SÉMINAIRE N. BOURBAKI

GEORGES POITOU

Minorations de discriminants

Séminaire N. Bourbaki, 1977, exp. n° 479, p. 136-153

<http://www.numdam.org/item?id=SB_1975-1976__18__136_0>

Séminaire BOURBAKI 479-01
28e année, 1975/76, n° 479 Février 1976

MINORATIONS DE DISCRIMINANTS

[d'après A. M. ODLYZKO]

par Georges POITOU

Que les discriminants des corps de nombres aient une valeur absolue strictement supérieure à 1 (excepté $\mathbb{Q}$, bien sûr) était en 1881 un problème ouvert par une phrase de L. Kronecker [1] : "Sind die Grössen $\mathfrak{R}$ die Elemente eines natürlichen Rationalitätsbereichs, d.h. kommen unter den Grössen $\mathfrak{R}$ keine algebraischen Grössen sondern nur unabhängige Variable vor, so giebt es stets eine ganze ganzzahlige Function derselben (für $\mathfrak{R} = 1$ eine ganze von Eins verschiedene Zahl) welche gemeinsamer Teiler aller Discriminanten des Fundamentalsystems und deshalb füglich (wie in meinem citirten Aufsatze von April 1874) als "Discriminante der Art oder Gattung" bezeichnet werden kann".

Ceci fut prouvé en 1890 par H. Minkowski [2], qui créa à cette occasion la géométrie des nombres. Il s'aperçut presque aussitôt [3] que cette méthode impliquait pour les valeurs absolues des discriminants des minorations tendant vers l'infini avec le degré. Ces minorations ont été améliorées par divers auteurs (cf. la bibliographie donnée dans W. Narkiewicz [4], page 81) par des raffinements géométriques de la même idée.

Dans le livre classique d'E. Landau [5] figure une identité (Satz 180, page 99) sur les fonctions zêta de Dedekind, dont H. M. Stark s'est aperçu [6] qu'elle implique immédiatement une minoration des valeurs absolues des discriminants, déjà meilleure asymptotiquement que celle de Minkowski, et qu'elle porte en elle des possibilités encore plus grandes. Son élève A. M. Odlyzko a mis en oeuvre cette nouvelle idée. Il combine très ingénieusement l'identité de Landau avec certaines de ses dérivées, et surpasse ainsi toutes les minorations d'origine géométrique.

Enfin J.-P. Serre a vu que les identités d'Odlyzko, comme celle de Landau dont elles dérivent, sont des cas particuliers des formules très générales qu'a établies André Weil [7] pour embrasser les diverses formules dites explicites de la théorie des nombres premiers. Pour retrouver celles-là, il suffit de spécialiser une certaine fonction arbitraire F. Dans les notations de [8], la formule de Landau correspond au choix de la fonction $F(x) = e^{-a|x|}$, et celles d'Odlyzko au choix de cette même fonction, multipliée par des polynômes. Serre a proposé de meilleurs choix de F, qui donnent les meilleures estimations connues.

Bien sûr, comme les zéros non triviaux des fonctions zêta de Dedekind interviennent de façon essentielle dans ces formules explicites, il n'est pas surprenant que les résultats obtenus soient plus forts si l'on veut bien admettre que ces zéros ont pour partie réelle $\frac{1}{2}$ (Hypothèse de Riemann généralisée, en abrégé GRH).

Sous GRH, les estimations asymptotiques de Serre résultent du choix de $F(x) = e^{-x^2/4b}$, avec b grand ; sans cette hypothèse, Odlyzko a montré que l'idée reste valable avec $F(x) = e^{-x^2/4b} / \mathrm{ch}(x/2)$.

A ce point, il vaut mieux entrer dans quelques détails.

1. Les discriminants

Le discriminant d'un polynôme unitaire est le produit des carrés des différences des racines. Pour un corps de nombre K (extension de $\mathbb{Q}$ de degré fini) le PGCD des discriminants des polynômes minimaux des entiers de K, de même degré que K, peut contenir des facteurs parasites (cf. par exemple [4] page 65). Le discriminant $d(K)$ peut être défini comme suit : dans le cas particulier où l'anneau des entiers de K est engendré comme $\mathbb{Z}$-algèbre par un unique élément x, $d(K)$ est le discriminant du polynôme minimal de x. On voit alors que les facteurs premiers du discriminant de K sont exactement les nombres premiers ramifiés dans K, c'est-à-dire ceux dont la décomposition en idéaux premiers de K comporte des facteurs multiples. Dans le cas général, on peut partir

d'une base sur Z de l'anneau des entiers de K, former avec elle et ses conjuguées une matrice carrée, et prendre pour $d(K)$ le carré du déterminant de cette matrice. C'est la même chose dans le cas particulier où la base est $(1, x, x^2, \ldots, x^{n-1})$ par le calcul classique de VanderMonde. On peut aussi procéder localement, car le cas particulier suffit pour les corps locaux (cf. par exemple [9] page 66). Cette méthode s'étend à la définition des discriminants relatifs $d(L/K)$ et conduit à la formule

$$(1) \qquad d(L) = d(K)^{[L:K]} N_{L/K} d(L/K) .$$

De ceci, et du théorème de Dedekind sur la ramification, dont un cas particulier a été rappelé ci-dessus, on déduit que le nombre

$$|d(K)|^{1/[K:Q]}$$

ne change pas par passage de K à un surcorps L, si l'extension L/K est non-ramifiée (c'est-à-dire si aucun idéal premier de K n'a de facteurs multiples dans L). Par exemple, on peut prendre pour L le corps de classes de Hilbert de K (extension non-ramifiée abélienne maximale) ; dans ce cas, le degré relatif est égal au nombre de classes d'idéaux de K.

