Division de la Lemniscate

Jérémie Bettinelli

Juin 2006

Sujet proposé par Mr Yves Benoist

Remerciements

Je tiens à remercier Mr Yves Benoist qui a proposé ce sujet et m'a encadré tout au long de la rédaction de ce rapport.

Table des matières

Introduction

En 1796, Gauss découvre le moyen de construire, à la règle et au compas, un polygone régulier à 17 cotés, qu'il donne dans *Disquisitiones Arithmeticae* [3]. Nous n'exposerons pas ici cette construction fastidieuse et sans grand intérêt théorique[1]. Il montre plus généralement qu'on peut découper le cercle à la règle et au compas en n parties égales si et seulement si n est de la forme 2^α, $\alpha \geq 2$, ou $2^\alpha p_1 p_2 ... p_k$ où $\alpha \in \mathbb{N}$ et les p_i, pour $i \in \{1, ..., k\}$ sont des nombres de Fermat premiers et distincts, c'est-à-dire premiers de la forme $2^{2^r} + 1$ avec $r \in \mathbb{N}$, grâce à sa théorie des nombres cyclotomiques. Sa théorie s'applique en outre à une classe beaucoup plus large que celle des fonctions circulaires $(\sin, \cos, ...)$, et il connaît une grande partie de la théorie de ces fonctions, actuellement connues sous le nom de fonctions elliptiques, sur lesquelles Abel et Jacobi ont ensuite travaillé.

Après s'être intéressé au cas du cercle, Gauss exhibe une méthode qui permet de diviser la lemniscate en cinq parties de même longueur à la règle et au compas, ce qui prouve qu'il pressentait à l'époque la multiplication complexe des fonctions elliptiques.

Fortement intrigué par les travaux de Gauss et le mystère qui les entoure, Abel se penche sur ces derniers et pose les fondements de la théorie des fonctions elliptiques, avec notamment le résultat, très proche de celui de Gauss, disant qu'on peut diviser la lemniscate à la règle et au compas en n parties égales si $n = 2^\alpha$, $\alpha \geq 2$, ou $n = 2^\alpha p_1 p_2 ... p_k$ où $\alpha \in \mathbb{N}$ et les p_i, pour $i \in \{1, ..., k\}$, sont des nombres premiers de Fermat distincts.

Dans un premier temps, nous formaliserons la notion de construction à la règle et au compas, et nous établirons le **Théorème de Gauss** par des moyens modernes, à l'aide de la théorie des corps d'une part et grâce à la théorie de Galois d'autre part, puis nous nous intéresserons à une étude succincte des fonctions elliptiques, pour finalement démontrer le **Théorème d'Abel** et sa réciproque grâce à cette classe de fonctions.

[1] Voir [1] pour la méthode utilisée par Gauss, ainsi qu'une construction plus élégante due à H. W. Richmond en 1893.

Chapitre 1

Théorème de Gauss

Dans ce chapitre, nous définirons les nombres constructibles et exposerons une démonstration du **Théorème de Gauss**. Nous noterons $\mathcal{C}(A, r)$, où $r \geq 0$, le cercle de centre A et de rayon r, et si $a \in \mathbb{C}$, P_a le point du plan complexe d'affixe a, i.e de coordonnées $(\mathfrak{Re}(a), \mathfrak{Im}(a))$. On notera encore $\mathrm{Aff}(P)$ l'affixe du point P, autrement dit $P = P_{\mathrm{Aff}(P)}$.

1.1 Nombres constructibles

1.1.1 Définitions

On se donne deux points distincts O et I du plan, appelés *points de base* et on cherche à caractériser les points que l'on peut construire à l'aide de la règle et du compas, à partir de ceux-ci. On définit ainsi par récurrence un ensemble de points, appelés *points constructibles à la règle et au compas*. On commence par

$$\Omega_0 = \{O, I\},$$

et on définit ensuite Ω_{n+1} à partir de Ω_n. On a droit à deux types de constructions : on peut soit tracer la droite qui passe par deux points de Ω_n, soit tracer le cercle de centre un point et de rayon la distance entre deux points de Ω_n. De tels cercles et droites sont dits *constructibles à la règle et au compas*. On prend alors pour Ω_{n+1} l'ensemble des points d'intersection de deux tels éléments. On définit enfin l'ensemble des points constructibles à la règle et au compas par

$$\Omega = \bigcup_{n \in \mathbb{N}} \Omega_n.$$

Pour simplifier, on appellera *constructibles* les objets constructibles à la règle et au compas.

