Communiqué le 28 mai 1952

Remarques sur les corps résolvants des coniques, cubiques et quartiques

Par Trygve Nagell

1. Coniques. — Dans une note qui vient de paraître dans ce Journal (voir Nagell, Un théorème arithmétique sur les coniques, Arkiv f. Matematik, Bd 2, Nr 14, Stockholm 1952) j'ai établi le résultat suivant:

Théorème 1. *Soit C une conique propre (irréductible) rationnelle dans le domaine Ω, qui n'admet aucun point rationnel dans Ω. Alors tout corps résolvant de C dans Ω est d'un degré pair relativement à Ω.*

Nous allons compléter un détail dans la démonstration de cette proposition. Supposons qu'il y ait sur C un système rationnel S_n de n points et que $n = 2m-1$ soit un nombre impair $\geqq 3$. Par ces points et par

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

points rationnels $P_1, P_2, \ldots, P_\mu$ en dehors de la conique je puis faire passer une courbe algébrique $C^{(m)}$ de degré m. Cette courbe aura évidemment les coefficients rationnels. On voit que $\mu \geqq 2$.

Pour $m=2$ on a $\mu = 2$; dans ce cas les deux coniques C et $C^{(2)}$ sont distinctes, vu que les points rationnels P_1 et P_2 sont en dehors de C. Pour $m \geqq 3$ on a $\mu \geqq 4$; dans ces cas on peut choisir les μ points $P_1, P_2, \ldots, P_\mu$ de telle façon que la courbe $C^{(m)}$ ne contienne pas la conique C. En effet, pour obtenir cela il suffit de les choisir tels qu'ils ne soient pas tous sur une même courbe algébrique $C^{(m-2)}$ de degré $m-2$. C'est possible puisqu'on a

$$\mu = \tfrac{1}{2} m(m+3) - 2m + 1 > \tfrac{1}{2}(m-2)(m+1).$$

Alors la courbe $C^{(m)}$ coupera la conique en exactement $2m$ points, qui formeront un système rationnel. Parmi ces points se trouvent aussi le système rationnel S_n de $n = 2m-1$ points. On en conclut qu'il y a nécessairement un point rationnel sur la conique C. Comme cela est contre l'hypothèse, le théorème 1 se trouve démontré.

2. Cubiques. — D'une manière analogue on peut compléter la démonstration de la proposition suivante (voir Nagell, Sur la résolubilité des équations cubiques à deux inconnues dans un domaine relativement algébrique, Nova Acta Regiae Societatis Scientarum Upsaliensis, Ser. IV, Vol. 13, N:o 3, p. 5 Uppsala 1942):

Théorème 2. *Soit C une cubique propre (irréductible) rationnelle dans le domaine Ω, qui n'admet aucun point rationnel dans Ω. Alors le degré relativement à Ω de tout corps résolvant de C dans Ω est divisible par 3.*

Supposons qu'il y ait sur la cubique C un système rationnel S_n de n points et que n soit indivisible par 3.

Soit d'abord $n=3m-1$. Par les n points du système S_n et par

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

points rationnels $P_1, P_2, \ldots, P_\mu$ en dehors de la cubique je puis faire passer une courbe algébrique $C^{(m)}$ de degré m. Cette courbe aura évidemment les coefficients rationnels.

Pour $m=1$ et pour $m=2$ on a $\mu=0$; dans ce cas la courbe $C^{(m)}$ représente ou une droite ou une conique, et ainsi elle ne peut pas contenir la cubique C. Pour $m=3$ on a $\mu=1$; dans ce cas les deux courbes C et $C^{(m)}$ ne coincident pas, puisque le point rationnel P_1 est en dehors de la cubique C. Pour $m\geqq 4$ on a $\mu\geqq 3$. Dans ces cas on peut choisir les points rationnels $P_1, P_2, \ldots, P_\mu$ de telle façon que la courbe $C^{(m)}$ ne contienne pas la cubique C. En effet, pour obtenir cela il suffit de les choisir tels qu'ils ne soient pas tous sur une même courbe algébrique $C^{(m-3)}$ de degré $m-3$. C'est possible puisqu'on a

$$\mu=\tfrac{1}{2}m(m+3)-3m+1>\tfrac{1}{2}(m-3)m.$$

Alors la courbe $C^{(m)}$ coupera la cubique C en exactement $3m$ points, qui formeront un système rationnel. Parmi ces points se trouvent aussi le système rationnel S_n de $n=3m-1$ points. On en conclut qu'il y a nécessairement un point rationnel sur la cubique C. Comme cela est contre l'hypothèse, le théorème 2 est démontré dans ce cas.

