B. Segre

332

As an immediate consequence of theorems III, VI and of the first part of theorem VII, we obtain

THEOREM VIII. In S<sub>3,8</sub> there exist ovaloids which are not quadrics. However, each of them defines a null polarity, exactly in the same way as it was a quadric.

#### References

- [1] A. Barlotti, Un'estensione del teorema di Segre-Kustaanheimo, Boll. Un. Mat. Ital., (3) 10 (1955), p. 498-506.
- [2] G. F. Panella, Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, Boll. Un. Mat. Ital. (3) 10 (1955), p. 507-513.
- [3] E. Seiden, A theorem in finite projective geometry and an application to statistics, Proc. Amer. Math. Soc. 1 (1950), p. 282-286.
  - [4] B. Segre, Lezioni di geometria moderna, vol. I, Bologna, Zanichelli, 1948.
- [5] Ovals in a finite projective plane, Canadian Journ. of Math. 7 (1955), p. 414-416.
- [6] Sui k-archi nei piani finiti di caratteristica due, Revue de Math. pures et appl. 2 (1957), p. 283-294.
- [7] On Galois geometries (Lecture given at the Edinburgh Internat. Congr. of Math., on August 19, 1958).
  - [8] Le geometrie di Galois, Annali di Mat. (4) 48 (1959), p. 1-97.

Recu par la Rédaction le 4. 3. 1959



#### ACTA ARITHMETICA V (1959)

# Les points exceptionnels rationnels sur certaines cubiques du premier genre

par

T. NAGELL (Uppsala)

#### § 1. Les points exceptionnels sur une cubique

1. Soit donnée la cubique C de genre un représentée par l'équation

$$(1) F(x,y,z) = 0$$

en coordonnées homogènes. Soit P un point sur la cubique. La tangente à la cubique en ce point rencontre la cubique en un second point  $P_1$ , le point tangentiel de P. Soit ensuite  $P_2$  le point tangentiel de  $P_1$  et soit  $P_3$  le point tangentiel de  $P_2$  et ainsi de suite. Nous aurons alors une suite infinie de points.

(2) 
$$P = P_0, P_1, P_2, P_3, \dots, P_m, \dots,$$

où  $P_m$  est le point tangentiel de  $P_{m-1}$ . Si tous ces points sont distincts, nous appelons le point P point normal. Dans le cas contraire, il n'y a qu'un nombre fini de points distincts, et nous appelons le point P point exceptionnel. J'ai proposé cette notion dans un travail publié en 1935, voir [1], [2] et [3] (1). Si le point P est exceptionnel, tous les autres points dans la suite (2) sont aussi exceptionnels.

Les neuf points d'inflexion sont évidemment des points exceptionnels.

Choisissons la représentation paramétrique des coordonnées de la cubique (1) par des fonctions elliptiques de telle façon que le point d'argument u=0 corresponde à un point d'inflexion. Soit u l'argument du point P. L'argument du point tangentiel  $P_1$  est alors -2u et l'argument du point  $P_m$  dans la suite (2) est  $(-2)^m u$ . Si, dans la suite (2), tous les points coincident, le point initial P est un point d'inflexion.

<sup>(1)</sup> Les numéros figurant entre crochets renvoient à la Bibliographie placée à la fin de ce travail.

2. Pour toute cubique de la forme

$$Y^2 = X^3 - AX - B$$

on a la représentation paramétrique donnée par les formules

(4) 
$$\begin{split} X &= \wp\left(u; 4A, 4B\right) = \wp\left(u; \omega, \omega'\right), \\ 2Y &= \wp'\left(u; 4A, 4B\right) = \wp'\left(u; \omega, \omega'\right), \end{split}$$

où 4A et 4B sont les invariants, et où  $\omega$  et  $\omega'$  désignent une paire de périodes primitive.

Alors on voit aisément: pour que le point P d'argument u sur la cubique (3) soit exceptionnel, il faut et il suffit que u soit commensurable à une période de la fonction  $\wp(u)$ . Le point d'argument u=0 est le point d'inflexion à l'infini.

Quand n est le plus petit nombre naturel, tel que nu soit égal à une période, nous dirons que le point d'argument u est de l'ordre n. Les abscisses X des points exceptionnels d'ordre n (> 2) de (3) sont les zéros d'un polynome  $\Phi_n(X)$  du degré

$$\frac{1}{2}n^2\prod_p\left(1-\frac{1}{p^2}\right)$$

en X, le produit étant étendu à tous les nombres premiers p qui divisent n; les coefficients du polynome  $\Phi_n$  sont des polynomes en A et B à coefficients rationnels en K(1); voir [27].

Les points d'inflexion sont du troisième ordre sauf le point d'argument u=0 qui est d'ordre 1.

En prenant l'addition pour mode de composition on voit que les arguments u des points exceptionnels sur la cubique (3) forment un groupe abélien infini. Nous appelons ce groupe le groupe exceptionnel de la cubique.

3. Considérons la cubique spéciale

(5) 
$$ax^3 + by^3 + cz^3 + dxyz = 0,$$

où  $abc \neq 0$  et  $27abc \neq -d^3$ . Les neuf points d'inflexion de cette cubique sont évidemment

$$(1, \alpha_1, 0), (1, \alpha_2, 0), (1, \alpha_3, 0), (1, 0, \beta_1), (1, 0, \beta_2), (1, 0, \beta_3), (0, 1, \gamma_1),$$
  
 $(0, 1, \gamma_2) \text{ et } (0, 1, \gamma_3),$ 

où  $a_1$ ,  $a_2$  et  $a_3$  sont les racines de l'équation  $ba^3 + a = 0$ , où  $\beta_1$ ,  $\beta_2$  et  $\beta_3$  sont les racines de l'équation  $c\beta^3 + a = 0$  et où  $\gamma_1$ ,  $\gamma_2$  et  $\gamma_3$  sont les racines de l'équation  $c\gamma^3 + b = 0$ .

On vérifie aisément que les coordonnées  $x_1, y_1, z_1$  du point tangentiel  $P_1(x_1, y_1, z_1)$  du point P(x, y, z) sur la cubique (5) sont données par les formules

 $z_1 = z(ax^3 - by^3).$ 

Si P(x, y, z) est un point sur la cubique (5) les points  $P^*(x, y\varrho_1, z\varrho_2)$  se trouve aussi sur la cubique, quand  $\varrho_1^3 = \varrho_2^3 = \varrho_1\varrho_2 = 1$ . Si P(x, y, z) est un point exceptionnel, le point  $P^*(x, y\varrho_1, z\varrho_2)$  l'est aussi. En effet, soit  $P_1^*$  le point tangentiel du point  $P^* = P^*(x, y\varrho_1, z\varrho_2)$ . Soit ensuite  $P_2^*$  le point tangentiel de  $P_1^*$  et soit  $P_3^*$  le point tangentiel de  $P_2^*$  et ainsi de suite. Désignons par  $x_m$ ,  $y_m$ ,  $z_m$  les coordonnées du point  $P_m$  dans la suite (2). Alors, en appliquant les formules (6) on trouve que les coordonnées du point  $P_m^*$  dans la suite

$$(2^*) P^*, P_1^*, P_2^*, P_3^*, \dots, P_m^*, \dots$$

sont  $x_m, y_m \varrho_1, z_m \varrho_2$ . Donc, si on a  $P_m = P_n$ , on a aussi  $P_n^* = P_n^*$ . On en conclut, si la suite (2) est limitée, la suite (2\*) l'est aussi.

Si on prend, dans (5), d=0, la cubique sera

(7) 
$$ax^3 + by^3 + cz^3 = 0.$$

Pour cette cubique on aura par la même méthode le résultat plus général: Si P(x, y, z) est un point exceptionnel sur la courbe (7), tous les points  $P^*(x, y_{\varrho_1}, z_{\varrho_2})$  sont aussi exceptionnels quand  $\varrho_1$  et  $\varrho_2$  sont des racines quelconques de l'équation  $\varrho^3 = 1$ . Cela donne neuf points différents si P(x, y, z) n'est pas un point d'inflexion, et seulement trois points différents dans le cas contraire.

## § 2. Les points rationnels appartenant à un corps donné

4. Prenons pour domaine de rationalité fondamental un corps quelconque donné x. Dans la suite nous entendons, sauf avis contraire, par
nombre rationnel un nombre appartenant à x. Le point P(x, y, z) en
coordonnées homogènes dans le plan est appelé point rationnel, quand x, y et z sont proportionnels à trois nombres rationnels.

Nous dirons que la cubique

$$(8) F(x,y,z) = 0$$

appartient à 2, quand elle a des coefficients rationnels.

Soient données les deux cubiques C et C' appartenant à  $\mathbf{a}$ . S'il existe une transformation birationnelle à coefficients rationnels qui transforme l'une des deux cubiques dans l'autre, on dit qu'elles sont équivalentes

337

dans 2. J'ai étudié la classification des cubiques au moyen des transformations birationnelles dans des travaux antérieurs; voir p. ex. [41]

Si. dans la suite (2) du § 1, le point initial P est rationnel, tous les autres points sont aussi rationnels.

