MÉTHODES GÉOMÉTRIQUES DANS LA RECHERCHE DES PETITS DISCRIMINANTS

JACQUES MARTINET

Ce texte reproduit à quelques corrections mineures près l'article des actes du Séminaire de Théorie des Nombres de Paris, année 1983-1984, publié chez Birkhäuser dans la collection *Progress in Mathematics*, **59** (1985), 147–179. Noter que pour ce volume, les usuels tirés-à-part (*reprints*) n'avaient pas été distribués aux auteurs.

Cet exposé a été rédigé à l'intention de Francisco Diaz y Diaz, auprès de qui je venais de remplacer Georges Poitou en tant que directeur de thèse, et a été rapidement utilisé par le destinataire dans la recherche de petits discriminants en degrés 7 et 8.

Quelques années plus tard, j'ai découvert que pour la partie consacrée aux extensions relatives, j'avais été précédé par Godwin; voir

H.J.Godwin, *The determination of fields of small discriminant with a given subfield*, Math. Scand **6** (1958), 40–46 ; MR0105404.

Je m'excuse auprès de son auteur de ne pas avoir tenu compte de cet article.

MÉTHODES GÉOMÉTRIQUES DANS LA RECHERCHE DES PETITS DISCRIMINANTS

Jacques Martinet

On sait depuis Hermite qu'il n'y a, à isomorphisme près, qu'un nombre fini de corps de nombres dont le discriminant a pour valeur un entier donné. Il est donc naturel de chercher à classer les corps de nombres par leur discriminant, c'est-à-dire de donner pour chaque entier la liste des corps de nombres ayant cet entier pour discriminant. En plus du discriminant, il est raisonnable de faire intervenir la signature (nombres de places réelles et complexes); on sait en effet depuis Minkowski que, à degré égal, les discriminants ont tendance à croître avec le nombre de places réelles. Par ailleurs, dans l'état actuel de nos connaissances, on n'a pas d'autre moyen pour décrire les corps de degré ≥ 5 que donner un polynôme définissant le corps. La question précise que l'on se pose est la suivante : étant donné un entier n, un couple (r,s) avec $r+2s=n$ et un réel positif M, trouver des réels $M_1,\ldots,M_n$ tels que tout corps de degré n, de signature (r,s) et de discriminant $\leq M$ en valeur absolue puisse être défini par un polynôme $X^n - a_1X^{n-1} + a_2X^{n-2} + \ldots + (-1)^n a_n$ de $\mathbb{Q}[X]$ avec $|a_i| \leq M_i$ pour $1 \leq i \leq n$, et, en fait, trouver le plus de contraintes possibles pour les coefficients a_i.

Un problème technique apparaît alors : s'il s'agit d'un corps imprimitif, c'est-à-dire contenant un sous-corps non trivial, il faut s'assurer que les éléments définis à conjugaison près par les polynômes ne sont pas dans un sous-corps. On peut faire en sorte qu'il en soit ainsi, mais il semble à l'expérience plus commode de majorer les discriminants

des sous-corps éventuels et de définir les corps imprimitifs par des polynômes à coefficients dans un sous-corps non trivial, dont on majore les coefficients en chacune des places à l'infini.

Nous allons donner dans la suite, en toute généralité, des inégalités permettant de résoudre les problèmes considérés. Nous utilisons la géométrie des nombres, en nous plaçant dans le cadre de la "méthode de Hunter" (cf. [Hu]); on pourrait utiliser la théorie des formes quadratiques - cf. [DyD 2] pour un exposé récent. Les inégalités en question sont écrites dans le paragraphe 2, précédé par le paragraphe 1 consacré à des rappels de géométrie des nombres, et suivi du paragraphe 3 consacré à des exemples.

On donne dans le paragraphe 4 un complément très utile au paragraphe 2, à savoir l'utilisation des méthodes analytiques par le biais des "corrections locales" : si l'on se contente des discriminants qui ne dépassent pas trop les minorations issues des méthodes analytiques, on peut diminuer considérablement le nombre de polynômes à examiner.

On examine dans le paragraphe 5 les techniques permettant à tout possesseur d'une calculatrice de poche programmable de traiter les questions inévitables liées à la classification des corps de discriminant donné : irréductibilité des polynômes, détection de sous-corps, tests d'isomorphisme,... En particulier, (a_2) présente un algorithme commode, et, semble-t-il, original.

On montre dans le paragraphe 6 comment les minorations de discriminants peuvent être utilisées dans l'identification des corps de nombres; on montrera en particulier que certains corps sont caractérisés par leur discriminant et leur signature sans avoir recours aux calculs un peu pénibles du paragraphe 5.

Enfin, le paragraphe 7 est une bibliographie commentée des diverses listes de corps dont j'ai eu connaissance.*

§ 1 - Rappels de géométrie des nombres.

Soit E un espace vectoriel euclidien de dimension n. Rappelons qu'un réseau de E est un sous-groupe discret de E qui engendre E en tant qu'espace vectoriel. Si R est un réseau de E, le déterminant d'une base $(e_1,\ldots,e_n)$ de R par rapport à une base orthonormée de même sens que E est un réel >0 qui ne dépend que du réseau, et que l'on appelle discriminant du réseau; notation : $\Delta(R)$. Son carré est le dé-

* Divers compléments ont été ajoutés en octobre 1984 après le §7.

terminant des produits scalaires $e_i \cdot e_j$. Soit U un ouvert de E contenant l'origine. La borne inférieure des discriminants des réseaux R permis pour U (i.e. tels que $U \cap R = \{0\}$) est un nombre réel > 0 (ou $+\infty$), appelé constante de réseau de U, que nous notons $c(U)$, et évidemment fini si U est borné. L'un des problèmes de la géométrie des nombres est la détermination de $c(U)$ pour certains ouverts U, ou tout au moins l'obtention de bonnes minorations de $c(U)$. On en déduit alors des inégalités utiles en écrivant que l'on a $\Delta(R) \geq c(U)$ pour tout réseau permis R.

On va s'intéresser en particulier au cas où U est une boule de centre 0 (ou l'intérieur d'un ellipsoïde, cela revient au même par linéarité). La détermination de la constante de réseau de la boule unité B_n d'un espace euclidien de dimension n, notée classiquement Γ_n, est l'un des problèmes majeurs de la géométrie des nombres. On peut traduire la définition de Γ_n dans le langage des formes quadratiques : une forme quadratique q sur l'espace euclidien E possède un discriminant $D(q)$ dans $\mathbb{R}$ (pas seulement dans $\mathbb{R}^{*2} \backslash \mathbb{R}$), à savoir le déterminant de la forme bilinéaire $(x,y) \longmapsto \frac{1}{2}[q(x+y) - q(x) - q(y)]$ sur une base orthonormée de E. On définit la constante d'Hermite γ_n comme la borne inférieure des réels positifs t vérifiant la propriété suivante : pour toute forme quadratique q définie positive sur $\mathbb{R}^n$ muni de sa structure euclidienne canonique, il existe un élément x non nul de $\mathbb{Z}^n$ qui satisfait à l'inégalité $q(x) \leq t\, D(q)^{1/n}$. L'existence de γ_n résulte de celle de Γ_n : pour des raisons d'homogénéité, on a $\gamma_n = \Gamma_n^{-2/n}$. On utilisera γ_n sous la forme suivante : c'est la borne inférieure des réels positifs t tels que tout réseau R de E possède un point $x \neq 0$ de norme $\leq t\,\Delta(R)^{2/n}$. Les constantes γ_n sont connues pour $n \leq 8$ (cf. [B1], ou [Ca], p. 332, ou [M-H], p. 29); la table suivante en donne les valeurs :

n	1	2	3	4	5	6	7	8
γ_n^n	1	$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	256

Les résultats sont dûs à Lagrange pour $n = 2$, à Gauss pour $n = 3$, à Korkine et Zolotareff pour $n = 4$ et 5, et à Blichfeldt pour $n = 6$, 7 et 8 (les 4 pages de [B1] sont quelque peu insuffisantes, mais les résultats ont été vérifiés, par G.L. Watson en particulier). En revanche, les

* cf. [B1'].

valeurs données par Chaundy ([Ch]) pour $n = 9$ et 10 n'ont pas été acceptées par la communauté mathématique, plusieurs témoignages concordants affirmant qu'il existe des "trous" dans l'étude de cas faite par Chaundy. Pour $n \geq 9$, on trouvera dans [Ca] et [M-H] diverses majorations de γ_n. Signalons simplement le résultat suivant, dû à Mordell (cf. [Ca], p. 269): on a, pour tout n, l'inégalité $\gamma_n^n \leq \gamma_{n-1}^{(n-1)n/(n-2)}$. On trouve en particulier $\gamma_9^9 \leq 2^{72/7}$ et $\gamma_{10}^{10} \leq 2^{90/7}$, majorations un peu moins bonnes que les valeurs conjecturales de γ_9^9 et de γ_{10}^{10} qui sont dans [Ch], à savoir 2^9 et $\frac{2^{10}}{3}$ respectivement.

Notons pour terminer ce paragraphe qu'il est souvent commode de considérer des réseaux relatifs, c'est-à-dire des réseaux d'un sous-espace de E. Dans ce cas, leurs discriminants sont définis à l'aide de la structure euclidienne induite.

§ 2 - Application aux corps de nombres.

Soit K un corps de nombres, ou plus généralement une $\mathbb{Q}$-algèbre étale, c'est-à-dire un produit fini d'extensions (séparables) de $\mathbb{Q}$, dont on note n le degré. Par extension des scalaires à $\mathbb{R}$, on obtient la $\mathbb{R}$-algèbre étale $\mathbb{R} \otimes_{\mathbb{Q}} K$, notée $\hat{K}$, qui est isomorphe à un produit $\mathbb{R}^r \times \mathbb{C}^s$; le couple (r,s) s'appelle la signature de K (ou de $\hat{K}$); on a $r + 2s = n$. Il y a n $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$, dont r ont une image réelle et $2s$ ont une image non réelle; autrement dit, K possède r places réelles et s places complexes, donc $(r+s)$ places à l'infini, dont l'ensemble est noté S.

L'identification de $\hat{K}$ à $\mathbb{R}^r \times \mathbb{C}^s$ n'est pas canonique : elle n'est définie qu'à composition près avec l'un des $r!s!2^s$ $\mathbb{R}$-automorphismes de $\hat{K}$. Ce qui est canonique, c'est l'identification de $\hat{K}$ à $\prod_{v \in S} \mathbb{R} e_v$, $(e_v)_{v \in S}$ désignant l'ensemble des idempotents irréductibles de $\hat{K}$. Néanmoins, on identifiera le plus souvent $\hat{K}$ à l'algèbre $A_{r,s} = \mathbb{R}^r \times \mathbb{C}^s$; les images dans $\mathbb{C}$ d'un élément $\theta \in K$ seront alors notées $\theta_1, \ldots, \theta_n$, en convenant que θ_k est réel pour $1 \leq k \leq r$, et que l'on a $\theta_{k+s} = \overline{\theta_k}$ pour $r + 1 \leq k \leq s$.

Il faut maintenant munir la $\mathbb{R}$-algèbre $A_{r,s}$ d'une structure euclidienne, c'est-à-dire d'une forme quadratique définie positive q_0. Dans la suite, sauf mention expresse du contraire, q_0 sera la forme qui prend sur $x = (x_1, \ldots, x_r, z_1, \ldots, z_s) \in A_{r,s}$ la valeur $x_1^2 + \ldots + x_r^2 + 2|z_1|^2 + \ldots + 2|z_s|^2$. On constatera que c'est ce choix qui

conduit aux formules les plus simples. C'est le choix fait par Hunter dans [Hu], et il est logique du point de vue des formes quadratiques : la forme naturelle $x \longmapsto Tr_{K/\mathbb{Q}}(x^2)$ a pour signature $(r+s,s)$, et l'on obtient q_0 en "rendant positive" la forme $x \longmapsto Tr_{K/\mathbb{Q}}(x^2)$; ce choix apparaît également chez Lenstra ([Ln]), qui identifie $\mathbb{C}$ à $\mathbb{R}^2$ par $a+bi \longmapsto (a+b,a-b)$.