Considérons ensuite le cas de $n=3m-2$, m entier $\geqq 2$. Par les n points du système S_n et par

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

points rationnels $P_1, P_2, \ldots, P_\mu$ en dehors de la cubique je puis faire passer une courbe algébrique $C^{(m)}$ de degré m. Cette courbe aura évidemment les coefficients rationnels.

On peut choisir les μ points rationnels $P_1, P_2, \ldots, P_\mu$ de telle façon que la courbe $C^{(m)}$ ne contienne pas la cubique C. Cela est évident quand $m=2$ et $\mu=1$. Pour $m=3$ on a $\mu=2$; dans ce cas les deux courbes C et $C^{(m)}$ ne coincident pas, vu que le point rationnel P_1 est en dehors de la cubique C. Pour $m\geqq 4$ on a $\mu\geqq 4$. Dans ces cas il suffit de choisir les points $P_1, P_2, \ldots, P_\mu$ tels qu'ils ne soient tous sur une même courbe algébrique $C^{(m-3)}$ de degré $m-3$. C'est possible puisqu'on a

$$\mu=\tfrac{1}{2}m(m+3)-3m+2>\tfrac{1}{2}(m-3)m.$$

Alors la courbe $C^{(m)}$ coupera la cubique C en exactement $3m$ points, qui formeront un système rationnel. Parmi ces points se trouvent aussi le système rationnel S_n de $n=3m-2$ points. On en conclut qu'il y a nécessairement une couple rationnelle sur la cubique C. Or, nous venons de montrer que la cubique n'admet aucun corps résolvant quadratique. Donc le théorème 2 se trouve démontré dans tous les cas.

3. Quartiques. — La démonstration du théorème 4 dans la note précitée est incomplète, parce que la courbe auxiliaire du $m^{\text{ième}}$ degré peut contenir la quartique. Il faut remplacer ce théorème par la proposition suivante:

Théorème 3. *Soit Q une quartique propre (irréductible) rationnelle dans le domaine Ω. Si Q admet un système rationnel dans Ω d'un nombre impair de points, elle admet un triplet rationnel dans Ω.*

Démonstration. Supposons qu'il y ait sur la quartique Q un système rationnel S_n de n points, n impair $\geqq 5$.

Soit d'abord $n = 4m - 3$, où m est un entier $\geqq 2$. Par les n points du système S_n et par

$$\mu = \tfrac{1}{2} m (m + 3) - (4m - 3)$$

points rationnels $P_1, P_2, \ldots, P_\mu$ en dehors de la quartique je puis faire passer une courbe algébrique $C^{(m)}$ de degré m. Cette courbe aura évidemment les coefficients rationnels.

Pour $m = 2$ et pour $m = 3$ on a $\mu = 0$. Dans ces deux cas il est évident que la courbe $C^{(m)}$ ne peut pas contenir la quartique Q. Pour $m = 4$ on a $\mu = 1$; dans ce cas les deux quartiques Q et $C^{(4)}$ ne coincident pas, puisque le point rationnel P_1 est en dehors de la quartique Q. Pour $m \geqq 5$ on a $\mu \geqq 3$. Dans ces cas on peut choisir les points $P_1, P_2, \ldots, P_\mu$ de telle façon que la courbe $C^{(m)}$ ne contienne pas la quartique Q. En effet, pour obtenir cela il suffit de les choisir tels qu'ils ne soient pas tous sur une même courbe algébrique $C^{(m-4)}$ de degré $m - 4$. C'est possible puisqu'on a

$$\mu = \tfrac{1}{2} m (m + 3) - 4m + 3 > \tfrac{1}{2} (m - 4)(m - 1).$$

Alors la courbe $C^{(m)}$ coupera la quartique Q en exactement $4m$ points, qui formeront un système rationnel. Parmi ces points se trouvent aussi le système rationnel S_n de $n = 4m - 3$ points. On en conclut qu'il y a nécessairement un triplet rationnel sur la quartique Q.

