

SÉMINAIRE N. BOURBAKI

GEORGES POITOU

Solution du problème du dixième discriminant

Séminaire N. Bourbaki, 1968, exp. n° 335, p. 367-374

http://www.numdam.org/item?id=SB_1966-1968__10__367_0

© Association des collaborateurs de Nicolas Bourbaki, 1968, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

SOLUTION DU PROBLÈME DU DIXIÈME DISCRIMINANT

(d'après STARK)

par Georges POITOU

STARK [6] résout un problème posé depuis GAUSS [1], celui de la détermination des entiers D tels que toutes les formes quadratiques binaires définies positives de discriminant D soient équivalentes, ou, ce qui revient au même, de la détermination des corps quadratiques imaginaires dont tous les idéaux sont principaux. Neuf étaient connus de GAUSS ; HEILBRONN et LINFOT [4] ont montré qu'au plus un autre existe ; STARK prouve qu'il n'existe pas.

1. Etant donné un entier d sans facteurs carrés et différent de 1 , le discriminant D du corps $\mathbb{Q}(\sqrt{d})$ est d ou $4d$ selon que d est ou non congru à 1 modulo 4 . D'après la loi de réciprocité quadratique, il existe un unique caractère quadratique φ modulo $|D|$, tel que, pour p premier ne divisant pas $2D$, $\varphi(p)$ soit 1 ou -1 selon que D est ou non un carré modulo p . Si l'on pose

$$L(s, \varphi) = \sum_{n=0}^{\infty} \varphi(n) n^{-s}$$

alors, le nombre $h(d)$ des classes d'idéaux (modulo les idéaux principaux) du corps $\mathbb{Q}(\sqrt{d})$ est donné, d'après LEJEUNE-DIRICHLET [2], pour $d < 0$, $d \neq -1, -3$, par

$$h(d) = \frac{\sqrt{-D}}{\pi} L(1, \varphi)$$

et pour $d > 0$ par

$$h(d) = \frac{\sqrt{D}}{2 \log \epsilon} L(1, \varphi)$$

où ϵ désigne l'unité fondamentale du corps.

On peut utiliser ce théorème, ou d'autres, pour calculer $h(d)$ pour d donné, et il existe des tables pour les petites valeurs de $|d|$; notre question se ramène donc en fait à montrer que $h(d)$ est différent de 1 pour $-d$ assez

grand, avec une limitation explicite (sans limitation explicite, c'est une conséquence du résultat de HEILBRONN et LINFOT, et aussi d'un article antérieur de HEILBRONN [3], prouvant que $h(d)$ tend vers l'infini avec $-d$).

2. L'idée de HEILBRONN et LINFOT consiste à considérer deux entiers d et d' tels que $-d$ et $-d'$ soient grands et que $h(d) = 1 = h(d')$, et à étudier les fonctions L correspondant aux caractères associés φ et φ' , ainsi qu'au caractère $\varphi\varphi'$, et notamment le signe de ces fonctions pour s peu inférieur à 1 ; on en tire une contradiction, en utilisant en particulier un développement de la fonction $L(s, \varphi)L(s, \varphi\varphi')$; chez STARK, ceci se retrouve, ainsi modifié : on considère les nombres d tels que $-d$ soit grand et $h(d) = 1$, et on étudie l'entier $h(d')$, lorsque le caractère $\varphi\varphi'$ correspond à un corps quadratique réel fixe ; on peut en dire assez sur la variation de cet entier avec d pour qu'une contradiction apparaisse en comparant le résultat obtenu dans les deux cas où le corps quadratique réel en question est $\mathbb{Q}(\sqrt{2})$, puis $\mathbb{Q}(\sqrt{3})$.

