JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

H. POINCARÉ

Sur les propriétés arithmétiques des courbes algébriques

Journal de mathématiques pures et appliquées 5^e série, tome 7 (1901), p. 161-233.
<http://www.numdam.org/item?id=JMPA_1901_5_7__161_0>

Sur les propriétés arithmétiques des courbes algébriques;

PAR M. H. POINCARÉ.

I. — Introduction.

Les propriétés arithmétiques de certaines expressions et, en particulier, celles des formes quadratiques binaires, se rattachent de la façon la plus étroite à la transformation de ces formes par des substitutions linéaires à coefficients entiers. Je n'ai pas à insister ici sur le parti qui a été tiré de l'étude de ces substitutions et qui est assez connu de tous ceux qui s'intéressent à l'Arithmétique.

On peut supposer que l'étude de groupes de transformations analogues est appelée à rendre de grands services à l'Arithmétique. C'est ce qui m'engage à publier les considérations suivantes, bien qu'elles constituent plutôt un programme d'étude qu'une véritable théorie.

Je me suis demandé si beaucoup de problèmes d'Analyse indéterminée ne pourraient pas être rattachés les uns aux autres par un lien systématique, grâce à une classification nouvelle des polynomes homogènes d'ordre supérieur de trois variables, analogue à certains égards à la classification des formes quadratiques.

Cette classification aurait pour base le groupe des transformations birationnelles *à coefficients rationnels* que peut subir une courbe algébrique.

II. — Courbes unicursales.

Soit $f(x, y, z)$ un polynome homogène en x, y, z, à coefficients entiers. On pourra regarder l'équation

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

comme représentant une courbe algébrique plane en coordonnées homogènes. Deux courbes $f = 0$ et $f_1 = 0$ seront alors regardées 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 entiers ou rationnels*.

J'observe d'abord que deux droites

$$ax + by + cz = 0, \qquad a_1 x + b_1 y + c_1 z = 0$$

(où les coefficients des premiers membres sont, bien entendu, entiers ou rationnels) sont toujours équivalentes. Il suffit, en effet, de faire correspondre au point M de la première droite le point M_1 de la seconde droite, de telle façon que la droite MM_1 aille passer par un point donné fixe F *à coordonnées rationnelles*. Il n'y a donc qu'une seule classe de droites.

Considérons maintenant les coniques.

Soit donc $f = 0$ l'équation d'une conique. Si cette conique passe par un point C à coordonnées rationnelles (c'est ce que j'appellerai pour abréger un *point rationnel*), elle est équivalente à une droite. Il suffit, en effet, de considérer une droite quelconque D à coefficients rationnels (ce que j'appellerai une *droite rationnelle*) et de faire correspondre à un point M de la conique, un point M_1 de la droite D tel que les trois points MM_1C soient en ligne droite.

Il résulte immédiatement de là que, si une conique admet un point rationnel, elle en admet une infinité. On peut le voir aussi comme il suit. Soit C un point rationnel de la conique, soit P un point rationnel *quelconque* du plan. Joignons PC, cette droite coupera la conique en un second point M qui sera évidemment rationnel.

Les coniques qui admettent un point rationnel forment donc une seule classe, et cette classe comprend également toutes les droites. Reconnaître si une conique admet un point rationnel, c'est un problème que Gauss nous a enseigné à résoudre, dans son Chapitre des *Disquisitiones*, intitulé *Representatio ciffræ*.

Les coniques qui n'ont pas de point rationnel se répartissent en plusieurs classes et les conditions de cette répartition se déduisent immédiatement des principes de ce même Chapitre de Gauss.

Considérons maintenant une cubique unicursale (à coefficients rationnels), cette cubique a un point double qui, étant unique, est forcément rationnel. Soit C ce point double, je dis que notre cubique est équivalente à une droite. En effet, soit D une droite rationnelle quelconque, nous pouvons faire correspondre au point M de la cubique un point M_1 de la droite D, de telle façon que la droite MM_1 passe en C.

Les mêmes principes sont applicables à une courbe unicursale quelconque. Soit $f = 0$ une courbe unicursale rationnelle de degré m; elle aura $\frac{(m-1)(m-2)}{2}$ points doubles. Par ces

$$\frac{(m-1)(m-2)}{2}$$

points doubles, je puis faire passer ∞^{m-2} courbes de degré $m-2$. Comme nos $\frac{(m-1)(m-2)}{2}$ points doubles sont les seuls points doubles d'une courbe à coefficients rationnels, toute fonction symétrique de leurs coordonnées sera rationnelle.

D'où il suit que je pourrai 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 une seule, et que *cette courbe sera rationnelle* (je veux dire à coefficients rationnels).

L'équation générale des courbes de degré $m-2$ passant par les points doubles sera donc de la forme suivante

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \ldots + \alpha_{m-1} \varphi_{m-1} = 0,$$

les α étant des coefficients arbitraires et les φ étant des polynomes en-

tiers homogènes d'ordre $m-2$ en x, y, z, à coefficients rationnels.

Posons

$$(1) \qquad \frac{\xi_1}{\varphi_1} = \frac{\xi_2}{\varphi_2} = \ldots = \frac{\xi_{m-1}}{\varphi_{m-1}}.$$

Si nous regardons les ξ comme les coordonnées homogènes d'un point dans l'espace à $m-2$ dimensions, les équations (1) définissent une transformation qui change la courbe unicursale plane $f=0$ en une certaine courbe de cet espace à $m-2$ dimensions; cette courbe, je l'appelle K.

J'observe d'abord que cette courbe est de degré $m-2$. En effet, soit

$$\alpha_1\xi_1 + \alpha_2\xi_2 + \ldots + \alpha_{m-1}\xi_{m-1} = 0$$

l'équation d'un plan quelconque de l'espace à $m-2$ dimensions; pour avoir les points d'intersection de ce plan avec K, je n'ai qu'à chercher ceux de $f=0$ avec la courbe

$$\alpha_1\varphi_1 + \alpha_2\varphi_2 + \ldots + \alpha_{m-1}\varphi_{m-1} = 0.$$

Cette courbe étant de degré $m-2$, le nombre total des points d'intersection est $m(m-2)$, dont $(m-1)(m-2)$ sont confondus avec les points doubles et dont $m-2$ seulement sont mobiles.

Le nombre des points d'intersection du plan et de K est donc $m-2$.

C. Q. F. D.

Je remarque ensuite que la transformation (1) est birationnelle; en effet, d'abord l'on a directement les rapports des ξ en fonctions rationnelles de x, y, z à coefficients rationnels. Je cherche maintenant à exprimer inversement les rapports des trois coordonnées x, y, z en fonctions des ξ.

Pour avoir $\frac{x}{z}$ par exemple, je prends deux quelconques des équations (1), par exemple,

$$\frac{\xi_1}{\varphi_1} = \frac{\xi_2}{\varphi_2} = \frac{\xi_3}{\varphi_3},$$

et entre l'équation $f = 0$ et ces deux équations j'élimine $\frac{y}{z}$; il restera deux équations

$$F = 0, \qquad F_1 = 0, \tag{2}$$

dont les premiers membres seront homogènes en x, z d'une part, en ξ_1, ξ_2, ξ_3 d'autre part. Entre ces deux équations, éliminons maintenant $\frac{x}{z}$ par la méthode du plus grand commun diviseur. Nos divisions successives nous conduiront à une série d'équations :

$$F_2 = 0, \qquad F_3 = 0, \qquad \ldots, \qquad F_p = 0,$$

dont les premiers membres seront des polynomes homogènes en x, z d'une part, en ξ_1, ξ_2, ξ_3 d'autre part, et *à coefficients rationnels*. Mais dans cette série, le degré des polynomes successifs en x et z ira en décroissant. La dernière équation $F_p = 0$ ne contiendra plus x et z; elle exprimera la condition pour que les deux équations (2) aient une racine commune.

C'est donc l'équation de la projection de la courbe K sur le plan à 2 dimensions

$$\xi_4 = \xi_5 = \ldots = \xi_{m-1} = 0.$$

L'équation précédente $F_{p-1} = 0$ est homogène du premier degré en x et en z. On en tirera donc le rapport $\frac{x}{z}$ en fonction rationnelle de ξ_1, ξ_2, ξ_3 à coefficients rationnels, à moins que $F_{p-1} = 0$ ne se réduise à une identité, soit par elle-même, soit en vertu de $F_p = 0$. Mais si cette dernière circonstance se présentait, cela voudrait dire que les équations

$$f = 0, \qquad \frac{\xi_1}{\gamma_1} = \frac{\xi_2}{\gamma_2} = \frac{\xi_3}{\gamma_3}$$

ont deux solutions communes toutes les fois qu'elles en ont une. Or la théorie *algébrique* des courbes unicursales, sur laquelle je n'ai pas à revenir, nous apprend qu'il n'en est pas ainsi. Nous n'avons donc pas à nous occuper de cette exception qui ne se présentera pas.

La conclusion est que la transformation (1) est une transformation birationnelle à coefficients rationnels (je dirai pour abréger une *transformation purement rationnelle*) et même qu'il en est de même de la transformation

$$\frac{\xi_1}{\varphi_1} = \frac{\xi_2}{\varphi_2} = \frac{\xi_3}{\varphi_3},$$

qui transforme la courbe plane $f = 0$ en la courbe plane $F_p = 0$.

La courbe unicursale plane $F_p = 0$, étant la projection de K, est de degré $m - 2$, d'où cette conséquence :

Une courbe unicursale rationnelle est toujours équivalente à une autre courbe unicursale dont le degré est de deux unités plus petit.

De proche en proche, on arrive au résultat suivant :

Une courbe unicursale rationnelle est toujours équivalente à une droite ou à une conique.

Sur une droite ou sur une conique rationnelles, il y a une infinité de couples de points, tels que toutes fonctions symétriques de leurs coordonnées soient rationnelles (c'est ce que j'appellerai des *couples rationnels*); ces couples rationnels s'obtiennent sur une conique en coupant cette conique par une droite rationnelle quelconque.

Donc, *sur une courbe unicursale rationnelle quelconque, il y a toujours une infinité de couples rationnels.*

Sur une droite rationnelle, il y a toujours une infinité de points rationnels.

Donc, *sur une courbe unicursale rationnelle quelconque de degré impair, il y a une infinité de points rationnels.*

Ces résultats peuvent encore s'obtenir d'une autre manière.

J'appellerai *groupe rationnel* un groupe de points tels que toute fonction symétrique de leurs coordonnées soit rationnelle.

Je dis d'abord que, sur la courbe $f = 0$, il y a une infinité de groupes rationnels de $m - 2$ points. On les obtient de la façon suivante :

Considérons la courbe de degré $m - 2$

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \ldots + \alpha_{m-1} \varphi_{m-1} = 0,$$

et donnons aux coefficients arbitraires α des valeurs rationnelles.

Cette courbe coupera $f = 0$ en $m - 2$ points, outre les points doubles, et ces $m - 2$ points formeront évidemment un groupe rationnel.

Je dis maintenant qu'il y a une infinité de couples rationnels.

En effet, par les points doubles, je puis faire passer $\infty^{2(m-1)}$ courbes de degré $m - 1$. Prenons ensuite deux groupes rationnels de $m - 2$ points; par les points doubles et par ces deux groupes, je pourrai faire passer ∞^2 courbes de degré $m - 1$ dont l'équation générale pourra s'écrire

$$\alpha_1 \psi_1 + \alpha_2 \psi_2 + \alpha_3 \psi_3 = 0, \tag{3}$$

où les α sont des coefficients arbitraires et les ψ des polynomes homogènes de degré $m - 1$ en x, y, z, *à coefficients rationnels*.

Donnons aux arbitraires α des valeurs rationnelles quelconques; la courbe (3) coupera la courbe $f = 0$:

1° Aux points doubles, ce qui compte pour $(m - 1)(m - 2)$ intersections;

2° Aux points des deux groupes rationnels, ce qui fait $2(m - 2)$ intersections;

3° En deux autres points mobiles.

Ces deux points mobiles formeront évidemment un couple rationnel.

C. Q. F. D.

Considérons la transformation

$$\frac{\xi_1}{\psi_1} = \frac{\xi_2}{\psi_2} = \frac{\xi_3}{\psi_3},$$

on verrait, comme pour la transformation (1), qu'elle est purement rationnelle; et elle transforme $f = 0$ en une conique, puisque les courbes (3) coupent $f = 0$ en deux points mobiles.

Toute courbe unicursale est donc équivalente à une conique.

Supposons enfin m impair, je dis qu'il y aura une infinité de points rationnels.

Considérons, en effet, $\frac{m-3}{2}$ couples rationnels quelconques, par ces couples et par les points doubles je puis faire passer un faisceau

de courbes de degré $m-2$ ayant pour équation générale

$$\alpha_1 0_1 + \alpha_2 0_2 = 0, \tag{4}$$

les α étant arbitraires et les 0 ayant leurs coefficients rationnels.

Donnons aux α des valeurs rationnelles quelconques. La courbe (4) coupera $f=0$, non seulement aux points doubles et aux $m-3$ points de nos couples rationnels, mais encore en un autre point qui, étant unique, devra être rationnel. C. Q. F. D.

III. — Points rationnels des cubiques.

On voit avec quelle facilité se traite le cas des courbes unicursales. Passons maintenant aux courbes de genre 1 et d'abord aux plus simples d'entre elles, je veux dire aux cubiques.

Étudions d'abord la distribution des points rationnels sur ces courbes.

J'observe que la connaissance de deux points rationnels sur une cubique rationnelle suffit pour en faire connaître un troisième. En effet, la droite qui joint deux points rationnels donnés va couper la cubique en un troisième point qui, étant unique, sera encore rationnel.

De même, si nous connaissons un point rationnel, nous pouvons en déduire un second. Pour cela, considérons la tangente à la cubique en un point rationnel. Ce sera une droite rationnelle, et elle coupera la cubique en un autre point qui sera rationnel.

Voyons quels sont les points rationnels que l'on peut déduire ainsi de la connaissance de un, deux, trois, etc., points rationnels donnés.

A chaque point d'une courbe de genre 1 est attaché un *argument elliptique* et de telle façon que, sur une cubique, la somme des arguments elliptiques de trois points en ligne droite soit constante à une période près. Nous définirons l'argument de telle façon que cette constante soit nulle. Nous devons remarquer que l'argument n'est défini de la sorte qu'à $\frac{1}{3}$ de période près. Car, si l'on ajoute à tous les arguments $\frac{1}{3}$ de période la somme des arguments de trois points en ligne droite ne cessera pas d'être égale à une période.

Cela posé, soit M_0 un point rationnel dont l'argument elliptique soit α.

La tangente en M_0 ira couper la cubique en un point rationnel M_{-1} dont l'argument elliptique sera -2α. La tangente en M_{-1} ira couper la cubique en un point rationnel M_1 dont l'argument elliptique sera 4α.

La droite M_1M_0 ira couper la cubique en un point rationnel M_{-2}, dont l'argument sera -5α; la droite $M_{-2}M_{-1}$ ira couper la cubique en un point rationnel M_2 d'argument 7α.

La droite M_2M_0 coupera la cubique en un point M_{-3} d'argument -8α et la droite $M_{-3}M_{-1}$ la coupera en un point M_3 d'argument 10α.

La loi est manifeste et il existera sur la cubique une série de points rationnels M_n (n étant un indice entier variant de $-\infty$ à $+\infty$) et l'argument elliptique de M_n est $(3n+1)\alpha$.

Ces points sont tous distincts, à moins que α ne soit commensurable avec une période.

La droite qui joint deux de ces points M_n et M_p passe par un troisième point rationnel dont l'argument elliptique est

$$[3(-n-p-1)+1]\alpha,$$

et qui fait, par conséquent, encore partie de la série des points M_n.

Soient maintenant M_0 et N_0 deux points rationnels d'arguments α et β; les points M_n et N_p d'arguments

$$(3n+1)\alpha \quad \text{et} \quad (3p+1)\beta$$

seront encore rationnels; le troisième point d'intersection de la cubique avec la droite M_nN_p aura pour argument

$$-(3n+1)\alpha-(3p+1)\beta$$

et sera rationnel. Les deux points

$$\beta \quad \text{et} \quad -(3n+1)\alpha-(3p+1)\beta$$

étant rationnels, il en sera de même de

$$(3n+1)\alpha+3p\beta.$$

Et, de même, le point

$$3n\alpha + (3p+1)\beta$$

devra être rationnel.

En résumé, seront rationnels tous les points d'argument

$$a\alpha + b\beta,$$

où a et b sont des entiers satisfaisant à l'un des trois systèmes de congruences :

$$\left.\begin{array}{ll} a \equiv 1, & b \equiv 0 \\ a \equiv 0, & b \equiv 1 \\ a \equiv -1, & b \equiv -1 \end{array}\right\} \pmod 3;$$

en d'autres termes, tous les points d'argument

$$\alpha + 3n\alpha + p(\beta - \alpha),$$

n et p étant des entiers.

Observons que si l'on joint deux de ces points, la droite rationnelle ainsi obtenue coupera la cubique en un troisième point dont l'argument sera encore de même forme.

Cela montre que *tous* les points rationnels que l'on peut déduire de M_0 et N_0 sont compris dans cette même formule.

Plus généralement, si les points d'arguments elliptiques

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

sont rationnels, il en sera de même de tous les points dont les arguments elliptiques sont compris dans la formule

$$(1) \qquad \alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha)$$

où n et les p sont entiers.

Tous les points compris dans la formule (1) sont-ils distincts? Ils le seront à moins qu'il n'y ait, entre les arguments

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

et une période, une relation linéaire à coefficients entiers.