2. Exemples de petits discriminants

Pour les petits degrés, les discriminants les plus petits en valeur absolue sont connus pour chaque type $(r_1, 2r_2)$ - ici r_1 et $2r_2$ représentent les nombres de conjugués réels et complexes. En voici la table :

degré n	type	$\lvert d(K)\rvert$	$\lvert d(K)\rvert^{1/n}$	Observations
2	2,0	5	2,236 ...	$\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\cos\frac{2\pi}{5})$
2	0,2	3	1,732 ...	$\mathbb{Q}(\zeta_3)$
3	3,0	49	3,659 ...	$\mathbb{Q}(\cos\frac{2\pi}{7})$
3	1,2	23	2,844 ...	$K \subset$ Hilbert de $\mathbb{Q}(\sqrt{-23})$
4	4,0	725	5,189 ...	$\mathbb{Q}(\sqrt{7+2\sqrt{5}})$
4	2,2	275	4,072 ...	$\mathbb{Q}(\sqrt{-(1+3\sqrt{5})/2})$
4	0,4	117	3,289 ...	$\mathbb{Q}(\sqrt{(7+\sqrt{-3})/2})$
5	5,0	14641	6,809 ...	$\mathbb{Q}(\cos\frac{2\pi}{11})$
5	3,2	4511	5,381 ...	$x^5 - 2x^3 + x^2 - 1$
5	1,4	1609	4,378 ...	$x^5 - x^3 + x^2 + x - 1$
6	6,0	300125	8,182 ...	$\mathbb{Q}(\cos\frac{2\pi}{7}, \sqrt{5})$
7	7,0	20134393	11,05 ...	$x^7+x^6-6x^5-5x^4+8x^3+5x^2-2x-1$

Les références sont dans [4], page 81, à l'exception de [10].

Parmi les corps de classes de Hilbert des corps quadratiques imaginaires, les suivants donnent de petits discriminants :

degré $n=2r_2$	$\lvert d(K)\rvert^{1/n}$	Hilbert de $\mathbb{Q}(\sqrt{-m})$ avec $m=$
6	4,796 ...	23
8	6,245 ...	39
10	6,856 ...	47
14	8,426 ...	71
16	9,747 ...	95
20	10,909 ...	119
26	13,820 ...	191
28	14,663 ...	215
30	15,460 ...	239
36	18,303 ...	335

Ces exemples commencent à n'être plus très bons, car J. Tate a donné un exemple d'un corps de degré 48 avec $|d| = 283^{24}$, donc $|d|^{1/n} = 16,822 \ldots$

Pour des degrés un peu plus grands, on a de bons exemples avec les corps de classes des corps des racines p-ièmes de l'unité (lui-même de degré $p-1$ et de discriminant p^{p-2}) correspondant au premier facteur h^* du nombre de ses classes d'idéaux

degré $n=2r_2$	$\lvert d(K)\rvert^{1/n}$	p	h^*
224	25,71 ...	29	8
270	27,45 ...	31	9
1 332	33,47 ...	37	37
4 840	37,36 ...	41	121
31 970	43,23 ...	47	695
2 391 978	54,99 ...	59	$3\times59\times223$
68 733 790 638	78,64 ...	83	$3\times279\,405\,653$

D'autre part, les théorèmes de Golod et Chafariévitch [11] (renforcés par A. Brumer, voir P. Roquette [12]) montrent qu'un corps quadratique imaginaire a une tour de corps de classes infinie dès que six nombres premiers au moins s'y ramifient. Il en est ainsi pour $\mathbb{Q}(\sqrt{-3.5.7.11.19})$, qui fournit donc des exemples de corps K, avec des degrés arbitrairement grands, et la même valeur de

479-06

$|d(K)|^{1/n} = 2(3.5.7.11.19)^{1/2} = 296{,}2 \ldots$.

3. Minorations géométriques

Celle de Minkowski [3] s'écrit $|d(K)| > (\frac{\pi}{4})^{2r_2} (\frac{n^n}{n!})^2$ qui surpasse pour $n \geq 2$

$$(e^2)^{r_1} \cdot (\frac{e^2\pi}{4})^{2r_2} \cdot \frac{11}{12} \cdot \frac{1}{2\pi n} \ ,$$

de sorte que l'on a

(A) $\quad |d(K)|^{1/n} > (7{,}3)^{r_1/n} \ (5{,}8)^{2r_2/n}$ pour n assez grand.

Celle de H. P. Mulholland [13] implique que l'on a

(B) $\quad |d(K)|^{1/n} > (32{,}5)^{r_1/n} \ (15{,}7)^{2r_2/n}$ pour n assez grand.

