MÉMORIAL DES SCIENCES MATHÉMATIQUES

T. NAGELL

L'analyse indéterminée de degré supérieur

Mémorial des sciences mathématiques, fascicule 39 (1929)

<http://www.numdam.org/item?id=MSM_1929__39__1_0>

MÉMORIAL

DES

SCIENCES MATHÉMATIQUES

PUBLIÉ SOUS LE PATRONAGE DE

L'ACADÉMIE DES SCIENCES DE PARIS,

DES ACADÉMIES DE BELGRADE, BRUXELLES, BUCAREST, COÏMBRE, CRACOVIE, KIEW, MADRID, PRAGUE, ROME, STOCKHOLM (FONDATION MITTAG-LEFFLER), DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE, AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

DIRECTEUR :

Henri VILLAT

Correspondant de l'Académie des Sciences de Paris,
Professeur à la Sorbonne,
Directeur du « Journal de Mathématiques pures et appliquées ».

FASCICULE XXXIX

L'analyse indéterminée de degré supérieur

PAR M. T. NAGELL

Docteur ès Sciences, chargé de cours à l'Université d'Oslo.

PARIS

GAUTHIER-VILLARS ET Cie, ÉDITEURS

LIBRAIRES DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE

Quai des Grands-Augustins, 55.

1929

AVERTISSEMENT

La Bibliographie est placée à la fin du fascicule, immédiatement avant la Table des Matières.

L'ANALYSE INDÉTERMINÉE

DE DEGRÉ SUPÉRIEUR

Par M. T. NAGELL,
Docteur ès sciences, chargé de cours à l'Université d'Oslo.

I. — Introduction.

1. Les problèmes de l'Analyse indéterminée. — On appelle Analyse indéterminée la partie de la théorie des nombres qui s'occupe des solutions en *nombres rationnels* ou en *nombres entiers* d'une ou de plusieurs équations. Le problème le plus important de ce domaine est l'étude des solutions rationnelles ou entières $x, y, z, \ldots$ de l'équation

$$f(x, y, z, \ldots) = 0,$$

où f est une fonction entière rationnelle de $x, y, z, \ldots$ à coefficients rationnels ou entiers. On peut, par exemple, demander si cette équation possède un nombre fini ou une infinité de solutions; ou l'on peut demander une méthode pour déterminer toutes les solutions. Dans le cas d'une équation homogène, le problème de trouver les solutions rationnelles coïncide avec le problème de trouver les solutions entières.

Au lieu d'une seule fonction f, on peut prendre un nombre fini de fonctions entières rationnelles et demander les solutions rationnelles ou entières $x, y, z, \ldots$ du système simultané

$$f_1(x, y, z, \ldots) = 0, \quad f_2(x, y, z, \ldots) = 0, \quad \ldots, \quad f_n(x, y, z, \ldots) = 0.$$

On peut évidemment généraliser ces problèmes dans plusieurs directions; on peut, par exemple, demander les solutions en nombres entiers ou fractionnaires d'un corps algébrique donné: et l'on peut

remplacer les fonctions f_i par d'autres fonctions qui ne sont pas nécessairement des polynomes.

Les géomètres grecs ont déjà étudié de tels problèmes. On doit surtout mentionner Diophante d'Alexandrie (environ 250 ans après J.-C.), qui a traité un grand nombre d'équations indéterminées dans son livre arithmétique [4]. Mais c'est Pierre de Fermat qui doit être considéré comme le vrai fondateur de cette discipline. En effet, ses idées fécondes dominent encore aujourd'hui l'Analyse indéterminée.

Depuis les importants travaux de Euler, Lagrange, Legendre, Gauss et d'autres, il existe une théorie classique des équations indéterminées du premier et du deuxième degré.

Le présent fascicule sera consacré aux équations indéterminées de degré supérieur, c'est-à-dire de degré $\geqq 3$. Il existe un très grand nombre de travaux sur ce sujet. On trouvera la bibliographie complète dans l'important Ouvrage de L. E. Dickson (p. 59). Mais la grande majorité des résultats sont trop spéciaux et sans importance. En général, on a seulement traité des cas numériques et presque toujours avec des méthodes spéciales qui ne sont pas susceptibles de généralisation. On s'est surtout intéressé à trouver des équations qui sont impossibles, sauf pour des valeurs triviales. Malgré les efforts de nombreux géomètres, les résultats sont jusqu'ici incomplets. L'image que nous offre l'ensemble des résultats de l'Analyse indéterminée est très hétérogène. Les méthodes varient considérablement d'un problème à l'autre et l'on utilise des ressources de domaines très différents : fonctions elliptiques et algébriques, transformations birationnelles, théorie des groupes, nombres algébriques et théorie des idéaux.

La plupart des travaux les plus importants s'occupent des propriétés arithmétiques des courbes algébriques planes, c'est-à-dire qu'ils traitent les problèmes suivants : Étant donnée la courbe algébrique plane (de degré $\geqq 3$),

$$f(x, y) = 0 \tag{1}$$

à coefficients rationnels, trouver : 1° les points à coordonnées rationnelles, les *points rationnels*, et 2° les points à coordonnées entières, les *points entiers* de cette courbe. Si

$$F(x, y, z) = 0 \tag{2}$$

est l'équation de la courbe en coordonnées homogènes, il est évident que le premier problème revient au problème de résoudre en nombres entiers x, y, z l'équation (2). Pour $z = 0$, l'équation $F(x, y, 0) = 0$ donne les points rationnels qui sont à l'infini. Il y a lieu de remarquer que, dans ce problème, c'est plutôt le genre que le degré de la courbe qui intervient. On a établi des résultats très intéressants sur les courbes de genre 0 et de genre 1. Ces résultats, qui seront exposés dans le Chapitre II, sont surtout dus à Poincaré, Hurwitz, Hilbert, Maillet et Mordell.

Le deuxième problème est, en général, beaucoup plus difficile que le premier. Tout d'abord, il se pose la question de savoir reconnaître si la courbe admet une infinité ou seulement un nombre limité de points entiers. Cette question n'est pas complètement résolue; mais il semble que les courbes ayant une infinité de points entiers soient exceptionnelles. On connaît des classes très étendues où il n'y a qu'un nombre limité de points entiers. Cependant, c'est seulement dans un petit nombre de cas qu'on sait effectivement déterminer tous les points entiers (*cf.* les n^{os} 6, 9, et 10); on ne peut même assigner une limite supérieure du nombre des points entiers en fonction des coefficients de la courbe que dans des cas exceptionnels (*cf.* le n^{o} 9).

Ces résultats, dont les plus importants sont dus à Thue et à Siegel, seront exposés dans le Chapitre III.

Hors les resultats sur les équations homogènes à trois variables qui sont exposés dans le Chapitre II, il n'existe pas beaucoup de résultats généraux sur les équations indéterminées à trois ou plusieurs variables. La place étant très limitée, nous nous bornons ici à exposer les résultats de l'arithmétique des courbes algébriques.

II. — Les points rationnels des courbes algébriques planes.

2. Les courbes unicursales. — Deux courbes algébriques à coefficients rationnels sont considérées comme *équivalentes* ou appartenant à la même *classe* si l'on peut passer de l'une à l'autre par une *transformation birationnelle à coefficients rationnels*. Deux courbes équivalentes sont du même genre.

D'après Lagrange [17] et Gauss [10], nous savons trouver tous les points rationnels des droites et des coniques (à coefficients ration-

nels). Une droite admet toujours une infinité de points rationnels et on les obtient par une formule (en coordonnées homogènes)

$$x : y : z = (at_1 + bt_2) : (ct_1 + dt_2) : (et_1 + ft_2),$$

où les nombres a, b, c, d, e, f sont rationnels et où les paramètres t_1 et t_2 prennent toutes les valeurs rationnelles possibles.

Pour reconnaître si une conique admet un point rationnel, on peut la transformer par une transformation linéaire à coefficients rationnels en la forme

$$ax^2 + by^2 + cz^2 = 0,$$

où les a, b, c sont des nombres entiers sans facteurs quadratiques > 1 et premiers entre eux deux à deux. Pour que cette équation soit possible en nombres entiers (ou rationnels) x, y, z (qui ne sont pas tous $= 0$), il faut et il suffit : 1° que les nombres a, b, c ne soient pas tous de mêmes signes; 2° que les nombres $-bc$, $-ac$, $-ab$ soient restes quadratiques respectivement de a, b, c.

Si une conique admet un point entier, elle en admet une infinité.

Toutes les droites et toutes les coniques qui admettent un point rationnel forment une seule classe.

Le problème de trouver les points rationnels des courbes algébriques unicursales de degré $\geqq 3$ a été complètement résolu par les travaux de Hilbert, de Hurwitz [13] et de Poincaré [29]. En effet, ils ont démontré le théorème suivant :

I. *Une courbe unicursale à coefficients rationnels de degré impair est équivalente à une droite et admet ainsi une infinité de points rationnels. Lorsque le degré est pair, elle est équivalente à une conique.*

Soit la courbe en coordonnées homogènes

$$f(x, y, z) = 0. \tag{1}$$

Si elle est de degré $m \geqq 3$ et de genre zéro, elle aura $\frac{1}{2}(m-1)(m-2)$ points doubles; toute fonction symétrique des coordonnées des points doubles sera un nombre rationnel. D'où il suit qu'on peut faire passer par ces points doubles et par $m - 2$ points rationnels pris à volonté dans le plan une courbe de degré $m-2$, et que cette courbe aura des coefficients rationnels. L'équation générale des courbes adjointes de

degré $m-2$ passant par les points doubles sera donc de la forme

$$\lambda_1\varphi_1+\lambda_2\varphi_2+\ldots+\lambda_{m-1}\varphi_{m-1}=0, \tag{2}$$

les λ_i étant des paramètres arbitraires et les φ_i étant des polynomes entiers homogènes d'ordre $m-2$ en x, y, z à coefficients rationnels. Alors, si nous posons

$$\Phi_1=\sum_1^{m-2}\lambda_{1,i}\varphi_i, \qquad \Phi_2=\sum_1^{m-2}\lambda_{2,i}\varphi_i, \qquad \Phi_3=\sum_1^{m-2}\lambda_{3,i}\varphi_i,$$

où les λ sont des coefficients rationnels, nous pouvons transformer la courbe (1) par la transformation birationnelle à coefficients entiers

$$x_1 : y_1 : z_1 = \Phi_1 : \Phi_2 : \Phi_3$$

et nous aurons la courbe

$$g(x_1, y_1, z_1)=0,$$

qui est aussi de genre zéro, mais de degré $m-2$ seulement. Donc, une courbe unicursale est équivalente à une autre courbe unicursale dont le degré est de deux unités plus petit. En procédant de la même manière on arrivera au théorème indiqué. On aura ainsi une méthode pour effectivement déterminer les points rationnels de la courbe s'il y en a. Puisque la transformation cesse à être uniformément réversible dans les points doubles, on aura à examiner à part si ces points ont des coordonnées rationnelles.

Supposons que la courbe (1) admette $m-3$ points simples rationnels. Si nous assujettissons la courbe (2) à passer par eux, elle aura la forme suivante en coordonnées non homogènes :

$$\lambda_1\Psi_1(x, y)+\lambda_2\Psi_2(x, y)=0.$$

Posant $\Psi_2:\Psi_1=\lambda_1:-\lambda_2=t$, les coordonnées x, y de (1) s'expriment en fonction rationnelle de t sous la forme

$$x=\frac{f_2(t)}{f_1(t)}, \qquad y=\frac{f_3(t)}{f_1(t)}, \tag{3}$$

où f_1, f_2, f_3 sont des polynomes entiers en t à coefficients rationnels. D'où suit le théorème de Maillet [23, c] :

II. *Lorsque la courbe* (1) *admet une infinité de points ration-*

nels, on les obtient tous, à un nombre limité d'exceptions près dues, le cas échéant, aux points doubles, en donnant à t dans les équations (3) *toutes les valeurs rationnelles possibles et, éventuellement, la valeur $t = \infty$.*

Si la courbe (1) a un nombre limité de points rationnels (ce qui exige m pair $\geqq 4$), elle en a au plus $m - 4$ en dehors des points doubles. Si la courbe est directement donnée par les équations (3), les points rationnels s'obtiennent par la même règle que ci-dessus.

On voit que tout ce que nous venons de dire sur les courbes unicursales reste vrai dans un domaine de rationalité quelconque, avec une réserve, bien entendu, pour le théorème sur la conique

$$a x^2 + b y^2 + c z^2 = 0.$$

3. **Les courbes de genre 1.** — La recherche des points rationnels des courbes de genre 1 est beaucoup plus difficile que pour les courbes unicursales. Il n'existe pas une théorie aussi complète que pour celles-là. Remarquons d'abord qu'il n'existe jusqu'ici aucune méthode générale pour reconnaître si une courbe de genre 1 admet un point rationnel ou non.

On doit à Poincaré [29] le théorème suivant :

I. *Une courbe $f = 0$ de genre 1, qui admet un point rationnel, est équivalente à une cubique.*

(L'équivalence est définie comme pour les courbes unicursales.)

Pour démontrer cela, considérons les courbes adjointes d'ordre $m - 2$ (m est l'ordre de $f = 0$) qui passent par les $\frac{1}{2}m(m-3)$ points doubles et ayant un contact du second ordre avec $f = 0$ en le point rationnel donné. Ces adjointes seront

$$\lambda_1 \varphi_1 + \lambda_2 \varphi_2 + \ldots + \lambda_{m-3} \varphi_{m-3} = 0,$$

où les φ_i sont des polynomes homogènes, d'ordre $m - 2$, à coefficients rationnels. Si l'on donne aux λ des valeurs rationnelles, les adjointes couperont $f = 0$ en un groupe de $m - 3$ points mobiles, tels que toute fonction symétrique de leurs coordonnées soit rationnelle. Par un de ces groupes de $m - 3$ points et par les points doubles,

nous pouvons faire passer une infinité de courbes d'ordre $m-2$, dont l'équation générale sera

$$\alpha_1\Psi_1+\alpha_2\Psi_2+\alpha_3\Psi_3=0,$$

où les α sont des arbitraires et les Ψ des polynomes homogènes, d'ordre $m-2$, à coefficients rationnels. Alors, la courbe $f=0$ est transformée en une cubique par la transformation birationnelle à coefficients rationnels

$$u:v:w=\Psi_1:\Psi_2:\Psi_3.$$

Il suffit donc de considérer les cubiques. Quand on connaît un ou plusieurs points rationnels d'une cubique, on peut en trouver d'autres par l'un des trois procédés suivants (Lucas [22, *b*]): 1° Si P_1 est un point rationnel de la cubique, la tangente en P_1 rencontre la courbe en un autre point rationnel. Cependant, lorsque P_1 est un point d'inflexion, cette méthode est en défaut. (Cette méthode a été donnée en forme algébrique par Cauchy [2].) 2° Si P_1 et P_2 sont deux points rationnels, on obtient, en général, un troisième point rationnel en prenant l'intersection de la sécante P_1P_2 avec la courbe. 3° Si l'on connaît cinq points rationnels, on obtient, en général, un sixième point rationnel en prenant le point d'intersection avec la courbe de la conique passant par les cinq points; on peut, d'ailleurs supposer plusieurs de ces points réunis en un seul et en particulier tous les cinq réunis en un seul.

Ces résultats sont aussi valables pour les cubiques unicursales. Quand la cubique est du genre 1, on peut interpréter les deux premières méthodes analytiquement de la manière suivante (Poincaré [29], Hurwitz [14]) : A chaque point de la courbe est attaché un argument elliptique u, que nous pouvons supposer choisi de telle façon que la somme des arguments de trois points en ligne droite soit nulle. Cela posé, soit P_1 un point rationnel dont l'argument elliptique soit u_1. La tangente en P_1 coupera la cubique en un point rationnel P_2 dont l'argument sera $-2u_1$. La tangente en P_2 donnera un troisième point rationnel P_3 d'argument $4u_1$. La droite P_1P_3 coupera la cubique en un point rationnel d'argument $-5u_1$. Ainsi, tous les points d'arguments $(3n+1)u_1$, avec n entier quelconque, seront rationnels. En général, en partant de p points rationnels initiaux d'arguments $u_1, u_2, \ldots, u_p$, on déduit par cette méthode les points

rationnels d'arguments

$$m_1 u_1 + m_2 u_2 + \ldots + m_p u_p,$$

où $m_1, m_2, \ldots, m_p$ sont des nombres entiers tels que leur somme soit $\equiv 1 \pmod 3$. Cependant, on ne connaît aucune méthode générale pour reconnaître si ce procédé donne une infinité de points rationnels ou non.

On sait qu'une cubique peut être transformée birationnellement en une cubique de la forme normale de Weierstrass

$$y^2 = 4x^3 - g_2 x - g_3. \tag{1}$$

Si la cubique admet un point rationnel, on voit aisément que la transformation peut être choisie de telle façon qu'on ne quitte pas le domaine de rationalité des coefficients, donc :

II. *Une cubique qui admet un point rationnel est équivalente à une cubique de la forme* (1) *à coefficients rationnels.*

(Le point rationnel correspond ici à $x = \infty$.) Pour la cubique (1), on a la représentation elliptique

$$x = \mathfrak{p}(u), \qquad y = \mathfrak{p}'(u).$$

Supposons que la cubique admette les points rationnels d'arguments $u_1, u_2, \ldots, u_p$. Alors tous les points d'arguments

$$m_1 u_1 + m_2 u_2 + \ldots + m_p u_p$$

sont rationnels pour *toutes* les valeurs entières de $m_1, m_2, \ldots, m_p$. Car la formule d'addition de la fonction $\mathfrak{p}(u)$ montre que $\mathfrak{p}(mu)$, m entier quelconque, est une fonction rationnelle de $\mathfrak{p}(u)$ et $\mathfrak{p}'(u)$ à *coefficients rationnels*. En général, on aura ainsi une infinité de points rationnels, sauf dans le cas où tous les arguments $u_1, u_2, \ldots, u_p$ sont des parties aliquotes d'une période de $\mathfrak{p}(u)$.