La forme q_0 sur $A_{r,s}$ définie ci-dessus induit sur $\hat{K}$ une forme quadratique qui ne dépend pas de l'identification de $\hat{K}$ à $A_{r,s}$ et que l'on note encore q_0.

Soit M un réseau de $\mathbb{Z}$ dans K, c'est-à-dire un sous-$\mathbb{Z}$-module de K de rang n; M possède un discriminant, à savoir $d_K(M) = \det Tr_{K/\mathbb{Q}}(e_i e_j)$, où $\{e_1,\dots,e_n\}$ est une base arbitraire de M sur $\mathbb{Q}$. Pour la topologie usuelle de K identifié à $\mathbb{Q}^n$, M est discret, et s'identifie donc après complétion à un réseau de $\hat{K}$, que l'on note encore M. A ce réseau et à une structure euclidienne q sur $\hat{K}$ est associé un discriminant noté $\Delta_{K,q}(M)$, et simplement $\Delta_K(M)$ si $q = q_0$.

Proposition 2.1. $\Delta_K(M)^2 = (-1)^s d_K(M)$.

En effet, $\Delta_K(M)^2$ et $d_K(M)$ sont les discriminants de $M \subset \hat{K}$ pour les formes quadratiques $x \longmapsto q_0(x)$ et $q : x \longmapsto Tr_{\hat{K}/\mathbb{R}}(x^2)$; la décomposition de $A_{r,s}$ en somme directe $\mathbb{R}^r \oplus \mathbb{C}^s$ de $(r+s)$ corps est orthogonale pour q et pour q_0, qui coïncident sur les facteurs réels, et dont les matrices dans les bases $(1,i)$ des facteurs complexes sont respectivement $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ et $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$; le quotient des discriminants est donc $(-1)^s$, c.q.f.d.

Remarque 2.2. Le calcul de $\Delta_{K,q}(M)$ pour une structure euclidienne arbitraire q se déduit tout de suite de la Proposition 2.1 : on trouve la formule

$$\Delta_{K,q}(M) = D(q)\sqrt{|d_K(M)|}$$

Par exemple, pour $q(x) = x_1^2 + \dots + x_r^2 + |z_1|^2 + \dots + |z_s|^2$, on a $\Delta_{K,q}(M) = 2^{-s}\sqrt{|d_K(M)|}$. Le facteur inutile et usuel 2^{-s} réapparaît.

Nous allons maintenant examiner le cas où la $\mathbb{Q}$-algèbre K est munie d'une structure d'algèbre sur un corps de nombres K' de signature (r',s') et de degré $n' = r' + 2s'$. Comme K' est un corps, le degré

$m = [K : K']$ est défini. Pour chaque place à l'infini $v \in S(K')$, notons ρ_v (resp. σ_v) le nombre de places réelles (resp. complexes) de K au-dessus de v, et soit $m_v = \rho_v + \sigma_v$ le nombre de places de K au-dessus de v; on écrit ρ_i, σ_i, m_i lorsque l'on identifie $\hat{K}$ à $A_{r,s}$. On a $\rho_k + 2\sigma_k = m$ si $k \leq r'$ et $\rho_k = 0$, $m_k = \sigma_k = m$ si $k > r'$, d'où les relations $r = \sum_{k=1}^{r'} \rho_k$ et $s = \sum_{k=1}^{r'+s'} \sigma_k$, et bien sûr $n = mn'$. Etant donnés une structure euclidienne q sur $\hat{K}$ et un réseau relatif M de $\hat{K}$, on note $\Delta_{K,q}(M)$ le discriminant de M pour la restriction de q au sous-espace vectoriel $\mathbb{R}M$ de $\hat{K}$ engendré par M, et l'on écrit simplement $\Delta_K(M)$ si $q = q_0$. Il faut prendre garde au fait que les calculs faits pour une forme q définie en fonction de la signature de K peuvent conduire à des résultats différents dans K' pour la restriction de q et pour la forme analogue q'. La situation est particulièrement simple pour la forme q_0, la signature n'intervenant pas explicitement :

Proposition 2.3. Pour un réseau M de K', on a l'égalité

$$\Delta_K(M) = m^{n'/2} \, |d_{K'}(M)|^{1/2}.$$

En effet, la restriction de q_0 à $\hat{K}'$ est le produit par m de la forme analogue attachée à $\hat{K}'$, à cause des égalités $\rho_k + 2\sigma_k = m$ pour $k \leq r'$ et $\sigma_k = m$ pour $k > r'$; le déterminant qui définit $\Delta_{K'}(M)^2$ est donc multiplié par $m^{n'}$ lorsque l'on passe de K' à K.

Remarque 2.4. La forme $q : x \longmapsto \sum_{k=1}^{r} x_k^2 + \sum_{k=1}^{s} |z_k|^2$ a pour restriction à K' la forme $x \longmapsto \sum_{k=1}^{r'} m_k x_k^2 + m \sum_{k=1}^{s} |z_k|^2$, et l'on trouve la formule peu commode

$$\Delta_{K,q}(M) = \Big(\prod_{i=1}^{r'+s'} m_i \Big)^{1/2} 2^{-s'} \, |d_{K'}(M)|^{1/2}.$$

Nous allons maintenant voir comment, étant donnés K, K' et une forme quadratique définie positive q sur K, on peut donner une majoration de la valeur que prend q en un élément bien choisi de K qui n'est pas dans K'.

Lemme 2.5. Soient E un espace euclidien, F un sous-espace de E, $F^{\perp}$ son supplémentaire orthogonal, $(e_1, \ldots, e_p)$ une base orthogonale de F et pr la projection de E sur $F^{\perp}$ parallèlement à F. Alors, on a

l'identité $q\circ pr(x) = q(x) - \sum_{k=1}^{P} q(e_k)^{-1} b(x,e_k)^2$, b désignant le produit scalaire associé à q.

En effet, la forme quadratique $q' = q\circ pr$ de E est caractérisée par les égalités $q'(x) = q(x)$ si $x \in F^{\perp}$ et $q'(x) = 0$ si $x \in F$.

Théorème 2.6. Pour tout corps de nombres L, notons $\mathbb{Z}_L$ l'anneau des entiers de L. Soit q une forme quadratique définie positive sur K, soit q_1 la forme $q\circ pr$, pr désignant la projection orthogonale (pour q) de $\hat{K}$ sur $\hat{K}'$, et soit q' la restriction de q à K'. Il existe un élément $\theta \in \mathbb{Z}_K$, $\theta \notin K'$, vérifiant l'inégalité

$$q_1(\theta) \leq \gamma_{n-n'} \left(\Delta_{K,q}(\mathbb{Z}_K)/\Delta_{K',q'}(\mathbb{Z}_{K'})\right)^{2/(n-n')}$$

(γ_p est la constante d'Hermite pour la dimension p).

En effet, $\hat{K}'^{\perp}$ est un sous-espace de $\hat{K}$ de dimension $n-n'$; comme $\mathbb{Z}_{K'} = \hat{K}' \cap \mathbb{Z}_K$, toute projection parallèlement à $\hat{K}'$ sur un supplémentaire de $\hat{K}'$ transforme $\mathbb{Z}_K$ en un réseau de ce supplémentaire et applique $\mathbb{Z}_{K'}$ sur $\{0\}$. Lorsque l'on projette sur le supplémentaire orthogonal pour q, on voit tout de suite que le discriminant de $\mathbb{Z}_K$ pour q est le produit des discriminants des projections pour les restricitons de q, c.q.f.d.

Nous allons maintenant pousser les calculs dans le cas de la forme q_0. L'évaluation du nombre de droite est immédiate par la Proposition 2.3. Pour évaluer $q_1(\theta)$, nous appliquons le Lemme 2.5, en utilisant les idempotents irréductibles de $\hat{K}'$. Auparavant, nous devons introduire les n' "fonctions trace" associées à la structure de K'-algèbre de K. Soit J(K') l'ensemble des $\mathbb{Q}$-isomorphismes de K' dans $\mathbb{C}$. Pour $\sigma \in J(K')$, soit $J_\sigma(K)$ l'ensemble des $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$ qui ont σ pour restriction à K'.

Définition 2.7. Avec les notations ci-dessus, pour tout $\sigma \in J(K')$, on appelle σ-trace d'un élément $\theta \in K$ la somme $\sum_{t \in J_\sigma(K)} t\theta$.

Notation : $Tr_{\sigma,K/K'}(\theta)$, ou $Tr_\sigma(\theta)$, ou $Tr_k(\theta)$ si l'on indexe J(K') par $\{1,\ldots,r', r'+1,\ldots,r'+s', r'+s'+1,\ldots,n'\}$.

Les σ-traces sont des éléments de K', de somme la trace $Tr_{K/\mathbb{Q}}$.

Soient $(e'_v)_{v\in S}$ (ou e'_k, $1 \leq k \leq r'+s'$ si l'on identifie $\hat{K}'$ à $A_{r',s'}$) les idempotents irréductibles de $\hat{K}'$. Ils sont deux-à-deux or-

thogonaux pour la forme q_0 définie sur $\hat{K}'$, donc aussi pour la forme q_0 définie sur $\hat{K}$; pour cette dernière forme, on a $q_0(e'_k) = m$ si $k \leq r'$, et $q_0(e'_k) = 2m$ si $r'+1 \leq k \leq s'$. On complète cette famille en une base orthogonale de $\hat{K}'$, en posant $e'_k = ie'_{k-s'}$ $(i^2=-1)$ pour $r'+s'+1 \leq k \leq n'$; on a encore $q_0(e'_k) = 2m$ pour $k > r'+s'$.

Pour $1 \leq k \leq r'$, $b(x,e_k) = \mathrm{Tr}_k(x)$. Pour $r' < k \leq r'+s'$, on a $\frac{1}{2}\, b(x,e_k)^2 + \frac{1}{2}\, b(x,e_{k+s'})^2 = \frac{1}{2}\,|\mathrm{Tr}_k(x)|^2 + \frac{1}{2}\,|\mathrm{Tr}_k(x)|^2$. En reportant dans la formule du Théorème 2.6, on arrive à l'énoncé suivant :

Théorème 2.8. Soit K un corps de nombres de degré n, extension de degré m d'un sous-corps K' de degré n'. Il existe un élément entier θ de K, qui n'appartient pas à K', et qui vérifie l'inégalité suivante (cf. 2.7 pour la définition de $\mathrm{Tr}_{\sigma,K/K'}$) :

$$\sum_{i=1}^{n} |\theta_i|^2 \leq \frac{1}{m} \sum_{\sigma \in J(K')} |\mathrm{Tr}_{\sigma,K/K'}(\theta)|^2 + \gamma_{n-n'}\, |d_K/m^{n'} d_{K'}|^{1/(n-n')}.$$

En outre, cette inégalité est vérifiée par tout élément de K différent de θ par un élément de K'.