4. Identité de Landau et inégalité de Stark

La fonction zêta de Dedekind

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

($\mathfrak{a}$ décrit les idéaux entiers de K , $\mathfrak{p}$ ses idéaux premiers ; N désigne la norme $N_{K/\mathbb{Q}}$) possède, d'après E. Hecke, une équation fonctionnelle (cf. [5] par exemple) qui s'exprime par l'invariance, par changement de s en $1-s$, de la fonction

$$\Lambda(s) = |d|^{s/2} \ g_1(s)^{r_1} \ g_2(s)^{r_2} \ \zeta_K(s) \ .$$

Ici, on a posé

$$g_1(s) = \pi^{-s/2} \ \Gamma(s/2) \ , \quad g_2(s) = (2\pi)^{-s} \ \Gamma(s) \ .$$

La fonction $s(s-1) \ \Lambda(s)$ est une fonction entière d'ordre 1 dont les zéros ρ sont les zéros non triviaux de $\zeta_K(s)$, c'est-à-dire ceux qui ne sont pas des entiers négatifs. Leur partie réelle est comprise strictement entre 0 et 1 , et conjecturalement (GRH) égale à $\frac{1}{2}$. On a donc un produit de Weierstrass-Hadamard :

(2) $\quad s(s-1) \ \Lambda(s) = e^{a+bs} \ \prod_{\rho} (1 - \frac{s}{\rho}) e^{s/\rho}$.

On peut même enlever les facteurs correctifs $e^{s/\rho}$ (remarque de D. Zagier) à

condition de grouper dans le produit, pour qu'il converge, les termes correspondant à ρ et $\bar{\rho}$, ou bien, ce qui revient au même, à ρ et $1-\rho$.

En indiquant cette convention par la notation Π', on a alors

$$(3) \qquad s(s-1)\,\Lambda(s) = A \prod_{\rho}' \left(1 - \frac{s}{\rho}\right) \qquad (A = \text{constante}) .$$

En effet, le quotient des seconds membres de (2) et (3) est une fonction exponentielle invariante par changement de s en $1-s$, donc constante. L'identité de Landau est la dérivée logarithmique de (3). Soit $\psi(s)$ la dérivée logarithmique de $\Gamma(s)$. Alors on a

$$(4) \quad \tfrac{1}{2}\log|d_K| = \frac{r_1}{2}\left(\log\pi - \psi\left(\frac{s}{2}\right)\right) + r_2(\log 2\pi - \psi(s)) - \frac{1}{s} - \frac{1}{s-1} + \sum_{\rho}' \frac{1}{s-\rho} - \frac{\zeta_K'}{\zeta_K}(s) .$$

Comme la somme Σ' est positive pour s réel > 1, ainsi que

$$(5) \qquad -\frac{\zeta_K'}{\zeta_K}(s) = \sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^s - 1} = \sum_{\mathfrak{p},\,m} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{ms}}$$

il en résulte l'inégalité

$$(6) \quad \frac{1}{n}\log|d_K| \geq \frac{r_1}{n}\left(\log\pi - \psi\left(\frac{s}{2}\right)\right) + \frac{2r_2}{n}(\log 2\pi - \psi(s)) - \frac{2}{n}\left(\frac{1}{s} + \frac{1}{s-1}\right) .$$

Pour en tirer parti pour n grand, on prend s voisin de 1, par exemple $s = 1 + 1/\sqrt{n}$. On connaît $-\psi(1) = \gamma = 0{,}577\ldots$ et $-\psi(\frac{1}{2}) = \gamma + 2\log 2$ par exemple par la décomposition en produit de $1/\Gamma(z)$, qui donne

$$(7) \qquad \psi(z) = -\gamma - \frac{1}{z} + \sum_{1}^{\infty} \left(\frac{1}{n} - \frac{1}{z+n}\right)$$

d'où

$$\log\pi - \psi\left(\tfrac{1}{2}\right) = \log(4\pi e^{\gamma}) = \log(22{,}38\ldots)$$

$$\log 2\pi - \psi(1) = \log(2\pi e^{\gamma}) = \log(11{,}19\ldots)$$

et l'on a donc l'inégalité

$$(C) \qquad |d_K|^{1/n} > (22{,}38)^{r_1/n}\,(11{,}19)^{2r_2/n} \qquad \text{pour } n \text{ assez grand.}$$

La force de cette inégalité est intermédiaire entre celles de (A) et (B) au § 3.

5. La méthode d'Odlyzko

Le premier article paru [14] comporte les calculs numériques les plus simples et donne les meilleurs résultats pour les petits degrés, jusqu'à l'ordre de grandeur de la centaine. Il utilise une identité obtenue en ajoutant à (4), prise

pour $s = \sigma > 1$, l'identité dérivée, prise pour $s = \sigma' > 1$, et multipliée par $\sigma - \frac{1}{2}$. Comme ce nombre est positif, le passage à une inégalité analogue à (6) sera possible si l'on peut affirmer les inégalités

$$(8) \qquad \mathrm{Re}\left(\frac{1}{\sigma - \rho} + \frac{\sigma - \frac{1}{2}}{(\sigma' - \rho)^2} \right) \geq 0$$