Il est alors clair que le symétrique I' de I par rapport à O est constructible, ainsi que la médiatrice de $[II']$ et le point J image de I par la rotation de centre O et d'angle $\frac{\pi}{2}$.

Pour formaliser ceci, nous sommes conduits à le définition suivante :

Définition 1.1.1 *Un point $\alpha \in \mathbb{C}$ est dit* constructible à la règle et au compas *ou plus simplement* constructible *s'il est l'affixe d'un point constructible du plan dans le repère (O, I, J).*

Cette définition permet de travailler dans $\mathbb{C}$, plutôt que sur le plan, et ainsi, de se ramener à des propriétés plus algébriques que géométriques.

1.1.2 Propriétés immédiates

On a aisément la proposition suivante :

Proposition 1.1.1 *Si les droites concourantes D et D', les points A et B, ainsi que $\alpha \in \mathbb{C}$ sont constructibles, il en est de même de :*

- *la perpendiculaire à D passant par A*
- *la parallèle à D passant par A*
- *le milieu de $[AB]$*
- *la médiatrice de $[AB]$*

– *les bissectrices des angles déterminés par D et D'*
– *le cercle de centre A et de rayon $|\alpha|$*
– *le cercle de diamètre $[AB]$.*

Preuve. Ceci résulte de constructions élémentaires, et du fait que $|\alpha|$ est la longueur du segment $[OC]$ si α est l'affixe de C. □

Remarque. On a alors immédiatement que a est constructible si et seulement si $\mathfrak{Re}(a)$ et $\mathfrak{Im}(a)$ le sont, en considérant les parallèles aux axes, et si a est constructible, il en est de même de $|a|$.

1.1.3 Corps des nombres constructibles

On s'intéresse maintenant à la structure de l'ensemble des nombres constructibles. On se place dans le cas où O est le point d'affixe 0, et I celui d'affixe 1.

Proposition 1.1.2 *L'ensemble, noté $\mathcal{C}$, des nombres constructibles est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q} + i\mathbb{Q}$.*

Remarques.

i. Tout sous-corps de $\mathbb{C}$ contient 1, donc $\mathbb{Z}$ par stabilité par addition et donc $\mathbb{Q}$ par stabilité par passage à l'inverse.

ii. De la propriété et de la remarque précédente, il résulte que a est constructible si et seulement si $\bar{a}$ l'est.

Preuve. Montrons dans un premier temps que $\mathcal{C}$ est un sous-corps de $\mathbb{C}$.

Il est clair que $\mathcal{C} \subseteq \mathbb{C}$.

Comme 1 est l'affixe de I, il est dans $\mathcal{C}$. De même, $J = P_i$ donc $i \in \mathbb{C}$.

Le nombre $-a$ est l'affixe du symétrique de P_a par rapport à O, une des intersections de $\mathcal{C}(O, |a|)$ et de (OP_a), et $a + b$ est l'affixe d'une des intersections de $\mathcal{C}(P_a, |b|)$ et de la parallèle à (OP_a) passant par P_b, donc $\mathcal{C}$ est un sous-groupe de $(\mathbb{C}, +)$.

Comme

$$(x + iy).(u + iv) = xu - yv + i(xv + yu),$$

il suffit de montrer que pour a, b réels, $ab \in \mathcal{C}$. Or dans ce cas, P_{ab} est l'intersection de (OI) et de la parallèle à (JP_b) passant par P_{ia}.

Enfin, si $a \in \mathbb{R}^*$, $P_{1/a}$ est l'intersection de (OI) et de la parallèle à (IP_{ia}) passant par J. Et si $a \in \mathbb{C}^*$, $a = |a|e^{i\theta}$ où $\frac{1}{|a|}$ est constructible, donc par multiplication $e^{i\theta}$ l'est aussi, ainsi que $e^{-i\theta}$ et finalement $\frac{1}{a} = \frac{1}{|a|}e^{-i\theta}$ aussi. On a ainsi un sous-corps de $\mathbb{C}$.

