Factorisation des polynômes de Poncelet *

Dominique Hulin

1 Introduction

Soient C et D deux coniques (réelles ou) complexes, non dégénérées. Le théorème de Poncelet affirme que si, partant d'un point $m \in C$, on peut construire un polygône à n côtés inscrit dans C et circonscrit à D, tout autre point de C sera sommet d'un tel n-gone ([14]). Introduisons la courbe de Poncelet associée, soit

$$F = \{(m, \xi) \in C \times D^* \mid \xi(m) = 0\}$$

(une tangente à D, soit $\xi \in D^*$ où D^* est la conique duale de D, contenant un point $m \in C$), et la transformation de Poncelet $\phi : F \to F$ définie par $\phi(m_1, \xi_1) = (m_2, \xi_2)$, où m_2 est le deuxième point d'intersection de ξ_1 avec C et ξ_2 la deuxième tangente à D issue de m_2. Le théorème de Poncelet se réénonce comme suit : si l'application $\phi^n : F \to F$ possède un point fixe, alors $\phi^n = \mathrm{Id}$.

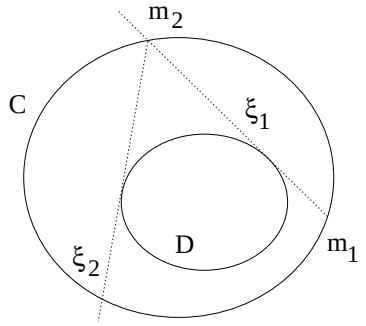

FIGURE 1 – La transformation de Poncelet $\phi : (m_1, \xi_1) \mapsto (m_2, \xi_2)$

De nombreux auteurs se sont intéressés à ce résultat, que ce soit pour en revisiter la preuve, ou bien pour en proposer des généralisations ; parmi eux, je citerai simplement Jacobi, Cayley [5], Lebesgue [11], Griffiths-Harris [10], Bos-Kers-Oort-Raven [3], et enfin Jakob [12] et Barth-Michel [1].

*Geometriae Dedicata vol. 130 (2007) pp. 109-136

Dans cet article, nous nous limiterons au cas où les coniques ont pour équations respectives

$$C = \{(x,y) \in \mathbb{C}^2 \mid x^2 + y^2 = R^2\} \quad \text{et} \quad D = \{(x,y) \in \mathbb{C}^2 \mid (x+a)^2 + y^2 = r^2\} \ :$$

lorsque les paramètres sont réels, ces coniques sont alors des cercles (c'est la configuration intialement considérée par Poncelet).

Observons que lorsque les coniques C et D sont transverses (ce que nous supposerons désormais), ou de façon équivalente lorsqu'elles se coupent en quatre points distincts de $\mathrm{P}^2\mathbb{C}$, on se ramène facilement à ce cas particulier ; il suffit en effet de choisir deux points parmi les quatre points d'intersection de C et D, et de se placer dans une carte affine relativement à laquelle ces deux points se lisent comme les points cycliques $[1, \pm i, 0]$.

Pour chaque entier $n \geq 2$, la condition sous laquelle la transformation de Poncelet vérifie $\phi^n = \mathrm{Id}$ est alors polynomiale en les paramètres (a, R, r) définissant les coniques C et D. Dans cet article, nous poursuivons deux objectifs :

- Tout d'abord obtenir des formules de récurrence simples à manipuler pour déterminer ces polynômes (§2.1).
- Ensuite, décomposer les polynômes ainsi obtenus en produits de facteurs irréductibles que l'on interprétera géométriquement (§2.2).

Rappelons que Cayley ([5, 10]) propose une méthode élégante pour déterminer les conditions (portant sur des coniques générales C et D) sous lesquelles $\phi^n = \mathrm{Id}$, mais que celle-ci est, en pratique, difficilement exploitable pour n grand.

2 Principaux résultats

2.1 Relations de récurrence pour les conditions de Poncelet

Reprenons nos deux coniques C et D, et introduisons l'involution $\sigma : F \to F$ induite sur la courbe de Poncelet par la symétrie par rapport à l'axe défini par leurs centres. En nous intéressant simultanément aux conditions sous lesquelles la transformation de Poncelet vérifie respectivement $\phi^n = \mathrm{Id}$, ou bien $\phi^n = \sigma$, nous constaterons que celles-ci sont reliées par des relations de récurrence particulièrement simples (théorèmes 2.1 et 2.2 ; ceci sera développé dans la section 3, et les paragraphes §4.1 et §4.2).

Dans le premier énoncé, nous introduisons les polynômes qui interviendront dans les conditions de Poncelet, et les relations de récurrence qui les lient.

Théorème 2.1 • *Il existe deux suites de polynômes en trois variables, soient $p_n(x,y,z)$ et $q_n(x,y,z)$ ($n \in \mathbb{N}$), définies de façon unique par leurs premiers termes :*

$$p_0 = 0\,,\ q_0 = 1\,,\ p_1 = x\,,\ q_1 = y\,,\ p_2 = xyz^2\,,$$

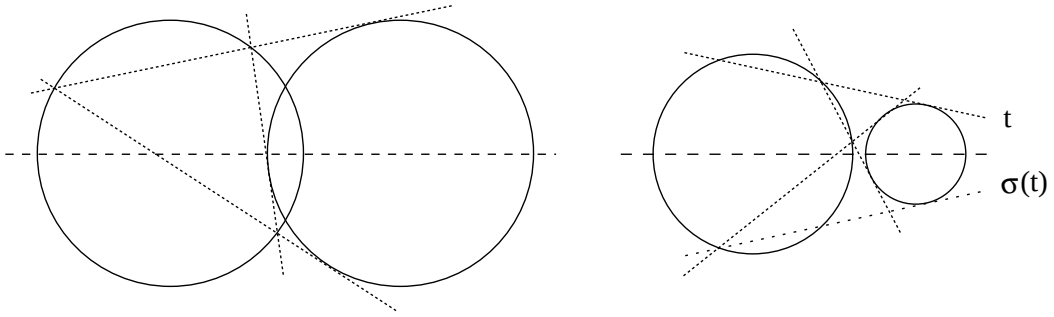

FIGURE 2 – Une configuration avec $\phi^3 = \mathrm{Id}$; une autre avec $\phi^3 = \sigma$.

et, pour $m \geq n$, les relations :

$$p_{m+n}p_{m-n} = p_m^2 q_n^2 - p_n^2 q_m^2 \quad (1)$$
$$q_{m+n}q_{m-n} = q_m^2 q_n^2 - p_m^2 p_n^2 \,. \quad (2)$$

• Quelques propriétés : *les polynômes p_n et q_n sont homogènes de degré n^2 en (x, y, z), avec*

$$\textit{pour } n \textit{ impair} \quad : \quad p_n \in x\,\mathbb{Z}[x^4, y^4, z^4] \textit{ et } q_n \in y\,\mathbb{Z}[x^4, y^4, z^4], \quad (3)$$
$$\textit{pour } n \textit{ pair} \quad : \quad p_n \in xyz^2\,\mathbb{Z}[x^4, y^4, z^4] \textit{ et } q_n \in \mathbb{Z}[x^4, y^4, z^4]\,; \quad (4)$$

de plus le produit $p_\ell\, q_\ell$ divise $p_{2\ell}$ dans $\mathbb{Z}[x, y, z]$ ($\ell \in \mathbb{N}^*$), et le calcul récursif de ces polynômes est facilité par les relations suivantes : pour $k, \ell \in \mathbb{N}^*$,

$$p_{k\ell} = p_k\Big(p_\ell, q_\ell, \sqrt{\frac{p_{2\ell}}{p_\ell q_\ell}}\Big) \quad \text{et} \quad q_{k\ell} = q_k\Big(p_\ell, q_\ell, \sqrt{\frac{p_{2\ell}}{p_\ell q_\ell}}\Big)\,. \quad (5)$$

Le théorème suivant affirme que les polynômes p_n et q_n fournissent effectivement les conditions sous lesquelles la transformation de Poncelet vérifie respectivement $\phi^n = \mathrm{Id}$, ou bien $\phi^n = \sigma$.

Théorème 2.2 *Soient deux coniques d'équations $C = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = R^2\}$ et $D = \{(x, y) \in \mathbb{C}^2 \mid (x+a)^2 + y^2 = r^2\}$ (supposés transverses), $\phi : F \to F$ la transformation de Poncelet correspondante, et $\sigma : F \to F$ l'application associée à la symétrie d'axe Ox. Alors, pour tout choix des racines carrées $\sqrt{a}$, $\sqrt{R}$ et $\sqrt{2r}$:*

$$\phi^n = \mathrm{Id} \quad \textit{si et seulement si} \quad p_n(\sqrt{a}, \sqrt{R}, \sqrt{2r}) = 0$$
$$\textit{et} \quad \phi^n = \sigma \quad \textit{si et seulement si} \quad q_n(\sqrt{a}, \sqrt{R}, \sqrt{2r}) = 0.$$

Signalons que Halphen propose des relations de récurrence ne faisant intervenir que les polynômes (p_n) (voir [9], [2], et la remarque à la fin du §4.1).

2.2 Les polynômes de Poncelet ; factorisation

A d'éventuels facteurs non significatifs $\sqrt{a}$ et $\sqrt{R}$ près, les expressions $p_n(\sqrt{a},\sqrt{R},\sqrt{2r})$ et $q_n(\sqrt{a},\sqrt{R},\sqrt{2r})$ que nous venons d'obtenir sont polynomiales, et à coefficients entiers, en (a,R,r) (voir (3) et (4) ci-dessus). Nous voulons maintenant décomposer ces polynômes en produit de facteurs irréductibles dans $\mathbb{C}[a,R,r]$ (corollaire 2.5 et théorème 2.6), et interpréter géométriquement les facteurs qui apparaissent. Ceci constitue le résultat principal de cet article.

Une première décomposition apparaît naturellement. Soit en effet $n \geq 2$. Dire que $p_n(\sqrt{a},\sqrt{R},\sqrt{2r})$ s'annule, c'est dire que $\phi^n = \mathrm{Id}$, et donc que la transformation ϕ est d'ordre fini égal à d pour un entier d divisant n, ce qui fournira autant de facteurs pour $p_n(\sqrt{a},\sqrt{R},\sqrt{2r})$. On peut aller plus loin. En effet si ϕ est d'ordre pair $d = 2k$, il se peut que $\phi^k = \sigma$; les facteurs qu'on vient d'évoquer ne seront donc pas tous irréductibles.

Cette discussion nous amène à introduire les définitions suivantes. On notera que les notions de période et de semi-période ci-dessous sont relatives à la transformation σ (voir également la définition 5.1).

Définition 2.3 *On dira que la configuration de Poncelet associée aux coniques C et D est* σ-semi-périodique *s'il existe un entier $n \in \mathbb{N}^*$ pour lequel la transformation de Poncelet satisfait $\phi^n = \sigma$. La σ-semi-période de ϕ est alors le plus petit entier n pour lequel $\phi^n = \sigma$.*

On dira que la configuration est σ-strictement périodique *si elle n'est pas σ-semi-périodique, et s'il existe un entier $n \in \mathbb{N}^*$ pour lequel $\phi^n = \mathrm{Id}$. La période σ-stricte de ϕ est alors le plus petit entier n pour lequel $\phi^n = \mathrm{Id}$.*

Ces considérations suggèrent le résultat suivant qui sera démontré, avec son corollaire, dans le paragraphe §4.3.

Proposition 2.4 *Il existe deux suites de polynômes homogènes $\varphi_n(x,y,z)$ et $\psi_n(x,y,z)$ ($n \in \mathbb{N}^*$), premiers entre eux deux à deux, avec $\varphi_1 = x$, $\psi_1 = y$, $\varphi_2 = z^2$ et $\varphi_n, \psi_n \in \mathbb{Z}[x^4,y^4,z^4]$ sinon, et tels que pour $n \geq 1$ on ait les factorisations :*

$$p_n = \Big(\prod_{d|n} \varphi_d\Big)\Big(\prod_{\substack{d|n \\ \frac{n}{d}\text{ pair}}} \psi_d\Big) \tag{6}$$

$$\text{et} \quad q_n = \prod_{\substack{d|n \\ \frac{n}{d}\text{ impair}}} \psi_d\,. \tag{7}$$

Définition–Corollaire 2.5 *On introduit les polynômes de Poncelet $\Phi_n(a,R,r) \in \mathbb{Z}[a,R,r]$, et leurs analogues $\Psi_n(a,R,r) \in \mathbb{Z}[a,R,r]$, définis respectivement pour $n \geq 2$ par*

$$\Phi_n(a,R,r) := \varphi_n(\sqrt{a},\sqrt{R},\sqrt{2r}) \text{ et } \quad \Psi_n(a,R,r) := \psi_n(\sqrt{a},\sqrt{R},\sqrt{2r})\,.$$

Une configuration de Poncelet de paramètre $[a,R,r] \in \mathrm{P}^2\mathbb{C}$ *(avec* $a,r,R \in \mathbb{C}^*$*, et* $a \pm r \pm R \neq 0$*) sera :*
– *σ-strictement périodique de période σ-stricte n si et seulement si* $\Phi_n(a,R,r)=0$*,*
– *σ-semi-périodique de σ-semi-période n si et seulement si* $\Psi_n(a,R,r)=0$*.*

Notons que Cayley a abordé la question de la décomposition des $p_n(\sqrt{a},\sqrt{R},\sqrt{2r})$, et a remarqué l'existence des facteurs φ_n et ψ_n ci-dessus (voir [4], ou la fin de la p.306 de [5]).

Les facteurs $\Phi_n(a,R,r)$ et $\Psi_n(a,R,r)$ que nous venons d'obtenir ne seront pas tous irréductibles : intéressons-nous par exemple au polynôme Ψ_n. La courbe de Poncelet $(F;\sigma)$ est une courbe elliptique munie d'une translation d'ordre 2. Soit alors $F^* \to F$ le revêtement de degré 2 de F pour lequel les relèvements $\tilde{\sigma}$ et $\tilde{\sigma}' : F^* \to F^*$ de $\sigma : F \to F$ sont encore (des translations) d'ordre 2. Soit $\tilde{\phi} : F^* \to F^*$ un relèvement de $\phi : F \to F$. La condition « $\phi^n = \sigma$ » se scinde alors en les deux conditions « $\tilde{\phi}^n = \tilde{\sigma}$, ou bien $\tilde{\phi}^n = \tilde{\sigma}'$ » : il y aura donc deux façons pour ϕ d'être σ-semi-périodique, de σ-semi-période n, qui correspondront aux deux facteurs $\Phi_{n,1}$ et $\Phi_{n,3}$ ci-dessous dans la décomposition du polynôme $\Psi_n(a,R,r)$ (section 5).

Le théorème suivant décrit la factorisation des polynômes de Poncelet Φ_n et Ψ_n en produits de facteurs irréductibles.

Théorème 2.6 *Il existe des polynômes* $\Phi_{m,1}, \Phi_{m,2}, \Phi_{m,3}$ *et* $\Phi_{2n+1,0}$ *appartenant à* $\mathbb{Z}[a,R,r]$ *($m \geq 2$, $n \geq 1$), qui sont irréductibles dans* $\mathbb{C}[a,R,r]$*, et tels que :*

$$\begin{aligned} \textit{pour } n \textit{ impair :} \qquad & \Phi_n(a,R,r) = \Phi_{n,0}(a,R,r)\ \Phi_{n,2}(a,R,r) \\ \textit{pour } n \textit{ pair :} \qquad & \Phi_n(a,R,r) = \Phi_{n,2}(a,R,r) \\ \\ \textit{pour } n \textit{ quelconque :} \qquad & \Psi_n(a,R,r) = \Phi_{n,1}(a,R,r)\ \Phi_{n,3}(a,R,r)\,. \end{aligned}$$

Nous venons d'indiquer la signification géométrique des facteurs φ_n et ψ_n (resp. $\Phi_{n,k}$) qui interviennent dans la proposition 2.4 et le théorème 2.6 (il en résulte que les polynômes $\Phi_{n,k}$ sont deux à deux distincts). Il faudra montrer que ces facteurs sont effectivement polynomiaux en (a,R,r), et à coefficients entiers. Ce sera l'objet du §4.3 et de la section 5.