On peut se proposer de choisir les arguments

$$(2) \qquad \alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q,$$

de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q+1$ points rationnels qui ont les arguments (2) formeront alors ce que nous appellerons un *système de points rationnels fondamentaux*.

Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux. On devra tout d'abord dans ce choix s'arranger de telle façon que le nombre $q+1$ des points fondamentaux soit aussi petit que possible. Cette valeur minima de ce nombre $q+1$ sera ce que j'appellerai le *rang* de la cubique; c'est évidemment un élément très important de la classification des cubiques rationnelles.

Il y en a d'autres.

On sait que les cubiques réelles se partagent en deux catégories : les unes ont une seule branche où tous les arguments elliptiques sont réels; les autres ont deux branches; tous les points de la première branche (branche impaire) ont leurs arguments réels, tous ceux de la seconde branche (branche paire) ont leurs arguments égaux à une quantité réelle augmentée d'une demi-période imaginaire que j'appellerai $\frac{\omega'}{2}$.

Dans le premier cas, tous les points rationnels ont leur argument réel, de sorte que les quantités $\alpha, \alpha_1, \ldots, \alpha_q$ sont toutes réelles.

Dans le second cas, il peut encore arriver que toutes ces quantités soient réelles et il arrive alors que tous les points rationnels sont sur la branche impaire et qu'il n'y en a pas sur la branche paire.

Mais il peut arriver également que l'une des quantités α soit égale à une quantité réelle augmentée de $\frac{\omega'}{2}$, de sorte que l'un des points rationnels fondamentaux soit sur la branche paire. Nous pouvons toujours supposer qu'il n'y en a qu'un. Si, en effet, nous avions sur cette branche paire deux points fondamentaux d'arguments β et γ, nous pourrions les remplacer par les points dont les arguments sont β et

$-\beta-\gamma$ et le second de ces nouveaux points fondamentaux serait sur la branche impaire.

Supposons donc $\alpha, \alpha_1, \ldots, \alpha_{q-1}$ réels et soit

$$\alpha_q = \beta + \frac{\omega'}{2},$$

β étant réel; alors les points rationnels de la branche impaire seront donnés par la formule

$$\alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_{q-1}(\alpha_{q-1} - \alpha) + 2p_q(\beta - \alpha).$$

A chacun des points rationnels de la branche impaire en correspondra un sur la branche paire et la différence des arguments de deux points correspondants sera $\beta - \alpha + \frac{\omega'}{2}$.

A ce point de vue, nous devons considérer trois catégories de cubiques rationnelles (outre celles de rang zéro qui n'ont pas de point rationnel) : 1° celles qui n'ont qu'une seule branche; 2° celles qui ont deux branches, mais n'ont de points rationnels que sur la branche impaire; 3° celles qui ont deux branches et des points rationnels sur les deux branches.

Nous devons encore faire une autre distinction; il peut se faire que, parmi les quantités

$$2n\alpha + p_1(\alpha_1 - \alpha) + \ldots + p_q(\alpha_q - \alpha) \qquad (3)$$

(qui représentent les différentes valeurs que peuvent prendre les différences des arguments des points rationnels), il y en ait qui soient des parties aliquotes d'une période réelle. Considérons toutes celles des quantités (3) qui sont ainsi commensurables avec la période réelle, période que j'appellerai ω; leur plus grand commun diviseur fera encore partie des quantités (3) et comme toutes ces quantités ne sont définies qu'à un multiple près de ω, le plus grand commun diviseur de ω et de celles des quantités (3) qui sont commensurables avec ω pourra encore être regardé comme faisant partie de ces quantités (3).

Soit $\frac{\omega}{m}$ ce plus grand commun diviseur; tous les multiples de $\frac{\omega}{m}$ feront partie des quantités (3) et ce seront les seules quantités (3) qui soient commensurables avec ω.

Nous pourrons supposer alors soit $\alpha = \frac{\omega}{3m}$, soit $\alpha_1 = \alpha + \frac{\omega}{m}$.

La connaissance du nombre m, s'il existe des quantités (3) commensurables avec ω, est évidemment aussi un des éléments les plus importants de la classification des cubiques rationnelles.

Il arrivera quelquefois que le seul point rationnel fondamental sera $\frac{\omega}{3m}$; plus généralement, il pourra se faire que les points rationnels soient tous donnés par l'une des formules :

$$\frac{K\omega}{m}, \quad \frac{K\omega}{m} + \frac{\omega}{3m}, \quad \frac{K\omega}{m} + \frac{2\omega}{3m}; \tag{4}$$

ou bien que les points rationnels de la branche impaire étant donnés par l'une des formules (4), ceux de la branche paire s'en déduisent en ajoutant aux arguments elliptiques soit $\frac{\omega'}{2}$, soit $\frac{\omega}{2m} + \frac{\omega'}{2}$.

Dans ces divers cas il n'y aura qu'un nombre fini de points rationnels; dans tous les autres cas il y en aura une infinité; j'ajouterai qu'il y en aura une infinité sur tout arc de la cubique si celle-ci n'a qu'une branche, sur tout arc de sa branche impaire si elle a deux branches, et enfin sur tout arc de l'une quelconque des deux branches s'il y a deux branches et qu'il y ait des points rationnels sur chaque branche.

Ainsi se pose naturellement le problème suivant :

Quelles valeurs peut-on attribuer au nombre entier que nous avons appelé le rang *d'une cubique rationnelle? Quelles sont, parmi les catégories que nous venons d'énumérer et qui sont jusqu'ici logiquement possibles, celles qui existent réellement?*

IV. — Autres courbes de genre 1.

Les principes précédents sont applicables à des courbes quelconques de genre 1.

Considérons, par exemple, une quartique gauche. Chaque point de cette courbe possède un argument elliptique; et la somme des arguments des quatre intersections de la courbe et d'un plan est nulle.

Si donc les points α, β, γ sont rationnels, il en est de même du point

$$-\alpha-\beta-\gamma.$$

Si le point α est rationnel, il en est donc de même du point -3α, puis des points

$$\begin{aligned} 5\alpha &= -|\alpha+2(-3\alpha)|,\\ -7\alpha &= -|5\alpha+\alpha+\alpha|,\\ 9\alpha &= -|(-7\alpha)+\alpha+(-3\alpha)|,\\ -11\alpha &= -|9\alpha+\alpha+\alpha|, \end{aligned}$$

et, en général, de tous les points $(4n+1)\alpha$.

Si γ, β et α sont rationnels, il en sera de même de

$$-\alpha-\beta-\gamma$$

et de

$$-(2\alpha+\gamma)$$

et, par conséquent, de

$$\gamma+\beta-\alpha=-|2\alpha+(-\alpha-\beta-\gamma)|.$$

Si donc

$$\alpha,\quad \alpha_1,\quad \alpha_2,\quad \ldots,\quad \alpha_q$$

sont rationnels, il en sera de même de

$$(1)\quad (4n+1)\alpha+p_1(\alpha_1-\alpha)+p_2(\alpha_2-\alpha)+\ldots+p_q(\alpha_q-\alpha),$$

quels que soient les entiers $n, p_1, p_2, \ldots, p_q$.

C'est là une formule analogue à la formule (1) du paragraphe précédent et qui se discuterait de la même manière.

Considérons plus généralement une courbe de genre 1 et de degré m dans l'espace à $m-1$ dimensions. Un *plan* coupera cette courbe en m points et la somme de leurs arguments elliptiques sera nulle.

Le même raisonnement pourra donc s'appliquer.

Si $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_q$ sont rationnels, il en sera de même de

$$-(\alpha_1 + \alpha_2 + \ldots + \alpha_{m-1})$$

et des divers points

$$-(m-1)\alpha, \quad -\alpha_2-(m-2)\alpha, \quad -\alpha_2-\alpha_1-(m-3)\alpha,$$
$$-\alpha_2+(\alpha_1-\alpha) = -\{-(m-2)\alpha-[-\alpha_2-\alpha_1-(m-3)\alpha]\},$$

et plus généralement de

$$(nm+1)\alpha + p_1(\alpha_1-\alpha) + p_2(\alpha_2-\alpha) + \ldots + p_q(\alpha_q-\alpha),$$

formule analogue à la formule (1).

On arriverait aisément aux mêmes résultats en raisonnant directement sur les courbes planes. Soit C une courbe plane de degré m et de genre 1; elle aura

$$\frac{(m-1)(m-2)}{2} - 1$$

points doubles. Par ces points doubles je peux faire passer ∞^{m-1} courbes d'ordre $m-2$ qui couperont la courbe en m points mobiles; j'appelle ces courbes K. Si nous avons $m-1$ points rationnels d'arguments elliptiques

$$\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_{m-1},$$

par ces points je pourrai faire passer une courbe K, cette courbe coupera C en un $m^{\text{ième}}$ point qui aura pour argument

$$-(\alpha_1 + \alpha_2 + \ldots + \alpha_{m-1})$$

et qui sera évidemment rationnel.

Le reste du raisonnement se poursuit comme plus haut.

Cherchons maintenant dans quels cas une quartique ou une courbe de degré plus grand peut être équivalente à une cubique.

Soit d'abord une quartique plane rationnelle quelconque de genre 1. Supposons qu'elle possède un point rationnel P. Par ce point P et par les deux points doubles, je puis faire passer ∞^2 coniques, qui couperont la quartique en trois points mobiles. L'équation générale de ces coniques pourrait s'écrire

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \alpha_3 \varphi_3 = 0,$$

les α étant des arbitraires et les φ des polynomes du second degré à coefficients rationnels.

Considérons alors la transformation

$$\frac{\xi_1}{\varphi_1} = \frac{\xi_2}{\varphi_2} = \frac{\xi_3}{\varphi_3},$$

où les ξ sont considérés comme les coordonnées homogènes d'un point dans un plan. Elle transforme notre quartique en une cubique, et l'on verrait, comme pour la transformation (1) du § II, que c'est une transformation purement rationnelle.

La quartique est donc équivalente à une cubique.

Réciproquement, considérons une quartique et supposons qu'elle soit équivalente à une cubique, je dis qu'elle admettra un point rationnel.

En effet, soit u l'argument elliptique d'un point de la quartique; l'argument elliptique du point correspondant de la cubique sera $u + k$, k étant une constante. Si trois points de la cubique sont sur une droite rationnelle, les trois points correspondants de la quartique, qui auront pour arguments elliptiques α, β, γ, formeront un groupe rationnel, et l'on aura

$$\alpha + \beta + \gamma = -3k.$$

Par ces trois points et les deux points doubles je puis faire passer une conique qui sera rationnelle et qui coupera la quartique en un

autre point qui, étant unique, devra être rationnel. Ce point rationnel aura pour argument $-\alpha-\beta-\gamma$, c'est-à-dire $3k$.

La cubique devra avoir aussi un point rationnel. En effet, par les points doubles de la quartique je fais passer une conique rationnelle qui coupe la quartique en quatre points simples. Les quatre points correspondants sur la cubique formeront un groupe rationnel. Par les quatre points de ce groupe je puis faire passer une infinité de coniques rationnelles, qui couperont la cubique en deux autres points. Ces deux points formeront un couple rationnel. En joignant les deux points d'un de ces couples rationnels on obtiendra une droite rationnelle qui coupera la cubique en un troisième point qui sera rationnel.

C. Q. F. D.

Réciproquement, si une cubique a un point rationnel P, elle est équivalente à une quartique. En effet, je considère dans l'espace un point rationnel quelconque S; et je considère ce point comme le sommet d'un cône C du troisième degré ayant pour directrice la cubique. Par le point P je puis faire passer une droite rationnelle quelconque qui coupe la cubique en deux points M et M_1 formant un couple rationnel. Par les droites SM et SM_1 je puis faire passer une surface du second degré rationnelle. L'intersection complète de cette surface et du cône étant du sixième degré se décompose en deux droites SM et SM_1 et une quartique gauche rationnelle. La projection de cette quartique gauche sur un plan rationnel quelconque est une quartique plane rationnelle.

En résumé :

La condition nécessaire et suffisante pour qu'une quartique rationnelle soit équivalente à une cubique, c'est qu'elle ait un point rationnel.

La condition nécessaire et suffisante pour qu'une cubique rationnelle soit équivalente à une quartique, c'est qu'elle ait un point rationnel.

Soit $f=0$ une courbe plane de genre 1 et de degré m. Quelle est la condition pour qu'elle soit équivalente à une courbe de degré p, dont l'équation sera $f_1=0$?

Il faut d'abord qu'il y ait sur $f=0$ un groupe rationnel de p points. Si, en effet, nous coupons la transformée $f_1=0$ par une droite ra-

tionnelle quelconque, cette droite la coupera en p points formant un groupe rationnel. Les points correspondants sur $f=0$ formeront aussi un groupe rationnel.

Je dis maintenant que cette condition est suffisante. En effet, s'il existe un groupe rationnel de p points, par ce groupe et par les points doubles je pourrai faire passer une infinité de courbes de degré $m-3+k$, dont l'équation générale sera

$$\alpha_1\varphi_1+\alpha_2\varphi_2+\ldots+\alpha_q\varphi_q+\theta f=0,$$

où $q=km-p$, où les α sont des arbitraires, les φ des polynomes d'ordre $m-3+k$ à coefficients rationnels et θ un polynome arbitraire de degré $k-3$ (le terme θf disparaît si $k<3$).

Ces courbes couperont $f=0$ en $km-p$ points mobiles. Si l'on donne aux α des valeurs rationnelles, ces $km-p$ points formeront un groupe rationnel.

Considérons maintenant un de ces groupes rationnels de $km-p$ points, par ce groupe et les points doubles nous pourrons faire passer une infinité de courbes de degré $m-3+k$, dont l'équation générale sera

$$\alpha_1\psi_1+\alpha_2\psi_2+\ldots+\alpha_p\psi_p+\eta f=0, \tag{2}$$

où les α sont des arbitraires, les ψ des polynomes d'ordre $m-3+k$ à coefficients rationnels et η un polynome arbitraire d'ordre $k-3$.

Ces courbes couperont $f=0$ en p points mobiles. Si alors on considère la transformation

$$\frac{\xi_1}{\psi_1}=\frac{\xi_2}{\psi_2}=\frac{\xi_3}{\psi_3}$$

(où les ξ sont les coordonnées homogènes d'un point dans un plan), elle sera purement rationnelle, toujours en vertu du raisonnement, et elle transformera $f=0$ en une courbe de degré p [parce que les courbes (2) coupent $f=0$ en p points mobiles].

Cette démonstration suppose :

1° Que $km>p$, on peut toujours prendre k assez grand pour cela ;

2° Que $p \geq 3$. Si $p = 1$ ou 2, il est clair que le théorème est en défaut, puisqu'il n'y a pas de courbe de genre 1 et de degré 1 ou 2.

Si $p = 1$, c'est-à-dire s'il y a un point rationnel, il existe aussi un groupe rationnel de trois points (à savoir le groupe qui comprendrait trois points confondus entre eux et avec ce point rationnel); la courbe est donc équivalente à une cubique. Et l'on démontrerait de même qu'elle est équivalente à une courbe de degré quelconque.

Si $p = 2$, c'est-à-dire s'il y a un couple rationnel, il existe aussi un groupe rationnel de quatre points (à savoir le groupe qui comprendrait quatre points confondus deux à deux et avec les deux points du couple); la courbe est donc équivalente à une quartique. Et l'on démontrerait de même qu'elle est équivalente à une courbe d'un degré *pair* quelconque.

Si m est impair et qu'il y ait un couple rationnel, il y a aussi un point rationnel. Car, par les points doubles et par un groupe rationnel de $m - 1$ points qui comprendrait $m - 1$ points confondus $\frac{m-1}{2}$ à $\frac{m-1}{2}$ et avec les deux points du couple, on peut faire passer une courbe de degré $m - 2$ et une seule. Cette courbe est rationnelle et elle coupe $f = 0$ en un autre point qui est unique et rationnel.

En résumé :

Pour qu'une courbe rationnelle de genre 1 et de degré m soit équivalente à une courbe de degré $p > 3$, il faut et il suffit qu'elle possède un groupe rationnel de p points.

Pour aller plus loin, supposons que notre courbe, de degré m, admette un certain nombre de groupes rationnels. Supposons-en trois pour fixer les idées.

Soient G_1, G_2, G_3 ces groupes qui seront formés respectivement de p_1, p_2 et p_3 points. Soit δ le plus grand commun diviseur des quatre nombres

$$m, \quad p_1, \quad p_2, \quad p_3.$$

Je dis qu'il existe un groupe rationnel de δ points.

En effet, on peut trouver quatre nombres entiers positifs

$$K, \quad h_1, \quad h_2, \quad h_3,$$

tels que

$$Km - h_1 p_1 - h_2 p_2 - h_3 p_3 = \delta.$$

Nous pourrons alors mener une infinité de courbes de degré

$$m - 3 + K,$$

passant par les points doubles et ayant avec $f = 0$ un contact d'ordre $h_1 - 1$ aux points du groupe G_1, d'ordre $h_2 - 1$ aux points du groupe G_2, d'ordre $h_3 - 1$ aux points du groupe G_3. Parmi ces courbes, il y en aura une infinité qui seront rationnelles.

Elles couperont $f = 0$, aux points doubles, en $h_1 p_1$ points confondus avec le groupe G_1, en $h_2 p_2$ points confondus avec le groupe G_2, en $h_3 p_3$ points confondus avec le groupe G_3, et en

$$Km - h_1 p_1 - h_2 p_2 - h_3 p_3 = \delta$$

autres points. Ces δ points formeront un groupe rationnel.