Le deuxième point de la proposition est simple, $i \in \mathcal{C}$ et $\mathbb{Q} \subseteq \mathcal{C}$ donc $\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q} \subseteq \mathcal{C}$, ce qui termine la preuve. □

Proposition 1.1.3 *Le corps $\mathcal{C}$ est stable par passage à la racine carrée, c'est-à-dire que, si $a \in \mathcal{C}$ et $a = b^2$, alors $b \in \mathcal{C}$.*

Preuve. Commençons par le cas réel. Soit $a \in \mathcal{C} \cap \mathbb{R}^+$, montrons que $\sqrt{a} \in \mathcal{C}$.

Considérons $A = P_{1+a}$, le cercle de diamètre $[OA]$ et l'intersection P de ce cercle avec la parallèle à (OJ) passant par I du demi-plan supérieur. Alors OPA est rectangle et homothétique à OIP et PIA, ce qui montre que

$$\frac{IP}{IO} = \frac{IA}{IP}$$

donc $IP = \sqrt{a}$ et $\sqrt{a} = \mathfrak{Im}(\mathrm{Aff}(P))$ est constructible.

Dans le cas général, $a = |a|e^{i\theta}$ et ses deux racines sont $\pm\sqrt{|a|}e^{i\frac{\theta}{2}}$, et comme $P_{e^{i\frac{\theta}{2}}}$ est une des intersections du cercle trigonométrique et de la bissectrice de (OI) et $(OP_{e^{i\theta}})$, si a est constructible, $e^{i\theta}$ aussi (comme précédemment), puis $e^{i\frac{\theta}{2}}$ et enfin $\pm\sqrt{|a|}e^{i\frac{\theta}{2}}$. □

1.2 Caractérisation des nombres constructibles

On verra deux caractérisations des nombres constructibles, la première à l'aide de tours d'extensions quadratiques de $\mathbb{Q}$ et la seconde en utilisant la théorie de *Galois*.

1.2.1 Première approche

On rappelle que L est une *extension* du corps K, notée $K \subseteq L$, si K est un sous-corps de L. En considérant L comme un K-espace vectoriel, on définit le *degré* de L sur K si la dimension de L en tant qu'espace vectoriel est finie, comme étant cette dimension, notée $[L : K]$. Dans ce cas, on parle d'extension *finie*. Pour une extension de degré 2, on parlera d'extension *quadratique*. On a la propriété classique, pour des extensions finies $K \subseteq L$ et $L \subseteq M$, $K \subseteq M$ est finie et

$$[M : K] = [M : L][L : K].$$

Si $K \subseteq L$ est une extension de corps, $a \in L$ est dit *algébrique* sur K s'il annule un polynôme non nul de $K[X]$, il est dit *transcendant* (sur K) dans le cas contraire. Tout nombre algébrique a admet un *polynôme minimal* sur K, i.e un polynôme irréductible unitaire qui l'annule. On définit alors le *degré* de a (sur K) comme le degré du polynôme minimal, ou encore $[K(a) : K]$, car $K(a)$ est engendré, en tant que K-espace vectoriel, par la base des (a^i) pour $0 \leq i \leq n-1$.

Nous allons maintenant démontrer le théorème suivant,

Théorème 1.2.1 *Le complexe α est constructible si et seulement s'il existe une tour d'extensions quadratiques*

$$\mathbb{Q} \subset L_1 \subset ... \subset L_n$$

telle que $\alpha \in L_n$.