Corollaire 2.9 (Hunter). Tout corps de nombres K de degré n contient un entier θ irrationnel vérifiant l'inégalité

$$\sum_{i=1}^{n} |\theta_i|^2 \leq \frac{1}{n}\, (\mathrm{Tr}_{K/\mathbb{Q}}(\theta))^2 + \gamma_{n-1}\, |d_K/n|^{1/(n-1)}.$$

On peut écrire sous une forme un peu différente l'inégalité du Théorème 2.8, en utilisant l'identité suivante qui s'applique à tout espace affine quadratique $(E, \vec{E}, q)$: étant donnés $(m+1)$ points $0, M_1, \ldots, M_m$ de E, on a l'identité :

$$\sum_{i<j} q(\overrightarrow{M_i M_j}) = m \sum_i q(\vec{0M_i}) - q\Big(\sum_i \vec{0M_i}\Big),$$

qui se démontre en développant $\sum_{i<j} q(\vec{0M_j} - \vec{0M_i})$. En appliquant cette identité à la forme q_0 de $\hat{K}$ et aux $(m+1)$ points $0, \theta_{i_1}, \ldots, \theta_{i_m}$, les m indices décrivant les $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$ prolongeant un même $\mathbb{Q}$-isomorphisme de K' dans $\mathbb{C}$, et en sommant sur $J(K')$, on obtient l'énoncé suivant :

Corollaire 2.10. Sous les hypothèses du Théorème 2.8, il existe un élément $\theta \in \mathbb{Z}_K$, $\theta \notin K'$, vérifiant l'inégalité :

$$\sum_{i=1}^{n'} \sum_{k<\ell} |\theta_\ell - \theta_k|^2 \leq m\gamma_{n-n'} \, |d_K/m^{n'} d_{K'}|^{1/(n-n')} ,$$

les indices k et ℓ de la somme intérieure désignant des conjugués de θ relatifs aux $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$ prolongeant successivement chacun des n' $\mathbb{Q}$-isomorphismes de K' dans $\mathbb{C}$. Dans le cas particulier où $K' = \mathbb{Q}$, cette inégalité s'écrit simplement

2.10 bis. $$\sum_{1\leq k<\ell\leq n} |\theta_\ell - \theta_k|^2 \leq n \, \gamma_{n-1} \, |d_K/n|^{1/(n-1)}.$$

Montrons rapidement comment les inégalités des énoncés 2.8, 2.9 et 2.10 permettent de chercher les corps K de signature (r,s) donnée et de discriminant d_K majoré en valeur absolue par une borne M donnée. Tout d'abord, on regarde pour les différents diviseurs $n' > 1$ de n la possibilité qu'un élément θ du Théorème 2.8 soit dans un sous-corps de K de degré n'. L'inégalité 2.10 bis montre que l'on doit avoir

2.11. $$\sum_{1\leq k<\ell\leq n'} |\theta_\ell - \theta_k|^2 \leq (n'/m) \, \gamma_{n-1} \, |d_K/n|^{1/(n-1)} \quad (mn' = n).$$

Par l'inégalité entre moyennes arithmétique et géométrique, on majore le discriminant $d_{K'}(\theta)$ de θ dans K' (i.e. de son polynôme caractéristique dans K'), et donc aussi $|d_{K'}|$. On a alors l'inégalité :

2.12. $$|d_{K'}| \leq [2 \, \gamma_{n-1} |d_K/n|^{1/(n-1)}/m(n'-1)]^{n'(n'-1)/2}.$$

Cette inégalité limite considérablement le nombre de sous-corps de K qu'il est indispensable de considérer. On se ramène à l'aide de plusieurs applications de ce procédé à étudier les éléments $\theta \in K$ qui engendrent K sur un sous-corps donné K'.

On utilise alors le Théorème 2.8. Tout d'abord, par translation par un élément de K', on ramène $\mathrm{Tr}_\sigma(\theta)$ à parcourir un système de représentants de $\mathbb{Z}_{K'}$ modulo $m\mathbb{Z}_{K'}$; on peut donc se limiter à $m^{n'}$ valeurs pour $\mathrm{Tr}_\sigma(\theta)$, et l'on peut du reste diminuer ce nombre en multipliant θ par une racine de l'unité de K' (si $K' = \mathbb{Q}$, on peut supposer que l'on a $0 \leq \mathrm{Tr}_{K/\mathbb{Q}}(\theta) \leq n/2$). Ensuite, on utilise la majoration de la somme $\sum_{i=1}^{n} |\theta_i|^2$: pour K' donné, on a une majoration en $O(M^{1/2(n-n')})$ de chacune des racines. Si l'on note $f(X) = X^m - a_1 X^{m-1} + a_2 X^{m-2} + \ldots + (-1)^m a_m$ le polynôme caractéristique de

θ dans K/K', on voit que l'on a une majoration de la borne supérieure des valeurs absolues des a_k $(k \geq 2)$ en $O(M^{k/2(n-n')})$ (utiliser les fonctions symétriques des racines).

Bien entendu, on a perdu beaucoup d'information en majorant $\mathrm{Sup}|\theta_i|^2$ par $\Sigma|\theta_i|^2$. Si l'on est amené à calculer une approximation des racines (par exemple, pour tester des isomorphismes entre corps), alors on peut éliminer les polynômes pour lesquels la somme $\Sigma|\theta_i|^2$ est trop grande. Mais, quel que soit la méthode que l'on emploie, il est vraisemblable que la majoration en $O(M^{k/2(n-1)})$ pour le coefficient a_k du polynôme caractéristique d'un élément irrationnel de K est ce que les méthodes géométriques peuvent donner de mieux. Toutefois, la question suivante est sans doute intéressante : peut-on améliorer la majoration du coefficient a_k lorsque l'on s'est donné les coefficients $a_1,\ldots,a_{k-1}$? Il en est ainsi lorsque $K' = \mathbb{Q}$, et que l'on utilise la signature des corps que l'on cherche (en écrivant que l'on a $f(a) > 0$ pour tout a si $r = 0$, ou que les dérivées de f ont le nombre maximum de racines si $s = 0,\ldots$).

Remarque 2.13. Les autres formes quadratiques (par exemple, la forme $q(x) = \sum_{i=1}^{r} x_i^2 + \sum_{i=1}^{s} |z_i|^2$) sont d'un maniement moins commode que la forme q_0, et, en particulier, ne permettent pas de majorer efficacement les discriminants des sous-corps éventuels que l'on doit considérer. Pour être complet, nous donnons le résultat analogue à celui du Corollaire 2.9 pour la forme q (cf. [Go1]; on pose $\theta_k = \phi_k + i\psi_k$ pour $1 \leq k \leq r+s$) :

Tout corps de nombre contient un entier irrationnel θ vérifiant l'inégalité

$$\sum_{1 \leq k < \ell \leq r+s} (\phi_\ell - \phi_k)^2 + (r+s) \sum_{k=1}^{s} \psi_k^2 \leq (r+s)^{(n-2)/(n-1)} 2^{-2s/(n-1)} \gamma_{n-1} |d_K|^{1/(n-1)}.$$

Remarque 2.14. L'inégalité du Corollaire 2.10 donne une majoration de la norme du discriminant relatif $d_{K/K'}(\theta)$ par l'utilisation de l'inégalité entre moyennes arithmétique et géométrique ; en effet, avec les notations du Corollaire 2.10, on a :

$$N_{K'/\mathbb{Q}}(d_{K/K'}(\theta)) = \prod_{i=1}^{n'} \prod_{k<\ell} |\theta_\ell - \theta_k|^2$$

$$\leq \left(\frac{\Sigma|\theta_\ell - \theta_k|^2}{n'm(m-1)/2} \right)^{n'm(m-1)/2}$$

Cette inégalité, très utile pour les petits degrés, est d'un intérêt moindre pour les degrés assez grands, mais permet néanmoins d'éliminer des polynômes lorsque l'on construit des tables. Dans le cas où $K' = \mathbb{Q}$, on obtient l'inégalité

$$|d_K(\theta)| \leq \left(\frac{2\gamma_{n-1}^{n-1}\,|d_K|}{n(n-1)}\right)^{n/2}$$ qui majore le facteur inessentiel de $d_K(\theta)$ en $O(|d_K|^{n/4})$.

Bien entendu, si l'on calcule les racines, la comparaison de la somme $\Sigma|\theta_k|^2$ aux discriminants a priori possibles est une source bien plus importante d'élimination de polynômes; du reste, un calcul partiel des racines (par exemple, le calcul des racines réelles lorsque r n'est pas trop petit) permet des estimations utiles de la somme $\Sigma|\theta_i|^2$; cette idée apparaît dans [Po3]. Enfin, on trouvera dans les articles de Hunter, Godwin et Pohst cités dans la bibliographie diverses propriétés des coefficients des polynômes de $\mathbb{R}[X]$ ayant une signature donnée qui sont d'une très grande utilité.

Terminons ce paragraphe par une dernière remarque : le choix de la forme q_0, s'il semble conduire aux formules les plus simples, n'est peut-être pas le meilleur pour toutes les signatures; Godwin ([Go2]; voir aussi [An 1]) suggère de remplacer q_0 par des formes quadratiques du type $\sum_{i=1}^{r} |x_i|^2 + \sigma \sum_{j=1}^{s} |z_i|^2$ où σ est un réel >0 à choisir en fonction de la signature.

§ 3 - Exemples.

Nous allons examiner d'abord quelques exemples d'extensions cubiques. Auparavant, il est bon de revenir sur la discussion qui suit le corollaire 2.10; lorsque l'on majore le discriminant des sous-corps à considérer, il est sous-entendu qu'un corps imprimitif contenant un sous-corps de même degré mais de discriminant plus grand contient de toute façon un élément θ vérifiant le Théorème 2.8 et n'appartenant pas à ce sous-corps. Si l'on désire cependant classer les extensions contenant un sous-corps de degré n' et de discriminant $\leq M$, on doit considérer tous les sous-corps K' vérifiant l'inégalité $|d_{K'}| \leq M^{1/m}$, inégalité a priori moins bonne que l'inégalité 2.12.

Voyons ce qui se passe pour le degré 6. Donnons-nous $M > 0$. En combinant les inégalités qui figurent dans 2.9 et 2.14, on obtient le ré-

sultat suivant : soit K un corps de degré 6, de discriminant d_K, vérifiant l'inégalité $|d_K| \leq M$; il existe alors dans K un élément θ vérifiant l'une des conditions suivantes :

(i) $K = \mathbb{Q}(\theta)$ et $\sum_{i=1}^{6} |\theta_i|^2 \leq \frac{1}{6} \mathrm{Tr}_{K/\mathbb{Q}}(\theta)^2 + (4M/3)^{1/5}$

(ii) θ appartient à un corps cubique K_3 dont le discriminant vérifie l'inégalité $|d_{K_3}| \leq (M/24)^{3/5}$

(iii) θ appartient à un corps quadratique K_2 dont le discriminant vérifie l'inégalité $|d_{K_2}| \leq (128M/729)^{1/5}$.

Si l'on désire construire la liste des corps K imprimitifs avec $|d_K| \leq M$, on doit se contenter des inégalités $|d_{K_3}| \leq M^{1/2}$ et $|d_{K_2}| \leq M^{1/3}$ (on peut montrer que l'on a en fait $|d_{K_3}| \leq (M/3)^{1/2}$).

D'après [B-R], il y a deux discriminants de corps primitifs jusqu'à $-22\,000$ dans le cas $n = 6$, $r = 0$ ($-14\,731$ et $-20\,627$, premiers). Si l'on désire pour $n = 6$ et $r = 0$ les corps imprimitifs jusqu'à $-22\,000$, il suffit d'examiner les corps K_3 avec $|d_{K_3}| \leq 59$ (5 corps; $d_{K_3} = -23$, -31, -44, -59 ou $+49$) et les corps K_2 avec $|d_{K_2}| \leq 5$ (3 corps, avec $d_{K_2} = -3$, -4 ou $+5$, mais l'hypothèse $r = 0$ élimine $+5$), cela si l'on admet que les corps imprimitifs sont effectivement signalés par [B-R]. Sinon, on doit utiliser les inégalités $|d_{K_3}| \leq 85$ et $0 < -d_{K_2} < 28$. En utilisant la théorie du corps de classes, on traite facilement les extensions d'un corps cubique; les discriminants qui apparaissent sont $-81^2.3$, $-49^2.7$, $-44^2.11$, $-31^2.11$, $-23^2.19$, $-23^2.23$, $-23^2.27$, $-23^2.35$ (les normes des discriminants relatifs sont congrues à 0 ou -1 mod 4). On traite de même assez facilement les extensions d'un corps quadratique K_2 avec d_{K_2} assez grand. En fait, si l'on écrit le discriminant relatif sous la forme $\delta\phi^2$, δ correspondant à une extension quadratique de K_2, la norme N de δ est congrue à 0 ou 1 mod 4. Pour le cas $N = 1$, on trouve des extensions cycliques, dont les discriminants sont -23^3, $-11^3.2^4$, $-7^3.7^2$ et $-3^3.3^6$, déja rencontrés, et $-4^3.13^2$ et $-3^3.19^2$, nouveaux. On arrive à se débarasser par des arguments algébriques des possibilités $N = 4$, 5, 8, 9, 12, 13 et 16, et on est ramené au cas où $d_{K_2} = -3$ ou -4. Faute de tables assez étendues en degré 4, on doit utiliser les résultats du paragraphe 2. Tenant compte des racines de l'unité, on est amené à considérer les polynômes $f(X) = X^3 - aX^2 + bX - c$,

avec $a,b,c \in \mathbb{Z}_{K_2}[X]$, $a \in \{0,1,1+i,j-j^2\}$ $(i^2=-1,\ j^3=1,\ j\neq 1)$, $f \notin \mathbb{Z}[X]$ et f sans racine dans K_2. Posons $d = -d_{K_2}$ $(d=+3$ ou $+4)$. Le Théorème 2.8 donne alors l'inégalité suivante pour les racines x_1, x_2, x_3 de f : $2(|x_1|^2+|x_2|^2+|x_3|^2) \leq (4M/9d)^{1/4} + \frac{2}{3}|a|^2$. On peut ensuite majorer $|c|^2$ par l'inégalité entre moyennes et $|b|$ par l'égalité $-2b = \Sigma x_i^2 - a^2$, d'où $2|b| \leq |a|^2+|x_1|^2+|x_2|^2+|x_3|^2$, et $|b| \leq \frac{1}{4}(4M/9d)^{1/4} + \frac{2}{3}|a|^2$. Voici ce que l'on trouve pour $|b|^2$ et $|c|^2$ en fonction de $(d,|a|^2)$:

(d, a^2)	(4,0)	(4,1)	(4,2)	(3,0)	(3,1)	(3,3)
$\lvert c\rvert^2 <$	1,61	2,12	2,71	2,00	2,58	4,04
$\lvert b\rvert^2 <$	3,09	5,88	9,56	3,57	6,54	15,13

(on a $|c|^2 \leq [\frac{1}{6}(4M/9d)^{1/4} + \frac{1}{9}|a|^2]^3$).