3. Soient donc χ le caractère associé à un corps quadratique réel de discriminant f , et φ le caractère associé au corps $K = \mathbb{Q}(\sqrt{d})$, avec $h(d) = 1$ et $-d$ assez grand. Soit $(1, \omega)$ une base sur $\mathbb{Z}$ des entiers de K , et soit $Q(x, y) = N_{K/\mathbb{Q}}(x + \omega y)$. La fonction dzêta du corps

$$\zeta_K(s) = \sum N(\mathfrak{a})^{-s} \quad (\mathfrak{a} \text{ décrit les idéaux non nuls})$$

s'écrit encore, puisque tous les idéaux sont principaux,

$$\zeta_K(s) = \frac{1}{2} \sum Q(x, y)^{-s} \quad (x, y, \text{ entiers rationnels non tous deux nuls})$$

mais aussi, par la loi de réciprocité quadratique,

$$\zeta_K(s) = \zeta(s) L(s, \varphi)$$

d'où l'on déduit facilement l'identité

$$(1) \quad L(s, \chi) L(s, \varphi\chi) = \frac{1}{2} \sum \chi(Q(x, y)) Q(x, y)^{-s}.$$

Comme $L(1, \chi)$ est connu (c'est $2^{-\frac{1}{2} \log(1 + \sqrt{2})}$ pour $\mathbb{Q}(\sqrt{2})$ et

$3^{-\frac{1}{2} \log(2 + \sqrt{3})}$ pour $\mathbb{Q}(\sqrt{3})$) et que $L(1, \varphi\chi)$ vaut $\frac{\pi}{\sqrt{-fd}} h(fd)$, l'évaluation

de $h(f_d)$ revient à celle du second membre de (1) pour s tendant vers 1. Or, on peut donner à cette limite la forme d'une série entière en $\exp(-\pi\sqrt{-d}/f)$ - ce nombre est petit - dont les coefficients croissent assez lentement pour qu'importent seuls les premiers termes.

Avant d'exposer ce point, fixons nos idées en observant que $-d = p$ est un nombre premier ; sinon, les facteurs premiers de p seraient ramifiés sans pourtant être des carrés de nombres entiers de K , ce qui impliquerait l'existence d'idéaux non principaux ; de même, 2 n'est pas ramifié, de sorte que p est congru à 3 modulo 4, que le discriminant est d , et qu'on peut prendre $w = \frac{1}{2}(1 + \sqrt{d})$, donc $Q(x, y) = x^2 + xy + ry^2$, avec $r = \frac{1}{4}(p + 1)$; toujours pour les mêmes raisons, 2 n'est pas décomposé, de sorte que p est congru à 3 modulo 8, et 3 n'est pas décomposé, de sorte que p est congru à 19 modulo 24 (ces conclusions valent dès que $-d > 11$, puisqu'alors il n'existe pas dans K d'entiers de norme 2 ou 3) ; de même, dès que $-d > 19$, 5 ne peut être décomposé, etc ...

4. Pour développer le second membre de (1), STARK choisit, en considérant

$Q(x, y)$ comme la valeur pour $u = \frac{1}{2}$, $v = \frac{\sqrt{p}}{2}$ de $(x + uy)^2 + v^2 y^2$, de développer en série de Fourier par rapport à u (on reconnaît une méthode de la théorie des formes modulaires) la somme pour $y \neq 0$.

D'abord, la somme pour $y = 0$ vaut

$$\frac{1}{2} \sum_{x \neq 0} \chi(x^2) x^{-2s} = \zeta(2s) \prod_q (1 - q^{-2s}),$$

où q décrit les facteurs premiers de f ; ensuite, la somme pour $y \neq 0$ vaut

$$\sum_{y=1}^{\infty} \sum_x \chi(Q(x, y)) [(x + uy)^2 + v^2 y^2]^{-s} = \sum_{n=-\infty}^{+\infty} A_n(s) e(nu/f)$$

(où l'on a posé $e(t) = \exp(2i\pi t)$) avec les coefficients de Fourier

$$(2) \quad A_n(s) = f^{-1} v^{1-2s} \int_{-\infty}^{+\infty} e(-nvt/f) (t^2 + 1)^{-s} dt \sum_{\substack{m|n \\ m > 0}} m^{1-2s} S(m, n/m)$$

avec

$$(3) \quad S(m, m') = \sum_{k \bmod f} \chi(Q(k, m)) e(km'/f) .$$

Comme le changement de n en $-n$ se traduit par la conjugaison complexe, on peut se borner aux indices n positifs. Lorsque n est au moins égal à 1, la somme au second membre de (2) est finie et la limite pour s tendant vers 1 de $A_n(s)$ est

$$A_n(1) = \pi f^{-1} v^{-1} \exp(-2\pi m v f^{-1}) \sum_{\substack{m|n \\ m>0}} m^{-1} S(m, n/m) .$$