Nous commençons par établir le lemme suivant

Lemme 1.2.1 *Soient α, β, γ trois complexes avec $\alpha \neq \beta$. Alors les coefficients des équations cartésiennes de $(P_\alpha P_\beta)$ et de $\mathcal{C}(P_\alpha, P_\beta P_\gamma)$ sont respectivement dans $\mathbb{Q}(i, \alpha, \bar{\alpha}, \beta, \bar{\beta})$ et $\mathbb{Q}(i, \alpha, \bar{\alpha}, \beta, \bar{\beta}, \gamma, \bar{\gamma})$.*

Preuve. La droite $(P_\alpha P_\beta)$ a pour équation

$$xi(-\alpha + \bar{\alpha} + \beta - \bar{\beta}) + y(\beta + \bar{\beta} - \alpha - \bar{\alpha}) + i(\alpha\bar{\beta} - \bar{\alpha}\beta)$$

et le cercle $\mathcal{C}(P_\alpha, P_\beta P_\gamma)$

$$(x - \frac{\alpha + \bar{\alpha}}{2})^2 + (y - \frac{\alpha - \bar{\alpha}}{2i})^2 - (\beta - \gamma)(\bar{\beta} - \bar{\gamma}) = 0$$

qui sont bien de la forme voulue. □

Puis nous montrons le théorème 1.2.1.

Preuve. ($\Rightarrow$) Notons $0, 1, i, \alpha_1, \alpha_2, ..., \alpha_k = \alpha$ les affixes des points qui ont servi à construire le point P_α, $K_0 = \mathbb{Q}(i)$ et pour $j \in \{1, ..., k\}$, $K_j = \mathbb{Q}(i, \alpha_1, \bar{\alpha}_1, \alpha_2, ..., \alpha_j, \bar{\alpha}_j)$. Le nombre i n'est pas indispensable, mais on peut tout de même l'ajouter pour simplifier les choses.

On a déjà la tour d'extensions $\mathbb{Q} \subseteq K_0 = \mathbb{Q}(i) \subseteq K_1 \subseteq ... \subseteq K_k$ et $\alpha \in K_k$. Il suffit donc de montrer que

$$\forall j \in \{0, ..., k-1\}, [K_{j+1} : K_j] \in \{1, 2\}$$

pour conclure, en considérant ensuite les L_j ordonnés et tels que $\{L_j, j \in \{1, ..., n\}\} = \{K_j, j \in \{1, ..., k\}\}$, car on sait déjà que $\mathbb{Q} \subseteq \mathbb{Q}(i)$ est quadratique.

On a

$$K_{j+1} = K_j(\alpha_{j+1}, \bar{\alpha}_{j+1}) = K_j(\mathfrak{Re}(\alpha_{j+1}), \mathfrak{Im}(\alpha_{j+1}))$$

Distinguons les trois cas possibles :

- Le point $P_{\alpha_{j+1}}$ est à l'intersection de deux droites, alors $\mathfrak{Re}(\alpha_{j+1})$ et $\mathfrak{Im}(\alpha_{j+1})$ sont solutions d'un système linéaire à coefficients dans K_j d'après le lemme, donc restent dans K_j et $K_{j+1} = K_j$.
- Le point $P_{\alpha_{j+1}}$ est à l'intersection d'une droite et d'un cercle dont les équations ont leurs coefficients dans K_j d'après le lemme. Grâce à l'équation de la droite, on peut exprimer une des inconnues x comme combinaison linéaire à coefficients dans K_j de l'autre (y) et de 1. On reporte x dans l'équation du cercle et on trouve que y est solution d'une équation de degré 2 à coefficients dans K_j donc $[K_j(y) : K_j] \leq 2$. Et comme $x \in K_j(y)$, on a $[K_{j+1} : K_j] \leq 2$.
- Le point $P_{\alpha_{j+1}}$ est à l'intersection de deux cercles dont les équations normalisées (i.e. dont les coefficients de x^2 et y^2 sont égaux à 1) ont leurs coefficients dans K_j d'après le lemme. Alors on se ramène au cas précédent en soustrayant une des équations à l'autre.

Dans tous les cas, on trouve bien que $[K_{j+1} : K_j] \leq 2$.

($\Leftarrow$) Réciproquement, si on dispose d'une tour d'extensions quadratiques $\mathbb{Q} = L_0 \subseteq L_1 \subseteq ... \subseteq L_n$, alors

$$\forall j \in \{0, ..., n\}, L_j \subseteq \mathcal{C}$$

En effet, $L_0 \subseteq \mathcal{C}$ et si $L_j \subseteq \mathcal{C}$, montrons que $L_{j+1} \subseteq \mathcal{C}$. Soit $a \in L_{j+1} \backslash L_j$, alors il est algébrique de degré 2 sur L_j, et il existe u, v dans L_j tels que $a^2 + 2au + v = 0$. Ainsi

$$a = -u \pm b$$

où b est tel que $b^2 = u^2 - v$. D'après la proposition 1.1.3, $a \in \mathcal{C}$. □

Nous déduisons, de ce théorème, un corollaire, connu sous le nom de **Résultat de Wantzel**, permettant de montrer rapidement qu'un nombre n'est pas constructible.