Mordell [24, *e*] a démontré le théorème très important :

III. *Il existe un système d'un nombre fini de points rationnels fondamentaux d'arguments* $u_1, u_2, \ldots, u_p$, *tel que tous les points rationnels de la cubique* (1) *soient donnés par les formules*

$$x = \mathfrak{p}(m_1 u_1 + m_2 u_2 + \ldots + m_p u_p),$$
$$y = \mathfrak{p}'(m_1 u_1 + m_2 u_2 + \ldots + m_p u_p),$$

où $m_1, m_2, \ldots, m_p$ prennent toutes les valeurs entières possibles.

Ce théorème est évident lorsque la cubique n'a qu'un nombre limité de points rationnels. S'il y en a une infinité, il est clair qu'on peut choisir d'une infinité de manières le système des points fondamentaux. On peut choisir le système tel que le nombre p soit aussi petit que possible. Cette valeur minima du nombre p que Poincaré a appelé le *rang* de la cubique est évidemment un élément très important de la classification des cubiques.

La démonstration de Mordell repose sur le fait que la cubique (1), dans le cas où elle admet le point rationnel (à distance finie), $x = c$, $y = d$, est équivalente à la quartique

$$v^2 = u^4 - 6cu^2 + 4du + e,$$

où $d^2 = 4c^3 - g_2 c - g_3$ et $e = g_2 - 3c^2$. En effet, les deux courbes sont liées par la transformation birationnelle à coefficients rationnels

$$2u = \frac{y - d}{x - c}, \qquad v = -u^2 + 2x + c.$$

Le problème de résoudre l'équation (1) en nombres rationnels est ainsi équivalent au problème de résoudre en nombres entiers x, y, z (x et y premiers entre eux), l'équation indéterminée

$$x^4 - px^3y - qx^2y^2 - rxy^3 - sy^4 = tz^2, \tag{2}$$

où les nombres p, q, r, s, t sont entiers. Supposons d'abord que l'équation $\theta^4 - p\theta^3 - q\theta^2 - r\theta - s = 0$ n'ait pas de racine rationnelle; θ est alors du second ou du quatrième degré. Le côté gauche de (2) est le produit de $x - \theta y$ et $x^3 - (\theta - p)x^2 + \ldots$. Puisque ces nombres n'ont qu'un nombre fini de diviseurs idéaux communs dans le corps algébrique $K(\theta)$, l'équation (2) entraîne

$$(x - \theta y) = \mathfrak{A}.\mathfrak{U}^2,$$

où $\mathfrak{A}$ et $\mathfrak{U}$ sont des idéaux dans $K(\theta)$, dont le premier ne prend qu'un nombre fini de valeurs. Cette équation conduit à

$$x - \theta y = \frac{\sigma}{m}\,\nu^2, \tag{3}$$

où σ est l'un d'un nombre fini de nombres algébriques entiers, où m est l'un d'un nombre fini de nombres entiers ordinaires, et où ν est

un nombre algébrique entier de la forme

$$\nu = a + b\,\theta + c\,\theta^2 + d\,\theta^3,$$

avec a, b, c, d, entiers rationnels. Si l'équation (3) admet une autre solution x_0, y_0, on aura, par multiplication,

$$m^2(x - \theta y)(x_0 - \theta y_0) = (A + B\,\theta + C\,\theta^2 + D\,\theta^3)^2.$$

De cette équation, Mordell déduit une nouvelle solution x_1, y_1, z_1 de l'équation (2), où x_1 et y_1 sont des fonctions linéaires de A, B, C et D. Les solutions x, y, z sont exprimables en fonctions rationnelles à coefficients rationnels de x_1, y_1 et z_1; on a ainsi

$$(4)\quad x = R_1(x_1, y_1, z_1), \qquad y = R_2(x_1, y_1, z_1), \qquad z = R_3(x_1, y_1, z_1).$$

En désignant par $M[|x|, |y|]$ le plus grand des nombres $|x|$ et $|y|$, il résulte de ces relations entre les deux systèmes de solutions que

$$M[|x_1|, |y_1|] < k\sqrt{M[|x|, |y|]},$$

où k est une constante positive, qu'on peut déterminer si l'on connaît une solution initiale x_0, y_0 de toutes les équations (3). Pour toutes les solutions avec $M[|x|, |y|] \geqq k^2$, on a alors pour la solution dérivée

$$M[|x_1|, |y_1|] < M[|x|, |y|].$$

Puisqu'il n'y a qu'un nombre fini de solutions avec $M[|x|, |y|] < k^2$, il résulte que toutes les solutions de (2) peuvent s'exprimer en fonctions rationnelles d'un nombre fini entre elles. Plus précisément, on aura de proche en proche toutes les solutions possibles par un nombre fini de systèmes (4) en partant d'un nombre fini de solutions « fondamentales » x_1, y_1, z_1. C'est, en réalité, la même méthode que Fermat a appelé *descente infinie*, et dont il s'est servi pour démontrer l'impossibilité de l'équation indéterminée $x^4 - y^4 = z^2$; pour cette équation, on aura, en effet, $k = 1$.

Il est facile d'interpréter ce résultat géométriquement : en effet, soient P_1, P_2, ..., P_p les points rationnels de la quartique qui correspondent aux solutions fondamentales de l'équation (2).

En posant $\xi = \frac{x}{y}$ et $\eta = \frac{z}{y^2}$, nous aurons la quartique sous la forme

$$\eta_1^2 = a\xi^4 + b\xi^3 + c\xi^2 + d\xi + e.$$

Considérons les coniques adjointes, qui sont ici les paraboles

$$\eta = f\xi^2 + g\xi + h. \tag{5}$$

Elles coupent la quartique en quatre points mobiles en dehors du point multiple à l'infini. Faisons la parabole passer par trois des points P_i, alors elle coupera la quartique en un quatrième point rationnel, soit P_{p+1}; on peut aussi supposer deux ou tous les trois de ces points confondus en un seul. En ajoutant maintenant P_{p+1} aux autres points et en continuant le même procédé, on aura de proche en proche tous les points rationnels de la courbe. En passant de l'équation (2) à la quartique, les systèmes (4) seront remplacés par un nombre fini de systèmes

$$\xi = F(\xi_1, \eta_1), \qquad \eta = G(\xi_1, \eta_1), \tag{6}$$

où F et G sont des fonctions rationnelles à coefficients rationnels de ξ_1 et η_1. Ces formules de récurrence donnent tous les points rationnels en partant des points rationnels fondamentaux ξ_1, η_1. Il est très remarquable que le procédé géométrique ci-dessus a déjà été donné, en langage algébrique, par Fermat [8], et plus tard par Euler [7, *a*], pourtant sans qu'il a pu montrer que cette méthode résout complètement le problème. Il a même parlé de solutions *primitives*, qui sont indépendantes l'une de l'autre. Ainsi, il a donné six solutions primitives de l'équation

$$y^2 = x^4 + 4x^3 + 10x^2 + 20x + 1.$$

Il serait très intéressant de reconnaître si ces solutions font un système fondamental au sens de Mordell.

Quand on transforme la quartique en une cubique de la forme (1), la parabole (5) sera transformée en une autre parabole qui coupera la cubique en quatre points d'arguments u_1, u_2, u_3, u_4, dont la somme doit être égale à une période de la fonction $\wp(u)$. Il suit de là facilement l'interprétation analytique du résultat, donnée par le théorème III. Jacobi [15] a déjà donné une interprétation en langage elliptique des résultats de Fermat et Euler ci-dessus.

Dans le cas où le côté gauche de l'équation (2) a un facteur $x - ay$, avec a rationnel, on arrivera au même résultat par une méthode analogue; c'est toujours une descente infinie qui conduit au but.

L'analyse de Mordell montre l'existence d'un système fondamental

d'un nombre fini de points. Mais elle ne donne pas, en général, un procédé pour effectivement déterminer un tel système. Pour cela, il fallait, en effet, connaître un certain nombre de solutions de l'équation (3) ou bien de l'équation (2). Or, nous n'avons, même pour une cubique, aucune méthode générale pour reconnaître si une courbe de genre 1 admet un point rationnel. La théorie est ainsi loin d'être complète.

Dans le numéro suivant, nous allons exposer comment on a pu pour certaines classes d'équations résoudre le problème complètement. C'est un fait très remarquable que la méthode repose dans tous les cas sur une descente infinie.

On ne possède aucun moyen général pour déterminer si une courbe de genre 1, sur laquelle on connaît déjà un certain nombre de points rationnels, admet une infinité ou seulement un nombre fini de points rationnels. Seulement pour certaines cubiques et quartiques, on a pu démontrer l'existence d'une infinité de points rationnels, ainsi que nous allons le voir dans le numéro suivant.

Poincaré [29] et Hurwitz [14] ont énoncé le théorème suivant sur la distribution des points rationnels sur les branches :

IV. *Supposons qu'une cubique admette une infinité de points rationnels. Alors, il y en aura toujours une infinité sur tout arc de sa branche impaire et sur tout arc de sa branche paire si cette dernière en admet un.*

La démonstration de Hurwitz n'est pas suffisante, mais facile à compléter.

Il est évident que tous les résultats de ce numéro, sauf celui de Mordell, restent encore valables dans un domaine de rationalité quelconque. Cependant, le dernier théorème est vrai seulement dans un domaine réel.

4. Courbes spéciales de genre 1. — Il existe un grand nombre de travaux sur des cubiques et des quartiques spéciales. On s'est occupé surtout des équations qui ne possèdent qu'un nombre limité de solutions. Fermat et Euler en ont donné les premiers exemples, comme $x^3+y^3=1$, $x^4-1=y^2$, ... Pour la bibliographie complète et détaillée, nous renvoyons le lecteur à l'Ouvrage de Dickson. Nous pouvons ici seulement résumer les résultats. Commençons avec les

cubiques. Une question se pose très naturellement : Étant donné le nombre entier n, existe-t-il une cubique qui admet exactement n points rationnels? Cette question a été traitée par Hurwitz [14] et Levi [21]. Il est facile de construire une infinité de cubiques n'ayant aucun point rationnel. C'est le cas pour les courbes

$$x^3 + (9a + b)y^3 = 9z^3,$$

où a est un entier quelconque et où $b = \pm 2$, ± 3 ou ± 4.

Soit donnée une cubique qui admet exactement n points rationnels et considérons la représentation elliptique par la fonction $p(u)$; soit u l'argument d'un point rationnel. Si $n = 1$, on a $u = 0$. Si la courbe a deux points rationnels, il existe les trois possibilités

$$u = 0, \frac{\omega}{2}; \qquad u = 0, \frac{\omega'}{2}; \qquad u = 0, \frac{\omega + \omega'}{2},$$

où ω et ω' désignent une paire de périodes primitives, ω est supposée réelle. Si $n = 3$, les arguments sont donnés par

$$u = 0, \frac{\omega}{3}, \frac{2\omega}{3}.$$

Pour $n = 4$, on a les trois possibilités suivantes :

$$0, \pm\frac{\omega}{4}, \frac{\omega}{2}; \qquad 0, \frac{\omega}{2}, \frac{\omega'}{2}, \frac{\omega + \omega'}{2}; \qquad 0, \pm\frac{\omega}{4} + \frac{\omega'}{2}, \frac{\omega}{2}.$$

Dans le cas général, les n points sont donnés par l'un des trois systèmes suivants :

$$1^0 \quad u = \frac{k\omega}{n} \qquad (k = 0, 1, 2, \ldots, n-1);$$

$$2^0 \quad u = \frac{2k\omega}{n} + \varepsilon\frac{\omega'}{2} \qquad \left(k = 0, 1, 2, \ldots, \frac{n}{2} - 1;\ \varepsilon = 0, 1\right);$$

$$3^0 \quad u = \frac{2k\omega}{n} + \varepsilon\left(\frac{\omega}{n} + \frac{\omega'}{2}\right) \qquad \left(k = 0, 1, 2, \ldots, \frac{n}{2} - 1;\ \varepsilon = 0, 1\right).$$

Dans le premier cas, tous les points sont sur la branche impaire de la courbe. Dans les deux derniers cas, il y a $\frac{n}{2}$ points sur chacune des deux branches. Les points dont l'argument contient la quantité $\frac{\omega'}{2}$ sont sur la branche paire.

On ne sait pas jusqu'ici s'il existe réellement une cubique qui admet exactement n points rationnels, pour n arbitraire. C'est seulement pour les cas de $n = 1, 2, 3, 4$ et 6 qu'on a pu construire de telles cubiques. Pour $n = 1$, les résultats les plus importants ont été trouvés par Legendre [20], Lucas [22, *b*], Sylvester [33], Pépin [27, *a*] et Hurwitz [14] :

Il n'y a que le seul point rationnel $(1, -1, 0)$ *sur la cubique*

$$x^3 + y^3 = A z^3, \tag{1}$$

où A *a l'une des valeurs suivantes :*

$$\begin{array}{c} 3,\ 14,\ 18,\ 21,\ 36,\ 38,\ 39,\ 57,\ 76,\ 196, \\ p,\ q(>2),\ p^2,\ q^2,\ 9p,\ 9q,\ 9p^2,\ 9q^2,\ pq,\ p^2q^2,\ pp_1^2,\ qq_1^2; \end{array}$$

p *et* p_1 *sont ici des nombres premiers différents* $\equiv 5 \pmod 9$, *et* q *et* q_1 *des nombres premiers différents* $\equiv 2 \pmod 9$. *Lorsque* $A = 2$, *elle admet exactement les deux points* $(1, -1, 0)$ et $(1, 1, 1)$. *Lorsque* $A = 1$, *elle admet exactement les trois points* $(1, -1, 0)$, $(0, 1, 1)$ et $(1, 0, 1)$.

C'est très intéressant d'observer que, dans tous les cas, la démonstration de ce théorème repose sur une descente infinie. Pour illustrer la méthode, prenons l'exemple où $A = p$ est un nombre premier $\equiv 5 \pmod 9$. Dans ce cas, si l'on suppose x et y premiers entre eux, z doit être divisible par 3. Si $\rho = \frac{1}{2}(-1 + \sqrt{-3})$, le côté gauche de (1) se décompose en trois facteurs, $x + y$, $x + \rho y$, $x + \rho^2 y$, qui sont des nombres entiers du corps quadratique $K(\rho)$, ayant le plus grand commun diviseur $1 - \rho$. Alors, en vertu des propriétés du corps $K(\rho)$, l'équation (1) entraîne

$$x + y = 9pw^3, \tag{2}$$

$$\begin{cases} x + \rho y = (1 - \rho)(u + v\rho)^3, \\ x + \rho^2 y = (1 - \rho^2)(u + v\rho^2)^3, \end{cases} \tag{3}$$

où u, v, w sont des nombres entiers ordinaires, u et v premiers entre eux et $v \equiv 0 \pmod 3$. Les équations (3) donnent

$$\begin{aligned} x &= u^3 + 3u^2v - 6uv^2 + v^3, \\ y &= -u^3 + 6u^2v - 3uv^2 - v^3, \end{aligned}$$

donc $x+y=9uv(v-u)$, et grâce à l'équation (2),

$$uv(v-u)=pw^3.$$

Les nombres u, v et $v-u$ étant premiers entre eux deux à deux, il faut que les deux entre eux soient des cubes et que le troisième soit de la forme pz_1^3. Il résulte donc une équation

$$x_1^3+y_1^3=pz_1^3$$

en nombres entiers x_1, y_1, z_1 différents de zéro, de la même forme que (1), mais où

$$|x_1y_1z_1|=|w|\leqq\left|\frac{1}{3}xyz\right|<|xyz|.$$

Or, cela conduit à une contradiction, s'il existe une valeur minima de $|xyz|$ qui est $\geqq 1$.

Dans les autres cas, la méthode est tout à fait analogue.

Quand $A=2$, il y a deux points rationnels d'arguments o et $\frac{\omega}{2}$.

Quand $A=1$, il y a trois points rationnels d'arguments o, $\frac{\omega}{3}$, $\frac{2\omega}{3}$.

On peut ajouter à ce théorème le résultat suivant qui se démontre aussi à l'aide d'une descente infinie (Nagell [25, *c*]) :

Soit D *un nombre entier, positif ou négatif, qui n'est divisible par d'autres nombres premiers que* 3 *et ceux qui ont la forme* $12m+5$. *Cela posé, la cubique*

$$x^3-1=Dy^2$$

n'admet que le point rationnel $x=-1$, $y=0$, *en dehors du point à l'infini. Cela est encore vrai pour* $D=-1$. *Pour* $D=1$, *elle passe encore par les points rationnels* $x=2$, $y=\pm 3$ et $x=0$, $y=\pm 1$.

On a ici une infinité de cubiques inéquivalentes qui admettent exactement deux points rationnels; les arguments sont o, $\frac{\omega}{2}$.

Dans le cas $D=1$, on a six points rationnels; les arguments sont o, $\frac{1}{6}\omega$, $\frac{1}{3}\omega$, $\frac{1}{2}\omega$, $\frac{2}{3}\omega$, $\frac{5}{6}\omega$, correspondant à $x=\infty$, 2, 0, -1, o et 2.

Il est facile de montrer que la cubique

$$x(x^2-1)=y^2$$

n'admet pas d'autres points rationnels que ceux d'arguments o, $\frac{\omega}{2}$, $\frac{\omega'}{2}$ et $\frac{\omega+\omega'}{2}$.

On connaît aussi un certain nombre de quartiques de la forme

$$ax^4+b=cy^2$$

qui n'ont qu'un nombre limité de points rationnels. Le point double à l'infini est toujours rationnel. Fermat a donné l'exemple

$$x^4-1=y^2,$$

qui n'admet que les points $x=\pm 1$. Désignons, pour abréger, les quartiques de cette forme par (a, b, c). Alors, on peut résumer les résultats les plus importants comme il suit (1) :

. *Les quartiques*

$$(1, \pm 1, 1),\ (1, \pm 1, 2),\ (1, \pm 4, 1),\ (1, 2, 1),\ (1, -8, 1),\ (1, 6, 1),$$
$$(1, 12, 1),\ (1, -18, 1),\ (1, 27, 1),\ (1, -24, 1),\ (1, \pm 108, 1),$$
$$(1, 54, 1),\ (1, -216, 1),\ (4, 9, 1),\ (4, -27, 1),\ (8, 9, 1),$$
$$(1, -1, p),\ (1, -p^n, 1),\ (1, -1, 2q),\ (1, -q^3, 1),$$

où p est un nombre premier $\equiv 3 \pmod 8$, *et où q est un nombre premier* $\equiv 5 \pmod 8$, *ne peuvent avoir d'autres points rationnels (à distance finie) que* $x=\pm 1$ *et* $x=0$.