Pour démontrer l'irréductibilité des polynômes $\Phi_{n,k}$, nous nous intéresserons alors aux composantes irréductibles de l'ensemble des configurations de Poncelet de période donnée (section 6). Le point clé sera l'identification de l'ensemble des configurations de Poncelet, éventuellement dégénérées lorsque $r=0$, soit

$$\mathbf{U} = \{[a,R,r] \in \mathrm{P}^2\mathbb{C} \mid a,R \in \mathbb{C}^*\,,\ r \in \mathbb{C}\,,\ a \pm R \pm r \neq 0\}\,,$$

avec l'espace des modules des courbes elliptiques munies d'une structure de niveau 2 et d'une paire de points opposés (voir le §6.1).

Table des matières

3 Points de torsion sur une courbe elliptique

La démonstration « moderne » du théorème de Poncelet consiste à remarquer que la courbe de Poncelet F est une courbe elliptique, et que la transformation de Poncelet $\phi : F \to F$ est une translation sur cette courbe elliptique (voir par exemple [10]). L'application $\sigma : F \to F$ est également une translation, qui est d'ordre 2, sur F. On veut déterminer à quelle condition sur les paramètres (a, R, r) on aura $\phi^n = \mathrm{Id}$, ou bien $\phi^n = \sigma$ (proposition 3.3).

3.1 Courbes elliptiques avec un point d'ordre 2

On se donne une courbe elliptique avec un point d'ordre 2, soit $(E\,;\frac{\omega_1}{2})$, c'est-à-dire un quotient $E = \mathbb{C}/\Lambda$ où $\Lambda = \mathbb{Z}\cdot\omega_1 \oplus \mathbb{Z}\cdot\omega_2 \subset \mathbb{C}$ est un réseau, et sur laquelle on a privilégié le point de 2-torsion $(\frac{\omega_1}{2} + \Lambda) \in E$. On introduit la fonction de Weierstrass $\wp : \mathbb{C} \to \mathrm{P}^1\mathbb{C}$ associée au réseau Λ (voir [13]). On fixe $n \in \mathbb{N}^*$.

Le but de ce paragraphe est de montrer les relations (13) et (14), analogues aux relations (1) et (2), et qui relient les valeurs prises par $\wp$ sur les ensembles $E_0[n] = \{u \in E \mid u \not\equiv 0\,,\ nu \equiv 0\ [\Lambda]\}$ et $E_1[n] = \{v \in E \mid nv \equiv \frac{\omega_1}{2}\ [\Lambda]\}$.

Notons $\omega_3 = \omega_1 + \omega_2$. Rappelons que la fonction de Weierstrass est paire, de degré 2 sur E, ramifiée en l'origine et en chacun des points $\frac{\omega_i}{2}$ ($i \in \{1,2,3\}$), et satisfait l'équation fonctionnelle :

$$\wp'(z)^2 = 4\prod_{i=1}^{3}(\wp(z) - e_i) \quad \text{avec } e_1 + e_2 + e_3 = 0, \tag{8}$$

où $e_i = \wp(\frac{\omega_i}{2})$ désignent les valeurs distinctes prises par $\wp$ aux trois points d'ordre 2 de E.

Lemme 3.1 *Pour $n \in \mathbb{N}^*$, on a* $\wp(nz) - e_1 = \dfrac{1}{n^2}\,\dfrac{\prod_{v\in E_1[n]}(\wp(z)-\wp(v))}{\prod_{u\in E_0[n]}(\wp(z)-\wp(u))}$.

Démonstration Notons $E[n] = \{u \in E \mid nu \equiv 0\ [\Lambda]\}$. Les expressions qui apparaissent de part et d'autre de l'identité à démontrer définissent des fonctions elliptiques sur E, qui ont même diviseur $(-2)\cdot(E[n]) + 2\cdot(E_1[n])$, et même terme dominant $\frac{1}{n^2 z^2}$ dans leur développement asymptotique en l'origine. □

On introduit, pour $n \in \mathbb{N}^*$, les polynômes $P_n, Q_n \in \mathbb{C}[X]$ (qui dépendent de la courbe $(E; \frac{\omega_1}{2})$ considérée), de coefficients dominants positifs et pour lesquels, pour tout $z \in \mathbb{C}$:

– lorsque n est impair :

$$P_n^2(\wp(z)) = n^2 \prod_{u\in E_0[n]} (\wp(z) - \wp(u)) \tag{9}$$

$$(\wp(z) - e_1)\, Q_n^2(\wp(z)) = \prod_{v\in E_1[n]} (\wp(z) - \wp(v))\,; \tag{10}$$

– lorsque n est pair :

$$\frac{1}{4}\wp'(z)^2\, P_n^2(\wp(z)) = n^2 \prod_{u\in E_0[n]} (\wp(z) - \wp(u)) \tag{11}$$

$$Q_n^2(\wp(z)) = \prod_{v\in E_1[n]} (\wp(z) - \wp(v))\,. \tag{12}$$

On conviendra de poser $P_0 = 0$ et $Q_0 = 1$. Par construction, les polynômes P_n et Q_n sont sans facteurs multiples. La quantité $P_n(\wp(z))$ s'annule si et seulement si $(z+\Lambda) \in E[n]$ et $2z \not\equiv 0\,[\Lambda]$. De même, $Q_n(\wp(z))$ s'annule si et seulement si $(z+\Lambda) \in E_1[n]$ mais $z \not\equiv \frac{\omega_1}{2}\ [\Lambda]$.

Corollaire 3.2 *Choisissons un complexe d_1 pour lequel $d_1^2 = (e_2 - e_1)(e_3 - e_1)$, et une racine carrée $\sqrt{d_1}$.*

Soit $z \in \mathbb{C}$ avec $z \not\equiv 0\,[\Lambda]$. On choisit une racine carrée pour $\wp(z) - e_1$ et on introduit, pour $n \in \mathbb{N}$, les quantités $\mathcal{P}_n(z)$ et $\mathcal{Q}_n(z)$ définies comme suit :

$$\begin{aligned} \textit{pour } n \textit{ impair :} \qquad & \mathcal{P}_n(z) := \sqrt{d_1}\, P_n(\wp(z))\,, \qquad \mathcal{Q}_n(z) := \sqrt{\wp(z) - e_1}\, Q_n(\wp(z))\,, \\ \textit{pour } n \textit{ pair :} \qquad & \mathcal{P}_n(z) := \frac{1}{2}\sqrt{d_1}\, \wp'(z)\, P_n(\wp(z))\,, \quad \mathcal{Q}_n(z) := Q_n(\wp(z))\,. \end{aligned}$$

Ces quantités satisfont alors, pour $m, n \in \mathbb{N}$ avec $m \geq n$, les relations :

$$\mathcal{P}_{m+n}(z)\,\mathcal{P}_{m-n}(z) = \mathcal{P}_m^2(z)\,\mathcal{Q}_n^2(z) - \mathcal{P}_n^2(z)\,\mathcal{Q}_m^2(z)\,, \tag{13}$$

$$\mathcal{Q}_{m+n}(z)\,\mathcal{Q}_{m-n}(z) = \mathcal{Q}_m^2(z)\,\mathcal{Q}_n^2(z) - \mathcal{P}_m^2(z)\,\mathcal{P}_n^2(z)\,. \tag{14}$$

N.B. La notation $d_1^2 := (e_2 - e_1)(e_3 - e_1)$ est standard, et les choix de racines sont sans importance. L'introduction du facteur $\sqrt{d_1}$ (normalisation des $\mathcal{P}_n$) permet de simplifier la relation (14).

Remarques – Soient $z_0 \in \mathbb{C}$ (avec $z_0 \notin \Lambda$) et $n \in \mathbb{N}^*$. La quantité $\mathcal{P}_n(z_0)$ (resp. $\mathcal{Q}_n(z_0)$) s'annule si et seulement si $(z_0 + \Lambda) \in E_0[n]$ (resp. $(z_0 + \Lambda) \in E_1[n]$).

– Les suites $(\mathcal{P}_n(z_0))$ et $(\mathcal{Q}_n(z_0))$ satisfont les mêmes relations de récurrence (qui ne dépendent pas de la courbe elliptique E !) que les suites de polynômes (p_n) et (q_n) évoquées dans l'introduction (théorème 2.1) avec, pour « conditions initiales » :

$$\mathcal{P}_0(z_0) = 0, \qquad \mathcal{Q}_0(z_0) = 1, \tag{15}$$

$$\mathcal{P}_1(z_0) = \sqrt{d_1}, \quad \mathcal{Q}_1(z_0) = \sqrt{\wp(z_0) - e_1} \quad \text{et} \quad \mathcal{P}_2(z_0) = \sqrt{d_1}\,\wp'(z_0). \tag{16}$$

Démonstration Pour montrer la relation (13) (lorsque $m \neq n$), on introduit la fonction elliptique définie sur E par $f(z) = \wp(nz) - \wp(mz)$ et on évalue le diviseur correspondant

$$\operatorname{div}(f) = (-2) \cdot (E[m]) + (-2) \cdot (E[n]) + (E[m+n]) + (E[m-n])\,.$$

Lorsque m et n sont par exemple pairs (les autres cas se traitant de façon semblable), on a d'après le lemme 3.1 et les identités (11), (12) :

$$f(z) = \frac{1}{\frac{1}{4}\,\wp'(z)^2}\, \frac{P_m^2(\wp(z))\,Q_n^2(\wp(z)) - P_n^2(\wp(z))\,Q_m^2(\wp(z))}{P_n^2(\wp(z))\,P_m^2(\wp(z))}\,,$$

ce qui permet de constater que les fonctions elliptiques sur E suivantes :

$$\begin{aligned} z &\mapsto P_m^2(\wp(z))\,Q_n^2(\wp(z)) - P_n^2(\wp(z))\,Q_m^2(\wp(z)) \\ \text{et} \quad z &\mapsto P_{m+n}(\wp(z))\,P_{m-n}(\wp(z)) \end{aligned}$$

ont même diviseur, donc sont proportionnelles ; on en déduit la relation (13) puisque ces deux fonctions sont polynomiales en $\wp(z)$, et de coefficient dominant $m^2 - n^2$.

Pour démontrer la relation (14), on introduit cette fois la fonction elliptique définie sur E par $g(z) = (\wp(nz) - e_1)(\wp(mz) - e_1) - d_1^2$. Pour calculer le diviseur associé, on remarque

d'abord que la fonction elliptique $z \mapsto (\wp(z) - e_1)\,(\wp(z + \frac{\omega_1}{2}) - e_1)$ n'a pas de pôles : elle est donc constante, égale à d_1^2. On en déduit que

$$\begin{aligned} g(z) &= (\wp(nz) - e_1)\,(\wp(mz) - \wp(nz + \frac{\omega_1}{2}))\,, \\ \text{puis} \quad \mathrm{div}(g) &= (-2)\cdot(E[m]) + (-2)\cdot(E[n]) + (E_1[m+n]) + (E_1[m-n])\,. \end{aligned}$$

On termine alors la preuve comme ci-dessus. □
N.B. Pour des calculs similaires, on renvoie au §9.5 de [17].

3.2 Un exemple : la courbe de Poncelet $(F;\sigma)$

Au choix d'une origine près, la courbe de Poncelet $(F;\sigma)$ de paramètres (a,R,r), munie de la symétrie σ, est une courbe elliptique avec un point d'ordre 2. On applique ce qui a été fait dans le paragraphe précédent à $(F;\sigma)$ pour montrer la proposition 3.3. Pour cela, on suit Griffiths-Harris [10].

Proposition 3.3 *Il existe un réseau $\Lambda = \mathbb{Z}\cdot\omega_1 \oplus \mathbb{Z}\cdot\omega_2 \subset \mathbb{C}$, un point $z_0 \in \mathbb{C}^*$, et un isomorphisme $F \xrightarrow{\simeq} \mathbb{C}/\Lambda$ à travers lequel la transformation de Poncelet ϕ et la symétrie σ s'identifient respectivement aux translations par z_0 et $\frac{\omega_1}{2}$. Avec les notations du corollaire 3.2, on a :*

$$\begin{aligned} \phi^n = \mathrm{Id} \quad &ssi \quad nz_0 \equiv 0\,[\Lambda] \quad ssi \quad \mathcal{P}_n(z_0) = 0 \\ \text{et} \quad \phi^n = \sigma \quad &ssi \quad nz_0 \equiv \frac{\omega_1}{2}[\Lambda] \quad ssi \quad \mathcal{Q}_n(z_0) = 0\,, \end{aligned}$$

les quantités $\mathcal{P}_n(z_0)$ et $\mathcal{Q}_n(z_0)$ étant liées par les relations de récurrence (13) *et* (14) *et les conditions initiales* (15) *et* (16)*, avec ici*

$$d_1^2 = \frac{a^2}{R^2}\,, \quad \wp(z_0) - e_1 = 1 \quad \text{et} \quad \wp'(z_0) = \frac{2r}{R}\,.$$

Démonstration Soient C et D nos coniques, supposées transverses ($a, r, R \in \mathbb{C}^*$ avec $a \pm r \pm R \neq 0$) ; on note $F \subset C \times D^*$ la courbe de Poncelet associée. La projection $p : (m,\xi) \in F \mapsto m \in C$ fait de F un revêtement à deux feuillets de C, ramifié aux quatre points d'intersection de C et D. Notons $x_0 = [1,i,0]$, $x_1 = [1,-i,0]$, x_2 et x_3 ces points d'intersection.

La courbe F est une courbe elliptique lisse. La transformation de Poncelet est une translation sur F (comme composée des deux involutions associées aux revêtements, de degré 2, $p : (m,\xi) \in F \mapsto m \in C$ et $p' : (m,\xi) \in F \mapsto \xi \in D^*$). La transformation $\sigma : F \to F$ est une involution sans point fixe ; c'est donc également une translation.

On cherche à réaliser F comme une cubique de $\mathrm{P}^2\mathbb{C}$, pour en trouver une paramétrisation de Weierstrass. On paramètre la conique C par le faisceau des droites issues du point cyclique x_0, ou encore par l'ensemble des tangentes en x_0 aux coniques du faisceau $< C, D >$ engendré par C et D. A travers cette paramétrisation

$$j : t \in \mathrm{P}^1\mathbb{C} \longmapsto j(t) = T_{x_0}(tC + D) \cap C \in C\,,$$

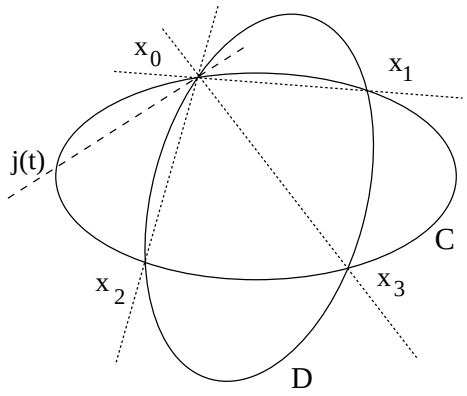

FIGURE 3 – Paramétrisation de C

chacun des points x_i provient d'un paramètre $t_i \in \mathrm{P}^1\mathbb{C} = \mathbb{C} \cup \infty$ (pour $i \in \{0,1,2,3\}$), avec $t_0 = \infty$, et où $t_1 = -1, t_2, t_3$ sont les paramètres qui correspondent aux coniques dégénérées du faisceau $< C, D >$ et sont donc les racines du polynôme

$$P(t) = \det(t\,\mathrm{Id} + M_C^{-1} M_D) = (t+1)\,(t^2 + \tfrac{R^2+r^2-a^2}{R^2}\,t + \tfrac{r^2}{R^2}),$$

M_C et M_D désignant respectivement les matrices symétriques associées aux formes quadratiques définissant C et D.