Corollaire. Tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.

Preuve. Soit α constructible. On considère la tour du théorème ; alors, d'une part,

$$[L_n : \mathbb{Q}] = [L_n : L_{n-1}]...[L_1 : \mathbb{Q}] = 2^n$$

et d'autre part,

$$[L_n : \mathbb{Q}] = [L_n : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

d'où le résultat, car $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid 2^n$. □

On en déduit notamment que les nombres constructibles sont algébriques, et donc, en notant $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$, on a $\mathbb{Q}(i) \subseteq \mathcal{C} \subseteq \overline{\mathbb{Q}}$. On a, en particulier, que $\mathcal{C}$ est dénombrable vu que $\overline{\mathbb{Q}}$ l'est. Ceci permet, par exemple, de montrer que la quadrature du cercle ou la duplication du cube sont impossibles, car il reviennent à construire π qui est transcendant et $\sqrt[3]{2}$ qui est algébrique de degré 3 sur $\mathbb{Q}$[1].

Corollaire. L'ensemble $\mathcal{C}$ est le plus petit sous-corps de $\mathbb{C}$ stable par passage à la racine.

Preuve. En effet, $\mathcal{C}$ est stable par passage à la racine et si K l'est, $\mathcal{C} \subseteq K$ car si $\alpha \in \mathcal{C}$, on dispose d'une tour d'extensions quadratiques $\mathbb{Q} = L_0 \subseteq L_1 \subseteq ... \subseteq L_n$, avec $\alpha \in L_n$ et

$$\forall j \in \{0, ..., n\}, L_j \subseteq K$$

En effet, $L_0 \subseteq K$ et si $L_j \subseteq K$, montrons que $L_{j+1} \subseteq K$. Soit $a \in L_{j+1} \backslash L_j$, alors il est algébrique de degré 2 sur L_j, et il existe u, v dans L_j tels que $a^2 + 2au + v = 0$. Ainsi

$$a = -u \pm b$$

où b est tel que $b^2 = u^2 - v$. Par stabilité, $b \in K$ et a aussi. □

1.2.2 Deuxième approche

Nous utiliserons ici la théorie de Galois pour caractériser les complexes constructibles. Rappelons ici quelques résultats basiques dont nous nous servirons.

Commençons par un résultat très classique dont nous adapterons la démonstration au cas plus complexe de la lemniscate en fin de rapport.

Proposition 1.2.1 *Soit ζ_n une racine primitive n-ième de l'unité, alors $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ est galoisienne de groupe de* Galois

$$Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \approx \left(\mathbb{Z}/n\mathbb{Z}\right)^*.$$

Preuve. Il est clair que l'extension est galoisienne, car $\mathbb{Q}(\zeta_n)$ est le corps de décomposition du polynôme séparable $X^n - 1$.

Appelons U_n l'ensemble des racines n-ièmes de l'unité et μ_n l'ensemble des racines primitives n-ièmes de l'unité. On sait que

$$G := \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$$

agit par permutation des racines de $X^n - 1$ donc

$$G \hookrightarrow \mathrm{Aut}(U_n) \approx \left(\mathbb{Z}/n\mathbb{Z}\right)^* \approx \mu_n.$$

L'identification étant

$$\begin{array}{ccc} \mathrm{Aut}(U_n) & \approx & \mu_n \\ \sigma & \mapsto & \sigma(\zeta_n) \end{array}.$$

Ainsi, si

$$G \not\approx \left(\mathbb{Z}/n\mathbb{Z}\right)^*,$$

alors on peut décomposer[2]

$$\mu_n = \mu_n^1 \cup \mu_n^2,$$

avec μ_n^1 et μ_n^2 non triviaux et stables par G.