Pour $n = 0$, on peut montrer que

$$\sum_{m=1}^{\infty} m^{1-2s} S(m, 0)$$

a une limite pour s tendant vers 1 (c'est le produit de $\zeta(2s-1)$ par une fonction élémentaire nulle pour $s = 1$), d'ailleurs égale à $\pi(\log 2/\sqrt{6})$ pour $Q(\sqrt{2})$ et 0 pour $Q(\sqrt{3})$.

On tire donc de l'identité (1)

$$(4) \quad \frac{1}{\sqrt{2}} \log(1+\sqrt{2}) \frac{\pi}{\sqrt{8p}} h(-8p) = L(1, \chi_8) L(1, \overline{\chi}_8) = \frac{\pi^2}{8} - \frac{\pi \log 2}{4\sqrt{p}} + 2\Re \sum_{n=1}^{\infty} A_n(1) e(n/16)$$

$$(5) \quad \frac{1}{\sqrt{3}} \log(2+\sqrt{3}) \frac{\pi}{\sqrt{12p}} h(-12p) = L(1, \chi_{12}) L(1, \overline{\chi}_{12}) = \frac{\pi^2}{9} + 2\Re \sum_{n=1}^{\infty} A_n(1) e(n/24)$$

où il reste à calculer les coefficients $A_n(1)$, donc les sommes $S(m, m')$.

Des identités $\chi_8(a+4) = -\chi_8(a)$, $\chi_4(a+2) = -\chi_4(a)$, on déduit que $S(m, m')$ est nul si m et m' n'ont pas la même parité; donc $A_n(1)$ est nul si n est le double d'un nombre impair.

Dans le cas où m et m' ont même parité, on trouve pour la série (4) :

$$\frac{1}{2} S_8(m, m') = \chi_8(m^2) [\chi_8(r) + e(\frac{m'}{4}) \chi_8(r - 2\chi_4(m))] - \chi_8(1+m+rm^2) e(\frac{m'}{8}) + \chi_8(1-m+rm^2) e(\frac{-m'}{8})$$

d'où en particulier :

$$A_1(1) e(1/16) = \frac{\pi}{\sqrt{p}} [\chi_8(r) \cos \frac{\pi}{8} + \chi_8(r+2) \cos \frac{3\pi}{8}] \exp(\frac{-\pi\sqrt{p}}{8}) .$$

Pour la série (5), on remarque que $S_{12}(m, m')$ égale $S_4(m, m') S_3(m, m')$, ces dernières sommes étant formées avec les caractères χ_4 et χ_3 . Leurs valeurs sont :

$$S_3(m, m') = \begin{cases} 2 & \text{si } 3 \text{ divise } m \text{ et } m' \\ -1 & \text{si } 3 \text{ divise } m \text{ ou } m' \text{ mais non les deux} \\ 2 e(mm'/3) & \text{si } 3 \text{ ne divise ni } m \text{ ni } m' . \end{cases}$$

$$\frac{1}{2} S_4(m, m') = \begin{cases} 0 & \text{si } m \text{ et } m' \text{ n'ont pas la même parité} \\ e((m + m')/4) & \text{si } m \text{ et } m' \text{ sont pairs} \\ \chi_4(r)(1 + e(mm'/4)) & \text{si } m \text{ et } m' \text{ sont impairs} \end{cases}$$

d'où en particulier

$$A_1(1)e(1/24) = -\chi_4(r)(2\pi\sqrt{2}/3\sqrt{p})\exp(-\pi\sqrt{p}/12)$$

$$A_3(1)e(3/24) = -\chi_4(r)(4\pi\sqrt{2}/9\sqrt{p})\exp(-\pi\sqrt{p}/4) .$$

En tous cas, les nombres $A_n(1)e(n/2f)$ s'écrivent $B_n x^n$, où

$x = \exp(-\pi\sqrt{p}/f)$ est petit et B_n croît au plus comme $\sum_{d|n} d^{-1}$; la grandeur de $h(-fp)$ est donc fournie raisonnablement par les premiers termes :

$$\frac{1}{4} h(-8p)\log(1 + \sqrt{2}) = -\frac{1}{4} \log 2 + \frac{\pi\sqrt{p}}{8} \pm \sqrt{2(2 \pm \sqrt{2})}y \mod 0(y^3)$$

$$\frac{1}{8} h(-12p)\log(2 + \sqrt{3}) = \frac{\pi\sqrt{p}}{12} - \chi_4(r)\sqrt{2}z - \chi_4(r)\frac{2\sqrt{2}}{3}z^3 \mod 0(z^4)$$

avec $y = \exp(-\pi\sqrt{p}/8)$, $z = \exp(-\pi\sqrt{p}/12)$; on en déduit, en posant

$$h(-8p) = 4N + 2, \quad h(-12p) = 8M + 4,$$

$$(6) \quad \sqrt{2 + \sqrt{2}} (1 + \sqrt{2})^N = y^{-1} [1 \pm \sqrt{2(2 \pm \sqrt{2})}y + \dots] \quad (\text{les } \pm \text{ dépendent de } r \mod 8)$$

$$(7) \quad \frac{1 + \sqrt{3}}{2} (2 + \sqrt{3})^M = \frac{1}{\sqrt{2}} z^{-1} [1 \mp \sqrt{2}z + z^2 \mp \sqrt{2}z^3 + \dots] \quad (\mp 1 = -\chi_4(r)) .$$

$$\frac{1}{2}fp$$

Or, si l'on calcule $h(-fp)$ à partir de la formule $\frac{1}{2} \sum_{j=1}^{fp} \chi(j)\varphi(j)$ (cf. [6] th. 5.4.3), on trouve que M et N sont entiers - ce qui signifie que la puissance de 2 contenue dans le nombre de classes est celle mise en évidence par la théorie des genres; les premiers membres de (6) et (7) sont donc voisins de nombres entiers rationnels. On pose

$$a_m = \frac{1 + \sqrt{3}}{2} (2 + \sqrt{3})^m + \frac{1 - \sqrt{3}}{2} (2 - \sqrt{3})^m + \chi_4(r)$$

$$b_n = \frac{1}{2\sqrt{2}} [(1 + \sqrt{2})^n - (1 - \sqrt{2})^n]$$

$$c_n = \frac{1}{2} [(1 + \sqrt{2})^n + (1 - \sqrt{2})^n] .$$

Supposons pour simplifier r congru à 1 modulo 8 (les autres cas sont analogues) ; alors les équations (6) et (7) donnent

$$(8) \quad c_{2N+1} - 4b_N = \frac{1}{2\sqrt{2}} \exp(\pi\sqrt{p}/4) \quad \text{modulo} \quad \exp(-\pi\sqrt{p}/8)$$

$$(9) \quad a_M^3 + 3 = \frac{1}{2\sqrt{2}} \exp(\pi\sqrt{p}/4) \quad \text{modulo} \quad \exp(-\pi\sqrt{p}/12)$$

de sorte que, pour p assez grand, on a forcément l'égalité

$$(10) \quad c_{2N+1} - 4b_N = a_M^3 + 3 .$$

Le "modulo" des formules (8) et (9) signifie seulement que l'erreur est une série entière en $\exp(-\pi\sqrt{p}/f)$ à coefficients modérément croissants ; en précisant le calcul à partir de (4) et (5) sous forme d'inégalités, on trouve que pour p supérieur à 200, la somme des erreurs dans (8) et (9) est inférieure à 1, donc (10) vaut.

Remarque. - C'est même vrai pour p supérieur à 12 ; on peut le vérifier cas par cas ; on peut aussi préciser (6) et (7) par application de la formule-limite de Kronecker [5] : Ecrivons $Q(x,y) = |x + \tau y|^2$ avec $\Im(\tau) > 0$; alors (1) s'écrit pour $s = 1$:

$$\frac{1}{2} \sum \frac{\chi(Q(x,y))}{Q(x,y)} = \frac{\pi^2}{f^3} \sum_m \sum_n n^2 \chi(Q(m,n)) - \frac{\pi}{f\Im(\tau)} \log \prod_{m,n} \left| \theta\left(\frac{m + n\tau}{f}\right) \right|^{\chi(Q(m,n))}$$

avec $0 \leq m \leq f-1$, $0 \leq n \leq f-1$ et $\theta = \theta_{11}$ dans les notations de WEBER.

On en déduit, par exemple, si r est congru à 1 modulo 4, que le crochet de (7) est $A(z^3)^2 A'(z)^{-1} A'(z^9)^{-1}$ en désignant par $A(t)$ le produit

$$\prod_{i=0}^{\infty} (1 - 2t \cos \frac{2i+1}{4} \pi + t^2) (1 - t^{8(2i+1)})^{-1}$$

et par $A'(t)$ celui qui s'en déduit par changement de $\sqrt{2}$ en $-\sqrt{2}$.

5. La démonstration s'achève par le fait que l'équation (10) ne peut avoir lieu que pour un nombre fini de valeurs de p ; en fait, il n'y a qu'un nombre fini d'entiers N tels que $c_{2N+1} - 4b_N - 3$ soit un cube a^3 . Ceci implique en effet, par l'identité $c_{2N+1} = 4b_N b_{N+1} + (-1)^N$, que a est pair et N impair, disons $a = 2b$ et $N = 2n - 1$; d'où l'identité $2b^3 + 1 = b_{2n-1}(b_{2n} - 1)$ qui se ramène, suivant que n est pair ou impair, à $b^3 = c_n^3 c_{n-1}$ ou $b^3 = 4b_n^3 b_{n-1}$; prenons par exemple le premier cas : on montre que la suite (c_k) ne contient qu'un nombre fini de cubes d'après l'identité $c_k^2 = 2b_k^2 + (-1)^k$ et le fait que l'égalité $c^6 \pm 1 = 2d^2$ entre entiers c et d implique $c = 1$.

Dans tous les cas, on trouve que les valeurs de p correspondantes sont inférieures à 200 ; donc le corps $\mathbb{Q}(\sqrt{-p})$ n'a ses idéaux tous principaux que pour p inférieur à 200 ; on constate que c'est vrai pour les nombres premiers compris entre 12 et 200, et congrus à 19 modulo 24, sauf pour 139, car 5 se décompose dans $\mathbb{Q}(\sqrt{-139})$; que cela soit vrai pour 19, 43, 67 et 163 résulte de ce que dans leurs corps, les nombres 2, 3, 5 et 7 sont inertes ou décomposés en idéaux principaux, et du théorème classique selon lequel toutes les classes sont représentées parmi les facteurs des entiers inférieurs à $\sqrt{-D/3}$. Enfin, c'est vrai pour les discriminants de valeur absolue inférieure à 12, pour des raisons analogues, ou d'après l'algorithme d'EUCLIDE.

BIBLIOGRAPHIE

- [1] C. F. GAUSS - Disquisitiones arithmeticae, (1801), art. 303.
- [2] G. LEJEUNE-DIRICHLET - Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres. Première Partie. Crelle 19 (1839), pp. 324-369.
- [3] H. HEILBRONN - On the class-number in imaginary quadratic fields. Quarterly J. of math. (Oxford), 5 (1934), pp. 150-160.

- [4] H. HEILBRONN and E. H. LINFOOT - On the imaginary quadratic corpora of class-number one. Quarterly J. of math. (Oxford), 5 (1934), pp. 293-307.
- [5] C. L. SIEGEL - Lectures on advanced number theory - Tata Institute 1961.
- [6] Z. I. BOREVITCH et I. R. CHAFAREVITCH - Théorie des nombres. Moscou 1964.
- [7] H. M. STARK - A complete determination of the complex quadratic fields of class-number one. Michigan Math. J. 14 (1967), pp. 1-27.