Introduisons la cubique plane $F' = \{[t,y,1] \mid y^2 = P(t)\} \subset \mathrm{P}^2\mathbb{C}$, et le morphisme de degré 2 défini par $\varpi : [t,y,1] \in F' \mapsto t \in \mathrm{P}^1\mathbb{C}$, qui est ramifié au-dessus des points t_i $(0 \leq i \leq 3)$. La paramétrisation j induit alors un isomorphisme de revêtements $J : F' \to F$

$$\begin{array}{ccc} [t,y,1] \in F' & \xrightarrow{J} & F \\ \varpi \downarrow & & \downarrow p \\ t \in \mathrm{P}^1\mathbb{C} & \xrightarrow{j} & C \end{array}$$

défini à échange des feuillets près. Soient y_i $(i \in \{1,2,3\})$ les points de F pour lesquels $p(y_i) = x_i$. La symétrie σ et la transformation de Poncelet ϕ envoient respectivement le point y_0 sur y_1, et sur l'un des points de F situés au-dessus de $j(0)$. Quitte à échanger les feuillets de F', les applications ϕ et σ se lisent donc à travers l'isomorphisme J comme les translations $\phi_{F'}$ et $\sigma_{F'}$ de la courbe elliptique F' définies par

$$\phi_{F'}([0,1,0]) = [0, \tfrac{r}{R}, 1] \quad \text{et} \quad \sigma_{F'}([0,1,0]) = [-1,0,1].$$

La cubique $F' = \{[t,y,1] \mid y^2 = \prod_{i=1}^{3}(t-t_i)\} \subset \mathrm{P}^2\mathbb{C}$ que nous venons d'introduire n'est, sous cette forme, pas tout à fait l'image d'une paramétrisation de Weierstrass (voir en effet les équations (8)). Cependant, pour $s := \frac{1}{3}\,(t_1+t_2+t_3)$, la transformation projective

$$[t,y,1] \in \mathrm{P}^2\mathbb{C} \longmapsto [u,v,1] := [t-s, 2y, 1] \in \mathrm{P}^2\mathbb{C}$$

envoie la cubique $F' \subset \mathrm{P}^2\mathbb{C}$ sur une cubique normalisée

$$E = \{[u,v,1] \mid v^2 = 4\prod_{i=1}^{3}(u-e_i)\ \} \subset \mathrm{P}^2\mathbb{C}\,,$$

où maintenant $e_1+e_2+e_3=0$. Il existe donc ([15] p.318) un réseau $\Lambda = \mathbb{Z}\cdot\omega_1 \oplus \mathbb{Z}\cdot\omega_2 \subset \mathbb{C}$ (de fonction de Weierstrass associée $\wp$) et un point $z_0 \in \mathbb{C}$, de sorte que la composée des isomorphismes

$$z \in \mathbb{C}/\Lambda \longmapsto [\wp(z), \wp'(z), 1] \in E \longmapsto [\wp(z)+s, \wp'(z)/2, 1] \in F'$$

envoie respectivement les points 0, $\frac{\omega_1}{2}$ et z_0 de $\mathbb{C}/\Lambda$ sur les points $m := [0,1,0]$, $\sigma_{F'}(m) = [-1,0,1]$ et $\phi_{F'}(m) = [0, \frac{r}{R}, 1]$ de F'. On conclut en calculant

$$\begin{aligned} d_1^2 &= (e_2-e_1)(e_3-e_1) = (t_2-t_1)(t_3-t_1) = \frac{a^2}{R^2}\,, \\ \wp(z_0)-e_1 &= (\wp(z_0)+s)-(e_1+s) = 1\,, \quad \text{et} \quad \wp'(z_0) = 2\,\frac{r}{R}\,. \end{aligned}$$

□

4 Les polynômes p_n et q_n, période et semi-période

4.1 Les polynômes p_n et q_n

Dans ce paragraphe, nous démontrons le théorème 2.1, i.e. construisons les suites de polynômes (p_n) et (q_n). Le résultat suivant, dont le théorème 2.2 est un corollaire immédiat, s'en déduit. Les notations sont celles du §3.1.

Théorème 4.1 *Soient $\Lambda = \mathbb{Z}\cdot\omega_1 \oplus \mathbb{Z}\cdot\omega_2 \subset \mathbb{C}$ un réseau, $(E\,; \frac{\omega_1}{2})$ la courbe elliptique $E = \mathbb{C}/\Lambda$ munie du point $(\frac{\omega_1}{2}+\Lambda) \in E$ (d'ordre 2), et $z_0 \in \mathbb{C}$ tel que $z_0 \notin \Lambda$. On note $\mathbf{x}_1 = \sqrt{d_1}$, $\mathbf{y}_1 = \sqrt{\wp(z_0)-e_1}$ et on choisit $\mathbf{z}_1 \in \mathbb{C}$ tel que $\mathbf{y}_1\mathbf{z}_1^2 = \wp'(z_0)$. Alors, pour tout $n \in \mathbb{N}^*$,*

$$\mathcal{P}_n(z_0) = p_n(\mathbf{x}_1, \mathbf{y}_1, \mathbf{z}_1) \quad \text{et} \quad \mathcal{Q}_n(z_0) = q_n(\mathbf{x}_1, \mathbf{y}_1, \mathbf{z}_1).$$

N.B. Les indices des variables $(\mathbf{x}_1, \mathbf{y}_1, \mathbf{z}_1)$ font référence au point d'ordre 2 de E qui a été choisi, ici $\frac{\omega_1}{2}+\Lambda \in E$. Cette distinction sera indispensable par la suite : voir les §5.1 et §5.3.

Démonstration des théorèmes 4.1 et 2.2 Pour toute condition initiale

$$a_0 = 0\,,\ b_0 = 1 \ \text{ et } \quad a_1, b_1, a_2 \in \mathbb{C}^*$$

il existe au plus un couple de suites complexes $(a_n), (b_n)$ vérifiant les relations $(m \geq n)$:

$$\begin{aligned} a_{m+n}a_{m-n} &= a_m^2 b_n^2 - a_n^2 b_m^2 \qquad (1)_{m,n} \\ b_{m+n}b_{m-n} &= b_m^2 b_n^2 - a_m^2 a_n^2 \qquad (2)_{m,n} \end{aligned}$$

(utiliser les relations $(2)_{n,n}$ $(2)_{n+1,n}$ $(1)_{n+1,n}$ et $(1)_{n+2,n}$).

On sait, d'après le corollaire 3.2, que ces suites existent pour toute condition initiale

$$(a_1, b_1, a_2) \in \mathcal{D} := \{\big(\sqrt{d_1}, \sqrt{\wp(z_0) - e_1}, \sqrt{d_1}\,\wp'(z_0)\,\big)\} \subset (\mathbb{C}^*)^3$$

associée à une courbe elliptique $E = \mathbb{C}/\Lambda$ avec un point d'ordre 2, et un point $z_0 \in \mathbb{C}$ tel que $2z_0 \not\equiv 0\,[\Lambda]$: poser $a_n = \mathcal{P}_n(z_0)$ et $b_n = \mathcal{Q}_n(z_0)$ (voir les relations (13) et (14)). Une fois les suites (p_n) et (q_n) construites on saura donc (en vertu de l'unicité évoquée ci-dessus) que, pour toute condition initiale $(a_1, b_1, a_2) \in \mathcal{D}$, $a_n = p_n\big(a_1, b_1, \sqrt{a_2/(a_1 b_1)}\,\big)$ et $b_n = q_n\big(a_1, b_1, \sqrt{a_2/(a_1 b_1)}\,\big)$ pour tout $n \geq 0$.

Ceci démontre le théorème 4.1. Le théorème 2.2 s'en déduit en revenant à l'interprétation des quantités $\mathcal{P}_n(z_0)$ et $\mathcal{Q}_n(z_0)$, et aux calculs explicites de la proposition 3.3. □

Remarque 4.2 Lorsque le couple $(a_n), (b_n)$ satisfait les relations de récurrence ci-dessus, avec $(a_1, b_1, a_2) \in (\mathbb{C}^*)^3$ et $a_4 \neq 0$, les suites définies par $(\tilde{a}_n) := (a_{2n})$ et $(\tilde{b}_n) := (b_{2n})$ vérifient de nouveau les relations de récurrence $(1)_{m,n}$ et $(2)_{m,n}$, mais avec cette fois les conditions initiales

$$\tilde{a}_0 = 0\,,\ \tilde{b}_0 = 1 \ \text{ et } \ \tilde{a}_1 = a_2\,,\ \tilde{b}_1 = b_2\,,\ \tilde{a}_2 = a_4 \in \mathbb{C}^*\,;$$

on aura donc $\tilde{a}_n = a_{2n} = p_n\big(a_2, b_2, \sqrt{a_4/(a_2 b_2)}\,\big)$ et $\tilde{b}_n = b_{2n} = q_n\big(a_2, b_2, \sqrt{a_4/(a_2 b_2)}\,\big)$.

Constatation analogue pour tout $\ell \geq 2$, et les suites $(\tilde{a}_n) := (a_{2n\ell})$ et $(\tilde{b}_n) := (b_{n\ell})$.

Cette remarque nous sera utile dans la démonstration suivante.

Démonstration du théorème 2.1 Dans un premier temps, nous montrons qu'en partant des données initiales

$$p_0 = 0\,,\ q_0 = 1\,,\ p_1 = x\,,\ q_1 = y\,,\ p_2 = xyz^2\,,$$

on peut construire récursivement des polynômes $p_m \in \mathbb{Z}[x, y, z^2]$ et $q_m \in \mathbb{Z}[x, y, z^2]$:

– satisfaisant les relations de divisibilité :

$q_1 | q_{2k+1}$ (correspondant, via le th. 4.1, à $z_0 \equiv \frac{\omega_1}{2}\,[\Lambda] \Rightarrow (2k+1)\,z_0 \equiv \frac{\omega_1}{2}\,[\Lambda]$)
$q_1 | p_{2k}$ (correspondant à $z_0 \equiv \frac{\omega_1}{2}\,[\Lambda] \Rightarrow 2k\,z_0 \equiv 0\,[\Lambda]$)
et $p_1 | p_n$ (correspondant à $z_0 \equiv 0\,[\Lambda] \Rightarrow n\,z_0 \equiv 0\,[\Lambda]$) ;

– et vérifiant *une partie* des relations (1) et (2).

On distingue selon la parité de m.

– D'une part on pose $q_{2n} = q_0 q_{2n} = q_n^4 - p_n^4$.
D'autre part on définit q_{2n+1} par la relation $q_{2n+1} q_1 = q_{n+1}^2 q_n^2 - p_{n+1}^2 p_n^2$. Par récurrence, q_1 divise p_n ou p_{n+1}, et q_1 divise q_n ou q_{n+1}. Donc q_{2n+1} est un polynôme divisible par q_1.

– On définit p_{2n+1} par la relation $p_{2n+1}p_1 = p_{n+1}^2 q_n^2 - p_n^2 q_{n+1}^2$. Par récurrence, $p_1 | p_k$ pour $k < 2n+1$, donc p_{2n+1} est un polynôme divisible par p_1.
On souhaite enfin définir les polynômes p_{2n} ($n \geq 2$). Commençons par définir p_4. On détermine explicitement $p_3 = x[y^4z^4 - (y^4 - x^4)^2]$, $q_3 = y[(y^4 - x^4)^2 - x^4z^4]$, et l'on constate que la relation $p_4 p_2 = p_3^2 q_1^2 - p_1^2 q_3^2$ définit un polynôme $p_4 \in \mathbb{Z}[x, y, z^2]$, divisible par le produit $p_2 q_2$, à savoir $p_4 = p_2 q_2 \, (4y^4x^4 + x^4z^4 + y^4z^4 - 2(x^8 + y^8))$. Les $p_k \in \mathbb{Z}[x, y, z^2]$ étant supposés déjà construits pour $0 \leq k \leq 2n-1$, on peut alors définir un polynôme $p_{2n} \in \mathbb{Z}[x, y, z^2]$ en posant

$$p_{2n}(x, y, z) = p_n\Big(p_2, q_2, \sqrt{\frac{p_4}{p_2 q_2}}\Big) .$$

On observe que $p_1 q_1$ divise p_2, donc divise p_{2n}.

D'après la discussion menée dans la preuve du théorème 4.1, les fonctions polynomiales $p_{m+n}p_{m-n}$ et $p_m^2 q_n^2 - p_n^2 q_m^2$ (resp. $q_{m+n}q_{m-n}$ et $q_m^2 q_n^2 - p_m^2 p_n^2$) coïncident sur un ouvert non vide de $\mathbb{C}^3$; les suites (p_n) et (q_n) vérifient donc *toutes* les relations de récurrence (1) et (2).

On vérifie facilement que les polynômes p_n et q_n construits ci-dessus sont homogènes de degré n^2, et que pour n impair $p_n \in x\,\mathbb{Z}[x^4, y^4, z^4]$ et $q_n \in y\,\mathbb{Z}[x^4, y^4, z^4]$, tandis que pour n pair $p_n \in xyz^2\,\mathbb{Z}[x^4, y^4, z^4]$ et $q_n \in \mathbb{Z}[x^4, y^4, z^4]$.

Les relations (5) découlent de la remarque 4.2. Il restera à montrer, pour achever la preuve du théorème 2.1, que les quotients $p_{2\ell}/(p_\ell q_\ell)$ intervenant dans les relations (5) sont des fonctions polynomiales en (x, y, z). Ce sera fait au corollaire 4.7. □

Remarque Lorsque C et D sont deux coniques (quelconques) transverses, Halphen ([9] vol.II p. 377, ou [2]) introduit les birapports α et γ de leurs quatre points d'intersection, pris respectivement sur C et D ; le couple (α, γ) est un invariant projectif associé au couple de coniques (C, D). En utilisant la formule d'addition, il construit une suite de fonctions H_n pour lesquelles $\phi^n = \mathrm{Id}$ si et seulement si $\mathrm{H}_n(\alpha, \gamma) = 0$ ([9] vol.I p.102). Ces fonctions vérifient les relations

$$\mathrm{H}_{m+n}\mathrm{H}_{m-n} = \mathrm{H}_{m+1}\mathrm{H}_{m-1}\mathrm{H}_n^2 - \mathrm{H}_{n+1}\mathrm{H}_{n-1}\mathrm{H}_m^2 . \tag{17}$$

Dans cette note, nous avons imposé aux deux coniques de passer par les points cycliques. Ceci nous a permis, en nous intéressant simultanément aux conditions sous lesquelles $\phi^n = \mathrm{Id}$ ou $\phi^n = \sigma$, d'obtenir des relations de récurrence plus faciles à manipuler que (17) : voir en particulier la relation (5). Cela dit, la méthode que nous avons suivie est semblable à celle de Halphen : les quantités p_n du théorème 2.2 sont liées aux fonctions de Halphen par les relations

$$\mathrm{H}_n(\alpha, \gamma) = \tfrac{p_n}{p_1}\,\big(\sqrt{\tfrac{a}{R}}, 1, \sqrt{\tfrac{2r}{R}}\big),$$

et l'on retrouve la relation (17) en éliminant q_n^2 et q_m^2 de l'identité (1) à l'aide de cette même identité, exprimée pour les couples $(m, 1)$ et $(n, 1)$.