C. Q. F. D.

Soit alors δ le plus petit nombre tel qu'il existe sur $f = 0$ un groupe rationnel de δ points. D'après ce qui précède :

1° Le degré m est un multiple de ce nombre caractéristique δ;

2° Il en est de même du degré de toutes les courbes équivalentes à $f = 0$;

3° Il en est encore de même du nombre des points d'un groupe rationnel quelconque de $f = 0$.

Ce nombre caractéristique δ est donc un des éléments les plus importants de la classification des courbes rationnelles de genre 1.

Il me reste à parler d'un point de détail.

Considérons une quartique gauche équivalente à une cubique plane. Par exemple, la cubique sera la perspective de cette quartique, en prenant pour point de vue un point S de la quartique.

D'après ce qui précède, ce point S doit être rationnel. Soit α son argument elliptique sur la quartique et

$$\alpha' = \alpha + k$$

son argument sur la cubique. Soient, d'autre part,

$$\alpha_1, \alpha_2, \ldots, \alpha_9$$

les arguments des autres points rationnels fondamentaux sur la quartique et

$$\alpha'_i = \alpha_i + k \qquad (i = 1, 2, \ldots, 9)$$

leurs arguments sur la cubique.

Nous avons vu que les arguments des points rationnels sur la quartique sont donnés par la formule :

$$\beta = \alpha + 4n\alpha + \Sigma p_i(\alpha_i - \alpha),$$

et sur la cubique par la formule

$$\beta' = \alpha' + 3n\alpha' + \Sigma p_i(\alpha'_i - \alpha').$$

Il faut démontrer que ces deux formules concordent, c'est-à-dire que l'on a

$$\beta' = \beta + k.$$

Or c'est ce qui est évident, si l'on observe que

$$3k = \alpha, \qquad \alpha_i - \alpha = \alpha'_i - \alpha', \qquad 3\alpha' = 4\alpha.$$

V. — Étude de quelques transformations.

Soit α l'argument d'un point rationnel quelconque sur une cubique ; la transformation qui change le point d'argument u, dans le point d'argument $-\alpha - u$, sera évidemment (les trois points $\alpha, u, -\alpha - u$ étant en ligne droite) une transformation *purement rationnelle* qui changera la cubique en elle-même.

Si α et β sont les arguments de deux points rationnels, les transformations

$$(u, -\alpha - u),$$
$$(u, -\beta - u)$$

seront purement rationnelles; il en sera de même de leur résultante

$$(u, \beta - \alpha + u).$$

D'ailleurs, si α est rationnel, il en est de même de -2α, de sorte que la transformation $(u, 3\alpha + u)$ est purement rationnelle.

Étudions de plus près ces transformations $(u, \beta - \alpha + u)$.

Si x, y, z sont les coordonnées du point d'argument u, et ξ, η, ζ celles du point transformé d'argument $\beta - \alpha + u$, les équations de la transformation devront être de la forme

$$\frac{\xi}{X} = \frac{\eta}{Y} = \frac{\zeta}{Z}, \tag{1}$$

X, Y, Z étant des polynomes entiers en x, y, z à coefficients rationnels.

Comment former ces polynomes?

La droite $x = 0$ coupera la cubique en trois points M_1, M_2, M_3 d'arguments $\gamma_1, \gamma_2, \gamma_3$. Considérons les transformés de ces trois points par la transformation inverse de (1), qui auront pour arguments

$$\alpha - \beta + \gamma_1, \quad \alpha - \beta + \gamma_2, \quad \alpha - \beta + \gamma_3,$$

et que j'appellerai M'_1, M'_2, M'_3.

On aura

$$\gamma_1 + \gamma_2 + \gamma_3 = 0. \tag{2}$$

Considérons d'abord trois points P_1, P_2, P_3 d'arguments $\varepsilon_1, \varepsilon_2, \varepsilon_3$, assujettis à la condition unique

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 3\beta - 3\alpha. \tag{3}$$

On pourra choisir ces trois points de façon qu'ils forment un groupe rationnel.

Les six points $M'_1, M'_2, M'_3, P_1, P_2, P_3$ seront, à cause des relations (2) et (3), sur une même conique, et cette conique sera ration-

nelle. Soit

$$X_1 = 0$$

l'équation de cette conique; je puis supposer qu'elle est écrite de telle façon que les coefficients de X_1 soient entiers et premiers entre eux.

D'autre part, la droite $y = 0$ coupe la cubique en trois points N_1, N_2, N_3 ayant pour transformés N'_1, N'_2, N'_3. Les six points N'_1, N'_2, N'_3, P_1, P_2, P_3 sont sur une même conique rationnelle dont l'équation peut s'écrire

$$Y_1 = 0,$$

les coefficients de Y étant entiers et premiers entre eux.

De même, la droite $z = 0$ coupe la cubique en trois points Q_1, Q_2, Q_3 ayant pour transformés Q'_1, Q'_2, Q'_3. Les six points Q'_1, Q'_2, Q'_3, P_1, P_2, P_3 sont sur une même conique rationnelle dont l'équation peut s'écrire

$$Z_1 = 0,$$

les coefficients de Z étant entiers et premiers entre eux.

Considérons alors la fonction

$$\frac{XY_1}{YX_1};$$

ce sera une fonction doublement périodique de l'argument elliptique du point x, y, z; cette fonction ne pourra devenir infinie, car le dénominateur ne peut s'annuler sans que le numérateur s'annule. Elle se réduira donc à une constante; pour la même raison

$$\frac{XZ_1}{ZX_1}$$

est une constante. Nous pourrons donc poser

$$X = aX_1, \qquad Y = bY_1, \qquad Z = cZ_1,$$

a, b, c étant trois entiers premiers entre eux.

Ainsi la transformation (1) peut s'écrire de telle façon que X, Y, Z

soient des polynomes du second ordre. Cela est même possible d'une infinité de manières, car les trois points P_1, P_2, P_3 ne sont assujettis qu'à une seule égalité.

Soient X', Y', Z' trois polynomes du second degré formés comme X, Y, Z, mais en remplaçant les trois points P_1, P_2, P_3 par trois autres points P'_1, P'_2, P'_3 assujettis comme eux à la condition (3). La transformation

$$\frac{\xi}{X'} = \frac{\eta}{Y'} = \frac{\zeta}{Z'} \qquad (1\ bis)$$

devra être la même que la transformation (1); je veux dire par là qu'un point de la cubique $f = 0$ a même transformé, qu'on lui applique l'une ou l'autre des deux transformations. Les deux transformations (1) et (1 *bis*) pourraient être appliquées à un point quelconque du plan; mais alors les deux transformés ne seraient pas les mêmes.

Il résulte de là que les trois polynomes du quatrième degré

$$YZ' - ZY', \quad ZX' - XZ', \quad XY' - YX'$$

sont divisibles par f.

Il importe de remarquer que la transformation (1) est une *transformation Cremona;* c'est-à-dire qu'on peut en tirer les rapports $\frac{x}{z}$, $\frac{y}{z}$ en fonctions rationnelles de ξ, η, ζ, alors même que le point x, y, z n'est pas assujetti à rester sur la cubique; et, en effet, deux des coniques

$$\alpha X + \beta Y + \gamma Z = 0, \qquad \alpha' X + \beta' Y + \gamma' Z = 0$$

ne se coupent qu'en un seul point mobile, en dehors des trois points fixes P_1, P_2, P_3.

Ces trois points fixes sont les *points-bases* de la transformation.

Si l'on résout les équations (1), on trouve

$$\frac{x}{X_0(\xi, \eta, \zeta)} = \frac{y}{Y_0(\xi, \eta, \zeta)} = \frac{z}{Z_0(\xi, \eta, \zeta)}, \qquad (4)$$

X_0, Y_0, Z_0 étant des polynomes du second degré. La transforma-

tion (4) est ainsi la transformation inverse de (1). Quels sont les points-bases de cette transformation inverse?

Je rappelle que, dans une transformation quadratique Cremona, toute droite passant par un point-base se transforme en une droite passant par un point-base de la transformation inverse.

Soit donc une droite D passant par P_1; elle coupera la cubique en deux autres points H_1 et H_2; la somme des arguments de ces deux points sera constante et égale à $-\varepsilon_1$. Soient H'_1 et H'_2 les transformés de H_1 et H_2; la somme de leurs arguments sera constante et égale à

$$2(\beta - \alpha) - \varepsilon_1.$$

La droite H'_1, H'_2, transformée de D, coupera la cubique en un troisième point R_1 dont l'argument sera

$$\varepsilon_1 - 2(\beta - \alpha).$$

Cette quantité étant constante, ce point R_1 restera fixe quand la droite D tournera autour de P_1. Donc R_1 est un des points-bases de (4). Les deux autres, R_2 et R_3, auront pour arguments

$$\varepsilon_2 - 2(\beta - \alpha),$$
$$\varepsilon_3 - 2(\beta - \alpha).$$

Ainsi les trois points-bases de (4) sont encore sur la cubique, et la somme de leurs arguments est

$$3\alpha - 3\beta.$$

Si donc nous considérons les trois points R_1, R_2, R_3, leurs transformés, que j'appellerai Q_1, Q_2, Q_3, seront en ligne droite, et les transformés de leurs transformés sont les trois points P_1, P_2 et P_3.

Considérons maintenant l'expression

$$f(X, Y, Z);$$

c'est un polynome du sixième degré en x, y, z; comme la transfor-

mation n'altère pas la cubique $f = 0$, on aura identiquement

$$f(X, Y, Z) = f(x, y, z)\eta_1(x, y, z), \tag{5}$$

η_1 étant un polynome du troisième degré.

Comme les trois points-bases P_1, P_2, P_3 doivent être des points triples pour la sextique

$$f(X, Y, Z) = 0$$

et que ce sont des points simples pour la cubique

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

ce seront des points doubles pour la cubique $\eta_1 = 0$; de sorte que cette cubique $\eta_1 = 0$ se décomposera en trois droites qui seront les côtés du triangle $P_1P_2P_3$.

D'autre part, les transformations (1) et (4) étant inverses l'une de l'autre, on aura

$$\frac{X_0(X, Y, Z)}{x} = \frac{Y_0(X, Y, Z)}{y} = \frac{Z_0(X, Y, Z)}{z} = \eta_1',$$

ou

$$\begin{cases} X_0(X, Y, Z) = x\eta_1', \\ Y_0(X, Y, Z) = y\eta_1', \\ Z_0(X, Y, Z) = z\eta_1'. \end{cases} \tag{6}$$

Les premiers membres étant des polynomes du quatrième degré, η_1' sera un polynome du troisième degré; les trois points-bases étant des points doubles pour les quartiques

$$X_0(X, Y, Z) = 0, \qquad Y_0 = 0, \qquad Z_0 = 0,$$

seront aussi des points doubles pour la cubique $\eta_1' = 0$. Cette cubique se décompose ainsi encore en trois droites qui sont les trois côtés du triangle $P_1P_2P_3$.

Ainsi les deux polynomes η_1 et η_1' ne peuvent différer que par un facteur constant.

Le polynome η_i est décomposable *au point de vue algébrique* en trois facteurs linéaires; mais il n'arrivera pas toujours que cette décomposition soit possible au point de vue arithmétique. Cela arrivera si les trois points P_1, P_2 et P_3 sont rationnels. Il est clair qu'il est toujours possible de choisir ces trois points (qui sont assujettis seulement à la condition 3) de telle façon qu'ils soient rationnels; et cela d'une infinité de manières en prenant

$$\varepsilon_i = q_i(\beta - \alpha) + \alpha + 3p_i\alpha \qquad (i = 1, 2, 3),$$

avec la condition

$$q_1 + q_2 + q_3 = 3, \qquad p_1 + p_2 + p_3 = -1.$$

C'est la supposition que nous adopterons désormais, sauf avis contraire.

Supposons que x, y, z soient trois entiers premiers entre eux; X, Y, Z sont également trois entiers; il importe de savoir quel est leur plus grand commun diviseur S.

Observons que

$$X_0(X, Y, Z), \quad Y_0(X, Y, Z), \quad Z_0(X, Y, Z)$$

sont divisibles par S^2. Il en résulte que η' est divisible par S^2. C'est déjà une considération qui pourra nous aider à déterminer S.

Considérons de nouveau les neuf points

$$P_i, \quad Q_i, \quad R_i \qquad (i = 1, 2, 3).$$

Nous avons vu qu'ils ont pour arguments

$$\varepsilon_i, \quad \varepsilon_i - (\beta - \alpha), \quad \varepsilon_i - 2(\beta - \alpha),$$

avec la condition

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 3(\beta - \alpha).$$

De là résulte immédiatement que ces neuf points se trouvent trois à

trois sur sept droites, qui sont les droites

$$Q_1Q_2Q_3,\quad P_1Q_2R_3,\quad P_3Q_2R_1,\quad Q_1R_2P_3,$$
$$P_1R_2Q_3\quad Q_1P_2R_3,\quad R_1P_2Q_3.$$

De plus, la somme des arguments des neuf points (de même que celle des arguments des six points P_i et R_i) étant nulle, on conclut que les six points P_i et R_i sont sur une même conique C, et que les neuf points sont sur une infinité de cubiques.

On voit alors que les six points P_i et R_i sont les sommets d'un hexagone de Pascal inscrit dans une conique C, et que les points Q_1, Q_2, Q_3 en ligne droite sont les intersections des trois paires de côtés opposés de cet hexagone.

Considérons les cubiques qui passent par les neuf points; elles forment un faisceau. L'une d'elles est la cubique proposée $f = 0$. Une se décompose en une conique qui est la conique C circonscrite à l'hexagone de Pascal, et en une droite qui est $Q_1Q_2Q_3$. Deux des cubiques se décomposent en trois droites qui sont pour l'une d'elles

$$(7)\qquad R_1Q_2P_3,\quad R_3Q_1P_2,\quad R_2Q_3P_1$$

et pour l'autre

$$(8)\qquad R_1Q_3P_2,\quad R_2Q_1P_3,\quad R_3Q_2P_1.$$

La transformation change la cubique f en elle-même; elle change la conique C dans la droite $Q_1Q_2Q_3$ et inversement; elle change les trois droites (7) les unes dans les autres, de même que les trois droites (8). Il y a donc quatre cubiques du faisceau pour lesquelles on voit immédiatement qu'elles ne sont pas altérées par la transformation. Il suffirait de le savoir de deux d'entre elles pour conclure que cela est vrai pour toutes les cubiques du faisceau.

Toutes les cubiques du faisceau sont donc inaltérées par la transformation (1). Si

$$f(x, y, z) = 0,\qquad \varphi(x, y, z) = 0$$

sont les équations de deux de ces cubiques, on aura évidemment

$$f(X, Y, Z) = f(x, y, z)\eta,$$
$$\varphi(X, Y, Z) = \varphi(x, y, z)a\eta,$$

a étant une constante, et de même

$$f(X, Y, Z) + \lambda\varphi(X, Y, Z) = [f(x, y, z) + \lambda\varphi(x, y, z)]b\eta,$$

b étant une autre constante. Or cela n'est possible que si $a = b = 1$; d'où il suit que le coefficient η qui figure dans l'équation (5) est le même pour toutes les cubiques du faisceau.

Soit maintenant

$$D = \alpha x + \beta y + \gamma z = 0$$

l'équation de la droite $Q_1Q_2Q_3$; soit

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

celle de la conique C; je supposerai que les coefficients du polynome D, de même que ceux du polynome S sont premiers entre eux. L'équation de C pourra également se mettre sous l'une des deux formes

$$\alpha X + \beta Y + \gamma Z = 0, \qquad \alpha X_0 + \beta Y_0 + \gamma Z_0 = 0,$$

de sorte que nous aurons identiquement

$$\alpha X + \beta Y + \gamma Z = \theta S,$$
$$\alpha X_0 + \beta Y_0 + \gamma Z_0 = \theta_0 S,$$

θ et θ_0 étant des entiers.

Nous trouverons ensuite

$$\theta_0 S(X, Y, Z) = \alpha X_0(X, Y, Z) + \beta Y_0(X, Y, Z) + \gamma Z_0(X, Y, Z) = D\eta$$

et, d'autre part,

$$S(X, Y, Z)(\alpha X + \beta Y + \gamma Z) = \eta S(x, y, z)D;$$

d'où

$$\theta_0\gamma_1 SD = \theta\gamma_1' SD$$

et enfin

$$\theta_0\gamma_1 = \theta\gamma_1'.$$

VI. — Subdivision des classes en sous-classes.

Soient C et C′ deux cubiques équivalentes; on pourra passer de C à C′ par une transformation purement rationnelle T qui, comme nous allons le voir, sera généralement une transformation quadratique. Soit

$$(1) \qquad \frac{\xi}{X} = \frac{\eta}{Y} = \frac{\zeta}{Z}$$

cette transformation où X, Y, Z seront des polynomes entiers à coefficients rationnels. La droite $x = 0$ coupera la cubique C′ en trois points M_1, M_2, M_3 d'arguments $\gamma_1, \gamma_2, \gamma_3$. Soient M_1', M_2', M_3' les transformés de ces trois points par la transformation T^{-1} inverse de T; ces trois points seront sur la cubique C et auront pour arguments

$$\gamma_1 - k, \quad \gamma_2 - k, \quad \gamma_3 - k \quad (\gamma_1 + \gamma_2 + \gamma_3 = 0).$$

Par ces trois points qui formeront sur C un groupe rationnel et par deux points rationnels quelconques du plan, je puis faire passer une conique rationnelle qui coupera C en trois autres points que j'appellerai P_1, P_2, P_3, qui formeront un groupe rationnel et dont les arguments $\varepsilon_1, \varepsilon_2, \varepsilon_3$ seront liés par la relation

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 3k.$$

Soit $X_1 = 0$, l'équation de cette conique.