Les inégalités que l'on obtient pour la norme de b ne sont pas excellentes, et recenser les polynômes est une tâche un peu ardue pour une machine de poche, mais facile pour un micro-ordinateur. On peut néanmoins raccourcir la liste des polynômes en utilisant les "corrections locales" (cf. paragraphe 5) : on montre en effet qu'il n'y a pas d'idéal de norme 2 dans K pour $|d_K| \leq 24050$; on peut donc supposer que l'on a $f(0) \equiv f(1) \equiv 1 \bmod (1+i)$ si $d=4$, d'où $|c|=1$, et $a+b \equiv 1 \bmod (1+i)$. On peut de même montrer que l'on ne peut avoir en même temps un idéal premier de norme 3 et un idéal premier de norme 4 pour $|d_K| \leq 28534$. On arrive alors à vérifier qu'il y a 15 corps de discriminants $\geq -22\,000$, et que ces corps sont caractérisés par leur discriminant (on utilise les méthodes du paragraphe 5 pour les corps imprimitifs, et on vérifie directement (cf. paragraphe 4) que les deux corps de discriminant $-20\,627$ donnés dans [B-R] définissent le même corps). Voici les 15 discriminants : $-9\,747$, $-10\,051$, $-10\,571$, $-10\,816$, $-11\,691$, $-12\,167$, $-14\,283$, $-14\,731$, $-16\,551$, $-16\,807$, $-18\,515$, $-19\,683$, $-20\,627$, $-21\,168$ et $-21\,296$; douze de ces corps sont définis par un polynôme dans [Ln], table 5; les trois autres corps sont les corps cyclotomiques de discriminants $-7^5 = -16\,807$ et $-3^9 = -19\,683$, et le corps primitif de discriminant $-20\,687$, défini par le polynôme $X^6+X^5+X^4+2X^3+2X^2+X+1$. On vérifie du reste que les majorations de $|b|$ et de $|c|$, comme les corrections locales utilisées, s'appliquent jusqu'au discriminant $24\,050$;

on en déduit que les corps imprimitifs K vérifiant l'inégalité $-24\,050 \leq d_K \leq -22\,000$ sont les quatre extensions de corps quadratiques de discriminants $-22\,592 = -2^6.363$, $-22\,707 = -3^3.29^2$, $-23\,031 = -3^3.843$ et $-24\,003 = -3^3.7.127$, définies respectivement par les polynômes $X^3 - X^2 + (1+i)X - i$, $X^3 - (j-j^2)X^2 + jX - j^2$, $X^3 - X - j$ et $X^3 - X^2 - X - j$, et l'extension de corps cubique, de discriminant $-22\,747 = -23^2.43$.

Les calculs ci-dessus montrent que tous les corps que l'on trouve comme extension d'un corps quadratique peuvent être obtenus avec un coefficient b tel que $|b|^2 = 0,1,2$ ou 3. Cela indique que les majorations utilisées sont loin d'être optimales, et soulève la question suivante : étant donné un polynôme $X^n - a_1X^{n-1} + a_2X^{n-2} + \ldots + (-1)^n a_n$, de racines $\theta_1,\ldots,\theta_n$, peut-on majorer les coefficients a_k pour $2 \leq k \leq n$ en fonction de $a_1,\ldots,a_{k-1}$ et $M = \Sigma\,|\theta_i|^2$, de façon à obtenir des résultats meilleurs que ceux donnés par une majoration brutale utilisant les fonctions symétriques des racines, à savoir $|a_k| \leq \binom{n}{k} M^{k/2}$? On parvient effectivement à démontrer de telles majorations en utilisant les places réelles de K' lorsqu'il y en a; le cas où K' est totalement imaginaire est, de ce point de vue, le plus difficile à étudier.

Il serait intéressant d'étudier certaines extensions relatives sur le modèle des extensions cubiques des corps quadratiques imaginaires, et notamment les extensions de degré 4 des corps quadratiques, dont l'étude est indispensable pour la recherche des petits discriminants en degré 8.

En outre, de telles études permettent de résoudre des problèmes de nombres de classes.

Considérons par exemple les corps K de degré 4, de nombre de classes multiple de 3, et contenant un corps quadratique imaginaire K_2. Si K_2 lui-même a un nombre de classes divisible par 3, on vérifie que le corps K de discriminant minimum est $\mathbb{Q}(\sqrt{\frac{-3+\sqrt{-23}}{2}})$, de discriminant $2^3.23^2 = 4\,232$. Sinon, K/K_2 possède une classe relative d'ordre 3, ce qui entraîne l'existence d'une extension cubique de K_2 ayant même discriminant relatif que K/K_2. L'étude qui précède montre que, si $d_K < 4\,232$, alors : ou bien $K_2 = \mathbb{Q}(\sqrt{-3})$, K est isomorphe à $\mathbb{Q}(\sqrt{\frac{35+13\sqrt{-3}}{2}})$, l'extension cubique correspondante étant définie par le polynôme $X^3 - X^2 + X + j$, ou bien $d_{K_2} \leq -7$. Une étude un peu plus précise montrerait sans doute que les discriminants $3\,897$ et $4\,232$ sont

les deux plus petits parmi les extensions quadratiques de corps quadratiques imaginaires de nombre de classes divisibles par 3.

Il n'y a pas de raison de se limiter aux cas totalement imaginaires: aux extensions quadratiques d'un corps quadratique réel correspondent, selon que r vaut 0, 2 ou 4, des corps de degré 6 avec 2, 4 ou 6 places réelles. Compte-tenu des tables de [Ln], [L-M] et [B-R], il est probable que les discriminants minimaux respectifs pour le nombre de classes divisible par 3 sont $30\,125 = 5^3.241$, $-104\,875 = -5^3.839$, et $485\,125 = +5^3.3\,881$, correspondant respectivement aux corps $\mathbb{Q}(\sqrt{-31+12\sqrt{5}})$, $\mathbb{Q}(\sqrt{21+16\sqrt{5}})$ et $\mathbb{Q}(\sqrt{109+40\sqrt{5}})$, les extensions cubiques respectives étant définies par les polynômes $X^3 - \theta X^2 + X + (1-\theta)$, $X^3 - X^2 - X - \theta$ et $X^3 + X^2 + (\theta-3)X + (\theta-2)$, avec $\theta = (1+\sqrt{5})/2$

Il serait de même intéressant de savoir si le discriminant minimum d'une extension quadratique d'un corps cubique de discriminant < 0, dont le nombre de classes est divisible par 3, est atteint par le corps $\mathbb{Q}(\sqrt{-18-\alpha+6\alpha^2})$ avec $\alpha^3 - \alpha - 1 = 0$, dont le discriminant est $-1\,400\,263 = -23^2.2\,647$, le corps de degré 9 correspondant étant défini par le polynôme $X^3 - \alpha^3X^2 + \alpha^2X - 1$ (trouvé par Leutbecher, qui montre que le corps est euclidien), ou encore si le plus petit discriminant d'un corps de degré 4, de nombre de classes divisible par 5, et contenant un corps quadratique imaginaire, est bien $12\,176 = 2^6.761$, correspondant au corps $\mathbb{Q}(\sqrt{19+20i})$, trouvé par les méthodes de Mestre ([Me], appendice, N = 11).

§ 4 - Utilisation des méthodes analytiques.

Les travaux de Stark, Odlyzko, Poitou et Serre, faisant appel à des méthodes analytiques, ont conduit à des progrès décisifs dans les minorations des discriminants pour une signature donnée, mais n'ont pas fait progresser de façon comparable la construction de tables des corps ayant une signature donnée. Toutefois, si l'on se contente de rechercher les discriminants proches du minimum escompté, on peut utiliser les méthodes analytiques pour raccourcir la recherche des corps.

En effet, les "formules explicites" (cf. [Poi]) tiennent compte de la décomposition de toutes les places de $\mathbb{Q}$, contrairement aux inégalités de la géométrie des nombres dans lesquelles seul le comportement de la place à l'infini de $\mathbb{Q}$ est pris en compte. De façon précise, pour un corps K de degré n, de signature (r,s) et de discriminant de valeur

absolue d, on obtient des inégalités de la forme :

$$\log d \geq An + Br + C + Dn^{-1} + 2 \sum_{\mathfrak{P},m} \frac{\log N\mathfrak{P}}{(N\mathfrak{P})^{m/2}} F(m \log N\mathfrak{P}),$$

où F est une fonction réelle positive convenable, $\mathfrak{P}$ parcourt l'ensemble des idéaux premiers de K, m parcourt l'ensemble des entiers >0, N désigne la norme, et A, B, C, D sont des réels dépendant de F. La somme sur $\mathfrak{P}$ et m (dite : "correction locale") joue un rôle important lorsque K possède des idéaux premiers de petites normes (la correction locale n'est intéressante que pour les petites normes, les fonctions F devant être rapidement décroissantes à l'infini).

En conséquence, si l'on recherche des discriminants assez petits à l'aide des méthodes du paragraphe 2, on empêche la présence d'idéaux de petites normes, et l'on empêche ainsi certaines décompositions dans $\mathbb{F}_p$ des polynômes que l'on trouve pour les petites valeurs de p. Le nombre de polynômes à considérer est de ce fait réduit, souvent dans des proportions considérables (et en outre, l'étude de l'irréductibilité est elle aussi simplifiée). Cette remarque a été utilisée au paragraphe 3, les corrections locales ayant été calculées à l'aide des tables d'Oklyzko ([Odl], table IV; on obtiendrait des inégalités un tout petit peu meilleures à l'aide des fonctions utilisées par Poitou et Diaz y Diaz).

Le fait qu'il n'y ait pas d'idéal premier de norme $<p^m$ au-dessus d'un nombre premier p donné entraîne, si $m>1$, que les valeurs prises en un entier k par un polynôme f définissant un entier θ de K sont premières à p, ou bien que, en posant $f(X+h)=X^n+a_1X^{n-1}+\ldots+a_{n-1}X+a_n$, on ait $p^{n-i} | a_{n-i}$ pour $0 \leq i < n$. Cette remarque, combinée avec une majoration de la somme $\sum_{i=1}^{n} |\theta_i|^2$ (notations des paragraphes 2 et 3) et avec l'inégalité entre moyennes, suffit à prouver dans certains cas que le terme constant de f est égal à +1 ou à -1 : c'est ce qui se passe pour $n=7$ dans [DyD 3] et [DyD 4], pour les intervalles dans lesquels les discriminants prennent leurs valeurs. On peut améliorer la remarque par une étude locale, et, en particulier, mettre en jeu les résultants de f et des polynômes irréductibles g de degré $i<m$, la valeur de f en h étant le cas particulier où $i=1$ et $g(X)=X-h$.