4.2 Quelques propriétés des polynômes p_n et q_n

L'objectif de ce paragraphe est de montrer que le polynôme $p_{2\ell}$ est divisible par le produit $p_\ell q_\ell$ ($\ell \in \mathbb{N}^*$).

Lemme 4.3 *Il existe une suite de polynômes en une variable $g_n \in \mathbb{Z}[t]$ (polynômes de Tchebychev) telle que, pour tous $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, $g_n(\cos\theta) \cdot \sin\theta = \sin(n\theta)$. Cette suite est définie de façon unique par les conditions*

$$g_0 = 0\,,\ g_1 = 1\,,\ g_2(t) = 2t \tag{18}$$

$$g_{m+n}\, g_{m-n} = g_m^2 - g_n^2 \qquad (m \geq n)\,. \tag{19}$$

Démonstration C'est une conséquence bien classique des formules de trigonométrie

$$\begin{aligned} & \sin(n+1)\theta + \sin(n-1)\theta = 2\sin n\theta\cos\theta \\ \text{et} \qquad & \sin(m+n)\theta\ \sin(m-n)\theta = \sin^2 m\theta - \sin^2 n\theta\,. \end{aligned}$$ □

Lemme 4.4 *On introduit, pour $n \in \mathbb{N}$, la fonction polynomiale $f_n \in \mathbb{Z}[x, y, z^2]$ pour laquelle $p_n(x, y, z) = x\, f_n(x, y, z)$. Alors, pour tout $t \in \mathbb{C}$, $f_n(0, 1, \sqrt{2t}) = g_n(t)$.*

Démonstration La relation (2) montre que, pour tous $n \in \mathbb{N}$ et $s \in \mathbb{C}$, on a $q_n(0, 1, s) = 1$. On déduit alors de (1) que la suite de fonctions $t \in \mathbb{C} \mapsto f_n(0, 1, \sqrt{2t})$ satisfait les relations (18) et (19), d'où la conclusion. □

Corollaire 4.5 *Aucun des polynômes $2x^2 \pm 2y^2 \pm z^2$ ne divise p_n ou q_n ($n \in \mathbb{N}^*$).*

Démonstration Le polynôme $2x^2 \pm 2y^2 \pm z^2$ ne peut diviser p_n ; sinon le lemme 4.4 montrerait que $1 \pm t$ divise $g_n(t)$, une contradiction. De même pour q_n, puisqu'on a vu que $q_n(0, 1, s) = 1$.

□

Terminons par un petit formulaire qui nous sera utile par la suite.

Lemme 4.6 *Soit $n \geq 2$. Pour chacun des polynômes p_n et q_n, les termes de degré maximal en x d'une part, et de degré maximal en y d'autre part, sont donnés par les expressions suivantes :*

$$\begin{aligned} \textit{lorsque } n \textit{ est impair :} \qquad p_n &= (-1)^{\frac{n-1}{2}}\, x\,[x^{n^2-1} + y^{n^2-1}] + \cdots \\ q_n &= y\,[x^{n^2-1} + y^{n^2-1}] + \cdots \\ \textit{lorsque } n \textit{ est pair :} \qquad p_n &= xyz^2\,[\frac{n}{2}\, x^{n^2-4} + (-1)^{\frac{n}{2}-1}\,\frac{n}{2}\, y^{n^2-4}] + \cdots \\ q_n &= (-1)^{\frac{n}{2}} x^{n^2} + y^{n^2} + \cdots\,. \end{aligned}$$

De plus, ces polynômes possèdent les symétries suivantes :

$$p_{2n}(x, y, z) = (-1)^{n+1} p_{2n}(y, x, z)$$

$$\begin{aligned} q_{2n}(x,y,z) &= (-1)^n\ q_{2n}(y,x,z) \\ p_{2n+1}(x,y,z) &= (-1)^n\ q_{2n+1}(y,x,z)\,. \end{aligned}$$

Enfin : $q_{2n}(x,y,0) = (y^4-x^4)^{n^2}\,,\qquad q_{2n+1}(x,y,0) = \ y\,(y^4-x^4)^{n(n+1)}\,,$
$p_{2n+1}(x,0,z) = (-1)^n x^{4n^2+4n+1}$ *et* $\qquad q_{2n}(x,0,z) = x^{4n^2}\,.$

Démonstration Récurrence élémentaire, que nous laissons au lecteur. □

Corollaire 4.7 *Pour tout entier $\ell \geq 1$, le polynôme $p_{2\ell}$ est divisible par le produit $p_\ell q_\ell$, avec quotient dans $\mathbb{Z}[x^2,y^2,z^2]$.*

Démonstration Dans la proposition 3.3, nous avons associé à chaque configuration de Poncelet de paramètres $(a,R,r) \in (\mathbb{C}^*)^3$, avec $a \pm R \pm r \neq 0$, une courbe elliptique $(E;\frac{\omega_1}{2})$ (où $E = \mathbb{C}/\Lambda$) et un point $z_0 \in E$ pour lesquels, avec les notations du théorème 4.1 :

$$(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) = \Big(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}}\Big)\,.$$

Introduisons, pour $n \in \mathbb{N}^*$, les ensembles $A_0[n] = \{\wp(u) \in \mathbb{C} \mid 2u \not\equiv 0\,,\ nu \equiv 0\ [\Lambda]\}$ et $A_1[n] = \{\wp(v) \in \mathbb{C} \mid v \not\equiv \frac{\omega_1}{2}\,,\ nv \equiv \frac{\omega_1}{2}\ [\Lambda]\}$ ($\wp$ désignant la fonction de Weierstrass de $E = \mathbb{C}/\Lambda$). D'après le théorème 4.1 on a :

$$p_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) = n \prod_{\alpha\in A_0[n]} (\wp(z_0)-\alpha) \quad \text{et} \quad q_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) = \prod_{\beta\in A_1[n]} (\wp(z_0)-\beta)\,.$$

Pour $\ell \geq 1$, les ensembles $A_0[\ell]$ et $A_1[\ell]$ sont disjoints et inclus dans $A_0[2\ell]$. On conclut donc, par homogénéité des polynômes $p_{2\ell}$, p_ℓ et q_ℓ, que le quotient $p_{2\ell}/(p_\ell\, q_\ell)$ est non singulier en tout point de

$$\mathbf{D} := \{(x,y,z) \in (\mathbb{C}^*)^3 \mid 2x^2 \pm 2y^2 \pm z^2 \neq 0\}\,.$$

Supposons alors (par exemple) ℓ impair. Nous avons $p_{2\ell} \in xyz^2\mathbb{Z}[x,y,z]$. Or, d'après le corollaire 4.5 et le lemme 4.6, les facteurs irréductibles des polynômes p_ℓ/x et q_ℓ/y sont distincts de x, y, z et des polynômes $2x^2 \pm 2y^2 \pm z^2$. Il existe donc un polynôme $r_\ell \in \mathbb{Q}[x,y,z]$ pour lequel $p_{2\ell} = p_\ell q_\ell r_\ell$. Le fait que r_ℓ soit à coefficients entiers s'obtient en constatant, avec le lemme 4.6, que les contenus des polynômes p_ℓ/x et q_ℓ/y sont égaux à 1. □

4.3 Les polynômes φ_n et ψ_n

L'objet de ce paragraphe est de démontrer la proposition 2.4, i.e. de construire les suites de polynômes (φ_n) et (ψ_n). La proposition suivante s'en déduira.

On introduit la suite $(\gamma_n)_{n\geq 1}$ définie par $\gamma_n = p$ lorsque $n = p^r$ est puissance d'un nombre premier p, et $\gamma_n = 1$ sinon, de sorte que pour tout $n \in \mathbb{N}^*$ on a $n = \prod_{d|n} \gamma_d$.

Proposition 4.8 *Soient $\Lambda = \mathbb{Z}\cdot\omega_1 \oplus \mathbb{Z}\cdot\omega_2 \subset \mathbb{C}$ un réseau, $(E\,;\frac{\omega_1}{2})$ la courbe elliptique $E=\mathbb{C}/\Lambda$ munie du point $(\frac{\omega_1}{2}+\Lambda)\in E$ (d'ordre 2). On note :*

$$\begin{aligned} V_0[n] &= \{\, \wp(u)\in\mathbb{C} \mid u \text{ de période } \tfrac{\omega_1}{2}\text{-stricte } n \text{ dans } E=\mathbb{C}/\Lambda \,\}\,, \\ V_1[n] &= \{\, \wp(u)\in\mathbb{C} \mid u \text{ de } \tfrac{\omega_1}{2}\text{-semi-période } n \text{ dans } E=\mathbb{C}/\Lambda \,\}\,. \end{aligned}$$

Soit $z_0\in\mathbb{C}$ tel que $z_0\notin\Lambda$. Avec les notations du théorème 4.1, on a pour tout $n\geq 3$:

$$\varphi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1)=\gamma_n\prod_{\alpha\in V_0[n]}(\wp(z_0)-\alpha)\quad et\qquad \psi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1)=\prod_{\beta\in V_1[n]}(\wp(z_0)-\beta)\,.$$

Démonstration Conséquence immédiate des relations (6), (7), et du théorème 4.1. □

Démonstration de la proposition 2.4 On pose $\psi_1=q_1=y$. On suppose construits les polynômes ψ_k pour $k\leq n-1$, de sorte que les relations $(7)_k$ soient satisfaites pour $1\leq k\leq n-1$, et l'on veut construire ψ_n.

On va procéder comme dans la preuve du corollaire 4.7. On applique la proposition précédente (pour les polynômes qui ont déjà été construits) à la courbe elliptique $(E\,;\frac{\omega_1}{2})$ et au point z_0 associés à une configuration de Poncelet de paramètres $a,r,R\in\mathbb{C}^*$ avec $a\pm r\pm R\neq 0$; on obtient, pour tout $1\leq k\leq n-1$, l'identité :

$$\psi_k\Big(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}}\Big)=\prod_{\beta\in V_1[k]}(\wp(z_0)-\beta)\,, \tag{20}$$

et l'on déduit alors du théorème 4.1 que :

$$q_n\Big(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}}\Big)\;=\;\prod_{\beta\in V_1[n]}(\wp(z_0)-\beta)\prod_{\substack{d\leq n-1\,,\,d|n\\ \frac{n}{d}\text{ impair}}}\psi_d\Big(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}}\Big)\,. \tag{21}$$

Le quotient de q_n par le produit $\prod\psi_d$ (portant sur $d\leq n-1$, et $d|n$ avec n/d impair) est donc non singulier en tout point de $\mathbf{D}=\{(x,y,z)\in(\mathbb{C}^*)^3 \mid 2x^2\pm 2y^2\pm z^2\neq 0\}$. On conclut donc que ce quotient est un polynôme homogène $\psi_n\in\mathbb{Z}[x^4,y^4,z^4]$. Par construction, et lorsque $k\neq\ell$, les quantités $\psi_k(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}})$ et $\psi_\ell(\sqrt{\frac{a}{R}},1,\sqrt{\frac{2r}{R}})$ ne s'annulent pas simultanément ; les polynômes ainsi construits sont donc premiers entre eux deux à deux.

Les mêmes arguments permettent ensuite de construire récursivement les polynômes φ_n vérifiant les identités (6). □

4.4 Les premiers polynômes de Poncelet Φ_n et Ψ_n

Pour rendre ce texte encore plus concret nous indiquons ci-dessous les premiers polynômes de Poncelet $\Phi_n(a,R,r):=\varphi_n(\sqrt{a},\sqrt{R},\sqrt{2r})$ et leurs analogues $\Psi_n(a,R,r):=\psi_n(\sqrt{a},\sqrt{R},\sqrt{2r})$ $(2\leq n\leq 7)$, ainsi que leurs décompositions en facteurs irréductibles de $\mathbb{C}[a,R,r]$. L'idée n'est pas de suggérer au lecteur de retenir ces expressions... mais de donner une idée de leur complexité.

Des considérations de géométrie élémentaire montrent que, pour a, R, r réels avec $R, r > 0$, la configuration de Poncelet correspondante est de σ-semi-période 2 lorsque le centre du cercle D appartient à C, i.e. lorsque $a = \pm R$.

De même, elle est de période σ-stricte 3 lorsque C et D sont respectivement le cercle circonscrit et le cercle inscrit (ou le cercle circonscrit et un cercle exinscrit) relativement à un même triangle, c'est-à-dire lorsque $a^2 = R^2 - 2rR$ (ou $a^2 = R^2 + 2rR$) : ce sont les formules d'Euler. (On retrouvera les facteurs correspondants, soient $R \pm a$, ou bien $a^2 \pm 2rR - R^2$, dans Ψ_2 et Φ_3 ci-dessous).

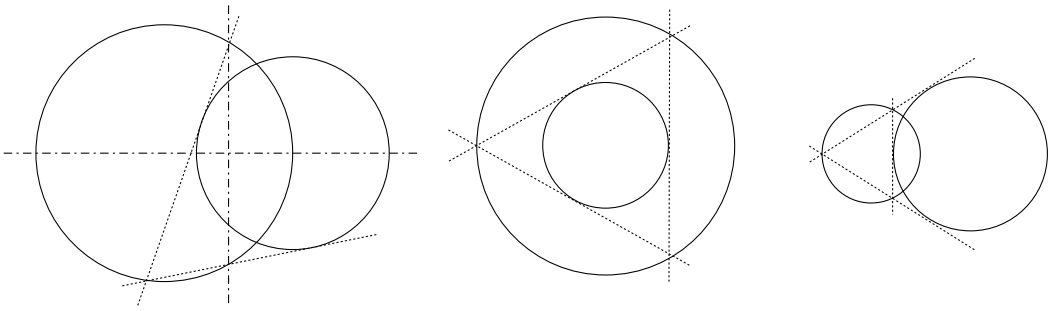

FIGURE 4 – Une configuration de Poncelet de σ-semi-période 2 ; deux configurations de Poncelet de période σ-stricte 3, correspondant à chacun des deux facteurs de Φ_3

