[11] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Annalen 37 (1890), pp. 321–367.
[12] K. Williams, *A rational octic reciprocity law*, Pacific J. Math. 63 (1976), pp. 564–570.
[13] — *Note on Burde's rational biquadratic reciprocity law*, Canad. Math. Bull. 20 (1977), pp. 145–146.
[14] P. Wu, *A rational reciprocity law*, Ph. D. thesis, Univ. S. California, 1975.

*Received on 4. 12. 1978* (1121)

ACTA ARITHMETICA
XXXIX (1981)

# Corps cubiques de discriminant donné

par

PH. SATGÉ (Caen)

**Introduction.** Soit $d \neq -3$ un discriminant de corps quadratique imaginaire et $q \neq 2, 3$ un nombre premier. On sait ([2], [3], [4] par exemple) que la congruence $q \equiv \left(\frac{d}{q}\right) \bmod 3$ est une condition nécessaire pour que $dq^2$ soit un discriminant de corps cubique, et que cette condition est suffisante si 3 ne divise pas le nombre de classes de $Q(\sqrt{d})$. L'exemple $d = -23$ et $q = 5$ montre que cette congruence n'est plus suffisante lorsque 3 divise le nombre de classes de $Q(\sqrt{d})$: en effet, on a $5 \equiv \left(\frac{-23}{5}\right) \bmod 3$ mais $-23 \cdot 5^2 = -575$ n'est pas un discriminant de corps cubique. Depuis le mémoire de Hasse [2], la question suivante est donc posée: soit $d$ un discriminant de corps quadratique imaginaire dont le nombre de classes est divisible par 3; quels sont les nombres premiers $q$ tels que $dq^2$ est discriminant d'un corps cubique? Nous répondons ici à cette question (théorème du § 4): si $\delta$ est le discriminant du corps $Q(\sqrt{-3d})$, il existe un ensemble fini de formes quadratiques binaires de discriminant $3^r\delta$, avec $r = 0$, 2 ou 4, telles que $dq^2$ est un discriminant de corps cubique si et seulement si l'on a $q \equiv \left(\frac{d}{q}\right) \bmod 3$ et si $q$ est représenté par l'une de ces formes. Dans le cas $d = -23$ par exemple, nous montrons que cet ensemble de formes peut être réduit à la forme $X^2 + 3XY - 153Y^2$; ainsi $-23q^2$ est un discriminant de corps cubique si et seulement si $q$ est congru à $\left(\frac{-23}{q}\right) \bmod 3$ et est de la forme $x^2 + 3xy - 153y^2$ avec $x$ et $y$ entiers rationnels.

**Notations.** Soit $k$ un corps quadratique imaginaire de discriminant $d \neq -3$ et $q$ un nombre premier différent de 2 et 3. On désigne par $J$, $J_Q$ les groupes des idèles des corps $k$ et $Q$ (où $Q$ est le corps des rationnels), par $W_1$ le sous groupe de $J$ formé des idèles dont les composantes en toutes les places finies sont des unités, et par $W_q$ le sous groupe de $W_1$ formé

des idèles dont les composantes aux places divisant $q$ sont des unités principales (i.e. sont congrus à 1 modulo l'idéal de la place). Enfin nous notons $\tilde{k}$ le corps $Q(\sqrt{-3d})$. De plus tous les corps cubiques envisagés ici sont non galoisiens, non totalement réels et considérés à conjugaison près.

**1.** En traduisant les résultas de [2] et [4] dans le langage des idèles, on obtient:

(a) Si $r$ désigne le 3-rang du groupe $J/(k^*W_qJ_Q)$, alors il y a $(3^r-1)/2$ corps cubiques (comptés à conjugaison près) dont le discriminant divise $dq^2$.

(b) $d$ est le seul diviseur strict de $dq^2$ susceptible d'être discriminant d'un corps cubique.

(c) Si $h$ est le 3-rang de groupe des classes de $k$, il y a $(3^h-1)/2$ corps cubiques de discriminant $d$.

De ceci résulte que l'inégalité stricte $r > h$ est la condition d'existence d'un corps cubique de discriminant $dq^2$.