Dans la suite nous avons besoin des résultats suivants:

THÉORÈME I. Si la cubique (8), appartenant à 2, admet un point rationnel, elle est équivalente dans 2 à une cubique de la forme de Weierstrass.

(9) 
$$Y^2 = X^3 - AX - B,$$

où A et B sont des nombres rationnels.

Pour la démonstration voir [4].

Un cas spécial de ce théorème est le

THÉORÈME II. Si a, b et c sont des nombres rationnels, différents de zéro, et si la cubique

$$ax^3 + by^3 + cz^3 = 0$$

admet un point rationnel, elle est équivalente dans 2 à la cubique

$$(10) X^3 + Y^3 = abcZ^3$$

et à la cubique

$$(11) Y^2 = X^3 - 2^4 \cdot 3^3 \cdot (abc)^2.$$

Pour la démonstration voir [5] et [3].

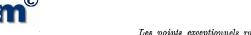
TÉORÈME III. Supposons que la cubique (8), appartenant à 2, n'admet aucun point rationnel. Soit 21 le corps engendré en adjoignant à 2 un nombre algébrique, dont le degré, relatif à 2, est indivisible par 3. Alors la cubique n'admet aucun point rationnel dans 21.

Pour la démonstration voir [8].

5. Si la cubique (8), dans 2, n'admet qu'un seul point rationnel, il est évident que ce point est un point d'inflexion. Cela reste vrai si on remplace "point rationnel" par point exceptionnel rationnel.

Si elle admet exactement 2 points rationnels, l'un de ces points est nécessairement un point d'inflexion. En effet, si dans la suite (2) du § 1 on suppose  $P_2 = P_0$ , on trouve, en comparant les arguments, que  $P_0$ doit être un point d'inflexion, contre l'hypothèse. Il faut donc que  $P_2 = P_1$ , c'est-à-dire  $P_1$  est un point d'inflexion. Cela reste vrai si on remplace "points rationnels" par points exceptionnels rationnels.

Si la cubique admet exactement 3 points rationnels, on voit aisément qu'il n'y a pas nécessairement un point d'inflexion parmi eux. En effet, les arguments de ces points peuvent être  $\omega/9$ ,  $-2\omega/9$  et  $4\omega/9$ , où  $\omega$  est une période de la fonction  $\wp(u)$ .



Si deux points d'inflexion sont rationnels, il y a toujours un troisième point d'inflexion qui est rationnel. En effet, la droite rationnelle menée par les deux points d'inflexion rencontre la courbe dans un troisième point rationnel qui est aussi un point d'inflexion.

Rappelons ensuite des résultats suivants relatifs aux points exceptionnels rationnels dans 2.

THÉORÈME IV. Supposons que les deux cubiques (8) et (9) sont équivalentes dans 2. Si le nombre n des points exceptionnels rationnels sur la cubique (9) est limité, le nombre m des points exceptionnels rationnels sur la cubique (8) est aussi limité, et on a ou m = 0 ou m = n.

. Pour la démonstration voir [3], I.

Les points exceptionnels rationnels dans 2 forment un sous-groupe du groupe exceptionnel de la cubique (9). Nous désignons ce sous-groupe par G. Si le groupe G est fini, il est cyclique ou bicyclique; voir [3], I. Il est fini quand 2 est un corps algébrique, et dans ce cas on peut toujours déterminer les points et le groupe exceptionnels de (9) dans 2: voir [1] et [6]. Alors on peut même déterminer les points exceptionnels dans 2 sur une cubique quelconque; voir [3], I.

Dans des travaux antérieurs nous avons déterminé les conditions nécessaires et suffisantes auxquelles doivent satisfaire les invariants A et B pour que le groupe G admette un sous-groupe G, d'ordre fini n pour les valeurs suivantes n = 3, 4, 5, 6, 7 et 9; voir [7].

Théorème IV peut être complété par la proposition suivante:

Si deux cubiques dans 2 sont reliées par une transformation linéaire à coefficients rationnels dans 2, cette transformation fait correspondre à chaque point exceptionnel rationnel de l'une des cubiques un point exceptionnel rationnel de l'autre; spécialement, les points d'inflexion se correspondent entre eux. Ainsi, dans ce cas, les deux cubiques ont le même nombre de points exceptionnels rationnels, pourvu que ce nombre soit limité. Cela n'est pas en général vrai quand la transformation birationnelle qui relie les deux cubiques, n'est pas linéaire.

# 8 3. La cubique $ax^3+by^3+cz^3=0$ dans un corps quelconque

6. Dans la suite nous allons nous occuper surtout de la cubique spéciale

(7) 
$$ax^3 + by^3 + cz^3 = 0,$$

où a, b et c sont des nombres rationnels (dans 2), différents de zéro. Si cette cubiqe admet un point d'inflexion rationnel, elle peut s'écrire

$$(12) x^3 + y^3 + abcz^3 = 0.$$

En effet, dans ce cas l'un (au moins) des nombres a/b, a/c, b/c doit être égal au cube d'un nombre rationnel Si on a p. ex.  $a = bh^3$ , h rationnel, la cubique (7) peut s'écrire

$$(hx)^3 + y^3 + abc\left(\frac{z}{bh}\right)^3 = 0.$$

En y remplaçant hx par x et z/bh par z on aura la cubique (12).

Pour que la cubique (12) admette trois points d'inflexion rationnels il faut évidemment qu'on ait l'un des deux cas: a contient le nombre  $\sqrt{-3}$ . Le nombre abc est égal au cube d'un nombre rationnel. Dans le dernier cas la cubique (12) peut s'écrire

$$(13) x^3 + y^3 + z^3 = 0.$$

Supposons que la cubique (7) admet un point exceptionnel rationnel  $P(\alpha, \beta, \gamma)$ , avec  $\gamma \neq 0$ , tel que son point tangentiel soit égal à un point d'inflexion. Nous écrivons la cubique sous la forme (12) en supposant que le point d'inflexion en question correspond à z = 0. Alors on a, d'après les formules (6),  $\alpha^3 - \beta^3 = 0$ . Vu que  $\alpha^3 + \beta^3 = -abc\gamma^3$ , on aura donc  $abc = 2(-a/\gamma)^3$ . Ainsi la cubique peut s'écrire

$$(14) x^3 + y^3 + 2z^3 = 0.$$

Supposons maintenant que la cubique (7) admet exactement  $m \ (\geqslant 1)$  points exceptionnels rationnels (dans 2). D'après le Théorème II cette cubique est équivalente (dans 2) à la cubique (11). D'après le Théorème III celle-ci admet aussi exactement m points exceptionnels rationnels (dans 2). Désignons par G le groupe des points exceptionnels (dans 2) sur la cubique (11).

Dans ce qui suivra nous allons appliquer les résultats que nous avons obtenus dans notre travail [7], § 1-§ 6, sur l'existence de certains sous-groupes exceptionnels.

Si abc est le cube d'un nombre rationnel, la courbe (7) est équivalente à la courbe

$$(13) x^3 + y^3 + z^3 = 0$$

et à la courbe

$$(13a) Y^2 = X^3 - 432.$$

Le groupe G de cette cubique a évidemment un sous-groupe d'ordre 3 (trois points d'inflexion, dont les deux à distance finie ont les coordonnées  $X=12,\ Y=\pm 36$ ). On en conclut que, dans ce cas, m est divisible par 3.

Si abc est égal au double du cube d'un nombre rationnel, la courbe

$$(14) x^3 + y^3 + 2z^3 = 0$$

et à la courbe

$$(15) Y^2 = X^3 - 27.$$

L'ordre m du groupe G de cette cubique est évidemment un nombre pair.

Si a contient le nombre  $\sqrt{-3}$ , on démontre sans difficulté: Le nombre m est divisible par 9 sauf dans le cas suivant; s'il y a exactement 3 points d'inflexion rationnels sur la cubique (7), le nombre m-3 est divisible par 9. En effet, si P=P(x,y,z) est un point rationnel sur (7), les neuf points  $P^*=P^*(x,y\varrho_1,z\varrho_2)$ , où  $\varrho_1$  et  $\varrho_2$  sont des racines quelconques de l'équation  $\varrho^3=1$ , sont aussi rationnels; et si P est un point exceptionnel, les points  $P^*$  sont aussi exceptionnels (voir le numéro 3). Les points  $P^*$  sont différents entre eux, sauf si P est un point d'inflexion; dans le dernier cas il n'y a que trois des points  $P^*$  qui sont distincts, et ceux-ci sont des points d'inflexion. Enfin, s'il y a quatre points d'inflexion rationnels sur (7), tous les neuf points d'inflexion sont rationnels (cp. le numéro 3). Sur la cubique (11) il y a, en dehors du point d'inflexion à l'infini, les deux points d'inflexion rationnels aux coordonnées X=0,  $Y=\pm 4(\sqrt{-3})^a abc$ .

7. Si m=1, le point exceptionnel est un point d'inflexion. Alors il faut que l'un des trois nombres a/b, a/c, b/c soit le cube d'un nombre rationnel. Si deux de ces nombres sont des cubes, il est évident que trois points d'inflexion sont rationnels. S'il y a un second point rationnel sur la cubique, ce point est normal, et alors la courbe admet une infinité de points rationnels.

