JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

JACQUES MARTINET

Les discriminants quadratiques et la congruence de Stickelberger

Journal de Théorie des Nombres de Bordeaux, tome 1, n° 1 (1989), p. 197-204

<http://www.numdam.org/item?id=JTNB_1989__1_1_197_0>

Séminaire de Théorie des Nombres,
Bordeaux, **1**, *197–204 (1989)*

Les discriminants quadratiques et la congruence de Stickelberger

par JACQUES MARTINET

1. Introduction. Le but de cet article est de démontrer une forme relative du théorème de Stickelberger sur les discriminants, indiquée sans démonstration aux Journées Arithmétiques d'Exeter de 1980 ([6], appendice II) ; nous donnons en outre une généralisation de cet énoncé.

Soit K un corps de nombres, et soit L une extension finie de K. Notons $\mathfrak{d}_{L/K}$ ou simplement $\mathfrak{d}$ le discriminant relatif de L/K, c le nombre de places complexes de L qui sont au-dessus d'une place réelle de K, et N la norme $N_{K/\mathbf{Q}}$ de K sur $\mathbf{Q}$.

1.1 THÉORÈME. *On a* $(-1)^c N(\mathfrak{d}) \equiv 0$ *ou* $1 \mod 4$.

Lorsque $K = \mathbf{Q}$, c est le nombre r_2 de places complexes de L, et la norme de $\mathfrak{d}$ est la valeur absolue du discriminant d de L. Comme d a le signe de $(-1)^{r_2}$, on retrouve le résultat de Stickelberger publié en 1897 dans les actes du premier congrès international([9]), résultat dont une démonstration très simple a été donnée par Schur en 1928 ([7]) :

1.2 COROLLAIRE. *Le discriminant d'un corps de nombres est congru à* 0 *ou* $1 \mod 4$.

Soit μ le sous-groupe des racines de l'unité de K dont l'ordre est une puissance de 2, et notons 2^m le nombre d'éléments de μ. Dans le théorème 1.1, on supposait seulement $m \geq 1$. Lorsque m est ≥ 2 (ce qui entraîne que c est nul), on a une congruence plus précise :

1.3 THÉORÈME. *Si* K *contient les racines quatrièmes de l'unité, on a* $N(\mathfrak{d}) \equiv 0, 1$ *ou* $4 \mod 8$.

La démonstration des théorèmes 1.1 et 1.3 se fait par réduction au cas où L/K est une extension quadratique pour laquelle $N(\mathfrak{d})$ est impair. Après un paragraphe 2 consacré à l'énoncé de quelques compléments sur les discriminants, nous effectuons cette réduction au paragraphe 3. L'énoncé dans le cas quadratique est démontré au paragraphe 4, sous la forme plus générale suivante :

Manuscrit reçu le 16 mars 1989, révisé le 29 mars 1989.

1.4 THÉORÈME. *Si L/K est une extension quadratique dont le discriminant relatif $\mathfrak{d}$ est de norme impaire, et si K contient une racine de l'unité d'ordre 2^m $(m \geq 1)$ on a $N(\mathfrak{d}) \equiv (-1)^c \mod 2^{m+1}$.*

Je remercie Jean-Pierre Serre pour ses remarques. En outre, c'est au cours d'une discussion avec lui qu'a été trouvée une démonstration du th.3.1 ne nécessitant aucune hypothèse de séparabilité résiduelle.

2. Compléments sur les discriminants. Dans ce paragraphe, K désigne un corps sur lequel aucune hypothèse particulière n'est faite, K_s une clôture séparable de K, et V un K-espace vectoriel muni d'une forme bilinéaire symétrique T non dégénérée. On se donne en outre d'une part une extension séparable finie L de K (on pourrait considérer plus généralement une algèbre étale sur K, c'est-à-dire un produit fini d'extensions séparables finies de K), et d'autre part un anneau de Dedekind A de corps des fractions K et un réseau M de A dans V (A-module de type fini engendrant V). Lorsque $V = L$, on prend pour forme T l'application $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ et pour M la clôture intégrale de A dans L.