**2.** Désignons par $J^3$ le sous groupe des cubes de $J$; posons $cl_q = J/(k^*W_qJ_QJ^3)$ et $cl = J/(k^*W_1J^3)$. Ces deux quotients sont des espaces vectoriels sur le corps à 3 éléments; leurs dimensions sont respectivement les entiers $r$ et $h$ introduit au paragraphe précédent.

La surjection canonique $cl_q \to cl$ a pour noyau le groupe $(k^*W_1J^3)/(k^*W_qJ_QJ^3)$, qui est isomorphe à $W_1/\big((k^*W_qJ_QJ^3)\cap W_1\big)$. Mais on a $J_Q = Q^*\cdot(W_1\cap J_Q)$ et $W_q \subset W_1$, donc on a

$$(k^*W_qJ_QJ^3)\cap W_1 = W_q\cdot(W_1\cap J_Q)\cdot\big((k^*J^3)\cap W_1\big).$$

En posant

$$X = W_1\Big/\Big(W_q\cdot(W_1\cap J_Q)\cdot\big((k^*J^3)\cap W_1\big)\Big),$$

on a donc la suite exacte d'espaces vectoriels

$$0 \to X \to cl_q \to cl \to 0$$

qui montre que l'on a $r > h$ si et seulement si $X$ est non nul.

Pour étudier $X$, introduisons $Y = W_1/(W_q\cdot(W_1\cap J_Q)\cdot W_1^3)$ où $W_1^3$ est le groupe des cubes de $W_1$, i.e. $W_1^3 = W_1\cap J^3$. Il résulte de [2] et [4] que l'espace vectoriel $Y$ est de dimension 1 ou 0 sur le corps à 3 éléments suivant que $q$ est ou n'est pas congru à $\left(\frac{d}{q}\right)$ mod 3.

D'autre part on a une surjection naturelle de $Y$ sur $X$, donc $X$ est non trivial si et seulement si les deux conditions suivantes sont réalisées:

(I) $q \equiv \left(\frac{d}{q}\right) \bmod 3$ (c'est la condition nécessaire énoncée dans l'introduction).



(II) la surjection $Y \to X$ est un isomorphisme.

Les résultats de ces deux paragraphes se résument donc dans la proposition suivante:

PROPOSITION 1. *Les conditions* (I) *et* (II) *énoncées ci-dessus sont équivalentes à l'existence d'un corps cubique de discriminant* $dq^2$.

Remarque. Lorsqu'il existe un corps cubique de discriminant $dq^2$, il y en a exactement $3^h$ (à conjugaison près) qui ont ce discriminant: en effet $X$ est alors de dimension 1 et donc $r = h+1$; il en résulte alors des points (a), (b), et (c), du § 1 qu'il y a $\dfrac{3^{h+1}-1}{2} - \dfrac{3^h-1}{2} = 3^h$ corps cubiques de discriminant $dq^2$.

**3.** Pour étudier la condition (II) du paragraphe précédent, introduisons la définition suivante: un élément de $k^*$ est appelé pseudo-cube si l'idéal qu'il engendre est le cube d'un idéal. On a la proposition suivante:

PROPOSITION 2. *La surjection* $Y \to X$ *est un isomorphime si et seulement si tous les pseudo-cubes de* $k$ *sont des cubes dans les complétés* $k_v$ *de* $k$ *aux places* $v$ *divisant* $q$.

Démonstration. Si $z$ est une idèle de $k$, nous notons $z'$ l'image de $z$ par l'élément non trivial de $\mathrm{Gal}(k/Q)$ et pour une place $w$ de $k$, nous notons $z_w$ la $w$-composante de $z$. Il est clair que la surjection $Y \to X$ est bijective si et seulement si l'on a l'inclusion $(k^*J^3)\cap W_1 \subset W_q\cdot(W_1\cap J_Q)\cdot W_q^3$.

