ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

FRANÇOIS CHATELET

Sur la réalité des courbes de genre Un

Annales de la faculté des sciences de Toulouse 4e série, tome 11 (1947), p. 75-92
<http://www.numdam.org/item?id=AFST_1947_4_11__75_0>

SUR LA RÉALITÉ DES COURBES DE GENRE UN.

par François CHATELET.

Les problèmes de réalité sur les courbes algébriques ont été étudiés par Klein [1] à l'aide de méthodes profondes qui utilisent les propriétés topologiques des surfaces de Riemann. Mais, dans les cas les plus simples, on peut employer des méthodes qui, sans être essentiellement distinctes de celles de Klein, ne font appel qu'à des résultats plus élémentaires d'algèbre et d'analyse. Il m'a semblé intéressant de développer ces dernières en utilisant le minimum de connaissances transcendantes, mais en détaillant les difficultés de leur application.

J'ai étudié ailleurs les problèmes de réalité des courbes unicursales [2]; j'ai ainsi obtenu une application simple des propriétés des représentations unicursales propres. Je vais étudier ici de façon analogue les problèmes de réalité des courbes de genre un. L'emploi de la représentation de ces courbes par les fonctions elliptiques (à la place des représentations unicursales) rend la méthode beaucoup moins élémentaire que dans le cas des courbes unicursales. Mais l'étude des fonctions elliptiques est aujourd'hui si complète qu'elle permet de développer l'étude de la réalité jusqu'aux applications numériques.

J'ai fait usage des notions algébriques abstraites qui jouent un grand rôle dans les théories géométriques récentes : correspondances birationnelles entre 2 courbes, produits de telles correspondances et relations symboliques entre elles, groupe birationnel sur une courbe, ... Les problèmes étudiés, ainsi que les résultats obtenus restent pourtant du domaine de l'intuition géométrique classique. J'espère que cette application nouvelle de ces notions abstraites à des théories bien connues sera utile à ceux qui veulent s'initier aux relations entre les différentes branches des mathématiques.

1. — On peut définir les « *courbes de genre un* » de plusieurs façons équivalentes : d'après le nombre de leurs points multiples (comptés un nombre de fois convenable suivant le genre de leur multiplicité), d'après la nature topologique des surfaces de Riemann qui leur correspondent, d'après les propriétés de leurs séries linéaires, ... On trouvera dans les traités classiques la démonstration de l'équivalence entre ces définitions et la suivante : une courbe de genre un est une courbe algébrique (C) qui peut être représentée, à l'aide de fonctions elliptiques d'un paramètre u, tout point correspondant biunivoquement à la valeur de u définie au module

1. F. Klein. — Riemannschen Flächen. Cours polycopié professé à l'Université de Göttingen en 1891-92, (Leipzig, 1906).
2. Revue scientifique, t. 85 (1947), pp. 709-15.

près des périodes (à l'exception des points multiples de (C) qui peuvent correspondre à plusieurs valeurs de u). Comme les fonctions elliptiques de mêmes périodes peuvent être exprimées au moyen des fonctions de Weierstrass $\wp u$ et $\wp' u$, cette définition peut se traduire en langage géométrique : une courbe de genre un est une courbe (C) qui peut être transformée, par une correspondance birationnelle $\mathcal{R}$ en une cubique (w) d'équation :

$$y^2 = x^3 + p\,x + q,$$

où p et q sont des constantes complexes telles que $4\,p^3 + 27\,q^2 \neq 0$.

Rappelons qu'une correspondance birationnelle entre 2 courbes est définie par 2 systèmes de formules :

$$\mathrm{X} = \mathrm{F}(x, y), \ \mathrm{Y} = \mathrm{G}(x, y)\,;$$

et

$$x = f(\mathrm{X}, \mathrm{Y}), \ y = g(\mathrm{X}, \mathrm{Y})\,;$$

où F, G, f et g sont des fonctions rationnelles à coefficients complexes telles que :

1° si on remplace X et Y par F et G dans l'équation de la seconde courbe, on obtient une équation en x et y équivalente à l'équation de la première, et de même pour x et y dans l'équation de la première courbe;

2° les 2 systèmes précédents sont équivalents sur les courbes transformées, c'est-à-dire lorsque X, Y et x, y vérifient respectivement les équations de ces courbes.

Ces relations déterminent une correspondance biunivoque entre les points de ces 2 courbes, sauf pour un nombre fini de points dont les coordonnées annulent à la fois le numérateur et le dénominateur d'une des fonctions F, G, f ou g, points dont le transformé n'est pas déterminé par ces formules.

C'est cette définition du genre que nous utiliserons dans la suite; elle nous permettra de ramener l'étude des courbes de genre un à celle des cubiques (w). Aussi nous commencerons par rappeler les propriétés les plus simples de ces dernières courbes [3].

La cubique (w) :

$$y^2 = x^3 + px + q, \qquad (4p^3 + 27\,q^2 \neq 0),$$

n'est pas de genre 0, c'est-à-dire n'admet pas de représentation unicursale propre, mais admet la représentation par fonctions elliptiques :

$$x = \wp u, \qquad y = \frac{1}{2}\,\wp' u,$$

où $\wp u$ et $\wp' u$ sont les fonctions de Weierstrass d'invariants $g_2 = -4\,p$ et $g_3 = -4\,q$. Sur une telle courbe, on peut appeler *somme* $\mathrm{M}_1 + \mathrm{M}_2$ *de 2 points* M_1 et M_2, le point de (w) dont l'argument elliptique u est la

3. On trouvera la démonstration de ces propriétés dans les traités concernant les fonctions elliptiques, ou plus simplement dans les « Leçons sur les théories générales de l'Analyse » de R. Baire, tome II, p. 281 et suivantes, (Gauthiers-Villars, 1908).

somme des arguments u_1 de M_1 et u_2 de M_2 au module près des périodes. Les coordonnées de la somme peuvent être calculées par des opérations rationnelles sur les coordonnées des 2 termes (formules d'addition des fonctions de Weierstrass).

Cette notion peut aussi être définie de façon géométrique par les 2 conditions : la somme $M_1 + M_2 + M_3$ est nulle si et seulement si les 3 points M_1, M_2 et M_3 sont alignés, le point « nul » sur (w) est le point à l'infini (unique) sur cette courbe. On montre que cette opération vérifie les règles de calcul élémentaires de l'addition ordinaire : associativité, commutativité, existence d'un opposé unique pour chaque point de (w).