La démonstration dépend dans tous les cas d'une descente infinie. Prenons, par exemple, la quartique $x^4-1=py^2$. Le problème sera de montrer que l'équation

$$x^4-y^4=pz^2 \tag{4}$$

est impossible en nombres entiers x, y, z, sauf pour $z=0$. On peut supposer x et y premiers entre eux. Puisque $p\equiv 3 \pmod 8$, z doit être pair. L'équation (4) conduit à l'un ou l'autre des deux systèmes

$$x\pm y=2pu^2,\ x\mp y=4v^2,\ x^2+y^2=2w^2, \tag{5}$$

(1) Il est facile de construire une infinité de quartiques qui n'admettent aucun point rationnel à distance finie. C'est le cas pour $x^4+1=py^2$, si p est un nombre premier de la forme $4m+3$.

ou

$$x \pm y = 2u^2,\ x \mp y = 4pv^2,\ x^2 + y^2 = 2w^2, \tag{6}$$

où les nombres u, v, w sont premiers entre eux deux à deux ; u et w sont impairs. En éliminant x et y, le système (5) donne

$$p^2u^4 + 4v^4 = w^2,$$

d'où l'on tire

$$w \pm pu^2 = 2a^4, \qquad w \mp pu^2 = 2b^4,$$

donc

$$\pm pu^2 = a^4 - b^4,$$

équation impossible puisque u est impair. Le système (6) donne

$$4p^2u^4 + v^4 = w^2,$$

d'où l'on tire

$$w \pm 2pv^2 = a^4, \qquad w \mp 2pv^2 = b^4,$$

donc

$$a^4 - b^4 = \pm p(2v)^2$$

ou bien

$$x_1^4 - y_1^4 = pz_1^2,$$

équation de même forme que (4), mais où $|z_1| < |z|$. On aura ainsi une descente infinie, et l'équation (4) est impossible parce que la méthode s'applique sans exception pour tous les $z \neq 0$. Pour les autres quartiques, la méthode est analogue. Il y a des résultats semblables pour un petit nombre de quartiques de la forme

$$x^4 + ax^2 + b = cy^2$$

(Pocklington [28]).

Il existe une infinité de cubiques inéquivalentes qui ont un nombre infini de points rationnels. Cela résulte du théorème de Hurwitz [14] :

Soient a, b, c des nombres entiers positifs, premiers entre eux deux à deux et indivisibles par le carré d'un nombre premier; et soit d un nombre entier quelconque. Alors, si $c > b > a \geq 1$, la cubique

$$ax^3 + by^3 + cz^3 + dxyz = 0 \tag{7}$$

admet une infinité de points rationnels si elle en admet un. Si $c > 1$, et si la cubique

$$x^3 + y^3 + cz^3 + dxyz = 0 \tag{8}$$

admet trois points rationnels, elle en admet une infinité. Enfin, si d est différent de 1, -3 *et* -5, *et si la cubique*

$$x^3+y^3+z^3+dxyz=0 \tag{9}$$

admet quatre points rationnels, elle en admet une infinité.

La démonstration prend pour point de départ le fait que les coordonnées x_1, y_1, z_1 du point d'intersection de la tangente en le point x, y, z sont données par la formule

$$x_1 : y_1 : z_1 = x(by^3-cz^3) : y(cz^3-ax^3) : z(ax^3-by^3).$$

Il est évident qu'on peut dans (7) choisir les nombres a, b, c, d d'une infinité de manières tels que l'équation soit possible en nombres entiers x, y, z. Ainsi, il s'ensuit que la cubique

$$x^3+2y^3+3z^3=0$$

admet une infinité de points rationnels. Pour les cubiques

$$x^3+y^3=Az^3,$$

on peut montrer qu'elles ont une infinité de points rationnels quand A a l'une des valeurs

$$6,\ 7,\ 9,\ 12,\ 15,\ 17,\ 19,\ 20,\ 22,\ 26,\ 28,\ 30,\ 37.$$

Quand la courbe de genre 1 a une infinité de points rationnels, c'est seulement dans un petit nombre de cas qu'on a pu résoudre complètement le problème et déterminer un système de points rationnels fondamentaux. Lagrange [17] a donné les premiers exemples en résolvant complètement les équations

$$2x^4-y^4=\pm z^2 \qquad \text{et} \qquad x^4+8y^4=z^2.$$

Pour donner une idée de la méthode, considérons l'équation

$$2x^4-y^4=z^2; \tag{10}$$

x et y sont supposés positifs et premiers entre eux. En passant au corps quadratique $K(\sqrt{2})$, cette équation entraîne (sauf dans le cas de $x^2=y^2=1$)

$$\sqrt{2}\,x^2+y^2=(\sqrt{2}+1)(a+b\sqrt{2})^2,$$

où a et b sont des entiers (ordinaires) premiers entre eux, donc

$$x^2 = (a+b)^2 + b^2 \qquad \text{et} \qquad y^2 = (a+2b)^2 - 2b^2,$$

d'où

$$x = c^2 + d^2, \qquad a = c^2 - d^2 - 2cd,$$
$$\pm y = r^2 - 2s^2, \qquad a = -4rs \pm (r^2 + 2s^2);$$

c et d sont premiers entre eux, ainsi que r et s; on a $cd = rs$. En posant $c = k\lambda$, $d = \mu l$, $r = kl$ et $s = \mu\lambda$, et en égalant les deux expressions pour a, il vient

$$\frac{\mu}{k} = \frac{l\lambda \pm \sqrt{2\lambda^4 - l^4}}{2\lambda^2 + l^2}. \tag{11}$$

On tombe ainsi sur une nouvelle solution $x_1 = \lambda$, $y_1 = l$ de l'équation (10), et l'on a

$$x = k^2 x_1^2 + \mu^2 y_1^2, \qquad \pm y = k^2 y_1^2 - 2\mu^2 x_1^2, \tag{12}$$

où k et μ (premiers entre eux) sont déterminés par l'équation (11). Puisque $x > x_1^2$, la méthode de la descente infinie s'applique et elle peut s'appliquer jusqu'au moment où x_1^2 sera $= y_1^2 = 1$. Inversement, en partant de cette solution, on aura de proche en proche toutes les solutions positives à l'aide des formules (12) et (11). Par conséquent, $x = 1$, $y = 1$ est la seule solution fondamentale positive.

On peut exprimer le résultat comme il suit : tous les points rationnels u, v de la quartique

$$2u^4 - 1 = v^2$$

s'obtiennent de la formule de récurrence

$$\pm u = \frac{u_1^2(2u_1^2+1)^2 + (u_1 \pm v_1)^2}{(2u_1^2+1)^2 - 2u_1^2(u_1 \pm v_1)^2} \tag{13}$$

en commençant avec la solution $u_1 = v_1 = 1$. On aura ainsi les solutions (positives)

$$u = 13, \qquad v = 239; \qquad u = \frac{1525}{1343}, \qquad v = \frac{2750257}{(1343)^2}, \qquad \ldots.$$

On a en même temps résolu le problème pour la cubique équivalente

$$s^2 = 4t^3 + 2t.$$

On peut prendre comme solutions fondamentales $t_1 = p\left(\frac{\omega}{2}\right) = 0$ et $t_2 = \frac{1}{4}$. Le rang de la cubique est égal à 2.

Lucas [22, a] a poursuivi les recherches de Lagrange, et avec la même méthode, résolu le problème complètement pour les quartiques

$$(4, -1, 3),\ (1, 9, 1),\ (1, -36, 1),\ (1, -1, 24),\ (1, 36, 1),\ (9, -1, 8),$$
$$(3, -1, 2)\ (1, 3, 1),\ (4, -3, 1),\ (1, -12, 1),\ (3, -2, 1),\ (1, 24, 1),$$
$$(1, -6, 1),\ (1, 2, 3),\ (1, 18, 1),\ (9, -8, 1),\ (1, -72, 1),$$
$$(27, -2, 1),\ (1, -54, 1),\ (1, 216, 1).$$

(a, b, c) désigne comme ci-dessus la quartique $ax^4 + b = cy^2$. On a ainsi résolu complètement toutes les quartiques (a, b, c), où abc n'est divisible par d'autres nombres premiers que 2 et 3. Dans tous ces cas, il n'y a qu'une seule solution fondamentale positive.

Pépin [27, b, c] a poussé les résultats encore plus loin en résolvant complètement les cas suivants :

$$(1, 7, 8),\ (7, -2, 5),\ (1, 28, 1),\ (1, -350, 1),\ (1, 20, 1),$$
$$(5, -1, 4),\ (8, -3, 5),\ (5, -3, 2),\ (5, -2, 3),\ (3, 5, 8),$$
$$(8, -5, 3),\ (7, -5, 2),\ (1, 35, 1),\ (13, -11, 2),\ (11, -7, 1).$$

Dans le dernier cas, il existe deux solutions fondamentales positives, savoir : $x = 1, y = 2$ et $x = 2, y = 13$. La méthode est toujours la même que ci-dessus.

Les cas que nous venons d'indiquer sont à peu près les seuls, où l'on a jusqu'ici pu déterminer un système de points rationnels fondamentaux d'une courbe de genre 1.

Dans ce qui précède, nous sommes toujours restés dans le domaine de rationalité ordinaire. Or, il faut aussi mentionner un certain nombre de cas, où l'on a résolu les équations dans un domaine de rationalité étendue. Ainsi, l'équation

$$x^3 + y^3 = z^3,$$

est impossible en nombres entiers x, y, z, du corps quadratique engendré par $\rho = \frac{1}{2}(-1 + \sqrt{-3})$, sauf pour $xyz = 0$. C'est le même cas pour l'équation

$$x^3 + y^3 = \varepsilon p z^3,$$

où ε a une des valeurs 1, ρ ou ρ^2, et où p est un nombre premier impair $\equiv 2$ ou $\equiv 5 \pmod 9$ (Hurwitz [14]).

Fueter a démontré le théorème suivant [9] : « Pour que l'équation

$$x^3 + y^3 = z^3 \qquad (xyz \neq 0) \tag{14}$$

soit possible en nombres entiers x, y, z d'un corps quadratique $K(\sqrt{-m})$, m positif, et $m \equiv 1 \pmod 3$, il faut que le nombre de classes d'idéaux du corps soit divisible par 3. »

Burnside [1] a montré comment on peut résoudre l'équation (14) dans une infinité de corps quadratiques à l'aide de l'identité

$$(6k)^3 + [3 + \sqrt{-3(1+4k^3)}]^3 + [3 - \sqrt{-3(1+4k^3)}]^3 = 0.$$

On peut montrer que l'équation

$$x^4 + y^4 = z^2$$

est impossible en nombres entiers x, y, z du corps $K(\sqrt{-1})$, sauf pour $xyz = 0$ (Hilbert [12]).

5. **Les courbes de genre > 1.** — Les résultats sur les courbes de genre supérieur à 1 ne sont pas nombreux. On a presque exclusivement examiné les courbes de la forme (en coordonnées homogènes)

$$a x^n + b y^n = c z^n,$$

qui sont de genre ≥ 2 pour $n \geq 4$. L'équation la plus simple de cette forme est

$$x^n + y^n = z^n. \tag{1}$$

Il est bien connu que Fermat a affirmé, sans démonstration, que cette équation est impossible en nombres entiers, sauf pour $xyz = 0$. Malgré les efforts de nombreux mathématiciens, ce théorème fameux n'a pas encore été démontré, sauf pour des valeurs spéciales de n. Puisque un fascicule spécial de cette Collection sera consacré à ce sujet, nous nous bornons ici à citer le résultat principal de Kummer [16] :

L'équation (1) *est impossible en nombres entiers* $x, y, z \neq 0$ *quand* n *est un nombre premier régulier.*

Un nombre premier p est régulier quand le nombre de classes d'idéaux du corps algébrique engendré par une racine primitive $p^{\text{ième}}$ de l'unité est indivisible par p. L'équation (1) est même impossible en nombres entiers de ce corps algébrique. La démonstration de Kummer utilise la théorie des idéaux de ce corps et repose sur une descente infinie. Tous les nombres premiers < 100 sont réguliers, sauf 37, 59 et 67. On ne sait pas s'il y en a un nombre infini.

Maillet [23, a] a appliqué la méthode de Kummer pour démontrer l'impossibilité d'un grand nombre d'équations de la forme

$$x^p + y^p = c\,z^p, \tag{2}$$

où p est un nombre premier régulier > 3. Ainsi, il a été établi les résultats suivants :

L'équation indéterminée (2) *est impossible en nombres entiers* $\neq 0$, *si* $c = p$. *Elle est impossible pour* $c = q^b$, *où* q *désigne un nombre premier :* 1° *quand* $q^b \equiv -1 + c_1 p \pmod{p^2}$, *quel que soit* p, c_1 *étant un au moins des nombres* $1, 2, \ldots, p-1$ *qui dépend de* p; 2° *quand* $p = 5, 7$ *ou* 17 *et* $c = q^b \equiv 4 \pmod{p^2}$; 3° *quand* $p = 11$ *et* $c = q^b \equiv 5$ *ou* $47 \pmod{11^2}$; 4° *quand* $p = 13$ *et* $c = q^b \equiv 17 \pmod{13^2}$. *L'équation*

$$x^7 + y^7 = q\,z^7$$

est impossible en nombres entiers quand q *est premier et d'une des formes*

$$49k \pm 3, \quad \pm 4, \quad \pm 5, \quad +6, \quad -8, \quad \pm 9, \quad \pm 10,$$
$$-15, \quad \pm 16, \quad -22, \quad \pm 23 \quad \text{ou} \quad \pm 24.$$

Il a aussi démontré quelques théorèmes sur l'équation de la forme

$$x^n + y^n = nb\,z^n,$$

où n est un nombre entier composé ≥ 4 [23, b].

Dirichlet [5] et Lebesgue [19] ont étudié l'équation

$$x^5 + y^5 = A\,z^5,$$

où A est un nombre entier n'ayant aucun facteur premier de la forme $5m + 1$, et ils ont démontré le théorème suivant :

Cette équation est impossible en nombres entiers x, y, z, *tels que*

$|xyz| > 1$, *quand* A *satisfait à l'une des congruences*

$$A \equiv \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 9, \pm 10, \pm 11, \pm 12 \pmod{25}.$$

La démonstration repose sur le fait que l'équation

$$u(u^4 + 10u^2v^2 + 5v^4) = 2^m \cdot 5^n \cdot A w^5$$

est impossible, sauf pour $u = 0$, ce qu'on peut démontrer aisément à l'aide d'une descente infinie.

Pour les courbes de genre $p \geqq 2$, il n'y a qu'un nombre fini de transformations birationnelles de la courbe en elle-même; leur nombre est au plus égal à $84(p-1)$. Ainsi, en partant d'un point rationnel connu, on n'en peut déduire qu'un nombre fini d'autres points rationnels à l'aide de ces transformations (*voir* Nagy [26]). En général, on ne peut pas d'un seul point rationnel donné déduire tous les points rationnels de cette manière. Car, la courbe hyperelliptique

$$x^6 + 4x^4 - 2x^2 + 1 = y^2$$

possède les transformations birationnelles en elle-même,

$$\begin{pmatrix} x' = x \\ y' = y \end{pmatrix}, \quad \begin{pmatrix} x' = x \\ y' = -y \end{pmatrix}, \quad \begin{pmatrix} x' = -x \\ y' = y \end{pmatrix}, \quad \begin{pmatrix} x' = -x \\ y' = -y \end{pmatrix}$$

et elle admet les points rationnels $(0,1)$, $(1,2)$, $(11,3)$, qui sont évidemment indépendants l'un de l'autre.

Dans tous les cas où l'on a pu déterminer tous les points rationnels d'une courbe de genre $\geqq 2$, on n'en a trouvé qu'un nombre fini. Il semble vraisemblable qu'en général une courbe de genre $\geqq 2$ ne peut jamais admettre une infinité de points rationnels.

III. — Les points entiers des courbes algébriques planes.

6. Remarques générales. Les résultats de Runge et de Skolem. — Les courbes sont toujours supposées à coefficients entiers quand on n'a pas dit autre chose.

Il existe une infinité de courbes algébriques qui admettent un nombre infini de points entiers. En effet, on peut satisfaire à l'équation

$$x^n = y^m$$

en posant $x = t^m$, $y = t^n$; chaque valeur entière de t donne un point entier de la courbe (1). (*Voir* aussi la dernière partie du n° 8.)

De l'autre côté, aux n^{os} 2, 4 et 5, nous avons fait la connaissance d'une infinité de courbes dont le nombre de points rationnels est limité. Il existe ainsi une infinité de courbes qui n'ont qu'un nombre fini de points entiers. Il est facile d'indiquer une autre catégorie de courbes jouissant de la même propriété : si tous les points (réels) d'une courbe sont à distance finie, il est évident qu'elle n'a qu'un nombre fini de points entiers, et l'on peut trouver une limite supérieure des coordonnées de ces points. On peut aussi construire des courbes qui n'admettent aucun point entier; c'est le cas, par exemple, pour les courbes $x^2 + 1 = 3y^n$ puisque -1 n'est pas reste quadratique de 3.

Si les deux courbes $f(x, y) = 0$ et $\varphi(u, v) = 0$ sont reliées par les équations à coefficients entiers,

$$x = au + bv + e, \qquad y = cu + dv + f,$$

et si $f(x, y) = 0$ n'a qu'un nombre limité de points entiers, $g(x, y) = 0$ jouit de la même propriété. Si $ad - bc = \pm 1$, les deux courbes ont le même nombre de points entiers.

On ne connaît jusqu'ici aucune méthode générale pour reconnaître si une courbe algébrique donnée possède une infinité ou seulement un nombre fini de points entiers. Maillet a donné une telle méthode pour les courbes unicursales. (*Voir* le n° 8.)

Dans tous les cas connus de courbes ayant une infinité de points entiers, ce sont des courbes unicursales. Très probablement, les courbes de genre ≥ 1 n'admettent qu'un nombre limité de points entiers.

Skolem a étudié la distribution des points entiers dans le cas où il y en a une infinité. Supposons que l'équation $F(x, y) = 0$ ne soit pas remplie par un polynome $y = f(x)$ à coefficients rationnels. Supposons, de plus, qu'il y ait une infinité de solutions entières positives x,

$$x_1 < x_2 < x_3 < \dots$$

(1) On pourrait aussi prendre le cas trivial $y = f(x)$.

