ARKIV FÖR MATEMATIK Band 2 nr 9

Communiqué le 27 février 1952

Un théorème arithmétique sur les coniques

Par

TRYGVE NAGELL

1. Nous prenons pour domaine de rationalité fondamental un corps quelconque donné Ω. Par nombre rationnel nous entendons un nombre appartenant à Ω.

Le point dans le plan $P(x, y, z)$, en coordonnées homogènes, est appelé *point rationnel* quand les coordonnées sont proportionnels à trois nombres rationnels. Le point $P(x, y, z)$, sera appelé *point (relativement) algébrique* quand x, y et z sont proportionnels à trois nombres algébriques relativement à Ω. Sans restreindre la généralité nous pouvons supposer que l'un des nombres x, y, z soit égal à 1. Quand ces trois nombres appartiennent au corps $\boldsymbol{K}$, algébrique relativement à Ω, le point sera appelé *point algébrique du corps* $\boldsymbol{K}$ ou *appartenant au corps* $\boldsymbol{K}$. Supposons que le corps $\boldsymbol{K}_1 = \Omega(x, y, z)$, engendré en adjoignant à Ω les nombres x, y et z, soit du $m^{\text{ième}}$ degré relativement à Ω. Alors nous dirons que le point $P(x, y, z)$ est un *point algébrique du* $m^{\text{ième}}$ *degré*, et nous l'appellerons *point primitif du corps* $\boldsymbol{K}_1$. En désignant par $\alpha^{(i)}$ un nombre conjugué à α relativement à Ω nous dirons que le point $P(x^{(i)}, y^{(i)}, z^{(i)})$ est un *point conjugué* au point $P(x, y, z)$ relativement à Ω.

L'ensemble des points conjugués sera appelé *système rationnel irréductible* de m points dans Ω. Nous appellerons *système rationnel* dans Ω tout système de points composé d'un nombre de systèmes rationnels irréductibles dans Ω. Ce système est réductible, s'il est composé de plus d'un système irréductible. Un système rationnel de deux points est appelé *couple rationnel*, et un système rationnel de trois points *triplet rationnel.*

2. Nous dirons qu'une courbe algébrique plane

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

en coordonnées homogènes appartient à Ω quand les coefficients de la forme ternaire $f(x, y, z)$ appartiennent à Ω. J'appellerai une droite à coefficients rationnels une *droite rationelle* (dans Ω), et d'une façon analogue je parlerai d'une *conique rationnelle.*

Soit $\boldsymbol{K}$ un corps algébrique du $m^{\text{ième}}$ degré relativement à Ω. Supposons donnée la courbe (1) appartenant à Ω et supposons que l'équation (1) ait une solution en nombres x_0, y_0, z_0 appartenant à $\boldsymbol{K}$. Cette solution sera appelée *solution primitive en* $\boldsymbol{K}$ de l'équation (1), si le point $P(x_0, y_0, z_0)$ est un point primitif de

$\boldsymbol{K}$. Nous dirons alors que l'équation diophantienne (1) est *effectivement résoluble dans* $\boldsymbol{K}$, et nous appellerons $\boldsymbol{K}$ *corps résolvant de la courbe* (1) *dans le domaine* $\boldsymbol{\Omega}$.

HILBERT et HURWITZ ont examiné le cas dans lequel l'équation (1) représente une courbe unicursale; voir [1].[1] Il résulte de leurs recherches: Si la courbe (1) est de degré impair, elle est birationnellement équivalente dans $\boldsymbol{\Omega}$ à une droite rationnelle. Si elle est de degré pair, elle est birationellement équivalente dans $\boldsymbol{\Omega}$ à une conique rationnelle. On en conclut: Si l'équation (1) est de genre zéro et de degré impair, elle est effectivement résoluble dans un corps algébrique quelconque relativement à $\boldsymbol{\Omega}$.

3. Soit C une conique rationnelle dans $\boldsymbol{\Omega}$, qui n'admet aucun point rationnel dans $\boldsymbol{\Omega}$.

Soit $\boldsymbol{K}$ un corps algébrique du $n^{ième}$ degré relativement à $\boldsymbol{\Omega}$. Supposons que la conique C admette un point algébrique primitif du corps $\boldsymbol{K}$; alors elle admet aussi les points conjugués relativement à $\boldsymbol{\Omega}$.

Supposons que n soit impair et posons $n = 2m - 1$. Par les n points conjugués sur la conique et par

$$\tfrac{1}{2} m(m + 3) - n$$

points rationnels quelconques dans le plan je puis faire passer une courbe algébrique de degré m. Cette courbe aura évidemment les coefficients rationnels. Elle coupera la conique en $2m$ points qui formeront un système rationnel. Parmi ces points se trouvent les $n = 2m - 1$ points conjugués relativement à $\boldsymbol{\Omega}$, qui forment aussi un système rationnel sur la conique. On en conclut qu'il y a nécessairement un point rationnel sur la conique. Comme cela est contre l'hypothèse nous concluons:

Théorème 1. *Soit C une conique rationnelle dans $\boldsymbol{\Omega}$, qui n'admet aucun point rationnel dans $\boldsymbol{\Omega}$. Si $\boldsymbol{K}$ est un corps résolvant de C dans $\boldsymbol{\Omega}$, le degré de $\boldsymbol{K}$, relatif à $\boldsymbol{\Omega}$, est un nombre pair.*

Ce résultat peut aussi être énoncé de la manière suivante:

Théorème 2. *Si l'équation quadratique homogène*

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

à coefficients rationnels dans le domaine $\boldsymbol{\Omega}$, n'admet aucune solution rationnelle dans $\boldsymbol{\Omega}$, hors $x = y = z = 0$, elle restera irrésoluble même après l'adjonction d'un nombre algébrique, dont le degré est impair relativement à $\boldsymbol{\Omega}$.