Pour tout idéal premier non nul $\mathfrak{p}$ de A, le localisé $A_\mathfrak{p}$ de A en $\mathfrak{p}$ est un anneau de valuation discrète, et $M_\mathfrak{p} = A_\mathfrak{p} M$ est un $A_\mathfrak{p}$-module libre. Le discriminant pour T d'une base de ce module est bien défini dans $K^*/A_\mathfrak{p}^{*2}$; il en est de même de sa valuation $\lambda_\mathfrak{p} \in \mathbf{Z}$. En outre, $\lambda_\mathfrak{p}$ est nul pour presque tout $\mathfrak{p}$, ce qui permet de définir le discriminant $\mathfrak{d}_T(M) = \mathfrak{d}$ de T sur M : c'est l'idéal fractionnaire de A tel que $v_\mathfrak{p}(\mathfrak{d}) = \lambda_\mathfrak{p}$ pour tout idéal premier non nul $\mathfrak{p}$ de A. On définit de la même façon le discriminant $d_T(V) \in K^*/K^{*2}$ à partir d'une K-base de V. Sa valuation est définie modulo 2 en chaque idéal premier non nul de A.

2.1 PROPOSITION. *Pour tout idéal premier non nul $\mathfrak{p}$ de A, on a*

$$v_\mathfrak{p}(\mathfrak{d}) \equiv v_\mathfrak{p}(d_T(V)) \mod 2.$$

En effet, pour tout $\mathfrak{p}$, $d_T(V)$ est l'image dans K^*/K^{*2} du discriminant local défini dans $K^*/A_\mathfrak{p}^{*2}$.

Les considérations qui précèdent s'appliquent en particulier à l'extension L/K ; on obtient alors un discriminant $\mathfrak{d}_{L/K} = \mathfrak{d}$, qui est un idéal entier de K, et un discriminant $d_{L/K}$, qui est un élément de K^*/K^{*2} ; $d_{L/K}$ définit une extension de K de degré ≤ 2 (qui est purement inséparable si car $K = 2$).

Dans la suite, nous employons l'expression *extension quadratique* pour

désigner une sous-extension de degré 1 ou 2 de K_s/K. (On pourrait de façon plus intrinsèque considérer les classes d'isomorphisme d'algèbres étales de dimension 2.)

La théorie de Galois permet d'associer à L/K une telle extension quadratique. En effet, on peut faire du groupe de Galois G_K de K_s/K un groupe de permutation de degré $n = [L : K]$ en le faisant opérer sur l'ensemble des racines dans K_s du polynôme minimal d'un élément primitif de L/K, ou encore sur l'ensemble des K-homomorphismes de L dans K_s. On montre sans peine que l'on obtient dans tous les cas la même classe d'équivalence forte. Les signatures des permutations définissent alors un homomorphisme canonique $\varepsilon : G_K \to \{-1, +1\}$, auquel on associe une extension quadratique K'/K, qui définit elle-même un élément de K^*/K^{*2} (théorie de Kummer) si car K est $\neq 2$ et de $K/\wp(K)$ (théorie d'Artin-Schreier ; $\wp$ est l'application $x \mapsto x^2 - x$) si car $K = 2$.

Le résultat suivant est bien connu (voir par exemple Weil, [10], pp. 155-156) :

2.2 PROPOSITION. *Si car $K \neq 2$, on a $d_{K'/K} = d_{L/K}$ dans K^*/K^{*2} ; si car $K = 2$, $d_{L/K}$ est trivial.*

Démonstration. Le cas de la caractéristique 2 est évident, l'extension de degré 1 ou 2 définie par L/K devant être à la fois séparable et purement inséparable. Supposons maintenant car $K \neq 2$, et soit θ un élément primitif de L/K. Alors, $d_{L/K}$ est l'image dans K^*/K^{*2} du discriminant pour la forme $\mathrm{Tr}_{L/K}(xy)$ de la base $\{1, \theta, ..., \theta^{n-1}\}$ de L/K, discriminant égal à $\prod_{\tau<\sigma} (\tau\theta - \sigma\theta)^2$. (Dans ce produit, τ et σ parcourent l'ensemble, ordonné arbitrairement, des K-homomorphismes de L dans K_s.) Comme l'élément $\gamma = \prod(\tau\theta - \sigma\theta)$ de K_s vérifie la formule de transformation $s\gamma = \varepsilon(s)\gamma$ pour tout $s \in G_K$, on a $K' = K\sqrt{(\gamma)}$, **c.q.f.d.**

2.3 *Remarque.* On peut aussi donner une interprétation analogue de K'/K lorsque K est de caractéristique 2, à condition d'utiliser une forme quadratique convenable à la place de la forme bilinéaire $\mathrm{Tr}(xy)$ et de remplacer en outre l'espace vectoriel L par le produit $L \times K$ lorsque n est impair, cf. [1].