Cela posé, Skolem [**32**, *b*] a montré qu'on a

$$\lim_{\nu=\infty} \frac{x_\nu}{\nu} = \infty.$$

Ce résultat a été précisé par Dörge [**6**, *a*, *b*], qui a montré qu'il existe un nombre entier positif m et une quantité positive α, telle qu'on ait pour tous les ν suffisamment grands,

$$x_{\nu+m} - x_\nu > x_\nu^\alpha.$$

La démonstration repose sur l'étude de la fonction algébrique correspondante.

On doit à Runge [**30**] le résultat suivant :

Soit $f(x, y)$ une fonction entière rationnelle et irréductible à coefficients entiers. Alors, pour que l'équation $f(x, y) = 0$ admette une infinité de solutions en nombres entiers x, y, il faut que les conditions suivantes soient remplies : 1° *les plus hautes puissances de x et y dans $f(x, y)$ doivent appartenir à des termes isolés ax^m et by^n ;* 2° *la fonction algébrique y, définie par l'équation $f(x, y) = 0$, doit devenir infiniment grande de l'ordre $x^{\frac{m}{n}}$ par rapport à x. Si, dans $f(x, y)$, x^ρ et y^σ sont multipliés, on doit avoir $n\rho + m\sigma \leqq mn$;* 3° *la somme des termes pour lesquels $n\rho + m\sigma = mn$ doit être représentable dans la forme*

$$b \prod_\beta (y^\lambda - d^{(\beta)} x^\mu) \qquad \left(\beta = 1, 2, \ldots, \frac{n}{\lambda}\right),$$

où $\prod_\beta (u - d^{(\beta)})$ est la puissance d'une fonction entière rationnelle irréductible.

Ajoutons que ces conditions ne sont pas suffisantes. La démonstration de Runge s'appuie sur des considérations sur le développement de la fonction algébrique correspondante en série suivant des puissances fractionnaires et décroissantes de x (ou de y) autour du point à l'infini. Skolem [**32**, *a*] a, indépendamment de Runge, établi le même résultat par une méthode élémentaire et beaucoup plus simple. Le théorème nous donne des catégories très étendues d'équations qui n'ont qu'un nombre limité de solutions en nombres entiers. La démonstration donne en même temps une méthode pour déterminer toutes les solutions.

Un corollaire très important est le théorème suivant :

Soit $f(x, y)$ une fonction entière rationnelle irréductible à coefficients entiers de degré n. Alors, si l'ensemble des termes de degré n, soit $\varphi_n(x, y)$, n'est pas la puissance d'une fonction irréductible, l'équation $f(x, y) = 0$ ne possède qu'un nombre fini de solutions entières x, y.

Pour démontrer ce théorème, Skolem pose

$$\varphi_n(x, y) = g_p(x, y)\, g_{n-p}(x, y),$$

où g_p et g_{n-p} sont deux polynomes homogènes, premiers entre eux des degrés p et $n - p$, et à coefficients entiers. Soit d le plus grand commun diviseur de p et $n - p$. Alors, transformons la courbe $f(x, y) = 0$ par les équations

$$\xi = g_p(x, y)^{\frac{n-p}{d}}, \qquad \eta = g_{n-p}(x, y)^{\frac{p}{d}}$$

en une autre courbe $F(\xi, \eta) = 0$. Il est facile de voir que la partie homogène du plus haut degré dans $F(\xi, \eta)$ est de la forme

$$\lambda \xi^{\mu} \eta^{\nu},$$

où μ et ν sont des nombres entiers positifs et λ un nombre entier $\neq 0$. Il résulte de là qu'il suffit de démontrer le théorème pour l'équation

$$x^{\nu} y^{n-\nu} + f_{n-1}(x, y) = 0, \tag{1}$$

où f_{n-1} est de degré $n - 1$ à coefficients entiers. Sur toutes les branches de la courbe ou le quotient $\frac{y}{x}$ ou le quotient $\frac{x}{y}$ doit converger vers zéro. A cause de la symétrie par rapport à x et y, il suffit de considérer le premier cas. Supposons d'abord que f_{n-1} soit au plus du degré $n - \nu - 1$ par rapport à y. Alors, l'équation (1) peut s'écrire

$$y^{n-\nu} = \frac{A_{\nu}(x)}{x^{\nu}} y^{n-\nu-1} + \frac{A_{\nu+1}(x)}{x^{\nu}} y^{n-\nu-2} + \ldots + \frac{A_{n-1}(x)}{x^{\nu}},$$

où les polynomes $A_l(x)$, à coefficients entiers, sont au plus de degré l. A l'aide de cette équation, on peut exprimer $y^{n-\nu+r}$ $(r = 0, 1, 2, \ldots)$ par $y^{n-\nu-1}$, $y^{n-\nu-2}$, ... de la manière suivante :

$$y^{n-\nu+r} = \frac{A_{r,\nu}(x)}{x^{\nu(r+1)}} y^{n-\nu-1} + \frac{A_{r,\nu+1}(x)}{x^{\nu(r+1)}} y^{n-\nu-2} + \ldots + \frac{A_{r,n-1}(x)}{x^{\nu(r+1)}},$$

où les polynomes A ont des coefficients entiers. En se procurant un nombre suffisamment grand de ces équations, on peut éliminer tous les quotients $\frac{y^s}{x^t}$, où $t < s$ et $s = 1, 2, \ldots, n - \nu - 1$. Le résultat de cette élimination sera de la forme

$$(2) \qquad C_0 y^{n-\nu} + C_1 y^{n-\nu+1} + \ldots + C_N y^{n-\nu+N} = F(x, y) + R(x, y),$$

où $C_0, \ldots, C_N$ sont des nombres entiers dont un au moins est $\neq 0$. $F(x, y)$ est un polynome à coefficients entiers, qui est au plus du degré $n - \nu - 1$ par rapport à y. $R(x, y)$ est une fonction linéaire de certains quotients $\frac{y^s}{x^t}$, où $t \geqq s (s = 0, 1, 2, \ldots, n - \nu - 1)$. Quand x croît indéfiniment, le nombre $R(x, y)$ doit donc tendre vers zéro. Nous pouvons ainsi trouver un nombre M tel qu'on ait sur la branche considérée $|R(x, y)| < 1$ pour tous les $|x| > M$. Dans ce cas, l'équation (2) est évidemment impossible en nombres entiers x, y, sauf pour $R(x, y) = 0$. Or, la courbe

$$C_0 y^{n-\nu} + C_1 y^{n-\nu+1} + \ldots + C_N y^{n-\nu+N} = F(x, y)$$

n'a qu'un nombre fini de points communs avec la courbe (1). Par conséquent, on peut trouver un nombre M_1 tel qu'on ait pour toutes les solutions entières $|x| \leqq M_1$.

D'une manière analogue, on peut traiter les cas où f_{n-1} est d'un degré $\geqq n - \nu$ par rapport à y. Il résultera de là que l'équation (1) n'a qu'un nombre limité de solutions, qui peuvent toutes être trouvées par un nombre fini d'opérations. Par une méthode analogue, on peut démontrer le théorème de Runge dans toute son extension.

Pour donner une idée de la démonstration de Runge, considérons l'exemple

$$(3) \qquad x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = y^m,$$

où les a sont entiers et où m est un diviseur de n et > 1. Le côté gauche ne doit pas être une puissance $m^{\text{ième}}$ d'un polynome en x. En développant en série suivant des puissances croissantes de $\frac{1}{x}$, on aura (1)

$$y = x^{\mu} + e_1 x^{\mu-1} + e_2 x^{\mu-2} + \ldots + e_{\mu} + e_{\mu+1} x^{-1} + \ldots,$$

(1) Quand m est pair, on doit remplacer y par $\pm y$.

où $\mu = \frac{n}{m}$. Les coefficients e_i sont rationnels. Posons pour abréger

$$\varphi(x) = x^{\mu} + e_1 x^{\mu-1} + \ldots + e_{\mu},$$

et soit N le plus petit nombre entier positif tel que tous les nombres Ne_i soient entiers. Alors il y a un nombre x_0 tel qu'on ait, pour tous les $|x| > x_0$,

$$|y - \varphi(x)| < \frac{1}{N}.$$

Quand x est entier et $|x| > x_0$, on doit alors avoir $y = \varphi(x)$. Or, l'équation

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = [\varphi(x)]^m$$

ne peut subsister que pour un nombre fini de valeurs x. On aura ainsi une limite supérieure de solutions entières de (3). Ainsi, dans l'exemple

$$x^n + x^{n-1} + \ldots + x + 1 = y^2 \qquad (n \text{ pair}),$$

on aura facilement la limite $|x| \leqq 2^{n-2}$.

Maillet [23, d, f] a donné une méthode pratique pour calculer une limite supérieure du module des solutions entières dans le cas spécial où la courbe (de degré n) a k asymptotes réelles, à distance finie et de coefficients angulaires distincts et rationnels, et $n - k$ asymptotes imaginaires.

7. **Les résultats de Thue et de Siegel.** — Les méthodes du numéro précédent ne suffisent pas dans le cas où la partie homogène du plus haut degré dans $f(x, y) = 0$ est irréductible. C'est pourtant le cas le plus intéressant. Pour le traiter, il faut une méthode plus effective et des ressources plus profondes. Il est facile de voir que le problème est intimement lié aux propriétés des nombres algébriques. Considérons, en effet, la courbe (à coefficients entiers, comme toujours dans la suite)

$$\varphi_n(x, y) + f_m(x, y) = 0, \tag{1}$$

de degré n, où φ_n est un polynome homogène irréductible de degré n et où f_m est un polynome de degré $m < n$ (1). Supposons d'abord

(1) Nous pouvons faire abstraction du cas où toutes les racines de l'équation $\varphi_n(x, 1) = 0$ sont imaginaires. Il y a ainsi toujours, au moins, une asymptote réelle.

que $|y|>|x|$. Alors, il existe une constante c_1 telle que

$$|f_m(x, y)|<c_1|y|^m,$$

pour tous les $|y|$ suffisamment grands. Posons

$$\varphi_n(x, y)=a\prod(x-\xi_i y).$$

Alors il résulte de l'équation (1) qu'on a pour l'un au moins des facteurs $x-\xi_i y$

$$|x-\xi y|<\sqrt[n]{\frac{c_1}{a}|y|^m}=c_2|y|^{\frac{m}{n}}.$$

On a donc, si ξ_i est différent de ξ,

$$|x-\xi_i y|=|(\xi-\xi_i)y+x-\xi y|>c_3|y|-c_2|y|^{\frac{m}{n}}>c_4|y|,$$

pour tous les $|y|$ suffisamment grands. L'équation (1) entraîne ainsi

$$a|x-\xi y|(c_1|y|)^{n-1}<c_1|y|^m,$$

donc

$$\left|\frac{x}{y}-\xi\right|<\frac{c_5}{|y|^{n-m}}. \tag{2}$$

Dans le cas de $|x|>|y|$, on aura une inégalité analogue. On est ainsi conduit à étudier avec quelle exactitude on peut approximer un nombre algébrique ξ de degré n par des nombres rationnels $\frac{x}{y}$. Si l'on peut démontrer l'impossibilité de l'inégalité (2) pour des valeurs entières suffisamment grandes de $|x|$ et $|y|$, ainsi que celle de l'inégalité analogue pour $|x|>|y|$, on peut en conclure que l'équation (1) n'a qu'un nombre limité de solutions entières x, y.

Axel Thue a attaqué cette question difficile par une méthode vraiment géniale; ses recherches profondes l'ont conduit à une des plus belles découvertes de la théorie des nombres.

En effet, il a démontré le théorème suivant : « Soit ξ un nombre algébrique de degré n; et soient c et ε deux quantités positives quelconques. Alors l'inégalité

$$\left|\xi-\frac{x}{y}\right|<\frac{c}{|y|^{\frac{n}{2}-1+\varepsilon}}, \tag{3}$$

n'a qu'un nombre limité de solutions entières x et y [35, a, f]. »

Il résulte de là que l'équation (1) n'a qu'un nombre fini de solutions entières, si $m < \frac{n}{2} - 1$. Thue s'est contenté de prononcer le théorème dans le cas spécial de $m = 0$: *L'équation indéterminée*

$$\varphi_n(x, y) = C,$$

où C *est un nombre entier, n'admet qu'un nombre fini de solutions entières si* $n \geqq 3$. Cela reste vrai aussi pour un φ_n réductible, qui n'est pas (à un facteur entier constant près) la puissance d'un polynome du premier ou du deuxième degré à coefficients entiers (1). (*Voir* aussi Maillet [23, e].)

Siegel [31, a, b] a ensuite, en précisant la méthode de Thue, montré que le théorème est même vrai pour l'inégalité

$$\left|\xi - \frac{x}{y}\right| < \frac{c}{|y|^{\mu+\varepsilon}}, \tag{4}$$

où μ est la plus petite valeur du nombre

$$\left(\frac{n}{\lambda+1} + \lambda\right) \qquad \text{pour } \lambda = 1, 2, 3, \ldots, n.$$

Le nombre $\left(\frac{n}{\lambda+1} + \lambda\right)$ prend sa valeur minima quand λ est le plus grand nombre entier $\leqq \frac{1}{2}\left(\sqrt{4n+1} - 1\right)$. On a

$$2\sqrt{n} - 1 \leqq \mu \leqq \sqrt{4n+1} - 1.$$

Pour démontrer ce théorème, il suffit de prendre $c = 1$ et de supposer que ξ soit un nombre algébrique entier.

L'idée fondamentale de la démonstration est l'établissement de certaines identités. En effet, on démontre d'abord le lemme suivant : « Soit ξ un nombre algébrique entier de degré $n \geqq 2$. Soient, de plus, r et s deux nombres entiers positifs, $s \leqq n - 1$. Soit enfin $0 < \theta < 1$; et désignons par m le plus grand nombre entier $\leqq \left(\frac{n+\theta}{s+1} - 1\right) r$. Cela posé, il existe trois polynomes $F(x, y)$, $G(x, y)$ et $R(x, y)$ en x et y, F et G à coefficients entiers du corps algébrique engendré par ξ, et R à coefficients entiers rationnels, qui remplissent l'identité

(1) Dans la suite, nous appelons ce résultat « théorème de Thue ».

suivante :

$$(x-\xi)^r F(x,y)+(y-\xi)G(x,y)=R(x,y).$$

F est au plus du degré m en x et du degré s en y. G est au plus du degré $m+r$ en x et du degré $s-1$ en y. R est au plus du degré $m+r$ en x et du degré s en y. Si l'on pose pour tous les nombres entiers $\rho=0, 1, 2, \ldots, r-1$,

$$F_\rho(x,y)=\sum_{\lambda=0}^{\rho}\binom{r}{\rho-\lambda}(x-\xi)^\lambda\frac{\partial^\lambda F(x,y)}{\lambda!\,\partial x^\lambda},$$

$$G_\rho(x,y)=\frac{\partial^\rho G(x,y)}{\rho!\,\partial x^\rho},$$

$$R_\rho(x,y)=\frac{\partial^\rho R(x,y)}{\rho!\,\partial x^\rho},$$

on a l'identité

$$(x-\xi)^{r-\rho}F_\rho(x,y)+(y-\xi)G_\rho(x,y)=R_\rho(x,y).$$

Enfin, il existe deux quantités positives c_1 et c_2 qui dépendent seulement de ξ et θ (et non pas de r et s) tels que tous les coefficients de F, G et R soient absolument $<c_1^r$ et tels qu'on ait

$$|F_\rho(x,y)|<c_2^r(1+|x|)^m\qquad(1+|y|)^s,$$
$$|G_\rho(x,y)|<c_2^r(1+|x|)^{m+r-\rho}(1+|y|)^{s-1},$$
$$|R_\rho(x,y)|<c_2^r(1+|x|)^{m+r-\rho}(1+|y|)^s,$$

pour tous les x et y. »

Si l'on suppose $r\geqq 2n^2$ et $\theta\leqq\frac{1}{2}$, on peut de ce lemme tirer le résultat suivant : Soient $\frac{p_1}{q_1}$ et $\frac{p_2}{q_2}$ deux fractions rationnelles réduites telles que $q_2\geqq c_1^r$. Alors il existe un nombre entier

$$\rho\geqq 0\qquad\text{et}\qquad\rho<\theta r+n^2\leqq r-1,$$

et un nombre entier positif c_3, ne dépendant que de ξ et de θ, tel que l'un au moins des nombres

$$E_1=c_3^r q_1^{m+r}q_2^s\left|\xi-\frac{p_1}{q_1}\right|^{r-\rho},\qquad E_2=c_3^r q_1^{m+r}q_2^s\left|\xi-\frac{p_2}{q_2}\right|$$

soit plus grand que 1.

A l'aide de ce résultat, il est facile de montrer le théorème sur l'inégalité (4). Supposons, en effet, que cette inégalité ait une infinité de solutions entières x et y. Nous choisissons le nombre θ égal à $\frac{\varepsilon}{8n}$. De plus, parmi les solutions de (4), nous en choisissons une, $x = p_1$, $y = q_1$, telle que $q_1 >$ le plus grand des nombres c_1 et $c_3^{\frac{4}{\varepsilon}}$, et une autre, $x = p_2$, $y = q_2$, telle que

$$q_2 > q_1^{\frac{8n^3}{\varepsilon}+1} \geqq q_1^{2n^2+1}. \tag{5}$$

Enfin, on prend r égal au plus grand nombre entier $\leqq \frac{\log q_2}{\log q_1}$. Cela posé, on montrera facilement que les nombres E_1 et E_2 seront tous les deux < 1, contrairement au résultat précédent. L'inégalité (4) ne peut ainsi avoir qu'un nombre fini de solutions.

On doit remarquer que la méthode ne donne aucun procédé général pour effectivement déterminer les solutions de l'inégalité (4); elle ne donne aucun moyen général pour l'évaluation d'une limite supérieure des valeurs absolues des solutions x, y. Cela est une conséquence de la supposition (5).

En appliquant le résultat à l'équation (1), on aura le théorème :

I. *L'équation indéterminée*

$$\varphi_n(x, y) + f_m(x, y) = 0,$$

où φ_n est un polynome homogène irréductible de degré $n \geqq 3$ et où f_m est un polynome de degré $m < n - \mu$, n'a qu'un nombre limité de solutions entières, x, y.