§ 5 - Tests d'isomorphisme et d'irréductibilité, et détection des sous-corps.

On considère dans ce paragraphe des corps de signature (r,s) donnée et de degré $n = r+2s$.

Lorsque l'on recherche les corps ayant un discriminant de valeur absolue d majorée par un réel M donné au moyen des méthodes du paragraphe 2, on se trouve en présence d'une longue liste de polynômes. On calcule leur discriminant, et l'on dispose pour cela de divers procédés. Le plus rapide est sans doute le calcul du résultant du polynôme et de sa dérivée, mais on rencontre parfois des phénomènes d'instabilité. On peut calculer les discriminants en entiers par un déterminant, ou encore, si l'on a en définitive besoin d'une approximation des racines $\theta_1,\dots,\theta_n$ des polynômes, on peut utiliser la formule $d_f = \pi f'(\theta_i)$ qui donne le discriminant du polynôme f. Si l'on effectue un calcul de racines dans $\mathbb{C}$, on peut en profiter pour éliminer les polynômes pour lesquels $\Sigma|\theta_i|^2$ est trop grand. Quel que soit le procédé employé pour calculer le discriminant, on peut éliminer les polynômes de discriminant trop grand en utilisant la remarque 2.14. Il faut ensuite, pour chaque polynôme f, calculer le discriminant d_K de l'algèbre $K = \mathbb{Q}[X]/(f)$, i.e. chercher l'entier $a > 0$ tel que $d_K = a^2 d_f$. Cela se fait classiquement en cherchant une base d'entiers de $K/\mathbb{Q}$, et en essayant les diviseurs carrés possibles de d_f (noter que d_K est de la forme $a^2\, d_{K_2}$, K_2 désignant le corps quadratique associé à K par la signature d'une permutation; éventuellement, $K_2 = \mathbb{Q}$). On élimine les cas où $|d_K|$ est inférieur aux minorations connues des discriminants, K ne pouvant pas alors être un corps. Il reste alors à tester l'irréductibilité des polynômes conservés, et à voir si deux discriminants égaux correspondent au même corps à isomorphisme près.

a) Isomorphismes. On se donne deux polynômes f et g de discriminants non nuls, et l'on cherche si les algèbres $K = \mathbb{Q}[X]/(f)$ et $L = \mathbb{Q}[X]/(g)$ sont isomorphes. Nous allons donner deux algorithmes, dont le point de départ est le même. On commence par choisir un complété $\mathbb{Q}_v$ de $\mathbb{Q}$, et l'on suppose que les algèbres complétées K_v et L_v sont isomorphes. On va chercher si, parmi les $\mathbb{Q}_v$-isomorphismes de K_v sur L_v (en nombre égal à l'ordre du groupe d'automorphismes de $K_v/\mathbb{Q}_v$), il y en a un qui est rationnel sur $\mathbb{Q}$ (i.e. provient d'un $\mathbb{Q}$-isomorphisme de K sur L par extension des scalaires). Pour cela, on calcule dans

une extension finie $\mathbb{Q}_v'$ convenable de $\mathbb{Q}_v$ des approximations des racines $\theta_1,\ldots,\theta_n$ et $\theta_1',\ldots,\theta_n'$ de f et de g respectivement, avec une précision à déterminer, dépendant de l'algorithme (si $\mathbb{Q}_v = \mathbb{R}$, on prend $\mathbb{Q}_v' = \mathbb{C}$; si v est p-adique, il est commode de prendre p non ramifié dans $K[X]/(f)$: p est une uniformisante, et on calcule pratiquement dans un corps fini). S'il existe un $\mathbb{Q}$-isomorphisme σ de K sur L, alors, pour une permutation de $\theta_1',\ldots,\theta_n'$ respectant la structure de $\mathbb{Q}_v$-algèbre de L_v, la somme $S = \sum_{i=1}^{n} \theta_i\theta_i'$ est un entier de l'intervalle $[-S',+S']$ où $S' = \sum_{i=1}^{n} |\theta_i\theta_i'|_\infty$ se majore par Cauchy-Schwartz : $S' \leq (\Sigma|\theta_i|_\infty^2)^{1/2}\,(\Sigma|\theta_i'|_\infty^2)^{1/2}$. Si la permutation choisie convient, alors S est entier aux erreurs de calculs près, et l'on remarque en outre, pour v finie, que cet entier est dans $[-S',+S']$. L'expérience prouve qu'il reste peu de choix possibles pour une permutation (en général, 0 ou 1 si L n'a pas d'automorphismes non triviaux). Maintenant, il faut donner un test de rationalité pour une permutation qui n'est pas rejetée. Le principe consiste à trouver un entier ϕ de $\mathbb{Q}[X]/(f)$ dont les fonctions symétriques sont très voisines de celles de θ' (l'image de X dans $\mathbb{Q}[X]/(g)$). Alors, comme ces fonctions symétriques sont des entiers, elles coïncident, et les algèbres sont isomorphes.

a_1) On cherche ϕ sous la forme $x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}$, $x_i \in \mathbb{Q}$, θ désignant l'image de X dans K. Si ϕ est entier les x_i sont dans $\frac{1}{a}\mathbb{Z}$, a désignant l'entier >0 tel que $d_f = a^2 d_K$. On calcule une valeur approchée de la solution $(x_0,\ldots,x_{n-1})$ du système linéaire $\sum_{j=0}^{n-1} x_j\theta_i^j = \theta_i'$ $(1 \leq i \leq n)$. Ecrivons la solutions sous la forme $x_i = m_i + \varepsilon_i$ avec $m_i \in \frac{1}{a}\mathbb{Z}$ et $\varepsilon_i \in]-\frac{1}{2a},\frac{1}{2a}]$, et posons $\psi = m_0 + m_1\theta + \ldots + m_{n-1}\theta^{n-1}$. Alors ϕ et ψ ont des fonctions symétriques à valeurs dans $\frac{1}{a}\mathbb{Z}$, qui sont proches, donc coïncident si les ε_i sont assez petits. On a alors les égalités $\sum_{j=0}^{n-1} m_j\theta_i^j = \theta_i'$, et σ est un isomorphisme.

Ce procédé, qui ne nécessite qu'une approximation médiocre des racines de f et de g, fournit une transformation de Tschirnhausen de θ à θ' explicitement, mais nécessite la résolution d'un système linéaire (que l'on peut du reste prendre à coefficients entiers : considérer le système $\sum_{j=0}^{n-1} x_j\,\mathrm{Tr}\,(\theta^{j+k}) = s_k$ pour $k = 0,1,\ldots,n-1$, dans lequel on a posé $s_k = \sum_{i=1}^{n} \theta_i^k\varepsilon_i'$; les s_k doivent être entiers aux erreurs d'arrondis près, et on utilise l'entier le plus proche pour déterminer les x_i).

a_2) On cherche à montrer l'existence d'un $\phi \in K$ comme ci-dessus, mais sans le déterminer. Posons, pour $0 \leq k,\ell \leq n-1$, $s_{k,\ell} = \sum_{i=1}^{n} \theta_i^k \theta_i'^{\ell}$, et écrivons $s_{k,\ell} = m_{k,\ell} + \varepsilon_{k,\ell}$ avec $m_{k,\ell} \in \mathbb{Z}$ et $\varepsilon_{k,\ell} \in [\frac{1}{2}, -\frac{1}{2}[$. On doit supposer que le calcul numérique fournit des $s_{k,\ell}$ entiers aux erreurs de calcul près, et dans un intervalle acceptable si l'on travaille en p-adique; sinon, la permutation choisie ne correspond pas à un isomorphisme sur $\mathbb{Q}$. Maintenant, pour $\ell = 0,1,\ldots,n-1$, soit $(\phi_1^{(\ell)},\ldots,\phi_n^{(\ell)})$ la solution du système linéaire

$$\sum_{i=1}^{n} \theta_i^k x_i = m_{k,\ell} \qquad (k = 0,1,\ldots,n-1).$$

On définitainsi pour $0 \leq \ell \leq n-1$ un élément $\phi^{(\ell)}$ de K (et l'on écrit simplement ϕ et ϕ_i au lieu de $\phi^{(1)}$ et $\phi_i^{(1)}$); mieux, $\phi^{(\ell)}$ appartient à la codifférente D_θ de l'ordre $\mathbb{Z}[\theta]$ (module dual pour la forme bilinéaire $(x,y) \longrightarrow Tr_{K/\mathbb{Q}}(xy)$ de $\mathbb{Z}[\theta]$). En particulier, $d\,\phi^{(\ell)}$ est entier, d désignant la valeur absolue du discriminant de f.

Le calcul numérique des $s_{k,\ell}$ donne des majorations des $\varepsilon_{k,\ell}$ à partir desquelles on peut majorer $\eta = \mathrm{Sup}\,|\phi_i - \theta_i'|$ (on majore η en étudiant le système linéaire ci-dessus lorsque $\ell = 1$). Il est clair que l'on a $Tr_{K/\mathbb{Q}}(\phi^{(\ell)}) = Tr_{L/\mathbb{Q}}(\theta'^{\ell})$ puisqu'il s'agit d'entiers dans les deux cas. Nous allons montrer maintenant que $\phi^{(\ell)}$ et ϕ^{ℓ} coïncident pour $0 \leq \ell \leq n-1$ pourvu que les $\varepsilon_{k,\ell}$ soient assez petits (et alors, ils seront tous nuls). Tout d'abord, on a les inégalités $|\theta_i'^{\ell} - \phi_i^{\ell}| \leq \ell\, A^{\ell-1} |\theta_i' - \phi_i|$ dans lesquelles A désigne un majorant commun aux θ_i' et aux ϕ_i, d'où l'on déduit les inégalités $\left|\sum_{i=1}^{n} \theta_i^k \phi_i^{\ell} - \sum_{i=1}^{n} \theta_i^k \phi_i^{(\ell)}\right| \leq \varepsilon_{k,\ell} + n\,\ell\, A^{\ell-1} B^k \eta$ quels que soient $k,\ell \in [0,n-1]$, B désignant le maximum des $|\theta_i|$. Si donc les $|\varepsilon_{k,\ell}|$ et par suite η sont assez petits, on obtiendra pour tout ℓ l'inégalité

$$\left|\sum_{i=1}^{n} \theta_i^k \phi_i^{\ell} - \sum_{i=1}^{n} \theta_i^k \phi_i^{(\ell)}\right| \leq \frac{1}{2d}\,.$$

Il est clair que l'on a $\phi^{\ell} = \phi^{(\ell)}$ pour $\ell = 0$ ou 1. Pour $\ell = 2$, on remarque que ϕ^2 est un élément de $\frac{1}{d} D_\theta$ ($d\phi^2 = d\phi.\phi \in \mathbb{Z}[\theta] D_\theta \subset D_\theta$); donc, les sommes $\sum_{i=1}^{n} \theta_i^k \phi_i^2$ sont dans $\frac{1}{d}\mathbb{Z}$; comme les sommes $\sum_{i=1}^{n} \theta_i^k \phi_i^{(2)}$ sont entières, on a en fait l'égalité des deux sommes pour $k = 0,1,\ldots,n-1$, donc l'égalité $\phi^{(2)} = \phi^2$ dans K; en particulier,

$\phi^2 \in D_\theta$, donc $\phi^3 \in \frac{1}{d} D_\theta$, et le même argument prouve que l'on a $\phi^3 = \phi^{(3)}$; on montre ainsi de proche en proche que ϕ^j et $\phi^{(j)}$ coïncident pour $0 \leq j \leq n-1$. On a donc $Tr_{K/\mathbb{Q}}(\phi^j) = Tr_{L/\mathbb{Q}}(\theta'^j)$ pour $0 \leq j \leq n-1$, ce qui prouve que ϕ et θ' ont même polynôme caractéristique, c.q.f.d.