et même seulement les inégalités

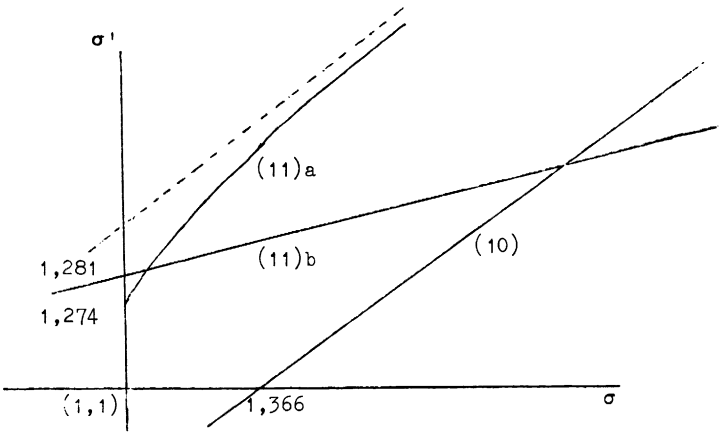
$$(9) \qquad \mathrm{Re}\left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - 1 + \bar{\rho}} + \frac{\sigma - \frac{1}{2}}{(\sigma' - \rho)^2} + \frac{\sigma - \frac{1}{2}}{(\sigma' - 1 + \bar{\rho})^2} \right) \geq 0 .$$

Or l'inégalité (8) est valable, sous GRH, dès que σ et σ' vérifient l'inégalité

$$(10) \qquad \sigma - \tfrac{1}{2} \leq \sqrt{3}\,(\sigma' - \tfrac{1}{2})$$

comme le montre un calcul immédiat. Avec un peu plus de peine, on obtient (9) sans GRH, pourvu que σ et σ' vérifient les deux inégalités

$$(11)_a \qquad \sigma' \geq \frac{5}{6} + \frac{1}{6}\sqrt{12\sigma^2 - 5} \qquad (11)_b \qquad \frac{\sigma' - 1}{\sigma} \geq \frac{1}{\sqrt{7 + 4\sqrt{2}}} = 0{,}281\ldots$$



La région définie par ces deux inégalités peut d'ailleurs être un peu agrandie. Des inégalités obtenues, on tire, par des choix judicieux de (σ , σ'), des tables pour n petit (seule joue alors l'inégalité (11)a), et des estimations asymptotiques

(D) $\quad |d_K|^{1/n} > (50{,}66)^{r_1/n}\,(19{,}96)^{2r_2/n}$ pour n assez grand,

(E) (sous GRH) $\quad |d_K|^{1/n} > (94{,}69)^{r_1/n}\,(28{,}76)^{2r_2/n}$ pour n assez grand.

L'article [15] vise à de meilleures estimations asymptotiques par de bonnes combinaisons linéaires de (6) et de sa dérivée seconde en divers points complexes. Les estimations asymptotiques obtenues sont

(F) $\quad |d_K|^{1/n} > (55)^{r_1/n}\,(21)^{2r_2/n}$ pour n assez grand,

(G) (sous GRH) $\quad |d_K|^{1/n} > (136)^{r_1/n}\,(34{,}5)^{2r_2/n}$ pour n assez grand.

Un aspect intéressant de cette méthode est que l'obtention de (G) n'exige qu'une forme très affaiblie de GRH, qui est la suivante :

La fonction $\zeta_K(s)$ n'a pas de zéro $\beta+i\gamma$ avec $\beta>\frac{1}{2}$ et $\frac{1}{2}(1-\beta)<\gamma<10$.

L'article [16] fait encore mieux avec des combinaisons linéaires d'une douzaine et plus de dérivées de (6) en divers points réels très soigneusement choisis. Au prix de calculs numériques assez considérables, on obtient :

(H) $\quad |d_K|^{1/n} > (60{,}1)^{r_1/n}\,(22{,}2)^{2r_2/n}$ pour n assez grand,

(I) (sous GRH) $\quad |d_K|^{1/n} > (188)^{r_1/n}\,(41)^{2r_2/n}$ pour n assez grand.

Ici encore, (I) n'exige en fait que l'hypothèse suivante :

La fonction $\zeta_K(s)$ n'a pas de zéro $\beta+i\gamma$ avec $\beta>\frac{1}{2}$ et $0<\gamma<3$.

Outre les minorations de discriminants, ces articles contiennent aussi des applications intéressantes et des résultats sur les nombres de classes d'idéaux. Ajoutons que l'estimation de la série (5) pour les corps où certains nombres premiers se décomposent de manière connue (par exemple si 2 se décompose complètement) permet d'améliorer les minorations de discriminants de manière spectaculaire.

6. Les formules explicites de Weil

Soit F une fonction de variable réelle, que nous pouvons supposer paire, différentiable et $O(e^{-(\frac{1}{2}+\varepsilon)|x|})$ ainsi que sa dérivée, pour un $\varepsilon > 0$ (pour des hypothèses plus larges, cf. [8]). Posons :

479-10

$$\Phi(s) = \int_{-\infty}^{+\infty} F(x)\, e^{(s-\frac{1}{2})x}\, dx\ , \qquad \varphi(t) = \Phi(\tfrac{1}{2}+it)$$

et supposons encore $F(0) = 1$, de sorte que l'on a l'égalité $\frac{1}{2\pi}\int_{-\infty}^{+\infty}\varphi(t)\,dt = 1$.