Si $n = 3$, il faut que $m = 0$; si $n = 4$, 5 ou 6, on peut aussi prendre $m = 1$; si $n = 7$, on a $m \leqq 2$; si $n = 8$, on a $m \leqq 3$, ...

Dans un nombre de cas spéciaux où l'on connaît déjà une solution qui satisfait à certaines conditions, on peut, en modifiant la méthode, déterminer une limite supérieure des modules de toutes les solutions. Ainsi, Thue a démontré le théorème suivant [35, *h*] :

II. *Supposons qu'on ait en nombres entiers positifs a, b, α, β, γ, r, où r est la puissance d'un nombre premier, $r \geqq 3$, les rela-*

tions

$$a\alpha^r - b\beta^r = \gamma,$$

$$(6) \qquad (4a\alpha^r)^{r-2} > \gamma^{2r-2} r^{\frac{r^2}{r-1}} \left(\frac{a\alpha^r}{b\beta^r}\right)^{\frac{2(r-1)^2}{r}}.$$

Alors, si l'on a

$$K = \frac{r^{\frac{r^2-2r+1}{r-1}} b^{\frac{r^2-r+1}{r}} \beta^{(r-1)^2}}{2^{r+4}\gamma^{r-1}\alpha^{2r} a^{\frac{r+1}{r}}},$$

$$L = \frac{(4a\alpha^r)^{r-2}}{\gamma^{2r+2} r^{\frac{r^2}{r-1}} \left(\frac{a\alpha^r}{b\beta^r}\right)^{\frac{2(r-1)^2}{r}}},$$

$$|ap^r - bq^r| \leqq c,$$

$$n \geqq \frac{\log c - \log K}{\log L},$$

où p, q et n sont des nombres entiers positifs, $n \geqq 0$ et c une quantité positive, il faut que

$$p \leqq \frac{rb\beta^{r-1}}{2\gamma} \left[\frac{4a\alpha^r}{\gamma^2 r^{\frac{r}{r-1}} \left(\frac{a\alpha^r}{b\beta^r}\right)^{\frac{2r-2}{r}}}\right]^n.$$

On peut prendre, par exemple,

$$a = 1, \quad b = 17, \quad r = 7, \quad \alpha = 3, \quad \beta = 2, \quad \gamma = 14.$$

Dans ce cas, l'inégalité (6) est remplie. On aura

$$\log K = 5,2548601\ldots \qquad \text{et} \qquad \log L = 0,2886780\ldots$$

Si l'on prend $c = 10^6$, on aura $n \geqq 2,58\ldots$. Nous pouvons prendre $n = 3$. On a donc pour tous les p de l'inégalité

$$|p^7 - 17q^7| \leqq 1000000, \qquad p < 14293.$$

Il résulte de là que pour toutes les solutions entières x de l'équation

$$x^7 - 17y^7 = \gamma, \qquad \text{où} \qquad |\gamma| \leqq 10^6,$$

on a

$$|x| < 14293.$$

Siegel a aussi généralisé les résultats de Thue dans une autre direction. En effet, en étudiant l'approximation d'un nombre algébrique

par un autre nombre algébrique, il a démontré les théorèmes suivants : « Soit ξ un nombre algébrique de degré $n \geqq 2$. De plus, soit K un corps algébrique donné, et soit ξ la racine d'une équation de degré $d \geqq 2$ à coefficients appartenant au corps K et irréductible dans ce corps. Si η est un nombre algébrique $\neq 0$, nous désignons par $H(\eta)$ la plus grande des valeurs absolues de tous les coefficients entiers rationnels de l'équation irréductible dont α est racine. Cela posé, on a

1° Soient A et θ des nombres positifs donnés. Alors, l'inégalité

$$|\xi - \eta| \leqq \frac{A}{H(\eta)^{\frac{d}{s+1}+s+0}} \qquad (0 < s < d)$$

n'a qu'un nombre limité de solutions η en nombres primitifs du corps K;

2° Si h est un nombre entier $\geqq 1$, l'inégalité

$$|\xi - \eta| \leqq \frac{A}{H(\eta)^{h\left(\frac{n}{s+1}+s\right)+\theta}} \qquad (0 < s < n)$$

n'a qu'un nombre limité de solutions η en nombres algébriques de degré h [31, a]. »

Ces résultats conduisent aux théorèmes suivants sur le nombre de solutions de certaines équations en nombres entiers algébriques :

III. *Soit* K 1° *un corps algébrique de degré* h_0, *et soit* $U(x, y)$ *une forme homogène binaire de degré* d, *sans facteurs linéaires multiples, à coefficients appartenant au corps* K_0.

1° *Soit* K *un corps multiple de* K_0 *du degré relatif* h, *et soit, de plus,*

$$d > h\left(\frac{d}{s+1} + s\right), \qquad \text{où } s = \tfrac{1}{2}(\sqrt{4d+1} - 1).$$

Désignons enfin par $V(x, y)$ *un polynome qui jouit des propriétés suivantes : son degré est* $< d - h\left(\frac{d}{s+1} + s\right)$; *ses coefficients appartiennent au corps* K_0; *il n'a pas de facteur commun à* $U(x, y)$. *Cela posé, l'équation indéterminée*

$$U(x, y) = V(x, y)$$

n'a qu'un nombre fini de solutions en nombres entiers x, y du corps K;

2° *Soit* $d > h'\left(\frac{dh_0}{s'+1} + s'\right)$, *où* $s' = \frac{1}{2}\left(\sqrt{4dh_0+1} - 1\right)$. *Désignons par* $V(x, y)$ *un polynome qui jouit des propriétés suivantes : son degré est* $< d - h'\left(\frac{dh_0}{s'+1} + s'\right)$; *ses coefficients appartiennent au corps* K_0; *il n'a pas de facteur commun à* $U(x, y)$. *Cela posé, l'équation indéterminée*

$$U(x, y) = V(x, y),$$

n'a qu'un nombre fini de solutions en nombres entiers algébriques x, y de degré $\leqq h$.

8. **Quelques applications du théorème de Thue.** — Il y a certaines classes d'équations indéterminées qui peuvent être réduites à des équations de la forme

$$\varphi_n(x, y) = c,$$

où φ_n est homogène et sans facteurs multiples et de degré $\geqq 3$. Il résulte ainsi du théorème de Thue que les équations proposées n'ont qu'un nombre limité de solutions entières.

De cette manière, Thue [35, g] a démontré le théorème suivant :

I. *Désignons par* $P(x, y)$ *et* $Q(x, y)$ *deux polynomes homogènes à coefficients entiers des degrés p et q, respectivement,* $p > q$ *et* $p > 2$; *et soit* $P(x, y)$ *irréductible. Cela posé, l'équation indéterminée*

$$P(x, y) = Q(x, y) \tag{1}$$

n'a qu'un nombre limité de solutions en nombres entiers x, y.

Supposons que (1) ait une infinité de solutions x, y et posons

$$x = k\xi \quad \text{et} \quad y = k\eta,$$

où ξ et η sont premiers entre eux. Alors il y a une infinité de solutions entières ξ, η de l'équation

$$k^{p-q} P(\xi, \eta) = Q(\xi, \eta). \tag{2}$$

Or, on peut trouver deux polynomes homogènes à coefficients

entiers $A(\xi, \eta)$ et $B(\xi, \eta)$, tels qu'on ait

$$A(\xi, \eta)P(\xi, \eta) - B(\xi, \eta)Q(\xi, \eta) = h\eta^r,$$

où h est une constante entière, différent de zéro, et r une constante entière positive. En combinant cette équation avec (2), il vient

$$P(\xi, \eta)[A(\xi, \eta) - k^{p-q}B(\xi, \eta)] = h\eta^r.$$

On aura ainsi, pour une infinité de valeurs entières ξ, η,

$$P(\xi, \eta) = m,$$

où m est une constante. Or, cela est impossible.

Siegel [31, a] a montré que le théorème reste encore vrai si l'on remplace dans (1) $Q(x, y)$ par $Q(x, y).M(x, y)$, où $M(x, y)$ est un polynome (pas nécessairement homogène), à coefficients entiers, de degré $m < \frac{p-q}{p}.\left(p - \frac{p}{s+1} - s\right)$, où s est le plus grand nombre entier $\leqq \frac{1}{2}(\sqrt{4p+1}+1)$.

Thue a aussi appliqué son théorème pour établir le résultat suivant [35, i] :

II. *Soient a, b, c, d des nombres entiers, tels que $a \neq 0$, $b^2 - 4ac \neq 0$ et $d \neq 0$. Cela posé, l'équation indéterminée*

$$ay^2 + by + c = dx^n, \tag{3}$$

où n est un entier $\geqq 3$, n'a qu'un nombre limité de solutions.

Landau et Ostrowski [18] ont démontré ce théorème indépendamment de Thue à l'aide de la théorie des idéaux. Il suffit de prendre $a = 1$. Soit α une racine de l'équation $\alpha^2 + b\alpha + c = 0$: supposons que α soit irrationnel, et soit 1, ω une base des nombres entiers du corps quadratique engendré par α. Alors l'équation (3) entraîne

$$(y - \alpha) = \mathfrak{a}.\mathfrak{j}^n,$$

où $\mathfrak{a}$ et $\mathfrak{j}$ sont des idéaux du corps dont le premier ne prend qu'un nombre fini de valeurs. Il résulte de cette équation

$$\beta(y - \alpha) = \gamma(u + v\omega)^n,$$

où β et γ sont des nombres entiers du corps qui ne prennent qu'un

nombre fini de valeurs; u et v sont des entiers ordinaires. En prenant l'équation conjuguée, et en éliminant y, on aura

$$\frac{\beta\beta'(\alpha-\alpha')}{\omega-\omega'} = \frac{\beta\gamma'(u+v\omega')^n - \beta'\gamma(u+v\omega)^n}{\omega-\omega'} = f(u, v),$$

où $f(u, v)$ est un polynome homogène à coefficients entiers, de degré $n \geqq 3$, qui n'a pas de racine multiple. Le théorème de Thue s'applique ainsi; et le nombre de solutions entières de (3) est limité. Si les racines α et α' de $\alpha^2 + b\alpha + c = 0$ sont rationnelles, on aura

$$y - \alpha = ku^n, \qquad y - \alpha' = lv^n,$$

donc

$$\alpha' - \alpha = ku^n - lv^n,$$

où k et l ne prennent qu'un nombre fini de valeurs. On aura donc le même résultat.

Mordell [24, c] a appliqué la théorie des formes binaires biquadratiques à l'équation indéterminée

$$Ax^3 + Bx^2 + Cx + D = Ey^2, \tag{4}$$

où tous les coefficients sont entiers, $A \neq 0$, et où le polynome cubique n'a pas de facteur multiple, Il est facile de voir qu'il suffit de considérer l'équation suivante

$$v^2 = 4u^3 - g_2 u - g_3, \tag{5}$$

où g_2 et g_3 sont entiers. A chaque solution de cette équation correspond une forme binaire biquadratique

$$X^4 - 6uX^2Y^2 + 4vXY^3 + eY^4 = (1, 0, -u, v, e)(X, Y)^4, \tag{6}$$

où $e = g_2 - 3u^2$, aux invariants g_2, g_3. Toutes les formes binaires biquadratiques ayant ces invariants se divisent en un nombre fini de classes, c'est-à-dire elles se dérivent toutes d'un nombre fini d'entre elles,

$$ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 = (a, b, c, d, e)(x, y)^4,$$

par des substitutions unimodulaires

$$x = pX + rY, \qquad y = qX + sY$$

avec $ps - qr = 1$. Le coefficient de X^4 dans (6) est égal à 1, donc

$$ap^4 + 4bp^3q + 6cp^2q^2 + 4dpq^3 + eq^4 = 1. \tag{7}$$

Si l'équation (5) possède une infinité de solutions entières u, v, il existe donc une équation de la forme (7) ayant une infinité de solutions entières p, q. Or, cela est impossible d'après le théorème de Thue. Car, le côté gauche de (7) n'est jamais un carré parfait, puisque $4u^3 - g_2u - g_3$ ont toutes ses racines différentes. Il résulte de là le théorème :

III. *Si la courbe* (4) *est de genre* 1, *elle n'admet qu'un nombre fini de points entiers.*

Mordell [24, *d*] a aussi donné une autre démonstration de ce théorème. Considérons l'équation

$$x^3 + bx^2 + cx + d = y^2, \tag{8}$$

où le côté gauche est supposé irréductible. Soit θ une racine de $\theta^3 + b\theta^2 + c\theta + d = 0$. Alors l'équation proposée entraîne

$$(x - \theta) = \mathfrak{a}.\mathfrak{j}^2, \tag{9}$$

où $\mathfrak{a}$ et $\mathfrak{j}$ sont des idéaux du corps cubique engendré par θ, dont le premier ne prend qu'un nombre fini de valeurs. Si x_1 est une solution de l'équation (9), on est conduit à une équation

$$N^2(x - \theta)(x_1 - \theta) = (u + v\theta + w\theta^2)^2,$$

où N ne prend qu'un nombre fini de valeurs entières. Il résulte de là trois équations entre x, u, v et w. En éliminant x, on aura les équations

$$\Phi(u, v, w) = N^2, \qquad \Phi_1(u, v, w) = 0,$$

où Φ et Φ_1 sont des polynomes homogènes quadratiques en u, v et w. Les solutions de la dernière équation sont données par les formules

$$u = f_1(p, q), \qquad v = f_2(p, q), \qquad w = f_3(p, q),$$

où f_1, f_2, f_3 sont des formes binaires quadratiques de p et q. En introduisant ces valeurs de u, v, w dans la première équation, on aura l'équation

$$F(p, q) = N^2,$$

où F est une forme binaire biquadratique de p et q qui n'est pas un carré parfait. Ainsi, le théorème de Thue s'applique. Le cas où le côté gauche de (8) est réductible peut être traité d'une manière analogue.

Du théorème III, on tire le résultat suivant : La courbe

$$ax^4 + bx^3 + cx^2 + dx + e = y^2,$$

où le côté gauche a un facteur linéaire rationnel et n'admet aucun facteur multiple, n'a qu'un nombre limité de points entiers. On ne sait rien jusqu'ici sur le cas général où le côté gauche est irréductible.

D'une manière analogue, on peut montrer que l'équation

$$Ax^{2n} + Bx^n + C = y^2 \qquad (n \geqq 2)$$

n'admet qu'un nombre limité de solutions entières si le côté gauche n'est pas un carré parfait.

Maillet [23, c] a donné une méthode qui permet de reconnaître si une courbe de genre zéro possède une infinité ou seulement un nombre fini de points entiers. En effet, d'après son théorème du n° 2, les points rationnels (s'il y en a une infinité) sont donnés (à part un nombre fini) par les formules

$$x = \frac{f_2(t)}{f_1(t)}, \qquad y = \frac{f_3(t)}{f_1(t)}, \tag{10}$$

où f_1, f_2 et f_3 sont des polynomes en t à coefficients entiers, sans facteur commun. Supposons que f_i soit du degré n_i et posons

$$f_i(p, q) = q^{n_i} f_i\left(\frac{p}{q}\right).$$

Alors, pour déterminer les valeurs rationnelles de $t = \frac{p}{q}$ pour lesquelles x et y sont entiers, on aura à résoudre en nombres entiers l'équation indéterminée

$$f_1(p, q) = \pm B,$$

où B est un nombre entier positif qui n'a qu'un nombre fini de valeurs. On peut ainsi appliquer le théorème de Thue du numéro précédent. En particulier, on voit que, lorsque la courbe de degré n a une infinité de points entiers, $f_1(t)$ est ou bien une constante, ou bien, à un facteur entier constant près, une puissance $n^{\text{ième}}$ d'un poly-

nome de premier degré à coefficients entiers

$$f_1(t) = \alpha(\mathrm{M}t + \mathrm{N})^n, \tag{11}$$

ou bien, n étant pair, une puissance $\left(\frac{n}{2}\right)^{\text{ième}}$ d'un polynome irréductible du deuxième degré à coefficients entiers

$$f_1(t) = \alpha(\mathrm{M}t^2 + \mathrm{N}t + \mathrm{P})^{\frac{n}{2}} \tag{12}$$

avec $\mathrm{N}^2 - 4\mathrm{MP}$ positif. Il résulte de là le théorème :

IV. *Soit une équation algébrique indécomposable* $f(x, y) = 0$ *de degré* $n \geqq 2$ *et de genre* 0 *à coefficients entiers, qui possède une infinité de solutions en nombres entiers* x, y *: les coordonnées* x, y *peuvent s'exprimer en fonction rationnelle, à coefficients entiers, de la forme* (10), *d'un paramètre* t. *Les conditions suivantes sont nécessaires : si* $f_1(t)$ *n'est pas une constante,* f_1 *sera de degré* $n_1 = n$ *et d'une des formes* (11) *ou* (12); *dans ces deux derniers cas, les solutions (à part un nombre limité pouvant correspondre aux points doubles et à* $t = \infty$) *sont données par des valeurs rationnelles* $\frac{p}{q}$ *de* t, *où* p, q *sont aussi des solutions en entiers d'une des équations*

$$\mathrm{M}p + \mathrm{N}q = \pm\beta, \qquad \mathrm{M}p^2 + \mathrm{N}pq + \mathrm{P}q^2 = \pm\beta, \tag{13}$$

respectivement, β *étant une constante qui n'a qu'un nombre fini de valeurs.*

On sait résoudre complètement les équations (13). Quand elles sont possibles, il y a une infinité de solutions p, q. Si toutes les équations (13) sont impossibles, il n'y a qu'un nombre limité de points entiers. S'il y a des solutions p, q, pour une valeur de β, on aura à satisfaire aux conditions simultanées

$$f_1(p, q) = \pm \mathrm{B},$$
$$f_2(p, q) \equiv 0 \pmod{\mathrm{B}}, \qquad f_3(p, q) \equiv 0 \pmod{\mathrm{B}},$$

où $\mathrm{B} = \alpha\beta^n$ ou $= \alpha\beta^{\frac{n}{2}}$. Il est évident qu'on peut résoudre ce système par un nombre fini d'opérations. On peut ainsi reconnaître si la

courbe admet une infinité de points entiers ou non. La méthode permet aussi de déterminer tous les points entiers de la courbe, sauf dans le cas où $f_1(t)$ est la puissance d'une fonction irréductible de degré ≥ 3. Dans ce dernier cas, il n'y a qu'un nombre limité de points entiers, ainsi qu'il résulte du théorème de Thue; ce théorème ne donne pourtant aucun moyen pour effectivement déterminer les solutions.