Considérons ensuite le cas de $n = 4m - 5$, où m est un entier $\geqq 3$. Par les n points du système S_n et par

$$\mu = \tfrac{1}{2} m (m + 3) - (4m - 5)$$

points rationnels $P_1, P_2, \ldots, P_\mu$ en dehors de la quartique je puis faire passer une courbe algébrique $C^{(m)}$ de degré m. Cette courbe aura évidemment les coefficients rationnels. On a $\mu \geqq 2$.

Pour $m = 3$ on a $\mu = 2$; dans ce cas la courbe $C^{(m)}$ est une cubique, et ainsi elle ne peut pas contenir la quartique Q. Pour $m = 4$ on a $\mu = 3$; dans ce cas les deux quartiques Q et $C^{(4)}$ ne coincident pas, vu que le point rationnel P_1 est en dehors de la quartique Q. Pour $m \geqq 5$ on a $\mu \geqq 5$; dans ces cas on peut choisir les points $P_1, P_2, \ldots, P_\mu$ de telle façon que la courbe $C^{(m)}$ ne contienne pas la quartique Q. En effet, pour obtenir cela il suffit de choisir ces points tels qu'ils ne soient pas tous sur une même courbe algébrique $C^{(m-4)}$ de degré $m - 4$. C'est possible puisqu'on a

$$\mu = \tfrac{1}{2} m (m + 3) - 4m + 5 > \tfrac{1}{2} (m - 4)(m - 1).$$

Alors la courbe $C^{(m)}$ coupera la quartique en exactement $4m$ points, qui formeront un système rationnel. Parmi ces points se trouvent aussi le système rationnel S_n de $n = 4m - 5$ points. On en conclut qu'il y a nécessairement un système rationnel de 5 points sur la quartique Q. D'après ce que nous venons de montrer il y a donc un triplet rationnel sur Q. Le théorème 3 est ainsi démontré.

4. Systèmes rationnels des points singuliers sur les courbes algébriques. — Soit $C^{(n)}$ une courbe algébrique propre du $n^{\text{ième}}$ degré, rationnelle dans le domaine Ω et représentée par l'équation en coordonnées homogènes

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

où F est une forme ternaire du $n^{\text{ième}}$ degré en x, y, z à coefficients rationnels. On obtiendra les points singuliers de celle-ci par le système d'équations suivant:

$$\frac{\partial F}{\partial x} = 0, \quad \frac{\partial F}{\partial y} = 0, \quad \frac{\partial F}{\partial z} = 0. \tag{2}$$

La première polaire du point (a, b, c) par rapport à la courbe $C^{(n)}$ a l'équation

$$a\frac{\partial F}{\partial x} + b\frac{\partial F}{\partial y} + c\frac{\partial F}{\partial z} = 0. \tag{3}$$

Cette courbe a $n(n-1)$ points d'intersection avec la courbe $C^{(n)}$.

Soient maintenant a, b et c des nombres rationnels dans Ω. Alors les coefficients de la courbe (3) appartiennent à Ω. Dans ce cas les points d'intersection des deux courbes (1) et (3) forment un système rationnel de $n(n-1)$ points. Il en résulte que les points singuliers de $C^{(n)}$ sont des points algébriques d'un degré $\leqq n(n-1)$ relativement à Ω. On voit aisément que la courbe (3) ne peut passer par aucun point fixe autre que les points singuliers, lorsque les nombres (rationnels) a, b et c varient de toutes les manières. Il en résulte que les points singuliers ne peuvent être conjugués qu'entre eux. Ainsi les points singuliers de $C^{(n)}$ forment un système rationnel de $\frac{1}{2}(n-1)(n-2)$ points au plus. On en conclut:

Théorème 4. *Les points singuliers d'une courbe algébrique propre du $n^{\text{ième}}$ degré dans le domaine Ω forment un système rationnel dans Ω de $\frac{1}{2}(n-1)(n-2)$ points au plus.*

5. Systèmes rationnels et points singuliers sur les quartiques. — Soit donnée la quartique propre Q dans le domaine Ω. D'après le théorème 4 les points singuliers de Q forment un système rationnel dans Ω de trois points au plus.