3. Réduction aux discriminants quadratiques. Nous conservons dans ce paragraphe les notations du paragraphe précédent.

3.1 THÉORÈME. *Il existe un idéal entier $\mathfrak{F}$ de K tel que $\mathfrak{d}_{L/K} = \mathfrak{d}_{K'/K} \cdot \mathfrak{F}^2$.*

Le fait que le quotient des discriminants de L/K et de K'/K soit le carré d'un idéal fractionnaire est une conséquence immédiate des prop. 2.1 et 2.2. Pour montrer que ce quotient est un idéal entier, nous nous servons du résultat suivant, que nous prouvons en adaptant l'idée utilisée par Schur dans [7] :

3.2 PROPOSITION. *Soit B un ordre de L. Si $d_{L/K}$ est non trivial, il existe un unique ordre B' de K' qui a même discriminant que B. (Dans le cas où $d_{L/K} = 1$, il faut remplacer K' par l'algèbre $K \times K$.)*

Le théorème 3.1 est une conséquence facile de la proposition 3.2, puisque, quelque soit B, $\mathfrak{d}_{K'/K}$ divise le discriminant de B'.

Pour prouver 3.2, nous examinons d'abord le cas particulier où B est un A-module libre. Choisissons une base $\{\omega_1, ..., \omega_n\}$ de B sur A. Le discriminant de B est le carré du déterminant $\det(\sigma_i\omega_j)$ $(\sigma_i \in \mathrm{Hom}(L, K_s))$. Ce déterminant est de la forme $\alpha - \beta$, où α (resp. β) désigne la somme des termes qui apparaissent dans le développement du déterminant avec le signe + (resp. le signe −). Un élément s du groupe G_K stabilise ou échange α et β selon que $\varepsilon(s)$ vaut +1 ou -1. Mais α et β sont les racines dans K_s du polynôme $f(X) = X^2 - (\alpha + \beta)X + \alpha\beta \in A[X]$. On a $K' = K(\alpha - \beta) = K(\alpha) = K(\beta)$, et l'ordre $A[\alpha] = A[\beta]$ de K' est l'ordre cherché : son discriminant, qui est engendré par le discriminant de f, est égal à $(\alpha - \beta)^2$, et coïncide donc avec celui de B. Le cas général se ramène tout de suite au cas précédent par localisation, ou en considérant l'ordre engendré sur A par les discriminants des sous-modules libres de B. Quant à l'unicité de l'ordre B', elle résulte simplement de ce que les ordres d'une algèbre quadratique étale sont classés par leurs conducteurs, **c.q.f.d.**

Dans le cas où l'on suppose les extensions résiduelles séparables, la divisibilité de $\mathfrak{d}_{L/K}$ par $\mathfrak{d}_{K'/K}$ peut également se démontrer en interprétant ces discriminants comme les conducteurs d'Artin respectifs du caractère de permutation de G_K associé à L/K et de son déterminant, et en appliquant le théorème suivant :

3.3 THÉORÈME. (Serre) *Soit ρ une représentation de G_K dans un espace vectoriel complexe V. Alors, le conducteur du déterminant $\det_\rho$ de ρ divise celui de ρ.*

Comme le schéma de démonstration qui est proposé en exercice dans [5], p. 79, est un peu succinct, nous donnons une démonstration un peu détaillée ci-dessous.

Par localisation et complétion, on se ramène au cas où K est complet.

La représentation ρ relève une représentation encore notée ρ du groupe de Galois G d'une extension finie L/K. Notons alors G_i ($i \geq 0$) la suite des groupes de ramification de L/K, et soit g_i l'ordre de G_i. L'exposant v de l'idéal de valuation de K dans le conducteur de ρ est alors donné par la formule (cf. [5], p. 13) :

$$v = \sum_{i \geq 0} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}.$$

L'exposant v' relatif à la représentation $\det_\rho$ s'obtient par une formule analogue, dans laquelle l'espace V est remplacé par sa puissance extérieure $W = \bigwedge^n V$. Nous devons prouver l'inégalité $v \geq v'$, et, pour cela, il suffit de montrer que l'on a $\operatorname{codim} V^{G_i} \geq \operatorname{codim} W^{G_i}$ pour tout i. C'est vrai lorsque G_i opère trivialement sur V parce que les deux membres sont alors nuls, et lorque G_i n'opère pas trivialement parce que $\operatorname{codim} W^{G_i}$ est ≤ 1, **c.q.f.d.**