Plus généralement, et d'après ce qui précède, une configuration de Poncelet associée aux paramètres complexes a, R, r sera de période σ-stricte (resp. de σ-semi-période) n lorsque $\Phi_n(a, R, r) := \varphi_n(\sqrt{a}, \sqrt{R}, \sqrt{2r})$ (resp. $\Psi_n(a, R, r) := \psi_n(\sqrt{a}, \sqrt{R}, \sqrt{2r})$) s'annule ; lorsque $n \geq 2$, ces expressions sont polynomiales en (a, R, r). Pour les premières valeurs de n, on obtient (après factorisation pour $n \geq 2$) :

$$
\begin{aligned}
\Phi_1 &= \sqrt{a} \\
\Psi_1 &= \sqrt{R} \\
\Phi_2 &= 2r \\
\Psi_2 &= (R-a)\,(R+a) \\
\\
\Phi_3 &= -(a^2 - 2rR - R^2)\,(a^2 + 2rR - R^2) \\
\Psi_3 &= (a^2 - 2ra - R^2)\,(a^2 + 2ra - R^2) \\
\\
\Phi_4 &= 4r^2R^2 - 2R^4 + 4a^2r^2 + 4a^2R^2 - 2a^4 \\
\Psi_4 &= (a^4 + 4aRr^2 - 2a^2R^2 + R^4)\,(a^4 - 4aRr^2 - 2a^2R^2 + R^4) \\
\\
\Phi_5 &= (a^6 - 2a^4rR + 8a^2r^3R - 3a^4R^2 - 4a^2r^2R^2 + 4a^2rR^3 + 3a^2R^4 + 4r^2R^4 - 2rR^5 - R^6) \\
&\quad\ (a^6 + 2a^4rR - 8a^2r^3R - 3a^4R^2 - 4a^2r^2R^2 - 4a^2rR^3 + 3a^2R^4 + 4r^2R^4 + 2rR^5 - R^6) \\
\Psi_5 &= (R^6 - 2R^4ra + 8R^2r^3a - 3R^4a^2 - 4R^2r^2a^2 + 4R^2ra^3 + 3R^2a^4 + 4r^2a^4 - 2ra^5 - a^6) \\
&\quad\ (R^6 + 2R^4ra - 8R^2r^3a - 3R^4a^2 - 4R^2r^2a^2 - 4R^2ra^3 + 3R^2a^4 + 4r^2a^4 + 2ra^5 - a^6)
\end{aligned}
$$

$$
\begin{aligned}
\Phi_6 &= 4\,R^6r^2 - 3\,R^8 + 16\,a^2R^2r^4 - 4\,a^2R^4r^2 + 12\,a^2R^6 \\
&\quad -4\,a^4R^2r^2 - 18\,R^4a^4 + 4\,a^6r^2 + 12\,a^6R^2 - 3\,a^8 \\
\Psi_6 &= (R^8 + 16\,r^2a^3R^3 - 8\,r^2a^5R - 4\,a^2R^6 + 6\,a^4R^4 \\
&\quad -16\,a^2R^2r^4 + 16\,a^3r^4R + 16\,ar^4R^3 - 8\,r^2aR^5 - 4\,a^6R^2 + a^8) \\
&\quad (R^8 - 16\,r^2a^3R^3 + 8\,r^2a^5R - 4\,a^2R^6 + 6\,a^4R^4 \\
&\quad -16\,a^2R^2r^4 - 16\,a^3r^4R - 16\,ar^4R^3 + 8\,r^2aR^5 - 4\,a^6R^2 + a^8)
\end{aligned}
$$

$$
\begin{aligned}
\Phi_7 &= (48\,a^4R^5r^3 + 15\,a^4R^8 + R^{12} - 20\,R^9a^2r + 20\,a^8R^3r + 40\,a^4R^7r - 64\,a^6R^3r^3 + 64\,a^2R^4r^6 \\
&\quad -16\,a^6R^2r^4 - 24\,a^4R^6r^2 + 24\,a^8Rr^3 + 32\,a^4R^4r^4 - 4\,a^8R^2r^2 - 40\,a^6R^5r \\
&\quad -16\,a^2R^6r^4 + 15\,a^8R^4 - 4\,a^{10}Rr - 4\,R^{10}r^2 + 4\,R^{11}r - 8\,R^9r^3 - 6\,a^{10}R^2 \\
&\quad -6\,R^{10}a^2 + a^{12} - 32\,a^6Rr^5 + 32\,a^2R^5r^5 - 20\,a^6R^6 + 16\,R^8a^2r^2 + 16\,a^6R^4r^2) \\
&\quad (48\,a^4R^5r^3 - 15\,a^4R^8 - R^{12} - 20\,R^9a^2r + 20\,a^8R^3r + 40\,a^4R^7r - 64\,a^6R^3r^3 - 64\,a^2R^4r^6 \\
&\quad +16\,a^6R^2r^4 + 24\,a^4R^6r^2 + 24\,a^8Rr^3 - 32\,a^4R^4r^4 + 4\,a^8R^2r^2 - 40\,a^6R^5r \\
&\quad +16\,a^2R^6r^4 - 15\,a^8R^4 - 4\,a^{10}Rr + 4\,R^{10}r^2 + 4\,R^{11}r - 8\,R^9r^3 + 6\,a^{10}R^2 \\
&\quad +6\,R^{10}a^2 - a^{12} - 32\,a^6Rr^5 + 32\,a^2R^5r^5 + 20\,a^6R^6 - 16\,R^8a^2r^2 - 16\,a^6R^4r^2) \\
\Psi_7 &= (R^{12} + 16\,R^2r^2a^8 + 20\,rR^8a^3 - 4\,rR^{10}a + 40\,rR^4a^7 + 64\,R^2r^6a^4 - 32\,r^5R^6a \\
&\quad -64\,r^3R^6a^3 - 40\,rR^6a^5 + 48\,r^3R^4a^5 + 32\,r^5R^2a^5 - 20\,rR^2a^9 + 24\,r^3R^8a \\
&\quad -20\,R^6a^6 - 6\,R^2a^{10} - 6\,R^{10}a^2 + 15\,R^4a^8 + a^{12} + 15\,a^4R^8 + 16\,R^6r^2a^4 - 24\,R^4r^2a^6 \\
&\quad -4\,R^8r^2a^2 - 16\,R^2r^4a^6 - 16\,R^6r^4a^2 + 32\,R^4r^4a^4 - 8\,r^3a^9 - 4\,r^2a^{10} + 4\,ra^{11}) \\
&\quad (R^{12} + 16\,R^2r^2a^8 - 20\,rR^8a^3 + 4\,rR^{10}a - 40\,rR^4a^7 + 64\,R^2r^6a^4 + 32\,r^5R^6a \\
&\quad +64\,r^3R^6a^3 + 40\,rR^6a^5 - 48\,r^3R^4a^5 - 32\,r^5R^2a^5 + 20\,rR^2a^9 - 24\,r^3R^8a \\
&\quad -20\,R^6a^6 - 6\,R^2a^{10} - 6\,R^{10}a^2 + 15\,R^4a^8 + a^{12} + 15\,a^4R^8 + 16\,R^6r^2a^4 - 24\,R^4r^2a^6 \\
&\quad -4\,R^8r^2a^2 - 16\,R^2r^4a^6 - 16\,R^6r^4a^2 + 32\,R^4r^4a^4 + 8\,r^3a^9 - 4\,r^2a^{10} - 4\,ra^{11})\,.
\end{aligned}
$$

Remarque Les symétries (géométriquement surprenantes)

$$
\begin{aligned}
\Phi_{2n+1}(a,R,r) &= \pm\Psi_{2n+1}(R,a,r) \\
\Phi_{2n}(a,R,r) &= \pm\Phi_{2n}(R,a,r) \\
\text{et}\quad \Psi_{2n}(a,R,r) &= \pm\Psi_{2n}(R,a,r)\,,
\end{aligned}
$$

sont conséquence du lemme 4.6 (symétries en (x,y) des polynômes p_n et q_n). Elles avaient été remarquées par Chaundy (voir [6] p.110 et [7]). On s'intéressera à d'autres symétries dans le corollaire 5.11.

On veut maintenant comprendre géométriquement ce qui apparaît sur ces premiers exemples (voir le théorème 2.6) : chacun des polynômes $\Phi_{2n+1}(a,R,r)$ et $\Psi_m(a,R,r)$ se factorise, contrairement aux $\Phi_{2n}(a,R,r)$. Comme il a été expliqué dans l'introduction, cela nous amène à introduire le relèvement de la transformation de Poncelet $\phi : F \to F$ à un revêtement de degré 2 convenable de la courbe elliptique $(F;\sigma)$.

5 Revêtement double d'une courbe avec un point d'ordre 2

5.1 Revêtement double de $(E; \frac{\omega_1}{2})$; période et semi-période

On se place, en un premier temps, sur une courbe elliptique avec un point d'ordre 2 générale, soit $(E\,; \frac{\omega_1}{2})$. On introduit le revêtement de degré 2, soit $E^* \to (E\,; \frac{\omega_1}{2})$, qui nous intéressera ainsi que les notions de période et de semi-période dans $(E\,; \frac{\omega_1}{2})$ et dans E^* qui seront pertinentes pour la suite.

Soit $E = \mathbb{C}/\Lambda$ la courbe elliptique associée au réseau $\Lambda = \mathbb{Z} \cdot \omega_1 \oplus \mathbb{Z} \cdot \omega_2$. Le réseau Λ possède trois sous-réseaux d'indice 2 que l'on désignera par $\Lambda_i \subset \Lambda$ ($i \in \{1, 2, 3\}$) et qui sont respectivement caractérisés par les propriétés suivantes (voir la figure 5) :

$$\omega_i \in \Lambda_i\,, \qquad \omega_k \notin \Lambda_i \quad \text{lorsque } k \in \{1, 2, 3\} \text{ avec } k \neq i\,.$$

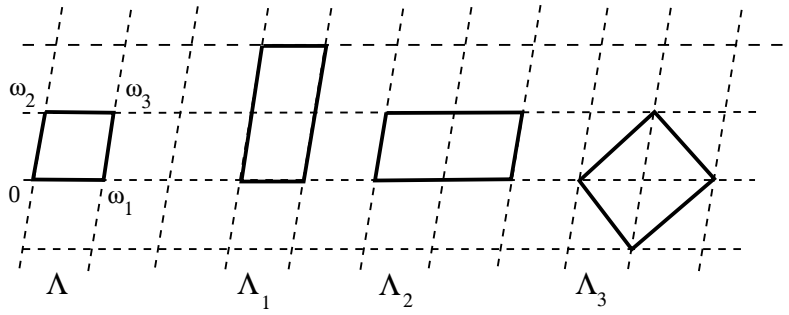

FIGURE 5 – Mailles pour les réseaux Λ et Λ_i, $i \in \{1, 2, 3\}$

On munit désormais E du point $(\frac{\omega_1}{2} + \Lambda)$, d'ordre 2. On note alors $\Lambda^* := \Lambda_1$, et on introduit l'unique revêtement à deux feuillets de E, soit

$$E^* = \mathbb{C}/\Lambda^* \to E = \mathbb{C}/\Lambda\,,$$

pour lequel notre point $(\frac{\omega_1}{2} + \Lambda) \in E$ se relève en deux points d'ordre 2 de E^*. On notera alors $(\frac{\omega_i^*}{2} + \Lambda^*)$ (pour $i \in \{1, 2, 3\}$) les trois points d'ordre 2 de E^*, $(\frac{\omega_2^*}{2} + \Lambda^*)$ se projetant dans E sur $(0 + \Lambda)$, les deux autres (pour le moment indistinguables) sur $(\frac{\omega_1}{2} + \Lambda)$.

Observons que, pour $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$, on a :

$$nz \equiv 0\,[\Lambda] \qquad \text{ssi} \qquad nz \equiv 0\,[\Lambda^*] \quad \text{ou} \quad nz \equiv \frac{\omega_2^*}{2}\,[\Lambda^*] \tag{22}$$

$$nz \equiv \frac{\omega_1}{2}\,[\Lambda] \qquad \text{ssi} \qquad nz \equiv \frac{\omega_1^*}{2}\,[\Lambda^*] \text{ ou } nz \equiv \frac{\omega_3^*}{2}\,[\Lambda^*]\,. \tag{23}$$

On précise alors ce qu'on entendra par « période stricte » et « semi-période » sur chacune des deux courbes elliptiques $(E; \frac{\omega_1}{2})$ et E^*. Sur $(E; \frac{\omega_1}{2})$, le point d'ordre 2 qu'on a choisi,

soit $\frac{\omega_1}{2} + \Lambda \in E$, joue un rôle particulier (on retrouve la définition 2.3 donnée dans l'introduction pour $(F;\sigma)$). Sur E^*, on prend en compte les trois points d'ordre 2.

Définition 5.1 *Soit $z \in \mathbb{C}$.*

Dans la courbe elliptique $(E\,;\frac{\omega_1}{2})$ avec point d'ordre 2, *on dira que :*

- *z est $\frac{\omega_1}{2}$-semi-périodique s'il existe un entier $n \in \mathbb{N}^*$ pour lequel $nz \equiv \frac{\omega_1}{2}\,[\Lambda]$;*
- *z est strictement périodique s'il n'est pas $\frac{\omega_1}{2}$-semi-périodique, et s'il existe un entier $n \in \mathbb{N}^*$ pour lequel $nz \equiv 0\,[\Lambda]$.*

Dans la courbe elliptique E^*, *on dira que :*

- *z est $\frac{\omega_k^*}{2}$-semi-périodique ($k = \{1,2,3\}$) s'il existe un entier $n \in \mathbb{N}^*$ avec $nz \equiv \frac{\omega_k^*}{2}\,[\Lambda^*]$;*
- *z est strictement périodique s'il n'est $\frac{\omega_k^*}{2}$-semi-périodique pour aucun $k = \{1,2,3\}$, et s'il existe un entier $n \in \mathbb{N}^*$ pour lequel $nz \equiv 0\,[\Lambda^*]$.*

On définit alors la période stricte, ou la semi-période de z, comme en 2.3.

Noter que si $(z + \Lambda^*) \in E^*$ est strictement périodique, sa période stricte est impaire. Le tableau suivant précise alors (22) et (23).

Propriété 5.2 Soit $z_0 \in \mathbb{C}$. On a les équivalences suivantes :

dans $(E\,;\frac{\omega_1}{2})$		*dans* E^*	
z_0 *est* $\frac{\omega_1}{2}$*-strictement périodique*	*ssi*	z_0 *est strictement périodique, ou* $\frac{\omega_2^*}{2}$*-semi-périodique*	*pour n impair*
		z_0 *est* $\frac{\omega_2^*}{2}$*-semi-périodique*	*pour n pair*
z_0 *est* $\frac{\omega_1}{2}$*-semi-périodique*	*ssi*	z_0 *est* $\frac{\omega_1^*}{2}$*-semi-périodique, ou* $\frac{\omega_3^*}{2}$*-semi-périodique*	

la période $\frac{\omega_1}{2}$-stricte, ou la $\frac{\omega_1}{2}$-semi-période de z_0 dans $(E\,;\frac{\omega_1}{2})$ étant alors égale à la période stricte, ou la $\frac{\omega_k^*}{2}$-semi-période ($k = \{1,2,3\}$) de z_0 dans E^*.

Il ne nous reste plus, pour obtenir les décompositions des polynômes de Poncelet (théorème 2.6), qu'à traduire analytiquement ces équivalences en termes des fonctions de Weierstrass des deux courbes elliptiques E et E^* (voir le corollaire 5.9).

5.2 La fonction de Weierstrass sur le revêtement double

On détermine, à partir de la fonction de Weierstrass $\wp : \mathbb{C} \to \mathrm{P}^1\mathbb{C}$ de E, la fonction de Weierstrass $\wp^* : \mathbb{C} \to \mathrm{P}^1\mathbb{C}$ du revêtement $E^* \to (E;\frac{\omega_1}{2})$ que nous avons introduit dans le paragraphe précédent.

On conserve les notations du §3.1, et l'on note de même $\wp^* : \mathbb{C} \to \mathrm{P}^1\mathbb{C}$ la fonction de Weierstrass associée au réseau Λ^*, $e_i^* = \wp(\omega_i^*/2)$ et $(d_i^*)^2 = \prod_{k\neq i}(e_k^* - e_i^*)$ (pour $i \in \{1,2,3\}$).

Lemme 5.3 *Pour tout $z \in \mathbb{C}$:*

$$\begin{aligned}(\wp^*(z) - e_2^*)\,(\wp^*(z+\omega_2) - e_2^*) &= (e_1^* - e_2^*)\,(e_3^* - e_2^*)\\ \wp^*(z) + \wp^*(z+\omega_2) &= e_2^* + \wp(z)\\ \wp^*(z)\,\wp^*(z+\omega_2) &= e_2^*\,\wp(z) + (d_2^*)^2\,.\end{aligned}$$

Démonstration Pour les deux premières identités, observer que les fonctions de z définies par les membres de gauche de ces identités sont Λ-périodiques, et conclure en déterminant leurs pôles et le début de leur développement asymptotique en l'origine. La dernière s'en déduit immédiatement. □

Corollaire 5.4 *Pour $z, u \in \mathbb{C}$, on a*

$$(\wp^*(z) - \wp^*(u))\,(\wp^*(z) - \wp^*(u+\omega_2)) = (\wp^*(z) - e_2^*)\,(\wp(z) - \wp(u))\,.$$

Démonstration Fixons $z \in \mathbb{C}$, avec $z \not\equiv 0\,[\Lambda^*]$. L'expression

$$f_z : u \in \mathbb{C} \mapsto (\wp^*(z) - \wp^*(u))\,(\wp^*(z) - \wp^*(u+\omega_2)) \in \mathrm{P}^1\mathbb{C}$$

définit une fonction elliptique sur E qui a un unique pôle double en l'origine avec, d'après le lemme 5.3, développement asymptotique $f_z(u) = (e_2^* - \wp^*(z))\,(\frac{1}{u^2} + \mathcal{O}(1))$ en ce point. De plus f_z s'annule si et seulement si $u \equiv \pm z\,[\Lambda^*]$ ou $u \equiv \pm z + \omega_2\,[\Lambda^*]$, c'est-à dire lorsque $\wp(u) = \wp(z)$. □

Pour déterminer plus précisément $\wp^*$, nous utiliserons les fonctions de Jacobi relatives au réseau Λ. Rappelons le résultat classique suivant (voir par exemple [8]).