D'autre part la droite $y = 0$ coupera C′ en trois points N_1, N_2, N_3 dont les transformés par T^{-1} que j'appelle N_1', N_2', N_3' auront des arguments dont la somme sera $-3k$ (pour la même raison que la somme des arguments des trois points M_1', M_2', M_3').

Il résulte de là que les six points $N_1', N_2', N_3', P_1, P_2, P_3$ sont sur une

même conique qui est rationnelle puisque ces six points forment deux groupes rationnels. Soit $Y_1 = 0$ l'équation de cette conique.

Enfin la droite $z = 0$ coupera C' en trois points dont les transformés par T^{-1} seront avec P_1, P_2 et P_3 sur une même conique rationnelle dont l'équation sera $Z_1 = 0$.

Les polynomes X_1, Y_1, Z_1 sont du deuxième degré et à coefficients rationnels.

On verrait comme dans le paragraphe précédent que les fonctions doublement périodiques

$$\frac{XY_1}{YX_1}, \quad \frac{XZ_1}{ZX_1}$$

se réduisent à des constantes rationnelles que nous pouvons supposer égales à 1 sans restreindre la généralité. On peut donc prendre

$$X = X_1, \qquad Y = Y_1, \qquad Z = Z_1.$$

Ainsi l'on peut toujours supposer que les polynomes X, Y et Z sont du deuxième degré et sont les premiers membres de l'équation de trois coniques ayant trois points communs. Il en résulte que la transformation T est une transformation quadratique Cremona, ayant pour points-bases P_1, P_2, P_3. Si nous résolvons les équations (1) nous trouvons

$$(2) \qquad \frac{x}{X_0(\xi, \eta, \zeta)} = \frac{y}{Y_0(\xi, \eta, \zeta)} = \frac{z}{Z_0(\xi, \eta, \zeta)},$$

X_0, Y_0, Z_0 étant trois polynomes du deuxième degré à coefficients rationnels.

Les équations (2) définiront la transformation T^{-1} inverse de T.

Quels sont les points-bases de cette transformation?

Soit D une droite quelconque passant par P_1; elle coupera C en deux autres points H_1 et H_2 dont les arguments u et v devront satisfaire à la relation

$$u + v + \varepsilon_1 = 0.$$

Les transformés H'_1 et H'_2 de ces deux points seront sur C' et auront pour arguments $u + k$ et $v + k$. La transformée de D est une conique

qui doit se décomposer en deux droites dont l'une est la droite R_2R_3 et l'autre est la droite $H'_1H'_2$ qui doit passer par R_1.

Or la droite $H'_1H'_2$ coupe C' en un troisième point dont l'argument doit être : $\varepsilon_1 - 2k$. Il reste donc fixe quand la droite D tourne autour du point P_1. Ce ne peut donc être que le point R_1.

En résumé les trois points-bases de (2) sont sur C' et ont pour arguments

$$\varepsilon_1 - 2k, \quad \varepsilon_2 - 2k, \quad \varepsilon_3 - 2k.$$

Remarquons que notre transformation Cremona (1) transforme toute cubique passant par les trois points P_1, P_2, P_3 en une cubique passant par les trois points R_1, R_2, R_3.

Quelle est la condition pour que parmi ces cubiques il y en ait qui, tout en étant de genre 1, soient leur propre transformée? D'après ce que nous avons vu dans le paragraphe précédent, il faut d'abord que les six points-bases soient sur une même conique. Si cette condition est remplie cette conique se transformera en une droite, de sorte que les trois points R_1, R_2, R_3 auront pour transformés trois points Q_1, Q_2, Q_3 en ligne droite.

Il faut ensuite que ces trois points Q soient les points d'intersection des côtés opposés de l'hexagone des points P et R. Si cette condition est remplie nous avons vu que les cubiques qui passent par les neuf points P, Q, R ne sont pas altérées par la transformation.

Il résulte d'abord de là que si la cubique C est équivalente à la cubique C' et de telle façon que les arguments des points correspondants diffèrent de k, il y aura sur C une infinité de groupes rationnels de trois points dont la somme des arguments sera $-3k$. Ce sont les points dont les transformés sont sur une droite rationnelle. Il y aura aussi sur C une infinité de groupes rationnels de trois points (je dirai de *triplets* rationnels ou simplement de triplets) dont la somme des arguments soit $-3k$, comme par exemple le triplet P_1, P_2, P_3.

Réciproquement s'il existe un triplet P_1, P_2, P_3 dont la somme des arguments soit $-3k$, la cubique C sera équivalente à une cubique C' de telle façon que les arguments des points correspondants diffèrent de k à un tiers de période près. En effet ces trois points formant un groupe rationnel, on pourra faire passer par ces trois points trois

coniques rationnelles

$$X = 0, \qquad Y = 0, \qquad Z = 0.$$

La transformation Cremona

$$\frac{\xi}{X} = \frac{\eta}{Y} = \frac{\zeta}{Z}$$

changera alors C en une autre cubique C′ satisfaisant à la condition proposée.

Si maintenant il existe un triplet dont la somme soit $3k$, il en existera une infinité dont la somme sera $-3k$; car par ce triplet on pourra faire passer une infinité de coniques rationnelles; chacune d'elles coupera la cubique en trois autres points formant un groupe rationnel de somme $-3k$. On en conclut immédiatement que s'il existe un triplet de somme $3k$, il y en a une infinité.

Je dis maintenant que s'il existe sur C un triplet de somme $3k$, il y en a une infinité de somme $3nk$, n étant un entier quelconque positif ou négatif. Pour cela, d'après ce qui précède, il me suffira d'établir que s'il y a un triplet de somme $3n'k$ et un triplet de somme $3n''k$, il y en aura aussi un de somme $-3k(n'+n'')$ et par conséquent un de somme $3k(n'+n'')$. Considérons en effet six points formant deux triplets de sommes $3n'k$ et $3n''k$.

Par ces six points et par trois points rationnels quelconques du plan, je pourrai faire passer une cubique qui sera rationnelle. Cette cubique coupera C en trois autres points formant un groupe rationnel et la somme des arguments sera $-3k(n'+n'')$. C. Q. F. D.

De là résulte la conséquence suivante :

Si C est équivalente à une cubique C_1, de telle façon que les arguments des points correspondants sur C et C_1 diffèrent de k, elle sera aussi équivalente à une infinité d'autres cubiques $C_2, C_3, \ldots, C_n, \ldots$ $C_{-1}, C_{-2}, C_{-3}, \ldots$; et cela de telle façon que les arguments des points correspondants sur C et C_n diffèrent de nk.

Une question se pose ensuite. D'après nos définitions deux cubiques sont équivalentes ou appartiennent à la même *classe* si l'on peut pas-

ser de l'une à l'autre par une transformation *birationnelle* à coefficients rationnels. Je dirai qu'elles appartiennent à la même *sous-classe* si l'on peut passer de l'une à l'autre par une transformation *linéaire* à coefficients rationnels (je ne dis pas entiers).

On peut alors se demander si toutes les cubiques C_n que je viens de définir appartiennent à des sous-classes différentes. Bien que l'on puisse passer de C à C_n par une transformation quadratique, de telle façon que les arguments des points correspondants diffèrent de nk, ce n'est pas une raison pour qu'on ne puisse pas également passer de C à C_n par une transformation *linéaire*, et par exemple de telle façon que les arguments des points correspondants soient égaux.

Il faut et il suffit, pour qu'il en soit ainsi, que C soit transformable en elle-même par une transformation quadratique, la différence des arguments des points correspondants étant nk.

Or je dis que C n'est pas altérée par une transformation quadratique rationnelle qui change le point d'argument u dans le point d'argument $u + 3k$. En d'autres termes, je dis que les coordonnées du point $u + 3k$ sont des fonctions rationnelles des coordonnées du point u, ou, si l'on aime mieux, les coordonnées de $u + 3k$ seront rationnelles, *après adjonction des coordonnées du point u au domaine de rationalité*.

Soient, en effet, ε_1, ε_2, ε_3 les arguments des points de C qui forment un triplet dont la somme est $-3k$. Par le point u et par un point rationnel quelconque du plan, je fais passer une droite qui coupe C en deux autres points ayant pour arguments v et w; on aura

$$u + v + w = 0.$$

Les deux points v et w formeront un couple rationnel *après adjonction des coordonnées du point u*.

Par les cinq points ε_1, ε_2, ε_3 u et w je puis faire passer une conique qui sera rationnelle *après adjonction des coordonnées de u*; cette conique coupera C en un sixième point qui sera rationnel après adjonction des coordonnées de u.

Ce point ne sera autre que le point $u + 3k$.

C'est ce qu'il fallait démontrer.

Ainsi les cubiques C et C_3 ou, plus généralement, les cubiques C_n et C_{n+3} appartiennent à une même sous-classe. Donc *les cubiques* C_n *se répartissent en trois sous-classes au plus.*

Pour aller plus loin, deux cas sont à distinguer : le premier est celui où la cubique C admet un point rationnel. Si alors α est l'argument de ce point rationnel, et si la cubique C n'est pas altérée par une transformation purement rationnelle telle que les arguments des points correspondants diffèrent de $3k$, le point d'argument $\alpha + 3k$ sera aussi rationnel.

Je dis que C admettra un triplet dont la somme des arguments sera $-3k$, de telle façon qu'elle sera équivalente à une cubique C_1, la différence des arguments des points correspondants étant k. En effet, par le point α je fais passer une droite rationnelle quelconque; elle coupera C en deux points d'arguments β et γ formant un couple rationnel. On aura

$$\alpha + \beta + \gamma = 0.$$

Par les deux points β et γ, par le point rationnel $\alpha + 3k$ et par deux points rationnels quelconques du plan je fais passer une conique qui est rationnelle; elle coupe C en trois autres points qui forment un triplet rationnel et dont la somme des arguments sera

$$-\beta - \gamma - (\alpha + 3k) = -3k. \qquad \text{C. Q. F. D.}$$

Si maintenant la cubique C a un point rationnel, tous ses points rationnels seront compris dans la formule

$$\alpha + 2n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

la cubique étant supposée de rang $q + 1$.

Je suppose de plus qu'aucune des quantités

$$3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_h(\alpha_h - \alpha)$$

ne soit une partie aliquote d'une période, mais que

$$\alpha_{h+1} - \alpha, \quad \alpha_{h+2} - \alpha, \quad \ldots, \quad \alpha_q - \alpha$$

soient des parties aliquotes d'une période, de telle façon que pour $s < q$

$$m_s(\alpha_s - \alpha)$$

soit une période (m_s étant un entier).

Quel sera le nombre des sous-classes de la classe dont fait partie C?

Quelle est la condition pour qu'il existe une cubique C_k équivalente à C, de telle manière que la différence des arguments soit k?

La condition nécessaire et suffisante c'est qu'il existe une transformation de C en elle-même, la différence des arguments étant $3k$; c'est-à-dire que

$$(3) \quad 3k = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha).$$

Maintenant, deux valeurs k' et k'' de k conduiront à deux cubiques $C_{k'}$ et $C_{k''}$ appartenant à la même sous-classe si

$$(4) \quad k' - k'' = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha) \ (^1).$$

L'équation (3) nous donnera les valeurs de k; on voit qu'à chaque valeur du second membre correspondent neuf valeurs distinctes de k, différant entre elles de $\frac{1}{3}$ de période. Mais il importe de remarquer que ces neuf valeurs ne nous conduiront pas à des cubiques C_k appartenant à des sous-classes différentes. En effet, l'argument d'un point de C_k est défini par cette condition que la somme des arguments de trois points en ligne droite soit égale à zéro (ou plutôt à une période). Mais cette condition ne définit évidemment l'argument qu'à $\frac{1}{3}$ de période près.

A chaque système de valeur des entiers

$$n, p_1, p_2, \ldots, p_q$$

correspond donc une cubique C_k. Mais si deux pareils systèmes d'en-

---

(1) C'est d'ailleurs le seul cas où l'on puisse passer de $C_{k'}$ à $C_{k''}$ par une transformation linéaire *de telle façon que la différence des arguments des points correspondants soit une constante;* mais il peut arriver aussi que l'on puisse passer d'une cubique à l'autre par des transformations linéaires d'une autre nature que nous appellerons *impropres.* Nous y reviendrons plus loin.

tiers ne diffèrent que par des multiples de 3, les cubiques correspondantes sont de la même sous-classe. Si le second membre de (3) ou de (4) ne pouvait jamais devenir égal à une partie aliquote d'une période, le nombre des sous-classes serait alors 3^{q+1} au plus.

Mais si, par exemple, $m_q(\alpha_q - \alpha)$ était une période, et que le nombre entier m_q ne fût pas divisible par 3, on pourrait prendre deux systèmes d'entiers

$$n', p'_1, p'_2, \ldots, p'_q,$$
$$n'', p''_1, p''_2, \ldots, p''_q,$$

de telle sorte que chaque nombre du premier système soit égal au nombre correspondant de second système, à l'exception des nombres p'_q et p''_q.

Si alors k' et k'' sont les valeurs de k correspondantes, on aurait

$$k' - k'' = \frac{p'_q - p''_q}{3}(\alpha_q - \alpha).$$

On peut alors prendre

$$\alpha_q - \alpha = \frac{\omega}{m_q},$$

et poser

$$p'_q - p''_q = 3\mu + m_q\nu$$

(μ et ν étant des entiers), d'où

$$k' - k'' = \frac{\mu\omega}{m_q} + \frac{\nu\omega}{3} = (\alpha_q - \alpha) + \frac{1}{3} \text{ de période.}$$

De telle façon que les deux cubiques $C_{k'}$ et $C_{k''}$ seront encore de la même sous-classe.

Donc, pour que deux cubiques soient de la même sous-classe, il suffit que les deux systèmes d'entiers correspondants ne diffèrent que par des multiples de 3, à l'exception de ceux des nombres de ces deux systèmes qui correspondent à des différences $\alpha_s - \alpha$, qui sont des fractions $\frac{m_s}{}$ d'une période, l'entier m_s n'étant pas divisible par 3.

Si donc il y a q' nombres m_s non divisibles par 3, *notre classe se composera de $3^{q+1-q'}$ sous-classes au plus.*

Considérons, par exemple, la cubique

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

En vertu du théorème de Fermat, elle n'a que trois points rationnels qui sont les trois points d'inflexion en ligne droite,

$$x = y + z = 0, \qquad \arg\ 0,$$

$$y = x + z = 0, \qquad \arg\ \frac{\omega}{3},$$

$$z = x + y = 0, \qquad \arg\ \frac{2\omega}{3}.$$

Il y aura donc, au plus, trois sous-classes distinctes qui correspondent aux valeurs de k,

$$k = 0, \qquad k = \frac{\omega}{9}, \qquad k = \frac{2\omega}{9}.$$

Si nous faisons la transformation

$$\frac{\xi}{x^2 - zx + z^2 - y^2} = \frac{\eta}{xy} = \frac{\zeta}{y(y+z)},$$

dont les points-bases sont les trois points d'inflexion non en ligne droite

$$x = y + z = 0, \qquad y = x^2 - zx + x^2 = 0;$$

et dont la transformation inverse est

$$\frac{x}{\eta(2\zeta - \eta + \xi)} = \frac{y}{\eta^2 - \eta\zeta + \zeta^2} = \frac{z}{\zeta^2 + \xi\zeta - \zeta^2};$$

notre cubique se transforme en la suivante :

$$\eta^3 + \zeta^3 + \xi(\zeta^2 - 2\eta^2 + 2\eta\xi) + \xi^2(\eta + \zeta) = 0,$$

qui appartient à la seconde sous-classe; elle admet trois points rationnels

$$\eta = \zeta = 0, \qquad \zeta = \xi - \eta = 0, \qquad \xi = \eta + \zeta = 0$$

correspondant à ceux de la cubique proposée. Il est aisé de vérifier que chacun d'eux se trouve sur la tangente menée à la courbe en l'un des deux autres; ils ont respectivement pour arguments

$$\frac{\omega}{9}, \quad \frac{4\omega}{9}, \quad \frac{7\omega}{9}.$$

Si l'on voulait maintenant construire une cubique équivalente à la cubique proposée et de telle façon qu'au point d'argument u correspondît le point d'argument $u + \frac{2\omega}{9}$, il suffirait d'intervertir dans nos transformations le rôle des lettres y et z. Il est clair qu'on retomberait de la sorte sur la même transformée.

Nous n'avons donc en tout que deux sous-classes, et le nombre des sous-classes n'atteint pas le maximum prévu par l'analyse précédente, qui serait 3. Cela tient à ce que C est transformable en elle-même par une de ces transformations linéaires impropres dont j'ai dit un mot plus haut et sur lesquelles je vais revenir.

Supposons qu'une cubique C soit transformable en une autre cubique C′ par une transformation birationnelle dont je ne suppose pas les coefficients rationnels.

Soit u l'argument d'un point M de C, et u' celui du point correspondant M′ de C′. Nous pourrons toujours supposer que ces arguments ont été définis de telle sorte que les périodes soient les mêmes pour les deux cubiques.

Cela posé, il est clair que u et u' devront être liés par une relation linéaire

$$u' = su + k,$$

et que cette relation devra être telle que u' augmente d'une période quand u augmente d'une période et réciproquement.

Cela peut arriver de trois manières :

1° Si $s = 1$, les périodes étant d'ailleurs quelconques. Je dirai alors que la transformation est *propre*.