3.4 *Remarque.* Une fois les discriminants de L/K et de K'/K interprétés en termes de conducteurs, on obtient une autre démonstration du fait que leur quotient est un carré en appliquant le théorème de Serre sur les conducteurs d'Artin des caractères réels ([8]). On peut aussi procéder en sens inverse, et utiliser ce théorème pour associer à tout caractère réel de G_K (i.e. différence des caractères de deux représentations de G_K à noyaux ouverts réalisables sur $\mathbf{R}$) un conducteur $f(\chi) \in K^*/K^{*2}$: il suffit de considérer l'extension M/K associée par la théorie de Galois au noyau du caractère

$$\det_\chi : G_K \mapsto \{-1, +1\},$$

et de poser $f(\chi) = d_{M/K} \mod K^{*2}$. On obtient une fonction additive sur le groupe des caractères virtuels de G_K, qui vérifie en outre une formule d'induction analogue à la formule de transitivité des discriminants, et joue vis-à-vis du conducteur d'Artin le rôle que joue $d_{L/K}$ vis-à-vis de $\mathfrak{d}_{L/K}$.

Il résulte immédiatement de 3.1 (et cela peut aussi se voir directement) que, si $\mathfrak{d}_{L/K}$ est divisible par un idéal premier $\mathfrak{p}$ de K au-dessus de 2, il est alors divisible par $\mathfrak{p}^2$: il suffit de remarquer qu'un tel idéal, s'il divise $\mathfrak{d}_{K'/K}$, n'est pas modérément ramifié dans K'/K.

Supposons maintenant que K soit un corps de nombres. Les résultats précédents s'appliquent avec $A = \mathbf{Z}_K$, clôture intégrale de $\mathbf{Z}$ dans K. Si la norme de $\mathfrak{d}_{L/K}$ est paire, elle est divisible par 4 d'après ce que nous venons de voir. Supposons-la impaire. On a alors $N(\mathfrak{F}^2) \equiv 1 \mod 8$. Pour

achever la réduction au cas quadratique des théorèmes 1.1 et 1.3, il suffit de montrer que les nombres de places complexes w dans L et w' dans K' qui sont au-dessus d'une place réelle donnée v de K ont même parité. Or, à la place v, $d_{L/K}$ et $d_{K'/K}$ ont pour signes respectifs $(-1)^w$ et $(-1)^{w'}$. Comme ces deux discriminants ont même image dans K^*/K^{*2}, on a bien $w \equiv w' \mod 2$.

4. Démonstration du théorème 1.4. Dans ce paragraphe, m désigne un entier > 0, K un corps de nombres contenant une racine de l'unité ζ d'ordre 2^m et L une extension *quadratique* de K dans laquelle les idéaux premiers ramifiés sont tous de norme *impaire*. Nous désirons prouver la congruence $N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) \equiv (-1)^c \mod 2^{m+1}$.

Écrivons $L = K(\sqrt{\gamma})$, et $(\gamma) = \mathfrak{a} \cdot \mathfrak{b}^2$, où $\mathfrak{a}$ est un idéal entier sans facteur carré de K. On a alors $\mathfrak{d}_{L/K} = \mathfrak{a}$. Puisque K contient le corps $\mathbb{Q}(\zeta)$, les idéaux premiers de K qui ne divisent pas (2) sont de norme congrue à 1 mod 2^m, donc à 1 ou $1 + 2^m \mod 2^{m+1}$. Soit S (resp. T) l'ensemble des diviseurs premiers de $\mathfrak{a}$ dont la norme est congrue à $1 + 2^m$ (resp. à 1) mod 2^{m+1}, et soit s le cardinal de S. On a $N(\mathfrak{a}) \equiv 1 + s\,2^m \mod 2^{m+1}$, et tout revient à montrer que s et c ont même parité. Pour cela, calculons les symboles de Hilbert quadratiques $(\alpha, \zeta)_v$ aux différentes places v de K. Ils sont égaux à 1 lorsque v est complexe, ce qui est le cas de toutes les places infinies de K lorsque m est > 1, et lorsque v est finie et non ramifiée dans L/K. Lorsque v est réelle, on a $m = 1$, $\zeta = -1$, et $(\alpha, -1)_v$ prend la valeur -1 si et seulement si α est < 0 à v, ce qui a lieu exactement lorsque v se prolonge à L en une place non réelle. Reste à examiner le cas où v est une place finie correspondant à un idéal premier $\mathfrak{p}$ de K ramifié dans L. Alors, $\mathfrak{p}$ divise $\mathfrak{a}$, et, comme $\mathfrak{p}$ est modérément ramifié, le symbole ne dépend que de l'image de ζ dans le quotient $(\mathbb{Z}_K/\mathfrak{p})^*$: il vaut $+1$ lorsque ζ est un carré modulo $\mathfrak{p}$ et -1 dans le cas contraire ; il prend donc les valeurs $+1$ sur T et -1 sur S. La formule du produit entraîne alors tout de suite le théorème 1.4, les contributions respectives à ce produit des places finies et infinies étant $(-1)^s$ et $(-1)^c$, **c.q.f.d.**

La démonstration que nous venons de donner du th. 1.4 est de type "corps de classes". Voici une démonstration de type "Kummer" qui s'applique dans le cas habituel de la congruence modulo 4.