Lemme 5.5 *La fonction de Jacobi $f_i : \mathbb{C} \to \mathrm{P}^1\mathbb{C}$ ($i \in \{1,2,3\}$) est la racine carrée de $z \mapsto \wp(z) - e_i$ qui a pour développement asymptotique en l'origine $f_i(z) = 1/z + \mathcal{O}(1)$. Elle satisfait, pour tout $z \in \mathbb{C}$, $f_i(z+\omega_i) = f_i(z)$ et $f_i(z+\omega_k) = -f_i(z)$ pour $k \neq i$; c'est une fonction elliptique d'ordre 2 pour le réseau Λ_i.*

Corollaire 5.6 *Pour tout $z \in \mathbb{C}$, on a :*

$$\wp^*(z) - e_2^* = \frac{1}{4}\left((\wp(z) - e_2) + (\wp(z) - e_3) + 2f_2f_3(z)\right).$$

En particulier, $(d_2^*)^2 = (e_2 - e_3)^2/16$.

Démonstration On observe que le quotient f_2/f_3 est une fonction d'ordre 2 sur $\mathbb{C}/\Lambda^*$, qui satisfait pour $z \in \mathbb{C}$:

$$\frac{f_2}{f_3}(z) = -\frac{f_2}{f_3}(z+\omega_2), \quad \text{avec} \quad \frac{f_2}{f_3}(z) = 1 + \frac{1}{2}(e_3 - e_2)z^2 + \mathcal{O}(z^2) \ \text{ quand } z \to 0\,.$$

On en déduit que la fonction $H := \frac{1+f_2/f_3}{1-f_2/f_3}$ définit également une fonction d'ordre 2 sur $\mathbb{C}/\Lambda^*$ qui possède un pôle double en l'origine et un zéro double en $\omega_2 = \frac{\omega_2^*}{2}$, et est donc proportionnelle à $z \mapsto \wp^*(z) - e_2^*$; on conclut en examinant son développement en l'origine que

$$\wp^*(z) - e_2^* = \frac{e_2 - e_3}{4}\, H = \frac{1}{4}\,(f_3 + f_2)^2\,.$$

Le calcul de $(d_2^*)^2$ s'en déduit, puisque $f_2 f_3(\omega_1^*/2)$ et $f_2 f_3(\omega_3^*/2)$ sont opposés, de carrés égaux à $(e_1 - e_2)(e_1 - e_3)$. □

5.3 Factorisation sur une courbe avec un point d'ordre 2

> On exprime, à l'aide des fonctions de Weierstrass $\wp$ et $\wp^*$, les relations (que nous avons résumées dans le tableau 5.2) entre les notions de période et semi-période dans $(E; \frac{\omega_1}{2})$ d'une part, et dans E^* d'autre part(corollaire 5.9).

On introduit les valeurs prises par les fonctions de Weierstrass $\wp$ et $\wp^*$ sur les points périodiques et semi-périodiques (au sens de la définition 5.1) de $(E; \frac{\omega_1}{2})$ et de E^*.

Définition 5.7 *Soit $n \geq 3$; on note (comme dans la proposition 4.8) :*

$$\begin{array}{rrcl}
 & V_0[n] & = & \{\ \wp(u) \mid u \text{ de période } \frac{\omega_1}{2}\text{-stricte } n \text{ dans } E = \mathbb{C}/\Lambda\ \}\,, \\
 & V_1[n] & = & \{\ \wp(u) \mid u \text{ de } \frac{\omega_1}{2}\text{-semi-période } n \text{ dans } E = \mathbb{C}/\Lambda\ \}\,, \\
\textit{(pour } n \textit{ impair)} & V_0^*[n] & = & \{\ \wp^*(u) \mid u \text{ de période stricte } n \text{ dans } E^* = \mathbb{C}/\Lambda^*\ \}\,, \\
\textit{et, pour } k \in \{1,2,3\}\,, & V_k^*[n] & = & \{\ \wp^*(u) \mid u \text{ de } \frac{\omega_k^*}{2}\text{-semi-période } n \text{ dans } E^* = \mathbb{C}/\Lambda^*\ \}.
\end{array}$$

Lemme 5.8 *Pour tous $n \geq 3$, on a les égalités :*

$$\deg \varphi_n = 2 \operatorname{card} V_0[n] \quad \text{et} \quad \deg \psi_n = 2 \operatorname{card} V_1[n]$$

$$\begin{array}{rl}
\textit{avec, pour } n \textit{ impair et } k \in \{0,1,2,3\}\ : & \operatorname{card} V_1[n] = \operatorname{card} V_k^*[n] = \operatorname{card} V_0[n], \\
\textit{et pour } n \textit{ pair et } k \in \{1,2,3\}\ : & \operatorname{card} V_1[n] = \operatorname{card} V_k^*[n] = 2 \operatorname{card} V_0[n]\,.
\end{array}$$

On note $c(n)$ le cardinal de $V_0[n]$; il est pair.

N.B. Nous n'aurons pas besoin de la valeur exacte de $c(n)$.

Démonstration On désigne par $F_1[d]$ l'ensemble des $u \in E$ qui sont de $\frac{\omega_1}{2}$-semi-période d dans E (pour $d \in \mathbb{N}^*$). D'une part $E_1[n] = \{u \in E \mid nu \equiv \frac{\omega_1}{2}\,[\Lambda]\}$ est de cardinal n^2, et s'écrit comme réunion disjointe $\sqcup_{d|n,\ \frac{n}{d}\,\text{impair}} F_1[d]$; d'autre part le polynôme q_n est de degré n^2 et se décompose en produit $q_n = \prod_{d|n,\ \frac{n}{d}\,\text{impair}} \psi_d$. On en déduit que pour $d \geq 1$ on a $\deg \psi_d = \operatorname{card} F_1[d]$ et donc que, pour $d \geq 3$, $\deg \psi_d = 2 \operatorname{card} V_1[d]$.

On introduit de même, pour $d \in \mathbb{N}^*$, l'ensemble $F_0[d] \subset E$ des points qui sont de période $\frac{\omega_1}{2}$-stricte d dans E. Un raisonnement analogue au précédent (comparer la partition $E[n] = (\sqcup_{d|n} F_0[d]) \sqcup (\sqcup_{d|n,\ \frac{n}{d}\,\text{pair}} F_1[d])$ et la décomposition $p_n = (\prod_{d|n} \varphi_d)\,(\prod_{d|n,\ \frac{n}{d}\,\text{pair}} \psi_d)$) montre que pour $d \geq 1$ on a bien $\deg \varphi_d = \operatorname{card} F_0[d]$ et donc que, pour $d \geq 3$, on a $\deg \varphi_d = 2 \operatorname{card} V_0[d]$.

Observons enfin que, pour chaque entier n, les cardinaux des $V_k^*[n]$ (pour $k \in \{1,2,3\}$) sont égaux. Lorsque n est impair, on a de plus $\operatorname{card} V_2^*[n] = \operatorname{card} V_0^*[n]$ (dans ce cas, $(u+\Lambda^*) \in E^*$ est en effet de période n dans E^* si et seulement si $(u+\omega_2+\Lambda^*)$ est de $\frac{\omega_2^*}{2}$-semi-période n dans E^*). Le reste du lemme est donc conséquence de la propriété 5.2, et de ce que $\varphi_n, \psi_n \in \mathbb{Z}[x^4, y^4, z^4]$ ($n \geq 3$). □

Corollaire 5.9 *Soit $z_0 \in \mathbb{C}$. On se donne des nombres complexes $\mathbf{x}_1$, $\mathbf{y}_1$, $\mathbf{z}_1$ et $\mathbf{x}_k^*$, $\mathbf{y}_k^*$, $\mathbf{z}_k^*$ (pour $k \in \{1,2,3\}$) dont les puissances quatrièmes satisfont :*

$$(\mathbf{x}_1)^4 = (d_1)^2\,, \qquad (\mathbf{y}_1)^4 = (\wp(z_0)-e_1)^2\,, \qquad (\mathbf{z}_1)^4 = 4\prod_{j\neq 1}(\wp(z_0)-e_j)$$
$$(\mathbf{x}_k^*)^4 = (d_k^*)^2\,, \qquad (\mathbf{y}_k^*)^4 = (\wp^*(z_0)-e_k^*)^2\,, \qquad (\mathbf{z}_k^*)^4 = 4\prod_{j\neq k}(\wp^*(z_0)-e_j^*)\,.$$

Alors
$$\begin{array}{rrcll} & (\mathbf{y}_2^*)^{2c(n)}\,.\,\varphi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) & = & \varphi_n(\mathbf{x}_2^*,\mathbf{y}_2^*,\mathbf{z}_2^*)\,.\,\psi_n(\mathbf{x}_2^*,\mathbf{y}_2^*,\mathbf{z}_2^*) & \textit{pour } n \textit{ impair} \\ \gamma_n & (\mathbf{y}_2^*)^{2c(n)}\,.\,\varphi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) & = & \psi_n(\mathbf{x}_2^*,\mathbf{y}_2^*,\mathbf{z}_2^*) & \textit{pour } n \textit{ pair} \end{array}$$

$$\begin{array}{rrcll} & (\mathbf{y}_2^*)^{2c(n)}\,.\,\psi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) & = & \psi_n(\mathbf{x}_1^*,\mathbf{y}_1^*,\mathbf{z}_1^*)\,.\,\psi_n(\mathbf{x}_3^*,\mathbf{y}_3^*,\mathbf{z}_3^*) & \textit{pour } n \textit{ impair} \\ \textit{et} & (\mathbf{y}_2^*)^{4c(n)}\,.\,\psi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) & = & \psi_n(\mathbf{x}_1^*,\mathbf{y}_1^*,\mathbf{z}_1^*)\,.\,\psi_n(\mathbf{x}_3^*,\mathbf{y}_3^*,\mathbf{z}_3^*) & \textit{pour } n \textit{ pair.} \end{array}$$

Démonstration Les identités (un peu rébarbatives) que nous voulons démontrer ne font en fait que traduire les équivalences géométriques du tableau 5.2, chaque paquet de variables $(\mathbf{x}_k^*, \mathbf{y}_k^*, \mathbf{z}_k^*)$ correspondant au choix du point (d'ordre 2) $\frac{\omega_k^*}{2}$ dans E^* ($k \in \{1,2,3\}$).

D'après la proposition 4.8, on a en effet pour $n \geq 3$, $m \geq 1$ et $k \in \{1,2,3\}$:

$$\varphi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) = \gamma_n \prod_{\alpha\in V_0[n]}(\wp(z_0)-\alpha)\,, \qquad \psi_n(\mathbf{x}_1,\mathbf{y}_1,\mathbf{z}_1) = \prod_{\beta\in V_1[n]}(\wp(z_0)-\beta)\,,$$
$$\varphi_{2m+1}(\mathbf{x}_2^*,\mathbf{y}_2^*,\mathbf{z}_2^*) = \gamma_{2m+1}\prod_{\alpha^*\in V_0^*[2m+1]}(\wp^*(z_0)-\alpha^*)\,,\ \psi_n(\mathbf{x}_k^*,\mathbf{y}_k^*,\mathbf{z}_k^*) = \prod_{\beta^*\in V_k^*[n]}(\wp^*(z_0)-\beta^*)$$

(noter, pour le calcul de $\varphi_{2m+1}(\mathbf{x}_2^*,\mathbf{y}_2^*,\mathbf{z}_2^*)$, que si $nz_0 \equiv 0\,[\Lambda^*]$ pour un premier entier impair $n = 2m+1$, alors $(z_0+\Lambda^*)$ est strictement périodique dans E^*).

Supposons par exemple n impair. Pour montrer la première des identités de 5.9, il nous faut donc comparer les produits

$$\prod_{\alpha\in V_0[n]}(\wp(z_0)-\alpha) \quad \text{et} \quad \prod_{\alpha^*\in V_0^*[n]}(\wp^*(z_0)-\alpha^*)\prod_{\beta^*\in V_2^*[n]}(\wp^*(z_0)-\beta^*)\,.$$

Soit $u \in \mathbb{C}$. Puisque n est impair, on a $\alpha^* := \wp^*(u) \in V_0^*[n]$ ssi $\beta^* := \wp^*(u+\omega_2) \in V_2^*[n]$; on peut alors regrouper les deux termes correspondant respectivement à α^* et β^* dans l'expression de droite pour obtenir, d'après le corollaire 5.4 :

$$(\wp^*(z_0)-\alpha^*)\,(\wp^*(z_0)-\beta^*) = (\wp^*(z_0)-e_2^*)\,(\wp(z_0)-\alpha)\,,$$

avec $\alpha := \wp(u) \in V_0[n]$. On conclut avec le lemme 5.8, puisque $c(n) = \operatorname{card} V_0[n]$ facteurs $(\wp^*(z_0) - e_2^*)$ vont ainsi apparaître.

Démonstration analogue pour les autres identités. □

5.4 Factorisation des polynômes de Poncelet

L'objet de ce paragraphe est d'obtenir les décompositions des polynômes de Poncelet Φ_{2m+1} et Ψ_n annoncées dans le théorème 2.6. Pour cela, il suffit d'appliquer les résultats du §5.3 à la courbe elliptique avec point d'ordre 2 associée à chaque configuration de Poncelet.

Soit $(F;\sigma)$ la courbe de Poncelet de paramètres (a,R,r). On considère $(E;\frac{\omega_1}{2})$ la courbe elliptique munie d'un point d'ordre 2 associée (proposition 3.3), E^* son revêtement à deux feuillets, et $z_0 \in \mathbb{C}^*$ correspondant à la transformation de Poncelet.

Proposition 5.10 *On peut choisir e_1^* et e_3^*, c'est-à-dire numéroter les points d'ordre 2 de E^*, de sorte que*

$$e_1^* = \frac{-a^2 - R^2 + r^2 + 6aR}{12\,R^2}\,,\ e_2^* = \frac{a^2 + R^2 - r^2}{6\,R^2}\,,\ e_3^* = \frac{-a^2 - R^2 + r^2 - 6aR}{12\,R^2}\,. \tag{24}$$

De plus, quitte à remplacer $z_0 \in \mathbb{C}$ par $z_0 + \omega_2 \in \mathbb{C}$, on peut supposer que :

$$\wp^*(z_0) - e_2^* = \frac{1}{4\,R^2}\,(R + r + a)(R + r - a)\,. \tag{25}$$

Démonstration Petit calcul, en utilisant le corollaire 5.6 et la proposition 3.3.

