 269, 0, 227)$
$(1, 0, -3, 0, -70, 0, 145, 0, 95, 0, -227)$	$(1, 0, 3, 0, -70, 0, -145, 0, 95, 0, 227)$
$(1, 0, -26, 0, 151, 0, -90, 0, -478, 0, -227)$	$(1, 0, 26, 0, 151, 0, 90, 0, -478, 0, 227)$
$(1, 0, 3, 0, -45, 0, -62, 0, 499, 0, -227)$	$(1, 0, -3, 0, -45, 0, 62, 0, 499, 0, 227)$
$(1, 0, 12, 0, -577, 0, 394, 0, 326, 0, -227)$	$(1, 0, -12, 0, -577, 0, -394, 0, 326, 0, 227)$
$(1, 0, 0, 0, -31, 0, 47, 0, 129, 0, -227)$	$(1, 0, 0, 0, -31, 0, -47, 0, 129, 0, 227)$
$(1, 0, -1, 0, -64, 0, -85, 0, 377, 0, -227)$	$(1, 0, 1, 0, -64, 0, 85, 0, 377, 0, 227)$
$(1, 0, -4, 0, -40, 0, 59, 0, 230, 0, -227)$	$(1, 0, 4, 0, -40, 0, -59, 0, 230, 0, 227)$
$(1, 0, 1, 0, -28, 0, 17, 0, 169, 0, -227)$	$(1, 0, -1, 0, -28, 0, -17, 0, 169, 0, 227)$
$(1, 0, 2, 0, -53, 0, 47, 0, 333, 0, -227)$	$(1, 0, -2, 0, -53, 0, -47, 0, 333, 0, 227)$
$(1, 0, -7, 0, -31, 0, 223, 0, -52, 0, -227)$	$(1, 0, 7, 0, -31, 0, -223, 0, -52, 0, 227)$
$(1, 0, -7, 0, -33, 0, 109, 0, 76, 0, -227)$	$(1, 0, 7, 0, -33, 0, -109, 0, 76, 0, 227)$
$(1, 0, -6, 0, -10, 0, 81, 0, 8, 0, -227)$	$(1, 0, 6, 0, -10, 0, -81, 0, 8, 0, 227)$

$(r\prime, s\prime) = (5, 0)$ et $d_{\mathcal{K}} = (-1)^s 2^{10} \cdot 277 \cdot 144209^2$	
$(6, 2)$	$(4, 3)$
$(1, 0, -18, 0, 12, 0, 237, 0, -132, 0, -227)$	$(1, 0, 18, 0, 12, 0, -237, 0, -132, 0, 227)$
$(1, 0, 29, 0, 159, 0, -728, 0, 757, 0, -227)$	$(1, 0, -29, 0, 159, 0, 728, 0, 757, 0, 227)$
$(1, 0, -6, 0, -50, 0, 267, 0, 554, 0, -2043)$	$(1, 0, 6, 0, -50, 0, -267, 0, 554, 0, 2043)$
$(1, 0, -25, 0, 123, 0, 538, 0, -1433, 0, -2043)$	$(1, 0, 25, 0, 123, 0, -538, 0, -1433, 0, 2043)$
$(1, 0, -14, 0, 25, 0, 289, 0, -557, 0, -2043)$	$(1, 0, 14, 0, 25, 0, -289, 0, -557, 0, 2043)$
$(1, 0, -23, 0, 24, 0, 427, 0, -287, 0, -2043)$	$(1, 0, 23, 0, 24, 0, -427, 0, -287, 0, 2043)$
$(1, 0, -7, 0, -51, 0, 426, 0, -193, 0, -2043)$	$(1, 0, 7, 0, -51, 0, -426, 0, -193, 0, 2043)$
$(1, 0, -32, 0, 292, 0, -365, 0, -2630, 0, -2043)$	$(1, 0, 32, 0, 292, 0, 365, 0, -2630, 0, 2043)$
$(1, 0, -37, 0, 412, 0, -1047, 0, -3557, 0, -2043)$	$(1, 0, 37, 0, 412, 0, 1047, 0, -3557, 0, 2043)$
$(1, 0, -21, 0, 99, 0, 136, 0, -911, 0, -227)$	
$(1, 0, 0, 0, -80, 0, -99, 0, 414, 0, -227)$	
$(1, 0, -6, 0, -111, 0, -44, 0, 424, 0, -227)$	
$(1, 0, -28, 0, 140, 0, 661, 0, 434, 0, -227)$	

Bibliographie

[1] JOSETTE CALAIS, élément de théorie des groupes.