Alors on a la formule suivante :

(12)
$$\log|d| + \frac{1}{2\pi}\int_{-\infty}^{+\infty}\varphi(t)\ 2\ \mathrm{Re}\,\frac{g'}{g}(\tfrac{1}{2}+it)\,dt =$$
$$-\Phi(0) - \Phi(1) + \sum_{\rho}\Phi(\rho) + \sum_{\mathfrak{p},\,m} 2\,\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}\,F(\log N\mathfrak{p}^{m})$$

où ρ décrit les zéros non triviaux de ζ_K , $\mathfrak{p}$ les idéaux premiers de K et m les entiers $1,2,\ldots$, et g désigne la fonction $g_1^{r_1} g_2^{r_2}$. Cette formule contient (4) par le choix de $F(x) = e^{-(s-\frac{1}{2})|x|}$ (la discontinuité de la dérivée à l'origine n'a pas d'importance).

La formule (12) se démontre en calculant $\frac{1}{2i\pi}\int \Phi(s)\, d\log\Lambda(s)$ dans un rectangle défini par les droites $\sigma = -\alpha$ et $1+\alpha$ (avec $\alpha > 0$), $t = \pm T$ (où $\sigma + it = s$ comme d'habitude). La somme des résidus est

$$-\Phi(0) - \Phi(1) + \sum_{|\gamma|<T}\Phi(\rho) \qquad (\rho = \beta + i\gamma)\ .$$

En s'arrangeant pour que la distance de T au γ le plus proche soit de l'ordre de $\frac{1}{\log T}$ (ce qui est possible d'après (4)) et en utilisant l'inégalité $|\psi(s) - \log s| \le \frac{2}{t}$ et encore (4), on majore $\frac{\Lambda'}{\Lambda}$ sur les côtés horizontaux par $O(\log^2 T)$, donc les intégrales correspondantes tendent vers 0 quand T tend vers l'infini. Quant aux intégrales sur les côtés verticaux, elles se regroupent, grâce à l'équation fonctionnelle, en

$$\frac{1}{2i\pi}\int_{1+\alpha-iT}^{1+\alpha+iT}\frac{\Lambda'}{\Lambda}(s)\,[\Phi(s) + \Phi(1-s)]ds\ .$$

Pour évaluer la limite de ceci quand T tend vers l'infini, on écrit

$$\frac{\Lambda'}{\Lambda}(s) = \tfrac{1}{2}\log|d| + \frac{g'}{g}(s) + \frac{\zeta_K'}{\zeta_K}(s)\ .$$

Le morceau correspondant à $-\frac{\zeta_K'}{\zeta_K}$ s'évalue par le développement (5) et la formule

de réciprocité de Fourier ; il tend vers la somme $\sum_{\rho,m}$ de (12). Pour le reste, c'est l'intégrale d'une fonction holomorphe pour $\sigma > 0$, qui a donc même limite que

$$\frac{1}{2i\pi}\int_{\frac{1}{2}-iT}^{\frac{1}{2}+iT}\{\tfrac{1}{2}\log|d| + \frac{g'}{g}(s)\}\,[\Phi(s) + \Phi(1-s)]ds$$

$$= \frac{1}{2\pi}\int_{-T}^{T}\{\log|d| + \frac{g'}{g}(\tfrac{1}{2}+it) + \frac{g'}{g}(\tfrac{1}{2}-it)\}\,\varphi(t)\,dt$$

$$= \frac{1}{2\pi}\int_{-T}^{T}\{\log|d| + 2\,\mathrm{Re}\,\frac{g'}{g}(\tfrac{1}{2}+it)\}\,\varphi(t)\,dt\ .$$

Sa limite est

$$\log|d| + \frac{1}{2\pi}\int_{-\infty}^{+\infty} 2\,\mathrm{Re}\,\frac{g'}{g}(\tfrac{1}{2}+it)\,\varphi(t)\,dt$$

$$= \log|d| - r_1\Big(\log\pi - \frac{1}{2\pi}\int_{-\infty}^{+\infty}\mathrm{Re}\,\psi(\tfrac{1}{4}+i\tfrac{t}{2})\varphi(t)dt\Big) - 2r_2\Big(\log 2\pi - \frac{1}{2\pi}\int_{-\infty}^{+\infty}\mathrm{Re}\,\psi(\tfrac{1}{2}+it)\varphi(t)dt\Big)\ .$$

Cette formule (12) suffit pour les évaluations asymptotiques du paragraphe suivant. Mais en appliquant la formule de Plancherel aux sommes partielles de la série (7), on obtient ces dernières intégrales en fonction de F :

$$-\frac{1}{2\pi}\int_{-\infty}^{+\infty}\mathrm{Re}\,\psi(\tfrac{1}{4}+i\tfrac{t}{2})\varphi(t)dt = \lim_{M\to\infty}\Big\{-\log M + \int_0^{\infty}\frac{e^{x/2}(1-e^{-2Mx})}{\mathrm{sh}\,x}\,F(x)\,dx\Big\}$$

$$-\frac{1}{2\pi}\int_{-\infty}^{+\infty}\mathrm{Re}\,\psi(\tfrac{1}{2}+it)\varphi(t)dt = \lim_{M\to\infty}\Big\{-\log M + \int_0^{\infty}\frac{1-e^{-Mx}}{2\,\mathrm{sh}\,\frac{x}{2}}\,F(x)\,dx\Big\}.$$