La formule symbolique :

$$M' = M + A,$$

ou la formule équivalente :

$$u' = u + a,$$

où A est un point fixe de (w) et où a est son argument elliptique, définit une correspondance birationnelle entre les points M et M′ de (w). Nous l'appelons *translation* $\mathcal{T}_A$ *sur* (w) *d'amplitude A*. Les translations sur (w) forment un groupe multiplicatif (au sens du produit ou succession des correspondances) isomorphe au groupe additif de leurs amplitudes A. Ce qui permet de remplacer toute relation multiplicative entre translations sur (w) par une relation additive entre leurs amplitudes.

D'autre part, on montre que les correspondances birationnelles $\mathfrak{J}$ sur (w) qui laissent invariant le point nul sont les homologies du plan définies par un système de formules :

$$y' = \lambda^3 y, \quad x' = \lambda^2 x;$$

ou par la formule équivalente :

$$u' = \lambda^{-1} u,$$

où λ peut prendre l'une des valeurs suivantes en nombre fini :

$+ 1$ ou $- 1$, dans tous les cas,

$+ i$ ou $- i$, mais seulement si $q = 0$ (i désigne l'imaginaire principale),

$+ j, + j^2, - j$ ou $- j^2$, mais seulement si $p = 0$ (j désigne une racine cubique imaginaire de l'unité).

Ces correspondances $\mathfrak{J}$ forment un groupe cyclique d'ordre 2, 4 ou 6 suivant que p et q sont tous deux $\neq 0$, ou que $p = 0$, ou que $q = 0$. Ce groupe est isomorphe au groupe multiplicatif des coefficients λ de ces correspondances; ce qui permet de remplacer toute relation multiplicative entre de telles correspondances par une relation multiplicative entre les *scalaires* λ correspondants.

Enfin on montre que le groupe birationnel sur (w) (c'est-à-dire l'ensemble des correspondances birationnelles sur (w), est le produit direct du groupe des correspondances $\mathfrak{J}$ et du groupe des translations. C'est-à-dire que toute correspondance birationnelle sur (w) peut être mise d'une manière unique sous la forme d'un produit :

$$\mathfrak{I} . \mathfrak{T}_A ,$$

ou peut être définie de façon univoque par une relation de la forme :

$$u' = \lambda^{-1} u + a,$$

où λ ne peut prendre que l'une des 2, 4 ou 6 valeurs précitées.

Ceci permet de remplacer toute relation multiplicative entre correspondances sur (w) par 2 relations : une relation additive entre points de (w) et une relation multiplicative entre scalaires. Pour écrire facilement ces relations, il nous sera commode dans la suite de pouvoir modifier l'ordre des produits de correspondances de manière à grouper ensemble, d'une part les translations, d'autre part les homologies $\mathfrak{I}$. Pour cela, nous utiliserons la *formule de permutation* (4) :

$$\mathfrak{T}_A . \mathfrak{I} = \mathfrak{I} . \mathfrak{T}_{\mathfrak{I}(A)}$$

cette formule est équivalente à la relation entre arguments elliptiques :

$$\lambda^{-1} (u + a) = \lambda^{-1} u + \lambda^{-1} a.$$

Si on considère maintenant 2 cubiques (w) et (w') différentes, il peut ne pas exister de correspondance birationnelle qui transforme (w) en (w'). La condition nécessaire et suffisante pour qu'il existe une telle correspondance — ou pour qu'il y ait une correspondance biunivoque entre les arguments elliptiques des points de ces 2 courbes — est que les coefficients de (w) et de (w') vérifient la relation :

$$\frac{p'^3}{q'^2} = \frac{p^3}{p^2}$$

Si cette condition est réalisée, il existe au moins un nombre (nombre complexe arbitraire) tel que :

$$p' = \lambda^4 p, \quad q' = \lambda^6 q.$$

Les formules :

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

définissent alors une correspondance birationnelle particulière $\mathfrak{L}$ entre (w) et (w') — à laquelle correspond la transformation des arguments :

$$u' = \lambda^{-1} u. \text{ —}$$

Ces homologies $\mathfrak{L}$ forment un groupe isomorphe au groupe multiplicatif de leurs coefficients λ. Ce qui permet de remplacer toute relation multiplicative entre homologies $\mathfrak{L}$ par une relation multiplicative entre scalaires λ. Celles des homologies $\mathfrak{L}$ qui conservent une cubique (w) sont précisemment les correspondances $\mathfrak{I}$ déjà définies. Le groupe des homologies $\mathfrak{L}$ et le groupe des translations sur (w) n'ont donc en commun que

4. Les produits de correspondances sont écrits dans ce travail dans le sens de gauche à droite : le produit $\mathfrak{T} . \mathfrak{I}$ signifie qu'il faut d'abord effectuer la correspondance $\mathfrak{T}$ sur l'objet à transformer, puis la correspondance $\mathfrak{I}$ sur le résultat ainsi obtenu.

l'élément unité; on peut encore remplacer toute relation multiplicative entre correspondances birationnelles de (w) en (w') par une relation additive entre points de (w) et une relation multiplicative entre scalaires. Pour écrire facilement ces relations, on utilisera la formule de permutation qui est encore vraie :

$$\mathcal{T}_A . \mathcal{L} = \mathcal{L} . \mathcal{T}_{\mathcal{L}(A)};$$

il y a lieu de remarquer que dans cette formule $\mathcal{T}_A$ est une translation sur (w), mais que $\mathcal{T}_{\mathcal{L}(A)}$ est une translation sur la cubique transformée de (w) par $\mathcal{L}$.

Ces propriétés permettent d'établir un lemne sur les courbes de genre un qui nous servira fréquemment dans la suite :

Lemne.

Si une courbe (C) *est de genre un* (c'est-à-dire si elle peut être déduite d'une cubique (w_1) par une correspondance birationnelle $\mathcal{R}_1$), il existe une *infinité de cubique* (w) *dont elle peut être déduite par des correspondances birationnelles.*

Les cubiques (w) *sont celles qui sont définies par les équations de la forme :*

$$y^2 = x^3 + \lambda^4 p_1 x + \lambda^6 q_1,$$

où λ *est une constante complexe* $\neq 0$ *et où* p_1 *et* q_1 *désignent les coefficients de* (w_1).

Les correspondances $\mathcal{R}$ *associées à* (w) *sont les produits :*

$$\mathcal{R} = \mathcal{L} . \mathcal{T}_A . \mathcal{R}_1$$

où $\mathcal{L}$ *est la correspondance définie par les formules :*

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

et où $\mathcal{T}_A$ *est une translation sur* (w_1) *d'amplitude* A *arbitraire.* (Il est à remarquer que la cubique (w) est déterminée par plusieurs valeurs différentes de λ, en nombre fini.)

Démonstration.