Si m est pair, il faut que le binome cubique à droite dans l'équation (1.1) ait un zéro rationnel. Donc le nombre  $2^4 \cdot 3^3 \cdot (abc)^2$  doit être le cube d'un nombre rationnel. Il en résulte que abc doit être égal au double du cube d'un nombre rationnel. Alors la cubique est équivalente aux cubiques (14) et (15).

Si spécialement m=2, il faut que l'un des nombres a/b, a/c, b/c soit le cube d'un nombre rationnel. Si aucun de ces nombres n'est égal au cube d'un nombre rationnel, et si  $abc=2h^3$ , h rationnel, on a  $m \ge 4$ .

Supposons que *m* est divisible par 3. Dans ce cas nous appliquons le Théorème 1, dans [7] à la cubique (11). Celle-ci doit avoir trois points d'inflexion rationnels. Alors elle est équivalente ou à chacune des deux cubiques (13) et (13a), ou à une cubique de la forme

$$(16) Y^2 = X^3 + h^2,$$

h étant un nombre rationnel. Si les cubiques (11) et (16) sont équivalentes,

il faut évidemment que  $\Omega$  contienne le nombre  $\sqrt{-3}$ . Les points d'inflexion rationnels à distance finie de (16) ont les coordonnées X=0, Y=+h

Pour que m soit divisible par 3 il faut et il suffit donc qu'une des deux conditions suivantes soit remplie: abc est le cube d'un nombre rationnel. a contient le nombre  $\sqrt{-3}$ .

**8.** Supposons que m est divisible par 4. Il y a deux cas différents à distinguer. Dans le premier cas nous adaptons le Théorème 3 dans [7]. En y posant A=0 on voit que a contient le nombre  $\sqrt{-3}$ . D'après ce que nous venons de montrer, il faut donc que m soit divisible par 3. Alors l'ordre m est divisible par 12. Ainsi les possibilités m=4 et m=8 sont exclues.

Dans le second cas nous aurons à adapter le Théorème 4 dans [7]. En y posant A=0 on aura  $B=a_1^3$  (en remplaçant a par  $a_1$ ) et

$$e=a_1\pm a_1\sqrt{3}.$$

Donc a contient le nombre  $\sqrt{3}$ . Puisque la cubique (11) est équivalente à la cubique (15), on peut mettre  $a_1 = 1$ . Alors on aura

$$\pm d = \sqrt{a_1 + 2e} = \sqrt{3 \pm 2\sqrt{3}}.$$

On en conclut que a doit contenir l'un ou l'autre des nombres

$$\sqrt{3+2\sqrt{3}}$$
 ou  $\sqrt{3-2\sqrt{3}}$ 

Cette condition est aussi suffisante quand  $abc = 2h^3$ , h rationnel.

9. Supposons que m est divisible par 5. Dans ce cas nous aurons à adapter le Théorème 5 dans [7]. Posons A=0 et désignons par  $\alpha$  une racine de l'équation biquadratique

$$a^4 + 3a^3 - a^2 - 3a + 1 = 0,$$

et par  $\beta$  la racine carrée du nombre

$$-19a^{6}-18a^{5}+15a^{4}+15a^{2}+18a-19$$
.

Alors  $\alpha$  doit contenir les nombres  $\alpha$  et  $\beta$ , et on doit avoir

$$abc = \beta h^3$$
,

h étant un nombre dans a.

10. Supposons que m est divisible par 6. Alors, il faut adapter le Théorème 6 dans [7]. Il y aura deux possibilités. On peut avoir le cas que la cubique (11) est équivalente à la cubique

$$(17) Y^2 = X^3 + 1.$$

Alors il faut que 2 contienne le nombre  $\sqrt{-3}$ . Puisque la cubique (17) admet (au moins) 12 points exceptionnels rationnels dans ce cas, on conclut que m est divisible par 12.

Dans le second cas il faut qu'on ait à la fois  $abc = h^3$  et  $abc = 2h_1^3$ , où h et  $h_1$  sont des nombres rationnels. Cette condition est aussi suffisante. Donc le nombre 2 est le cube d'un nombre rationnel.

Supposons spécialement que m=6. Dans ce cas la cubique (11) ne peut pas être équivalente à la cubique (17). Donc elle est équivalente à la cubique

$$(13) x^3 + y^3 + z^3 = 0.$$

Le corps 2 ne peut pas contenir le nombre  $\sqrt{-3}$ . En effet, tous les neuf points exceptionnels de la courbe (13) sont rationnels, si 2 contient  $\sqrt{-3}$ .

Supposons que m est divisible par 7. Dans ce cas il faut adapter le Théorème 7 dans [7]. Posons A=0 et désignons par  $\xi$  une racine de l'équation algébrique

$$\xi^8 - 20\xi^7 + 154\xi^6 - 616\xi^5 + 1435\xi^4 - 2016\xi^3 + 1666\xi^2 - 732\xi + 129 = 0$$

et par n la racine carrée du nombre

$$-2\xi^{12} + 60\xi^{11} - 762\xi^{10} + 5468\xi^{0} - 24972\xi^{8} + 77124\xi^{7} - 166362\xi^{6} + 254364\xi^{5} - 275796\xi^{4} + 208636\xi^{3} - 105426\xi^{2} + 32148\xi - 4482$$

Alors 2 doit contenir les nombres  $\xi$  et  $\eta$ , et on doit avoir

$$4abc = \eta h^6,$$

h étant un nombre dans 2.

11. Nous allons illustrer la discussion précédente par quelques exemples numériques.

Quand  $\mathbf{a} = \mathbf{K}(1)$ , il est bien connu que les cubiques suivantes réalisent les cas m = 1, m = 2 et la première catégorie du cas m = 3:

$$(18) x^3 + y^3 + 3z^3 = 0$$

avec le point (1, -1, 0);

$$(14) x^3 + y^3 + 2z^3 = 0$$

avec les points (1, 1, -1) et (1, -1, 0);

$$(13) x^3 + y^3 + z^3 = 0$$

avec les points (1, 0, -1), (0, 1, -1) et (1, -1, 0).

Quand  $\mathbf{2} = \mathbf{K}(\sqrt{-3})$ , la cubique (18) réalise la seconde catégorie du cas m=3 avec les points (1,-1,0),  $(1,-\varrho,0)$  et  $(1,-\varrho^2,0)$ , où  $\varrho^2+\varrho+1=0$ ; voir [9], Theorems 120-122.



Posons  $\alpha = \sqrt{3+2\sqrt{3}}$  et prenons  $\Omega = K(\alpha)$ . Alors la cubique (14) réalise le cas où m est divisible par 4; les points correspondants sont  $(1, -1, 0), (1, 1, -1), (1+\alpha, 1-\alpha, -1-\sqrt{3})$  et  $(1-\alpha, 1+\alpha, -1-\sqrt{3})$ . On a probablement dans ce cas m=4.

Posons  $\alpha = \sqrt[3]{2}$  et prenons  $\Omega = K(\alpha)$ . Alors la cubique (13) réalise le cas où m = 6; les points en question sont (1, -1, 0), (0, 1, -1), (1, 0, -1),  $(\alpha, -1, -1)$ ,  $(1, -\alpha, 1)$  et  $(1, 1, -\alpha)$ . Ce résultat est compris dans Théorème 4; voir le numéro 18.

12. En résumant quelques-uns des résultats obtenus dans ce paragraphe nous pouvons énoncer le

THEOREME 1. Désignons par m le nombre des points exceptionnels rationnels dans le corps 2 sur la cubique

$$ax^3 + by^3 + cz^3 = 0$$
.

où a, b et c sont des nombres rationnels dans a, abc  $\neq 0$ . Supposons que m > 0 et limité.

Premier cas. 2 ne contient pas le nombre  $\sqrt{-3}$ .

Si aucun des nombres a/b, a/c, b/c, abc, 4abc n'est égal au cube d'un nombre rationnel dans a, le nombre m n'est divisible ni par a ni par a, et on a a a b

Deuxième cas. Si on ajoute aux conditions faites dans le premier cas la condition suivante: 2 ne contient aucun des nombres  $\alpha$ ,  $\beta$ ,  $\xi$  et  $\eta$ , définis dans les numéros 9 et 10, le nombre m n'est divisible par aucun nombre premier < 11, et on  $a m \ge 11$ .

Troisième cas. 2 contient le nombre  $\sqrt{-3}$ .

Si exactement trois points d'inflexion de la cubique sont rationnels, on a  $m \equiv 3 \pmod{9}$ . Dans tous les autres cas on a  $m \equiv 0 \pmod{9}$ .

Si on y ajoute la condition suivante: Le nombre 4abc n'est pas égal au cube d'un nombre rationnel, le nombre m est impair.

Pour obtenir des résultats plus étendus il est évident qu'il faut spécialiser le corps a. Dans ce qui suivra le domaine fondamental sera un corps algébrique.