2° Si $s = -1$, les périodes étant d'ailleurs quelconques. Je dirai alors que c'est une *transformation impropre générale*.

3° Si s et les périodes ont des valeurs convenables. Je dirai alors que c'est une *transformation impropre spéciale*.

Il y en a de trois sortes :

1° $s = \pm i$, le rapport des périodes $= i$ (transf. quaternaires);

2° $s = e^{\pm\frac{2i\pi}{3}}$, le rapport des périodes $= s$ (transf. ternaires);

3° $s = e^{\pm\frac{i\pi}{3}}$, le rapport des périodes $= s$ (transf. sénaires).

Pour que la transformation soit linéaire, il faut et il suffit que trois points en ligne droite avant la transformation restent en ligne droite après la transformation; c'est-à-dire que si

$$u_1 + u_2 + u_3 = 0,$$

on devra avoir

$$u'_1 + u'_2 + u'_3 = 0,$$

$$u'_1 = su_1 + k, \qquad u'_2 = su_2 + k, \qquad u'_3 = su_3 + k,$$

ce qui veut dire que k doit être un tiers de période.

Les plus intéressantes de ces transformations sont celles qui transforment C en elle-même. Quelles sont les conditions pour que ces transformations soient purement rationnelles, c'est-à-dire aient leurs coefficients rationnels?

Je ne reviendrai pas sur les transformations propres. Commençons par les transformations impropres générales. La condition nécessaire et suffisante pour que la transformation $(u, -u + k)$ soit rationnelle, c'est-à-dire pour que les coordonnées du point $-u + k$ soient des fonctions rationnelles de celles du point u, c'est évidemment que le point d'argument $-k$ soit rationnel, puisque les trois points u, $-u + k$ et $-k$ sont en ligne droite.

Soit maintenant $s = i$ et supposons d'abord la transformation linéaire; nous pourrons supposer $k = 0$. Quelle est la condition pour que la transformation (u, iu) soit rationnelle?

Les points doubles de cette transformation seront donnés par l'équation

$$u = iu + m\omega + n\omega',$$

ω et ω' étant les périodes; mais le rapport de ces périodes étant égal

à i, on peut écrire

$$u = iu + \omega(m + ni) \qquad (m \text{ et } n \text{ entiers}),$$

qui admet deux solutions distinctes

$$u = 0, \qquad u = \frac{\omega}{2}(1 + i).$$

Ces deux points doivent donc former un couple rationnel si la transformation est rationnelle. Mais le premier étant un point d'inflexion, tandis qu'il n'en est pas de même de l'autre, les deux points devront être l'un et l'autre rationnels. Si d'ailleurs le second de ces points est rationnel, le premier l'est nécessairement, puisque la tangente au second va passer par le premier.

Soient alors A le point $u = 0$, B le point $\frac{\omega}{2}(1 + i)$, C et D les points $\frac{\omega}{2}$ et $i\frac{\omega}{2}$ (de telle façon que les trois points B, C, D soient en ligne droite). Soit M un point quelconque u et M′ son transformé iu. Le rapport anharmonique des quatre droites BA, BC, BM, BM′, qui est constant, devrait être rationnel si la transformation était rationnelle. Or il est égal à i; donc la transformation ne peut être rationnelle.

Il n'y a donc pas de transformation quaternaire rationnelle et linéaire d'une cubique en elle-même. Passons aux transformations ternaires.

Soit (u, su) une transformation ternaire linéaire; les périodes étant ω et $s\omega$, les points doubles de la transformation seront donnés par l'équation

$$u = su + \omega(m + ns),$$

qui admet trois solutions distinctes

$$u = 0, \qquad u = \frac{\omega}{3}(2 + s), \qquad u = \frac{\omega}{3}(1 + 2s).$$

Ces trois points doubles sont en ligne droite et sont des points d'inflexion. Ils doivent former un groupe rationnel si la transformation est rationnelle, de sorte que la droite qui les joint est rationnelle. Soit D cette droite.

Soient M un point u quelconque, M′ et M″ ses deux transformés successifs su et s^2u. Ces trois points sont en ligne droite, et toutes les droites MM′M″ vont concourir en un même point A (pôle de la droite D par rapport à la cubique) qui doit être rationnel si la transformation est rationnelle.

Cela posé, le rapport anharmonique du point A, des points M, M′ et de l'intersection de MM′ avec D, rapport qui est constant, devrait être rationnel si la transformation était rationnelle. Or il est égal à s.

Il ne peut donc y avoir de transformations ternaires linéaires et rationnelles d'une cubique en elle-même (ni par conséquent de transformations sénaires).

En résumé, *une cubique ne peut admettre une transformation en elle-même qui soit, à la fois, impropre spéciale, linéaire et rationnelle.*

A vrai dire, la démonstration qui précède est encore incomplète, puisqu'elle ne s'applique qu'au cas de $k = 0$ et que, pour qu'une transformation soit linéaire, il suffit que k soit un tiers de période. Mais nous allons étendre le résultat au cas de k quelconque, c'est-à-dire non seulement aux transformations linéaires où k est un tiers de période sans être nul, mais encore aux transformations birationnelles quelconques.

Soit $(u, iu + k)$ une transformation quaternaire de C en elle-même. Les points doubles seront

$$\frac{k}{2}(1+i), \qquad \frac{k+\omega}{2}(1+i),$$

et formeront un couple rationnel, d'où il résulte que le point

$$-\left(k+\frac{\omega}{2}\right)(1+i),$$

qui est en ligne droite avec les deux premiers, sera lui-même rationnel. J'appelle ces trois points A, A′ et B.

La transformation proposée *doublée* est la transformation impropre

générale $(u, -u+k+ki)$, et, si elle est rationnelle, le point

$$-k(1+i),$$

que j'appelle C, sera lui même rationnel.

Soit M un point quelconque u et M′ son transformé $iu+k$. La droite MB coupera la cubique en un troisième point M_1, et la droite M′B coupera la cubique en un troisième point M'_1 qui sera le transformé de M_1.

Les droites MB et M′B formeront donc un faisceau homographique dont les droites doubles seront la droite AA′B, qui est rationnelle, et la droite BD, qui joint le point B aux deux points

$$\frac{k}{2}(1+i)+\frac{\omega}{2}, \qquad \frac{k}{2}(1+i)+\frac{\omega i}{2},$$

qui sont transformés l'un de l'autre et forment un couple rationnel. Cette droite devrait également être rationnelle.

Le rapport anharmonique constant des quatre droites BA, BD, BM, BM′ devrait être rationnel si la transformation était rationnelle. Or, il est égal à i; donc notre transformation ne saurait être rationnelle.

Considérons maintenant une transformation ternaire $(u, su+k)$; les trois points doubles de cette transformation auront pour arguments

$$\frac{k}{1-s}, \quad \frac{k}{1-s}+\frac{\omega}{3}(2+s), \quad \frac{k}{1-s}+\frac{\omega}{3}(2s+1).$$

La somme de leurs arguments sera, à une période près, $k(2+s)$, et ils formeront un triplet rationnel. Soient A, A′, A″ ces trois points.

Par ce triplet rationnel, je pourrai faire passer une conique rationnelle que j'appelle K et qui coupera la cubique suivant un autre triplet rationnel que j'appelle T; la somme des arguments de ce triplet sera $-k(2+s)$.

Soient ensuite M le point u, M′ et M″ ses deux transformés successifs dont les arguments sont

$$su+k, \quad s^2u+k(1+s).$$

La somme de ces trois arguments étant $k(2+s)$, les trois points M, M′, M″ et le triplet T seront sur une même conique que j'appelle H.

Soit D l'intersection de H et de K.

On voit tout de suite que par un point de la cubique passe une seule des coniques H, d'où l'on conclut que ces coniques passent par quatre points fixes; trois de ces points forment le triplet T; le quatrième, que j'appelle E, est en dehors de la cubique. Étant unique, il est rationnel.

Le rapport anharmonique des quatre points E, D, M, M′ sur la conique H est constant. Si la transformation était rationnelle, il devrait être rationnel. Or il est égal à s.

Il ne peut donc y avoir de transformations rationnelles ternaires, ni par conséquent sénaires.

En résumé, *une transformation d'une cubique en elle-même ne peut pas être à la fois impropre spéciale et rationnelle.*

Si une transformation birationnelle T transforme une cubique C en une autre cubique C_1', nous appellerons u l'argument elliptique d'un point M de C et u' l'argument de son transformé M′ sur C′. Nous pourrons toujours supposer

$$du' = du,$$

car si du est une différentielle abélienne de première espèce pour C, c'en sera une aussi pour C′. Donc u' et u ne différeront que par une constante k, et l'on aura

$$u' = u + k.$$

Nous supposerons toujours u' défini de telle façon que la somme des arguments de trois points en ligne droite soit nulle, ce qui définit k à $\frac{1}{4}$ de période près.

Supposons que T ait ses coefficients rationnels, et qu'une seconde transformation T_1 à coefficients rationnels change C en une autre cubique C_1'. Soit M_1' le transformé de M sur C_1' et u_1' son argument elliptique sur C_1'. Soit

$$u_1' = u + k_1.$$

Les deux cubiques C′ et C_1' appartiennent à la même classe; dans quels cas appartiendront-ils à la même sous-classe, c'est-à-dire dans

quels cas pourra-t-on passer de C'_1 à C' par une transformation linéaire L à coefficients rationnels?

Soit N le transformé de M'_1 par L; N sera sur C', soit v l'argument de N sur C'. Je ne puis plus, cette fois, affirmer que $dv = du'_1 = du$, parce que les arguments elliptiques des points de C' ont déjà été définis et que j'ai, par conséquent, déjà disposé des arbitraires que comporte cette définition.

La transformation

$$T^{-1}T_1L$$

est purement rationnelle; elle change C' en elle-même et M' en N: *d'après ce que nous venons de voir, elle ne peut être impropre spéciale.* Elle sera donc propre ou impropre générale, c'est-à-dire qu'on aura

$$v = u' + \varepsilon \qquad \text{ou} \qquad v = -u' + \varepsilon,$$

ε étant une constante.

Quelles sont les valeurs que peut prendre ε?

1° Pour les transformations propres, ces valeurs sont

$$\varepsilon = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha).$$

2° Pour les transformations impropres générales, elles sont

$$\varepsilon = -(3n+1)\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha) - k$$

(car le point $-\varepsilon$ doit être rationnel sur C' et, par conséquent, le point $-\varepsilon - k$ sur C).

Considérons trois points sur C; soit Σu la somme de leurs arguments; considérons leurs transformés par T sur C' dont la somme des arguments sera $\Sigma u'$, leurs transformées par T_1 sur C'_1 dont la somme des arguments sera $\Sigma u'_1$; et enfin les transformés de ce dernier triplet par L; ces transformés formeront un triplet sur C', et la somme des arguments sera Σv.

La transformation L étant linéaire, si l'un de ces deux derniers triplets est en ligne droite, il doit en être de même de l'autre; c'est-à-dire que les deux sommes $\Sigma u'_1$ et Σv doivent s'annuler en même temps.

Or on a

$$\Sigma u'_1 = \Sigma u' + 3k_1 - 3k$$

et, de plus,

$$\Sigma v = \Sigma u' + 3\varepsilon$$

si L est propre, et

$$\Sigma v = -\Sigma u' + 3\varepsilon$$

si L est impropre.

On aura donc, dans le premier cas,

$$\Sigma v - \Sigma u'_1 = 3\varepsilon - 3k_1 + 3k$$

et, dans le second cas,

$$\Sigma v + \Sigma u'_1 = +3\varepsilon + 3k_1 - 3k.$$

Donc on devra avoir, dans le premier cas,

$$(4) \quad k_1 - k = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha)$$

et, dans le second,

$$(4\,bis) \quad \begin{cases} k_1 - 2k = +(3n+1)\alpha + p_1(\alpha_1 - \alpha) \\ \qquad\qquad + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha), \end{cases}$$

le tout à $\frac{1}{3}$ de période près.

La première de ces relations n'est autre que la relation (4) déjà discutée.

L'équation (3) nous apprend que k et k_1 doivent être tous deux de la forme

$$k = 3n'\alpha + p'_1(\alpha_1 - \alpha) + p'_2(\alpha_2 - \alpha) + \ldots + p'_q(\alpha_q - \alpha),$$
$$k_1 = 3n''\alpha + p''_1(\alpha_1 - \alpha) + p''_2(\alpha_2 - \alpha) + \ldots + p''_q(\alpha_q - \alpha),$$

chacun des nombres n', n'', p', p'' étant le $\frac{1}{3}$ d'un entier. Nous avons vu déjà que la relation (4') a lieu si les différences

$$n' - n'', \quad p'_1 - p''_1, \quad \ldots, \quad p'_q - p''_q$$

sont des nombres entiers, sauf pour les différences $p'_s - p''_s$ qui correspondent à un entier m_s non divisible par 3.

Dans quel cas maintenant la relation (4 *bis*) aura-t-elle lieu? Il faut que les différences

$$u'' - 2u' - \frac{1}{3}, \quad p''_1 - 2p'_1, \quad p''_2 - 2p'_2, \quad \ldots, \quad p''_q - 2p'_q$$

soient des nombres entiers.

Remarquons que nous pouvons toujours supposer $\alpha = 0$; si nous prenons, en effet,

$$k = -\alpha \qquad \left(u' = \frac{-1}{3},\ p'_s = 0\right),$$

et alors au point α de C correspondra le point $\alpha + k = 0$ de C'. En d'autres termes, si une cubique a un point rationnel, il y aura une cubique équivalente qui aura un point d'inflexion rationnel.

Supposons donc $\alpha = 0$, ce qui nous dispense de considérer les valeurs des nombres u' et u''. Le nombre p_k peut alors prendre deux valeurs distinctes 0 et $\frac{1}{3}$; les valeurs 1 et 0 par exemple ne sont pas distinctes, parce que leur différence est un entier; les valeurs $\frac{1}{3}$ et $\frac{2}{3}$ ne sont pas distinctes non plus, parce que la différence

$$p'' - 2p' = \frac{2}{3} - 2\left(\frac{2}{3}\right)$$

est un entier.

Il résulte de là que si α est nul et qu'il y ait q' entiers m, non divisibles par 3, *la classe comprendra $2^{q-q'}$ sous-classes.*

Il nous reste à examiner le cas où la cubique C n'admet pas de point rationnel.

La cubique C n'aura pas alors de transformation rationnelle impropre en elle-même, mais elle pourra admettre des transformations rationnelles propres en elle-même.

Ces transformations $(u, u + k)$ seront comprises dans une formule

$$k = p_1\beta_1 + p_2\beta_2 + \ldots + p_q\beta_q, \tag{5}$$

où les β sont des constantes données et les p des entiers arbitraires.

Si C est équivalente à une autre cubique C', de telle manière que le

point u ait pour transformé sur C' le point $u+k'$, c'est qu'il existe sur C une infinité de triplets rationnels dont la somme des arguments est $-3k'$. Soit T un de ces triplets.

Coupons ensuite C par une droite rationnelle quelconque; les trois points d'intersection u_1, u_2, u_3 formeront un triplet rationnel.

Par T, par u_1 et par un point rationnel quelconque A du plan, je fais passer une conique K_1; soit de même K_2 la conique Tu_2A et K_3 la conique Tu_3A. Chacune des coniques K_1, K_2, K_3 ne sera pas rationnelle, mais leur *ensemble* sera rationnel, de telle façon que le produit des premiers membres de leurs équations sera un polynome à coefficients rationnels.

K_1 coupera C en deux autres points c_1 et c'_1, K_2 et K_3 couperont C en deux autres couples de points c_2 et c'_2, c_3 et c'_3. Ces six points c et c' formeront un groupe rationnel, et l'ensemble des trois droites $c_1c'_1$, $c_2c'_2$, $c_3c'_3$ formera une cubique rationnelle, bien que chacune de ces trois droites, prise séparément, ne soit pas rationnelle.

La droite $c_1c'_1$ coupe C en un troisième point u_1-3k'. La droite $c_2c'_2$ coupe C au point u_2-3k'; la droite $c_3c'_3$ coupe C au point u_3-3k'. Ces trois points forment un triplet rationnel.

Si nous joignons les trois points d'un triplet rationnel aux trois points d'un autre triplet rationnel, on obtient neuf droites qui coupent C en neuf points formant un groupe rationnel. Si nous opérons ainsi sur les deux triplets rationnels

$$(u_1, u_2, u_3), \quad (u_1-3k', u_2-3k', u_3-3k'),$$

six de ces neuf points se confondent deux à deux, de sorte que notre groupe de neuf points se décompose en un triplet simple rationnel et un triplet double rationnel $(u_1+3k', u_2+3k', u_3+3k')$. (Attendu qu'un polynome à coefficients rationnels du neuvième degré, qui a trois racines doubles et trois racines simples, est le produit d'un polynome à coefficients rationnels du troisième degré et du carré d'un autre polynome à coefficients rationnels du troisième degré.)

Cela posé, on peut, comme au § V, construire une transformation Cremona rationnelle, dont les points-bases seront u_1+3k', u_2+3k', u_3+3k', ceux de la transformation inverse étant u_1-3k', u_2-3k', u_3-3k', qui transforme C en elle-même.

On devra donc avoir, d'après la formule (5),

$$3k' = p_1\beta_1 + \ldots + p_q\beta_q.$$

Les nombres entiers $p_1, \ldots, p_q$ peuvent-ils prendre des valeurs quelconques? Cela n'est pas certain. Tout ce que je puis affirmer, c'est que, si ces nombres peuvent prendre les valeurs p'_h et les valeurs p''_h, ils pourront prendre également les valeurs $p'_h + p''_h$, puisque l'existence de deux triplets dont la somme des arguments est $-3k'$ et $-3k''$ entraîne celle d'un autre triplet dont la somme des arguments est $-3k' - 3k''$.