De plus, on sait que le n-ième polynôme cyclotomique,

$$\phi_n(X) = \prod_{\zeta \in \mu_n} (X - \zeta) \in \mathbb{Z}[X].$$

Donc on peut écrire $\phi_n = F^1 F^2$ avec pour i valant 1 ou 2,

$$F^i(X) = \prod_{\zeta \in \mu_n^i} (X - \zeta) \in \mathbb{Z}[X],$$

[1] Voir [1] pour des énoncés similaires plus complets.

[2] On sépare les orbites qui sont au moins au nombre de deux par hypothèse.

le fait que ces polynômes sont à coefficients entiers provenant déjà du fait qu'ils sont invariants par G donc à coefficients rationnels, ensuite du **Lemme de Gauss**[3], les polynômes considérés étant unitaires et $\mathbb{Z}$ intégralement clos.

Maintenant, on peut trouver $\zeta \in \mu_n^1$ et p premier tels que $\zeta^p \in \mu_n^2$. En effet, on prend $\eta \in \mu_n^1$ et $\delta \in \mu_n^2$, alors il existe des nombres premiers $p_1, ...p_k$ tels que $\delta = \eta^{p_1 \cdots p_k}$, et on prend alors $\zeta = \eta^{p_1 \cdots p_j}$ et $p = p_{j+1}$ pour un certain $j \in \{0, ...k-1\}$ (dans le cas $j = 0$, on prend $\zeta = \eta$).

Par suite, les polynômes $F^1(X)$ et $F^2(X^p)$ ne sont pas premiers entre eux, et leur pgcd $D \in \mathbb{Z}[X]$ est unitaire.

On réduit enfin modulo p et on trouve

$$\overline{\phi_n} = \overline{F^1 F^2}$$

avec $\overline{\phi_n}$ séparable car il divise $\overline{X^n - 1}$ qui est séparable étant donné que sa dérivée vaut $\overline{nX^{n-1}} \neq 0$ et que $p \wedge n = 1$ vu que $\zeta^p \in \mu_n$.

Mais $\overline{D} \neq 1$, il a donc une racine dans une clôture de $\mathbb{F}_p$. Sa puissance p-ième est donc racine de $\overline{F^1}$ et $\overline{F^2}$, ce qui est impossible car $\overline{\phi_n}$ est séparable.

C'est donc que

$$G \approx \left(\mathbb{Z}/n\mathbb{Z}\right)^*,$$

ce qu'on voulait démontrer. □

On en déduit

Corollaire. Le polynôme ϕ_n est irréductible et est donc le polynôme minimal de ζ_n sur $\mathbb{Q}$. Il est aussi de degré

$$o\left(\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\right) = \varphi(n),$$

où φ représente l'indicatrice d'Euler.

On rappelle à présent, sans démonstration[4], un résultat utile sur les extensions composées,

Proposition 1.2.2 *Si $K \subseteq L_1$ et $K \subseteq L_2$ sont galoisiennes, alors il en est de même de $K \subseteq L_1 \cap L_2$ et $K \subseteq L_1 L_2$. De plus, on a*

$$Gal\left(L_1 L_2/K\right) = Gal\left(L_1/K\right) \times_{Gal\left(L_1 \cap L_2/K\right)} Gal\left(L_2/K\right),$$

où $G_1 \times_G G_2$ désigne le produit fibré de G_1 par G_2 au-dessus de G.

En particulier, si on considère $x_1, x_2, ...x_n$ algébriques sur $\mathbb{Q}$ tels que pour tout $i \in \{1, ..., n\}$,

$$\mathbb{Q} \subseteq \mathbb{Q}(x_i)$$

est galoisienne, alors $\mathbb{Q} \subseteq \mathbb{Q}(x_1, ...x_n)$ l'est aussi, car $\mathbb{Q}(x_1, ...x_n) = \mathbb{Q}(x_1)\mathbb{Q}(x_2)...\mathbb{Q}(x_n)$.

Par la suite, on utilisera le résultat simplifié où $L_1 \cap L_2 = K$ et donc

$$\mathrm{Gal}\left(L_1 L_2/K\right) = \mathrm{Gal}\left(L_1/K\right) \times \mathrm{Gal}\left(L_2/K\right),$$

avec ici un produit classique.