## § 4. La cubique $ax^3+by^3+oz^3=0$ dans un corps algébrique simple

13. Dans la suite nous supposons que  $\mathfrak A$  est un corps algébrique simple, c'est-à-dire un corps dans lequel le nombre des classes d'idéaux est égal à 1. Nombre rationnel signifie nombre dans  $\mathfrak A$ . Nombre entier signifie entier dans  $\mathfrak A$ . Si  $\pi$  est un nombre entier, tel que l'idéal  $(\pi)$  soit un idéal premier, nous dirons que  $\pi$  est un nombre premier (exception

faite du corps K(1) des nombres rationnels ordinaires, où les nombres premiers sont positifs). Dans un corps de ce type on n'a pas besoin des idéaux. Si  $\alpha$ ,  $\beta$ ,  $\gamma$  etc. sont des entiers, nous désignons par  $(\alpha, \beta, \gamma, \ldots)$  le "plus grand commun diviseur" de  $\alpha$ ,  $\beta$ ,  $\gamma$  etc. Ce nombre n'est déterminé qu'à une unité près. Nous écrivons  $(\alpha, \beta, \gamma, \ldots) = 1$  quand il n'y a aucun nombre premier qui divise tous les nombres  $\alpha$ ,  $\beta$ ,  $\gamma$  etc.

Soient a, b et c des nombres entiers (dans a) tels que  $abc \neq 0$ , et considérons la cubique

$$ax^3 + by^3 + cz^3 = 0.$$

Il est évident qu'on peut supposer que (a,b,c)=1. On peut aussi supposer que aucun des nombres a,b et c n'est divisible par le cube d'un nombre premier.

Soit P(x, y, z) un point rationnel (dans x) sur la cubique (19). Alors on peut supposer que les nombres x, y et z sont des nombres entiers tels que (x, y, z) = 1. On peut même supposer que (x, y) = (x, z) = (y, z) = 1. En effet, si le nombre premier x divise l'un et l'autre des nombres x et y, il résulte de (19) que  $x^3$  est divisible par  $x^3$ . Donc z serait divisible par x, ce qui est contre l'hypothèse que (x, y, z) = 1.

Si nous posons

(20) 
$$(a, b) = dd_1^2, \quad (a, c) = ee_1^2, \quad (b, c) = ff_1^2,$$

où  $d, d_1, e, e_1, f$  et  $f_1$  sont des nombres entiers tels que

$$(d, d_1) = (e, e_1) = (f, f_1) = 1,$$

nous avons

$$(22) (dd_1, ee_1) = (dd_1, ff_1) = (ee_1, ff_1) = 1.$$

Si nous posons ensuite

(23) 
$$a = dd_1^2 e e_1^2 a_1, \quad b = dd_1^2 f f_1^2 b_1, \quad c = e e_1^2 f f_1^2 c_1,$$

où  $a_1$ ,  $b_1$  et  $c_1$  sont des nombres entiers, nous avons

$$(24) (ee_1a_1, ff_1b_1) = (dd_1a_1, ff_1c_1) = (dd_1b_1, ee_1c_1) = 1.$$

Alors il résulte de (19) que  $z^3$  est divisible par  $dd_1^2$ , que  $y^3$  est divisible par  $ee_1^2$  et que  $x^3$  est divisible par  $ff_1^2$ . Il faut donc que

(25) 
$$x = ff_1x_1, \quad y = ee_1y_1, \quad z = dd_1z_1,$$

où  $x_1$ ,  $y_1$  et  $z_1$  sont des nombres entiers. En introduisant ces valeurs dans (19) on aura, après avoir divisé par  $dd_1^2 e c_1^2 f_1^2$ ,

(26) 
$$f^2 f_1 a_1 x_1^3 + e^2 e_1 b_1 y_1^3 + d^2 d_1 c_1 z_1^3 = 0.$$

Les points exceptionnels rationnels

Ici les coefficients  $f^2f_1a_1$ ,  $e^2e_1b_1$  et  $d^2d_1e_1$  sont premiers entre eux deux à deux. En effet, à cause de la symétrie, il suffit de montrer que  $(f^2f_1a_1, e^2e_1b_1) = 1$ . Il résulte de (22) que  $(ff_1, ee_1) = 1$ . Soit  $\pi$  un nombre premier qui divise l'un et l'autre des nombres  $a_1$  et  $ee_1$ . Alors il suit de (26) que  $d^2d_1e_1z_1^3$  est divisible par  $\pi$ . D'après (24) on a  $(a_1, e_1) = 1$  et d'après (22) on a  $(dd_1, ee_1) = 1$ . Donc il faut que  $\pi$  divise  $z_1$ . Alors y et z seraient, tous les deux, divisibles par  $\pi$ . Or, cela est contre l'hypothèse que (y, z) = 1. Daprès (24) on a  $(a_1, b_1) = 1$ . Si  $\pi$  est un nombre premier qui divise l'un et l'autre des nombres  $b_1$  et  $ff_1$ , il résulte de (26) que  $d^2d_1e_1z_1^3$  est divisible par  $\pi$ . Puisque  $(b_1, e_1) = (dd_1, ff_1) = 1$ , il faut que  $\pi$  divise  $z_1$ . Alors x et z seraient, tous les deux, divisibles par  $\pi$ . Or, cela est contre l'hypothèse que (x, z) = 1.

Il résulte de tout cela qu'on peut supposer dans (19), sans restreindre la généralité, que (a, b) = (a, c) = (b, c) = 1.

Ainsi, dans la suite de ce paragraphe, nous pouvons supposer que les coefficients a, b et c de la cubique (19) sont assujettis aux conditions suivantes:

Ils sont des entiers différents de zéro tels que aucun d'eux ne soit divisible par le cube d'un nombre premier. On a en outre

$$(a, b) = (a, c) = (b, c) = 1.$$

Deux cubiques de la forme (19) sont considérées comme identiques quand elles sont reliées par des transformations linéaires du type  $x' = \varepsilon x$ ,  $y' = \varepsilon_1 y$ ,  $z' = \varepsilon_2 z$ , où  $\varepsilon$ ,  $\varepsilon_1$  et  $\varepsilon_2$  sont des unités dans  $\boldsymbol{\varrho}$ .

Si P(x, y, z) est un point rationnel sur la cubique nous supposons dorénavant que x, y et z sont des entiers tels que

$$(28) (x,y) = (x,z) = (y,z) = 1.$$

Remarque. Il faut noter le résultat spécial suivant (comparez [10]):

Si la cubique a la forme

$$ax^3 + \pi b_1 y^3 + \pi^2 c_1 z^3 = 0,$$

où  $\pi$  est un nombre premier, qui ne divise ni a ni  $b_1$ , elle n'admet aucun point rationnel.

En effet, soit P(x, y, z) un point rationnel satisfaisant aux relations (28). Alors il faut que x soit divisible par  $\pi$ . Cela entraîne ensuite que y est divisible par  $\pi$ , ce qui est contre la condition que (x, y) = 1.

14. La condition nécessaire et suffisante pour que la cubique (19) admette un point d'inflexion rationnel, est que l'un (au moins) des nombres a/b, a/c, b/c soit le cube d'un nombre rationnel. Soit p. ex.  $a = b\eta^s$ , où

 $\eta$  est rationnel. Alors, si on pose  $X=\eta x,\ Y=y$  et  $Z=z/\eta b,$  la cubique aura la forme

$$(29) X^3 + Y^3 + abcZ^3 = 0.$$

Vu que (a, b) = 1, il résulte de la relation  $a = b\eta^3$  que les nombres a, b et  $\eta$  sont des unités (dans a), tous les trois. Supposons qu'on a en outre  $a = c\eta_1^3$ , où  $\eta_1$  est rationnel. Alors l'équation de la cubique peut s'écrire

$$(29') X^3 + Y^3 + Z^3 = 0,$$

où l'on a remplacé Z dans (29) par  $\frac{a}{\eta \eta_1} Z$ .

Soit donné le point rationnel P = P(x, y, z) sur la cubique (19). Nous supposons que P n'est pas un point d'inflexion et que le point tangentiel de P n'est pas un point d'inflexion non plus.

Les coordonnées  $\xi,\ \eta$  et  $\zeta$  du point tangentiel  $P_1$  de P sont données par les formules

(30) 
$$\delta \xi = x(by^3 - cz^3),$$

$$\delta \eta = y(cz^3 - ax^3),$$

$$\delta \xi = z(ax^3 - by^3).$$

où  $\delta$  est un nombre entier tel que  $\xi,\ \eta$  et  $\zeta$  soient des nombres entiers satisfaisant aux conditions

$$(\xi,\eta)=(\xi,\zeta)=(\eta,\zeta)=1.$$

Par suite de nos suppositions sur P tous les nombres

(31) 
$$x, y, z, by^3 - cz^3, cz^3 - ax^3, ax^3 - by^3$$

sont différents de zéro.

Soit  $\pi$  un nombre premier qui divise  $\delta$ . Si  $\pi$  divise x, il suit de (30) que  $\pi$  divise les deux nombres  $ycz^3$  et  $zby^3$ . Or, cela est impossible vu que (x, y) = (x, z) = (b, c) = 1. On a donc  $(\delta, x) = (\delta, y) = (\delta, z) = 1$ . Il faut par suite que

(32) 
$$by^3 - cz^3 \equiv cz^3 - ax^3 \equiv ax^3 - by^3 \equiv 0 \pmod{\delta}$$
.