On peut même remplacer ces limites par des intégrales portant sur F , en écrivant $\log M = \int_1^M \frac{dx}{x}$, en transformant les intégrales $\int_0^{\infty}$ après découpage en $\int_0^1 + \int_1^{\infty}$, et en utilisant le fait que les fonctions $\frac{F(x)}{\mathrm{sh}\,x} - \frac{1}{x}$ et $\frac{F(x)}{2\,\mathrm{sh}\,\frac{x}{2}} - \frac{1}{x}$ sont bornées, ce qui donne pour les limites ci-dessus les expressions :

$$\int_0^{\infty}\left(\frac{e^{x/2}\,F(x)}{\mathrm{sh}\,x} - \frac{e^{-2x}}{x}\right)dx\ ,$$

$$\int_0^{\infty}\left(\frac{F(x)}{2\,\mathrm{sh}\,\frac{x}{2}} - \frac{e^{-x}}{x}\right)dx\ .$$

Finalement, on peut regrouper tout ceci et écrire :

$$(13)\qquad \frac{1}{2\pi}\int_{-\infty}^{+\infty} 2\,\mathrm{Re}\,\frac{g'}{g}\left(\tfrac{1}{2}+it\right)\varphi(t)\,dt = n(\log 2\pi + I(F)) + r_1\,J(F)$$

avec $I(F) = \int_0^\infty \left(\frac{F(x)}{2\,\mathrm{sh}\,\frac{x}{2}} - \frac{e^{-x}}{x} \right) dx$ et $J(F) = \int_0^\infty \frac{F(x)}{2\,\mathrm{ch}\,\frac{x}{2}}\,dx$.

7. L'application des formules explicites

Elle consiste à choisir de bonnes fonctions F positives telles que $\sum_\rho \Phi(\rho)$ soit aussi positive. On a alors l'inégalité

$$(14)\qquad \log|d| \geq -\Phi(0) - \Phi(1) + n(\log 2\pi + I(F)) + r_1\,J(F)\ .$$

Admettons d'abord GRH. On peut alors prendre (avec $y = \frac{1}{4b}$)

$$F(x) = e^{-yx^2}\ ,\quad \Phi(s) = 2\sqrt{\pi b}\,e^{b(s-\frac{1}{2})^2}\ ,\quad \varphi(t) = 2\sqrt{\pi b}\,e^{-bt^2}\ .$$

Posons $f(y) = nI(F) + r_1 J(F)$ et écrivons (14) sous la forme

$$(15)\qquad \log|d| \geq n\log 2\pi + f\left(\frac{1}{4b}\right) - 4\sqrt{\pi}\,e^{b/4}\,b^{\frac{1}{2}}\ .$$

Le meilleur choix de b est obtenu en dérivant :

$$(16)\qquad 4\sqrt{\pi}\,e^{b/4}\,b^{\frac{1}{2}}(b+2) = -f'\left(\frac{1}{4b}\right)\ .$$

Pour cette valeur de b, l'inégalité (15) devient

$$(17)\qquad \log|d| \geq n\log 2\pi + f\left(\frac{1}{4b}\right) - \frac{1}{b(b+2)}\left|f'\left(\frac{1}{4b}\right)\right|\ .$$

A partir de (17) et des inégalités que fournissent la connaissance du sens de variation et des dérivées à l'origine de f, on peut obtenir une série de formules, dont la première est

$$(18)\qquad \log|d| \geq n\log 2\pi + f(0) - \left[\frac{1}{4b} + \frac{1}{b(b+2)}\right]|f'(0)|$$
$$= n(\log 8\pi + \gamma) + r_1\frac{\pi}{2} - \left[\frac{4}{b} + \frac{16}{b(b+2)}\right](\sigma_3 n + \sigma'_3 r_1)$$

avec $\sigma_k = 1 + \frac{1}{3^k} + \frac{1}{5^k} + \dots$ et $\sigma'_k = 1 - \frac{1}{3^k} + \frac{1}{5^k} + \dots$.

En tenant compte de (16), on voit que l'on a l'inégalité

(19) $\frac{1}{n}\log|d| \geq \log 8\pi + \gamma + \frac{r_1}{n}\frac{\pi}{2} - \frac{3}{\log n}$ pour n assez grand,

et en particulier l'estimation asymptotique meilleure que toutes les précédentes

(J) (sous GRH) $|d_K|^{1/n} > (215{,}3)^{r_1/n}\,(44{,}7)^{2r_2/n}$ pour n assez grand.