On pourra donc donner aux nombres p toutes les valeurs compatibles avec un certain nombre de relations linéaires à coefficients entiers.

Il est clair qu'on peut remplacer les β par des combinaisons linéaires des β à coefficients entiers, le déterminant de ces coefficients étant égal à 1. On pourra alors choisir ces combinaisons linéaires de telle façon que quelques-uns des nombres p pourront prendre des valeurs quelconques, tandis que les autres devront être nuls. Si l'une des quantités β_s est égale à une période divisée par m_s, sans que l'entier m_s soit divisible par 3, on pourra donner à p_s une valeur quelconque, les autres p étant nuls. La condition nécessaire et suffisante pour que deux cubiques équivalentes (correspondant à deux systèmes p'_h et p''_h des entiers p) appartiennent à une même sous-classe, c'est que

$$p'_h \equiv p''_h \pmod 3,$$

sauf pour les entiers p_s qui correspondent à des quantités β_s égales à une période divisée par m_s, l'entier m_s n'étant pas divisible par 3.

Le nombre des sous-classes est alors une puissance de 3.

Si une cubique a des points rationnels compris dans la formule

$$\alpha + 3n\alpha + \Sigma p_s(\alpha - \alpha_s), \tag{6}$$

nous venons de voir que, pour les triplets rationnels, la somme des

arguments est donnée par la formule

$$3n\alpha + \Sigma p_s(\alpha - \alpha_s). \tag{7}$$

J'ajoute que pour les couples rationnels la somme des arguments sera donnée par la formule

$$2\alpha + 3n\alpha + \Sigma p_s(\alpha - \alpha_s), \tag{8}$$

car la droite qui joint les deux points d'un couple rationnel doit couper la cubique en un troisième point qui est rationnel, et, réciproquement, toute droite rationnelle passant par un point rationnel va passer par un couple rationnel.

Je dis plus généralement que la somme des arguments d'un groupe rationnel de K points est donnée par la formule (6), (7) ou (8) suivant que K est congru à 1, 0 ou 2 suivant le module 3.

En effet, si par exemple $K = 3j + 2$, je puis, d'une infinité de manières, trouver j triplets rationnels satisfaisant à la formule (7) et un couple rationnel satisfaisant à la formule (8); l'ensemble de ces points formera un groupe rationnel de K points satisfaisant à la formule (8).

Réciproquement, si l'on a un groupe rationnel de

$$K = 3j + \varepsilon \qquad (\varepsilon = 1, 2 \text{ ou } 0),$$

je dis que la somme des arguments sera donnée par la formule

$$\varepsilon\alpha + 3n\alpha + \Sigma p_s(\alpha - \alpha_s).$$

En effet par ces K points je puis faire passer une courbe rationnelle d'ordre $j + 1$; elle coupera en outre la cubique suivant $1 - \varepsilon$ points, qui formeront un groupe rationnel dont la somme des arguments devra être de la forme

$$-\varepsilon\alpha - 3n\alpha + \Sigma p_s(\alpha - \alpha_s).$$

Or la somme des arguments des $3j + 1 = K + (1 - \varepsilon)$ points d'intersection doit être nulle.

VII. — Extension du domaine de rationalité.

On peut évidemment répéter les mêmes raisonnements en considérant comme rationnelles, non seulement les quantités rationnelles proprement dites, mais toutes les quantités rationnelles d'un corps algébrique déterminé; ou en d'autres termes en *adjoignant* au domaine de rationalité les nombres algébriques qui forment la base de ce corps algébrique.

Rien ne sera changé à nos résultats, sauf ce qui suppose la *réalité* des nombres rationnels. C'est ainsi qu'on ne pourra plus appliquer ce que j'ai dit au paragraphe III sur les deux branches que peut avoir une cubique, sur la distribution des points rationnels sur ces deux branches et les conséquences qui en résultent pour la classification des cubiques.

D'autre part, nous ne pourrons plus toujours affirmer qu'une cubique ne peut admettre de transformation rationnelle impropre spéciale en elle-même. Mais ce ne sont là que des points de détail, et les résultats essentiels vont subsister.

L'importance de ces résultats se trouve accrue. Par exemple, nos théorèmes, sous leur forme primitive, n'avaient pas d'application à la cubique

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

puisqu'elle n'a que trois points rationnels que l'on aperçoit immédiatement. Après l'adjonction d'un certain corps algébrique au domaine de rationalité, il n'en sera plus de même, puisque cette cubique pourra avoir une infinité de points rationnels appartenant à ce corps.

Remarquons que deux cubiques, non équivalentes avant l'adjonction d'un ou plusieurs nombres algébriques, pourront devenir équivalentes après cette adjonction. En revanche, si elles sont équivalentes avant l'adjonction, elles le seront *a fortiori* après l'adjonction.

D'autre part, il peut se faire que deux cubiques équivalentes n'appartiennent pas à la même sous-classe avant l'adjonction et soient de la même sous-classe après cette adjonction.

Dans tous les cas, ces considérations pourront servir de base à de nouveaux critères relatifs à la classification des cubiques.

Soit par exemple k une constante quelconque, et considérons la transformation $(u, u+k)$ de la cubique en elle-même. Cette transformation ne sera pas en général rationnelle, mais elle le deviendra après adjonction d'un corps algébrique convenablement choisi. Ce corps dépendra de la cubique choisie et de la quantité k. Mais il sera le même pour une même quantité k et pour toutes les cubiques d'une même classe.

C'est donc un nouvel élément de la classification des cubiques.

VIII. — Cubiques dérivées.

Supposons d'abord qu'une cubique ait trois points d'inflexion en ligne droite rationnels.

Son équation pourra se mettre sous la forme

$$(1) \qquad A^3 = XYZ$$

A, X, Y et Z étant des polynomes du premier degré en x, y, z à coefficients entiers. Supposons que la cubique admette un point rationnel outre ses trois points d'inflexion, et soient A_0, X_0, Y_0, Z_0 les résultats des substitutions dans X, Y, Z des coordonnées x_0, y_0, z_0 de ce point. Nous pourrons toujours supposer que ces coordonnées sont des nombres entiers, premiers entre eux; de sorte que $A_0, X_0, Y_0; Z_0$ seront aussi des entiers.

Soit p un nombre qui divise à la fois X_0 et Y_0; il devra diviser aussi A_0. Comme les nombres x_0, y_0, z_0 sont premiers entre eux, le nombre p devra diviser le déterminant Δ'' des trois fonctions linéaires A, X, Y; car il divise évidemment $\Delta'' x_0, \Delta'' y_0$, et $\Delta'' z_0$.

Donc X_0 et Y_0 ne pourront avoir d'autres facteurs communs que ceux qui divisent Δ''. De même Y_0 et Z_0 ne pourront avoir d'autres facteurs communs que ceux qui divisent Δ, déterminant de A, Y, Z; tandis que X_0 et Z_0 ne pourront avoir d'autres facteurs communs que ceux qui divisent Δ', déterminant de A, X, Z.

Soit δ le plus grand commun diviseur de X_0, Y_0, Z_0; α celui de $\frac{Y_0}{\delta}$

et $\frac{Z_0}{\delta}$; β celui de $\frac{X_0}{\delta}$ et $\frac{Z_0}{\delta}$; γ celui de $\frac{X_0}{\delta}$ et $\frac{Y_0}{\delta}$; α, β et γ seront premiers entre eux deux à deux. X_0 sera divisible par $\beta\gamma\delta$, Y_0 par $\alpha\gamma\delta$, Z_0 par $\alpha\beta\delta$. Soit

$$X_0 = a\beta\gamma\delta, \qquad Y_0 = b\alpha\gamma\delta, \qquad Z_0 = c\alpha\beta\delta.$$

On voit que $b\alpha$ est premier avec $a\beta$, $c\beta$ avec $b\gamma$, $a\gamma$ avec $c\alpha$; et par conséquent les nombres a, b, c sont premiers deux à deux; a premier avec α, b avec β, c avec γ.

Il vient alors

$$\Lambda_0^3 = abc(\alpha\beta\gamma)^2\delta^3.$$

Soient μ_1 le plus grand commun diviseur de a et $\alpha\beta\gamma$; μ_2 celui de b et $\alpha\beta\gamma$; μ^3 celui de c et $\alpha\beta\gamma$. Comme a, b, c sont premiers entre eux deux à deux, il en sera de même de μ_1, μ_2, μ_3 d'une part; de $\frac{a}{\mu_1}, \frac{b}{\mu_2}, \frac{c}{\mu_3}$ d'autre part. Il en résulte d'abord que $\alpha\beta\gamma$ est divisible par $\mu_1\mu_2\mu_3$, de sorte qu'on peut écrire

$$\Lambda_3^0 = \delta^3(\mu_1\mu_2\mu_3)^3\left(\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}\right)^2\frac{a}{\mu_1}\frac{b}{\mu_2}\frac{c}{\mu_3}.$$

Le produit

$$\left(\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}\right)^2\frac{a}{\mu_1}\frac{b}{\mu_2}\frac{c}{\mu_3}$$

est donc un cube parfait, et, comme les facteurs de ce produit sont premiers deux à deux, chacun des facteurs

$$\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}, \quad \frac{a}{\mu_1}, \quad \frac{b}{\mu_2}, \quad \frac{c}{\mu_3}$$

devra être un cube parfait.

Soient

$$\omega^3, \quad \xi_0^3, \quad \eta_0^3, \quad \zeta_0^3$$

ces quatre cubes; il viendra

$$X_0 = \xi_0^3\mu_1\beta\gamma\delta, \qquad Y_0 = \eta_0^3\mu_2\alpha\gamma\delta, \qquad Z_0 = \zeta_0^3\mu_3\alpha\beta\delta,$$

$$\Lambda_0 = \delta\mu_1\mu_2\mu_3\omega\xi_0\eta_0\zeta_0,$$

ce que je puis écrire

$$X_0 = h_1 \xi_0^3, \qquad Y_0 = h_2 \eta_0^3, \qquad Z_0 = h_3 \zeta_0^3, \qquad A_0 = k \xi_0 \eta_0 \zeta_0,$$

les coefficients h et k étant des entiers. Remarquons que ces entiers sont limités.

En effet α, β, γ doivent diviser respectivement Δ, Δ', Δ'', qui sont des entiers donnés; δ doit diviser ces trois déterminants; μ_1, μ_2, μ_3 doivent diviser $\alpha\beta\gamma$.

Donc tous ces entiers sont limités ainsi que les entiers

$$\omega, \quad h_1, \quad h_2, \quad h_3, \quad k. \qquad \text{C. Q. F. D.}$$

On ne peut donc faire au sujet de ces coefficients qu'un nombre fini d'hypothèses.

Posons alors

$$X = h_1 \xi^3, \qquad Y = h_2 \eta^3, \qquad Z = h_3 \zeta^3, \qquad A = k \xi \eta \zeta$$

et éliminons x, y, z entre ces quatre équations; nous aurons entre ξ^3, η^3, ζ^3, $\xi\eta\zeta$ une relation linéaire et homogène à coefficients entiers. C'est l'équation d'une cubique rationnelle C′ sur laquelle doit se trouver le point ξ, η, ζ. Je dirai que C′ est une cubique *dérivée* de C.

D'après ce qui précède, C n'aura qu'un nombre fini de dérivées puisqu'on ne peut faire sur les entiers h et k qu'un nombre fini d'hypothèses.

Le point ξ_0, η_0, ξ_0 sera un point rationnel de C′.

On voit ainsi qu'à chaque point rationnel de C correspond un point rationnel d'une de ses dérivées. Si donc C a une infinité de points rationnels, il en sera de même d'une au moins de ses dérivées.

Voyons quelle relation il y a entre les deux cubiques C et C′.

A chaque point de C′ correspond un seul point de C; à chaque point de C correspondront trois valeurs des rapports $\frac{\zeta}{\xi}$, $\frac{\eta}{\xi}$ et par conséquent trois points de C′. Ces trois points auront pour coordonnées

$$\xi, \eta, \zeta; \quad \alpha\xi, \alpha^2\eta, \zeta; \quad \alpha^2\xi, \alpha\eta, \zeta,$$

α étant une racine cubique de l'unité. Soient M_1, M_2, M_3 ces trois points; u_1, u_2, u_3 leurs arguments.

Considérons en particulier les trois points d'inflexion de C qui sont donnés par les équations

$$X = A = 0, \qquad Y = A = 0, \qquad Z = A = 0$$

qui ont pour arguments 0, $\frac{\omega}{3}$, $\frac{2\omega}{3}$, et que j'appelle J_1, J_2, J_3.

A ces trois points correspondront sur C′ les neuf points d'inflexion situés sur les trois droites $\xi = 0$, $\eta = 0$, $\zeta = 0$ et qui auront pour arguments

$$\frac{m\omega_1 + n\omega_1'}{3},$$

où ω_1 et ω_1' sont les périodes relatives à C′, m et n des entiers.

La courbe C′ n'est pas altérée quand on change ξ, η, ζ en $\alpha\xi$, $\alpha^2\eta$, ζ. Ce ne saurait être là une transformation impropre; car une transformation impropre a des points doubles sur la cubique elle-même et les trois points doubles de cette transformation sont $\xi = \eta = 0$, $\xi = \zeta = 0$, $\eta = \zeta = 0$ et ne sont pas sur la cubique. C'est donc une transformation de la forme $(u, u + k)$, et comme, après trois transformations, on revient au point primitif, il faut que k soit $\frac{1}{3}$ de période.

Si u est l'argument d'un point de C′ et v l'argument du point correspondant de C, v sera une fonction uniforme de u, car, si u décrit un petit contour dans son plan, v revient à sa valeur primitive. De même, si v décrit un petit contour dans son plan, les trois valeurs de ξ, η, ζ et, par conséquent, les trois valeurs de u ne peuvent s'échanger, puisque les points doubles $\xi = \eta = 0$, $\xi = \zeta = 0$, $\eta = \zeta = 0$ (pour lesquels deux des trois systèmes de valeurs de ξ, η, ζ se confondraient) n'appartiennent pas à la cubique C′. Donc u est fonction uniforme de v, et, comme v est fini quand u est fini et réciproquement, il doit y avoir entre u et v une relation linéaire.

Quand u augmente de k ou d'une période, v doit augmenter d'une période et, réciproquement, quand v augmente d'une période, u doit augmenter de k ou d'une période.

Soient $0, \frac{\omega'_1}{3}, \frac{2\omega'_1}{3}$ les arguments des trois points d'inflexion $\xi = 0$; $\frac{\omega_1}{3}, \frac{\omega_1+\omega'_1}{3}, \frac{\omega_1+2\omega'_1}{3}$ ceux des trois points d'inflexion $\eta = 0$; $\frac{2\omega_1}{3}, \frac{2\omega_1+\omega'_1}{3}, \frac{2\omega_1+2\omega'_1}{3}$ ceux des trois points d'inflexion $\zeta = 0$. Je vois tout de suite que

$$k = \frac{\omega'_1}{3},$$

car les trois points $\xi = 0$ se transforment les uns dans les autres par la transformation $(u, u+k)$. Soit

$$v = au + b.$$

D'après ce que nous venons de voir $a\omega_1$ et $\frac{a\omega'_1}{3}$ doivent être des combinaisons linéaires à coefficients entiers de ω et ω', et réciproquement, de sorte qu'on aura

$$a\omega_1 = m\omega + n\omega',$$
$$a\frac{\omega'_1}{3} = m_1\omega + n_1\omega',$$

m, n, m_1, n_1 étant des entiers tels que $mn_1 - nm_1 = 1$.

Nous pouvons toujours supposer $a = 1$, car les périodes de C (ou de C') ne sont définies qu'à un facteur constant près.

Pour $u = 0, \frac{\omega_1}{3}, \frac{2\omega'_1}{3}$, nous devons avoir

$$v = 0, \qquad \text{à une période près.}$$

Pour $u = \frac{\omega_1}{2}, \frac{\omega_1+\omega'_1}{3}, \frac{\omega_1+2\omega'_1}{3}$, nous devons avoir

$$v = \frac{\omega}{3}, \qquad \text{à une période près.}$$

Pour $u = \frac{2\omega_1}{3}, \frac{\omega_1+\omega'_1}{3}, \frac{2\omega_1+2\omega'_1}{3}$, nous devons avoir

$$v = \frac{2\omega}{3}, \qquad \text{à une période près.}$$

Nous en concluons d'abord que b doit être égal à une période et, par conséquent, que nous pouvons supposer cette constante nulle sans restreindre la généralité, ensuite que $\frac{\omega}{3}$ est égal à $\frac{\omega_1}{3}$, à une période de C près, ou, ce qui revient au même, que $\frac{\omega}{3}$ est le tiers d'une période de C'. Cette période, nous pouvons toujours l'appeler ω_1, de sorte que nous aurons $\omega = \omega_1$.

Enfin $k = \frac{\omega'_1}{3}$ doit être une période de C formant un système primitif avec ω; je l'appelle ω'; on a donc finalement

$$v = u, \qquad \omega = \omega_1, \qquad \omega' = \frac{\omega'_1}{3}.$$

De sorte que les fonctions elliptiques relatives à C' se déduisent de celles qui sont relatives à C par une transformation du troisième ordre.

Tous ces résultats ne s'appliquent qu'au cas où trois points d'inflexion de C sont rationnels. Cherchons à les généraliser.