La correspondance :

$$\mathcal{R}_1 : \quad (w_1) \rightarrow (C),$$

admet, en tant que correspondance birationnelle, un inverse :

$$\mathcal{R}_1^{-1} : \quad (C) \rightarrow (w_1),$$

qui est aussi une correspondance birationnelle. S'il existe une correspondance birationnelle :

$$\mathcal{R} : \quad (w) \rightarrow (C),$$

le produit $\mathcal{R} . \mathcal{R}_1^{-1}$ est défini et est une correspondance birationnelle :

$$\mathcal{R} . \mathcal{R}_1^{-1} : \quad (w) \rightarrow (w_1).$$

D'après les propriétés rappelées, l'existence d'une telle correspondance exige que (w) soit de la forme indiquée. On peut donc mettre l'équation de (w)

sous cette forme, déterminer l'une des valeurs possibles pour λ et former l'homologie $\mathcal{L}$ correspondante. L'inverse $\mathcal{L}^{-1}$ est alors une correspondance birationnelle :

$$\mathcal{L}^{-1} : \quad (w_1) \rightarrow (w),$$

donc le produit $\mathcal{L}^{-1}.\mathfrak{R}.\mathfrak{R}_1^{-1}$ est défini et est une correspondance birationnelle sur (w_1). D'après les propriétés rappelées, ce produit doit être de la forme $\mathfrak{J}.\mathfrak{T}_A$ donc $\mathfrak{R}$ est de la forme :

$$\mathcal{L}.\mathfrak{J}.\mathfrak{T}_A.\mathfrak{R}_1.$$

Mais les produits de la forme $\mathcal{L}.\mathfrak{J}$ sont les homologies $\mathcal{L}$ correspondant aux différentes valeurs de λ qui définissent la même cubique (w) ; donc $\mathfrak{R}$ est bien de la forme indiquée.

2. — Avant d'aborder l'étude des courbes de genre un, il convient de se poser une question préliminaire : *comment reconnaître si une courbe (C), donnée par une équation algébrique, à coefficients complexes :*

$$P(X, Y) = 0,$$

est de genre un et, s'il en est ainsi, comment déterminer une correspondance birationnelle $\mathfrak{R}$ qui transforme (C) en une cubique (w) ? On peut employer la méthode classique des adjointes passant par les points multiples de la courbe qu'on trouvera dans les traités de géométrie algébrique. On peut aussi employer une méthode analogue à celle que M. Lebesgue employait dans ses cours au Collège de France pour les courbes unicursales et que j'ai exposée ailleurs (5). Cette seconde méthode a l'avantage de n'utiliser que des opérations algébriques sur les coefficients de la courbe donnée et d'éviter la « résolution des singularités » dans le cas des points multiples d'ordres supérieurs à 2. Mais elle est notablement plus délicate pour les courbes de genre un que pour les courbes unicursales. Aussi nous ne l'exposerons pas ici pour ne pas alourdir l'exposé.

On constate par l'une ou l'autre de ces méthodes que la recherche de (w) et de $\mathfrak{R}$ exige en général l'introduction de nombres complexes, même si les coefficients de (C) sont tous réels. On peut ainsi obtenir une correspondance $\mathfrak{R}$ à coefficients complexes transformant la cubique (w) à coefficients complexes en la courbe (C) à coefficients réels. Il nous faut donc étudier les propriétés de réalité des courbes (C) déduites d'une cubique (w) à coefficients complexes par une correspondance birationnelle $\mathfrak{R}$ à coefficients complexes. Mais une telle courbe peut n'admettre aucune équation à coefficients réels; il se pose donc d'abord la question : à *quelle condition la courbe (C) déduite de (w) par la correspondance $\mathfrak{R}$ peut elle être définie par une équation à coefficients réels?*

Pour cela nous utiliserons les propriétés des imaginaires conjuguées. Suivant un langage commode et courant, nous appellerons « être géométrique conjugué » d'un être géométrique $\mathcal{E}$ (point, courbe, correspondance,

5. Revue Scientifique (article cité à la note 2).

...), l'être géométrique $\overline{\mathcal{E}}$ obtenu en remplaçant dans les formules de définition de $\mathcal{E}$ toutes les constantes par les nombres imaginaires conjugués sans changer les variables éventuelles. D'après les propriétés classiques du calcul des imaginaires, la correspondance $\overline{\mathfrak{R}}$ (imaginaire conjuguée de $\mathfrak{R}$) transforme la cubique $\overline{(w)}$ (imaginaire conjuguée de (w) en la courbe $\overline{(C)}$ (imaginaire conjuguée de (C). De plus, pour que (C) puisse être définie par une équation à coefficients réels, il faut et il suffit que $\overline{(C)}$ soit confondue avec (C).

En combinant les propriétés précédentes, on obtient une condition nécessaire et suffisante pour que (C) puisse être définie par une équation à coefficients réels : la courbe déduite de $\overline{(w)}$ par $\overline{\mathfrak{R}}$ doit être identique à la courbe déduite de (w) par $\mathfrak{R}$. Le lemne du paragraphe 1 permet encore de transformer cette condition en l'ensemble des 2 suivantes :

1° les coefficients p et q de (w) vérifient les relations :

$$\frac{\bar{p}^3}{\bar{q}^2} = \frac{p^3}{q^2}.$$

2° la correspondance $\overline{\mathfrak{R}}$ est identique à un produit de la forme :

$$\mathfrak{L}.\mathfrak{T}_A.\mathfrak{R};$$

où le coefficient λ de $\mathfrak{L}$ vérifie les relations :

$$\bar{p} = \lambda^4 p, \ \bar{q} = \lambda^6 q.$$

On peut reconnaitre effectivement si ces dernières conditions sont vérifiées : la condition 1 exige un simple calcul numérique sur les coefficients p et q; on peut alors déterminer les valeurs de λ (en nombre fini) vérifiant les relations imposées; on considère ensuite les coordonnées de A comme des indéterminées et on forme le produit $\mathfrak{L}.\mathfrak{T}_A.\mathfrak{R}$ en fonction de ces coordonnées indéterminées; en identifiant les coefficients de ce produit avec ceux de $\overline{\mathfrak{R}}$ on obtient un système de relations entre les coordonnées indéterminées; la condition 2 exige que ce système ait une solution (et une seule) pour une des valeurs possibles de λ. Le problème posé se trouve ainsi résolu; nous allons encore montrer que, si la courbe (C) admet une équation à coefficients réels, on peut simplifier sa définition par le théorème :

Théorème 1.

Une courbe de genre un à coefficients réels peut être déduite d'une cubique (w) :

$$y^2 = x^3 + px + q, \ (4\,p^3 + 27\,q^2 \neq 0);$$

à coefficients réels, par une correspondance birationnelle $\mathfrak{R}$ *à coefficients complexes, telle que le produit* $\overline{\mathfrak{R}}.\mathfrak{R}^{-1}$ *soit une translation sur* (w).

Démonstration.

Si une courbe (C) de genre un, à coefficients réels, est définie par une cubique (w_1) et une correspondance $\mathcal{R}_{\bar{1}}$ à coefficients complexes, les coefficients p_1 et q_1 de (w_1) vérifient la relation :

$$\frac{\overline{p_1}^3}{\overline{q_1}^2} = \frac{p_1^3}{q_1^2}.$$

Il en résulte l'existence d'un nombre fini de nombres complexes λ tels que :

$$\overline{p_1} = \lambda^4 p_1, \qquad \overline{q_1} = \lambda^6 q_1.$$

De plus, pour l'un de ces nombres λ, la correspondance $\mathcal{R}_1$ vérifie une identité de la forme :

(1) $$\overline{\mathcal{R}_1} = \mathcal{L}.\,\mathcal{T}_A.\,\mathcal{R}_1.$$

où $\mathcal{L}$ est l'homologie du plan définie par les relations :

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

et où A est un point convenablement choisi sur (w_1).

Or les règles de calcul des imaginaires montrent que, si une relation entre êtres géométriques est vérifiée, il en est de même de la relation obtenue en remplaçant chacun de ces êtres par son imaginaire conjugué. On déduit ainsi de la relation (1) :

(1') $$\mathcal{R}_1 = \overline{\mathcal{L}}.\,\mathcal{T}_{\overline{A}}.\,\overline{\mathcal{R}_1}.$$

En comparant (1) et (1'), on obtient encore :

$$\mathcal{R}_1 = \overline{\mathcal{L}}.\,\mathcal{T}_{\overline{A}}.\,\mathcal{L}.\,\mathcal{T}_A.\,\mathcal{R}_1;$$

ce qui exige que le produit :

$$\overline{\mathcal{L}}.\,\mathcal{T}_{\overline{A}}.\,\mathcal{L}.\,\mathcal{T}_A,$$

soit la correspondance identique sur (w_1) (puisque la correspondance $\mathcal{R}_1$ admet un inverse). La formule de permutation rappelée au paragraphe 1 permet d'écrire ce produit :

$$\overline{\mathcal{L}}.\,\mathcal{L}.\,\mathcal{T}_{\mathcal{L}(\overline{A})}.\,\mathcal{T}_A = \overline{\mathcal{L}}.\,\mathcal{L}.\,\mathcal{T}_{\mathcal{L}(\overline{A})+A}.$$

Nous avons rappelé que les correspondances sur (w_1) se mettent de façon *unique* sous la forme $\mathcal{J}.\,\mathcal{T}_A$; donc ce produit est la correspondance identique sur (w_1) si et seulement si :

$$\overline{\mathcal{L}}.\,\mathcal{L} = 1$$

$$\mathcal{L}(\overline{A}) + A = 0.$$

La première relation (entre homologies) est d'ailleurs équivalente à la relation entre scalaires :

$$\lambda.\,\overline{\lambda} = 1$$

puisque le groupe des homologies $\mathcal{L}$ est isomorphe au groupe multiplicatif de leurs coefficients λ.

Considérons alors la cubique (w) définie par la relation :

$$y^2 = x^3+(1+\lambda)^4 p_1 x+(1+\lambda)^6 q_1 \quad (\text{si } \lambda \neq -1)$$

ou :

$$y^2 = x^3+(1-\lambda)^4 p_1 x+(1-\lambda)^6 q_1. \quad (\text{si } \lambda = -1).$$

Cette cubique est bien de genre un, puisque :

$$4\,p^3+27\,q^2 = (4\,p_1^3+27\,q_1^2)\,(1+\lambda)^6 \neq 0, \qquad (\lambda \neq -1);$$
$$4\,p^3+27\,q^2 = (4\,p_1^3+27\,q_1^2)\,(1-\lambda)^6 \neq 0, \qquad (\lambda = -1).$$

D'ailleurs (w) se déduit de (w_1) par l'homologie plane non dégénérée $\mathcal{L}_1$ définie par les relations :

$$x' = (1+\lambda)^2 x, \quad y' = (1+\lambda)^3 y, \quad (\lambda \neq -1);$$

ou

$$x' = (1-\lambda)^2 x, \quad y' = (1-\lambda)^3 y, \quad (\lambda = -1).$$

Or la relation (2) et les relations entre p_1, q_1, $\overline{p_1}$, $\overline{q_1}$ et λ montrent que :

$$(1+\bar{\lambda})^4\,\bar{p}_1 = \left(1+\frac{1}{\lambda}\right)^4 \lambda^4\,p_1 = (1+\lambda)^4\,p_1,$$

$$(1-\bar{\lambda})^4\,\bar{p}_1 = \left(1-\frac{1}{\lambda}\right)^4 \lambda^4\,p_1 = (1-\lambda)^4\,p_1,$$

$$(1+\bar{\lambda})^6\,\bar{q}_1 = \left(1+\frac{1}{\lambda}\right)^6 \lambda^6\,q_1 = (1+\lambda)^6\,q_1,$$

$$(1-\bar{\lambda})^6\,\bar{q}_1 = \left(1-\frac{1}{\lambda}\right)^6 \lambda^6\,q_1 = (1-\lambda)^6\,q_1,$$

Donc les coefficients de (w) sont réels dans tous les cas.

D'autre part (C) peut aussi être déduite de (w) par la correspondance birationnelle :

$$\mathcal{R} = \mathcal{L}_1^{-1}.\,\mathcal{R}_1$$

Calculons le produit :

$$\overline{\mathcal{R}}.\,\mathcal{R}^{-1} = \overline{\mathcal{L}_1}^{-1}.\,\overline{\mathcal{R}_1}.\,\mathcal{R}_1^{-1}.\,\mathcal{L}_1,$$

ou, d'après la relation (1) :

$$\overline{\mathcal{R}}.\,\mathcal{R}^{-1} = \overline{\mathcal{L}_1}^{-1}.\,\mathcal{L}.\,\mathcal{T}_A.\,\mathcal{R}_1.\,\mathcal{R}_1^{-1}.\,\mathcal{L}_1$$
$$= \overline{\mathcal{L}_1}^{-1}.\,\mathcal{L}.\,\mathcal{T}_A.\,\mathcal{L}_1;$$

ou encore, d'après la formule de permutation :

$$\overline{\mathcal{R}}.\,\mathcal{R}^{-1} = \overline{\mathcal{L}_1}^{-1}.\,\mathcal{L}.\,\mathcal{L}_1.\,\mathcal{T}_{\mathcal{L}_1(A)}$$