Soit donc $L = K(\sqrt{\gamma})$ une extension quadratique de K, avec $(\gamma) = \mathfrak{a} \cdot \mathfrak{b}^2$, où $\mathfrak{a}$ est un idéal entier sans facteur carré de $\mathbb{Z}_K$. Quitte à remplacer $\mathfrak{b}$ par un idéal équivalent, on peut le supposer entier et premier à 2. Pour un idéal $\mathfrak{p}$ au-dessus de 2 dans K, "$v_\mathfrak{p}(\mathfrak{d})$ pair" équivaut à "$v_\mathfrak{p}(\mathfrak{a}) = 0$", et,

lorsque cette condition est vérifiée, " $v_{\mathfrak{p}}(\mathfrak{d}) = 0$ " équivaut à " α est congru à un carré modulo $\mathfrak{p}^{v_{\mathfrak{p}}(4)}$ " (cf. [4], §39). Il en résulte que, lorsque L/K est non ramifiée en 2, α est congru à un carré modulo 4 (que l'on pourrait du reste choisir égal à 1). Cela entraîne la congruence $N(\alpha) \equiv 1 \mod 4$. Mais $N(\alpha) = (-1)^c . |N(\alpha)|$, et $|N(\alpha)|$ est la norme de l'idéal principal (α). On en déduit

$$N(\mathfrak{a}) \equiv N(\mathfrak{a}).N(\mathfrak{b})^2 \equiv |N(\alpha)| \equiv (-1)^c \mod 4.$$

4.1 *Remarque.* Lorsque $m = 2$, les trois classes modulo 8 *a priori* possibles compte tenu du théorème 1.3 pour une extension quadratique sont effectivement réalisables, comme on le voit en prenant $K = \mathbb{Q}(i)$, les valeurs de $N(\mathfrak{d})$ pour $\alpha = i$, $1 + 4i$ et $1 + 2i$ étant respectivement 16, 17 et 20.

4.2 *Remarque.* Signalons que la congruence de Stickelberger a été considérée par Fröhlich dans le cadre des *discriminants idéliques* ([3], [4]). Nous laissons au lecteur le soin de vérifier que, pour un corps global, la connaissance du discriminant idélique est équivalente à celle du couple $(\mathfrak{d}_T(M), d_T(V))$ qui a été utilisé tout le long de cet article.

Bibliographie

[1] A-M. Bergé et J.Martinet, *Formes quadratiques et extensions en caractéristique 2*, Ann. Inst. Fourier **35, 2** (1985), 57–77.

[2] A. Fröhlich, *Discriminants of algebraic number fields*, Math. Z. **74** (1960), 18–28.

[3] A. Fröhlich, *Ideals in an extension field as modules over the algebraic integers in a finite number field*, Math. Z. **74** (1960), 29–38.

[4] E. Hecke, "Vorlesungen über die Theorie der algebraischen Zahlen," Chelsea, New York, 1948 (éd. originale : 1923).

[5] J. Martinet, *Character theory and Artin L-functions*, "Algebraic Number Fields (A. Fröhlich, éd.)," Academic Press, London, New York, 1977, pp. 2–87.

[6] J. Martinet, *Petits discriminants des corps de nombres*, London Math. Soc. Lecture Notes Series **56** (1982), 151–193.

[7] I.Schur, *Elementarer Beweis eines Satzes von L. Stickelberger*, Math. Z. **29** (1929), 87-88 (= Ges. Abh., vol. III, pp. 87-88).

[8] J-P. Serre, *Conducteurs d'Artin des caractères réels*, Invent. Math. **14** (1971), 173–183.

[9] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Int. Cong. Zürich (1897), 182–193.

[10] A. Weil, "Automorphic forms and Dirichlet Series," Springer Lecture Notes 189, Heidelberg, 1971.

Mots clefs: corps de nombres, discriminants.

Centre de Recherche en Mathématiques de Bordeaux, Université Bordeaux I
C.N.R.S. U.A. 226
351, cours de la Libération
33405 Talence Cedex, FRANCE.