En résumé, on a un procédé permettant de vérifier si un isomorphisme donné entre complétés est rationnel, en vérifiant que $(n-1)^{n-1}$ nombres réels (à savoir les $\Sigma \theta_i^k \theta_i'^\ell$ pour $1 \leq k,\ell \leq n-1$) sont très proches d'entiers. On a évité la résolution du système linéaire de a_1, mais les majorations d'erreurs à faire sont plus précises, la borne finale 1/2 devant être remplacée par 1/2d, et une estimation des solutions d'un système linéaire devant être faite.

Le plus pénible dans ces méthodes est la recherche des bonnes permutations. Pour $n = 6$, le nombre maximum d'essais nécessaire avec $\mathbb{Q}_v = \mathbb{R}$ est 48, 16, 48 et 720 selon que r vaut 0, 2, 4 ou 6; si v est p-adique pour un p de degrés résiduels (1,2,3), 12 essais suffisent.

b) Irréductibilité. Indiquons très brièvement quelques procédés pour un polynôme $f \in \mathbb{Z}[X]$ unitaire. Une méthode effective, mais peu efficace, consiste à vérifier l'absence de décomposition $f = gh$ pour des polynômes g,h à coefficients dans $\mathbb{Z}$ jusqu'à une certaine borne : comme on connait une majoration de $\Sigma |\theta_i|^2$ ($\theta_1,\ldots,\theta_n$ désignant toujours les racines de f), on majore les fonctions symétriques d'un nombre quelconque d'entre elles, donc les coefficients de g et de h pour les différents degrés possibles de g. On peut s'aider des décompositions de f modulo divers nombres premiers : éventuellement, l'irréductibilité s'impose; sinon, on obtient des congruences sur les coefficients des couples (g,h) possibles qui limitent les choix. Si l'on connait les racines, on peut rechercher des combinaisons de racines donnant des fonctions symétriques entières; on trouve alors rapidement un décomposition de f s'il en existe.

c) Recherche de sous-corps. On a un corps K, dont on connait le discriminant, défini par un polynôme irréductible f, de degré n. On cherche si K contient un sous-corps K' de degré n' divisant n; on pose $m = n/n'$. Comme $d_{K'}^m$ divise d_K, les choix pour K' sont limités. Comme les algorithmes décrits en a) et b) s'adaptent à des polynô-

mes à coefficients dans K', et que K contient K' si et seulement si f a un facteur de degré m dans K', on peut en principe adapter l'un des procédés de b). On peut s'inspirer de a_1) ou de a_2) pour simplifier les calculs, en cherchant à exprimer les éléments d'une base d'entiers $\theta_1,\ldots,\theta_{n'}$ de K' à l'aide de m racines bien choisies de f. L'exemple suivant indique succinctement un procédé généralisable : on cherche si K, supposé totalement imaginaire, contient le corps quadratique imaginaire de discriminant $-d$.

Soient $\theta_1,\overline{\theta}_1,\ldots,\theta_m,\overline{\theta}_m$ les racines de f. On cherche une suite $\varepsilon_2,\ldots,\varepsilon_m$ d'éléments de $\{\pm 1\}$ telle que $[(\theta_1-\overline{\theta}_1)+\sum_{k=2}^{m}\varepsilon_k(\theta_k-\overline{\theta}_k)]/i\sqrt{d}$ soit entier. En permuttant les couples $(\theta_i,\overline{\theta}_i)$ convenables, on suppose que la somme $\sum_k \frac{(\theta_k-\overline{\theta}_k)}{i\sqrt{d}}$ est dans $\mathbb{Z}$ aux erreurs de calculs près. Si le calcul des expressions $\sum_k(\theta_k^\ell+\overline{\theta}_k^\ell)$ et $\frac{1}{i\sqrt{d}}\sum_k(\theta_k^\ell-\overline{\theta}_k^\ell)$ donne un résultat très proche d'un entier, alors f est certainement réductible dans K' (et l'on peut, si on le souhaite, calculer un facteur de f dans K').

Nous arrêterons là l'étude des algorithmes, laissant au lecteur le soin d'écrire les algorithmes de c) en toute généralité, et d'écrire les majorations précises qui interviennent dans a), b) et c). On remarquera quand même que les procédés décrits en a) permettent de traiter d'autres questions; en particulier, on peut en tirer un moyen de reconnaître si une extension L/K de corps de nombres est galoisienne et de déterminer le cas échéant le groupe deGalois, et, plus généralement, de voir à quel type de permutation l'on a affaire.

§ 6 - Coïncidences de discriminants (étude a priori).

Les coïncidences de discriminants entre corps isomorphes de même signature sont vraisemblablement rares. En outre, dans tous les cas connus, il n'y en a pas qui mettent en jeu des discriminants petits. Ainsi, en degré 3, la première coïncidence a lieu pour $d=-972=-2^2.3^5$ si $r=1$ et pour $d=+3\,969=3^4.7^2$ si $r=3$; il y a 120 corps avec $-972<d<0$ et 133 corps avec $0<d<3\,969$. En degré 4, les tables de Godwin montrent que pour $r=0$, 2 et 4, il y a respectivement 18,30 et au moins 64 corps avant la première coïncidence. Les quelques résultats connus pour les degrés plus grands confirment la tendance observée en degré ≤ 4.

On ne connait pas d'explication à ce phénomène. On peut toutefois prouver a priori, à l'aide des minorations des discriminants, que certaines coïncidences sont impossibles. Le principe consiste à calculer, pour un hypothétique corps K' ayant même discriminant d qu'un corps K donné, le discriminant D de l'algèbre $K' \otimes_{\mathbb{Q}} L$ pour un sous-corps convenable L de K, par exemple K lui-même. Si $|D|$ est assez petit, $K' \otimes_{\mathbb{Q}} L$ n'est pas un corps (i.e. K' et L ne sont pas linéairement disjoints sur $\mathbb{Q}$), ce qui peut suffire à prouver que K et K' sont isomorphes.

Nous allons étudier quelques exemples pour des degrés ≥ 5. Pour les calculs qui vont suivre, il est commode d'introduire la définition suivante :

Définition 6.1. On dit qu'une algèbre étale sur un corps local a le type de ramification $(e_f, e'_{f'}, \ldots)$ si dans sa décomposition en produits d'extensions, les sommes des degrés résiduels correspondant aux indices de ramification $e, e', \ldots$ sont égales respectivement à $f, f', \ldots$ (on peut supposer que l'on a $e > e' > \ldots$).

Le type de ramification est clairement défini par la donnée de l'algèbre étendue à l'extension maximale non ramifiée du corps de base. Au produit direct correspond l'addition des indices correspondant à un même indice de ramification. La règle suivante détermine le type de ramification des produits tensoriels dans un certain nombre de cas, incluant les cas où la ramification est modérée : on pose $(e_f)(e'_{f'}) = (e''_{f''})$, avec, m désignant le P.G.C.D. de e et de e', $e'' = ee'/m$ et $f'' = mff'$, et l'on ajoute les indices correspondant à un même indice de ramification.

Exemple 6.2. Si d est produit de facteurs premiers distincts, le type de ramification sur $\mathbb{Q}_p$ des algèbres complétées K_p et K'_p de K et de K' est $(2_1, 1_{n-2})$ pour tout diviseur p de d. Celui de $K_p \otimes_{\mathbb{Q}_p} K'_p$ est alors $(2_{2n-2}, 1_{n^2-4n+4})$, d'où $D = \pm d^{2n-2}$ (noter que p est impair).

6.3. Corps de degré 5. Le calcul ci-dessus, joint aux minorations de [Dy D 1] pour les corps de degré 25 avec 1,9 ou 25 places réelles, donne, pour un corps de degré 5, les inégalités $d > 1\,905$, $-d > 4\,263$ et $d > 22\,679$ selon que r vaut 1, 3 ou 5. Les seules applications concernent le cas où $r = 1$: on voit qu'il existe (à isomorphisme près) un unique corps de degré 5 pour chacun des discriminants 1609 (premier),

1 649 (= 17.97) et 1 777 (premier), résultat qui apparaît pour la première fois dans [C-R] en 1974. On montre en fait un résultat plus précis : chacun des entiers 1 609, 1 649 et 1 777 n'est le discriminant que de deux corps : un corps de degré 5 et un corps quadratique. Le discriminant suivant pour $n = 5$ et $r = 1$ est $2\,209 = 47^2$. Le calcul fait en 6.2 ne montre pas directement qu'il s'agit d'un sous-corps du corps de classes de Hilbert de $\mathbb{Q}(\sqrt{-47})$. On s'en sort par l'argument suivant : pour $p = 47$, les types de ramification sur $\mathbb{Q}_p$ ne peuvent être que $(3_1,1_2)$ et $(2_2,1_1)$. Le premier cas impose que l'on ait un corps de type A_5, et alors sa clôture galoisienne a un discriminant trop petit pour le degré 60. On en déduit que le type de ramification est $(2_2,1_1)$, et le calcul du discriminant du produit tensoriel de deux corps ayant ce type de ramification permet de conclure. On montre également l'unicité des discriminants 11^4, 31^4 et 41^4 si $r = 5$ (corps cycliques); en fait, $11^4 = 14\,641$ et $47^2 = 2\,209$ sont chacun discriminant d'un unique corps.

6.4. Corps de degré 6. A partir du degré 6, le procédé ne permet plus d'exclure les coïncidences de discriminants sans facteur carré. En particulier, on ne peut pas traiter à l'aide de l'exemple 6.2 le cas du discriminant minimum pour $r = 4$ (mais l'unicité a été prouvée par Pohst dans [Po 3]).

a) Soit K de degré 6, de discriminant $D = d^3f$ ou d est le discriminant d'un corps quadratique k et f est premier à d. On cherche à prouver que K contient k. On montre que, si p divise d, l'exposant de p dans le discriminant de $K \otimes_{\mathbb{Q}} k$ est majoré par 8 pour $p > 3$, par 10 pour $p = 3$, par 18 pour $p = 2$ et $d \not\equiv 0 \bmod 8$ et par 30 pour $p = 2$ et $d \equiv 0 \bmod 8$. On en déduit, en utilisant les minorations de [Dy D1] pour le degré 12 avec 0,4,8 ou 12 places réelles, que les discriminants D suivants sont ceux d'un corps contenant un corps quadratique (et l'unicité en résulte pour les valeurs pas trop grandes de D en utilisant la théorie du corps de classes) :

$r = 0$, $d = -3$: $|D| \leq$ 18 436 ($D = -9\,747, -11\,691, -14\,283, -16\,551$)

$r = 0$, $d = -4$: $|D| \leq$ 20 741 ($D = -10\,816 = -2^6.13^2$)

$r = 2$, $d = 5$: $|D| \leq$ 129 763 ($D = 30\,125, 35\,125, \ldots, 66\,125 = 5^3.23^2, \ldots, 91\,125 = 3^6.5^3, \ldots$)

$r = 4$, $d = 5$: $|D| \leq$ 440 905 ($D = -104\,875, -144\,875, -149\,875, \ldots$)

$r = 6$, $d = 5$: $|D| \leq$ 2 391 345 ($D = 300\,125, 485\,125, \ldots, 2\,235\,125$)

En utilisant les clôtures galoisiennes des corps cubiques de discriminants -23, -44, -31 et +148, on prouve l'unicité pour les discriminants $-12\,167 = -23^3$, $-21\,296 = -2^4.11^3$, $-29\,791 = -31^3$ et $+810\,448 = 2^4.37^3$. On montre également l'unicité pour les discriminants $-16\,807 = -7^5$ et $+371\,293 = 13^5$ (corps cycliques), ainsi que pour divers autres discriminants de la forme $7^4 f$ en montrant qu'ils contiennent le corps $\mathbb{Q}(2\cos 2\pi/7)$ ($31\,213 = 7^4.13$, $69\,629 = 7^4.29$,... pour $r = 2$; $103\,243 = -7^4.43$, $-218\,491 = -7^5.13$,... pour $r = 4$; $300\,125 = 7^4.5^3$, $434\,581 = 7^4.181$, ... pour $r = 6$).