Rappelons que $\frac{\omega_1^*}{2} + \Lambda^*$ et $\frac{\omega_3^*}{2} + \Lambda^*$ sont les deux relèvements à E^* du point $\frac{\omega_1}{2} + \Lambda \in E$. De même, les points $z_0 \in \mathbb{C}$ et $z_0' := z_0 + \omega_2 \in \mathbb{C}$ fournissent les deux relèvements à E^*, soient $(z_0 + \Lambda^*)$ et $(z_0' + \Lambda^*) \in E^*$, du point $(z_0 + \Lambda) \in E$. On a :

$$\wp^*(z_0') - e_2^* = \frac{1}{4\,R^2}\,(R - r + a)(R - r - a)\,.$$

□

Corollaire 5.11 • *Il existe des polynômes $\Phi_{2n+1,0}, \Phi_{2n+1,2}$ et $\Phi_{m,1}, \Phi_{m,3}$ dans $\mathbb{Z}[a,R,r]$ ($n \geq 1$ et $m \geq 2$), avec $\deg \Phi_{2n+1,0} = \deg \Phi_{2n+1,2}$ et $\deg \Phi_{m,1} = \deg \Phi_{m,3}$, et tels que :*

$$\begin{aligned} \Phi_{2n+1}(a,R,r) &= \Phi_{2n+1,0}(a,R,r)\ \Phi_{2n+1,2}(a,R,r) \\ \Psi_m(a,R,r) &= \Phi_{m,1}(a,R,r)\ \Phi_{m,3}(a,R,r)\,. \end{aligned}$$

• *De plus, ces polynômes vérifient les relations suivantes (pour un signe dépendant de n) :*

$$\begin{aligned} \Phi_{2n+1,0}(a,R,r) &= \Phi_{2n+1,0}(-a,R,r) &&= \pm\Phi_{2n+1,2}(a,R,-r) = \pm\Phi_{2n+1,2}(a,-R,r) \\ \Phi_{2n+1,1}(a,R,r) &= \Phi_{2n+1,1}(a,-R,r) &&= \Phi_{2n+1,3}(-a,R,r) = \Phi_{2n+1,3}(a,R,-r) \\ \Phi_{2n,1}(a,R,r) &= \Phi_{2n,1}(a,R,-r) &&= \Phi_{2n,3}(-a,R,r) = \Phi_{2n,3}(a,-R,r)\,. \end{aligned}$$

Démonstration Les décompositions annoncées s'obtiennent en appliquant le corollaire 5.9 à la courbe elliptique avec point d'ordre 2 associée à chaque configuration de Poncelet.

On mène ci-dessous les calculs explicites, pour vérifier que les expressions obtenues sont effectivement polynomiales en (a,R,r), et pour mettre en évidence les symétries annoncées. La fin de ce paragraphe peut donc être omise en première lecture.

Notation Lorsque $p \in \mathbb{Z}[x^4,y^4,z^4]$, on définit $\widehat{p} \in \mathbb{Z}[x,y,z]$ par $p(x,y,z) = \widehat{p}(x^4,y^4,z^4)$.

En utilisant les valeurs des e_k^* et de $\wp^*(z_0)$ données dans la proposition 5.10, on détermine les valeurs des paramètres intervenant dans le corollaire 5.9. Les polynômes considérés étant tous homogènes, on est alors amenés à renormaliser et à introduire les variables :

$$\begin{array}{rrr} X_2 = (R-r+a)\,(R-r-a) & Y_2 = (R+r+a)\,(R+r-a) & Z_2 = 16\,R^2 \\ X_1 = -a\,(R-r-a) & Y_1 = R\,(R+r-a) & Z_1 = 2\,(R+r+a)^2 \\ X_3 = a\,(R-r+a) & Y_3 = R\,(R+r+a) & Z_3 = 2\,(R+r-a)^2\,, \end{array}$$

ce qui permet de réécrire les identités du corollaire 5.9 sous la forme :

$$\begin{array}{rrcl} \text{pour } n \text{ impair :} & (4R)^{c(n)}\ \Phi_n(a,R,r) & = & \widehat{\varphi}_n(X_2,Y_2,Z_2)\ \widehat{\psi}_n(X_2,Y_2,Z_2) \\ & (Y_2)^{c(n)/2}\ \Psi_n(a,R,r) & = & \widehat{\psi}_n(X_1,Y_1,Z_1)\ \widehat{\psi}_n(X_3,Y_3,Z_3)\,, \\ \text{et pour } n \text{ pair :} & (Y_2)^{c(n)}\ \Psi_n(a,R,r) & = & \widehat{\psi}_n(X_1,Y_1,Z_1)\ \widehat{\psi}_n(X_3,Y_3,Z_3)\,. \end{array} \quad (26)$$

Intéressons-nous alors pour commencer à la décomposition de Φ_n pour n impair. D'après le lemme 4.6, il existe un signe $\varepsilon(n) = \pm 1$ tel que $\varphi_n(x,y,z) = \varepsilon(n)\ \psi_n(y,x,z)$. En particulier la première des identités (26) peut se réécrire

$$(4R)^{c(n)}\ \Phi_n(a,R,r) = \varepsilon(n)\ \widehat{\varphi}_n(X_2,Y_2,Z_2)\ \widehat{\varphi}_n(Y_2,X_2,Z_2)\,,$$

d'où la décomposition et les symétries annoncées (voir également le lemme 5.12).

Passons aux polynômes Ψ_n. On observe que les paquets de variables (X_1,Y_1,Z_1) et (X_3,Y_3,Z_3) sont échangés lorsqu'on remplace a par $-a$; on en déduit la décomposition cherchée, et le fait que les polynômes satisfont la relation $\Phi_{n,1}(a,R,r) = \Phi_{n,3}(-a,r,R)$.

Il reste à comprendre les autres symétries ; celles correspondant à $r \mapsto -r$ seront conséquence du lemme suivant, et celles correspondant à $R \mapsto -R$ s'en déduiront, les variables (X_k,Y_k,Z_k) $(k \in \{1,2,3\})$ étant inchangées par la transformation par $(a,R,r) \mapsto (-a,-R,-r)$. □

Lemme 5.12 *Notons X_k', Y_k' et Z_k' ($k \in \{1,2,3\}$) les quantités obtenues à partir des X_k, Y_k et Z_k ci-dessus en remplaçant r par $-r$ (c'est-à-dire z_0 par z_0') ; on a alors :*

$$\begin{array}{rrcl} \textit{pour } n \textit{ pair :} & (R-r+a)^{c(n)}\ \widehat{\psi}_n(X_1,Y_1,Z_1) & = & (R+r+a)^{c(n)}\ \widehat{\psi}_n(X_1',Y_1',Z_1')\,, \\ & (R-r-a)^{c(n)}\ \widehat{\psi}_n(X_3,Y_3,Z_3) & = & (R+r-a)^{c(n)}\ \widehat{\psi}_n(X_3',Y_3',Z_3')\,; \end{array}$$

$$\begin{array}{rrcl} \textit{pour } n \textit{ impair :} & \widehat{\phi_n}(X_2,Y_2,Z_2) & = & \widehat{\psi}_n(X_2',Y_2',Z_2')\,, \\ \textit{et} & (R-r-a)^{c(n)/2}\ \widehat{\psi}_n(X_1,Y_1,Z_1) & = & (R+r+a)^{c(n)/2}\ \widehat{\psi}_n(X_3',Y_3',Z_3')\,. \end{array}$$

Démonstration Lorsqu'on change r en $-r$, on ne change pas de courbe elliptique $(E; \frac{\omega_1}{2})$, mais on remplace le point $(z_0 + \Lambda^*) \in E^*$ par $(z_0' + \Lambda^*) = (z_0 + \frac{\omega_2^*}{2} + \Lambda^*) \in E^*$ (tous deux au-dessus du même point de E, voir la proposition 5.10).

Démontrons par exemple la première de ces identités ; elle reflète le fait que, puisque n est pair, le point $(z_0+\Lambda^*) \in E^*$ est $\frac{\omega_1^*}{2}$-semi-périodique de $\frac{\omega_1^*}{2}$-semi-période n ssi $(z_0'+\Lambda^*) \in E^*$ l'est, ce qui correspond à l'annulation simultanée de $\widehat{\psi}_n(X_1, Y_1, Z_1)$ et de $\widehat{\psi}_n(X_1', Y_1', Z_1')$. D'après le corollaire 5.9, et par homogénéité de $\widehat{\psi}_n$, on a :

$$(4R^3)^{c(n)} \prod_{\beta^* \in V_1^*[n]} (\wp^*(z_0) - \beta^*) = (R + r - a)^{c(n)} \ \widehat{\psi}_n(X_1, Y_1, Z_1),$$
$$(4R^3)^{c(n)} \prod_{\beta^* \in V_1^*[n]} (\wp^*(z_0 + \tfrac{\omega_2^*}{2}) - \beta^*) = (R - r - a)^{c(n)} \ \widehat{\psi}_n(X_1', Y_1', Z_1').$$

La première identité du lemme 5.3 fournit, pour tout $u \in \mathbb{C}$, la relation :

$$(\wp^*(z_0) - \wp^*(u + \tfrac{\omega_2^*}{2}))\ (e_2^* - \wp^*(u)) = (\wp^*(z_0) - e_2^*)\ (\wp^*(z_0 + \tfrac{\omega_2^*}{2}) - \wp^*(u))\,,$$

d'où

$$\prod_{\beta^* \in V_1^*[n]} (\wp^*(z_0) - \beta^*) \prod_{\beta^* \in V_1^*[n]} (e_2^* - \beta^*) = (\wp^*(z_0) - e_2^*)^{2c(n)} \prod_{\beta^* \in V_1^*[n]} (\wp^*(z_0') - \beta^*)\,;$$

on conclut, puisqu'en appliquant cette fois le corollaire 5.9 au point $z_1 := \frac{\omega_2^*}{2} \in \mathbb{C}/\Lambda^*$ on obtient :

$$\prod_{\beta^* \in V_1^*[n]} (e_2^* - \beta^*) = \prod_{\beta^* \in V_1^*[n]} (\wp^*(z_1) - \beta^*) = \widehat{\psi}_n((d_1^*)^2, (e_2^* - e_1^*)^2, 0) = (d_2^*)^{c(n)}$$

(la dernière de ces égalités vient du lemme 4.6). □

6 Irréductibilité

Nous achevons la preuve du théorème 2.6, en montrant que les polynômes $\Phi_{n,k}$ ($k \in \{0, 1, 2, 3\}$) qui y interviennent sont tous irréductibles dans $\mathbb{C}[a, R, r]$.

6.1 Configurations de Poncelet, et courbes elliptiques avec structures de niveau 2

Dans ce paragraphe nous associons, à chaque configuration de Poncelet $[a, R, r]$, une courbe elliptique (E^*, Γ) avec une structure de niveau 2, ainsi qu'une paire de points opposés distincts $\pm z_0$ de E^*. Nous montrons que cette application induit une bijection biholomorphe entre l'espace des configurations de Poncelet, et l'espace des modules de tels triplets $(E, \Gamma^*, \pm z_0)$. Cette bijection sera le point clé pour démontrer l'irréductibilité des polynômes $\Phi_{n,k}$.

Rappelons qu'une courbe elliptique avec une structure de niveau 2, soit (E,Γ), est la donnée d'une courbe elliptique $E=\mathbb{C}/\Lambda$, et d'une numérotation des trois points d'ordre 2 de E. On désignera par $\mathcal{E}$ l'ensemble $\{(E,\Gamma,\pm z)\}$, où (E,Γ) est une courbe elliptique avec une structure de niveau 2, et $\pm z$ est une paire de points opposés, et distincts, de E.

La donnée d'un élément $(E,\Gamma,\pm z)\in\mathcal{E}$ équivaut à la donnée $(e_1,e_2,e_3;\wp(z))\in\mathbb{C}^4$ des valeurs prises par la fonction de Weierstrass aux points d'ordre 2 et en $\pm z$, assujetties aux conditions $e_j\neq e_k$ (si $j\neq k$), $e_1+e_2+e_3=0$ et $\wp(z)-e_k\neq 0$ $(k\in\{1,2,3\})$; on désignera par $W\subset\mathbb{C}^4$ l'ensemble ainsi défini.

On dira que deux éléments $e=(E,\Gamma,\pm z)$ et $e'=(E',\Gamma',\pm z')$ de $\mathcal{E}$ sont équivalents, soit $e\sim e'$, lorsqu'il existe un isomorphisme de courbes elliptiques $i:E\to E'$ envoyant Γ sur Γ' et $\pm z$ sur $\pm z'$ (un tel isomorphisme est alors défini à $\pm\mathrm{Id}$ près). Notons

$$V=\{(\lambda,\mu)\in\mathbb{C}^2\mid \lambda\neq\pm2\,,\ \mu\neq0\,,\ \lambda+\mu\neq\pm2\}\,.$$

Lemme 6.1 *L'application*

$$(e_1,e_2,e_3;\wp(z))\in W\subset\mathbb{C}^4\mapsto\Big(\frac{6\,e_2}{2e_1+e_2},4\,\frac{\wp(z)-e_2}{2e_1+e_2}\Big)\in\mathbb{C}^2$$

induit un biholomorphisme de $\mathcal{E}/_\sim$ sur V.

Démonstration L'espace $\mathcal{E}/_\sim$ possède une structure naturelle de variété complexe lisse. En effet le quotient de $\{M\in\mathrm{Sl}_2\mathbb{Z}\mid M\equiv\mathrm{Id}\,[2]\}$ par $\pm Id$ agit librement et proprement sur le demi-plan supérieur $\mathbb{H}$; de plus, à courbe elliptique fixée, les couples $\pm z$ de points opposés distincts sont paramétrés par les valeurs non stationnaires de la fonction de Weierstrass $\wp$.

Soit $(E,\Gamma,\pm z)\in\mathcal{E}$, correspondant aux valeurs $(e_1,e_2,e_3;\wp(z))$ de $\wp$. On observe que $2\,e_1+e_2\neq0$ (puisque $e_1\neq e_3$), et $\lambda:=\frac{6\,e_2}{2e_1+e_2}\neq\pm2$ (puisque $e_2\neq e_1,e_3$). Soit alors $\mu:=4\,\frac{\wp(z)-e_2}{2e_1+e_2}$. Les conditions $\wp(z)\neq e_2$ et $\wp(z)\neq e_1,e_3$ se traduisent respectivement par $\mu\neq0$ et $\mu\neq\pm2$. L'application définie ci-dessus induit une bijection de $\mathcal{E}/_\sim$ sur V, puisque deux éléments de $\mathcal{E}$ sont équivalents si et seulement s'ils sont associés à des quadruplets $(e_1,e_2,e_3;\wp(z))$ proportionnels. Cette bijection $\mathcal{E}/_\sim\ \to V$ est clairement biholomorphe. □

Introduisons alors l'ensemble des configurations de Poncelet, éventuellement dégénérées lorsque $r=0$, soit

$$\mathbf{U}=\{[a,R,r]\in\mathrm{P}^2\mathbb{C}\mid a,R\in\mathbb{C}^*\,,\ r\in\mathbb{C}\,,\ a\pm R\pm r\neq0\}\,.$$

Rappelons (voir la proposition 5.10) que nous avons associé, à chaque configuration de Poncelet $[a,R,r]\in\mathbf{U}$, un triplet $(E^*,\Gamma^*,\pm z_0)\in\mathcal{E}$ correspondant aux valeurs :

$$e_1^*=\frac{-a^2-R^2+r^2+6aR}{12\,R^2}\,,\ e_2^*=\frac{a^2+R^2-r^2}{6\,R^2}\,,\ e_3^*=\frac{-a^2-R^2+r^2-6aR}{12\,R^2}\,,$$

$$\text{et}\qquad \wp^*(z_0)-e_2^*=\frac{1}{4\,R^2}\,(R+r+a)(R+r-a)\,.$$

Proposition 6.2 *L'application* $\mathbf{U} \xrightarrow{f} \mathcal{E}$ *que l'on vient de définir induit une bijection biholomorphe de* $\mathbf{U}$ *sur* $\mathcal{E}/_\sim$.