[2] F. DIAZ Y DIAZ, Tables minorant la racine n-iéme du discriminant d'un corps de degré n, Publ. Math. d'Orsay 8O-06 (1980).

[3] F. Diaz y Diaz, Sur la construction explicite des extensions relatives, Preprint 1988.

[4] F. DIAZ Y DIAZ, sur les discriminants minimaux.Sém.théorie des nombres de bordeaux (1981/1982).exp N 14.

[5] F. Diaz y Diaz, Petits discriminants des corps de nombres totalement imaginaires de degré 8, J. Number Theory 25 (1987), 34-52.

[6] F. Diaz y Diaz, Discriminants minima et petits discriminants des corps de nombres de degré 7 avec cinq places réelles, J. London Math. Soc. 38 (2) (1988), 33-46.

[7] F. Diaz y Diaz, Valeurs minima du discriminant des corps de nombres de degré 7 ayant une seule place réelle, C. R. Acad. Sci. Paris 296 (1983), 137-139.

[8] F. DIAZ Y DIAZ, Le résultat de Ore-Mantes-nart. Seminaire de théorie des nombres de bordeaux (1991).

[9] H. J. Godwin, On totally complex quartic fields with small discriminant, Cambridge Philos. Soc. 53 (1957), 1-4.

[10] H. J. Godwin, Real quartic fields with small discriminant, J. London Math. Soc. 31 (1956), 478-485.

[11] J. HUNTER, The minimum discriminants of quintic fields, Proc. Glasgow Math. Assoc. 3 (1957), 57-67.

[12] H. W. LENSTRA. JR., Euclidean number fields of large degree, Invent Math. 38 (1977),237-254.

[13] A. Leutbecher, Lenstra's constant and Euclidean number fields, Astérisque, 94 (1982), 87-131.

[14] G. Poitou, Sur les petits discriminants, Sém. Delange-Pisot-Poitou (Théorie des nombres), 18-iéme année, 1976/1977, n^o 6, 1-18.

[15] G. Poitou, Minorations de discriminants (d'après A. M. Odlyzko), Sem. Bourbaki (Théorie des nombres), 28-iéme année, 1975/1976, n^o 479, 1-18.

[16] J. Martinet, Petits discriminants des corps de nombres, Journées arithmétiques 1980, J. V. Armitage Ed., London Math. Soc. Lecture Notes Séries 56 (1982), 151-193.

[17] J. Martinet, Méthodes géométriques dans la recherche des petits discriminants, Séminaire. de Théorie des nombres de paris 1983/1984, Birkhauser Verlag, Bassel (1985) 147-179.

[18] J. Martinet, Petits discriminants, Ann. Inst. Fourier (Grenoble) 29, $n°1$ (1979), 159 - 170.

[19] M. Olivier, The computation of sextic fields with a cubic subfield and no quadratic subfield.

[20] M. POHST. On the computation of number fields of small discriminants including the minimum discriminant of sixth degree fields, J. Number Théorie 14 (1982), 99-117.

[21] S. Omar Majoration du premier zéro de la fonction zêta de Dedekind par (Talence) (2000).

[22] S. Omar, Localization of the first zero of the Dedekind zeta function, Math. Comp., à paraître.

[23] E. Tollis, Zéros of Dedekind zeta functions in the critical strip, Math. Comp. 66 (1997), 1295-1321.

[24] S. Selmane, On the Multiplicity of discriminants of Relative Quadratic Extension of quintic.

[25] S. Selmane, Tenth degree numbre fields with quintic fields having one real place, Math. Comp. 70, 234 (2001), pp. 845 - 851.

[26] Site-Numbre fields-hopps.la.asu.edu/NFDB/.