(a) Supposons cette inclusion. Soit $\alpha$ un pseudo-cube de $k$. Par définition il existe un idèle $y$ tel que $x = \alpha y^3$ soit dans $W_1$. On a alors $x \in (k^*J^3)\cap W_1$ et donc (par hypothèse) $x \in W_q\cdot(W_1\cap J_Q)\cdot W_1^3$ ce qu'on peut écrire

$$\alpha y^3 = \varphi\psi\theta^3 \quad \text{avec} \quad \varphi \in W_q,\ \psi \in W_1\cap J_Q \text{ et } \theta \in W_1. \tag{1}$$

L'action de l'élément non trivial de $\mathrm{Gal}(k/Q)$ sur l'égalité (1) donne

$$\alpha' y'^3 = \varphi'\psi\theta'^3, \tag{1'}$$

les groupes $W_q$ et $W_1$ étant globalement invariant par $\mathrm{Gal}(k/Q)$ on a $\varphi' \in W_q$ et $\theta' \in W_1$.

Les composantes $\varphi_v$ et $\varphi'_v$ des idèles $\varphi$ et $\varphi'$ sont des unités principales de $k_v$, donc sont des cubes dans $k_v$ (puisque la caractéristique $q$ du corps résiduel de $k_v$ a été supposée différente de 3). D'autre part le produit $\alpha\alpha'$ est la norme du pseudo-cube $\alpha$, donc est un cube. Multiplions (1) et (1') et prenons les $v$-composantes; il vient:

$$\alpha_v\alpha'_v = \varphi_v\varphi'_v\psi_v^2\theta_v^3\theta_v'^3. \tag{2}$$

Mais on a $a_v a'_v = (aa')_v$ donc $a_v a'_v$ est un cube dans $k_v$ et $\varphi_v$ et $\varphi'_v$ sont des cubes dans $k_v$ comme nous venons de le voir. L'égalité (2) montre donc que $\psi_v^2$, et donc $\psi_v$, est un cube. Il reste alors à prendre les $v$-composantes dans l'égalité (1) pour constater que $a$ est un cube dans $k_v$.

(b) Supposons réciproquement que les pseudo-cubes sont des cubes dans les complétés de $k$ aux places divisant $q$. Soit $x \in (k^* J^3) \cap W_1$. On a $x = \alpha y^3$ avec $\alpha \in k^*$ et $y \in J$, et $a$ est un pseudo-cube puisque $\alpha y^3 \in W_1$.

Définissons les idèles $\varphi$ et $\psi$ par $\varphi_w = 1$ et $\psi_w = x_w$ pour toute place $w$ ne divisant pas $q$ et $\varphi_v = x_v$ et $\psi_v = 1$ pour les places $v$ divisant $q$. On a $x = \varphi\psi$ et $\psi \in W_q$. D'autre part, pour toute place $v$ divisant $q$, on a par hypothèse que $a_v$ est un cube dans $k_v$. Il en résulte que $\varphi_v = a_v y_v^3$ est un cube dans $k_v$; comme c'est aussi une unité, l'idèle $\varphi$ est dans $W_1^3$. Par conséquent, $x = \varphi\psi$ est dans $W_q \cdot (W_1 \cap J_Q) \cdot W_1^3$, ce qui achève la démonstration.

Remarque. En désignant toujours par $h$ le 3-rang du groupe des classes de $k$, le quotient du groupe des pseudo-cubes de $k$ par le groupe des cubes est un espace vectoriel de dimension $h$ sur le corps à trois éléments. Pour vérifier que tous les pseudo-cubes sont localement des cubes, il suffit de faire la vérification pour une base de cet espace vectoriel, i.e. pour $h$ pseudo-cubes bien choisis. En particulier, si $h = 0$, il n'y a rien à vérifier et la surjection $Y \to X$ est toujours bijective. La proposition 1, dans ce cas, exprime uniquement que la congruence $q \equiv \left(\frac{d}{q}\right) \bmod 3$ est nécessaire et suffisante pour que $dq^2$ soit discriminant d'un corps cubique.

**4.** Soit $a$ un pseudo-cube de $k$. Posons $k' = k(\sqrt{-3})$ et $N'_a = k'(\sqrt[3]{a})$. On vérifie aisément que $N'_a$ est une extension galoisienne de $\boldsymbol{Q}$ et une extension abélienne de $\tilde{k} = \boldsymbol{Q}(\sqrt{-3d})$. Il existe donc une extension cubique $N_a$ de $\tilde{k}$ et une seule qui, composée avec $k'$, donne $N'_a$. On montre facilement que $N_a$ est une extension galoisienne de $\boldsymbol{Q}$ dont le groupe de Galois est le groupe symétrique.