Il en résulte aisément, vu que  $ax^3 + by^3 + cz^3 = 0$ ,

$$3ax^3 \equiv 3by^3 \equiv 3cz^3 \equiv 0 \pmod{\delta}$$
.

On en conclut, vu que  $(\delta,x)=(\delta,y)=(\delta,z)=(a,b)=(a,c)=(b,c)=1$ , qu'on a

$$(33) 3 \equiv 0 \pmod{\delta}.$$

15. Soit P=P(x,y,z) un point rationnel sur la cubique, où x,y et z sont des entiers tels que (x,y)=(x,z)=(y,z)=1. Si N(a) signifie la norme du nombre a dans a, nous appelons le nombre |N(xyz)| l'index du point p. L'index d'un point rationnel est un nombre entier positif dans p dans p quand p est un point d'inflexion.

Supposons que P est un point exceptionnel, qui n'est pas un point d'inflexion et dont le point tangentiel n'est pas un point d'inflexion. Alors il résulte des relations (30) et (32) que

$$|N(xyz)| \leqslant |N(\xi\eta\zeta)|.$$

Vu que le nombre des points exceptionnels rationnels sur la cubique est limité, l'index de ces points a un certain maximum M. Si on suppose que |N(xyz)| = M, il faut donc qu'on ait

$$|N(xyz)| = |N(\xi\eta\zeta)|.$$

Alors il résulte des relations (30) et (32) que les nombres

$$\frac{1}{\delta}(by^3-cz^3), \quad \frac{1}{\delta}(cz^3-ax^3), \quad \frac{1}{\delta}(ax^3-by^3)$$

sont des unités dans  $\mathfrak L$ . Vu que  $\delta$  n'est déterminé qu'à une unité près, on peut supposer que le premier de ces nombres est égal à 1. On aura donc

$$\begin{split} \frac{1}{\delta}(by^3-cz^3) &= \frac{1}{\delta}(2by^3+ax^3) = 1,\\ \frac{1}{\delta}(cz^3-ax^3) &= \frac{1}{\delta}(-2ax^3-by^3) = E,\\ \frac{1}{\delta}(ax^3-by^3) &= E_1, \end{split}$$

où E et  $E_1$  sont des unités dans a. Il en résulte

(36) 
$$1+E+E_{1}=0$$
 et 
$$\frac{3}{\delta}ax^{3}=-1-2E,$$
 (37) 
$$\frac{3}{\delta}by^{3}=2+E,$$
 
$$\frac{3}{\delta}cz^{3}=-1+E.$$

Supposons qu'il existe des solutions de la relation (36), et soit E,  $E_1$  une paire de solutions de celle-ci. Nous pouvons écrire

(38) 
$$-1-2E = \frac{3}{\delta} \cdot \lambda \alpha^{3},$$
$$2+E = \frac{3}{\delta} \cdot \lambda_{1} \alpha_{1}^{3},$$
$$-1+E = \frac{3}{\delta} \cdot \lambda_{2} \alpha_{2}^{3},$$

où  $\lambda$ ,  $\lambda_1$ ,  $\lambda_2$ ,  $\alpha$ ,  $\alpha_1$  et  $\alpha_2$  sont des nombres entiers, tels que aucun des nombres  $\lambda$ ,  $\lambda_1$ ,  $\lambda_2$  ne soit divisible par le cube d'un nombre premier. Il en résulte qu'on peut prendre  $\alpha=\lambda$ ,  $b=\lambda_1$  et  $c=\lambda_2$ . (Cf. la définition faite au n° 13 à propos de l'identité des cubiques.) Ainsi la cubique aura la forme

$$\lambda x^3 + \lambda_1 y^3 + \lambda_2 z^3 = 0,$$

et les points rationnels en question seront donnés par les équations  $x^3 = \alpha^3$ ,  $y^3 = \alpha_1^3$  et  $z^3 = \alpha_2^3$ . Pour une valeur déterminée de E nous aurons une seule cubique et seulement les points rationnels  $P(\alpha, \alpha_1 \varrho_1, \alpha_2 \varrho_2)$ , où  $\varrho_1 = \varrho_2 = 1$  quand  $\Omega$  ne contient pas le nombre  $\sqrt{-3}$ , et où  $\varrho_1$  et  $\varrho_2$  sont des racines de l'équation  $\varrho^3 = 1$  dans le cas contraire. Il y a ainsi ou un seul point ou neuf points selon les cas. Cependant on ne peut pas être sûr que les points ainsi obtenus soient exceptionnels. Pour décider là-dessus il faut encore un examen additionnel.

Si on remplace dans le système (37) E par  $E_1$  on voit aisément qu'en remplaçant  $3/\delta$  par  $-3/\delta$  et en permutant b et c et y et z, on retombe sur le système (37). Ainsi on aura la même cubique et les mêmes points dans ce cas.

La relation (36) peut être satisfaite quand  $\boldsymbol{\varrho}$  contient le nombre  $\sqrt{-3}$ . En effet, si  $\varrho = \frac{1}{2}(-1+\sqrt{-3})$  on a  $1+\varrho+\varrho^2=0$ .

## 16. De ce qui précède nous aurons le résultat suivant:

THÉORÈME 2. Soit  $\mathfrak A$  un corps algébrique simple, qui ne contient pas le nombre  $\sqrt{-3}$ . Désignons par m le nombre des points exceptionnels rationnels sur la cubique (19). Si la relation (36) est impossible dans  $\mathfrak A$  ou si elle est satisfaite par une seule paire d'unités E et  $E_1$  dans  $\mathfrak A$ , on a m=0, sauf dans les cas suivants: Si la cubique a la forme

$$(40) x^3 + y^3 + cz^3 = 0,$$

où ni c ni 4c n'est égal au cube d'un nombre rationnel, on a m=1. Si la cubique a la forme

$$(41) x^3 + y^3 + 2z^3 = 0,$$

T. Nagell

et si le nombre 2 n'est pas égal au cube d'un nombre rationnel, on a m=2Enfin, pour la cubique

$$(42) x^3 + y^3 + z^3 = 0$$

on a m = 6 ou m = 3, selon que le nombre 2 est égal au cube d'un nombre rationnel ou non.

Soit  $\mathbf{Q}$  un corps algébrique simple qui contient le nombre  $\sqrt{-3}$ , et soit m le nombre des points exceptionnels rationnels sur la cubique (19). Si la relation (36) n'est satisfaite que par la paire d'unités o et o², où o =  $\frac{1}{2}(-1+\sqrt{-3})$ , on a m=0, sauf dans les cas suivants: Pour la cubique (40) on a m=3. Pour la cubique (41) on a m=12. Pour la cubique (42) on a m = 9. Pour la cubique

$$(43) x^3 + \varrho y^3 + \varrho^2 z^3 = 0$$

on a m = 9.

Démonstration. Supposons d'abord que  $\mathbf{a}$  ne contient pas  $\sqrt{-3}$ . Si la relation (36) est satisfaite par une seule paire E, E<sub>1</sub>, on aura un seul point rationnel  $P(\alpha, \alpha_1, \alpha_2)$ . Si ce point est exceptionnel, son index a la valeur maximale M. Alors l'index du point tangentiel  $P_1$  de P est aussi égal à M. Or, cela est en contradiction avec le fait que nous n'avons obtenu qu'un seul point dont l'index est maximal. Donc P n'est pas un point exceptionnel. Ainsi chaque point exceptionnel rationnel de la cubique est ou un point d'inflexion ou un point dont le point tangentiel est un point d'inflexion. Il est évident que au plus un seul point rationnel peu appartenir à la dernière catégorie puisque  $\sqrt{-3}$  n'appartient pas à  $\mathbf{a}$ . Un seul point d'inflexion peut être rationnel, sauf dans le cas de la cubique (42) avec trois points d'inflexion rationnels. On voit que la cubique doit être de l'un des types (40), (41) et (42).

Supposons ensuite que  $\mathbf{a}$  contient le nombre  $\sqrt{-3}$ . Alors, aucun des nombres 2 et  $\rho$  ne peut être le cube d'un nombre rationnel dans  $\Omega$ . En effet, considérons le corps  $K(\Theta, \sqrt{-3})$ , où  $\Theta = \sqrt[3]{2}$ , et posons

$$\varepsilon = \Theta - \varrho$$
,  $\varepsilon' = \Theta - \varrho^2$ ,  $\varepsilon'' = \Theta - 1$ .