Pour se passer de GRH, il faut en rabattre un peu. La positivité de φ ne suffit plus, et la question a été posée par Serre de trouver de bonnes fonctions F positives telles que $\mathrm{Re}\,\Phi(s)$ soit positif dans la bande critique. La réponse d'Odlyzko est $F(x) = e^{-yx^2}/\mathrm{ch}\,\frac{x}{2}$. En effet, on a alors

$$2\,\mathrm{Re}\,\Phi(s) = \int_{-\infty}^{+\infty} F(x)e^{(\sigma-\frac{1}{2})x}(e^{itx} + e^{-itx})dx = \int_{-\infty}^{+\infty} F(x)(e^{(\sigma-\frac{1}{2})x} + e^{-(\sigma-\frac{1}{2})x})e^{itx}dx$$

et, dans le cas particulier, on trouve pour $\sigma = 0$ et $\sigma = 1$

$$\int_{-\infty}^{+\infty} e^{-yx^2}\,e^{itx}\,dx$$

ce qui est positif. Comme la fonction $\mathrm{Re}\,\Phi(s)$ est harmonique dans la bande critique et nulle à l'infini, elle est positive dans toute la bande. De plus, on a $\Phi(0) = \Phi(1) = \int_{-\infty}^{+\infty} e^{-yx^2}\,dx = 2\sqrt{\pi b}$. On a donc l'inégalité (en posant encore $f(y) = nI(F) + r_1 J(F)$)

(20) $\log|d| \geq n\log 2\pi + f(\frac{1}{4b}) - 4\sqrt{\pi}\,b^{\frac{1}{2}}$

et la même méthode que ci-dessus conduit aux inégalités

(21) $\log|d| \geq n\log 2\pi + f(0) - \frac{1}{4b}|f'(0)| - 4\sqrt{\pi}\,b^{\frac{1}{2}}$

$$= n(\gamma + \log 4\pi) + r_1 - \frac{1}{4b}(4\sigma_3 n + 2\zeta(2)r_1) - 4\sqrt{\pi}\,b^{\frac{1}{2}},$$

ce qui donne la minoration simple

(22) $\frac{1}{n}\log|d| \geq \gamma + \log 4\pi + \frac{r_1}{n} - 8{,}6n^{-2/3}$ pour tout n,

et en particulier

(K) $|d_K|^{1/n} > (60{,}8)^{r_1/n}\,(22{,}3)^{2r_2/n}$ pour n assez grand,

ce qui est juste un peu mieux que (H). Mais on tire aussi de (20) des tables pour les bas degrés, et elles sont meilleures que celles de [14]. Les résultats

de ce paragraphe sont les meilleurs actuellement connus (début janvier), tant avec que sans GRH, asymptotiquement comme en bas degrés.

Par exemple, pour $n = 8$, $r_1 = 0$, il existe (Lenstra) un corps avec $|d|^{1/n} = 5{,}78\ldots$; la borne de Minkowski est 3,547..., celle de [14] est 4,77... et celle déduite de la formule (21) est 5,57... ; celle déduite sous GRH de la formule (17) est 5,60... .

Remarque.- Naturellement, les minorations obtenues excluent l'existence de certaines extensions non-ramifiées. Par exemple, le fait que $|d|^{1/n} > 6$ pour $n \geq 10$ empêche les corps quadratiques imaginaires de discriminant inférieur, en valeur absolue, à 36 d'avoir des extensions non-ramifiées de degré relatif ≥ 5 , donc $\mathbb{Q}(\sqrt{-19})$ n'en a pas du tout, et les corps $\mathbb{Q}(\sqrt{-a})$ avec $a = 15,5,23,6,31$ n'en ont pas d'autres que leur corps de classes de Hilbert ; le fait que $|d|^{1/n} > 8$ pour $n \geq 16$ implique que le corps de degré 8 , corps de classes de $\mathbb{Q}(\sqrt{-39})$, pour lequel $|d|^{1/n} = 6{,}245\ldots$, a lui-même un nombre de classes égal à 1 ; les minorations asymptotiques F , H ou K impliquent la finitude de la tour de corps de classes du corps $\mathbb{Q}(\sqrt{-105})$ (avec quatre places ramifiées), pour lequel $|d|^{1/n} < 20{,}5$; etc.

8. Généralisation aux conducteurs [17]

Les conducteurs des représentations généralisent les discriminants (cf. par exemple [9] p. 111), d'où l'idée d'en trouver aussi des minorations, voire de déterminer les plus petits conducteurs possibles pour les représentations irréductibles de degré donné et petit. Par exemple, 23 , qui est conducteur de la représentation irréductible de degré 2 attachée au corps de classes de $\mathbb{Q}(\sqrt{-23})$, est le plus petit conducteur d'une représentation irréductible de degré 2 sur $\mathbb{Q}$ (Serre).

Soient K un corps de nombres galoisien et G le groupe de Galois de $K/\mathbb{Q}$, soient $\rho : G \to GL_n(\mathbb{C})$ une représentation, χ son caractère et f son conducteur. La fonction $L(s,\rho)$ correspondante, définie par la formule

$$\log L(s,\rho) = \sum_{\mathfrak{p},m} \frac{1}{m} \chi(\mathfrak{p}^m) N\mathfrak{p}^{-ms} \quad , \tag{23}$$

est, comme l'on sait, un produit de fonctions L abéliennes avec des exposants entiers rationnels, et c'est donc une fonction méromorphe dans tout le plan, admettant une équation fonctionnelle, exprimant que la fonction

$$\Lambda(s,\rho) = \left(\frac{f}{\pi^n}\right)^{s/2} \Gamma(\tfrac{s}{2})^a \, \Gamma(\tfrac{s+1}{2})^b \, L(s,\chi) = f^{s/2} \, g_1(s)^{a-b} \, g_2(s)^b \, L(s,\chi)$$

est égale, à un facteur constant près, à $\Lambda(1-s,\bar{\rho})$. Les nombres entiers a et b ont pour somme n , et a - b est égal à $\chi(c)$, où $c \in G$ est la conjugaison complexe ; autrement dit, $\rho(c)$ a des valeurs propres +1 et -1 en nombres respectifs a et b .