Nous n'avons pour cela qu'à adjoindre au domaine de rationalité les coordonnées de trois points d'inflexion en ligne droite. L'équation de la cubique prendra la forme

$$XYZ = A^3, \tag{1 bis}$$

où X, Y, Z, A sont des polynomes du premier degré dont les coefficients sont des entiers du corps algébrique constitué par cette adjonction.

Considérons un point rationnel de notre cubique (soit rationnel proprement dit, soit devenu rationnel par l'adjonction). Soient x_0, y_0, z_0 les coordonnées de ce point; nous pourrons supposer que ce sont des entiers du corps algébrique.

Mais ici une première difficulté se présente : avons-nous le droit de supposer que ces entiers algébriques sont premiers entre eux? Il va sans dire que tous ces mots d'*entiers algébriques premiers entre eux*, de *divisibilité*, etc., doivent s'entendre dans le sens de la théorie des idéaux.

Si alors les nombres x_0, y_0, z_0 ont pour diviseur commun un nombre algébrique existant, c'est-à-dire un idéal principal, on pourra faire disparaître ce facteur commun sans altérer les rapports de ces trois quantités. Mais si x_0, y_0, z_0 ont pour diviseur commun un idéal non principal, on ne pourra pas faire la division, parce que les quotients ne seraient plus des nombres algébriques existants.

Soient alors J le plus grand commun diviseur de x_0, y_0, z_0 et J′ un idéal de la même classe. Il existe toujours deux entiers algébriques existants E et E′ tels que

$$EJ = E'J'.$$

Alors x_0E, y_0E, z_0E auront pour plus grand commun diviseur $EJ = E'J'$ et

$$\frac{x_0E}{E'}, \quad \frac{y_0E}{E'}, \quad \frac{z_0E}{E'}$$

seront trois entiers algébriques existants dont le plus grand commun diviseur sera J′.

On peut donc toujours remplacer les trois entiers algébriques dont le plus grand commun diviseur était J par trois autres dont le plus grand commun diviseur sera J′.

Comme il n'y a qu'un nombre fini de classes d'idéaux, on peut choisir un nombre fini d'idéaux J′ que j'appellerai *idéaux types*, de façon qu'il y en ait un, et un seul, dans chaque classe.

On ne peut pas toujours supposer que x_0, y_0, z_0 sont premiers entre eux, mais on peut supposer que leur plus grand commun diviseur est un idéal type.

J'ajoute que, si x_0, y_0, z_0 sont des *entiers rationnels ordinaires*, on peut supposer qu'ils sont premiers entre eux, car le plus grand commun diviseur de deux ou plusieurs entiers rationnels ordinaires est un entier rationnel ordinaire.

Soient A_0, X_0, Y_0, Z_0 le résultat de la substitution de x_0, y_0, z_0 dans A, X, Y, Z.

Si j'appelle encore $\Delta, \Delta', \Delta''$ les trois déterminants des quatre fonctions linéaires A, X, Y, Z, le plus grand commun diviseur de X_0 et Y_0 divisera $\Delta''J$, J étant le plus grand commun diviseur de x_0, y_0, z_0; d'où il suit encore que nous ne pouvons faire, au sujet de ce plus grand

commun diviseur, qu'un nombre fini d'hypothèses; il en sera de même pour le plus grand commun diviseur de X_0 et Z_0 ou de Y_0 et Z_0.

Nous ne pourrons donc faire qu'un nombre fini d'hypothèses sur les plus grands communs diviseurs de X_0, Y_0, Z_0 (que j'appelle δ), de $\frac{Y_0}{\delta}$ et $\frac{Z_0}{\delta}$, de $\frac{X_0}{\delta}$ et $\frac{Z_0}{\delta}$, de $\frac{X_0}{\delta}$ et $\frac{Y_0}{\delta}$ (que j'appelle α, β, γ). Ces diviseurs α, β, γ, δ sont des idéaux du corps algébrique considéré.

J'aurai encore

$$X_0 = a\beta\gamma\delta, \qquad Y_0 = b\alpha\gamma\delta, \qquad Z_0 = c\alpha\beta\delta,$$

a, b, c étant des idéaux du corps. Les idéaux a, b, c sont premiers entre eux deux à deux; a premier avec α, b avec β, c avec γ, et l'on a

$$A_0^3 = abc(\alpha\beta\gamma)^2\delta^3.$$

Il suit de cette égalité que, si l'on définit μ_1, μ_2, μ_3 comme plus haut, les expressions

$$\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}, \quad \frac{a}{\mu_1}, \quad \frac{b}{\mu_2}, \quad \frac{c}{\mu_3}$$

seront des cubes parfaits; mais je ne veux pas dire par là que ce sont les cubes d'entiers algébriques existants, mais les cubes d'idéaux du corps.

Soient alors λ_1, λ_2, λ_3 les idéaux types appartenant aux mêmes classes que

$$\sqrt[3]{\frac{a}{\mu_1}}, \quad \sqrt[3]{\frac{b}{\mu_2}}, \quad \sqrt[3]{\frac{c}{\mu_3}};$$

comme le nombre des classes est fini, on ne peut faire, au sujet des idéaux λ, qu'un nombre fini d'hypothèses.

Nous pourrons alors poser

$$\sqrt[3]{\frac{a}{\mu_1}} = \lambda_1\xi_0, \qquad \sqrt[3]{\frac{b}{\mu_2}} = \lambda_2\eta_0, \qquad \sqrt[3]{\frac{c}{\mu_3}} = \lambda_3\zeta_0,$$

et ξ_0, η_0, ζ_0 seront des nombres *rationnels* (qui ne seront peut-être pas entiers) du corps algébrique considéré.

Il vient alors

$$X_0 = h_1 \xi_0^3, \qquad Y_0 = h_2 \eta_0^3, \qquad Z_0 = h_3 \zeta_0^3, \qquad A_0 = h \xi_0 \eta_0 \zeta_0,$$

où

$$h_1 = \lambda_1^3 \mu_1 \beta\gamma\delta, \qquad h_2 = \lambda_2^3 \mu_2 \alpha\gamma\delta, \qquad h_3 = \lambda_3^3 \mu_3 \alpha\beta\delta,$$

$$k = \delta \mu_1 \mu_2 \mu_3 \sqrt[3]{\frac{\alpha\beta\gamma}{\mu_1 \mu_2 \mu_3}},$$

où les h et k seront des entiers du corps sur lesquels on ne pourra faire qu'un nombre fini d'hypothèses, puisqu'on n'en peut faire qu'un nombre fini sur les idéaux δ, α, β, γ, μ, λ.

Si le point x_0, y_0, z_0 est sur la cubique C, le point ξ_0, η_0, ζ_0 sera sur une cubique C′ que j'appellerai encore *dérivée de* C.

Nos théorèmes subsistent évidemment.

Une cubique C n'a qu'un nombre fini de dérivées, puisqu'on ne peut faire qu'un nombre fini d'hypothèses sur les coefficients h et k.

A tout point rationnel de C correspond sur l'une de ses dérivées un point rationnel, de sorte que si C a une infinité de points rationnels, il doit en être de même pour une au moins de ses dérivées.

Les fonctions elliptiques relatives à la dérivée se déduisent de celles de la cubique C par une transformation de troisième ordre.

On peut quelquefois tirer de là des résultats dans l'énoncé desquels n'interviennent que des entiers ordinaires. C'est ce qui arrive, par exemple, si l'un des trois points d'inflexion est rationnel ordinaire.

Si le point $X = A = 0$, que j'appelle M, est rationnel ordinaire, par ce point M passeront quatre droites qui contiendront chacune deux autres points d'inflexion. Soient

$$A_1 = 0, \qquad A_2 = 0, \qquad A_3 = 0, \qquad A_4 = 0$$

ces quatre droites. Si nous adjoignons au domaine de rationalité les coefficients de A_1, nous définirons un certain corps algébrique K_1.

Soient maintenant $Y_1 = 0$, $Z_1 = 0$ les deux tangentes d'inflexion aux points de rencontre de la cubique avec $A_1 = 0$.

Adjoignons au domaine de rationalité les coordonnées des deux points d'inflexion correspondants; nous définirons un nouveau corps

algébrique K'_1 qui contiendra K_1, et nous pourrons supposer que l'équation de la cubique s'écrit

$$XY_1Z_1 = A_1^3,$$

les coefficients de X étant des entiers ordinaires, ceux de Y_1 et de Z_1 des entiers du corps K'_1, ceux de A_1 des entiers du corps K_1.

Si x_0, y_0, z_0 est un point rationnel ordinaire de la cubique C et que x_0, y_0, z_0 soient des entiers premiers entre eux ; si X_0, Y_1^0, Z_1^0, A_1^0 sont les résultats de la substitution de x_0, y_0, z_0 ; on aura d'après ce qui précède

$$X_0 = h_1\xi_0^3, \qquad Y_1^0 = h_2\eta_0^3, \qquad Z_1^0 = h_3\zeta_0^3, \qquad A_1^0 = k\xi_0\eta_0\zeta_0;$$

les quantités qui figurent dans les seconds membres de ces équations sont des quantités rationnelles du corps K'_1. Mais nous devons observer que, si l'on échange les deux points d'inflexion $Y_1 = 0$, $Z_1 = 0$, toute quantité rationnelle du corps K'_1 se transformera en une autre quantité rationnelle du même corps que l'on appellera sa *conjuguée;* toute fonction symétrique et rationnelle de deux quantités conjuguées sera une quantité rationnelle du corps K_1.

Nous concluons que h_1, ξ_0 et k sont des quantités rationnelles du corps K_1, tandis que h_2 et h_3, η_0 et ζ_0 sont conjugués.

Cela posé, si l'on permute les quatre droites A_1, A_2, A_3, A_4, le corps K_1 se changera dans l'un des trois corps conjugués K_2, K_3, K_4.

Soient $h_{1.2}$, $h_{1.3}$, $h_{1.4}$ les quantités qui se déduisent de h_1 quand on remplace le corps K_1 par l'un des corps conjugués K_2, K_3, K_4. Ce seront des entiers algébriques de ces trois corps, de même que h_1 était un entier algébrique du corps K_1.

Soient de même $\xi_{0.2}$, $\xi_{0.3}$, $\xi_{0.4}$ les quantités qui se déduisent de ξ_0 par le même procédé. Ce seront des quantités rationnelles des trois corps K_2, K_3, K_4, de même que ξ_0 était une quantité rationnelle du corps K_1.

Sur les entiers algébriques $h_{1.2}$, $h_{1.3}$, $h_{1.4}$ on ne pourra faire qu'un nombre fini d'hypothèses.

X_0 étant un entier ordinaire, on aura

$$X_0 = h_1\xi_0^3, \qquad X_0 = h_{1.2}\xi_{0.2}^3, \qquad X_0 = h_{1.3}\xi_{0.3}^3, \qquad X_0 = h_{1.4}\xi_{0.4}^3,$$

les trois dernières égalités se déduisant de la première en passant du corps K_1 à l'un des corps conjugués. Si donc on pose

$$h_1 h_{1.2} h_{1.3} h_{1.4} = H, \qquad \xi_0 \xi_{0.2} \xi_{0.3} \xi_{0.4} = U,$$

il viendra

$$X_0^4 = HU^3$$

ou

$$X_0 = H\left(\frac{U}{X_0}\right)^3.$$

H est un entier ordinaire, puisque h_1, $h_{1.2}$, $h_{1.3}$, $h_{1.4}$ sont conjugués. De même, U est une fonction rationnelle ordinaire.

Comme on ne peut faire sur l'entier H qu'un nombre fini d'hypothèses, nous devons conclure que X_0 est égal à un cube parfait multiplié par un entier limité.

Cet énoncé suppose que les entiers x_0, y_0, z_0 sont premiers entre eux. Si l'on s'affranchit de cette restriction, il faudra dire que X_0 est égal à un cube parfait multiplié par le plus grand commun diviseur de x_0, y_0 et z_0 et par un entier limité. On appréciera mieux la généralité de cet énoncé si l'on se rappelle qu'une cubique qui a un point rationnel est toujours équivalente à une cubique qui a un point d'inflexion rationnel.

Pour généraliser nos résultats, nous pouvons encore chercher à mettre l'équation de la cubique sous la forme

$$(1\ ter) \qquad X_1 X_2 \ldots X_p = Y^n,$$

X_1, X_2, ..., X_p, Y étant des polynomes entiers à coefficients entiers. Je m'impose d'abord la condition que deux quelconques des courbes

$$X_i = 0, \qquad X_k = 0$$

n'aient aucun point commun sur la cubique.

Soient alors

$$u_i^{(1)}, \quad u_i^{(2)}, \quad \ldots, \quad u_i^{(q)}$$

les arguments des points d'intersection de la cubique avec $X_i = 0$;

$$v_1, \quad v_2, \quad \ldots, \quad v_m,$$

les arguments des points d'intersection de la cubique avec $Y = 0$.

On aura, à des périodes près,

$$\Sigma u_i = 0, \qquad \Sigma v = 0.$$

L'ensemble des points u devra reproduire n fois l'ensemble des points v. Chacun des points v devra figurer n fois dans l'ensemble des points u, et, comme l'ensemble des points u_i ne doit avoir aucun point commun avec l'ensemble des points u_k, chaque point v devra figurer n fois dans un des ensembles u_i. Il suit de là que les points u_i doivent être confondus n à n, et l'ordre de multiplicité de l'un quelconque d'entre eux doit être un multiple de n.

Considérons alors un ensemble d'arguments

$$w_i^{(1)}, \quad w_i^{(2)}, \quad \ldots, \quad w_i^{(s)} \quad \left(s = \frac{q}{n}\right),$$

qui seront les mêmes que les arguments u_i avec cette différence que leurs ordres de multiplicité seront n fois plus petits. Alors Σw_i est la $n^{\text{ième}}$ partie d'une période. D'ailleurs l'ensemble de tous les points w est identique à l'ensemble des points v.

Le problème revient donc à chercher p groupes rationnels; la somme des arguments de chaque groupe étant la $n^{\text{ième}}$ partie d'une période, la somme des arguments de tous les groupes étant une période. J'ajoute que le nombre des points de tous les groupes doit être divisible par 3 et qu'il en est de même du nombre des points de chaque groupe, à moins que n ne soit divisible par 3.

Réciproquement, si ces conditions sont remplies, on pourra mettre l'équation sous la forme (1 *ter*). On pourra trouver en effet un polynome X_i qui ait un zéro d'ordre n en chacun des points w_i et un polynome Y qui ait un zéro simple en chacun des points v_i. Considérons alors le rapport

$$\frac{Y^n}{X_1 X_2 \ldots X_p}.$$

Ce sera une fonction doublement périodique de l'argument elliptique d'un point de la cubique, et cette fonction ne deviendra jamais infinie; ce sera donc une constante que nous pourrons supposer égale à 1.

Soit x_0, y_0, z_0 un point rationnel de C. Pour plus de simplicité, j'entendrai de nouveau le mot *rationnel* dans le sens ordinaire; il serait d'ailleurs facile de généraliser pour un corps algébrique quelconque. Je pourrai donc supposer que x_0, y_0, z_0 sont des entiers premiers entre eux, et j'appellerai X_i^0 et Y_0 le résultat de la substitution de ces entiers dans X_i et Y. On aura alors

$$X_1^0 X_2^0 \dots X_p^0 = Y_0^n.$$

Le plus grand commun diviseur de X_1^0 et X_2^0 (qui sont des entiers) devra diviser Y_0, et par hypothèse les trois courbes $X_1 = 0$, $X_2 = 0$, $Y = 0$ n'ont aucun point commun.

Il en résulte évidemment qu'en appelant Δ le résultant de X_1, X_2, Y, il existe neuf polynomes P à coefficients entiers, tels que l'on ait identiquement

$$P_1 X_1 + P_2 X_2 + P_3 Y = \Delta x^q,$$
$$P_1' X_1 + P_2' X_2 + P_3' Y = \Delta y^q,$$
$$P_1'' X_1 + P_2'' X_2 + P_3'' Y = \Delta z^q,$$

q étant un exposant entier convenable. D'où il suit que le plus grand commun diviseur de X_1^0, X_2^0, Y_0 doit diviser à la fois Δx_0^q, Δy_0^q, Δz_0^q et par conséquent Δ.

On ne peut donc faire sur les diviseurs communs des X_i^0 et de Y_0 qu'un nombre fini d'hypothèses.

Par un raisonnement tout à fait pareil à celui qui précède, on en déduirait

$$X_1^0 = h_1 (\xi_1^0)^n, \qquad X_2^0 = h_2 (\xi_2^0)^n,$$
$$\dots\dots\dots\dots, \qquad \dots\dots\dots\dots,$$
$$X_p^0 = h_p (\xi_p^0)^n, \qquad Y_0 = k \xi_1^0 \xi_2^0 \dots \xi_p^0,$$

les h et k étant des entiers sur lesquels on ne peut faire qu'un nombre fini d'hypothèses, et les ξ_i^0 étant des entiers.

Nous sommes ainsi amenés à nous poser la question suivante :

Si l'on pose

$$X_i = h_i \xi_i^n, \qquad Y = k \xi_1 \xi_2 \dots \xi_p, \tag{2}$$

quel sera le lieu du point $\xi_1, \xi_2, \ldots, \xi_p$ dans l'espace à p dimensions quand le point x, y, z décrira la cubique C?

Les points rationnels de ce lieu correspondront aux points rationnels de C, de sorte que ce lieu jouera un rôle analogue à celui de la cubique dérivée C'.