9. **La représentation d'un nombre entier par une forme binaire de degré ≥ 3.** — Deux formes binaires à coefficients entiers, $f(x, y)$ et $\varphi(x', y')$, sont dites équivalentes ou de même classe quand elles sont liées par une transformation unimodulaire

$$x' = ax + by, \qquad y' = cx + dy,$$

où a, b, c, d sont des entiers tels que $ad - bc = \pm 1$. Deux formes équivalentes représentent les mêmes nombres entiers pour des valeurs entières des variables. D'après le théorème de Thue du n° 7, nous savons qu'il n'y a qu'un nombre limité de représentations d'un nombre entier donné quand la forme est irréductible et de degré ≥ 3.

Le nombre de représentations d'un nombre entier donné est le même pour deux formes équivalentes. Dans la suite, les formes sont toujours supposées irréductibles et, bien entendu, à coefficients entiers.

Lagrange [17] a montré comment on peut réduire le problème de résoudre en nombres entiers l'équation

$$\text{(1)} \qquad F(x, y) = N,$$

où F est une forme binaire, à coefficients entiers, et N un nombre entier différent de zéro, au problème de résoudre en nombres entiers u, v un certain nombre d'équations

$$\text{(2)} \qquad G(u, v) = 1,$$

où les G sont des formes binaires à coefficients entiers du même degré que F. En effet, supposons pour simplifier que x soit premier à N, et soit η_1 une racine de la congruence

$$F(1, y) \equiv 0 \pmod{N}.$$

En posant dans (1) $y = x\eta - Nz$, on aura

$$F(x, y) = F(x, x\eta - Nz) = N\,G(x, z) = N.$$

où les G ont tous leurs coefficients entiers. Le nombre des formes G est ainsi au plus égal à N.

Ainsi, on peut se borner à l'étude de la représentation de l'unité par les formes binaires. On ne possède aucun moyen général pour reconnaître si une forme binaire (de degré $\geqq 3$) donnée quelconque peut représenter l'unité ou non. Soit $f(x, y)$ une forme binaire irréductible de degré $n \geqq 3$, et soit α une racine de l'équation $f(x, 1) = 0$. Si l'équation $f(x, y) = 1$ possède une solution $x = x_0, y = y_0$, la forme f est équivalente à une autre forme g, où le coefficient de x^n est égal à 1. En effet, on aura une telle forme g en transformant la forme f par la transformation unimodulaire

$$x = x_0 u + bv, \qquad y = y_0 u + dv$$

avec $x_0 d - y_0 b = \pm 1$. Si le coefficient de x^n dans $f(x, y)$ est égal à 1, la racine α de l'équation $f(x, -1) = 0$ est un nombre algébrique entier de degré n. Alors, le problème de résoudre l'équation

$$f(x, y) = 1$$

en nombres entiers x, y reviendra au problème de déterminer toutes les unités, de norme 1, de la forme $x + \alpha y$ appartenant à l'anneau $R(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ dans le corps algébrique de degré n engendré par α.

Pour obtenir des résultats plus précis que celui de Thue, il faut spécialiser les formes. Les formes les plus simples sont les formes cubiques à discriminant négatif. Dans la suite, nous désignons la forme cubique

$$f(x, y) = ax^3 + bx^2 y + cxy^2 + dy^3$$

par (a, b, c, d) et son discriminant par D. Quand $D < 0$, l'équation

$$ax^3 + bx^2 + cx + d = 0$$

a une seule racine réelle. Dans le corps cubique engendré par cette racine, il existe une unité fondamentale ξ, $0 < \xi < 1$, telle que chaque unité ε puisse se mettre sous la forme

$$\varepsilon = \pm \xi^n,$$

où n est un entier quelconque. Il existe une telle unité fondamentale pour toutes les unités d'un anneau donné quelconque du corps.

Le premier résultat général sur ces formes a été donné par Delaunay [3, a, b, d, g], qui a démontré le théorème :

I. *L'équation indéterminée*

$$x^3 + dy^3 = 1 \tag{3}$$

possède au plus une seule solution en nombres entiers x, y en dehors de la solution triviale $y = 0$, $x = 1$. Si $x = x_1$, $y = y_1$ est une solution, le nombre

$$x_1 + y_1 \sqrt[3]{d}$$

est l'unité fondamentale de l'anneau $\mathrm{R}(1, \sqrt[3]{d}, \sqrt[3]{d^2})$ *du corps* $\mathrm{K}(\sqrt[3]{d})$ (1).

Pour démontrer ce théorème il suffit de montrer que, η étant une unité positive de l'anneau R, la puissance η^p, où p est un nombre premier quelconque, n'est jamais de la forme $\mathrm{X} + \mathrm{Y}\sqrt[3]{d}$. Une unité positive de cette forme est toujours < 1. Posons, pour abréger, $\sqrt[3]{d} = \theta$. Si $\eta = x + y\theta$, on aura à démontrer que l'équation

$$(x + y\theta)^p = \mathrm{X} + \mathrm{Y}\theta$$

est impossible. En effet, elle conduira à

$$\binom{p}{2} x^{p-2} y^2 + \binom{p}{5} x^{p-5} y^5 d + \binom{p}{8} x^{p-8} y^8 d^2 + \ldots = 0.$$

Il résulte de cette équation que tous les facteurs premiers de y divisent x et inversement. Or, x et y étant premiers entre eux, on a, par suite, $x = -1$, $y = 1$, ce qui est impossible. Ainsi η ne peut pas être de la forme $x + y\theta$; elle n'est non plus de la forme $x + z\theta^2$. Alors il faut que $\eta = x + y\theta + z\theta^2$, où y et z sont différents de zéro. Si η est positive, sa norme est égale à

$$\mathrm{N}(\eta) = x^3 + dy^3 + d^2 z^3 - 3\,dxyz = 1. \tag{4}$$

---

(1) On peut même montrer qu'il est l'unité fondamentale du corps, ou bien, dans un nombre limité de cas, le carré de l'unité fondamentale. (*Voir* Nagell [25, *e*].)

Soit p un nombre premier. En égalant à zéro le coefficient de θ^2 dans η^p, on aura l'équation

$$(x+y\theta+z\theta^2)^p = -\rho(x+y\rho\theta+z\rho^2\theta^2)^p - \rho^2(x+y\rho^2\theta+z\rho\theta^2)^p,$$

ρ étant une racine de l'équation $\rho^2+\rho+1=0$. Si p est de la forme $6n+1$, cette équation peut s'écrire

$$(x+y\theta+z\theta^2)^p = -(x\rho+y\rho^2\theta+z\theta^2)^p - (x\rho^2+y\rho\theta+z\theta^2)^p.$$

Puisque p est impair, il résulte de là que le nombre

$$(x\rho+y\rho^2\theta+z\theta^2)+(x\rho^2+y\rho\theta+z\theta^2) = -x-y\theta+2z\theta^2$$

est une unité du corps $K(\theta)$. En prenant la norme, on a donc

$$-x^3-dy^3+8d^2z^3-6dxyz = \pm 1. \tag{5}$$

Or, il est facile de montrer que cette équation est incompatible avec l'équation (4). Donc, η^p n'est jamais de la forme $X+Y\theta$ quand $p=6n+1$. D'une manière analogue, on traitera le cas de $p=6n-1$, ainsi que les cas de $p=2$ et $p=3$.

Par conséquent, si η est l'unité fondamentale de l'anneau R, la puissance η^n n'est jamais de la forme $x+y\theta$ lorsque $n>1$ et le théorème se trouve démontré. On sait ainsi résoudre complètement l'équation (3); car il existe des méthodes (de Minkovski, par exemple), pour déterminer l'unité fondamentale d'un anneau quelconque.

Ce résultat a été généralisé par Nagell qui a montré comment on peut résoudre complètement l'équation

$$Ax^3+By^3=C, \tag{6}$$

où C a une des valeurs 1 ou 3. Sans rien prendre de la généralité, nous pouvons faire les suppositions suivantes : les entiers A et B sont positifs et $A>B$. AB n'est pas divisible par le cube d'un nombre premier. Quand $C=3$, AB n'est pas divisible par 3. Lorsque les deux corps cubiques engendrés par $\sqrt[3]{\frac{A}{B}}$ et $\sqrt[3]{\frac{A_1}{B_1}}$ sont identiques, nous disons que les deux équations

$$Ax^3+By^3=C \qquad \text{et} \qquad A_1x^3+B_1y^3=C_1$$

appartiennent à la même famille, à la famille du corps $K\left(\sqrt[3]{\frac{A}{B}}\right)$.

Cela posé, les résultats principaux de Nagell peuvent se résumer comme il suit [25, *e*] :

II. *L'équation* (6) *possède au plus une seule solution en nombres entiers* x, y, *différents de zéro. Il y a l'unique exception pour l'équation*

$$2x^3+y^3=3,$$

qui possède exactement les deux solutions $x=y=1$ *et* $x=4$, $y=-5$.

Parmi toutes les équations de la même famille, il y en a au plus une seule qui est possible en nombres entiers, sauf pour les familles des corps $K(\sqrt[3]{2})$ *et* $K(\sqrt[3]{20})$. *Dans la famille du corps* $K(\sqrt[3]{2})$, *il y a trois équations possibles, savoir :*

$$2x^3+y^3=1, \qquad 2x^3+y^3=3 \qquad \text{et} \qquad 4x^3+y^3=3.$$

Dans la famille du corps $K(\sqrt[3]{20})$, *il y a deux équations possibles, savoir :*

$$20x^3+y^3=1 \qquad \text{et} \qquad 5x^3+2y^3=3.$$

Il est évident que le problème de résoudre l'équation (6) revient au même que de trouver toutes les unités positives de la forme

$$(7) \qquad \eta=\frac{1}{C}\left[x\sqrt[3]{A}+y\sqrt[3]{B}\right]^3=1+\frac{3}{C}x^2y\sqrt[3]{A^2B}+\frac{3}{C}xy^2\sqrt[3]{AB^2}$$

dans le corps $K(\sqrt[3]{AB^2})$. Une unité de cette forme est toujours <1, sauf dans le cas $\eta=\frac{1}{3}\left[\sqrt[3]{2}+1\right]^3$. Nous pouvons laisser de côté le cas de $B=C=1$. Le premier but de la démonstration est de montrer que, ξ étant une unité positive <1 du corps $K(\sqrt[3]{AB^2})$, la puissance ξ^m n'est jamais de la forme (7) quand m est impair >1. Posons $A=ac^2$ et $B=bd^2$, où a, b, c et d sont des entiers positifs, tels que $abcd$ ne soit divisible par aucun carré >1. Pour simplifier, bornons-nous au cas de $C=1$. Soit η une unité positive <1, et considérons l'équation

$$(x\sqrt[3]{ac^2}+y\sqrt[3]{bd^2})^3=\eta^p,$$

où p est un nombre premier impair. $p=3$ est évidemment impossible. Si nous supposons que $p=6m+1$, il suit de cette équation

que $\sqrt[3]{\eta}$ est de la forme

$$\varepsilon = \sqrt[3]{\eta} = \frac{1}{3}\left(x_1 \sqrt[3]{ac^2} + y_1 \sqrt[3]{bd^2} + z_1 \sqrt[3]{a^2cb^2d}\right)$$

ε est donc une unité dans le corps du neuvième degré $\Omega\left(\sqrt[3]{ac^2}, \sqrt[3]{bd^2}\right)$ et en prenant la norme de ε, on aura l'équation

$$x_1^3 ac^2 + y_1^3 bd^2 + z_1^3 a^2cb^2d - 3x_1y_1z_1abcd = 27. \tag{8}$$

Nous aurons à traiter l'équation suivante :

$$\varepsilon^p = x\sqrt[3]{ac^2} + y\sqrt[3]{bd^2}. \tag{9}$$

En prenant les équations conjuguées, où $\sqrt[3]{bd^2}$ est remplacé par $\rho\sqrt[3]{bd^2}$ et $\rho^2\sqrt[3]{bd^2}$, on peut éliminer x et y, et il viendra

$$-\varepsilon^p = \left[\frac{x_1\rho\sqrt[3]{ac^2} + y_1\rho^2\sqrt[3]{bd^2} + z_1\sqrt[3]{a^2cb^2d}}{3}\right]^p + \left[\frac{x_1\rho^2\sqrt[3]{ac^2} + y_1\rho\sqrt[3]{bd^2} + z_1\sqrt[3]{a^2cb^2d}}{3}\right]^p.$$

Il résulte de cette équation que le nombre

$$\begin{aligned} &\frac{1}{3}\left(x_1\rho\sqrt[3]{ac^2} + y_1\rho^2\sqrt[3]{bd^2} + z_1\sqrt[3]{a^2cb^2d}\right) \\ &+ \frac{1}{3}\left(x_1\rho^2\sqrt[3]{ac^2} + y_1\rho\sqrt[3]{bd^2} + z_1\sqrt[3]{a^2cb^2d}\right) \\ &= \frac{1}{3}\left(-x_1\sqrt[3]{ac^2} - y_1\sqrt[3]{bd^2} + 2z_1\sqrt[3]{a^2cb^2d}\right) \end{aligned}$$

est une unité dans le corps Ω. En prenant sa norme, on aura l'équation

$$-x_1^3 ac^2 - y_1^3 bd^2 + 8z_1^3 a^2cb^2d - 6x_1y_1z_1abcd = \pm 27.$$

Or, on démontrera facilement que cette équation est incompatible avec l'équation (8), sauf dans le cas de $z_1 = 0$. Dans ce cas, l'équation (9) deviendra

$$\left(\frac{1}{3}x_1\sqrt[3]{ac^2} + \frac{1}{3}y_1\sqrt[3]{bd^2}\right)^p = x\sqrt[3]{ac^2} + y\sqrt[3]{bd^2}.$$

L'impossibilité de cette équation résulte du lemme suivant : « Soient x, y et D des nombres rationnels différents de zéro, et soit $\sqrt[3]{D}$ irra-

tionnel. Alors, les coefficients rationnels X, Y, Z dans l'équation

$$(x+y\sqrt[3]{\mathrm{D}})^n = \mathrm{X}+\mathrm{Y}\sqrt[3]{\mathrm{D}}+\mathrm{Z}(\sqrt[3]{\mathrm{D}})^2,$$

avec n entier >1, sont tous différents de zéro, sauf dans les cas suivants :

$$n=4, \quad \mathrm{D}=-4\left(\frac{x}{y}\right)^3; \qquad n=5, \quad \mathrm{D}=-10\left(\frac{x}{y}\right)^3;$$
$$n=6, \quad \mathrm{D}=-\frac{5}{2}\left(\frac{x}{y}\right)^3.$$

On peut traiter le cas de $p=6m-1$ de la même manière. On aura ainsi le résultat suivant : *Si* ξ *est l'unité fondamentale du corps* $\mathrm{K}(\sqrt[3]{\mathrm{AB}^2})$, $0<\xi<1$, *et si* $(x\sqrt{\mathrm{A}}+y\sqrt[3]{\mathrm{B}})^3=\xi^m$, *on a forcément* $m=2^n$ *avec* $n=0, 1, 2, 3, \ldots$ (B est supposé >1). Pour les unités de la forme $\frac{1}{3}(x\sqrt[3]{\mathrm{A}}+y\sqrt[3]{\mathrm{B}})^3$, on trouvera le même résultat.

De ce résultat, on peut aisément, en se servant du lemme ci-dessus, déduire le théorème II.

La méthode donne aussi un procédé pour effectivement déterminer toutes les solutions de l'équation (6). En effet, on peut réduire le problème de résoudre l'équation

$$\mathrm{A}x^3+\mathrm{B}y^3=1 \qquad (\mathrm{A}>\mathrm{B}>1)$$

au problème de résoudre un nombre fini d'équations

$$\mathrm{A}_1x^3+\mathrm{B}_1y^3=1 \qquad (\mathrm{A}_1>\mathrm{B}_1\geqq 1),$$

où tous les facteurs premiers de $\mathrm{A}_1\mathrm{B}_1$ divisent A ou bien divisent B Le problème sera ainsi ramené à un nombre fini d'équations

$$dx^3+y^3=1,$$

où tous les facteurs premiers de d divisent A ou bien divisent B. Or, on sait résoudre complètement ces dernières équations en vertu du théorème I. La résolution de l'équation

$$\mathrm{A}x^3+\mathrm{B}y^3=3$$

peut être ramenée à celle de l'équation

$$\mathrm{A}x^3+\mathrm{B}y^3=1,$$

On doit noter que les théorèmes I et II, ainsi que les théo-

rèmes III et IV ci-après, sont démontrés sans application du théorème de Thue.

Le premier résultat sur la forme générale (a, b, c, d) à discriminant D négatif est aussi dû à Delaunay [3, c, e]. Il a démontré le théorème suivant sur le nombre de représentations de l'unité par cette forme :

III. *L'équation indéterminée* $(a, b, c, d) = 1$ *possède au plus quatre solutions en nombres entiers, sauf dans le cas d'une forme équivalente à* $(1, 0, -1, 1)$. *L'équation* $(1, 0, -1, 1) = 1$ *possède exactement cinq solutions, savoir* $x = 0$, $y = 1$; $x = 1$, $y = 0$; $x = y = 1$; $x = -1$, $y = 1$; $x = 4$, $y = -3$. *Si la forme n'est pas équivalente à une forme* $(1, p, q, 1)$, *l'équation* $(a, b, c, d) = 1$ *possède au plus deux solutions.*

Il suffit de démontrer le théorème pour la forme $(1, p, q, r)$. Soit α une racine de l'équation $(1, -p, q, -r) = 0$. Soit, de plus, ε l'unité fondamentale de l'anneau $R(\alpha)$, $0 < \varepsilon < 1$. Alors, il s'agit de trouver les exposants entiers n, pour lesquels on a

$$\varepsilon^n = x + \alpha y. \tag{10}$$

On vérifie aisément qu'il suffit de considérer le cas de n positif.