Les nombres  $\varepsilon$ ,  $\varepsilon'$  et  $\varepsilon''$  sont des unités dans K qui satisfont à la relation

$$\varepsilon + \varrho \varepsilon' + \varrho^2 \varepsilon'' = 0.$$

Donc, la relation (36) sera satisfaite par la paire d'unités dans K

$$E = \frac{\varrho \varepsilon'}{\varepsilon}, \quad E_1 = \frac{\varrho^2 \varepsilon''}{\varepsilon},$$

ce qui est contre l'hypothèse faite dans le Théorème 2,

D'une manière analogue, considérons le corps  $K_1(e^{2\pi i/9}) = K_1(\varepsilon, \sqrt{-3})$ , où  $\varepsilon$  est une racine de l'équation  $\varepsilon^3 - 3\varepsilon + 1 = 0$ . Si on pose  $\varepsilon_1 = -1 - \varepsilon$ , on vérifie aisément que  $\varepsilon_1$  est une racine de l'équation  $\varepsilon_1^3 + 3\varepsilon_1^2 - 1 = 0$ . Ainsi les deux nombres  $\varepsilon$  et  $\varepsilon_1$  sont des unités dans  $K_1$  qui satisfont à la relation (36). Pourtant, cela est contre l'hypothèse faite dans le Théorème 2.

On vérifie aisément que, dans le sous-corps  $K(\sqrt{-3})$ , la relation (36) n'est satisfaite que par la paire e, e2. Alors il vient de (37)

$$\frac{3}{\delta}ax^{3} = \mp \sqrt{-3},$$

$$\frac{3}{\delta}by^{3} = \frac{1}{2}(3\pm\sqrt{-3}),$$

$$\frac{3}{\delta}cz^{3} = \frac{1}{2}(-3\pm\sqrt{-3}).$$

Vu que les nombres ax3, by3 et cz3 sont premiers entre eux deux à deux, il en suit que  $\delta$  est associé avec le nombre  $\sqrt{-3}$ . Donc tous les nombres a, b, c, x, y et z sont des unités. Nous pouvons choisir  $\delta = \pm \sqrt{-3}$ ,  $\alpha = 1$ ,  $b = \frac{1}{2}(-1 \pm \sqrt{-3}), c = \frac{1}{2}(-1 \mp \sqrt{-3})$  et  $x^3 = y^3 = z^3 = 1$ . En prenant le signe supérieur on aura la cubique

$$(43) x^3 + \varrho y^3 + \varrho^2 z^3 = 0.$$

Cette cubique admet les neuf points suivants rationnels en 2:

Elle est équivalente en  $K(\sqrt{-3})$  à la cubique (42), qui admet exactement neuf points rationnels (en effet, ce sont les neuf points d'inflexion) dans  $K(\sqrt{-3})$ ; cp. [9], Theorem 120. Il en résulte que les neuf points indiqués ci-dessus sont les seuls points exceptionnels rationnels dans  $\boldsymbol{\varrho}$  sur la cubique (43). En effet, aucun des points d'inflexion de cette cubique ne peut être rationnel dans le cas en question, vu que le nombre  $\varrho$  n'est pas le cube d'un nombre rationnel.

Sur les autres cubiques chaque point exceptionnel rationnel doit être ou un point d'inflexion ou un point dont le point tangentiel est un point d'inflexion. Donc la cubique doit être de l'une des formes (40), (41) et (42). Dans le premier cas il n'y a aucun point de la dernière catégorie; dans le deuxième cas il y a exactement neuf points de cette catégorie; dans le troisième cas il n'y a aucun point de la dernière catégorie, vu que le nombre 2 n'est pas le cube d'un nombre rationnel (cp. le numéro 6). Le nombre des points d'inflexion rationnels est égal à trois pour les cubiques (40) et (41), et égal à neuf pour la cubique (42).

17. La relation (36) est impossible dans K(1). Si 2 est un corps quadratique, on peut montrer qu'elle est possible seulement dans les deux corps  $K(\sqrt{-3})$  et  $K(\sqrt{5})$ ; ces corps sont simples.

Traitons d'abord le cas d'un corps quadratique imaginaire. L'unité E de la relation (36) doit satisfaire à une équation de la forme

$$E^2 + hE + 1 = 0$$
,

où h est un nombre entier ordinaire. D'après (36) le nombre  $E_1=-1\!-\!E$  est une unité, qui satisfait à l'équation

$$(E_1+1)^2-h(E_1+1)+1=0$$
.

d'où

$$E_1^2 - (h-2)E_1 + 2 - h = 0$$
.

Il faut donc que h = 1, c'est-à-dire

$$E = \frac{1}{2}(-1 \pm \sqrt{-3}).$$

Cependant, le cas du corps  $K(\sqrt{-3})$  est compris dans le Théorème 2. Traitons ensuite le cas d'un corps quadratique réel. L'unité E de la relation (36) doit satisfaire à une équation de la forme

$$E^2+hE\pm 1=0,$$

où h est un nombre entier ordinaire. D'après (36) le nombre  $E_1=-1-E$  est une unité, qui satisfait à l'équation

$$E_1^2 - (h-2)E_1 + 1 - h \pm 1 = 0.$$

On aura donc h=3 ou h=-1, c'est-à-dire

ou 
$$E = \frac{1}{2}(-3\pm\sqrt{5})$$
 ou  $E = \frac{1}{2}(1\pm\sqrt{5})$ .

Dans le premier cas on obtient de (37)

(44) 
$$\frac{3}{\delta} ax^3 = 2 \mp \sqrt{5} ,$$

$$\frac{3}{\delta} by^3 = \frac{1}{2} (1 \pm \sqrt{5}) ,$$

$$\frac{3}{\delta} cz^3 = \frac{1}{2} (-5 \pm \sqrt{5}) .$$

on voit de là que  $\delta$  ne peut pas être une unité. Donc  $\delta$  est associé avec le nombre 3, et tous les nombres  $a, b, c/\sqrt{5}, x, y$  et z sont des unités. Alors nous pouvons prendre  $3/\delta = \frac{1}{2}(\pm 1 - \sqrt{5})$ ,  $c = \sqrt{5}$  et z = 1, ce qui entraîne

$$ax^3 = \frac{1}{2}(\pm 3 - \sqrt{5})$$
 et  $by^3 = \frac{1}{2}(\mp 3 - \sqrt{5})$ .

Nous pouvons choisir

$$a = \frac{1}{2}(\pm 3 - \sqrt{5})$$
 et  $b = \frac{1}{2}(\mp 3 - \sqrt{5})$ .

On aura ainsi x = y = z = 1, et la cubique sera

$$\frac{1}{2}(\pm 3 - \sqrt{5})x^3 + \frac{1}{2}(\mp 3 - \sqrt{5})y^3 + \sqrt{5}z^3 = 0.$$

Si elle admet un point exceptionnel rationnel (dans  $K(\sqrt{5})$ ) l'index a son maximum pour le point P=P(1,1,1). L'index de P est égal à 1. Les coordonnées du point tangentiel  $P_1=P_1(\xi,\eta,\zeta)$  de P sont évidemment

$$\xi = 1, \quad \eta = \frac{1}{2}(-3\pm\sqrt{5}), \quad \zeta = \frac{1}{2}(1\mp\sqrt{5}).$$

L'index de  $P_1$  est aussi égal à 1. Déterminons ensuite le point tangentiel  $P_2=P_2(\xi_1,\,\eta,\,\zeta_1)$  de  $P_1$ . Les coordonnées de ce point sont données par les équations

$$\delta_1 \, \xi_1 = \frac{1}{2} (\pm 17 - 7\sqrt{5}),$$

$$\delta_1 \, \eta_1 = \frac{1}{2} (-83 \pm 37\sqrt{5}),$$

$$\delta_1 \, \xi_1 = \frac{1}{8} (\mp 7 + 3\sqrt{5}).$$

Il en résulte que di est une unité, et on aura

Index
$$(P_2) = |N(\xi_1 \eta_1 \zeta_1)| = 121.$$

On en conclut que ni P2 ni P ne peut être exceptionnel.

Dans le second cas on a  $E = \frac{1}{2}(1 \pm \sqrt{5})$ , et on obtient de (37)

$$rac{3}{\delta}ax^3 = -2\mp\sqrt{5}\,,$$
  $rac{3}{\delta}by^3 = rac{1}{2}(5\pm\sqrt{5}\,)\,,$   $rac{3}{8}cz^3 = rac{1}{2}(-1\pm\sqrt{5}\,).$ 

Cependant, en remplaçant dans ces équations  $\sqrt{5}$  par  $-\sqrt{5}$  et  $3/\delta$  par  $-3/\delta$  et en permutant b et c et y et z, on retombe sur le système (44) que nous venons de traiter.

Il résulte de ce qui précède:

THÉORÈME 3. Soit  $\mathfrak A$  un corps quadratique simple différent de  $K(\sqrt{-3})$ . Désignons par m le nombre des points exceptionnels rationnels sur la cubique (19). Alors on a m=0 sauf dans les cas suivants: Si la cubique a la forme

$$x^3 + y^3 + c x^3 = 0,$$

où ni c ni 4c n'est égal au cube d'un nombre rationnel, on a m=1.

Si la cubique a la forme

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

on a m=2, et pour la cubique

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

on  $\alpha$  m=3.

18. Soit  $\boldsymbol{a}$  un corps cubique à discriminant négatif. Nous supposons qu'il est réel.

Nous allons d'abord établir le résultat suivant.