Soit $v'$ une place de $k'$ au dessus de $q$. Par la théorie de Kummer, on voit que $v'$ se décompose dans $N'_a$ si et seulement si $a$ est un cube dans le complété $k'_{v'}$ que $k'$ en $v'$. Désignons par $v$ et $\tilde{v}$ les places de $k$ et $\tilde{k}$ en dessous de $v'$ et par $k_v$ et $\tilde{k}_{\tilde{v}}$ les complétés correspondants. L'extension $k'/k$ étant de degré 2, le nombre $a$ est un cube dans $k'_{v'}$ si et seulement si c'est un cube dans $k_v$. L'extension $k'/\tilde{k}$ étant aussi de degré 2, la place $v'$ se décompose dans $N'$ si et seulement si $\tilde{v}$ se décompose dans $N_a$. Ceci, ajouté au fait que les nombres premiers $q$ congrus à $\left(\frac{d}{q}\right) \bmod 3$ sont totalement décomposés dans $\tilde{k}$, aux propositions 1 et 2 et à la remarque du § 3, se résume dans la proposition suivante:



Proposition 3. *Soit $q \neq 2, 3$ un nombre premier congru à $\left(\frac{d}{q}\right) \bmod 3$. L'entier négatif $dq^2$ est discriminant d'un corps cubique si et seulement si $q$ est totalement décomposé dans les corps $N_{a_i}$ pour $i = 1, \ldots, h$ où les $(a_i)_{i=1,\ldots,h}$ forment une base des pseudo-cubes de $k$ modulo les cubes.*

Pour tout pseudo-cube $a$ de $k$, le corps $\tilde{k}$ est la clôture abélienne de $\boldsymbol{Q}$ dans $N_a$. On sait donc [5] qu'il existe un ensemble fini de formes quadratiques tel que la représentation d'un nombre premier $q$ décomposé dans $\tilde{k}$ par l'une de ces formes soit équivalente à la décomposition totale de $q$ dans $N_a$. Ceci permet de reformuler la proposition 3 sous la forme suivante:

Théorème. *Soit $d \neq -3$ un discriminant de corps quadratique imaginaire. Il existe un ensemble fini de formes quadratiques tel que pour tout nombre premier $q \neq 2, 3$ il y ait équivalence entre les propriétés suivantes:*

(i) *$dq^2$ est discriminant d'un corps cubique.*

(ii) *$q \equiv \left(\frac{d}{q}\right) \bmod 3$ et $q$ est représenté par l'une de ces formes.*

Remarque. Pour la généralisation indiquée dans l'introduction, il faut remplacer pseudo-cube par pseudo-puissance $p^{\text{ième}}$, prendre pour $k'$ le corps engendré sur $k$ par les racines $p^{\text{ième}}$ le l'unité et pour $N'_a$ le corps $k'(\sqrt[p]{a})$. Le corps $\tilde{k}$ est alors cyclique de degré $p-1$ sur $\boldsymbol{Q}$ et donc les formes qui interviennent sont des formes homogènes de degré $p-1$ à $p-1$ variables.

**5.** Exemple numérique. Prenons $d = -23$. Avec les notations précédentes on a $h = 3$. Il faut donc trouver un pseudo-cube qui n'est pas un cube. Pour cela on remarque que, dans $k = \boldsymbol{Q}(\sqrt{-23})$, le nombre 2 est décomposé en le produit de deux idéaux non principaux. L'entier $a = (3+\sqrt{-23})/2$, qui a pour norme 8, engendre le cube de l'un d'eux et donc est un pseudo-cube. Ce n'est pas un cube car aucun entier de $k$ n'a 2 comme norme.