Si la quartique admet un point rationnel qui n'est pas singulier, elle admet une infinité de triplets rationnels. En effet, toute droite rationnelle passant par le point rationnel coupera la quartique en un triplet rationnel.

Si la quartique admet un point rationnel ordinaire P, qui n'est pas un point d'inflexion, elle admet une couple rationnelle. En effet, la tangente T en P est une droite rationnelle, qui coupera la quartique en une couple rationnelle. Si T est une tangente double ou si T passe par un point singulier, la couple se réduit à un seul point rationnel.

Quand la quartique est unicursale, elle est équivalente dans Ω ou à une droite rationnelle ou à une conique rationnelle, qui n'admet aucun point rationnel. Dans le premier cas elle admet une infinité de points rationnels; dans le second cas elle n'admet aucun système rationnel d'un nombre impair de points ordinaires. Par conséquent, si une quartique de genre zéro admet un système rationnel d'un nombre impair de points ordinaires, elle admet nécessairement un point rationnel ordinaire.

Exemple. Soit Ω réel. La quartique

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

est unicursale; elle a les trois points singuliers: (0, 1, 0), (0, 0, 1) et (1, 0, 0). Elle n'admet aucun autre point rationnel dans Ω. Donc, si elle admet un système rationnel de n points ordinaires, le nombre n est pair. Elle admet évidemment une infinité de couples rationnelles.

Considérons ensuite une quartique Q du premier genre. Si Q admet un point rationnel ordinaire, elle est équivalente dans Ω à une cubique rationnelle de genre un; voir H. POINCARÉ, Sur les propriétés arithmétiques des courbes algébriques, Journal de Mathématiques, 5^e série, t. 17, p. 161 (1901). Alors elle admet une infinité de triplets rationnels. Si Q n'admet aucun point rationnel ordinaire, on peut montrer qu'il n'y a aucun triplet rationnel de points ordinaires sur la courbe. Nous allons en donner la démonstration dans un travail qui paraîtra prochainement.

Exemple. La quartique

$$x^4 + y^4 = 3 y^2 z^2$$

est du premier genre; elle a les deux points singuliers confondus à l'origine (nœud de tangence). Elle n'admet aucun autre point rationnel dans $\boldsymbol{K}$ (1). Si elle admet un corps résolvant de degré $n > 1$, le nombre n est pair. Elle admet une infinité de corps résolvants quadratiques dans $\boldsymbol{K}$ (1).

Quand la quartique est du deuxième genre, elle admet une infinité de couples rationnelles. En effet, le point singulier est rationnel, et toute droite rationnelle menée par celui-ci coupera la quartique en une couple rationnelle.

Exemple. Soit Ω réel. La quartique

$$x^4 + y^4 + (x^2 + y^2) z^2 = 0$$

est du deuxième genre; le point singulier est à l'origine. Elle n'admet aucun autre point rationnel dans Ω. Donc, si elle admet un système rationnel de n points ordinaires, le nombre n est pair. Elle admet évidemment une infinité de couples rationnelles.

Une quartique du troisième genre n'a aucun point singulier. Elle peut admettre des triplets rationnels ou non.

Exemple. La quartique

$$a x^4 + b y^4 + c z^4 = 0$$

a évidemment le genre 3. Choisissons les coefficients a, b et c tels que la conique

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

n'admette aucun point rationnel dans Ω. Alors il est évident que la quartique n'admet aucun système rationnel de n points dans Ω, lorsque n est impair. (Théorème 1).

Nous allons continuer prochainement nos recherches sur l'arithmétique des quartiques.

Tryckt den 18 september 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB