Le théorème de Poncelet

Sylvain Ervedoza et Guillaume Pouchin

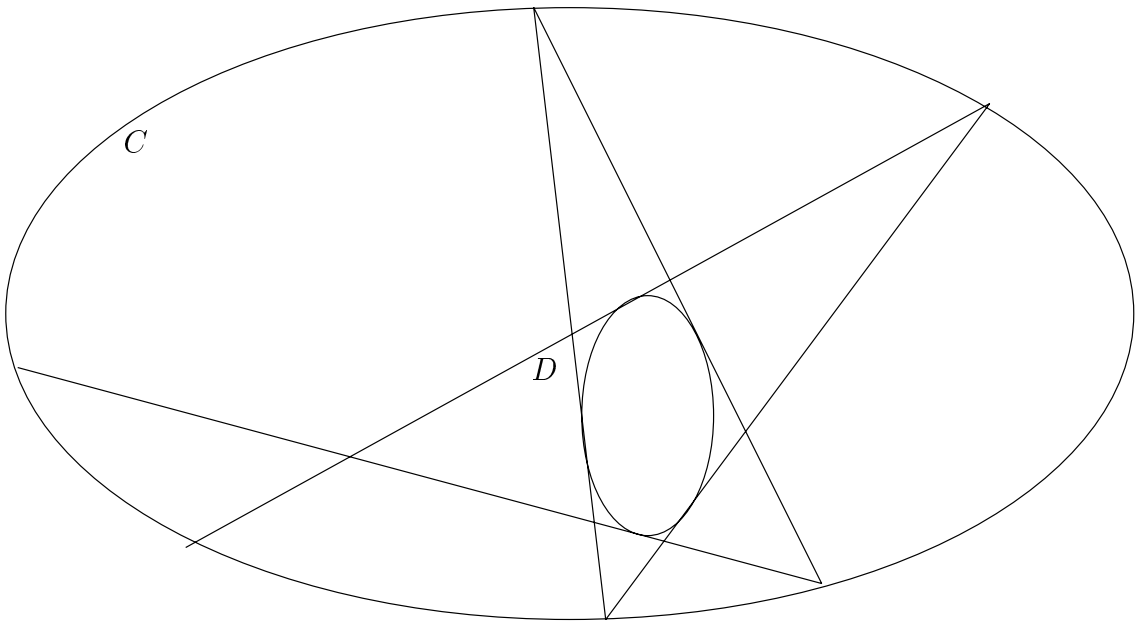
26 juin 2003

Table des matières

1 Partie théorique **2**
1.1 La correspondance entre $\mathbb{C}/\Lambda$ et les courbes elliptiques 2
1.1.1 La fonction $\wp_\Lambda$ de Weierstrass 2
1.1.2 Les courbes elliptiques 4
1.2 Théorème d'Abel 6

2 Application au théorème de Poncelet **9**
2.1 Introduction 9
2.2 Rapport avec les courbes elliptiques 9
2.3 Une démonstration du théorème de Poncelet 12

3 Quelques précisions ... **12**

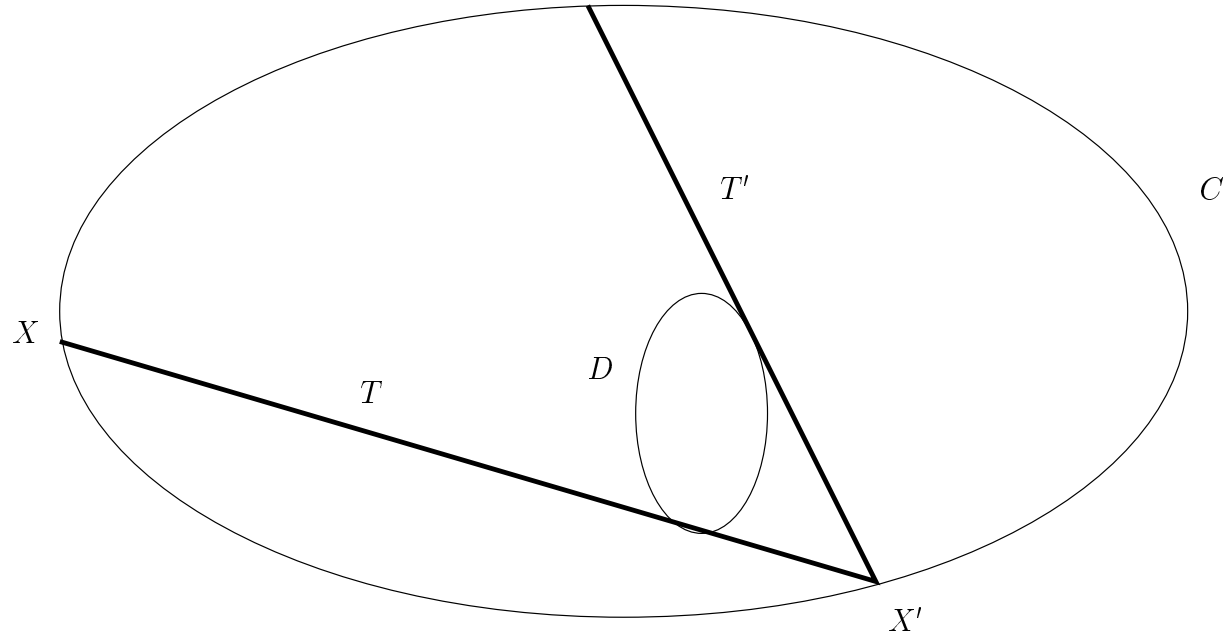


Une construction de Poncelet

Introduction

Cet exposé traite d'un problème géométrique, posé et résolu par Poncelet dans le courant du dix-neuvième siècle, qui s'énonce sous la forme :

Théorème 1 (Poncelet). *Soit deux coniques non dégénérées n'ayant pas de point d'intersection double. La construction de Poncelet est la suivante :*



La construction de Poncelet

On prend un point X sur la première conique C, on trace ensuite une des deux tangentes T à la deuxième D passant par ce point, puis l'autre tangente T' à D passant par X' le point d'intersection de C et T.

Le résultat est alors le suivant : si le procédé, partant de X fixé, boucle après n étapes, alors il boucle pour tout point de départ, le nombre d'étapes n étant toujours le même.

1 Partie théorique

1.1 La correspondance entre $\mathbb{C}/\Lambda$ et les courbes elliptiques

1.1.1 La fonction $\wp_\Lambda$ de Weierstrass

Définition 1. Les fonctions elliptiques sont des fonctions de $\mathbb{C}$ dans $\mathbb{C}$ méromorphes ayant une double périodicité, c'est-à-dire qu'il existe ω_1 et ω_2 qui ne sont pas $\mathbb{R}$-liés dans $\mathbb{C}$ tels que pour tout complexe z' du réseau $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, pour tout z dans $\mathbb{C}$, $f(z + z') = f(z)$

Le lien entre le quotient $\mathbb{C}/\Lambda$ et les courbes elliptiques est donné par une fonction elliptique importante : la fonction $\wp_\Lambda$ de Weierstrass. Avant de définir la fonction $\wp_\Lambda$ de Weierstrass on démontre le lemme suivant :

Lemme 1. Soit Λ un réseau. La série $\sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^\alpha}$ converge dès que $\alpha > 2$.

Démonstration . On pose $\Lambda' = \Lambda \setminus \{0\}$. On a la majoration suivante par simple dénombrement :

$$\sum_{\omega\in\Lambda',\|\omega\|=N} \frac{1}{\|\omega\|^s} = \frac{8N}{N^s} = \frac{8}{N^{s-1}}$$

avec $\|.\| = \|.\|_\infty$ la norme infinie associée au réseau. Or, pour une certaine constante positive C, on a :

$$\sum_{\omega\in\Lambda'} \frac{1}{|\omega|^s} \leq C \sum_{(m,n)\in\mathbb{Z}\setminus\{(0,0)\}} \frac{1}{[sup(m,n)]^s}$$

Donc $\sum_{N=1}^{\infty}(\sum_{\|\omega\|=N} \frac{1}{\|\omega\|^s})$ converge si $s > 2$. $\diamondsuit$

Définition 2. On définit la fonction $\wp_\Lambda$ de Weierstrass par la formule suivante :

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \frac{1}{(z-\omega)^2} - \frac{1}{w^2}$$

Par le lemme précédent, cette série converge absolument uniformément sur tout compact ne contenant pas de point de Λ. Cette fonction est donc méromorphe donc évidemment elliptique de réseau Λ, de pôles les éléments de Λ. Dans la suite, on notera $\wp$ à la place de $\wp_\Lambda$, en supposant que le réseau est déjà fixé. On remarque aussi que cette fonction est paire.

La propriété principale de $\wp$ qui nous servira est la suivante :

Théorème 2. *L'application $\wp$ vérifie l'équation différentielle*

$$(\wp'(z))^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

où les nombres G_4 et G_6 sont les fonctions de réseau :

$$G_{2k} = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^{2k}}$$

Démonstration . On peut considérer la différence du terme de gauche par le terme de droite ; la fonction obtenue sera elliptique (somme et produit de fonctions elliptiques) et sera un $\circ(1)$ en 0, en utilisant les développements en 0 :

$$\wp(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \circ(z^4)$$

$$\wp'(z) = -\frac{2}{z^3} + 6G_4z + 20G_6z^3 + \circ(z^3)$$

C'est donc une fonction elliptique bornée. En effet, ses pôles sont sur Λ, et elle est bornée en 0, donc elle n'a pas de pôle. Comme elle est aussi elliptique, elle est bornée, donc constante, et elle tend vers 0 en 0. Elle est donc nulle. $\diamondsuit$

On peut noter que, puisqu'on a convergence sur tout compact ne contenant pas de points dans Λ, la dérivée de $\wp$ s'écrit :

$$\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$$

qui est un fonction elliptique impaire. D'après la définition de l'ordre d'une fonction elliptique et un théorème de Liouville exposé dans la partie suivante, on peut déduire que comme $\wp'$ est d'ordre 3 (car son seul pôle à périodicité près est 0 qui est d'ordre 3), elle n'a que trois racines à périodicité près. Comme par imparité on trouve trois racines $\{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$, ce sont les seules à périodicité près. D'où

Théorème 3.

$$\wp'(z) = 0 \iff z \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\} \ mod\ \Lambda\ .$$

On utilise de même un théorème de Liouville pour démontrer le théorème suivant (en utilisant le fait que $\wp$ est d'ordre 2 et la remarque évidente $\wp(z) = 0 \Rightarrow \wp(-z) = 0$) :

Théorème 4. *L'équation $\wp(z) = u$ admet exactement deux solutions z,z' ou une solution double, l'autre solution étant $z' = -z$.*

1.1.2 Les courbes elliptiques

Définition 3. Une courbe elliptique E est définie par une équation :

$$y^2 = ax^3 + bx^2 + cx + d$$

où le polynôme $ax^3 + bx^2 + cx + d$ est séparable et de degré 3.

Définition 4. La complétée projective de E est définie par l'équation homogénéisée :

$$Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3$$

Cela ajoute le point à l'infini (0 :1 :0).

Par un changement affine sur x, on peut supprimer le terme de degré 2. De même en changeant y, on peut considérer que $a = 4$. Par la suite on considèrera l'équation $y^2 = 4x^3 + a'x + b'$. On peut voir alors le lien avec la fonction $\wp$ de Weierstrass. En effet l'équation de courbe elliptique la plus représentative est déduite de l'équation différentielle vérifiée par $\wp$. Plus exactement si on étudie la cubique de Weierstrass $E(\mathbb{C})$ associée au réseau Λ :

$$Y^2 = 4X^3 - g_2X - g_3$$

où g_2 et g_3 sont respectivement $60G_4$ et $140G_6$, alors, lorsqu'on la prolonge au plan projectif $\mathbb{P}^2(\mathbb{C})$ (prolongement noté $\bar{E}(\mathbb{C})$), on peut exhiber une application bijective holomorphe de $\mathbb{C}/\Lambda$ sur $\bar{E}(\mathbb{C})$.

Théorème 5. *L'application*

$$z \mapsto f(z) = (\wp(z) : \wp'(z) : 1) \ si\ z \in \mathbb{C} \setminus \Lambda,\ (0:1:0)\ sinon$$

est une bijection de $\mathbb{C}/\Lambda$ sur l'ensemble $\bar{E}(\mathbb{C})$ des points de la complétée projective de E dans $\mathbb{P}^2(\mathbb{C})$. De plus, cette fonction est holomorphe.

Démonstration . On appelle Π le parallélogramme fondamental délimité par ω_1 et ω_2 (où ω_1 et ω_2 sont associés à Λ). D'après l'équation différentielle vérifiée par $\wp$, on sait que f applique $\Pi \setminus \{0\}$ dans $E(\mathbb{C})$.

Montrons que f est injective. Supposons que $f(z_1) = f(z_2)$.

Si $\wp'(z_1) \neq 0$, alors on a les deux équations :

$$\wp(z_1) = \wp(z_2), \qquad \wp'(z_1) = \wp'(z_2).$$

D'après le théorème 4, la première équation donne $z_2 \in \{z_1, -z_1\}$, et combinée à la deuxième, on a, si on suppose que $z_2 = -z_1$, $\wp'(z_1) = -\wp'(z_1)$, ce qui implique que $\wp'(z_1) = 0$.

Si on a $\wp'(z_1) = 0$, alors $z_1 \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$.. Or les trois nombres $\wp(\frac{\omega_1}{2})$, $\wp(\frac{\omega_2}{2})$, $\wp(\frac{\omega_1+\omega_2}{2})$ sont différents (encore une application du théorème 4 : $\wp(\frac{\omega_1}{2}) = \wp(\frac{\omega_2}{2}) \Rightarrow \frac{\omega_1}{2} + \frac{\omega_2}{2} \in \Lambda$, ce qui est faux), on a d'après la première équation $z_1 = z_2$.

Montrons que f est surjective de $\Pi \setminus \{0\}$ dans $E(\mathbb{C})$:
Soient $(a, b) \in \mathbb{C}^2$ tels que $b^2 = 4a^3 - g_2 a - g_3$. Alors considérons les deux solutions z et $z' = -z$ de l'équation $\wp(u) = a$ dans $\Pi \setminus \{0\}$. L'équation différentielle donne $\wp'(z)^2 = \wp'(z')^2 = b^2$. Comme $\wp$ est impaire on a $\wp'(z) = -\wp'(z')$, z et z' satisfont $f(u) = (a : b : 1)$.

Montrons que $f(z)$ est holomorphe sur $\mathbb{C}$. Déjà, f est holomorphe sur $\mathbb{C} \setminus \Lambda$, car $\wp(z)$ et $\wp'(z)$ le sont. Si $z_0 \in \Lambda$, on a $f(z_0) = (0 : 1 : 0)$, donc on étudie l'équation

$$Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$$

pour $Y = 1$, ce qui donne alors

$$Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$$

d'où

$$f(z) = (X : 1 : Z) = (\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)}),$$

ce qui prouve que $f4$ est holomorphe en z_0, les deux fonctions apparaissant l'étant au voisinage de z_0. $\diamondsuit$

On peut alors construire une loi de groupe sur la courbe elliptique E par la formule :

$$P \oplus Q := f(f^{-1}(P) + f^{-1}(Q)).$$

qui n'est autre que l'addition sur les complexes transportée par la bijection f.

L'élément neutre est alors le point $(0 : 1 : 0)$ et l'opposé de $(X : Y : Z)$ est $(X : -Y : Z)$. Il reste maintenant à caractériser géométriquement la somme $P \oplus Q$. Cela sera fait dans une partie ultérieure.

1.2 Théorème d'Abel

Le théorème d'Abel est un résultat important qui va nous servir dans la suite de notre exposé. Il s'agit en fait de la réciproque d'un théorème classique d'analyse complexe, le quatrième théorème de Liouville.

Rappelons avant tout la définition d'une fonction elliptique, ainsi que quelques propriétés qui les caractérisent.

Définition 5. Une fonction $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ est dite elliptique si f est méromorphe dans $\mathbb{C}$ et s'il existe un réseau Λ tel que $f(z+\omega) = f(z)$ pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$.

On note Π un parallélogramme fondamental, délimité par $(0, \omega_1, \omega_2, \omega_1 + \omega_2)$ où ω_1 et ω_2 engendrent le réseau Λ.

Le troisième théorème de Liouville donne alors une condition sur le nombre de zéros et de pôles de cette fonction elliptique. Remarquons que, puisqu'une courbe elliptique ne possède qu'un nombre fini de pôles dans un domaine borné de $\mathbb{C}$, on peut choisir $\alpha \in \mathbb{C}$ tel qu'elle n'admette pas de pôles sur la frontière de $\alpha + \Pi$.

Théorème 6 (Liouville). *Soit f une fonction elliptique de réseau Λ qui est dépourvue de zéro et de pôle sur la frontière de $\alpha+\Pi$. Si on pose m_a les ordres des zéros a de f dans $\alpha+\Pi$ et n_b ceux de ses pôles b dans $\alpha+\Pi$, alors on a*

$$\Sigma m_a = \Sigma n_b$$

Ce nombre ne dépend pas de α. On l'appelle l'ordre de f.

Nous pouvons donc désormais énoncer le quatrième théorème de Liouville :

Théorème 7 (Liouville). *Soit f une fonction elliptique de réseau Λ qui est dépourvue de zéro et de pôle sur la frontière de $\alpha + \Pi$. Soit n son ordre. Si $(a_1, ..., a_n)$ sont les zéros de f dans $\alpha + \Pi$ et $(b_1, ..., b_n)$ ses pôles dans $\alpha + \Pi$, répétés avec leur multiplicité, alors on a*

$$a_1 + ... + a_n \equiv b_1 + ... + b_n \ mod\ \Lambda$$

Ces théorèmes sont des applications de la formule de Cauchy, que nous rappelons :

Lemme 2 (Formule de Cauchy). Soient $a \in \mathbb{C}$, $r > 0$, $f : \overline{B(a,r)} \to \mathbb{C}$ continue holomorphe sur $B(a,r)$, $b \in B(a,r)$. Alors on a

$$f(b) = \frac{1}{2\imath\pi} \int_{C(a,r)} \frac{f(z)}{z-b} dz$$

Le théorème qui nous importe est la réciproque du théorème de Liouville, c'est-à-dire :

Théorème 8 (Abel). *Soient $(u_1, ..., u_n)$ et $(v_1, ..., v_n)$ deux familles de nombres complexes et Λ un réseau. Alors il existe f une fonction elliptique de période Λ dont les zéros sont les $u_i + \Lambda$ et les pôles sont les $v_i + \Lambda$ si et seulement si*

$$a_1 + ... + a_n \equiv b_1 + ... + b_n \ mod\ \Lambda$$

Démonstration . Soient ω_1 et ω_2 deux générateurs de Λ. On définit alors $L : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ par

$$L(z) = \frac{1}{z} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{z-\omega} + \frac{1}{w} + \frac{z}{\omega^2}$$

Rappelons que

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{w^2}$$

On constate que $L'(z) = -\wp(z)$. Or on a vu qu $\wp$ était Λ périodique. On en déduit qu'il existe deux nombres η_1 et η_2 tel que

$$\forall z \in \mathbb{C}, L(z+\omega_j) = L(z) + \eta_j$$

pour $j = 1$ et $j = 2$. Posons $\sigma : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ la fonction définie par

$$\sigma(z) = z \prod_{\omega \in \Lambda \setminus \{0\}} (1 - \frac{z}{w}) exp(\frac{z}{w} + \frac{1}{2}(\frac{z}{w})^2)$$

Alors on constate que σ ne s'annule que sur Λ et que sa dérivée logarithmique est L, c'est-à-dire que $\forall z \in \mathbb{C}\setminus\Lambda$, $\frac{\sigma'(z)}{\sigma(z)} = L(z)$. On en déduit que la fonction v_j définie par $v_j(z) = \frac{\sigma(z+\omega_j)}{\sigma(z)}$ vérifie l'équation différentielle $v_j{}'(z) = \eta_j v_j(z)$. On peut de plus remarquer que $v_j(-\frac{\omega_j}{2}) = -1$. On a donc $\forall z \in \mathbb{C}\setminus\Lambda, v_j(z) = -exp(\eta_j(z + \frac{\omega_j}{2}))$. Choisissons des éléments $a_i \in u_i + \Lambda$ et $b_i \in v_i + \Lambda$ tel que $\sum a_i = \sum b_i$. Alors la fonction $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ définie par

$$f(z) = \prod_{i=1}^{n} \frac{\sigma(z-a_i)}{\sigma(z-b_i)}$$

est une fonction méromorphe de période Λ dont les zéros sont les $a_i + \Lambda$ et dont les pôles sont les $b_i + \Lambda$. $\diamondsuit$

Disposant des théorèmes de Liouville, on peut maintenant caractériser géométriquement la loi de groupe sur la courbe elliptique.

Théorème 9. *Une condition nécessaire et suffisante pour que trois points de $\bar{E}(\mathbb{C})$ soient alignés est que $P \oplus Q \oplus R = 0$.*

Démonstration . Supposons que $P,\ Q,\ R$ soient alignés sur la droite d'équation $aX + bY + cZ = 0$. Alors, en posant $u = f^{-1}(P),\ v = f^{-1}(Q)$ et $w = f^{-1}(R)$, par définition de la loi de groupe, $u,\ v,\ w$ sont les racines de la fonction elliptique $g(z) = a\wp(z) + b\wp'(z) + c$.

Si $b \neq 0$, cette fonction admet un pôle unique d'ordre 3 en $0 \in \mathbb{C}/\Lambda$. Le quatrième théorème de Liouville nous donne alors que $u + v + w \equiv 0 \in \mathbb{C}/\Lambda$.

Si $b = 0$ mais $a \neq 0$, la droite s'écrit $aX + cZ = 0$ qui passe par $(0 : 1 : 0) \in \bar{E}(\mathbb{C})$. On peut alors supposer que $R = 0$ de paramètre $w = f^{-1}(R) \equiv 0 \in \mathbb{C}/\Lambda$. Comme g admet un pôle unique d'ordre 2 dans $\mathbb{C}/\Lambda$, on a d'après le quatrième théorème de Liouville $u + v = 0\ mod\ \Lambda$, ce qui donne bien $u + v + w = 0\ mod\ \Lambda$.

Le dernier cas est celui où $a = b = 0$ et $c \neq 0$. Mais la cubique de Weierstrass :

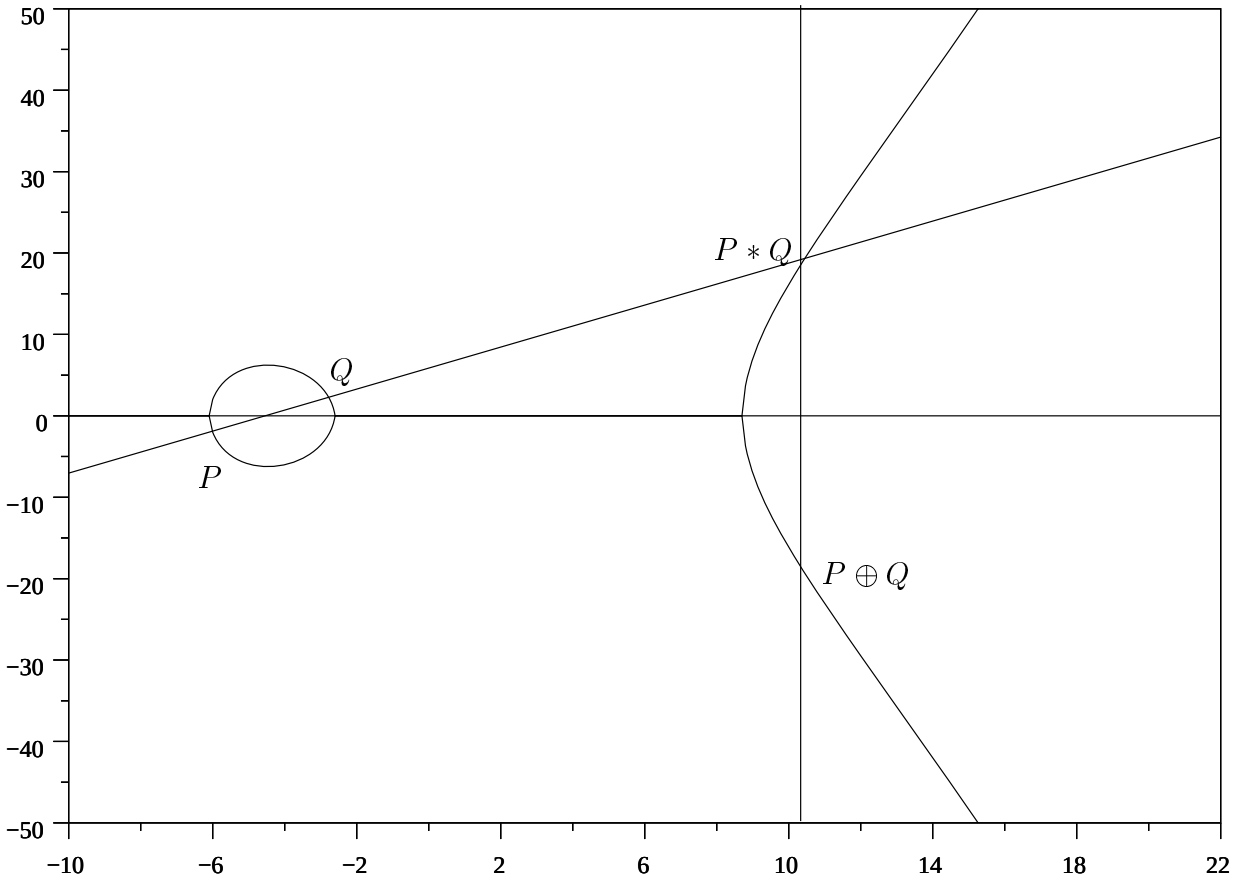
$$Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$$

admet $Z = 0$ comme tangente d'inflexion donc le point $(0 : 1 : 0) = 0$ est point triple de l'intersection de la cubique avec la droite $Z = 0$. D'où une fois de plus le résultat.

Réciproquement, si on suppose $u + v + w = 0$, alors d'après la première partie la droite passant par f(u) et f(v) coupe $\bar{E}(\mathbb{C})$ en un troisième point f(w') tel que :

$$u + v + w' = 0$$

D'où $w = w'$ et le résultat demandé. $\diamondsuit$



Construction de $P \oplus Q$

2 Application au théorème de Poncelet

2.1 Introduction

On considère deux coniques C et D non dégénérées n'ayant aucune intersection double dans le plan projectif $\mathbb{P}^2(\mathbb{C})$. On considère la conique duale $D^* \subset \mathbb{P}^{2*}$, qui représente les tangentes T à D, et la courbe $E \subset C \times D^*$ formée des éléments $P = (X, T)$ où $X \in C$ et $T \in D^*$ avec $X \in T$.

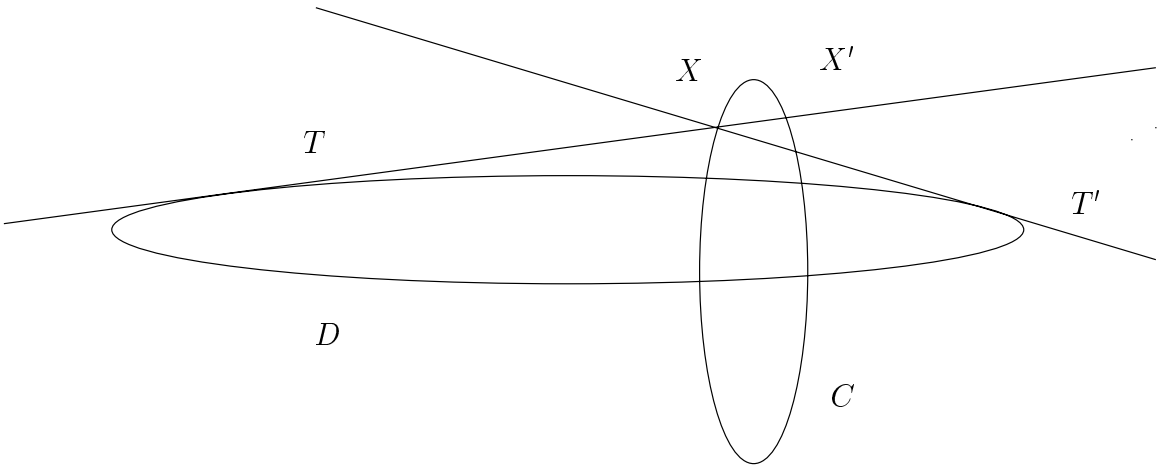
On définit sur E deux tranformations i et i' par :

$$i(X, T) = (X', T)$$

$$i'(X, T) = (X, T')$$

où X' est la deuxième intersection de T avec C et T' est la deuxième tangente à D passant par X, avec $X' = X$ lorsque T est tangente à C et $T' = T$ lorsque X appartient à D. On remarque que la construction de Poncelet consiste en une itération de l'application $j = i' \circ i$. Le théorème de Poncelet s'écrit alors : S'il existe un entier n tel que $j^n(P) = P$ pour un certain $P \in E$, alors $j^n(P) = P$ pour tout P de E.

Remarque . Il peut sembler sur le dessin que la construction de Poncelet ne soit pas toujours définie. Cela vient du fait que notre dessin est dans $\mathbb{R}^2$. En effet, si on prend un point de C qui se trouve à l'intérieur de D, les tangentes à D passant par ce point sont en fait complexes. Cette remarque pourra être affinée dans le calcul des tangentes effectuées dans la section suivante.



Les applications i et i'

2.2 Rapport avec les courbes elliptiques

Il s'agit pour nous d'utiliser les propriétés des courbes elliptiques pour résoudre ce problème géométrique. Pour cela, nous allons montrer que E est une courbe elliptique.

Théorème 10. *E est une courbe elliptique.*

Remarquons que, dans une bonne base, on peut supposer que l'équation projective de la conique D est de la forme $x^2 + y^2 + z^2 = 0$. Nous la supposerons désormais de cette

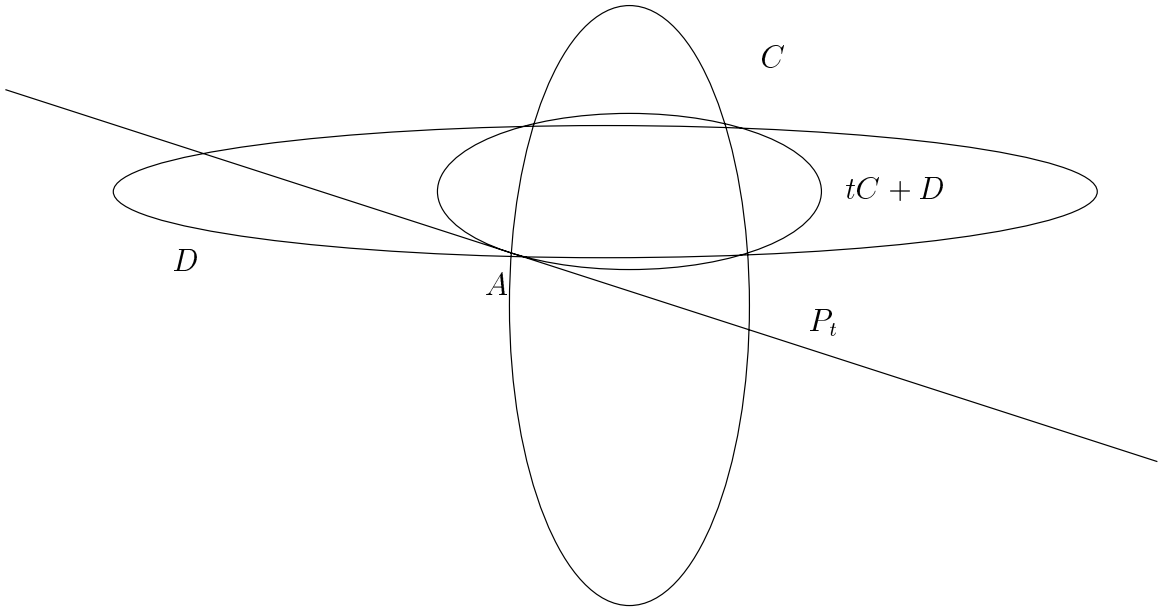
forme. Considérons alors un point $(x_0 : y_0 : z_0)$ de $\mathbb{P}^2$. Alors les coordonnées projectives des tangentes à la conique D passant par le point $(x_0 : y_0 : z_0)$ sont

$$\begin{cases} (-x_0z_0 - iy_0\sqrt{x_0^2+y_0^2+z_0^2} : -y_0z_0 + ix_0\sqrt{x_0^2+y_0^2+z_0^2} : x_0^2+y_0^2) \\ (-x_0z_0 + iy_0\sqrt{x_0^2+y_0^2+z_0^2} : -y_0z_0 - ix_0\sqrt{x_0^2+y_0^2+z_0^2} : x_0^2+y_0^2) \end{cases}$$

Nous pouvons remarquer que, comme attendu, si $(x_0 : y_0 : z_0)$ n'est pas un point de D, alors il y a deux tangentes qui passent par ce point. Nous avons ainsi une paramétrisation de nos tangentes par nos points. De plus, nous savons qu'une conique est paramétrable par $\mathbb{P}^1(\mathbb{C})$. Soit $\underline{C}$ un paramétrage. On a

$$\begin{aligned} &\underline{C} : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C}) \\ &\underline{C}(t) = (x(t) : y(t) : z(t)) \end{aligned}$$

Alors on s'aperçoit que, si on pose $\tau^2 = x(t)^2 + y(t)^2 + z(t)^2$, alors E est entièrement déterminé par le couple (t, τ). Il s'agit donc pour nous de trouver un bon paramétrage de E.



Paramétrage de C

Nous écrirons l'équation projective de C sous la forme $ax^2 + by^2 + cz^2 + 2dxy + 2eyz + 2fzx = 0$, et nous supposerons que le point $A = (\alpha : \beta : \gamma)$ est l'un des points d'intersection de C et de D (Rappelons qu'il s'agit d'un point d'intersection simple par hypothèse). Nous allons paramétrer C par le faisceau de coniques $tC + D$, c'est-à-dire que, pour tout $t \in \mathbb{P}^1(\mathbb{C})$, nous allons construire la tangente à $tC + D$ qui passe par le point A et nous lui associerons le point d'intersection avec C distinct de A (et A si cette droite est tangente à C, ce qui n'arrive que dans le cas $t = \infty$). Posons

$$\begin{aligned} X(t) &= t(\alpha a + \beta d + \gamma f) + \alpha \\ Y(t) &= t(\alpha d + \beta b + \gamma e) + \beta \\ Z(t) &= t(\alpha f + \beta e + \gamma c) + \gamma. \end{aligned}$$

Alors l'équation de la tangente à $tC+D$ passant par $(\alpha:\beta:\gamma)$ est $X(t)x+Y(t)y+Z(t)z=0$. On obtient alors le paramétrage suivant (en coordonnées projectives) :

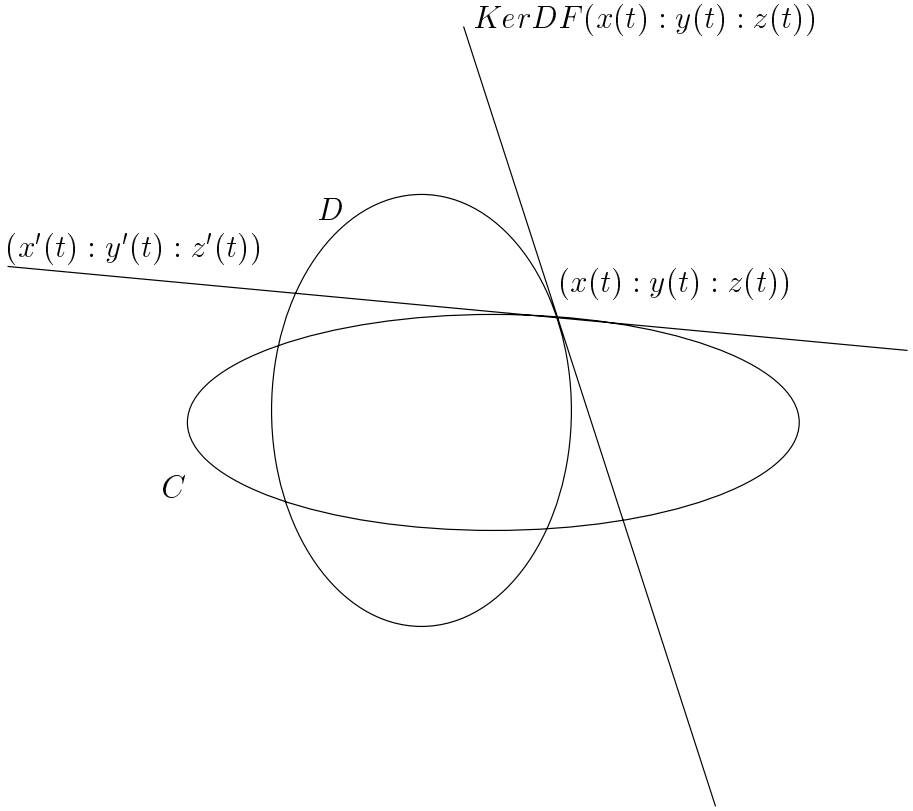
$$\begin{aligned}
x(t) &= Z(t)(-\alpha cX(t)^2 + 2\alpha X(t)Z(t) + 2fY(t)Z(t) + 2eX(t)Z(t) \\
&\qquad -2cX(t)Y(t) - (2d + a\alpha)Z(t)^2) \\
y(t) &= Z(t)(cX(t)^2 - 2fX(t)Z(t) + aZ(t)^2) \\
z(t) &= \alpha cX(t)^3 + cX(t)^2Y(t) - 2(e + f\alpha)X(t)^2Z(t) + (2d + \alpha a)X(t)Z(t)^2 + aZ(t)^2Y(t)
\end{aligned}$$

On en déduit qu'en posant

$$\tau^2 = x(t)^2 + y(t)^2 + z(t)^2$$

nous obtenons un paramétrage (t,τ) de E qui fait de E une courbe elliptique d'origine A de façon claire, puisque l'on a $\tau^2 = det(t\tilde{C} + \tilde{D})$ où $\tilde{C}$ et $\tilde{D}$ sont les matrices représentant les formes quadratiques définies par C et D.

Remarque . En fait, pour vérifier que $det(t\tilde{C} + \tilde{D}) = x(t)^2 + y(t)^2 + z(t)^2$, on s'aperçoit que ces polynômes ont les mêmes racines, que $det(t\tilde{C} + \tilde{D})$ est scindé à racines simples. De plus on peut se convaincre que $P(t) = x(t)^2 + y(t)^2 + z(t)^2$ est à racines simples. En effet en considérant la courbe $P(t) = 0$, si on avait une racine double, on aurait $P'(t) = 0 = DF(x(t), y(t), z(t)) \circ (x'(t), y'(t), z'(t))$ $(avec\ F(x,y,z) = x^2 + y^2 + z^2)$. Comme le noyau de $DF(x,y,z)$ est en fait la droite tangente à D en $(x,y,z) \in D$ *car* $x^2 + y^2 + z^2 = 0$ et le vecteur $(x'(t), y'(t), z'(t))$ le vecteur tangent à C en $(x(t), y(t), z(t))(\in C$ par définition du paramétrage), $P'(t) = 0$ implique alors que C et D ont une tangente commune, ce qui est faux.



Une preuve que $\tau^2(t)$ est à racines simples

Remarque . Par analogie avec les cercles, l'interprétation de τ est simple : il s'agit de la puissance du point $(x(t) : y(t) : z(t))$ par rapport à la conique D.

2.3 Une démonstration du théorème de Poncelet

Nous avons désormais tous les éléments pour démontrer le théorème de Poncelet. Puisque E est une courbe elliptique, E s'identifie à $\mathbb{C}/\Lambda$ où Λ est un certain réseau de $\mathbb{C}$ (cf Partie Théorique).

On considère la projection $p : E \to \mathbb{P}^1(\mathbb{C})$ définie par $p(X,T) = X$. Etant donné notre paramétrage, il est clair qu'il s'agit d'une fonction méromorphe Λ périodique. Le troisième théorème de Liouville affirme alors que la fonction i' est de la forme $i'(z) \equiv a - z \ mod \ \Lambda$ si on regarde son action sur $\mathbb{C}/\Lambda$. En effet, si α et β sont deux points de E, alors la fonction f définie par $f = \frac{p-p(\alpha)}{p-p(\beta)}$ a ses zéros en α et en $i'(\alpha)$, et ses pôles en β et en $i'(\beta)$. On a donc

$$\alpha + i'(\alpha) \equiv \beta + i'(\beta) \ mod \ \Lambda$$

On obtiendrait par ce même procédé la même égalité pour i en considérant la fonction $p'(X,T) = T$ définie sur E. Ainsi, en posant $i_0 = i(A)$ et en remarquant que $i'_0 = i'(A)$ est nul, on a

$$\begin{cases} i(z) \equiv i_0 - z \ mod \ \Lambda \\ i'(z) = -z \ mod \ \Lambda \end{cases}$$

Ainsi notre application j définie précédemment comme la composée des fonctions i et i' s'écrit $j(z) = z - i_0 \ mod \ \Lambda$. Il s'agit donc en fait juste d'une translation. Il est donc évident que si j^n admet un point fixe pour un certain n, c'est-à-dire si $ni_0 \equiv 0 \ mod \ \Lambda$, alors la transformation j^n induit l'identité sur la courbe E. On a donc démontré le théorème de Poncelet. $\diamondsuit$

3 Quelques précisions ...

Nous pouvons en effet avoir un résultat plus précis. Nous allons montrer le théorème suivant :

Théorème 11 (Cayley). *Soient deux coniques non dégénérées C et D représentées par les matrices $\tilde{C}$ et $\tilde{D}$, telles qu'elles ne possèdent pas de point d'intersection double. Écrivons*

$$\sqrt{det(t\tilde{C} + \tilde{D})} = A_0 + A_1 t + A_2 t^2 + ...$$

Alors la construction de Poncelet forme un n-gone si, et seulement si,

$$\begin{vmatrix} A_2 & \cdots & A_{m+1} \\ . & & . \\ . & & . \\ . & & . \\ A_{m+1} & \cdots & A_{2m} \end{vmatrix} = 0 \ si \ n = 2m+1$$

$$\begin{vmatrix} A_3 & \cdots & A_{m+1} \\ . & & . \\ . & & . \\ . & & . \\ A_{m+1} & \cdots & A_{2m-1} \end{vmatrix} = 0 \ si \ n = 2m$$

Remarque . Le coefficient A_0 est non nul puisqu'il vaut $det(\tilde{D})$ et que D est une conique non dégénérée.

Démonstration . Ce théorème découle d'un théorème plus général :

Lemme 3 (Cayley). Soient E une courbe elliptique d'origine o d'équation

$$y^2 = (x-a)(x-b)(x-c)$$

où $a,\ b,\ c$ sont des nombres distincts non nuls. Soit $p \in E$ tel que $x(p) = 0$. Si on écrit

$$y = \sqrt{(x-a)(x-b)(x-c)} = \sum_{k=0}^{\infty} A_k x^k$$

alors p est d'ordre n dans le groupe $\overline{E}(\mathbb{C})$ si et seulement si

$$\begin{vmatrix} A_2 & \cdots & A_{m+1} \\ . & & . \\ . & & . \\ . & & . \\ A_{m+1} & \cdots & A_{2m} \end{vmatrix} = 0 \ si \ n = 2m+1$$

$$\begin{vmatrix} A_3 & \cdots & A_{m+1} \\ . & & . \\ . & & . \\ . & & . \\ A_{m+1} & \cdots & A_{2m-1} \end{vmatrix} = 0 \ si \ n = 2m$$

En fait, ce théorème est une conséquence du théorème de Niels Abel (cf précédemment). Il s'agit pour nous d'exprimer sous quelle condition un point p de $\mathbb{C}/\Lambda$ vérifie $np \equiv 0 \ mod \ \Lambda$. Appelons $H^0(\vartheta_E[n.o])$ l'espace vectoriel des fonctions elliptiques sur E dont le seul pôle est 0 et dont l'ordre est inférieur ou égal à n. Il s'agit d'un espace vectoriel de dimension n.

Appelons $(f_1, ..., f_n)$ une base de $H^0(\vartheta_E[n.o])$. Alors

$$np \equiv 0 \ mod\Lambda \Leftrightarrow \exists f \in H^0(\vartheta_E[n0]),\ f(p) = f'(p) = ... = f^{(n-1)}(p) = 0$$

$$\Leftrightarrow \exists (a_1, ..., a_n) \in \mathbb{C}\backslash\{(0, ..., 0)\}, \forall j \in \{0, ..., n-1\}, \sum_{i=1}^{n} a_i f_i^{(j)}(p) = 0$$

$$\Leftrightarrow W(p) = \begin{vmatrix} f_1(p) & \cdots & f_n(p) \\ f_1'(p) & \cdots & f_n'(p) \\ . & & . \\ . & & . \\ . & & . \\ f_1^{(n-1)}(p) & \cdots & f_n^{(n-1)}(p) \end{vmatrix} = 0$$

On veut chercher si $W(p) = 0$. Pour cela, on remarque qu'il suffit de considérer la dérivée des fonctions de la base par rapport à x. En effet, il suffit de montrer que l'on peut utiliser le théorème d'inversion locale en p c'est-à-dire que $\frac{dx}{du}(u) = f'(u) \neq 0$. Ceci est vrai car on a pris $a, b, c \neq 0$ donc $f'(u) = y(u) \neq 0$ $(f'(u)^2 = -abc)$.

On va donc exprimer $W(x = 0)$ dans la base $1, x, x^2, ..., x^m, y, xy, x^2y, ..., x^{m-1}y$ si $n = 2m + 1$ et $x, x^2, ..., x^m, y, yx, ..., x^{m-2}y$ si $n = 2m$.

On écrit y sous la forme d'un développement en x, c'est-à-dire $y = A_0 + A_1x + A_2x^2 + ...$ Il faut donc évaluer les dérivées l-ième des fonctions de notre base par rapport à x en 0. Alors on a

$$\frac{d^l(x^\alpha y)}{dx^l} = l!A_{l-\alpha}$$

Cette remarque fait apparaître une matrice de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où la matrice A est une matrice diagonale dont les éléments sont de la forme $i!$ et on a, pour n = 2m+1

$$C = \begin{pmatrix} (m+1)!A_{m+1} & (m+1)!A_m & \cdots & (m+1)!A_2 \\ (m+2)!A_{m+2} & (m+2)!A_{m+1} & \cdots & (m+2)!A_3 \\ . & & & . \\ . & & & . \\ . & & & . \\ (2m)!A_{2m} & (2m)!A_{2m-1} & \cdots & (2m)!A_{m+1} \end{pmatrix}$$

Finalement,

$$\begin{aligned} W(p) = 0 &\Leftrightarrow det(C) = 0 \\ &\Leftrightarrow \begin{vmatrix} A_2 & \cdots & A_{m+1} \\ . & & . \\ . & & . \\ . & & . \\ A_{m+1} & \cdots & A_{2m} \end{vmatrix} = 0 \end{aligned}$$

On tombe ainsi sur le déterminant cherché. On a démontré le résultat pour $n = 2m + 1$. Le calcul est similaire pour $n = 2m$.

Enfin, il suffit d'appliquer le résultat à l'application $E \to \mathbb{P}^1(\mathbb{C})$ qui à tout point u de E associe t, qui est une application d'ordre 2 en o et qui s'annule en p, et à l'application $E \to \mathbb{P}^1(\mathbb{C})$, qui à tout point u de E associe τ, qui est d'ordre 3 en o. On obtient ainsi le résultat énoncé. $\diamondsuit$

Références

[1] **H. Lebesgue,** *Les coniques*, Gauthier-Villars, 1942

[2] **P. Griffith,J.Harris,** *L'enseignement mathématique 24*, 1978, pages 31-40

[3] **Y. Hellegouarch,** *Invitation aux mathématiques de Fermat-Wiles*, Masson, 1997

[4] **H.J.M. Bos, C. Kers, F. Oort, D.W. Raven,** *Poncelet's closure theorem*, Expositiones Mathematicae, 1987, pages 289-364

[5] **Mac Kean,** *Elliptic curves : function theory, geometry, arithmetic*, Cambridge University Press, 1997

[6] **D. Hüsemoller,** *Elliptic curves*, Springer, 1987