Or, d'après la relation (2) :

$$(1+\bar{\lambda})^{-1}\,\lambda\,(1+\lambda) = \left(1+\frac{1}{\lambda}\right)^{-1} \lambda\,(1+\lambda) = 1;$$

$$(1-\bar{\lambda})^{-1}\,\lambda\,(1-\lambda) = \left(1-\frac{1}{\lambda}\right)^{-1} \lambda\,(1-\lambda) = 1;$$

ce qui montre que le produit :

$$\overline{\mathcal{L}_1}^{-1}.\,\mathcal{L}.\,\mathcal{L}_1$$

est la correspondance identique sur (w). Donc le produit $\overline{\mathfrak{R}}.\mathfrak{R}^{-1}$ est une translation $\mathcal{T}_{\mathcal{L}_1(A)}$ sur (w).

3. — Abordons maintenant le problème essentiel : *reconnaître s'il existe des points réels sur une courbe (C) de genre un donnée.*

Si la courbe (C) n'admet pas d'équation à coefficients réels, les points reéls de (C) font partie de son intersection avec son imaginaire conjuguée $(\overline{C})$; or cette intersection est formée d'un nombre fini de points qu'on peut obtenir effectivement et dont on peut reconnaitre si certains sont réels.

Nous considèrerons alors seulement le cas où (C) admet une équation à coefficients réels. D'après le théorème 1, on peut supposer que (C) est définie par une cubique (w) à coefficients réels et une correspondance birationnelle $\mathfrak{R}$ telle que :

$$\overline{\mathfrak{R}}.\mathfrak{R}^{-1} = \mathcal{T}_A, \tag{1}$$

où A est un point convenablement choisi sur (w). Remarquons que la relation précédente et la relation imaginaire conjuguée :

$$\mathfrak{R}.\overline{\mathfrak{R}}^{-1} = \mathcal{T}_{\overline{A}}, \tag{1'}$$

entraînent que le produit :

$$\mathcal{T}_A.\mathcal{T}_{\overline{A}}$$

est la correspondance identique sur (w), donc encore que :

$$A + \overline{A} = 0. \tag{3}$$

Cette dernière relation exprime que les points imaginaires conjugués A et $\overline{A}$ sont opposés sur (w), c'est-à-dire alignés avec le point « nul » sur cette courbe qui est le point à l'infini dans la direction de Oy; comme (w) est symétrique par rapport à Ox, cette condition exprime encore que ces points sont symétriques par rapport à Ox. — On peut aussi utiliser le fait que $\wp u$ est une fonction paire et $\wp' u$ une fonction impaire de u. — Il en résulte que A et $\overline{A}$ ont une abscisse commune, donc réelle, et des ordonnées opposées, imaginaires pures. Il nous sera commode dans la suite d'associer au point A le point A′ *réel* qui s'en déduit par l'homologie :

$$x' = -x, \quad y' = i\,y;$$

il est situé sur la cubique (w') :

$$y^2 = x^3 + px - q.$$

Nous allons chercher les points réels de (C) en cherchant leurs images sur (w). Il y a lieu de remarquer que certains points de (C) échappent à cette méthode : ceux dont le transformé dans $\mathfrak{R}^{-1}$ n'est pas déterminé — ou qui admettent plusieurs paramètres elliptiques — c'est-à-dire les points multiples. Mais on peut obtenir directement ces points, qui sont en nombre fini, par des opérations algébriques et reconnaître si certains d'entre eux sont réels. Nous chercherons donc seulement les points réels *simples* sur (C) en démontrant le théorème :

Théorème 2.

Si $4p^3 + 27q^2 > 0$, *la courbe* (*C*) *contient des points réels simples; si* $4p^3 + 27q^2 < 0$, *la courbe* (*C*) *contient ou non des points réels simples suivant que le point réel* A′ *associé à la constante* A *de la translation* $\overline{\mathcal{R}}.\mathcal{R}^{-1}$ *est situé sur la branche infinie ou sur la branche fermée de la cubique* (w').

Démonstration.

Pour qu'un point M de (C) soit réel, il faut et il suffit qu'il soit identique à son imaginaire conjugué. Puisque M est simple, il a une image unique N sur (w) (transformé de M dans $\mathcal{R}^{-1}$) et le conjugué $\overline{\mathrm{M}}$ de M est le transformé de $\overline{\mathrm{N}}$ dans $\overline{\mathcal{R}}$. La condition nécessaire et suffisante pour que M soit réel peut donc s'écrire :

$$\mathcal{R}(\mathrm{N}) = \overline{\mathcal{R}}(\overline{\mathrm{N}});$$

ou encore, d'après la relation (1) :

$$\overline{\mathcal{R}}, \mathcal{R}^{-1}(\overline{\mathrm{N}}) = \mathcal{C}_{\mathrm{A}}(\overline{\mathrm{N}}) = \mathrm{N};$$

ou enfin :

$$\overline{\mathrm{N}} + \mathrm{A} = \mathrm{N}. \tag{4}$$

Si u désigne l'argument elliptique de N et a celui de A, cette relation est équivalente à l'égalité :

$$u - \overline{u} = a$$

au module près des périodes. Or $u - \overline{u}$ est un nombre imaginaire pur, puisque le nombre imaginaire conjugué $\overline{u} - u$ est son opposé. Inversement, tout nombre imaginaire pur bi est de la forme :

$$\frac{b}{2}i - \left(-\frac{b}{2}i\right) = u - \overline{u}.$$

Une condition nécessaire et suffisante pour qu'il existe des points réels sur (C) est donc que l'argument elliptique a de A soit un nombre imaginaire pur au module près des périodes. Comme l'argument elliptique de A′ est égal à $a' = \frac{a}{i}$, cette condition est encore équivalente à celle que l'argument elliptique de A′ sur (w') soit un nombre réel.

On est ainsi ramené à un problème classique en théorie des fonctions elliptiques; reconnaître si un point réel A′ sur une cubique (w') à coefficients réels admet un argument elliptique réel (au module près des périodes). La théorie des fonctions elliptiques montre qu'il faut distinguer 2 cas suivant le signe de la quantité $4p'^3 + 27q'^2 = 4p^3 + 27q^2$:

1° si $4p^3 + 27q^2 > 0$, les périodes principales 2ω et $2\omega'$ de (w') sont imaginaires conjuguées; la partie réelle de cette courbe est composée d'une seule branche formée par les points dont l'argument elliptique est réel (au module près des périodes);

2° si $4p^3 + 27q^2 < 0$, les périodes principales de (w') sont, l'une 2ω réelle, l'autre $2\omega'$ imaginaire pure; la partie réelle de (w') est composée d'une branche infinie formée par les points dont l'argument elliptique est réel et d'une branche fermée formée par les points dont l'argument elliptique est la somme de la demi-période ω' et d'un nombre réel (au module près des périodes).

Ce qui démontre le théorème.

4. — Nous allons encore compléter les résultats précédents en répartissant les courbes de genre un en classes de courbes qui se déduisent les unes des autres par des correspondances birationnelles à coefficients réels.

Démontrons d'abord le théorème :

Théorème 3.

Si $4p^3 + 27q^2 > 0$, la courbe (C) peut être déduite de la cubique (w) par une correspondance birationnelle à coefficients réels.

Démonstration.

Nous avons vu que, dans ce cas, il existe sur (w) des points qui vérifient la relation symbolique (4). Choisissons l'un d'entre eux que nous appelons B et formons le produit $\mathfrak{R}^* = \mathcal{T}_B . \mathfrak{R}$; ce produit est encore une correspondance birationnelle entre (w) et (C). De plus, la relation (1) montre que :

$$\overline{\mathfrak{R}^*} = \overline{\mathcal{T}_B} . \overline{\mathfrak{R}} = \mathcal{T}_{\overline{B}} . \mathcal{T}_A . \mathfrak{R}.$$

Or le produit $\mathcal{T}_{\overline{B}} . \mathcal{T}_A$ est la translation sur (w) d'amplitude $\overline{B} + A$ et cette amplitude est encore égale à B puisque B vérifie la relation (4). Donc :

$$\overline{\mathfrak{R}^*} = \mathcal{T}_B . \mathfrak{R} = \mathfrak{R}^*.$$

Ce qui montre que les coefficients de $\mathfrak{R}^*$ sont réels et démontre le théorème.

Une correspondance birationnelle à coefficients réels entre 2 courbes transforme les points réels simples de l'une en les points réels simples de l'autre. Si $4p^3 + 27q^2 < 0$ et si A' est sur la branche fermée de (w'), (C) ne contient pas de point réel simple, d'après le théorème 2; donc il ne peut être déduit par une correspondance birationnelle à coeffiicients réels de (w) qui contient des points réels simples. Nous allons préciser ce résultat :

Théorème 4.

Si $4p^3 + 27q^2 < 0$, les courbes (C) qui correspondent aux points A' de la branche infinie de (w') peuvent être déduites de (w) par des correspondances birationnelles à coefficients réels et celles qui correspondent aux points A' de la branche fermée de (w') peuvent être déduites de l'une d'entre elles (C_1) par des correspondances birationnelles à coefficients réels.

Démonstration.

La démonstration du théorème 3 reste valable pour les courbes (C) qui correspondent aux points A' de la branche infinie de (w') puisqu'il existe, dans ce cas, des points de (w) vérifiant la relation (4). Ce qui démontre la première partie du théorème.

Considérons maintenant 2 courbes (C_1) et (C) correspondant à 2 points A'_1 et A' de la branche fermée de (w'). La différence $A' - A'_1$ est un point de la branche infinie de (w'), car son argument elliptique est réel. (C'est la différence de 2 nombres de la forme : ω' + un nombre réel, au module près des périodes.) Donc il existe sur (w) des points qui vérifient la relation :

$$\overline{M} + A - A_1 = M. \tag{5}$$

Choisissons l'un d'entre eux B et formons le produit :

$$\mathfrak{R}^* = \mathfrak{R}_1^{-1}.\,\mathcal{T}_B.\,\mathfrak{R};$$

c'est une correspondance birationnelle entre (C_1) et (C). De plus, la relation (1) montre que :

$$\overline{\mathfrak{R}^*} = \mathfrak{R}_1^{-1}.\,\mathcal{T}_{\overline{B}}.\,\overline{\mathfrak{R}} = \mathfrak{R}_1^{-1}.\,\mathcal{T}_{-A_1}.\,\mathcal{T}_{\overline{B}}.\,\mathcal{T}_A.\,\mathfrak{R}.$$

Mais le produit $\mathcal{T}_{A_1}.\ \mathcal{T}_{\overline{B}}.\ \mathcal{T}_A$ est une translation sur (w) d'amplitude $A - A_1 + \overline{B}$ qui est égale à B, puisque B vérifie la relation (5). Donc :

$$\overline{\mathfrak{R}^*} = \mathfrak{R}_1^{-1}.\,\mathcal{T}_B.\,\mathfrak{R} = \mathfrak{R}^*.$$

Ce qui montre que la correspondance $\mathfrak{R}^*$ a ses coefficients réels et démontre le théorème.

Il reste encore à savoir s'il existe effectivement des courbes de genre un sans point réel simple et à construire des modèles de telles courbes. On obtient de telles courbes notamment dans l'étude de la réduction des intégrales elliptiques [6]. On est en effet conduit à remarquer que l'équation :

$$y^2 + R_4(x) = 0$$

n'a pas de solutions réelles si R_4 est un polynome du 4 degré constamment positif, c'est-à-dire dont les 4 racines sont toutes imaginaires et dont le coefficient de x^4 est positif (un tel polynome R_4 ne conduit pas à une intégrale elliptique dans le champ réel). Une des méthodes de réduction des intégrales elliptiques permet encore d'associer des quartiques de la forme précédente à toute cubique (w) telle que $4p^3 + 27q^2 > 0$. On est en effet conduit à considérer la courbe définie par la représentation elliptique :

$$x = \frac{1}{2}\,\frac{\wp'' u - \wp' a}{\wp u - \wp a}, \qquad Y = \wp u - \wp(u + a);$$

où a est une constante; cette courbe admet l'équation :

$$Y^2 = X^4 - 6\,\wp a\,X^2 + 4\,\wp' a\,X - 4p - 3\,\wp^2 a.$$

6. Voir, Baire, *loc. cit.*, pp. 330-34.

Il suffit de changer X en iX, Y en iY et a en $-a$ pour obtenir une courbe de la forme voulue :

$$Y^2 + X^4 + 6\,\wp a\, X^2 - 4\,i\,\wp' a\, X - 4p - 3\,\wp^2 a = 0.$$

On choisit a de manière que $\wp a$ soit réel et que $\wp' a$ soit imaginaire pur, donc que le point A d'argument elliptique a sur (w) vérifie la relation (3).

Cette courbe (C_A) admet la représentation elliptique :

$$i\,X = \frac{1}{2}\,\frac{\wp' u + \wp' a}{\wp u - \wp a}, \quad i\,Y = \wp u - \wp\,(u = a).$$

Il en résulte que (C_A) peut être déduite de (w) par la correspondance birationnelle $\mathcal{R}_A$:

$$X = -\,i\,\frac{y+\beta}{x-\alpha}, \quad Y = i\left(\frac{y+\beta}{x-\alpha}\right)^2 - 2\,ix - i\alpha;$$

$$x = \frac{1}{2}(i\,Y - X^2 - \alpha), \quad y = -\frac{X}{2}(Y + i\,X^2 + 3\,i\alpha) - \beta;$$

où α et β désignent les coordonnées du point de (w) d'argument elliptique a. Or, en remplaçant u par $u + a = u - \bar{a}$ (puisque A vérifie la relation (3) et en utilisant des formules classiques en théorie des fonctions elliptiques (7), on obtient la représentation :

$$i\,X = \frac{1}{2}\,\frac{\wp'(u-\bar{a}) - \wp'\bar{a}}{\wp(u-\bar{a}) - \wp\bar{a}} = \frac{1}{2}\,\frac{\wp'(-u) - \wp'\bar{a}}{\wp(-u) - \wp\bar{a}} = -\frac{1}{2}\,\frac{\wp' u + \wp'\bar{a}}{\wp u - \wp\bar{a}},$$

$$i\,Y = \wp\,(u - \bar{a}) - \wp\,u;$$

qui n'est autre que la représentation imaginaire conjuguée de la représentation primitive. Il en résulte que :

$$\overline{\mathcal{R}}_A = \mathcal{C}_A . \mathcal{R}_A;$$

donc (C_A) est associée à la cubique (w) et au point A sur (w) au sens du théorème 1. Il suffit alors de choisir A de manière que A′ soit sur la branche fermée de (w') pour obtenir une courbe de genre un sans point réel associé à (w).

Si on désigne, suivant l'habitude par e_1, e_2, e_3 les 3 racines (toutes réelles) de l'équation :

$$x^3 + px + q = 0, \quad (4\,p^3 + 27\,q^2 < 0),$$

rangées dans un ordre tel que :

$$e_1 > e_2 > e_3,$$

le point $-e_2$, 0 est sur la branche fermée de (w'). On peut donc choisir $\wp a = e_2$, $\wp' a = 0$; *la courbe* (C_{E_2}) correspondante est la quartique :

$$Y^2 + X^4 + 6\,e_2\,X^2 - 4\,p - 3\,e_2^2 = 0.$$

7. Voir Baire, *loc. cit.*, p. 309, formule (7).

On vérifie aisément directement que cette courbe n'a pas de point réel : e_2 est compris entre $-\sqrt{-\frac{p}{3}}$ et $+\sqrt{-\frac{p}{3}}$, donc :

$$3e_2^2 + p < 0$$

et par suite le polynome :

$$x^2 + 6e_2 x - 4p - 3e_2^2$$

n'a aucun zéro réel et il en est *à fortiori* de même du polynome :

$$X^4 + 6e_2 X - 4p - 3e_2^2.$$

Ce qui montre que toute courbe de genre un à coefficients réels peut être déduite, par une correspondance birationnelle à coefficients réels, soit d'une cubique (w) de la forme :

$$y^2 = x^3 + px + q \qquad (4p^3 + 27q^2 \neq 0)$$

soit d'une quartique (C_{E_2}) de la forme:

$$Y^2 + X^4 + 6e_2 X^2 - 4p - 3e_2^2 = 0 \quad (3e_2^2 + p < 0).$$

5. — Nous allons encore préciser le dernier résultat obtenu en démontrant le théorème :

Théorème 5.

Toute courbe de genre un à coefficients réels peut être déduite, par une correspondance birationnelle à coefficients réels, d'une et d'une seule courbe de l'une des formes suivantes :

(1) $y^2 = x^3 + px + 2$
(2) $y^2 = x^3 + px - 2$ — $p \neq -3$
(3) $Y^2 + X^4 + 6X^2 - 4p - 3 = 0$
(4) $Y^2 + X^4 - 6X^2 - 4p + 3 = 0$ — $p < -3$
(5) $y^2 = x^3 + x$
(6) $y^2 = x^3 - x$
(7) $Y^2 + X^4 + 4 = 0.$

Démonstration.

On voit qu'une cubique (w) :

$$y_2 = x^3 + px + q, \qquad (4p^3 + 27q_2 \neq 0);$$

peut être ramenée à l'une des 2 premières formes si $q \neq 0$, à la 5[e] ou à la 6[e] si $q = 0$, par une homologie du plan de la forme :

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

avec λ réel. Une quartique de la forme :

$$Y^2 + X^4 + 6e_2 X^2 - 4p - 3e_2^2 = 0 \quad (3e_2^2 + p < 0)$$

peut être ramenée à la 3[e] ou à la 4[e] forme si $e_2 \neq 0$, à la 7[e] si $e_2 = 0$, par une homologie de la forme :

$$X' = \lambda X, \quad Y' = \lambda^2 Y$$

avec λ réel. Il reste à démontrer que les courbes indiquées ne peuvent se déduire les unes des autres par des correspondances birationnelles à coefficients réels.

Cherchons d'abord à quelles conditions les 2 cubiques :

(w) $$y^2 = x^3 + px + q$$

et (w') $$y^2 = x^3 + p'x + q'$$

peuvent être déduites l'une de l'autre par une correspondance birationnelle à coefficients réels. D'après le lemne du paragraphe 1, il est nécessaire qu'il existe des nombres complexes λ tels que :

$$p' = \lambda^4 p, \quad q' = \lambda^6 q. \tag{6}$$

En désignant par $\mathcal{L}$ l'une des homologies du plan de la forme :

$$x' = \lambda^2 x, \quad y' = \lambda^3 y;$$

où λ est une solution des relations (6), toute correspondance birationnelle entre (w) et (w') peut être mise sous la forme d'un produit :

$$\mathcal{T}_A . \mathcal{L};$$

où $\mathcal{T}_A$ est une translation sur (w). Pour que les coefficients de cette correspondance soient réels, il faut et il suffit qu'elle soit identique à sa conjuguée, donc que :

$$\mathcal{T}_A . \mathcal{L} = \mathcal{T}_{\bar{A}} \overline{\mathcal{L}}.$$

Ce qui exprime encore que le produit :

$$\mathcal{T}_{-A} . \mathcal{T}_{\bar{A}} . \overline{\mathcal{L}} . \mathcal{L}^{-1} = \mathcal{T}_{-A+\bar{A}} . \overline{\mathcal{L}} . \mathcal{L}^{-1},$$

est la correspondance identique sur (w) ; puisque le groupe des translations sur (w) et le groupe des homologies $\mathcal{L}$ n'ont en commun que la correspondance identique sur (w), cette condition exige que le produit $\overline{\mathcal{L}} . \mathcal{L}^{-1}$ soit la correspondance identique. Mais, s'il en est ainsi, la correspondance $\mathcal{L}$ elle-même a ses coefficients réels, c'est-à-dire que λ est réel. Ainsi, les cubiques (w') qui peuvent se déduire de (w) par des correspondances à coefficients réels sont celles dont les coefficients sont de la forme :

$$p' = \lambda^4 p, \quad q' = \lambda^6 q;$$

avec λ *réel*. Ce qu'on peut encore exprimer par les 2 conditions : (w) et (w') ont même module :

$$\frac{4\,p^3 + 27\,q^2}{q^2} = \frac{4\,p'^3 + 27\,q'^2}{q'^2}$$

les coefficients correspondants de (w) et (w') ont le même signe.

Or on constate que 2 des cubiques indiquées dans le théorème ont, soit des modules différents, soit des coefficients de signes contraires.

Les quartiques indiquées dans le théorème n'ont pas de points réels donc ne peuvent se déduire des cubiques par des correspondances birationnelles à coefficients réels. Il reste à chercher si elles peuvent se déduire entre elles par de telles correspondances.

La quartique (C_{E_2})

$$Y^2 + X^4 + 6\,e_2\,X^2 - 4\,p - 3\,e_2^2 = 0$$

peut être déduite de la cubique (w) :

$$y^2 = x^3 + px - e^3_2 - p\, e_2$$

par la correspondance à coefficients complexes $\mathcal{R}_{E_2}$, où E_2 désigne le point de (w) de coordonnées e^2, 0. Pour la quartique $(C'_{E'_2})$:

$$Y^2 + X^4 + 6\, e'_2\, X^2 - 4\, p' - 3\, e'^2_2 = 0$$

puisse être déduite de (C_{E_2}) par une correspondance birationnelle à coefficients réels, il est d'abord nécessaire que (C_{E_2}) puisse être déduite de la cubique (w') par une correspondance birationnelle à coefficients complexes. Il doit donc exister un nombre complexe λ tel que :

$$p' = \lambda^4 p, \quad e^2_2 + p\, e_2 = \lambda^6 (e'^2_2 + p\, e'_2).$$

En désignant par $\mathcal{L}$ l'homologie :

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

toute correspondance birationnelle entre (w') et (C_{E_2}) est alors de la forme :

$$\mathcal{L}.\mathcal{T}_A.\, \mathcal{R}_{E_2},$$

en vertu du lemne du paragraphe 1. Donc les correspondances birationnelles entre $(C'_{E'_2})$ et (C_{E_2}) sont de la forme :

$$\mathcal{R}^{-1}_{E'_2}\, \mathcal{L}.\, \mathcal{T}_A.\, \mathcal{R}_{E_2}.$$

Pour qu'une telle correspondance ait ses coefficients réels, il faut et il suffit que :

$$\mathcal{R}^{-1}_{E'_2}.\, \mathcal{L}.\, \mathcal{T}_A.\, \mathcal{R}_{E_2} = \overline{\mathcal{R}^{-1}_{E'_2}}.\, \overline{\mathcal{L}}.\, \mathcal{T}_{\bar{A}}.\, \overline{\mathcal{R}_{E_2}}.$$

En vertu des relations :

$$\overline{\mathcal{R}_{E_2}} = \mathcal{T}_{E_2}.\, \mathcal{R}_{E_2},\ \overline{\mathcal{R}_{E'_2}} = \mathcal{T}_{E'_2}.\, \mathcal{R}_{E'_2},$$

cette relation peut encore s'écrire :

$$\mathcal{R}^{-1}_{E'_2}.\, \mathcal{L}.\, \mathcal{T}_A.\, \mathcal{R}_{E_2} = \overline{\mathcal{R}^{-1}_{E'_2}}.\, \mathcal{T}^{-1}_{E'_2}\, \overline{\mathcal{L}}.\, \mathcal{T}_{\bar{A}}.\, \mathcal{T}_{E_2}.\, \mathcal{R}_{E_2}$$

et encore :

$$\mathcal{L}^{-1}.\, \mathcal{T}^{-1}_{E'_2}.\, \overline{\mathcal{L}}.\, \mathcal{T}_{\bar{A}}.\, \mathcal{T}_{E_2}.\, \mathcal{T}^{-1}_A = \mathcal{L}^{-1}.\, \overline{\mathcal{L}}.\, \mathcal{T}_{-\mathcal{L}(E'_2)}.\, \mathcal{T}_{\bar{A}}.\, \mathcal{T}_{E_2}.\, \mathcal{T}_{-A} = 1.$$

Ce qui exige que le produit $\mathcal{L}^{-1}.\, \overline{\mathcal{L}}$ soit la correspondance identique sur (w), donc que $\mathcal{L}$ ait ses coefficients réels. D'après les résultats précédents, cette condition peut se traduire par l'égalité des modules de (w) et (w') et l'identité des signes de leurs coefficients. Or on constate que les cubiques (w) associées à 2 des quartiques du théorème ont, soit des modules différents, soit des coefficients de signes contraires.

Rappel des notations essentielles.

(w) : cubique définie par l'équation :

$$y^2 = x^3 + px + q \quad (4\,p^3 + 27\,q^2 \neq 0)$$

ou par la représentation elliptique :

$$x = \wp\, u\,, \qquad y = \frac{1}{2}\wp'\, u\,.$$

(C) : courbe de genre un.

$\mathfrak{T}_A$: translation sur (w) définie par les relations :

$$M' = M + A, \quad u' = u + a.$$

$\mathfrak{J}$: correspondance birationnelle sur (w) laissant invariant le point nul :

$$x' = \lambda^2 x, \quad y' = \lambda^3 y, \quad u' = \lambda^{-1} u$$
$$(\lambda = \pm 1, \quad \pm i\,(q = 0), \quad \pm j, \quad \pm j^2\,(p = 0)).$$

$\mathfrak{L}$: correspondance birationnelle particulière $(w) \rightarrow (w')$:

$$x' = \lambda^2 x, \quad y' = \lambda^3 y, \quad u' = \lambda^{-1} u$$
$$\text{si } p' = \lambda^4 p, \quad q' = \lambda^6 q.$$

$\mathfrak{R}$: correspondance birationnelle arbitraire $(w) \rightarrow (C)$:

(voir lemne du paragraphe 1).