On établit sans peine le lemme suivant : « Si $c + b\alpha$ est une unité, $b \neq 0$ et $\neq \pm 1$, et si $n > 1$, on n'a jamais

$$(c + b\alpha)^n = C + B\alpha.$$

Posons ensuite $\varepsilon = a\alpha^2 + b\alpha + c$. Il résulte de l'équation (10)

$$\varepsilon'^n - \varepsilon''^n = (\alpha' - \alpha'')y.$$

Tous les y sont ainsi divisibles par

$$\frac{\varepsilon' - \varepsilon''}{\alpha' - \alpha''} = a(\alpha' + \alpha'') + b = -a\alpha + b + ap,$$

Donc, si le plus grand commun diviseur de a et b est $(a, b) = d$, tous les y sont divisibles par

$$k = \frac{1}{d^2} N(-a\alpha + b + ap),$$

où $N(\beta)$ désigne la norme de β. Nous pouvons alors passer à l'an-

neau $R(k\alpha)$. Posons $y_1 = \frac{y}{k}$ et $\alpha_1 = k\alpha$, et soit

$$\alpha_1^3 = p_1\alpha_1^2 - q_1\alpha_1 + r_1.$$

Soit, de plus,

$$\varepsilon_1 = \varepsilon^{\nu} = a_1\alpha_1^2 + b_1\alpha_1 + c_1$$

l'unité fondamentale du nouvel anneau, $0 < \varepsilon_1 < 1$. Au lieu de l'équation (10), nous aurons donc

$$\varepsilon_1^{\overset{n}{\nu}} = x + \alpha_1 y_1.$$

Si $d_1 = (a_1, b_1)$, on conclut de cette équation que tous les y_1 sont divisibles par

$$k_1 = \frac{1}{d_1^2} N(-a_1\alpha_1 + b_1 + a_1 p_1).$$

Nous pouvons ainsi passer à l'anneau $R(\alpha_2)$ où $\alpha_2 = k_1\alpha_1$. Nous pouvons continuer de la même manière jusqu'à ce que nous nous trouvons dans l'anneau $R(\alpha_i)$. Alors, on a

$$\alpha_i = kk_1k_2\ldots k_{i-1}\alpha \qquad \text{et} \qquad \alpha_i^3 = p_i\alpha_i^2 - q_i\alpha_i + r_i.$$

L'unité fondamentale de l'anneau est

$$\varepsilon_i = \varepsilon^{\mu} = a_i\alpha_i^2 + b_i\alpha_i + c_i, \qquad 0 < \varepsilon_i < 1.$$

Au lieu de l'équation (10), on a

$$\varepsilon_i^{\overset{n}{\mu}} = x + \alpha_i y_i, \tag{11}$$

où $y = kk_1k_2\ldots k_{i-1}y_i$. Si $d_i = (a_i, b_i)$, tous les y_i sont divisibles par

$$k_i = \frac{1}{d_i^2} N(-a_i\alpha_i + b_i + a_i p_i).$$

Or, le nombre y n'a qu'un nombre fini de diviseurs. On tombera ainsi nécessairement une fois sur le cas, où k_i deviendra $= \pm 1$. Dans ce cas, on aura $d_i = 1$; et le nombre $-a_i\alpha_i + b_i + a_i p_i = \zeta$ doit être une unité. Soit d'abord $\zeta = \pm 1$, donc $a_i = 0$, $b_i = \pm 1$ et $\varepsilon_i = \pm\alpha_i + c_i$.

Alors il résulte de l'équation (11)

$$\varepsilon^n = (\pm kk_1k_2\ldots\alpha + c_i)^{\overset{n}{\mu}} = x + \alpha y.$$

Or, si l'équation (10) a au moins deux solutions y différentes de zéro, cette équation entraîne, à cause du lemme ci-dessus, que $kk_1k_2\ldots = \pm 1$. On a ainsi déjà $k = \pm 1$, donc $\varepsilon_i = \varepsilon = \pm\alpha + c$.

Soit ensuite ζ une unité algébrique $= \pm\varepsilon_i^m = \pm(A + \alpha_i C)$, où m est positif $\geqq 2$. Dans ce cas, les discriminants de ε_i et α_i sont égaux; les anneaux $R(\alpha_i)$ et $R(\varepsilon_i)$ sont identiques et les formes correspondantes sont équivalentes. On peut choisir B et D, tels que la transformation $x = Au + Bv$, $y_i = Cu + Dv$, avec $AD - BC = \pm 1$, transformera l'équation (11) en

$$\varepsilon_i^{\frac{n}{\mu}} = \varepsilon_i^m (u + \varepsilon_i v).$$

Posons $\varepsilon_i^{-1} = \eta$. Nous avons

$$\eta_1 = a'\alpha_i^2 + b'\alpha_i + c' = kk_1k_2\ldots\beta + c',$$

où β est un nombre entier algébrique. Pour $\frac{n}{\mu} = o$, on aura donc

$$\varepsilon_i^{-m-1} = u_1\varepsilon^{-1} + v_1 = \eta_1^{m+1} = u_1\eta_1 + v_1.$$

Or, cette équation est impossible d'après le lemme ci-dessus, sauf pour $kk_1k_2\ldots = \pm 1$. On a ainsi déjà $k = \pm 1$.

Il résulte de ce qui précède : Si la forme n'est pas équivalente à une forme $(1, p, q, 1)$, elle possède au plus deux représentations de l'unité. Une forme $(1, pk, qk^2, rk^3)$ avec $k > 1$, possède au plus deux représentations.

Delaunay a appelé cette méthode « l'algorithme de rehaussement ». Passons maintenant aux formes $(1, p, q, 1)$. Si ξ est la racine de $x^3 = px^2 - qx + 1$, on aura à étudier l'équation

$$\varepsilon^n = x + \varepsilon y.$$

Considérons d'abord le cas de n pair $= 2m$. Si m est positif, tous les y sont divisibles par $\frac{(\varepsilon')^2 - (\varepsilon'')^2}{\varepsilon' - \varepsilon''} = \varepsilon' + \varepsilon''$. Ainsi, tous les y sont divisibles par $k = N(\varepsilon' + \varepsilon'')$. Si m est négatif, tous les y sont divisibles par $\frac{(\eta')^2 - (\eta'')^2}{\varepsilon' - \varepsilon''}$, où $\eta = \varepsilon^{-1}$. Or, on a

$$N\left[\frac{(\eta')^2 - (\eta'')^2}{\varepsilon' - \varepsilon''}\right] = N(\varepsilon' + \varepsilon'').$$

Ainsi, tous les y sont toujours divisibles par k. Supposons que

$k \neq \pm 1$. Dans ce cas, on est ramené à une forme $(1, pk, qk^2, k^3)$, qui possède, d'après ce qui précède, au plus deux représentations.

Considérons ensuite le cas de n impair $= 2m + 1$. Dans ce cas, on aura

$$\varepsilon^{2m} = x\eta + y.$$

D'une manière analogue, on démontrera que tous les x sont divisibles par $N(\varepsilon' + \varepsilon'') = k$. Or, si $k \neq \pm 1$, on est ramené à une forme $(k^3, pk^2, qk, 1)$, qui possède au plus deux représentations. Ainsi, la forme $(1, p, q, 1)$ possède au plus quatre représentations.

Il reste encore à traiter le cas de $N(\varepsilon' + \varepsilon'') = \pm 1$, c'est-à-dire le cas de $p = 0$. [Le cas de $pq = 2$ conduit à $(1, 0, -1, 1)$.] On trouvera que la forme $(1, 0, q, 1)$ possède exactement trois représentations si $q \neq \pm 1$. Les formes $(1, 0, 1, 1)$ et $(1, 0, -1, 1)$ en ont quatre et cinq respectivement.

Dans un certain nombre de cas, cette méthode de « rehaussement » donne aussi la solution complète. En effet, supposons que la méthode nous a conduit à une forme « rehaussée » $(1, pk, qk^2, rk^3)$. Supposons, de plus, que le facteur k soit divisible par un nombre premier impair π. Soit $\varepsilon = a\alpha^2 + b\alpha + c$ l'unité fondamentale de la forme initiale $(1, p, q, r)$: et soit μ le plus petit exposant positif, tel que dans

$$\varepsilon^{\mu} = A\alpha^2 + B\alpha + C,$$

les coefficients A et B soient divisibles par π. Si A n'est pas divisible par π^2, il est facile de montrer que, dans l'équation

$$\varepsilon^{\mu\nu} = H\alpha^2 + K\alpha + L,$$

le coefficient H n'est jamais égal à zéro. Il résulte de là que l'équation $\varepsilon^n = x + \alpha y$ est impossible puisque y est divisible par k, et donc par π. Or, on n'a pu démontrer qu'un tel diviseur premier π doit nécessairement apparaître. D'ailleurs, dans tous les exemples numériques traités jusqu'ici, c'est le cas.

Delaunay a aussi proposé une méthode analogue dans le cas général d'une forme (a, b, c, d) [3, f].

Nagell [25, a, b, e, f] a, indépendamment de Delaunay, développé une autre méthode pour traiter les formes cubiques à discriminant négatif. Considérons d'abord l'équation $x^3 + dy^3 = 1$. Soit ζ l'unité fondamentale de l'anneau $R(\theta)$, où $\theta = \sqrt[3]{d}$, et soit $0 < \zeta < 1$. Pour

trouver les unités (positives) de la forme $x + y\theta$, on a à examiner la suite $\zeta, \zeta^2, \zeta^3, \ldots$. Soit

$$\eta = x + y\theta = \zeta^m$$

le premier terme de la suite ayant cette forme, et soit

$$\zeta^M = X + Y\theta$$

une autre unité de la même forme; donc, $M > m \geqq 1$. Soit encore $M = nm + r$ avec $0 < r \leqq m - 1$. Car, si $r = 0$, on aurait

$$(x + y\theta)^n = X + Y\theta.$$

Or, nous avons déjà vu que cette équation est impossible. Posons

$$\varepsilon = \zeta^r = u + v\theta + w\theta^2,$$

où u, v, w sont entiers; w est différent de zéro. Nous avons l'équation

$$\zeta^M = X + Y\theta = (x + y\theta)^n(u + v\theta + w\theta^2).$$

En y égalant à zéro, le coefficient de θ^2, on aura une équation entre x, y, u, v et w. Cette dernière équation entraîne que $w \equiv 0 \pmod{y}$.

Le nombre w peut être exprimé par ε et ses conjugués par l'équation

$$3w\theta^2 = \varepsilon + \varepsilon'\rho + \varepsilon''\rho^2;$$

w étant divisible par y, il résulte de là l'inégalité

$$3|y|\theta^2 \leqq 3|w\theta^2| < 1 + 2|\varepsilon'| < 1 + 2|\eta'|,$$

d'où

$$3|y|\theta^2 < 1 + 2\sqrt{3}(1 + |y|\theta).$$

Or, cette inégalité est impossible pour $|y| \geqq 1$ et $d \geqq 8$, ainsi que pour $|y| \geqq 2$ et $d \geqq 5$. Il résulte de là que l'équation proposée possède au plus une seule solution avec $y \neq 0$. (Les valeurs $d = 2$, 3, 4 et 7 qui échappent à l'analyse précédente peuvent être traitées directement.) On peut même, à l'aide de cette méthode, démontrer le théorème II [25, f].

En généralisant la méthode, Nagell [25, g] a démontré le théorème suivant :

IV. *L'équation indéterminée* $(a, b, c, d) = 1$, *à discriminant négatif, possède au plus trois solutions en nombres entiers, sauf dans les trois cas suivants :* 1° *Si* (a, b, c, d) *est équivalente*

à (1, 0, 1, 1), *il y a exactement quatre solutions;* 2° *si* (a, b, c, d) *est équivalente à* (1, — 1, 1, 1), *il y a exactement quatre solutions;* 3° *si* (a, b, c, d) *est équivalente à* (1, 0, — 1, 1), *il y a exactement cinq solutions.*

Pour établir ce théorème, on commencera par montrer qu'il suffit de traiter le problème suivant : Étant donnée une unité η, racine de l'équation $x^3 = px^2 - qx + 1$ à discriminant D négatif, trouver le nombre des unités de la forme $\eta^m = a\eta + b$. On aura à montrer que, à part les trois cas d'exception, il n'y a qu'une seule unité au plus de la forme $a\eta + b$ avec ab différent de zéro. Il est facile de voir qu'on peut supposer m positif. Soit maintenant η^m la première puissance dans la suite $\eta^2, \eta^3, \eta^4, \ldots$, qui est de la forme

$$\eta_1^m = a\eta_1 + b,$$

et soit $A\eta + B$ une autre unité de la même forme,

$$\eta_1^M = A\eta_1 + B.$$

Soit, de plus, $M = nm + r$, avec $0 \leq r \leq m - 1$. On peut même montrer que $3 \leq r \leq m - 2$. Si l'on pose

$$\varepsilon = \eta_1^r = x + y\eta_1 + z\eta_1^2,$$

le coefficient z est différent de zéro puisque $r < m$. Nous avons

$$(a\eta_1 + b)^n (x + y\eta_1 + z\eta_1^2) = A\eta_1 + B.$$

En y égalant à zéro le coefficient de η^2, on aura une équation entre a, b, x, y et z. Il résulte de cette équation que z est divisible par a. Le nombre z peut être exprimé par ε et ses conjugués comme il suit :

$$z = \pm \frac{1}{\sqrt{D}} [(\eta_1' - \eta'')\varepsilon + (\eta_1 - \eta_1')\varepsilon'' + (\eta'' - \eta_1)\varepsilon'], \tag{12}$$

D étant le discriminant de η. Nous avons les inégalités suivantes :

$$\eta_1^3 \geq \eta_1^r = \varepsilon \geq \eta_1^{m-3},$$

$$|\varepsilon'| = |\varepsilon''| \leq |\eta'|^{m-2} = \left|\frac{a\eta_1' + b}{\eta_1'^2}\right| < \left|\frac{a}{\eta_1'}\right| + \frac{|a| - 1}{|\eta_1'|^2}.$$

z étant divisible par a, on aura $|z| \geq |a|$ et l'équation (12) entraînera

$$|a\sqrt{D}| < \frac{2}{|\eta_1'|^3} + 2(1 + |\eta_1'|)\left(\left|\frac{a}{\eta_1'}\right| + \frac{|a| - 1}{|\eta_1'|^2}\right).$$

Puisque $|\eta'| > 1$, il résulte de là

$$|a\sqrt{D}| < -2 + 8a \qquad \text{ou bien} \qquad -D < 64.$$

Le théorème se trouve ainsi démontré pour tous les η à discriminant $D \geqq -64$. Les autres valeurs de η peuvent être traitées par des méthodes spéciales.

Le théorème IV n'est pas susceptible d'une précision ultérieure. Il existe, en effet, une infinité de formes (a, b, c, d) inéquivalentes qui admettent trois représentations de l'unité, par exemple les formes $(1, 0, q, 1)$, q positif, qui représentent l'unité pour $x = 0, y = 1$; $x = 1, y = 0$; $x = 1, y = -q$.

Il résulte des théorèmes III et IV, en profitant du résultat de Lagrange ci-dessus : *L'équation* $(a, b, c, d) = N$ *possède au plus* $5N$ *solutions en nombres entiers, premiers entre eux.*

C'est un fait remarquable que la limite est indépendante des coefficients de la forme. Cependant, on ne sait pas encore résoudre complètement cette équation dans le cas général.

On ne sait rien jusqu'ici sur les formes cubiques à discriminant positif en dehors du fait qu'il n'y a qu'un nombre limité de représentations d'un nombre entier. L'exemple le plus simple est l'équation

$$x^3 - 3xy^2 + y^3 = 1.$$

Soit η une racine de l'équation $x^3 - 3x + 1 = 0$. Un système d'unités fondamentales du corps $k(\eta)$ contient deux unités $\varepsilon_1, \varepsilon_2$.

On peut, par exemple, prendre $\varepsilon_1 = \eta$ et $\varepsilon_2 = 1 - \eta$. Le problème consiste donc à déterminer tous les nombres entiers n, m, tels que

$$\pm \eta^n (1 - \eta)^m = x - \eta y.$$

On n'a pas encore résolu complètement ce problème.

Tartakovski [34] a démontré le théorème suivant :

V. *L'équation indéterminée*

$$x^4 - dy^4 = 1$$

possède, en dehors de la solution triviale $y = 0$, *au plus une seule solution en nombres entiers positifs* x, y, *sauf peut-être dans le cas de* $d = 15$. *Si la norme de l'unité fondamentale* ε *de l'anneau* $R(\sqrt{d})$ *est égale à* -1, *il n'y a que la solution triviale, sauf*

dans le cas de $d = 5$ *où l'on a aussi* $x = 3, y = 2$. *Si la norme de* ε *est égale à* $+1$ *et si* $x = x_1, y = y_1$ *est une solution, le nombre*

$$x_1^2 + \sqrt{d}\, y_1^2$$

est égal à ε, *ou bien égal à* ε^2, *le dernier cas ne pouvant se présenter que dans un nombre limité de cas.*

Le nombre d est supposé positif ≥ 2 et non carré. Sur le cas $d = 15$, on ne peut rien dire. Il s'agit de montrer que, ε étant l'unité fondamentale de l'anneau $R(\sqrt{d})$, $(\varepsilon > 1)$, l'équation

$$\varepsilon^n = x^2 + \sqrt{d}\, y^2$$

est seulement possible pour $n = 1$ ou $n = 2$. La démonstration s'appuie sur le théorème II de Thue du n° 7. On ne connaît que les deux cas suivants où la solution est donnée par ε^2 : la solution de $x^4 - 5y^4 = 1$ est donnée par

$$\varepsilon^2 = (2 + \sqrt{5})^2 = 3^2 + 2^2\sqrt{5}.$$

Celle de $x^4 - 7140y^4 = 1$ par

$$\varepsilon^2 = (169 + 2\sqrt{7140})^2 = 239^2 + 26^2\sqrt{7140}.$$

Tartakovski a aussi énoncé le théorème plus général : l'équation indéterminée

$$x^{2n} - dy^{2n} = 1,$$

où $n \geq 3$, possède au plus une seule solution (en dehors de $y = 0$). Cette solution, si elle existe, est donnée par l'unité fondamentale de l'anneau $R(\sqrt{d})$, ou bien (ce qui ne peut arriver que dans un nombre limité de cas d'exception) par le carré ou le bicarré de cette quantité.