Les analogues des formules (4) et (12) sont valables pourvu que les fonctions L soient holomorphes hors de s = 1 (c'est la conjecture d'Artin) et on pourra en déduire, pourvu que les coefficients de (23) soient positifs, des inégalités telles que (6) ou (14), où r_1 et r_2 sont remplacés par a - b et b respectivement. L'ordre du pôle éventuel en s = 1 n'apparaît que comme multiple du terme négligé dans l'estimation asymptotique ; celle-ci reste donc valable.

Si les valeurs de χ ont seulement leurs parties réelles positives, on trouve un résultat analogue par la considération du produit $L(s,\rho)L(s,\bar{\rho})$.

Dans le cas général, on peut procéder de deux façons. Odlyzko ajoute à χ un multiple positif du caractère unité pour rendre sa partie réelle positive (le facteur n suffit en tous cas) et en appliquant la méthode de [14] il obtient des minorations comme

$$f > (3{,}70)^a \, (2{,}38)^b$$

pourvu que $L(s,\rho)$ vérifie la conjecture d'Artin.

Serre a remarqué que l'on peut prendre comme intermédiaire la fonction $L(s,\rho \otimes \bar{\rho})$, dont le logarithme a une série de Dirichlet à coefficients positifs, pour laquelle les analogues de r_1 et r_2 sont $(a-b)^2$ et 2ab . Si l'on suppose ρ irréductible, cette fonction a un pôle simple pour s = 1 , et, si elle vérifie la conjecture d'Artin, elle permettra d'étendre à $f(\rho \otimes \bar{\rho})$ toutes les minorations démontrées ci-dessus pour $|d_K|$. Or, en examinant la contribu-

tion des groupes de ramification supérieurs à chacun des deux conducteurs, on montre que $f(\rho \otimes \bar{\rho})$ divise $f(\rho)^{2(n-1)}$. Donc d'après (K) on a l'inégalité asymptotique

$$f(\rho)^{1/n} > (7,7)^{(a-b)^2/n^2} \ (4,7)^{4ab/n^2} \qquad \text{pour } n \text{ assez grand,}$$

pourvu que ρ soit irréductible et que $L(s,\rho \otimes \bar{\rho})$ vérifie la conjecture d'Artin.

BIBLIOGRAPHIE

[1] L. KRONECKER - Grundzüge einer arithmetischer Theorie der algebraischen Grössen, Festschrift zu Herrn Ernst Eduard Kummer's fünfzigjährigem Doctor-Jubilaüm, 10 September 1881, Crelle 92 (1882), 1-122 = Werke II, 237-387.

[2] H. MINKOWSKI - Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen, Crelle 107 (1881), 278-297 = Ges. Abh. I, 243-260.

[3] H. MINKOWSKI - Théorèmes arithmétiques (extrait d'une lettre à M. Hermite), C.R. Acad. Sci. Paris, 112 (26 janvier 1891), 209-212 = Ges. Abh. I, 261-263. Ce texte est annoncé dans une lettre à Hilbert datée de Bonn, le 22 décembre 1890, cf. H. Minkowski, Briefe an David Hilbert, Springer-Verlag (1973), p. 41.

[4] W. NARKIEWICZ - Elementary and analytic theory of algebraic numbers, Warszawa (1974).

[5] E. LANDAU - Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, zweite Auflage, Göttingen (1927).

[6] H.M. STARK - Some effective cases of the Brauer-Siegel theorem, Inventiones Math., 23 (1974), 135-152.

[7] A. WEIL - Sur les "formules explicites" de la théorie des nombres premiers, Comm. Sem. Math. Lund (volume dédié à M. Riesz), Lund (1952), 252-265. Sur les formules explicites de la théorie des nombres, Izvestia Akad. Naouk S.S.S.R., Ser. Math., 36 (1972), 3-18.

[8] S. LANG - Algebraic numbers, Addison-Wesley, 1964.

[9] J.-P. SERRE - Corps locaux, Hermann, Paris, 1962.

[10] M. POHST - The minimum discriminant of seventh degree totally real algebraic number field, J. Number Theory, à paraître.

[11] E.S. GOLOD et I.R. CHAFARIEVITCH - Sur les tours de corps de classes [en russe], Izvestia Akad. Naouk S.S.S.R., Ser. Math. 28 (1964), 261-272.

[12] P. ROQUETTE - On class field towers, p. 231-249 dans J.W.S. Cassels et A. Fröhlich, Algebraic Number Theory, Acad. Press 1967 (Colloque de Brighton).

[13] H.P. MULHOLLAND - On the product of n complex homogeneous linear forms, J. London Math. Soc., 35 (1960), 241-250.

[14] A.M. ODLYZKO - Some Analytic Estimates of Class Numbers and Discriminants, Inventiones Math., 29 (1975), 275-286.

[15] A.M. ODLYZKO - Lower Bounds for Discriminants of Number Fields, Acta Arith., à paraître.

[16] A.M. ODLYZKO - Lower Bounds for Discriminants of Number Fields II, à paraître.

[17] A.M. ODLYZKO - On Conductors and Discriminants, à paraître.