Exemples numériques. La conique

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

n'admet aucun point rationnel dans $\boldsymbol{K}(1)$. Par suite, elle n'admet aucun point rationnel dans $\boldsymbol{K}(\xi)$, si ξ est un nombre algébrique de degré impair.

Si une conique dans $\boldsymbol{K}(1)$ n'admet aucun point rationnel dans $\boldsymbol{K}(1)$, on montre aisément qu'elle n'admet aucun point rationnel dans le corps engendré

---

[1] Les numéros figurant entre crochets renvoient à la Bibliographie placée à la fin de cette Note.

par les racines cubiques irrationnelles et réelles

$$\sqrt[3]{a_1},\ \sqrt[3]{a_2},\ \sqrt[3]{a_3},\ \ldots \text{ in inf.},$$

où $a_1, a_2, a_3, \ldots$ sont des nombres entiers, $a_1 < a_2 < a_3 < \ldots$; ce corps n'est plus un corps algébrique de degré fini. En effet, pour cela il suffit de montrer que le corps algébrique

$$\boldsymbol{K}_1 = \boldsymbol{K}(\sqrt[3]{a_1},\ \sqrt[3]{a_2},\ \ldots,\ \sqrt[3]{a_m})$$

est de degré impair. Puisque le corps $\boldsymbol{K}_1$ est réel, il ne contient aucun des conjugués imaginaires du nombre

$$\xi = \sqrt[3]{a_{m+1}}.$$

Donc ξ est ou du premier ou du troisième degré relativement à $\boldsymbol{K}_1$. On en conclut que le degré de $\boldsymbol{K}_1$ est une puissance de 3 et par suite impair.

4. Dans un travail antérieur j'ai établi le résultat suivant analogue au théorème 1 (voir NAGELL [2]):

Théorème 3. *Soit C une cubique rationnelle dans $\boldsymbol{\Omega}$, qui n'admet aucun point rationnel dans $\boldsymbol{\Omega}$. Si $\boldsymbol{K}$ est un corps résolvant de C dans $\boldsymbol{\Omega}$, le degré de $\boldsymbol{K}$, relatif à $\boldsymbol{\Omega}$, est un nombre divisible par 3.*

Dans ce théorème il s'agit naturellement d'une cubique du premier genre. Quand $\boldsymbol{\Omega}$ est algébrique, j'ai montré que la cubique a une infinité de corps résolvants cubiques. Quand $\boldsymbol{\Omega}$ est algébrique et la cubique admet un point rationnel dans $\boldsymbol{\Omega}$, il y a une infinité de corps résolvants quadratiques.

5. Les théorèmes 1, 2 et 3 ne peuvent pas être étendus aux courbes algébriques d'un degré $\geqq 4$. Pour le montrer nous allons examiner le cas d'une quartique C, rationnelle dans $\boldsymbol{\Omega}$, qui n'admet aucun point rationnel dans $\boldsymbol{\Omega}$. Soit $\boldsymbol{K}$ un corps algébrique du $n^{\text{ième}}$ degré relativement à $\boldsymbol{\Omega}$. Supposons que la quartique C admette un point algébrique primitif du corps $\boldsymbol{K}$; alors elle admet aussi les points conjugués relativement à $\boldsymbol{\Omega}$.

Considérons d'abord le cas de $n \equiv -1 \pmod 4$ et posons $n = 4m - 1$. Par les n points conjugués sur la quartique et par

$$\tfrac{1}{2} m (m+3) - n \tag{2}$$

points rationnels quelconques dans le plan je puis faire passer une courbe algébrique de degré m. Cette courbe aura évidemment les coefficients rationnels. Elle coupera la quartique en $4m$ points qui formeront un système rationnel. Parmi ces points se trouvent les $n = 4m - 1$ points conjugués relativement à $\boldsymbol{\Omega}$, qui forment aussi un système rationnel. On en conclut qu'il y a nécessairement un point rationnel sur la quartique.

Pour que ce raisonnement soit valable if faut cependant que le nombre (2) soit $\geqq 0$, c'est-à-dire il faut que $m \geqq 5$ et que $n \geqq 19$.

Dans le cas de $n \equiv 2 \pmod 4$ on trouvera par un raisonnement analogue qu'il y a nécessairement un couple rationnel sur la quartique. Dans le cas de $n \equiv 1 \pmod 4$ on trouvera qu'il y a un triplet rationnel.

Par suite nous obtenons seulement le résultat partiel que voici:

Théorème 4. *Soit C une quartique rationnelle dans $\mathbf{\Omega}$, qui n'admet aucun point rationnel dans $\mathbf{\Omega}$. Si P est un point sur C du $n^{\text{ième}}$ degré relativement à $\mathbf{\Omega}$, on ne peut pas avoir $n \equiv -1 \pmod 4$ quand $n \geqq 19$.*

Pour les courbes de degré > 4 on aura des résultats analogues.

BIBLIOGRAPHIE. [1]. **D. Hilbert** u. **A. Hurwitz,** *Über die diophantischen Gleichungen vom Geschlecht Null,* Acta mathematica, t. 14 (1891), p. 217. — [2]. **T. Nagell,** *Sur la résolubilité des équations diophantiennes cubiques à deux inconnues dans un domaine relativement algébrique,* Nova Acta Regiae Societatis Scientarum Upsaliensis, Ser. IV, Vol. 13, N:o 3. — [3]. ——, *Sur quelques questions dans la théorie arithmétique des cubiques planes du premier genre, Colloques internationaux Centre national de la recherche scientifique,* vol. XXIV, Algèbre et Théorie des Nombres, Paris 1950.

Tryckt den 2 september 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB