ANNALES DE L'UNIVERSITÉ DE GRENOBLE

F. CHATELET

Sur l'arithmétique des courbes de genre un

Annales de l'université de Grenoble, tome 22 (1946), p. 153-165

<http://www.numdam.org/item?id=AUG_1946__22__153_0>

SUR L'ARITHMÉTIQUE DES COURBES DE GENRE UN (1)

par **F. CHATELET** (Lyon).

Une des questions essentielles de la théorie des nombres est la recherche des points rationnels (c'est-à-dire des points dont les coordonnées sont des nombres rationnels) sur une courbe donnée à coefficients rationnels. Cette question a été complètement résolue pour toutes les courbes de genre o grâce aux travaux de Poincaré, Hilbert et Hurwitz (1). Ces auteurs ont ramené le cas général des courbes de genre o au cas des coniques qui avait été traité auparavant par Lagrange et Gauss. Mais pour les courbes de genre positi on ne connaît encore dans cette voie que des résultats fort incomplets. Sans prétendre traiter ici le cas général des courbes de genre un, je vais exposer à ce sujet un résultat partiel inédit.

On peut décomposer le problème des points rationnels sur une courbe (C) de genre un en deux problèmes successifs : un *problème d'existence,* reconnaître s'il existe sur (C) au moins un point rationnel ; dans le cas où le premier problème se résout par l'affirmative, un *problème de détermination,* trouver une méthode qui permette d'obtenir effectivement tous ces points. Or il existe une catégorie spéciale de courbes de genre un pour lesquelles le problème d'existence est immédiatement résoluble : les cubiques de la forme normale de Weierstrass

$$y^2 = x^3 + Ax + B, \qquad (4A^3 + 27B^2 \neq 0).$$

Une telle courbe possède un seul point à l'infini dont les coordonnées homogènes o, 1, o sont rationnelles et qui doit, en consé-

(1) Mémoire présenté à la séance de la section rhodanienne de la Société mathématique de France tenue à Grenoble le 19 mai 1946. Pour tout ce qui concerne la bibliographie de ces questions, on peut consulter l'ouvrage de Th. SKOLEM : *Diophantische Gleichungen* paru dans la collection des «Ergebnisse der Math... » (Berlin, 1938).

quence, être considéré comme un point rationnel à l'infini. Il est classique d'utiliser les propriétés de ces courbes dans le problème de détermination de la façon suivante.

On sait qu'une courbe de genre un peut être ramenée par une transformation birationnelle de courbe à courbe $\mathcal{R}$ à la forme normale de Weierstrass. (Ce qui revient à dire que (C) peut être représentée univoquement par des fonctions elliptiques, ces dernières pouvant être exprimées en fonctions rationnelles d'un couple de fonctions $\wp u$ et $\wp' u$ de Weierstrass.) Un résultat de Poincaré [2] précise que, si on connaît sur (C) un point rationnel simple M_0, il est possible de construire $\mathcal{R}$ de manière que ses coefficients soient rationnels ; la cubique de Weierstrass (W) déduite de (C) par $\mathcal{R}$ a, à fortiori, tous ses coefficients rationnels. Une telle correspondance $\mathcal{R}$ entre (C) et (W) transforme les points rationnels de (C) en ceux de (W) et inversement. De telle sorte que le problème de détermination sur (C) peut se ramener au problème de détermination sur (W).

Dans le cas où le problème d'existence sur (C) ne se résout pas immédiatement, on ne peut utiliser les résultats précédents. J'ai pu établir néanmoins le théorème suivant dont on trouvera la démonstration en annexe :

Théorème 1. — On peut toujours construire la correspondance $\mathcal{R}$ de manière que la cubique de Weierstrass (W) *déduite de* (C) *par $\mathcal{R}$ ait tous ses coefficients rationnels, ceux de $\mathcal{R}$ étant en général algébriques.*

La correspondance $\mathcal{R}$ ne transforme plus les points rationnels sur (C) en ceux de (W). Mais je vais utiliser la cubique (W) ainsi construite dans le *problème d'existence* sur (C) et montrer que ce problème est équivalent à un problème concernant les points rationnels sur (W). De telle sorte que l'ensemble du problème des points rationnels sur les courbes de genre un sera ramené à des problèmes concernant les seules cubiques de Weierstrass.

Pour cela, j'utilise une méthode analogue à celle qui m'a permis, dans ma thèse [3], de généraliser les résultats de Poincaré et Hilbert pour les courbes de genre o à certaines variétés unicursales d'un

(2) H. Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *J. de math.*, 5e série, t. 7 (1901), p. 161-233.

(3) Variations sur un thème de Poincaré, *Annales scient. de l'École norm. sup.*, 3e série, t. 61, 1944, p. 249-300.

espace à plus de 2 dimensions. Cette méthode emprunte des idées dues à E. Galois et fait appel à la notion de *groupe de Galois* d'un corps de nombres algébriques.

Je choisis un corps normal (ou galoisien) qui contienne tous les coefficients de la correspondance $\mathfrak{R}$. Je désigne par n le degré de ce corps et je numérote, dans un ordre d'ailleurs quelconque, de 1 à n les éléments σ_i du groupe de Galois G de k. De telle sorte qu'un élément σ_i de ce groupe peut être déterminé par son indice i. Je puis remplacer maintenant chacun des coefficients de $\mathfrak{R}$ par son transformé dans l'élément σ_i. Comme les coefficients de (C) et ceux de (W) sont tous rationnels, j'obtiens encore une correspondance birationnelle entre (C) et (W) que je désigne par $\mathfrak{R}^{(i)}$ et que j'appelle $i^{\text{ème}}$ *conjuguée de* $\mathfrak{R}$. Le produit de correspondances (4)

$$\mathfrak{A}_i = \mathfrak{R}^{-1} \cdot \mathfrak{R}^{(i)}$$

est alors une correspondance birationnelle entre (W) et elle-même à coefficients dans k.

J'appelle encore $i^{\text{ème}}$ *conjuguée* d'un point N à coordonnées dans k le point $N^{(i)}$ dont les coordonnées sont les transformées dans σ_i de celles de N. Si M est un point rationnel sur (C), la correspondance $\mathfrak{R}$ transforme ce point en un point $N = \mathfrak{R}(M)$ sur (W) à coordonnées dans k; le $i^{\text{ème}}$ conjugué $N^{(i)}$ de N est le point $\mathfrak{R}^{(i)}(M)$ transformé de M dans $\mathfrak{R}^{(i)}$. Ainsi $N^{(i)}$ est un point sur W que je puis déduire de N :

$$N^{(i)} = \mathfrak{R}^{(i)}(M) = \mathfrak{R}^{-1} \cdot \mathfrak{R}^{(i)}(N) = \mathfrak{A}_i(N).$$

De façon plus précise, le système de relations :

$$N^{(i)} = \mathfrak{A}_i(N), \qquad (i = 1, 2, \ldots, n),$$

où N est un point arbitraire sur (W) à coordonnées dans k, est équivalent au suivant

$$\mathfrak{R}^{-1}(N) = [\mathfrak{R}^{-1}(N)]^{(i)}, \qquad (i = 1, 2, \ldots, n).$$

Ce dernier exprime que le point $M = \mathfrak{R}^{-1}(N)$ sur (C) à coordonnées dans k est identique à tous ces conjugués, donc est rationnel. Ainsi le problème d'équivalence sur (C) est équivalent à celui de l'existence d'une solution pour le système :

$$\text{I} \qquad \mathfrak{A}_i(N) = N^{(i)}, \qquad (i = 1, 2, \ldots, n).$$

(4) Les produits de correspondances, ou plus généralement d'opérateurs, sont notés ici dans l'ordre de gauche à droite.

J'ai bien ramené le problème envisagé à la résolution d'un système d'équations dont l'inconnue est un point N sur (W). Mais ce point n'est pas un point rationnel, seulement un point à coordonnées dans k. C'est pourquoi je précise encore et transforme le système précédent.

Tout d'abord je remarque l'ensemble des n correspondances $\mathfrak{A}_i$ n'est pas quelconque, mais que ces correspondances sont liées entre elles par des « relations de compatibilité » analogues à des relations du même nom obtenues dans ma thèse.

Théorème 2. — La correspondance $\mathfrak{A}_k$ déterminée par le produit $\sigma_k = \sigma_j \cdot \sigma_i$ dans le groupe de Galois G *se déduit des correspondances $\mathfrak{A}_i$ et $\mathfrak{A}_j$ par la relation de compatibilité :*

$$\text{II} \qquad \mathfrak{A}_k = \mathfrak{A}_i \cdot \mathfrak{A}_j^{(i)}.$$

(La démonstration se trouve en annexe.)

Je précise ensuite la forme de la correspondance $\mathfrak{A}_i$ à l'aide de la théorie des fonctions elliptiques. En tant que correspondance birationnelle entre (W) et elle-même, elle peut être définie par une relation entre l'argument elliptique u d'un point arbitraire N sur (W) et l'argument elliptique u_i du transformé de N dans $\mathfrak{A}_i$. La théorie des fonctions elliptiques nous apprend que cette relation est de la forme :

$$\text{III} \qquad u_i = \varepsilon_i u + c_i$$

où c_i est une constante et où ε_i est l'une des puissances de -1 si A et B sont différents de 0, de l'imaginaire principale I si $A \neq 0$ et $B = 0$, de l'imaginaire $-J$ telle que $J^3 = 1$ si $A = 0$, et $B \neq 0$.

Enfin la correspondance $\mathfrak{A}_i$ a ses coefficients dans k ; ce qui exige que ε_i soit un nombre de k, ainsi que les coordonnées du point C_i dont l'argument elliptique sur (W) est c_i.

Il m'est commode d'introduire, à la manière classique, la *notion de somme entre points de* (W) : la somme de 2 points N_1 et N_2 de (W) est le point de (W) dont l'argument elliptique est la somme des arguments elliptiques de N_1 et de N_2. Le théorème d'addition des fonctions elliptiques montre que les coordonnées de la somme

$$N_1 + N_2$$

peuvent être exprimées rationnellement en fonction de celles de N_1 et de N_2. En particulier si N_1 et N_2 sont des points rationnels sur

(W), leur somme $N_1 + N_2$ est un point rationnel. La relation III est ainsi équivalente à la suivante :

III' $$\mathfrak{A}_i(N) = \mathcal{E}_i(N) + C_i,$$

où $\mathcal{E}_i$ est une des puissances de la transformation plane :

$$\begin{array}{llllll} x' = x, & y' = -y, & \text{si} & A \neq 0, & B \neq 0; \\ x' = -x, & y' = Iy, & \text{si} & A \neq 0, & B = 0; \\ x' = Jx, & y' = -y, & \text{si} & A = 0, & B \neq 0; \end{array}$$

et où C_i est le point de (W) dont l'argument elliptique est C_i.

De telle sorte que le système I est encore équivalent au suivant :

I' $$N^{(i)} = \mathcal{E}_i(N) + C_i, \qquad (i = 1, 2, \ldots, n).$$

Enfin la relation de compatibilité II est équivalente à la suivante :

$$\mathcal{E}_k(N) + C_k = \mathcal{E}_i \cdot \mathcal{E}_j^{(i)}(N) + \mathcal{E}_j^{(i)}(C_i) + C_j^{(i)}$$

qui se décompose en l'ensemble des 2 relations :

II' $$\begin{cases} \mathcal{E}_k = \mathcal{E}_i \cdot \mathcal{E}_j^{(i)}, \\ C_k = \mathcal{E}_j^{(i)}(C_i) + C_j^{(i)}. \end{cases}$$

En utilisant la première des relations II', je montre alors :

Théorème 3. — Il est toujours possible de construire la cubique (W) *et la correspondance* $\mathfrak{R}$ *de manière que chacune des correspondances* $\mathcal{E}_i$ *soit la correspondance identique :*

$$x' = x, \qquad y' = y.$$

(La démonstration de ce théorème se trouve en annexe.)

Quand cette condition est remplie, je dis que la correspondance $\mathfrak{R}$ est paire (5). Le système I' se simplifie alors de la façon suivante :

I $$N^{(i)} = N + C_i, \qquad (i = 1, 2, \ldots, n).$$

Les relations de compatibilité II' se réduisent à la seule relation :

II'' $$C_k = C_i + C_j^{(i)}.$$

En ajoutant les relations II'' qui correspondent à une même valeur de i et aux différentes valeurs de j, j'en déduis encore :

$$C = nC_i + C^{(i)},$$

(5) Voir à ce sujet ma note aux Comptes Rendus : *Points rationnels et classification des courbes de genre* un. *Comptes Rendus Acad. Scien.*, t. 206 (1938), p. 1532.

où C désigne la somme $C=\sum_{j=1}^{n} C_j$ et où nC_i désigne, à la manière classique, la somme de n points identiques à C_i. En vertu du théorème d'addition des fonctions elliptiques, les coordonnées du point nC_i sont des nombres de k, comme celles du point C_i.

Ce qui montre que C vérifie le système :

$$\text{IV} \qquad N^{(i)}=-nC_i+N, \qquad (i=1, \ldots, n)$$

déduit du système I″ en remplaçant chaque C_i par $-nC_i$. Il est alors facile de ramener la résolution complète du système IV à la recherche des points rationnels sur (W). Il suffit de chercher la condition vérifiée par le point $P=N-C$, où N est une solution quelconque du système IV ; elle s'obtient en remplaçant N par $C+P$ dans ce système. En tenant compte du fait que C vérifie ce même système IV, la condition s'écrit :

$$P^{(i)}=P, \qquad (i=1, 2, \ldots, n).$$

Ce qui exprime une condition nécessaire et suffisante pour que P soit un point rationnel, de telle sorte que les solutions du système IV sont les sommes $C+P$, où P est un point rationnel sur (W).

Or toute solution N du système I″ engendre une solution du système IV, à savoir $-nN$. Cette dernière doit être de la forme $C+P$, donc N est de la forme $-\frac{C+P}{n}$ et le système I″ est encore équivalent au système suivant :

$$\text{I}''' \qquad \left(\frac{C+P}{n}\right)^{(i)}=\frac{C+P}{n}-C_i, \qquad (i=1, 2, \ldots, n).$$

J'ai bien ainsi ramené le problème d'existence sur (C) à l'étude d'un système d'équations dont l'inconnue est un point rationnel P sur (W). Remarquons que l'expression $\frac{C+P}{n}$ ne désigne pas un point sur (W) mais n^2 points distincts dont les coordonnées ne sont pas en général dans k, mais dans une extension de degré n^2. (Les arguments elliptiques de ces n^2 points se déduisent de l'un d'eux par addition des différents quotients par n des périodes de pu.) Le système I‴ exige que l'un au moins de ces n^2 points ait ses coordonnées dans k ; de plus l'expression du premier membre de I‴ désigne le point $i^{\text{ème}}$ conjugué de la détermination de $\frac{C+P}{n}$ qui

figure au second membre et non d'une quelconque des déterminations de cette expression. Enfin le fait que $C + P$ vérifie le système IV ne suffit pas pour que P vérifie le système I''' ; il entraîne seulement que P vérifie l'un des systèmes déduit du système I''' en remplaçant chaque C_i par la somme de celui-ci et d'un point de (W) dont le produit par n est nul. (L'argument elliptique de ce dernier point est le quotient par n d'une période de $\wp u$, mais peut ne pas être une période.)

J'ai ainsi démontré le :

Théorème 4. — Pour qu'il existe sur (C) *un point rationnel, il faut et il suffit qu'il existe sur* (W) *un point rationnel* P *tel que :*

1° *Les coordonnées de l'un au moins* P′ *des* n^2 *points* $\frac{C+P}{n}$ *sont dans* k *;*

2° P′ *vérifie le système de relations :*

$$P'^{(i)} = P' - C_i, \qquad (i = 1, 2, \ldots, n).$$

Je précise encore que la connaissance d'une base de Mordell-Weil sur (W) permettrait de reconnaître s'il existe sur (W) un tel point P impliqué par le théorème 4. On sait, en effet, lorsque P est choisi, reconnaître s'il vérifie les conditions de ce théorème 4 : les coordonnées du point P′ sont solutions d'un système d'équations à coefficients dans k qu'on sait former à partir des coordonnées de P et qui est de plus équivalent à une seule équation ne contenant qu'une inconnue ; pour pouvoir reconnaître si P vérifie les conditions du théorème 4, il s'agit donc de reconnaître si cette dernière équation est réductible dans k, s'il figure un facteur linéaire dans la décomposition et de former ce facteur ; toutes ces opérations peuvent se faire par la méthode classique de décomposition d'un polynome en facteurs irréductibles dans un corps de nombres algébriques. Les difficultés d'application du théorème 4 proviennent en fait de ce qu'on ne connaît pas les points rationnels P sur (W) et que d'ailleurs ces points sont, en général, en nombre infini.

Or Mordell et Weil (6) ont montré qu'il existe sur chaque cubique de Weierstrass (W) à coefficients rationnels un ensemble fini de points rationnels $P_1, P_2, \ldots, P_r$ tel que tout point rationnel sur (W)

(6) L. J. Mordell. On the rational solutions... *Proc. Cambridge Philos. Soc.*, t. 21 (1922), p. 169-171 et A. Weil. Sur un théorème de Mordell. *Bull. Sci. math.*, 2e série, t. 54 (1930), p. 182-191.

peut être mis sous la forme :

$$P = a_1 P_1 + a_2 P_2 + \cdots + a_r P_r,$$

où $a_1, a_2, \ldots, a_r$ sont des entiers rationnels positifs ou négatifs. L'ensemble $P_1, P_2, \ldots, P_r$ est appelé une *base de Mordell-Weil* sur (W) et permet d'obtenir tous les points rationnels sur (W) par des opérations rationnelles (en nombre infini). Le théorème de Mordell-Weil ne résout pas complètement le problème de détermination sur (W), car il ne donne pas de méthode pour déterminer effectivement une base de Mordell-Weil sur (W).

Or si les conditions du théorème 4 sont vérifiées par le point :

$$P = a_1 P_1 + a_2 P_2 + \cdots + a_r P_r,$$

elles le sont aussi par tout point qui s'en déduit en ajoutant aux différents a_i des multiples quelconques de n. Car cela revient à ajouter à P un produit nQ d'un point rationnel Q par n, ce qui ne modifie pas les conditions du théorème 4. Mais parmi ces différents points, il en existe un qui appartient à l'ensemble fini des n^2 points :

$$b_1 P_1 + b_2 P_2 + \cdots + b_r P_r$$

pour lesquels :

$$0 \leqslant b_i < n, \qquad (i = 1, 2, \ldots, n).$$

Pour reconnaître si les conditions du théorème 4 sont vérifiées par l'un des points rationnels sur (W), il suffit donc de reconnaître si elles sont vérifiées par l'un des n^2 points précédents. La connaissance d'une base de Mordell-Weil sur (W) permettrait de former ces n^2 points et, par suite, de reconnaître si l'un d'eux vérifie ces conditions, par un nombre fini d'opérations rationnelles, donc de résoudre effectivement le problème d'existence sur (C).

Ainsi les problèmes d'existence et de détermination sur les courbes de genre un à coefficients rationnels sont ramenés à la seule détermination des bases de Mordell-Weil sur les cubiques de Weierstrass.

Annexe.

Démonstration du théorème 1.

Il est toujours possible de construire sur (C) un point *simple* M_0 à coordonnées algébriques. Par exemple en prenant l'intersection de (C) et d'une droite à coefficients rationnels ne passant par aucun point multiple de (C), il est facile d'éviter les points multiples

puisqu'ils sont en nombre fini. Je désigne par k un corps normal contenant les coordonnées de M_0 et par n son degré. Comme précédemment je numérote de 1 à n les éléments du groupe de Galois G de k. La construction de Poincaré permet d'obtenir, à partir de M_0, une correspondance birationnelle $\mathcal{R}_1$ entre (C) et une cubique de Weierstrass (W_1) tels que les coefficients de $\mathcal{R}_1$ et ceux de (W_1) soient des nombres de k.

Je construis la $i^{\text{ème}}$ conjuguée de la correspondance $\mathcal{R}_1$; elle transforme (C) en la $i^{\text{ème}}$ conjuguée $(W_1)^{(i)}$ de (W_1). C'est dire que si (W_1) est définie par l'équation :

$$y^2 = x^3 + A_1 x + B_1,$$

$(W_1)^{(i)}$ peut être définie par l'équation :

$$y^2 = x^3 + A_1^{(i)} x + B_1^{(i)}.$$

Mais le produit des correspondances $\mathcal{R}_1^{-1} . \mathcal{R}_1^{(i)}$ définit une correspondance birationnelle entre (W_1) et $(W_1)^{(i)}$. Or la théorie des fonctions elliptiques montre que l'existence d'une correspondance entre ces 2 cubiques entraîne l'égalité de leurs modules :

$$\frac{4A_1^3 + 27B_1^2}{B_1^2} = \frac{4(A_1^{(i)})^3 + 27(B_1^{(i)})^2}{(B_1^{(i)})^2}.$$

Le nombre de k :

$$m = \frac{4A_1^3 + 27B_1^2}{B_1^2}$$

est par suite égal à chacun de ses n conjugués ; d'après un résultat classique de la théorie de Galois, il en résulte que m est rationnel. Il est alors facile de trouver 2 nombres rationnels A et B tels que

$$B^2 m = 4A^3 + 27B^2.$$

En effet toutes les solutions de cette équation diophantienne sont les couples de nombres :

$$A = 4(m - 27)\lambda^2, \qquad B = 16(m - 27)\lambda^3,$$

où λ est un nombre rationnel arbitraire. Je choisis l'une de ces solutions et je forme la cubique (W) :

$$y^2 = x^3 + Ax + B.$$

La théorie des fonctions elliptiques montre que l'égalité :

$$\frac{4A^3+27B^2}{B^2}=m=\frac{4A_1^3+27B_1^2}{B_1^2}$$

suffit pour que (W) puisse se déduire de (W_1) par une transformation homographique $\mathfrak{L}$ du plan qui détermine une correspondance birationnelle entre (W_1) et (W).

Le produit de correspondances $\mathfrak{R}_1 . \mathfrak{L} = \mathfrak{R}$ est alors une correspondance birationnelle à coefficients dans k entre (C) et la cubique de Weierstrass (W) à coefficients rationnels ; ce qui démontre le théorème 1.

*
* *

Démonstration du théorème 2.

Il suffit de reprendre la définition de la correspondance $\mathfrak{A}_k$:

$$\mathfrak{A}_k = \mathfrak{R}^{-1} . \mathfrak{R}^{(k)}$$

et de transformer son expression de la façon suivante :

$$\mathfrak{A}_k = \mathfrak{R}^{-1} . \mathfrak{R}^{(i)} . (\mathfrak{R}^{(i)})^{-1} . \mathfrak{R}^{(k)}.$$

Puisque $\sigma_k = \sigma_j . \sigma_i$, le produit :

$$(\mathfrak{R}^{(i)})^{-1} . \mathfrak{R}^{(k)}$$

est encore égal à :

$$(\mathfrak{R}^{-1} . \mathfrak{R}^{(j)})^{(i)} = \mathfrak{A}_j^{(i)}.$$

De telle sorte que :

$$\mathfrak{A}_k = \mathfrak{A}_i . \mathfrak{A}_j^{(i)}.$$

*
* *

Démonstration du théorème 3.

Je suppose avoir construit par la méthode du théorème 1 une correspondance $\mathfrak{R}$ qui ne vérifie peut-être pas le théorème 3. Je vais en déduire une correspondance paire $\mathfrak{R}'$ entre (C) et une cubique de Weierstrass (W') à coefficients rationnels, en général différente de (W).

La correspondance $\mathfrak{R}'$ que je vais construire sera un produit $\mathfrak{R}' = \mathfrak{R} . \mathfrak{L}$, où $\mathfrak{L}$ est une homographie de la forme :

$$x' = \lambda^2 x, \qquad y' = \lambda^3 y,$$

dont le coefficient λ est un nombre algébrique *différent de* o que je vais déterminer. On sait que $\mathfrak{L}$ transforme (W) en une cubique de Weierstrass (W′) ; la théorie des fonctions elliptiques montre d'ailleurs que si 2 cubiques de Weierstrass se déduisent l'une de l'autre par une correspondance birationnelle, il existe une infinité de telles correspondances dont une au moins peut être déterminée par une homographie plane de la forme précédente.

Il est d'abord nécessaire, pour la démonstration, que $\mathfrak{R}'$ transforme (C), donc que $\mathfrak{L}$ transforme (W) en une cubique (W′) à coefficients rationnels. Or les coefficients de (W′) sont :

$$A' = A\lambda^4, \qquad B' = B\lambda^6.$$

La condition est donc que λ^2 soit rationnel si $A \neq o$, $B \neq o$, que λ^4 soit rationnel si $A \neq o$, $B = o$, que λ^6 soit rationnel si $A = o$, $B \neq o$.

Si cette condition est réalisée, le produit :

$$\mathfrak{A}'_i = \mathfrak{R}'^{-1} . \mathfrak{R}'^{(i)} = \mathfrak{L}^{-1} . \mathfrak{R}^{-1} . \mathfrak{R}^{(i)} . \mathfrak{L}^{(i)} = \mathfrak{L}^{-1} . \mathfrak{A}_i . \mathfrak{L}^{(i)}$$

est une correspondance birationnelle entre (W) et elle-même. Je puis alors exprimer $\mathfrak{A}_i$ et $\mathfrak{A}'_i$ suivant des formules analogues à III′ ; j'obtiens ainsi :

$$\mathfrak{E}'_i(N) + C'_i = \mathfrak{L}^{(i)}[\mathfrak{L}^{-1} . \mathfrak{E}_i(N) + C_i].$$

On sait d'ailleurs que les homographies de la forme $\mathfrak{L}$ transforment la notion de somme sur (W) en la notion de somme sur (W′) ; ce qui permet encore d'écrire la relation précédente :

$$\mathfrak{E}'_i(N) + C'_i = \mathfrak{L}^{-1} . \mathfrak{E}_i . \mathfrak{L}^{(i)}(N) + \mathfrak{L}^{(i)}(C_i).$$

J'en déduis notamment :

V $$\mathfrak{E}'_i = \mathfrak{L}^{-1} . \mathfrak{E}_i . \mathfrak{L}^{(i)}.$$

Or les correspondances $\mathfrak{E}_i$ sont des cas particuliers des homographies $\mathfrak{L}$, cas particuliers pour lesquels le coefficient λ est l'un des nombres $+1$, -1, $+I$, $-I$, $+J$, $-J$, $+J^2$, $-J^2$. Je remarque de plus que le produit des homographies :

$$\mathfrak{L}_1 \qquad x' = \lambda_1^2 x, \qquad y' = \lambda_1^3 y$$
$$\mathfrak{L}_2 \qquad x' = \lambda_2^2 x, \qquad y' = \lambda_2^3 y$$

est une homographie de la même forme déterminée par le coefficient $\lambda_1\lambda_2$. (En particulier ce produit est commutatif.) Je désigne par e'_i et e_i les coefficients des homographies $\mathfrak{E}'_i$ et $\mathfrak{E}_i$. La relation V entre

correspondances est ainsi équivalente à la relation entre scalaires :

V' $$e'_i = e_i \cdot \lambda^{-1} \cdot \lambda^{(i)}.$$

D'autre part la relation de compatibilité :

$$\mathcal{E}_k = \mathcal{E}_i \cdot \mathcal{E}_j^{(i)}$$

est équivalente à la relation entre scalaires :

$$e_k = e_i \cdot e_j^{(i)}.$$

En additionnant entre elles, les relations ainsi obtenues et correspondant à une même valeur de i et aux différentes valeurs de j, j'obtiens :

$$E = e_i E^{(i)}$$

où E désigne la somme $E = \sum_{j=1}^{n} e_j$. A fortiori, j'en déduis :

$$E^{\alpha} = e_i (E^{\alpha})^{(i)},$$

où α est un entier rationnel quelconque. Comme e_i est égal à 1 pour $\alpha = 2$ si $A \neq 0$, $B \neq 0$, pour $\alpha = 4$ si $A \neq 0$, $B = 0$, pour $\alpha = 6$ si $A = 0$, $B \neq 0$, cette dernière relation montre que la puissance correspondante de E est un nombre rationnel. Donc si E est différent de O, j'obtiens, en choisissant $\lambda = E$, une correspondance $\mathcal{R}$ qui transforme (C) en une cubique de Weierstrass (W') à coefficients rationnels et pour laquelle ;

$$e'_i = e_i \cdot E^{-1} \cdot E^{(i)} = 1.$$

Ainsi les correspondances $\mathcal{E}'_i$ sont toutes identiques à l'unité et la correspondance $\mathcal{R}'$ est paire ainsi que je l'avais annoncé.

Lorsque E est égal à 0, le raisonnement précédent ne convient plus car il conduit à une homographie $\mathcal{L}$ dégénérée qui ne définit pas une correspondance birationnelle. Mais il est possible de tourner cette difficulté de la façon suivante. J'appelle Λ la somme :

$$\Lambda = \sum_{j=1}^{n} e_j \Theta^{(j)}$$

où Θ est un nombre arbitraire de k. Des relations de compatibilité entre e_i, je déduis que :

$$\Lambda^{(i)} = \sum_{k=1}^{n} e_j^{(i)} \Theta^{(k)} = \sum_{k=1}^{n} e_k e_i^{-1} \Theta^{(h)} = e_i^{-1} \Lambda.$$