Posons alors $N'_a = N'$ et $N_a = N$. Le conducteur de $N/\tilde{k}$ est l'idéal principal engendré par 3 (comme on le voit en calculant d'abord le conducteur de l'extension de Kummer $N'/k'$ puis en descendant). Les formes quadratiques associées par [5] au corps $N$ sont donc les formes normes associées aux classes d'idéaux de l'ordre de $\tilde{k}$ de conducteur 3. Avec les notations de [5], ce sont les formes associées à $cl(\theta_3)$ qui est isomorphe à $I(3)/N(3)$. Ce groupe est cyclique d'ordre 3 et l'action de $\mathrm{Gal}(\tilde{k}/\boldsymbol{Q})$ le partage en deux orbites: une formée de la classe neutre et l'autre formée des deux classes d'ordre 3.

Posons

$$\omega = \frac{1+\sqrt{69}}{2} \quad \text{et} \quad \overline{\omega} = \frac{1-\sqrt{69}}{2}.$$

Le couple $\{1, 3\omega\}$ est une base sur $\boldsymbol{Z}$ de $\theta_3$, donc la forme norme associée à la première orbite est $(X+3\omega Y)(X+3\overline{\omega}Y)$ soit $X^2+3XY-153Y^2$. Pour trouver la forme norme associée à l'autre orbite, on remarque que l'idéal principal de $\tilde{k}$ engendré par $5+\omega$ n'est pas dans $N(3)$ et que son intersection avec $\theta_3$ a pour base sur $\boldsymbol{Z}$ le couple $\{13, 15+3\omega\}$ (en effet, on voit, en développant, que $(x+y\omega)(5+\omega)$ est dans $\theta_3$ si et seulement si $3|x$; on en déduit que le couple $\{17+6\omega, 15+3\omega\}$ est une base sur $\boldsymbol{Z}$ de cette intersection et donc que $\{13, 15+3\omega\}$ est aussi une base de cette intersection). La norme de $5+\omega$ étant 13, la forme norme de cette deuxième orbite est

$$\frac{1}{13}\left(13X+(15+3\omega)Y\right)\left(13X+(15+3\overline{\omega})Y\right) \quad \text{soit} \quad 13X^2+33XY+9Y^2.$$

Il résulte donc de [5] et de ce travail que les nombres premiers $q \neq 2, 3$ et congrus à $\left(\frac{-23}{q}\right)$ mod 3 sont représentés par une et une seule de ces deux formes et que $-23q^2$ est discriminant ou n'est pas discriminant d'un corps cubique suivant que $q$ est représenté par la première ou la seconde de ces formes.

Sur les 168 nombres premiers plus petit que 1000, il y en a 85 qui vérifient la condition $q \equiv \left(\frac{-23}{q}\right)$ mod 3. Parmi ces derniers, 26 sont représentés par la forme $X^2+3XY-153Y^2$ et les 59 autres par la forme $13X^2+33XY+9Y^2$. La liste des 26 qui sont représentés par la première forme est la suivante:

83, 113, 137, 149, 151, 163, 307, 397, 409, 467, 521, 541, 547, 557, 601, 617, 641, 673, 797, 811, 823, 859, 911, 967, 977, 997.

Il y a donc 3 corps cubiques non conjugués de discriminant $-23\cdot(83)^2$, $-23\cdot(113)^2$, ..., $-23\cdot(997)^2$. Le dernier de ces discriminants est plus grand que 16 000 000, nombre qui sort des tables connues.

## Bibliographie


[1] I. O. Angel, *A table of complex cubic fields*, Bull. London Math. Soc. 5 (1973), p. 37–38.

[2] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper*, Math. Zeitschr. 31 (1930), p. 565–582.





[3] J. J. Payan et J. Martinet, *Sur les extensions cubiques non galoisiennes*, Journ. Reine Angew. Math. 228 (1967), p. 15–37.

[4] Ph. Satgé, *Corps de discriminant donné*, Thèse de 3ème cycle, Faculté des Sciences d'Orsay, 1972.

[5] — *Décomposition des nombres premiers dans des extensions non abéliennes*, Ann. Inst. Fourier 27 (1977), fasc. 4, p. 1–8.

[6] R. Smadja, *Calculs effectifs sur les ideaux de corps de nombres algébriques*, Publication de l'Université d'Aix-Marseille, Mars 1976.



U.E.R. DE MATHÉMATIQUES
FACULTÉ DES SCIENCES DE CAEN
Esplanade de la Paix
14032 Caen Cedex


*Reçu le 30. 1. 1979* (1131)