LEMME 1. Si O est une racine d'une des équations

$$\theta^{3} = 2$$
,  $\theta^{3} + \theta^{2} = 1$ ,  $\theta^{3} + \theta = 1$ ,  $\theta^{3} + \theta^{2} + \theta = 1$ ,

le corps cubique engendré par  $\Theta$  est simple, c'est-à-dire, le nombre h des classes d'idéaux est égal à 1.

Démonstration. Dans le premier cas le discriminant de  $\Theta$  est égal à -108. Vu que  $10 < \sqrt{108} < 11$  on aura à examiner les nombres premiers 2, 3, 5 et 7 pour déterminer le nombre h des classes d'idéaux. On a  $2 = \Theta^3$ ,  $3 = (\Theta-1)(\Theta+1)^3$ ,  $5 = (\Theta^2+1)(-\Theta^2+2\Theta+1)$ , où  $(\Theta), (\Theta+1)$ ,  $(\Theta^2+1)$  et  $(-\Theta^2+2\Theta+1)$  sont des idéaux premiers. L'idéal (7) est un idéal premier. Donc on a h=1.

Dans le deuxième cas le discriminant de  $\theta$  est égal à -23. Il suffit donc d'examiner les nombres premiers 2 et 3. On voit aisément que les idéaux (2) et (3) sont des idéaux premiers. Donc on a h=1.

Dans le troisième cas le discriminant de  $\theta$  est égal à -31. Il suffit donc d'examiner les nombres premiers 2, 3, et 5. On vérifie aisément que les déaux (2) et (5) sont des idéaux premiers. Outre cela on a  $3=(1+\theta)\times (2-\theta+\theta^2)$ . Donc on a h=1.

Dans le quatrième cas le discriminant de  $\theta$  est égal à -44. Il suffit donc d'examiner les nombres premiers 2, 3 et 5. Dans ce cas les idéaux (3) et (5) sont des idéaux premiers, et l'idéal (2) est le cube de l'idéal  $(1-\theta)$ . Donc on a h=1.

Dans a il y a une seule unité fondamentale, et nous la choisissons positive et < 1. Nous avons besoin du lemme suivant:

LEMME 2. Soit  $\eta$  l'unité fondamentale dans  $\mathbf{2}$ ,  $0 < \eta < 1$ . Alors le nombre  $1-\eta$  est une unité sculement quand  $\eta$  est une racine (réelle) de l'une ou de l'autre des équations

(45) 
$$z^3 + z^2 = 1$$
 et  $z^3 + z = 1$ .

La racine de chacune des ces équations est l'unité fondamentale dans le corps qu'elle engendre. Pour la racine  $\Theta$  de la première de ces équations on a  $\frac{1}{2} < \Theta < \frac{4}{5}$ , et pour la racine  $\Theta$  de la seconde équation on a  $\frac{1}{2} < \Theta < \frac{3}{4}$ .

Pour la démonstration je renvoie à mon travail [12]. Considérons maintenant la relation

$$(46) 1 + E + E_1 = 0.$$

Vu que l'une des unités E et  $E_1$  doit être négative, nous pouvons supposer que  $E=-\eta^N$ , où N est un nombre entier ordinaire, positif ou négatif. Alors il résulte de (46) que  $1-\eta$  est une unité. Par conséquent, d'après Lemme 2, la relation (46) est impossible, sauf dans les cas dans lesquels  $\mathbf{g}$  est engendré par une racine de l'une ou de l'autre des équations (45). Supposons ensuite que  $\mathbf{g} = \mathbf{K}(\Theta)$ , où  $\Theta$  est la racine réelle de  $\Theta^3 + \Theta^2 = 1$  ou la racine réelle de  $\Theta^3 + \Theta = 1$ . Posons  $E = -\Theta^N$  et  $E_1 = \pm \Theta^M$ , N et M étant des nombres entiers ordinaires. Il faut distinguer plusieurs cas.

1°  $E_1 = -\theta^M$ ; N > M > 0. D'après Lemme 2 on a  $\theta < \frac{4}{5}$  quand  $\theta^3 + \theta^2 = 1$  et  $\theta < \frac{3}{7}$  quand  $\theta^3 + \theta = 1$ . Il en résulte aisément que

$$\Theta^N + \Theta^M < 1$$
,

sauf dans les cas suivants: N=3, M=2 et N=5, M=1 quand  $\theta^3+\theta^2=1$ ; N=3, M=1 quand  $\theta^3+\theta=1$ .

2°  $E_1 = -\theta^M$ ; N < 0. Ce cas est impossible vu que  $\theta^N \ge \theta^{-1} > 1$ . 3°  $E_1 = \theta^M$ ; N > 0. Ce cas est impossible vu que  $\theta^N \le \theta < 1$ .

 $4^{\circ} E_1 = \Theta^{M}$ ;  $N = -N_1$  et  $M = -M_1$ , où  $M_1$  et  $N_1$  sont positifs. En multipliant la relation (46) par  $\Theta^{N_1}$  nous aurons

$$\Theta^{N_1} - 1 + \Theta^{N_1 - M_1} = 0.$$

Or, nous venons de montrer que cette relation entraîne que  $N_1 > M_1$  (deuxième cas). D'après le premier cas on aura donc: Les deux possibilités  $N_1 = 3$ ,  $N_1 - M_1 = 2$  et  $N_1 = 5$ ,  $N_1 - M_1 = 1$  quand  $\theta^3 + \theta^2 = 1$ ; la possibilité  $N_1 = 3$ ,  $N_1 - M_1 = 1$  quand  $\theta^3 + \theta = 1$ .

Les solutions de (46) dans les deux corps  $K(\Theta)$  sont ainsi données par les relations suivantes:

(47) 
$$1 - \theta^2 - \theta^3 = 0, \qquad 1 - \theta - \theta^5 = 0, \\ 1 - \theta^{-3} + \theta^{-1} = 0, \qquad 1 - \theta^{-5} + \theta^{-4} = 0,$$

et

(47') 
$$1 - \Theta - \Theta^3 = 0, \quad 1 - \Theta^{-3} + \Theta^{-2} = 0.$$

Dans (47) le discriminant est égal à -23, dans (47') il est égal à -31. Soit  $\mathcal{L}$  le corps  $K(\theta)$  où  $\theta^3 + \theta^2 = 1$ . Dans ce cas il y a les possibilités suivantes pour  $E : -\theta^3$ ,  $-\theta^2$ ,  $-\theta^5$ ,  $-\theta$ ,  $-\theta^{-3}$ ,  $\theta^{-1}$ ,  $-\theta^{-5}$  et  $\theta^4$ . D'après ce que nous venons de dire au numéro 15, il suffit d'examiner les quatre cas:  $E = -\theta^2$ ,  $E = -\theta$ ,  $E = \theta^{-1}$  et  $E = -\theta^{-5}$ .

Premier cas. Quand  $E = -\theta^2$ , nous aurons

$$rac{3}{\delta}ax^3=\Theta^7, \quad rac{3}{\delta}by^3=2-\Theta^2, \quad rac{3}{\delta}cz^3=-1-\Theta^2,$$

où  $N(2-\Theta^2) = 7$  et  $N(1+\Theta^2) = 5$ . Il en résulte qu'on peut choisir

$$\frac{3}{\delta}=1, \quad a=\theta^{7}, \quad b=2-\theta^{2}, \quad c=-1-\theta^{2},$$

correspondant au point x = y = z = 1.

Deuxième cas. Quand  $E = \Theta^{-1}$ , nous aurons

$$\frac{3}{\delta}ax^3\cdot\Theta^2=-1-\Theta^2,\quad \frac{3}{\delta}by^3\cdot\Theta^2=2-\Theta^2,\quad \frac{3}{\delta}cz^3\cdot\Theta^2=\Theta^7.$$

On peut donc choisir

$$rac{3}{\delta}=\Theta^{-2},\quad a=-1-\Theta^2,\quad b=2-\Theta^2,\quad c=\Theta^7,$$

correspondant au point x = y = z = 1. Cependant, en permutant x et z et a et c on retombe sur le premier cas.

Troisième cas. Quand  $E=-\theta$ , nous aurons

$$\frac{3}{\delta}ax^3 = -1 + 2\Theta, \quad \frac{3}{\delta}by^3 = 2 - \Theta, \quad \frac{3}{\delta}cz^3 = -\Theta^{-2},$$

où  $N(2\theta-1)=5$  et  $N(2-\theta)=11$ . Il en résulte qu'on peut choisir

$$\frac{3}{\delta}=1,\quad a=-1+2\theta,\quad b=2-\theta,\quad c=-\theta^{-2},$$

correspondant au point x = y = z = 1.

Quatrième cas. Quand  $E = -\Theta^{-5}$ , nous aurons

$$\frac{3}{\delta} a x^{\mathbf{3}} \cdot \boldsymbol{\Theta}^{\mathbf{5}} = \boldsymbol{\Theta}^{-\mathbf{2}}, \quad \frac{3}{\delta} b y^{\mathbf{3}} \cdot \boldsymbol{\Theta}^{\mathbf{5}} = \mathbf{1} - 2\boldsymbol{\Theta}, \quad \frac{3}{\delta} c z^{\mathbf{3}} \cdot \boldsymbol{\Theta}^{\mathbf{5}} = \boldsymbol{\Theta} - 2 \,.$$

On peut donc choisir

$$\frac{3}{\delta} = -\Theta^{-5}, \quad a = -\Theta^{-2}, \quad b = -1 + 2\Theta, \quad c = 2 - \Theta,$$

correspondant au point x = y = z = 1. Cependant, en remplaçant x = y = z, a par c, y par x, b par a, z par y et c par b, on retombe sur le troisième cas.