Ajoutons enfin que le théorème II de Thue du n° 7 permet de résoudre complètement des équations de la forme

$$A x^r + B y^r = C,$$

qui satisfont à certaines conditions.

10. Solution complète de quelques équations spéciales de la forme

$ay^2 + by + c = dx^n$. — Nous venons de voir dans le n° 8 que l'équation

$$ay^2 + by + c = dx^n, \tag{1}$$

où a et $ac - 4b^2$ sont différents de zéro, n'a qu'un nombre limité de solutions entières. Nombreux auteurs se sont occupés des cas spéciaux de cette équation, surtout de l'équation

$$y^2 - k = x^3, \tag{2}$$

où $k \neq 0$. Le premier exemple a été donné par Fermat qui a affirmé que l'équation

$$y^2 + 2 = x^3 \tag{3}$$

n'a aucune solution en dehors de $y = \pm 5$, $x = 3$. On a résolu l'équation (2) complètement dans un grand nombre de cas. Pour y parvenir, on s'est servi surtout de deux méthodes différentes. La première méthode traite l'équation (2) directement et peut être caractérisée par l'exemple suivant : Considérons l'équation

$$y^2 + 4 - (1 + 8c)^3 = x^3.$$

Si x est pair, y est forcément impair. Dans ce cas, l'équation est impossible, puisque

$$y^2 + 4 - (1 + 8c)^3 \equiv 4 \pmod 8.$$

Si x est impair, y est pair et l'équation peut s'écrire

$$y^2 + 4 = (x + 1 + 8c)[x^2 - x(1 + 8c) + (1 + 8c)^2].$$

Le côté gauche est divisible par 4, on aura donc

$$x + 1 \equiv 0 \pmod 4.$$

Il résulte ainsi

$$x^2 - x(1 + 8c) + (1 + 8c)^2 \equiv x^2 - x + 1 \equiv 3 \pmod 4.$$

Le côté droite a donc forcément un facteur premier de la forme $4n + 3$. Or, le nombre $y^2 + 4$ ne peut avoir un facteur de cette forme. L'équation proposée est ainsi impossible.

Cette méthode peut être considérablement généralisée ainsi que l'a montré Mordell [24, a]. Nous nous bornons ici à mentionner que

l'équation (2) est impossible si $k = A^3 - B^2$, où B est indivisible par 3, et où tous les facteurs impairs communs à A et B ont la forme $4n + 1$.

La deuxième méthode est la même que nous avons appliquée pour démontrer le théorème II du n° 8. Au lieu de l'équation (2), on aura à traiter un nombre fini d'équations

$$\varphi(u, v) = C, \tag{4}$$

où φ est une forme binaire cubique. Si k est positif, le discriminant de la forme est négatif; dans le cas contraire, il est positif. Le cas le plus simple est celui où la forme est réductible. Ainsi, l'équation (3) entraîne

$$y + \sqrt{-2} = (u + v\sqrt{-2})^3,$$

d'où

$$v(3u^2 - 2v^2) = 1,$$

ce qui donne

$$v = u = 1, \qquad x = 3, \qquad y = 5.$$

Lorsque la forme φ est irréductible, on peut souvent montrer que l'équation (4) est impossible suivant l'un des modules 7, 8 ou 9. Considérons, par exemple, le cas de $k = 27$. Supposons d'abord que x soit indivisible par 3. Dans ce cas, on a

$$y + 3\sqrt{3} = (a + b\sqrt{3})(u + v\sqrt{3})^3,$$

où l'on a $a = \pm 2$; $b = \pm 1$ ou $a = 1$, $b = 0$, donc

$$3 = a(3u^2v + 3v^3) + b(u^3 + 9uv^2).$$

$a = \pm 2$ est impossible puisque u est indivisible par 3; $b = 0$ ne donne aucune solution. Supposons ensuite que x soit divisible par 3, donc $x = 3\xi$, $y = 9\eta$. Dans ce cas, on aura

$$1 + \eta\sqrt{3} = (a + b\sqrt{3})(u + v\sqrt{3})^3,$$
$$1 = a(u^3 + 9uv^2) + 3b(3u^2v + 3v^3).$$

Si $a = \pm 2$, on aura

$$1 \equiv 2u^3 \pmod 9,$$

congruence absurde. Si $a = \pm 1$, on aura

$$u = 1, \qquad v = 0,$$

donc,

$$x = -3, \quad y = 0,$$

seule solution de l'équation proposée (Mordell [**24**, *a*]).

Lorsque le discriminant de φ est négatif, on peut aussi quelquefois appliquer les résultats du numéro précédent sur les formes cubiques à la résolution de l'équation (4), ainsi dans les cas $k = 1, 2, 3, 4, 5, 6$ et 17. Dans le dernier cas, l'équation (2) possède exactement les huit solutions suivantes :

$$x = -1, \quad y = 4; \qquad x = -2, \quad y = 3; \qquad x = 2, \quad y = 5;$$
$$x = 4, \quad y = 9; \qquad x = 8, \quad y = 23; \qquad x = 43, \quad y = 282;$$
$$x = 52, \quad y = 375; \qquad x = 5234, \quad y = 378661.$$

Par les méthodes précédentes, on a résolu l'équation (2) complètement dans les cas suivants :

$k = 1, 2, 3, 4, 5, 6, 7, 11, 13, 14, 16, 17, 20, 21, 23, 25, 27, 29, 32, 34, 39, 42, 45, 46, 47, 49, 51, 53, 58, 59, 60, 61, 62, 66, 67, 69, 70, 75, 77, 78, 83, 84, 85, 86, 87, 88, 90, 93, 95, 96;$

et pour les valeurs négatives de $k > -100$, sauf pour

$$-k = 7, 15, 18, 20, 23, 25, 26, 28, 31, 39, 40, 45, 47, 48, 53, 54, 55, 56, 60, 61, 63, 71, 72, 79, 83, 84, 87, 89, 95.$$

Il existe aussi un petit nombre de résultats sur l'équation (1) pour des valeurs de $n > 3$. Ainsi, on peut montrer que les équations

$$y^2 + 1 = x^n \qquad \text{et} \qquad y^2 + 1 = 2x^n$$

sont impossibles pour $|y| > 1$ si n n'est pas une puissance de 2. (La première est aussi impossible dans le dernier cas.) Les équations

$$y^2 + y + 1 = x^n \qquad \text{et} \qquad y^2 + y + 1 = 3x^n$$

sont aussi impossibles pour $|y| > 2$ si n n'est pas une puissance de 3. (La dernière est aussi impossible pour $n = 3^m$.)

Il y a des résultats plus généraux, comme, par exemple : L'équation

$$1 + Dy^2 = x^n,$$

où n est impair > 1, et où D est un nombre entier > 2, ne possède aucune solution en nombres entiers x, y, x impair > 1 si le nombre n

n'est pas un diviseur du nombre de classes d'idéaux du corps quadratique engendré par $\sqrt{-D}$. Dans le cas de $D = 2$, il y a la seule solution $n = 5, y = \pm 11, x = 3$ (Nagell [25, *d*]).

Pour démontrer ces résultats, on se sert de la même méthode que dans le n° 8. Le succès est dû au fait que la forme résultante du $n^{\text{ième}}$ degré est réductible.

Note. — Au moment de l'impression, M. A. Weil me communique qu'il a étendu le théorème de Mordell du n° 3 à un domaine de rationalité algébrique quelconque. Il a même démontré un théorème correspondant pour les courbes algébriques de genre > 1. Ses recherches seront publiées dans les *Acta mathematica*, 1928.

Au sujet des points rationnels des cubiques, *voir* aussi mon Mémoire : *Sur les propriétés arithmétiques des cubiques planes du premier genre* (*Acta mathematica*, t. 28, 1928).

OUVRAGE A CONSULTER.

Dickson (L.-E.). — *History of the theory of numbers*, vol. II. *Diophantine Analysis* (Carnegie Institution of Washington. Publ. n° 256. Washington, 1920).

INDEX BIBLIOGRAPHIQUE.

1. Burnside (W.). — On the rational solutions of the equation $X^3 + Y^3 + Z^3 = 0$ in quadratic fields (*Proc. London math. Soc.*, vol. 14, 1915).
2. Cauchy (A.). — Œuvres (t. VI, p. 302).
3. Delaunay (B.). — *a*. Solution complète de l'équation $X^3\rho + Y^3 = 1$ (en russe) (*Publ. Soc. math. Kharkow*, 1916). — *b*. La solution générale de l'équation $x^3\rho + y^3 = 1$ (*C. R. Acad. Sc.*, Paris, t. 162, 1916, p. 150). — *c*. Représentation d'un nombre entier par une forme cubique à discriminant négatif (*C. R. Acad. Sc.*, Paris, t. 171, 1920, p. 336, et t 172, 1921, p. 434). — *d*. Solution complète de l'équation $X^3q + Y^3 = 1$ (en

russe) (*Bull, Acad. Sc. de Russie*, 1922). — *e*. Le nombre de représentations d'un nombre entier par une forme cubique à discriminant négatif (en russe) (*Ibid.*). — *f*. Sur les formes binaires cubiques à discriminant négatif. (*C. R. Acad. Sc.*, Paris, t. 178, 1924, p. 1460). — *g*. Vollstandige Lösung der unbestimmten Gleichung $X^3q + Y^3 = 1$ in ganzen Zahlen. (*Math. Zeitschr.*, Bd 28, 1928).

4. Diophante (d'Alexandrie). — Les six livres arithmétiques et le livre des nombres polygones (trad. par Paul Ver Eecke; Bruges, 1926).
5. Dirichlet (Lejeune). — Werke (t. 1 et 2).
6. Dorge (K.). — *a*. Ein Beitrag zur Theorie der diophantischen Gleichungen mit zwei Unbekannten (*Math. Zeitschr.*, Bd 24, 1925). — *b*. Ueber die Seltenheit der reduziblen Polynome und der Normalgleichungen (*Math. Annalen*, Bd 95, 1925).
7. Euler (L.). — *a*. Opera Omnia (t. I et II). — *b*. Algebra (II).
8. Fermat (P.). — Œuvres.
9. Fueter (R.). — Die diophantische Gleichung $\xi^3 + \eta^3 + \zeta^3 = 0$ (*Sitz. ber. Heidelberger Akademie*, 1913).
10. Gauss (C.-F.). — Disquisitiones arithmeticæ.
11. Hermite (Ch.). — Œuvres (t. I, p. 224 et 415).
12. Hilbert (D.). — Die Theorie der algebraischen Zahlkorper (*Jahresbericht d. Deutschen Math. Ver.*, 1894-1895, p. 523).
13. Hilbert (D.) et Hurwitz (A.). — Ueber die Diophantischen Gleichungen vom Geschlecht Null (*Acta math.*, t. 14, 1891).
14. Hurwitz (A.). — Ueber ternare diophantische Gleichungen dritten Grades (Vierteljahrschr. d. Naturf. Gesellschaft in Zurich, t. 62, 1917).
15. Jacobi (C.). — Werke (t. II, p. 53).
16. Kummer (E.). — Allgemeiner Beweis des Fermatschen Satzes usf. (*Journ. fur Math.*, t. 40, 1850).
17. Lagrange (J.-L.). — Œuvres (t. II, p. 379, 662 et 675).
18. Landau (E.) et Ostrowski (A.). — On the diophantine equation $ay^2 + by + c = dx^n$ (*Proc. London math. Soc.*, vol. 19, 1920).
19. Lebesgue (V.-A.). — Sur l'impossibilité de l'équation indéterminée $x^3 + y^3 = Az^3$ (*Journ. de Math.*, t. 2, p. 49).
20. Legendre (A.-M.). — Théorie des nombres.
21. Levi (B.). — Saggio per una teoria aritmetica della forme cubiche ternari *Accademia Torino*, 1906-1908).
22. Lucas (E.). — *a*. Recherches sur l'Analyse indéterminée (Moulins, 1873). — *b*. Sur l'Analyse indéterminée du troisième degré (*Nouv. Annales de Math.*, 2e série, t. 17, 1878).
23. Maillet (E.). — *a*. Sur les équations de la forme $x^\lambda + y^\lambda = cz^\lambda$ (*Acta math.*, t. 24, 1900). — *b*. Sur les équations de la forme $x^\iota + y^\iota = ba\, z^a$ (*Annali di Mat.*, t. 12, 1906). — *c*. Détermination des points entiers des courbes algébriques unicursales à coefficients entiers (*C. R. Acad. Sc.*, Paris, t. 168, 1919, p. 217, et *Journ. École Polyt.*, 1919). — *d*. Sur les équations indéterminées à deux et trois variables qui n'ont qu'un nombre fini de solu-

tions en nombres entiers (*Journ de Math.*, 5e série, t. 6, 1900). — *e.* Sur un théorème de M. Axel Thue (*Nouv. Annales de Math.*, 4e série, t. 16, 1916). — *f.* Sur une catégorie d'équations indéterminées n'ayant en nombres entiers qu'un nombre fini de solutions (*Nouv. Annales de Math.*, 4e série, t. 18, 1918).

24. Mordell (L.-J.). — *a.* The diophantine equation $y^2 - k = x^3$ (*Proc. London Math. Soc.*, vol. 13, 1913). — *b.* Indeterminate equations of the third and fourth degrees (*Quart. Journ. Math.*, no 178, 1914). — *c.* Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$ (*Messenger of Math.*, vol. 51, 1922). — *d.* On the integer solutions of the equation $ey^2 = ax^3 + bx^2 + cx + d$ (*Proc. London Math. Soc.*, vol. 21, 1922). — *e.* On the rational solutions of the indeterminate equations of the third and fourth degrees (*Proc. Cambridge Philos. Soc.*, vol. 21, 1922). — *f.* Indeterminate equations of the third degree (*Science Progress*, London, 1923).

25. Nagell (T.). — *a.* Vollständige Lösung einiger unbestimmten Gleichungen dritten Grades (*Skrifter Videnskapsselskapet*, Kristiania, 1922). — *b.* Ueber die Einheiten in reinen kubischen Zahlkörpern (*Ibid.*, 1923). — *c.* Ueber die rationalen Punkte auf einigen kubischen Kurven (*Tôhoku Math. Journ.*, vol. 24, 1924). — *d.* Sur l'impossibilité de quelques équations à deux indéterminées (*Norsk Mat. For. Skrifter*, 1re série, no 13, Kristiania, 1923). — *e.* Solution complète de quelques équations cubiques à deux indéterminées (*Journ. de Math.*, 9e série, t. 4, 1925). — *f.* Ueber einige kubische Gleichungen mit zwei Unbestimmten (*Math. Zeitschr.*, Bd 24, 1925). — *g.* Darstellung ganzer Zahlen durch eine binäre kubische Form mit negativer Diskriminante (*Ibid.*, Bd 28, 1928).

26. Nagy (J.). — Die Anwendung der birationalen Transformationen einer Kurve von höherem Geschlechte in sich auf ein Diophantisches Problem (*Jahresber. d. Deutschen Math. Ver.*, Bd 21, 1912).

27. Pépin (le P.). — *a. Journ. de Math.*, 2e série, t. 15, 1870, p. 217, et 3e série, t. 1, p. 363. — *b. Atti Accad. Pont. Nuovi Lincei*, t. 34, 1880, p. 73; t. 30, 1876, p. 220; t. 36, 1882, p. 37; t. 31, 1877, p. 397; t. 36, 1882, p. 49; t. 42, 1888, p. 227. — *c. Journ. de Math..*, 3e série, t. 5, 1879, p. 405, et 5e série, t. 1, 1895, p. 351.

28. Pocklington (H.-C.). — Some diophantine impossibilities (*Proc. Cambridge Philos. Soc.*, vol. 17, 1914).

29. Poincaré (H.). — Sur les propriétés arithmétiques des courbes algébriques (*Journ. de Math.*, 5e série, t. 7, 1901).

30. Runge (C.). — Ueber ganzzahlige Lösungen von Gleichungen mit zwei Veränderlichen (*Journ. für Math.*, Bd 100, 1887).

31. Siegel (C.). — *a.* Approximation algebraischer Zahlen (*Math. Zeitschr.*, Bd 10, 1921). — *b.* Ueber den Thueschen Satz (*Skrifter Videnskapsselskapet*, Kristiania, 1922).

32. Skolem (Th.). — *a.* Ueber ganzzahlige Lösungen einer Klasse unbestimmter Gleichungen (*Norsk Mat. For. Skrifter*, 1re série, no 10; Kristiania, 1922).

— *b.* Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen (*Skrifter Videnskapsselskapet*, Kristiania, 1921).

33. Sylvester (J. J.). — *Collected Math. Papers*, vol. II, p. 63, et vol. III, p. 312, 347, 350, 430, 437.

34. Tartakowski (V.). — Auflösung der Gleichung $x^4 - \rho y^4 = 1$ (*Bull. Acad. Sc. de l'U. R. S. S.*, 1926).

35. Thue (A.). — *a.* Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen (*Skrifter Videnskapsselskapet*, Kristiania, 1908). — *b.* Ueber rationale Annäherungswerte der reellen Wurzel der ganzen Funktion dritten Grades $x^3 - ax - b$ (*Ibid.*, 1908). — *c.* Om en generel i store hele tal ulösbar ligning (*Ibid.*, 1908). — *d.* Ueber Annäherungswerte algebraischer Zahlen (*Journ. für Math.*, Bd 135, 1909). — *e.* Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen (*Ibid.*, Bd 138, 1910). — *f.* Eine Lösung der Gleichung $\rho P(x) - Q(x) = (x - \rho)^n R(x)$ in ganzen Funktionen, etc. (*Skrifter Videnskapsselskapet*, Kristiania, 1909). — *g.* Ueber einige in grossen ganzen Zahlen unmögliche Gleichungen (*Ibid.*, 1911). — *h.* Berechnung aller Lösungen gewisser Gleichungen von der Form $ax^n - by^n = f$ (*Ibid.*, 1918). — *i.* Ueber die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x und y (*Archiv f. Math. og Naturv.*, Kristiania, 1917).

36. Weil (A.). — L'arithmétique sur les courbes algébriques (*Acta mathematica*, t. 28, 1928).

TABLE DES MATIÈRES.

I. — Introduction.

II. — Les points rationnels des courbes algébriques planes.

III. — Les points entiers des courbes algébriques planes.