Démonstration La configuration de Poncelet associée à $[a, R, r] \in \mathbf{U}$ s'envoie sur le point de $\mathcal{E}/_\sim$ associé à $(\lambda, \mu) \in V$ (lemme 6.1) si et seulement si le triplet (a, R, r) est solution du système

$$\left\{ \begin{array}{rcl} R^2 + a^2 - r^2 & = & \lambda\, aR \\ (R+r)^2 - a^2 & = & \mu\, aR. \end{array} \right.$$

Les deux polynômes correspondants n'ont pas de facteur commun, donc ce système admet au plus quatre solutions dans $\mathrm{P}^2\mathbb{C}$. On cherche déjà les solutions pour lesquelles $aR = 0$: les trois points $[1, 0, \pm 1]$ et $[0, 1, -1]$ sont solutions mais n'appartiennent pas à $\mathbf{U}$. Il reste une dernière solution, pour laquelle $aR \neq 0$, et qui est définie par les conditions

$$R + r = \frac{\lambda + \mu}{2}\, a\,, \quad \Big(\big(\frac{\lambda + \mu}{2}\big)^2 - 1 \Big)\, a = \mu R\,.$$

Celle-ci satisfait $a \pm R \pm r \neq 0$ et appartient donc à $\mathbf{U}$; on vérifie en effet facilement que pour $[a, R, r] \in \mathrm{P}^2\mathbb{C}$ avec $R \neq 0$, le produit $(e_1^* - e_2^*)^2 (e_1^* - e_3^*)^2 (e_2^* - e_3^*)^2$ est proportionnel à

$$\frac{a^2\,(R + r + a)^2\,(R + r - a)^2\,(R - r + a)^2\,(R - r - a)^2}{R^{10}}\,.$$

□

6.2 Irréductibilité des polynômes $\Phi_{n,k}$

> Soit $\Phi \in \mathbb{C}[a, R, r]$ l'un de ces polynômes ; on considère sa décomposition en produit de facteurs irréductibles, soit $\Phi = \prod_{i=1}^{\ell} H_i^{m_i}$, avec $H_i \in \mathbb{C}[a, R, r]$ irréductibles distincts et $m_i \in \mathbb{N}^*$. Nous montrerons d'abord qu'un seul facteur intervient dans cette décomposition, c'est-à-dire que $\Phi = H^m$ est une puissance d'un polynôme irréductible ; ce sera le cas si la courbe $Z_\Phi := \{\Phi = 0\} \subset \mathrm{P}^2\mathbb{C}$ est irréductible, ou de façon équivalente si Z_Φ est connexe par arcs réguliers. On conclura ensuite que Φ est irréductible, en montrant que $\deg H = \deg \Phi$.

Pour $n \geq 3$ et $k \in \{0, 1, 2, 3\}$ (et lorsque les polynômes correspondants sont bien définis, selon la parité de n), on note

$$Z_{n,k} = \{\Phi_{n,k} = 0\} \subset \mathrm{P}^2\mathbb{C}\,, \text{ et} \qquad Z'_{n,k} = Z_{n,k} \cap \mathbf{U}\,.$$

Par construction, la courbe $Z'_{n,k}$ (soit $Z_{n,k}$ privée d'un nombre fini de points) correspond aux configurations de Poncelet $[a, R, r] \in \mathbf{U}$ pour lesquelles le point $(z_0 + \Lambda^*) \in \mathbb{C}/\Lambda^*$, qu'on a choisi pour relever à $E^* = \mathbb{C}/\Lambda^*$ la transformation de Poncelet, est de période (lorsque $k = 0$) ou de $\frac{\omega_k^*}{2}$-semi-période (lorsque $k \in \{1, 2, 3\}$) égale à n (voir le corollaire 5.11).

Fixons $k \in \{0,1,2,3\}$, et introduisons alors $\mathcal{E}_{n,k} \subset \mathcal{E}$ l'ensemble des triplets $(E, \Gamma, \pm z)$, avec $\Gamma = (\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2})$, et pour lesquels les points $\pm z \in E$ sont de période (lorsque $k = 0$) ou de $\frac{\omega_k}{2}$-semi-période (lorsque $k \in \{1,2,3\}$) égale à n. La bijection $f : \mathbf{U} \to \mathcal{E}/_\sim$ de la proposition 6.2 induit des bijections holomorphes $f_{n,k} : Z'_{n,k} \to \mathcal{E}_{n,k}/_\sim$ entre ces courbes. On veut montrer que $Z'_{n,k}$ est connexe par arcs lisses ; on commence donc par s'intéresser à $\mathcal{E}_{n,k}$.

Lemme 6.3 *Soient $\Lambda = \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2$ un réseau de $\mathbb{C}$ et (E, Γ) la courbe elliptique avec structure de niveau 2 définie par $E = \mathbb{C}/\Lambda$ et $\Gamma = (\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2})$. Soit $z \in \mathbb{C}$.*

(i) On suppose n impair. Si $(z + \Lambda) \in E$ est strictement périodique dans E, de période stricte n, il existe une $\mathbb{Z}$-base (ω'_1, ω'_2) de Λ pour laquelle $\Gamma = (\frac{\omega'_1}{2}, \frac{\omega'_2}{2}, \frac{\omega'_1+\omega'_2}{2})$ et $z \equiv \frac{\omega'_1}{n}\,[\Lambda]$.

(ii) L'entier n est quelconque. Si $(z + \Lambda) \in E$ est $\frac{\omega_k}{2}$-semi-périodique pour un $k \in \{1,2,3\}$, de $\frac{\omega_k}{2}$-semi-période n dans E, il existe une $\mathbb{Z}$-base (ω'_1, ω'_2) de Λ pour laquelle on aura $\Gamma = (\frac{\omega'_1}{2}, \frac{\omega'_2}{2}, \frac{\omega'_1+\omega'_2}{2})$, et $z \equiv \frac{\omega'_k}{2n}\,[\Lambda]$ (avec $\omega'_3 := \omega'_1 + \omega'_2$).

Démonstration C'est un résultat classique.

(i) Le point $z = x\,\omega_1 + y\,\omega_2$ est de période n dans $\mathbb{C}/\Lambda$ si et seulement si $x = \frac{a}{n}$ et $y = \frac{b}{n}$ avec $a, b \in \mathbb{Z}$ et $\mathrm{pgcd}\,(a, b, n) = 1$. Il existe alors une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2\mathbb{Z}$ telle que $\det A \equiv 1\,[n]$.

Rappelons alors (voir par exemple [16] ex. 1.2.2) que, pour tout entier $m \in \mathbb{N}^*$, le morphisme naturel $\mathrm{Sl}_2(\mathbb{Z}) \to \mathrm{Sl}_2(\mathbb{Z}/m\mathbb{Z})$ est surjectif. Nous utiliserons ici ce fait pour l'entier $m = 2n$. De plus, puisque n est ici supposé impair, le lemme chinois assure que le morphisme d'anneaux

$$\mathrm{M}_2(\mathbb{Z}/2n\mathbb{Z}) \xrightarrow{\ g\ } \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$$

est bijectif. Ce même lemme chinois assure alors que g induit une bijection

$$\mathrm{Sl}_2(\mathbb{Z}/2n\mathbb{Z}) \longrightarrow \mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{Sl}_2(\mathbb{Z}/2\mathbb{Z}),$$

et donc qu'il existe une matrice $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sl}_2\mathbb{Z}$ telle que $M \equiv A\,[n]$ et $M \equiv \mathrm{Id}\,[2]$. Le résultat en découle, en prenant $\omega'_1 = \alpha\omega_1 + \beta\omega_2$ et $\omega'_2 = \gamma\omega_1 + \delta\omega_2$.

(ii) Le point $z = x\,\omega_1 + y\,\omega_2$ est de semi-période n dans $\mathbb{C}/\Lambda$ si et seulement $x = \frac{a}{2n}$ et $y = \frac{b}{2n}$ avec $a, b \in \mathbb{Z}$ et $\mathrm{pgcd}\,(a, b, 2n) = 1$. Il existe donc, comme ci-dessus, une matrice $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sl}_2\mathbb{Z}$ avec $a \equiv \alpha\,[2n]$ et $b \equiv \beta\,[2n]$. On obtient la base cherchée en choisissant convenablement ω'_1 et ω'_2 parmi les trois vecteurs $\alpha\,\omega_1 + \beta\omega_2$, $\gamma\,\omega_1 + \delta\,\omega_2$ et $(\alpha + \gamma)\,\omega_1 + (\beta + \delta)\omega_2$. □

Proposition 6.4 *Les courbes $\mathcal{E}_{n,k}/_\sim$ (n quelconque, $k \in \{1,2,3\}$) et $\mathcal{E}_{n,0}/_\sim$ (n impair) sont connexes par arcs lisses, et les polynômes $\Phi_{n,k}$ correspondants possèdent chacun un unique facteur irréductible (éventuellement multiple).*

Démonstration On suppose n impair, et l'on veut montrer que $\mathcal{E}_{n,0}/_\sim$ est connexe par arcs lisses. On choisit un point de référence $e_0 = (E_0, \Gamma_0, \pm z_0) \in \mathcal{E}_{n,0}$, avec $E_0 = \mathbb{C}/\Lambda_0$, qui correspond à un point lisse dans le quotient $\mathcal{E}_{n,0}/_\sim$. Soit $e = (E, \Gamma, \pm z)$ un autre point de $\mathcal{E}_{n,0}$, avec $E = \mathbb{C}/\Lambda$. D'après le lemme 6.3, il existe une matrice $M \in \mathrm{Gl}_2^+\mathbb{R}$ qui envoie Λ_0 sur Λ, Γ_0 sur Γ et $(\pm z_0 + \Lambda_0)$ sur $(\pm z + \Lambda)$. Un arc lisse $t \in [0,1] \to M(t) \in \mathrm{Gl}_2^+\mathbb{R}$, transverse à l'action par translation à gauche des similitudes directes, et avec $M(0) = \mathrm{Id}$ et $M(1) = M$, fournira par projection un arc lisse tracée sur $\mathcal{E}_{n,0}/_\sim$ et joignant les points qui correspondent à e_0 et e dans ce quotient. On en déduit, avec la bijection $f_{n,0} : Z'_{n,0} \to \mathcal{E}_{n,0}/_\sim$, que $Z'_{n,0} \subset \mathrm{P}^2\mathbb{C}$ (et donc $Z_{n,0}$) sont également connexes par arcs lisses, d'où le fait que $\Phi_{n,0}$ est puissance d'un polynôme irréductible.

Raisonnement analogue pour les courbes $\mathcal{E}_{n,k}/_\sim$ (pour n quelconque et $k \in \{1,2,3\}$) en utilisant cette fois la seconde partie du lemme 6.3. □

Corollaire 6.5 *Chacun des polynômes $\Phi_{n,k}$ est irréductible dans $\mathbb{C}[a,R,r]$.*

Démonstration On vient de montrer que chaque polynôme $\Phi_{n,k}$ est une puissance d'un polynôme irréductible ; il reste à montrer que ce facteur irréductible a multiplicité 1.

D'après la proposition 6.2, l'ensemble $\{[a,R,r] \in \mathbf{U} \mid R^2 + a^2 - r^2 = 0\}$ est formé de toutes les configurations de Poncelet pour lesquelles la courbe elliptique avec structure d'ordre 2 associée (E^*, Γ^*) est isomorphe à la courbe elliptique avec structure de niveau 2 modèle $\varepsilon_0 = \big(\mathbb{C}/(\mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot i); (\frac{1}{2}, \frac{1+i}{2}, \frac{i}{2})\big)$ (c'est-à-dire que E^* est associée à un réseau carré, avec $e_2^* = 0$ et $e_1^* + e_3^* = 0$).

Pour $n \geq 3$ et $k \in \{0,1,2,3\}$, chacun des ensembles

$$A_{n,k} := \{[a,R,r] \in \mathbf{U} \mid R^2 + a^2 - r^2 = 0\ ,\ \Phi_{n,k}(a,R,r) = 0\}$$

est alors en bijection avec l'ensemble des points de $\mathbb{C}/(\mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot i)$ qui sont strictement périodiques de période stricte n (pour $k = 0$), ou $\frac{\omega_k^*}{2}$-semi-périodiques, de semi-période n (pour $k \in \{1,2,3\}$) dans $\varepsilon_0 = \big(\mathbb{C}/(\mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot i); (\frac{1}{2}, \frac{1+i}{2}, \frac{i}{2})\big)$.

Supposons n impair et $k = 0$ ou 2. On a alors $\operatorname{card} A_{n,k} = c(n)$ (voir le lemme 5.8), tandis que $A_{n,k}$ est défini par deux conditions polynomiales, l'une de degré 2, l'autre de degré $\deg \Phi_{n,k} = \frac{c(n)}{2}$. On conclut avec le théorème de Bezout que le polynôme $\Phi_{n,k}$ ne contient pas de facteurs carrés, et est donc irréductible d'après la proposition 6.4.

Lorsque n est pair, et que $k = 2$, on reprend le même raisonnement avec dans ce cas $\operatorname{card} A_{n,2} = \operatorname{card} V_2^*[n] = 2\,c(n)$ et $\deg \Phi_{n,2} = c(n)$.

De même pour les polynômes $\Phi_{n,1}$ et $\Phi_{n,3}$, puisque pour tout $n \geq 3$, on a l'égalité $\deg \Phi_{n,1} = \deg \Phi_{n,3} = \frac{1}{2} \operatorname{card} V_1[n]$, tandis que $\operatorname{card} V_1^*[n] = \operatorname{card} V_3^*[n] = \operatorname{card} V_1[n]$. □

Références

[1] W. Barth and J. Michel. Modular curves and Poncelet polygons. *Math. Ann.*, 295 :25–49, 1993.

[2] M. Berger. *L'échelle de Jacob de la géométrie*. Vuibert, 2007.

[3] H. Bos, C. Kers, F. Oort, and D. Raven. Poncelet's closure theorem. *Expo. math.*, 5 :289–364, 1987.

[4] A. Cayley. On the porism of the in-and-circumbscribed polygon. *Phil. Trans. of the Royal Soc. London*, CLI :225–239, 1861.

[5] A. Cayley. *The collected mathematical papers*, volume IV. Johnson reprint, 1963. [267].

[6] T.W. Chaundy. Poncelet's poristic polygons. *Proc. London Math. Soc.*, XXII :104–123, 1924.

[7] T.W. Chaundy. Poncelet's poristic polygons II. *Proc. London Math. Soc.*, XXV :17–44, 1926.

[8] P. Du Val. *Elliptic functions and elliptic curves*. CUP, 1973.

[9] G. Halphen. *Traité des fonctions elliptiques*, volume I, II. Gauthier-Villars, 1866-68.

[10] J. Harris and P. Griffiths. On Cayley's explicit solution to Poncelet porism. *L'Ens. Math.*, 24 :31–40, 1978.

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

[12] B. Jakob. Moduli of Poncelet polygons. *J. reine angew. Math.*, 436 :33–44, 1993.

[13] V. Moll and H. McKean. *Elliptic curves*. CUP, 1997.

[14] J.V. Poncelet. *Traité des propriétés projectives des figures*. Bachelier, 1865. 2nde édition.

[15] R.Busam and E. Freitag. *Funktionentheory*. Springer, 2000.

[16] J. Shurman and F. Diamond. *A first course in modular forms*. GTM. Springer, 2005.

[17] L. Washington. *Elliptic curves : number theory ans cryptography*. CRC Press, 2003.

Dominique Hulin
Université Paris-Sud
Laboratoire de Mathématiques – UMR 8628
ORSAY, F-91405

`dominique.hulin@math.u-psud.fr`