Il est évident que les deux cubiques que nous avons obtenues dans le premier cas et le troisième cas, sont différentes. D'après la discussion au numéro 15 on conclut que les points P(1,1,1) ne sont pas exceptionnels.

Soit ensuite  $\mathcal{Q}$  le corps  $K(\theta)$  où  $\theta^3 + \theta = 1$ . Dans ce cas il y a les possibilités suivantes pour l'unité  $E: -\theta, -\theta^3, -\theta^{-3}$  et  $\theta^{-2}$ . Il suffit d'examiner les cas  $E = -\theta$  et  $E = -\theta^{-3}$ .

Premier cas. Quand  $E = -\theta$ , nous aurons

$$rac{3}{\delta}ax^3=-1+2\Theta, \quad rac{3}{\delta}by^3=2-\Theta, \quad rac{3}{\delta}cz^3=-1-\Theta,$$

où  $N(-1+2\theta)=3,\ N(2-\theta)=9$  et  $N(1+\theta)=3.$  Il en résulte qu'on peut choisir

$$a = \frac{3}{\delta} = 1 + \Theta, \quad a = \Theta^4, \quad b = 1 - \Theta + \Theta^2, \quad c = -1,$$

correspondant au point x = y = z = 1.

Deuxième cas. Quand  $E=-\Theta^{-3}$ , nous aurons

$$\frac{3}{\delta} ax^3 \cdot \Theta^3 = 1 + \Theta, \quad \frac{3}{\delta} by^3 \cdot \Theta^3 = 1 - 2\Theta, \quad \frac{3}{\delta} cz^3 \cdot \Theta^3 = -2 + \Theta.$$

On peut donc choisir

$$\frac{3}{3} = -\Theta^{-2} - \Theta^{-3}, \quad a = -1, \quad b = \Theta^{4}, \quad c = 1 - \Theta + \Theta^{2},$$

correspondant au point x=y=z=1. Cependant, en remplaçant x par z, a par c, y par x, b par a, z par y et c par b, on retombe sur le premier cas.

D'après la discussion au numéro 15 on conclut que le point P(1,1,1) n'est pas exceptionnel. Ainsi nous avons établi le résultat suivant:

THÉORÈME 4. Soit  $\mathfrak Q$  un corps cubique simple à discriminant négatif. Désignons par m le nombre des points exceptionnels rationnels sur la cubique (19). Alors on a m=0, sauf dans les cas suivants: Si la cubique a la forme

$$(48) x^3 + y^3 + cz^3 = 0,$$

où ni c ni 4c n'est égal au cube d'un nombre rationnel, on a m=1. Si la cubique a la forme

$$(49) x^3 + y^3 + 2z^3 = 0.$$

et si le nombre 2 n'est pas égal au cube d'un nombre rationnel, on a m=2. Si la cubique a la forme

$$(50) x^3 + y^3 + z^3 = 0,$$



on a m=6 ou m=3, selon que le nombre 2 est égal au cube d'un nombre rationnel ou non.

En effet, il résulte de ce qui précède que chaque point exceptionnel rationnel de la cubique est ou un point d'inflexion ou un point dont le point tangentiel est un point d'inflexion. Par conséquent, le seul point exceptionnel rationnel de la cubique (48) est P(1, -1, 0); les points exceptionnels rationnels de la cubique (49) sont P(1, -1, 0) et P(1, 1, 1); ceux de la cubique (50) sont P(1, -1, 0), P(1, 0, -1), P(0, 1, -1) et si  $2 = a^3$ ,  $\alpha$  rationnel, il faut y ajouter les points P(1, 1, -a), P(1, -a, 1) et P(-a, 1, 1).

D'après le Lemme 1 les corps engendrés par les racines de chacune des équations  $\theta^3 = 2$ ,  $\theta^3 + \theta^2 = 1$  et  $\theta^3 + \theta = 1$ , sont simples.

19. Dans un travail qui suivra bientôt, nous allons continuer nos recherches sur les points exceptionnels rationnels de la cubique

$$ax^3 + by^3 + cz^3 = 0.$$

Nous allons traiter les cas suivants:  $\mathcal{Q}$  est un corps cubique simple à discriminant positif.  $\mathcal{Q}$  est un corps biquadratique simple, tel que tous les corps conjugés soient imaginaires.  $\mathcal{Q}$  est un corps algébrique dans lequel le nombre h des classes d'idéaux est égal à 3. Nous allons aussi établir quelques résultats dans le cas que le nombre h est quelconque.

On doit à Hurwitz un résultat relatif au nombre des points rationnels sur la cubique

(52) 
$$ax^3 + by^3 + cz^3 + dxyz = 0,$$

où a, b, c et d sont des nombres entiers (dans K(1)), tels que abc ne soit divisible par aucun carré > 1; voir [10]. Vu que le nombre des points exceptionnels est limité, son résultat peut être énoncé de la manière suivante:

1° Si tous les nombres |ab|, |ac| et |bc| sont > 1, la cubique (52) n'admet aucun point exceptionnel rationnel.

2° Si a=b=1 et c>1 la cubique admet un seul point exceptionnel rationnel, sauf dans les cas de  $d=-c\pm 2$  et  $d=-4c\pm 1$ , où elle admet exactement deux points exceptionnels rationnels.

3º Si a=b=c=1, la cubique admet exactement trois points exceptionnels rationnels, sauf peut-être dans les cas de d=1 et d=-5.

Ce résultat a été complété par Mordell qui a montré que chacune des cubiques

$$x^{3} + y^{3} + z^{3} + xyz = 0$$
$$x^{3} + y^{3} + z^{3} - 5xyz = 0$$

admet exactement six points rationnels dans K(1) (voir [13]). Ces six points sont forcément exceptionnels.

Plusieurs des résultats obtenus dans ce Mémoire sur la cubique (51) peuvent être considérés comme des généralisations du théorème de Hurwitz.

Si nous appliquons le Théorème III du numéro 4 à la première partie du théorème de Hurwitz nous aurons:

THÉORÈME 5. Si tous les nombres |ab|, |ac| et |bc| sont > 1, la cubique (52) n'admet aucun point exceptionnel dans un corps algébrique, dont le degré n'est pas divisible par 3.

Dans un travail qui va suivre, nous allons établir d'autres résultats sur la cubique (52) dans un corps algébrique.

#### Travaux cités

[1] T. Nagell, Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, Skrifter utg. av det Norske Videnskaps-Akademi i Oslo, 1935, Mat.-Naturv. Kl. No. 1.

[2] - Sur la division des périodes de la fonction Q (x) et les points exceptionnels des cubiques, Nova Acta Regiae Soc. Sci. Ups., Ser. IV, Vol. 15, No. 8, Uppsala 1953.

[3] — Les points exceptionnels sur les cubiques planes du premier genre, I et II, Nova Acta Regiae Soc. Soi. Ups., Ser. IV, Vol. 14, Nos. 1 et 3, Uppsala 1946 et 1947.

[4] — Sur la classification des cubiques planes du premier genre par des transformations birationnelles dans un domaine de rationalité quelconque, Nova Acta Regiae Soc. Sci. Ups., Scr. IV, Vol. 12, No 8, Uppsala 1941.

[5] — Über die gleichzeitige Lösbarkeit gewisser diophantischer Gleichungen dritten Grades, Det Kongel. Norske Vidensk. Selskab. Forh. Bd XI, Nr. 29, Trondhjem 1938.

[6] Gösta Bergman, On the exceptional group of a Weierstrass curve in an algebraic field, Acta Mathematica, t. 91, Uppsala 1954.

[7] T. Nagell, Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque, Nova Acta Regiae Soc. Sci. Ups., Ser. IV, Vol. 15, No. 6, Uppsala 1952.

[8] — Sur la résolubilité des équations diophantiennes cubiques à deux inconnues dans un domaine relativement algébrique, Nova Acta Regiae Soc. Sci. Ups., Ser. IV, Vol. 13, No. 3, Uppsala 1942.

[9] - Introduction to number theory, New York 1951.

[10] A. Hurwitz, Über ternäre diophantische Gleichungen dritten Grades, Vierteljahrsschrift d. Naturf. Gesellsch. in Zürich, Jahrg. 62, 1917.

[11] E. Selmer, The Diophantine Equation  $ax^3 + by^2 + cz^2 = 0$ , Acta Mathematica, t. 85, Uppsala 1951.

[12] T. Nagell, Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, Mathematische Zeitschrift, Bd. 28, Berlin 1928.

[13] L. J. Mordell, The Diophantine Equation  $x^2 + y^2 + z^3 + kxyz = 0$ , Colloque sur la Théorie des Nombres à Bruxelles 1955, Liège 1956.

Reçu par la Rédaction le 10. 3. 1959