La situation est moins favorable pour les discriminants de la forme $d^2 f$, où d est un discriminant de corps cubique non abélien. Le calcul du discriminant de $K \otimes_{\mathbb{Q}} k$ où k est un corps cubique de discriminant -23 ou -31, ou la clôture galoisienne d'un tel corps, ne permet pas de prouver l'unicité pour les discriminants $-10\,051 = -19.23^2$ et $-10\,571 = -11.31^2$, qui occupent probablement les deuxièmes et troisièmes positions pour $r = 0$; on prouve néanmoins l'unicité si l'on sait que le type de ramification de 23 ou 31 est (2_3) et non $(3_1, 1_3)$, un renseignement facile à obtenir lorsque l'on construit des tables en déterminant des polynômes; la situation est analogue pour $r = 2$ (on a toutefois l'unicité du discriminant minimal, à savoir $28\,037 = 23^2.53$, par [Po 3]).

6.5. Corps de degré 8. Les deux discriminants minimaux pour $r = 0$ sont conjecturalement $1\,257\,728 = 2^8.17^3$ et $1\,265\,625 = 3^4.5^6$, correspondant respectivement à une extension cyclique K_1 de $k = \mathbb{Q}(\sqrt{-1})$ ramifiée en un idéal au-dessus de 17 et au corps des racines 15-ièmes de l'unité. Soit K un corps de degré 8 dont le discriminant est $2^8.17^3$. En considérant $K \otimes_{\mathbb{Q}} k$, on montre que K contient k; en considérant $K \otimes_k K_1$, on montre que K est isomorphe à K_1; pour le discriminant $3^4.5^6$, on montre d'abord que K contient les corps $k = \mathbb{Q}(\sqrt{-3})$, ce qui assure que 5 est la puissance quatrième d'un idéal premier de degré 2. De nombreux autres résultats d'unicité peuvent être démontrés concernant entre autres les discriminants $1\,327\,833 = 3^4.13^2.97$, $1\,492\,101 = 3^4.13^2.109$, $1\,513\,728 = 2^8.3^4.73$, $1\,763\,584 = 2^8.83^2$ pour $r = 0$, $-4\,461\,875 = 5^4.11^2.59$ pour $r = 2$, $15\,243\,125 = 5^4.29^3$ pour $r = 4$; ces corps sont définis dans [Ln] ou [L-M].

6.6. Divers. Si l'on connaît des renseignements sur la décomposition des nombres premiers ramifiés, ou si l'on connaît a priori un sous-corps,

alors l'identification est facilitée. Par exemple, un corps de degré 10 et de discriminant $-7^5.11^4$, s'il contient $k = \mathbb{Q}(\sqrt{-7})$, est certainement le corps de classes sur k de rayon un idéal premier au-dessus de 11.

§ 7 - Tables numériques (bibliographie commentée).

Pour un degré n donné et une signature (r,s) donnée $(n = r+2s)$, on cherche à dresser la liste des corps K vérifiant l'inégalité $|d_K| \leq M$, où M est une constante que l'on se donne, aussi grande que possible. Il est utile de connaître divers renseignements sur les corps, en particulier groupe des classes d'idéaux (avec structure et générateurs) et groupes des unités; cela permet en particulier d'étudier les extensions abéliennes des corps K par la théorie du corps de classes. Malheureusement, on ne possède des tables étendues que jusqu'au degré 4.

Dans ce qui suit, on laisse de côté les corps quadratiques : la liste des corps est triviale, et de nombreuses tables circulent ; du reste, on peut obtenir les renseignements que l'on désire en s'aidant d'une machine de poche tant que les discriminants ne sont pas gigantesques.

a) Discriminants minimaux. Les minima de $|d_K|$ connus sont les suivants : $n = 3$, $r = 1$ et 3 (Furtwängler, 1896, cf. [Ma]) $n = 4$, $r = 0,2$ et 4 (Mayer, 1929, [Ma]); $n = 5$, $r = 1$, 3 et 5 (Hunter, 1957, [Hu]); $n = r = 6$ (Kaur, 1970, [Ka]); $n = 6$, $r = 0$, 2 et 4 (Pohst, 1982, [Po 3]); $n = 7$, $r = 1$ (Diaz y Diaz, 1982, [DyD 3]; $n = 7$, $r = 3$ (Diaz y Diaz, 1983, [DyD 4]); $n = r = 7$ (Pohst, 1977, [Po 2]).* Signalons que [Ka] contient une lacune, comblée dans [Po 3], et que l'étude du cas $n = 6$, $r = 0$ par Liang et Zassenhaus ([L-Z2]) ne peut être acceptée telle qu'elle est, à cause d'une erreur dans une inégalité (cf. [Po 3], p. 100).

On sait en outre qu'il y a un corps (à isomorphisme près) par discriminant (cf. [C-R] pour $n = 5$).

La référence de [Mr 3], p. 170, à Gauss pour $n = 3$ est une erreur.

b) Corps abéliens. Des techniques particulières se sont développées à la suite des travaux de Hasse et de Leopoldt; nous renvoyons le lecteur à l'ouvrage classique de Hasse ([Ha]), et à [Mr 4] pour une bibliographie récente. Notons simplement ici les tables de nombres de classes et d'unités calculées pour les corps cycliques de degré 3 et 4 (Marie-Nicole Gras, [Gr 1] et [Gr 2] et de degré 6 (Mäki, [Mk]), et signalons que les unités qui ne figurent pas dans [Gr 1] ont été par la suite déterminées

* cf. complément C1.

par Mäki et Godwin ([Go 4]). Les résultats pour les corps abéliens non cycliques de degré 4 se déduisent facilement de l'étude des corps quadratiques.

c) Corps cubiques. L'ouvrage classique de Delone et Fadeev ([D-F]) contient des tables de nombre de classes et d'unités pour les discriminants jusqu'à 1 000 ($r = 1$ et $r = 3$). Les premières tables très étendues sont celles de Angell ([An 1] pour $-20\,000 < d < 0$ et [An 2] pour $0 < d < 100\,000$). Angell signale que deux discriminants sont absents de la table antérieure de Godwin et Samet couvrant l'intervalle $0 < d < 20\,000$. L'étude des corps cubiques réels a été reprise à Turku par Ennola et Turunen ([E-T]),* qui ont étudié les corps totalement réels de discriminant $\leq 200\,000$. Il y a au moins dix discriminants oubliés par Angell (25 717, 32 404, 35 996, 37 108, 37 133, 38 905, 39 992, 43 165, 43 173, 43 176) dans l'intervalle $0 < d < 90\,000$. En outre, on ne peut exclure l'existence d'autres erreurs : par exemple, les unités données pour le corps de discriminant $39\,601 = 199^2$ ne sont pas fondamentales (cf. [Gr 1]).

d) Corps quartiques. A ma connaissance, les seules tables un peu étendues sont celles de Godwin ([Go 1], [Go 2], [Go 3]), correspondant à $r = 0$, 2 et 4, et donnant les corps K pour lesquels on a respectivement $d_K < 1\,458$, $d_K > -3\,280$ et $d_K < 11\,664$. Il serait intéressant de prolonger ces tables,** ainsi que de calculer les groupes de classes et d'unités. Signalons à ce sujet l'étude faite par Pohst ([Po 1]) des extensions quadratiques de $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(\sqrt{2})$.

Les discriminants minimaux pour 4 des 5 types de permutations possibles se déduisent des tables de Godwin : 125,-,1 125 pour le cas cyclique, 144,-,1 600 pour le cas bicyclique, 117,-275,725 pour le cas diédral et 229,-283,1 957 pour le cas symétrique. Les extensions alternées n'apparaissent pas, mais c'est un simple exercice de corps de classes que de constater que les discriminants minimaux sont $3\,136 = 2^6.7^2$ pour $r = 0$ et $26\,569 = 163^2$ pour $r = 4$, les extensions de degré 6 associées (définies à conjugaison près) étant respectivement $\mathbb{Q}(\sqrt{\eta})$, $\eta^3 + \eta^2 - 2\eta - 1 = 0$, et une extension quadratique non ramifiée du corps cubique de discriminant 163^2.

e) Corps quintiques. A partir du degré 5, les résultats sont souvent très partiels, et il est même parfois difficile de savoir ce que l'on peut tenir pour certain. Une étude numérique a été effectuée dès 1955 par Cohn ([Co]). Le travail de Matzat ([Mz]) contient des tables

* cf. Complément C2.

plus étendues et des exemples avec des nombres de classes >1; ajoutons à ces tables celles de Buhler ([Bu]) concernant les corps de type alterné, et une étude récente de Rish que je ne connais que par le Zentralblatt (Zbl 504, 25.10.83). Il est certain que les premiers discriminants sont 1 609, 1 649, 1 777 et 2 409 pour $r=1$, -4 511, -4 903 et -5 519 pour $r=3$, 14 641 et 24 217 pour $r=5$.

Plus précisément, on connaît les minima pour certains des 5 types de permutation (et les signatures permises) : ce sont les cas cycliques ($r=5$, $d=14\,641=11^4$), diédral ($r=1$, $d=2\,209=47^2$ et $r=5$, $d=160\,801=401^2$) et symétrique ($r=1$, $d=1\,609$, $r=3$, $d=-4\,511$ et $r=5$, $d=24\,217$). L'étude de Buhler des corps de type A_5 avec une place réelle montre, compte-tenu des inégalités de Hunter, que le discriminant minimum pour le cas alterné et $r=1$ est $18\,496=(2^3.17)^2$. Buhler donne le polynôme $X^5+7X^4+22X^3+34X^2+17X-17$, de discriminant $(2^9.17)^2$; le polynôme $X^5+2X^3+4X^2-3X+4$, trouvé par Matzat, a pour discriminant $(2^6.17)^2$, et définit le même corps : on passe du second polynôme au premier par la transformation $\theta \longmapsto 1-(\theta^4+\theta^3+\theta^2+5\theta)/2$. Le minimum n'est pas connu pour le type alterné lorsque $r=5$; le plus petit discriminant de [Bu] est $7\,017\,207=(3.883)^2$. Les minima ne sont pas non plus connus pour le groupe métacyclique d'ordre 20. L'exemple classique pour $r=1$ du corps $K=\mathbb{Q}(\sqrt[5]{2})$, avec $d_K=-50\,000$, peut être amélioré : en utilisant [Ha], conducteur 51, p. 162, on construit un corps de discriminant $44\,217=3^2.17^3$; pour $r=5$, en utilisant [Gr 2], conducteur 212, p. 123, on construit un exemple de discriminant $2\,382\,032=2^4.53^3$.

f) Corps sextiques. Il s'agit du plus grand degré pour lequel des recherches systématiques ont été entreprises (en l'occurence, pour $r=0$ et 3, par Biedermann et Richter, [B-R]). Il résulte de ces travaux que les corps primitifs sont connus pour $d \geq -22\,000$ si $r=0$ et $d \leq 600\,000$ si $r=6$; on trouve deux corps pour $r=0$, de discriminants -14 731 et -20 627 (les deux polynômes donnés dans [B-R] pour ce dernier discriminant définissent le même corps, fait vérifié par l'algorithme a_2 du paragraphe 5), et un corps pour $r=6$, de discriminant +592 661. Le plus petit discriminant pour un corps primitif dans le cas $n=6$, $r=2$ n'est pas connu; c'est probablement le corps de discriminant 29 077 de [Ln], table 6. Quant aux corps imprimitifs, les minima pour r croissant de 0 à 6 sont -9 747, +28 037, -103 243 et +300 125. Voici quelques remarques sur la table 6, p. 29 de [B-R] : il faut ajouter en numé-

ro 4 le discriminant $-10\,816 = 2^6.13^2$, et ajouter aussi les deux corps de discriminant $-33\,856 = -2^6.23^2$, à savoir $\mathbb{Q}(\sqrt{-\alpha})$ et $\mathbb{Q}(\alpha,i)$ avec $\alpha^3 - \alpha - 1 = 0$; il n'existe pas de corps imprimitif de discriminant $-27\,848 = -2^3.59^2$; il existe un unique corps imprimitif pour chacun des discriminants $-40\,203 = -3^3.1489$ et $-44\,496 = -2^4.3^3.103$. Cela se vérifie par la théorie du corps de classes.