Soient u l'argument elliptique sur C, ω et ω' les périodes; soit $\theta(u)$ une fonction θ définie de telle sorte que

$$\theta(0) = 0, \qquad \theta(u+\omega) = \theta(u),$$
$$\theta(u+\omega') = e^{au+b}\theta(u), \qquad a = \frac{2i\pi}{\omega}.$$

Soient λ_i le degré de X_i et

$$\Theta_i(u) = \theta(u - w_i^{(1)})\theta(u - w_i^{(2)})\ldots\theta(u - w_i^{(s)}) \qquad \left(s = \frac{3\lambda_i}{n}\right).$$

Soient $\alpha_1, \alpha_2, \alpha_3$ les arguments des points d'intersection de la cubique avec $x = 0$. Soit

$$\tau_i = \theta(u - \alpha_1)\theta(u - \alpha_2)\theta(u - \alpha_3).$$

Les expressions

$$\frac{X_i}{\Theta_i^n}\left(\frac{x}{\tau_i}\right)^{-\lambda_i}, \qquad \frac{Y}{\theta_1\theta_2\ldots\theta_p}\left(\frac{x}{\tau_i}\right)^{-q}$$

$\left(\text{où } q = \frac{\Sigma\lambda_i}{n} \text{ est le degré de } \lambda\right)$ sont des fonctions doublement périodiques de seconde espèce (se reproduisant à un facteur constant près par l'addition d'une période) qui ne deviennent jamais infinies. Elles se réduisent donc à des exponentielles, de sorte que l'équation de la cubique pourra s'écrire

$$X_i = \mu_i\Theta_i^n\left(\frac{x}{\tau_i}\right)^{\lambda_i} e^{n\rho_i u}, \qquad Y = \mu_{p+1}\Theta_1\Theta_2\ldots\Theta_p\left(\frac{x}{\eta}\right)^q e^{\rho u},$$

les μ et les ρ étant des constantes, ou bien encore

$$\xi_i = \nu_i\Theta_i\left(\frac{x}{\tau_i}\right)^{\frac{\lambda_i}{n}} e^{\rho_i u},$$

les ν étant des constantes.

Si les λ_i sont tous égaux, c'est là l'équation en coordonnées homogènes d'une courbe de genre 1 dans l'espace à $p-1$ dimensions. Quel est le degré de cette courbe et quelles sont les périodes correspondantes?

On a

$$\Theta_i(u+\omega)=\Theta_i(u); \qquad \Theta_i(u+\omega')=e^{a'u+b'-a\Sigma w_i}\Theta_i(u),$$

$$\Theta_i(u+h\omega')=e^{a''u+b''-ah\Sigma w_i}\Theta_i(u),$$

$$a'=\frac{3\lambda_i}{n}a, \qquad b'=\frac{3\lambda_i}{n}b; \qquad a''=ha', \qquad b''=hb'+a'\omega'\frac{h(h-1)}{2}.$$

Quand u augmente de ω, les quantités X_i, γ_i, Θ_i et x ne changent pas. Donc $e^{n\rho_i u}$ ne change pas. Quand u augmente de ω', les quantités X_i, x ne changent pas; Θ_i et γ_i sont multipliés par

$$e^{a'u+b'-a\Sigma w_i}, \qquad e^{3au+3b}.$$

Donc $e^{n\rho_i u}$ est multiplié par

$$e^{na\Sigma w_i}.$$

Donc $n\rho_i\omega$ est un multiple de $2i\pi$, $n\rho_i\omega'$ est égal à $na\Sigma w_i$ à un multiple près de $2i\pi$. Nous avons dit que Σw_i est le $n^{ième}$ d'une période. On a donc

$$n\Sigma w_i=\beta_i\omega+\beta'_i\omega',$$

β_i et β'_i étant des entiers. Il vient alors

$$\rho_i=\frac{2i\pi\beta'_i}{n}.$$

On a d'ailleurs

$$\rho=\Sigma\rho_i.$$

Quand u augmente de ω ou de ω', le logarithme de $\Theta_i e^{\rho_i u}$ augmente de

$$\frac{2i\pi\beta'_i}{n}+a'u+b'-a\Sigma w_i+\frac{2i\pi\beta'_i\omega'}{n\omega'}=a'u+b'-\frac{2i\pi\beta_i}{n}.$$

Il suit de là que les rapports des ξ_i sont des fonctions doublement

périodiques de u, dont les périodes dépendent des entiers β_i et β'_i, ou plutôt des restes de ces entiers à n. Ces fonctions admettront la période

$$\gamma\omega + \gamma'\omega',$$

pourvu que tous les $\gamma\beta_i + \gamma'\beta'_i$ donnent le même reste à n.

Il est aisé ainsi de déterminer ces périodes et l'on en déduit aisément le degré de notre courbe de genre 1, que nous pourrons appeler encore une *courbe dérivée de* C.

On voit que le nombre des courbes dérivées est encore fini, qu'à tout point rationnel de C correspond un point rationnel de l'une des dérivées et que les fonctions elliptiques relatives à une dérivée se déduisent de celles relatives à C par une transformation.

Toute courbe dérivée admettant un point rationnel étant équivalente à une cubique, comme on l'a vu au paragraphe IV, si la cubique C admet une infinité de points rationnels, on aura ainsi le moyen de définir un certain nombre d'autres cubiques (dont les fonctions elliptiques se déduisent de celles de C par une transformation) et sur l'une au moins desquelles il y aura une infinité de points rationnels.

Ne supposons plus que tous les λ_i soient égaux.

Nous pourrons trouver p^2 entiers β_{ik} et γ_i, dont le déterminant soit égal à 1 et tels que

$$\Sigma\beta_{ik}\lambda_i = 0, \qquad \Sigma\gamma_i\lambda_i = \delta,$$

δ étant le plus grand commun diviseur des λ_i.

Alors les produits

$$Z_k = \Pi\xi_i^{\beta_{ik}} = \Pi(\nu_i\Theta_i e^{\theta_i u})^{\beta_{ik}}$$

seront des fonctions doublement périodiques de u dont les périodes se détermineraient comme nous venons de le faire. Alors les $p-1$ quantités Z_k seront les coordonnées non homogènes d'un point décrivant une courbe de genre 1 dans l'espace à $p-1$ dimensions. Cette courbe pourra s'appeler encore une *courbe dérivée de* C, et ces courbes dérivées de C jouiront encore des mêmes propriétés que dans les cas examinés jusqu'ici.

On peut poser, par exemple,

$$Z'_k = \xi_k (\Pi \xi_i^{\gamma_i})^{-\frac{\lambda_k}{\mu}},$$

et Z'_k sera encore doublement périodique. (Inutile d'ajouter que ces résultats deviennent illusoires pour $p = 2$.)

Il n'y aurait rien à changer à ce qui précède si, au lieu de l'équation (1 *ter*), on partait d'une équation analogue

$$(1\,d) \qquad X_1^{q_1} X_2^{q_2} \dots X_p^{q_n} = Y^n,$$

où les q seraient des entiers quelconques. Ici encore on ne peut faire qu'un nombre fini d'hypothèses sur les diviseurs communs de X_1^0 et X_2^0 quand x_0, y_0, z_0 sont premiers entre eux. Il en résulte que X_k^0 (si q_k est premier avec n) sera une puissance $n^{\text{ième}}$ parfaite à un facteur constant près sur lequel on ne peut faire qu'un nombre fini d'hypothèses.

Voyons maintenant dans quels cas on pourra avoir une équation de la forme (1 *ter*).

Supposons que $\frac{3\lambda_i}{n}$ soit un multiple de 3 plus ε_i ($\varepsilon_i = 0, 1, 2$). Alors le groupe des points w_i étant rationnel, on devra avoir, d'après ce que nous avons vu à la fin du paragraphe VI,

$$(3) \qquad \Sigma w_i = \varepsilon_i \alpha + 3 n_i \alpha + \Sigma p_s (\alpha - \alpha_s).$$

Cette expression devra être la $n^{\text{ième}}$ partie d'une période, c'est-à-dire que l'argument d'un des points rationnels (à savoir le point Σw_i, si $\varepsilon_i = 1$, et le point $2\Sigma w_i$, si $\varepsilon_i = 2$) ou la différence des arguments de deux points rationnels (à savoir Σw_i, si $\varepsilon_i = 0$), devra être la $n^{\text{ième}}$ partie d'une période. Cette condition est d'ailleurs évidemment suffisante.

En effet, si par exemple

$$\alpha = \frac{\omega}{n},$$

nous pourrons trouver trois groupes rationnels Σw_1, Σw_2, Σw_3, tels

que

$$\Sigma w_1 = q_1 \alpha, \qquad \Sigma w_2 = q_2 \alpha, \qquad \Sigma w_3 = q_3 \alpha,$$

tels que $q_1 + q_2 + q_3 \equiv 0 \pmod{n}$ et que $\frac{3\lambda_i}{n} \equiv q_i \pmod 3$.

Si n n'est pas divisible par 3, q_i devra être divisible par 3; nous pourrons alors supposer $\lambda_1 = \lambda_2 = \lambda_3$. Si n est divisible par 3, nous pourrons encore prendre

$$q_1 = q_2 = q_3 \pmod 3,$$

puisqu'on aura

$$q_1 + q_2 + q_3 = 0 \pmod 3.$$

Si nous avions

$$3\alpha = \frac{\omega}{n},$$

nous prendrions encore

$$\Sigma w_1 = q_1 \alpha, \qquad \Sigma w_2 = q_2 \alpha, \qquad \Sigma w_3 = q_3 \alpha :$$

$$q_1 + q_2 + q_3 \equiv 0 \pmod{3n}, \qquad q_1 = q_2 = q_3 \equiv 0 \pmod 3.$$

$$\lambda_1 = \lambda_2 = \lambda_3, \qquad \frac{3\lambda_i}{n} \equiv 0 \pmod 3.$$

Je distinguerai deux cas :

1° Ou bien la différence des arguments de deux points rationnels est le $n^{ième}$ d'une période. Dans ce cas, *la considération des courbes dérivées nous apprend réellement quelque chose de nouveau.*

Si cette condition est remplie par une cubique, elle le sera par toutes les cubiques équivalentes; mais, en général, elle ne le sera pas par C, ni, par conséquent, par aucune des cubiques équivalentes, *à moins qu'on n'étende par voie d'adjonction le domaine de rationalité.*

2° Ou bien la différence des arguments de deux points rationnels ne sera jamais le $n^{ième}$ d'une période (à moins d'être d'une période).

S'il en est ainsi, il faudra, d'après ce que nous venons de voir, que l'argument d'un des points rationnels soit le $n^{ième}$ d'une période, soit

$$\alpha = \frac{\omega}{n}.$$

Alors

$$3\alpha = \frac{3\omega}{n}$$

sera la différence des arguments de deux points rationnels et en même temps le $n^{ième}$ d'une période; il faudrait donc que ce fût une période, ce qui ne peut arriver que de deux manières : si $\omega = 0$, si n est divisible par 3.

Le second cas se ramène aisément au premier, car si n est divisible par 3 et que $\frac{3\omega}{n}$ soit une période, α sera le tiers d'une période. Mais comme les arguments ne sont définis qu'à $\frac{1}{3}$ de période près, nous pouvons supposer $\alpha = 0$, d'où $\omega = 0$.

Si α est nul, on aura

$$\Sigma w_i = -\Sigma p_s \alpha_s,$$

et le second membre ne pourra être la $n^{ième}$ partie d'une période que si tous les p_s sont nuls; car l'expression $\Sigma p_s \alpha_s$ étant la différence des arguments de deux points rationnels ne peut être la $n^{ième}$ partie d'une période.

On a donc

$$\Sigma w_i = 0.$$

Dans ce cas que nous apprend l'analyse précédente? Que $\frac{X_1^{\lambda_2}}{X_2^{\lambda_1}}$ est la $n^{ième}$ puissance d'un nombre rationnel. Soit alors

$$\frac{3\lambda_1\lambda_2}{n} \equiv -\varepsilon \pmod 3.$$

Nous pourrons alors trouver deux courbes rationnelles $Z_1 = 0$ et $Z_2 = 0$, de degré $\frac{\lambda_1\lambda_2}{n} + \frac{\varepsilon}{3}$, passant toutes deux ε fois par le point rationnel, dont l'argument $\alpha = 0$; la première $Z_1 = 0$ passant λ_2 fois par chacun des $\frac{3\lambda_1}{n}$ points w_1; la seconde $Z_2 = 0$ passant λ_1 fois par chacun des $\frac{3\lambda_2}{n}$ points w_2.

On aura alors

$$\frac{X_1^{\lambda_1}}{X_2^{\lambda_1}} = \left(\frac{Z_1}{Z_2}\right)^n,$$

ce qui suffit déjà pour prouver que le premier membre est une puissance $n^{\text{ième}}$ parfaite.

Le résultat en question est donc illusoire, puisqu'on aurait pu l'obtenir par voie purement algébrique, sans faire intervenir le raisonnement arithmétique fondé sur l'impossibilité de décomposer un entier de plusieurs manières en facteurs premiers.

La considération des cubiques dérivées serait donc sans intérêt dans ce cas.

Nous voyons toutefois que X_1 doit être une puissance $n^{\text{ième}}$ parfaite, multipliée par un entier sur lequel on ne peut faire qu'un nombre fini d'hypothèses, *si l'on connaît le plus grand commun diviseur de* x_0, y_0, z_0. Cette restriction diminue un peu la portée du résultat, qui est d'ailleurs indépendant de la considération des cubiques dérivées.

Le cas où la considération des cubiques dérivées peut être utile est donc celui où les fonctions elliptiques relatives à ces cubiques dérivées se déduisent de celles qui correspondent à C par une transformation *qui n'est pas du premier ordre.*

IX. — Courbes de genre supérieur.

Je ne dirai que quelques mots des courbes de genre supérieur. Il n'est plus vrai que de la connaissance d'un point rationnel on puisse déduire celle d'une infinité d'autres points rationnels. Mais de la connaissance d'un *groupe* rationnel (et par conséquent de celle d'un point rationnel) on peut déduire celle d'une infinité d'autres groupes rationnels.

Soit en effet C une courbe rationnelle de genre p et de degré m, et soit un groupe rationnel de p points sur cette courbe. Le nombre des points doubles sera

$$d = \frac{(m-1)(m-2)}{2} - p.$$

Si nous coupons par une courbe adjointe C′ de degré $q \geq m-2$, le nombre des points d'intersection différents des points doubles sera

$$mq - 2d$$

et sur ce nombre, $mq - 2d - p$ pourront être choisis arbitrairement.

Soient $u_1, u_2, \ldots, u_p$ les p intégrales abéliennes de première espèce. Un groupe de p points sera défini quand on se donnera les p sommes

$$\Sigma u_1 = \alpha_1, \qquad \Sigma u_2 = \alpha_2, \qquad \ldots, \qquad \Sigma u_p = \alpha_p$$

pour ses p points, sommes que j'appellerai ses *arguments*. J'appellerai alors le groupe ainsi défini le *groupe* $(\alpha_1, \alpha_2, \ldots, \alpha_p)$ ou simplement le *groupe* α. On pourra choisir les constantes d'intégration de telle façon que la somme des arguments soit nulle pour les points d'intersection d'une courbe adjointe quelconque, les points doubles étant laissés de côté.

Si les groupes de p points α, β et γ sont rationnels, je dis qu'il en est de même du groupe $\beta + \gamma - \alpha$. En effet, par les groupes β et γ je puis faire passer une courbe adjointe rationnelle de degré $q > \frac{2d+3p}{m}$; elle coupera C en $mq - 2d - 2p$ autres points formant un groupe rationnel G dont la somme des arguments sera $-(\beta+\gamma)$. Par G et par le groupe α je puis faire passer une courbe rationnelle adjointe de degré q qui coupe C en p autres points formant un groupe rationnel d'arguments $\beta + \gamma - \alpha$.

Supposons maintenant que le groupe de p points α soit rationnel. Je mène d'abord une courbe adjointe rationnelle quelconque de degré $q \geq m-2$; elle coupera C suivant un groupe rationnel G de $mq - 2d$ points; la somme des arguments sera zéro.

Soit δ le plus grand commun diviseur de m et de $2d$; nous pourrons trouver deux nombres entiers positifs $q' \geq m-2$ et β tels que

$$m(q'-q) - \beta(mq - 2d) = \delta h,$$

h étant un entier positif quelconque. Je veux maintenant que

$$\delta h = (K+1)p.$$

Soit alors δ' le plus grand commun diviseur de m, $2d$ et p; soit $p = \xi\delta'$, $\delta = \varepsilon\delta'$; il nous suffira de prendre $h = \xi$, $K + 1 = \varepsilon$.

Cela posé, je fais passer une courbe adjointe rationnelle de degré q', $\beta + 1$ fois par le groupe G et K fois par le groupe α; cette courbe est ainsi entièrement déterminée, et elle coupe encore C en p autres points, car on a

$$mq' = (K + 1)p + (\beta + 1)(mq - 2d) + 2d.$$

Ces p autres points formeront un groupe rationnel et la somme des arguments sera $-K\alpha$ ou $\alpha - \varepsilon\alpha$.

Il résulte de tout cela que les groupes rationnels de p points situés sur C sont donnés par une formule

$$\alpha + \varepsilon n\alpha + \Sigma\mu_s(\alpha - \alpha_s)$$

tout à fait de même forme que les formules analogues relatives aux cubiques.

Le nombre ε (qui pour les cubiques est égal à 3) est le plus grand commun diviseur de m et $2d$ divisé par le plus grand commun diviseur de m, $2d$ et p.

On conçoit la possibilité de construire de cette manière une théorie analogue à celle des cubiques.