g) Utilisation de la constante de Lenstra. Les travaux de Lenstra ([Ln]), poursuivis par Leutbecher et moi-même ([L-M]) ont mis en évidence l'intérêt de cette constante, liée à la théorie des corps euclidiens, dans la recherche des petits discriminants. Ce fait a été confirmé par l'étude récente qu'a faite Diaz y Diaz des corps de degré 7 avec $r = 1$ ou 3. On trouve dans [Ln] et [L-M] des tables concernant les degrés 6 ($r = 0,2,4,6$), 7 ($r = 1,3,5$), 8 ($r = 0,2$), 9 ($r = 1$) et 10 ($r = 0$), et quelques exemples d'autres signatures. On trouvera dans [L-M] (paragraphe 8, p. 117 et "Added in proof", p. 118) des conjectures concernant les discriminants minimaux. D'autres corps ont été trouvés récemment par Leutbecher ([Lt]); en particulier, pour $n = 10$ et $r = 0$ est apparu le corps de discriminant $-209\,352\,647 = -23.(7.431)^2$, défini par le polynôme $X^2 - (1-\theta^2-\theta^4)X - \theta$ avec $\theta^5 - \theta^2 + 1 = 0$.

h) Autres problèmes diophantiens. A côté de la constante de Lenstra, diverses question peuvent jouer un rôle dans la recherche des petits discriminants, par exemple :

h1 - L'étude des nombres de Pisot et de Salem (sans nécessairement faire jouer un rôle spécial à une place réelle).

h2 - Le problème de Favard ([Fa]), qui m'a été signalé par Langevin (étude de Sup $|\theta_i-\theta_j|$ pour un entier algébrique θ).

h3 - Le problème de Lehmer, consistant essentiellement à évaluer $\prod_{i=1}^{n} \mathrm{Max}(1,|\theta_i|)$ pour un entier algébrique θ (cf. [Sch], paragraphe 19).

h4 - Le problème suivant de Siegel, enfin, qui m'a été signalé indépendamment par M. Langevin et J.-P. Serre, est très directement lié aux préoccupations de cet exposé : il s'agit de déterminer pour un entier k donné tous les entiers totalement positifs et totalement réels θ tels que $\mathrm{Tr}(\theta) - \deg(\theta) = k$. Siegel ([Si]) montre que l'on a $\mathrm{Tr}(\theta)/\deg(\theta) > 3/2$ sauf si $\theta = 1$ ou $(3\pm\sqrt{5})/2$. Ce résultat a été généralisé par Smyth ([Sm]), qui a montré que l'on avait l'inégalité $\deg(\theta) \leq 1{,}2955\ k$, sauf si θ est racine de l'un des polynômes $X-1$, X^2-3X+1, X^3-5X^2+6X-1, $X^4-7X^3+13X^2-7X+1$ ou $X^4-7X^3+14X^2-8X+1$.

Le problème de Siegel est voisin de ce que l'on a examiné au paragraphe 2, où c'est $Tr(\theta^2)$ qui est en cause. Il serait intéressant de trouver des analogues pour toutes les signatures, avec des formes positives à valeurs entières.

i) Grands degrés. On trouve dans [Mr 2] des exemples de corps totalement imaginaires jusqu'au degré 80; pour les très grands degrés, on peut avoir recours aux tours de corps de classes, cf. [Mr 1].

C - Compléments (octobre 1984).

C1) Le problème du discriminant minimal pour $n = 8$ et $r = 0$ a été résolu par Diaz y Diaz, qui montre en particulier que les deux premiers discriminants sont ceux qui sont décrits en 6.5.

C2) Une table concernant les corps cubiques réels de discriminant $\leq 100\,000$ a été dressée par P. Llorente et A.V. Oneto (Math. Comp. 39 (1982), 689-692). En tenant compte des 51 corps abéliens qui ne sont pas dans la liste, on arrive à 4804 corps, résultat identique à celui obtenu par Ennola et Turunen. Ces derniers ont prolongé leur table, et également fait une table donnant l'indice des unités totalement positives. Signalons également les articles (seuls ou en collaboration) de H.C. Williams parus depuis 1977 dans Mathematics of Computation, consacrés aux corps cubiques purs, qui contiennent des résultats sur les nombres de classes pour certains discriminants dépassant 10^9 (en particulier, 35 (1980), 1423-1434).

C3) Godwin a repris l'étude des corps de degré 4 et de signature mixte (Math. Comp. 42 (1984), 707-711), complétant la table de [Go 2] par les discriminants compris entre -3281 et -7776. Il faut toutefois prendre garde à l'impression défectueuse.

* p. 2 : Divers compléments ont été ajoutés en octobre 1984 à la suite du paragraphe 7.
* p. 25 : cf. complément C1.
* p. 26 : cf. complément C2.
** p. 26 : cf. complément C3.

BIBLIOGRAPHIE

[An 1] I.O. Angell.- A table of complex cubic fields, Bull. London Math. Soc. 5 (1973), 37-38.

[An 2] I.O. Angell.- A table of Totally Real Cubic Fields, Math. Comp. 30 (1976), 184-187.

[B-R] D. Biedermann et W. Richter.- Minimal discriminanten von primitiven Zahlkörpern sechsten Grades im totalreellen und totalcomplexen Fall, Université de Karlsruhe, 1974.

[Bl] H.F. Blichfeldt.- The minimum value of quadratic forms, and the closest packing of spheres, Math. Ann. 101 (1929), 605-608.

[Bl'] H.F. Blichfeldt.- Math.Zeit. 39 (1934-5), 1-15.

[Bu] J.P. Buhler.- Icosahedral Galois Representations, Springer Lecture Notes in Math. 654, Berlin, 1978.

[Ca] J.W.S. Cassels.- An introduction to the geometry of numbers, Springer-Verlag, Berlin, 1959.

[C-R] P. Cartier et Y. Roy.- On the enumeration of quintic fields with small discriminants, J. reine angew. Math. 268/269 (1974), 213-216.

[Ch] T.W. Chaundy.- The arithmetic minima of positive quadratic forms, Quart. J. Math. Oxford 17 (1946), 166-192.

[Co] H. Cohn.- A numerical study of quintics of small discriminant, Comm. Pure Appl. Math. 8 (1955), 377-386.

[D-F] B.N. Delone et D.K. Fadeev.- The Theory of Irrationalities of the Third Degree, Translations Amer. Math. Soc. 10, Providence, Rhode Island, 1964, édition originale (en russe) : Moscou, 1940.

[DyD 1] F. Diaz y Diaz.- Tables minorant la racine n-ième du discriminant d'un corps de degré n, Publ. Math. Orsay 80-06, 1980.

[DyD 2] F. Diaz y Diaz.- Sur les discriminants minimaux, Sém. de Théorie des Nombres, Bordeaux, 1981/82, 12 p.

[DyD 3] F. Diaz y Diaz.- Valeurs minima du discriminant des corps de degré 7 ayant une seule place réelle, C.R. Acad. Sc. Paris, Série I (1982), 137-139.

[DyD 4] F. Diaz y Diaz.- Valeurs minima du discriminant pour certains types de corps de degré 7, Ann. Inst. Fourier 34-3 (1984), à paraître.

[E-T] V. Ennola et R. Turunen.- Tables de corps cubiques, communication personnelle.

[Fa] J. Favard.- Sur les formes décomposables et les nombres algébriques, Bull. Soc. Math. France 57 (1929), 50-71.

[Go 1] H.J. Godwin.- On totally complex quartic fields with small discriminants, Proc. Cambridge Phil. Soc. 53 (1957), 1-4.

[Go 2] H.J. Godwin.- On quartic fields of signature one with small discriminant Quart. J. Math. Oxford 8 (1957), 214-222.

[Go 3] H.J. Godwin.- Real quartic fields with small discriminant, J. London Math. Soc. 31 (1956), 478-485.

[Go 4] H.J. Godwin.- The calculation of large units in cyclic cubic fields, J. reine angew. Math. 338 (1983), 216-220.

[G-S] H.J. Godwin et P. Samet.- A table of real cubic fields, J. London Math. Soc. 34 (1959), 108-110.

[Gr 1] M.-N. Gras.- Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, J. reine angew. Math. 277 (1975), 89-116.

[Gr 2] M.-N. Gras.- Classes et unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$, Ann. Inst. Fourier 29 (1979), 107-124.

[Ha] H. Hasse.- Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

[Hu] J. Hunter.- The minimum discriminants of quintic fields, Proc. Glasgow Math. Ass. 3 (1957), 57-67.

[Ka] G. Kaur.- The minimum discriminant of sixth degree totally real algebraic number fields, J. Indian Math. Soc. 34 (1970), 123-134.

[Ln] H.W. Lenstra Jr..- Euclidean Number Fields of Large Degree, Invent. Math. 38 (1977), 237-254.

[Lt] A. Leutbecher.- Euclidean Fields having a large Lenstra constant, Ann. Inst. Fourier 35-2 (1985), à paraître.

[L-M] A. Leutbecher et J. Martinet.- Lenstra's constant and Euclidean number fields, Astérisque 94 (1982), 87-131.

[L-Z1] J. Liang et H. Zassenhaus.- On a problem of Hasse, Math. Comp. 23 (1969), 515-519.

[L-Z2] J. Liang et H. Zassenhaus.- The Minimum Discriminant of Sixth Degree Totally Complex Algebraic Number Fields, J. Number Theory 9 (1977), 16-35.

[Mk] S. Mäki.- The Determination of Units in Real Cyclic Sextic fields, Springer Lecture Notes in Math. 797, Berlin, 1980.

[Mr 1] J. Martinet.- Tours de corps de classes et estimations de discriminants, Invent. Math. 44 (1978), 65-73.

[Mr 2] J. Martinet.- Petits discriminants, Ann. Inst. Fourier 29 (1979), 159-170.

[Mr 3] J. Martinet.- Petits discriminants des corps de nombres, in "Journées Arithmétiques 1980", J. V. Armitage éd., London Math. Soc. Lecture Notes Series 56 (1982), 151-193.

[Mr 4] J. Martinet.- Préface à la seconde édition de l'ouvrage [Ha] de Hasse, Akademie-Verlag et Springer-Verlag, à paraître.

[Mz] H. Matzat.- Zahlentheoretische Programme und einige Ergebnisse, Université de Karlsrube, 1969.

[My] J. Mayer.- Die absolut kleinsten Discriminanten der biquadratischen Zahlkörper, S.B. Akad. Wiss. Wien, IIa, 138 (1929), 733-742.

[Me] J.-F. Mestre.- Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. reine angew. Math. 343 (1983), 23-35.

[M-H] J. Milnor et H. Husemoller.- Symmetric bilinear forms, Springer-Verlag, Berlin, 1973.

[Od] A. Odlyzko.- Discriminant Bounds, tables multigraphiées datées du 29 novembre 1976 (reproduction partielle dans [Mr 3]).

[Po 1] M. Pohst.- Berechnung kleiner Discriminanten total reeller algebraischer Zahlkörper, J. reine angew. Math. 278/279 (1975), 278-300.

[Po 2] M. Pohst.- The Minimum Discriminant of Seventh Degree Totally Real Algebraic Number Fields, Number Theory and Algebra, H. Zassenhaus éd., 235-240, Academic Press, New-York, 1977.

[Po 3] M. Pohst.- On the Computation of Number Fields of Small Discriminants Including the Minimum Discriminants of Sixth Degree Fields, J. Number Theory 14 (1982), 99-117.

[Poi] G. Poitou.- Sur les petits discriminants, Sém. D.P.P., Paris, exposé N° 6, 1977.

[Sch] A. Schinzel.- Selected topics on polynomials, The University of Michigan Press, 1982.

[Si] C.L. Siegel.- The trace of totally positive and real algebraic integers, Ann. of Math. 46 (1945), 302-312 (premier article du tome 3 des oeuvres complètes).

[Sm] C.J. Smyth.- The mean values of totally real algebraic integers Math. Comp., à paraître*, et Totally positive algebraic integers of small trace, Ann. Inst. Fourier 34-3 (1984), à paraître.

* Vol. 42 (1984), 664-681.