On revient maintenant à la caractérisation des nombres constructibles

Théorème 1.2.2 *Un nombre complexe est constructible si et seulement s'il est dans une extension galoisienne de $\mathbb{Q}$ dont le groupe de Galois est un 2-groupe.*

Preuve. Nous utilisons la caractérisation vue à la section précédente.

($\Rightarrow$) Soit α constructible. Alors il existe une tour d'extensions quadratiques $\mathbb{Q} \subseteq L_1 \subseteq ... \subseteq L_n$ telle que $\alpha \in L_n$. Montrons alors par récurrence sur n qu'il existe une extension galoisienne $\mathbb{Q} \subseteq K$ telle que $L_n \subseteq K$ et

$$o\left(\mathrm{Gal}\left(K/\mathbb{Q}\right)\right)$$

soit une puissance de 2.

Le cas $n = 1$ est immédiat en prenant $K = L_1$ car une extension quadratique est toujours galoisienne. Il suffit donc de montrer que si

$$\mathbb{Q} \subseteq \underbrace{K \subseteq L}_{\text{d° } 2} \quad \text{et} \quad \underbrace{K \subseteq F}_{\text{d° } 2^r},$$

[3] On rappelle que si A est un anneau intégralement clos (c'est-à-dire A intègre et intégralement clos dans son corps des fractions Frac(A)) et que $P = QR$, avec $P \in A[X]$ unitaire et $Q, R \in \mathrm{Frac}(A)[X]$ unitaires, alors en fait $Q, R \in A[X]$.
Plus généralement, si $A \subseteq B$ est une extension d'anneau et $P = QR$, avec $P \in A[X]$ unitaire et $Q, R \in B[X]$ unitaires, alors les coefficients de Q et R sont entiers sur A.

[4] Voir [4] pour une démonstration de ce résultat.

avec $\mathbb{Q} \subseteq F$ galoisienne, alors il existe

$$\underbrace{L \subseteq E}_{\text{d}^\circ\ 2^s}$$

pour un certain s, avec $\mathbb{Q} \subseteq E$ galoisienne, en appliquant ceci à $K = L_n$ et $L = L_{n+1}$.

On peut alors écrire $L = K(\sqrt{\alpha})$ pour un certain $\alpha \in K$. Soit

$$P(x) = \prod_{\sigma \in \omega_\alpha} \left(x^2 - \sigma(\alpha)\right) \in \mathbb{Q}[x],$$

où ω_α est l'orbite de α sous l'action de $\mathrm{Gal}(F/\mathbb{Q})$, car il est invariant par $\mathrm{Gal}(F/\mathbb{Q})$. De plus, P est séparable car les $\sigma(\alpha)$ sont non nuls et distincts deux à deux.

Soit

$$E = \mathrm{Dec}_K(P),$$

alors $[E : K]$ est une puissance de 2 car P est un produit de facteurs quadratiques, et $\sqrt{\alpha} \in E$ puisque $id \in \mathrm{Gal}(F/\mathbb{Q})$, et par suite $L \subseteq E$ avec $[E : L] = [E : K]/2 = 2^s$ pour un certain s.

Enfin, comme $\mathbb{Q} \subseteq F$ est galoisien, $F = \mathrm{Dec}_{\mathbb{Q}}(Q)$, et si $R = P \vee Q \in \mathbb{Q}[x]$, alors R est séparable et ses racines sont celles de P et Q, donc $E = \mathrm{Dec}_{\mathbb{Q}}(R)$ et $\mathbb{Q} \subseteq E$ et galoisienne.

($\Leftarrow$) Si α est dans une extension galoisienne $\mathbb{Q} \subseteq L$ de degré 2^n, alors un **Théorème de Cauchy** affirme qu'il existe, dans $G := \mathrm{Gal}(L/\mathbb{Q})$, un sous-groupe d'ordre 2, noté H. Alors G/H est d'indice 2 ; on le note H_1. Mais comme H_1 est trivial ou encore un 2-groupe, on peut recommencer et trouver

$$H_n = \{id\} \subset H_{n-1} \subset ... \subset H_1 \subset H_0 = G,$$

avec $[H_{i+1} : H_i] = 2$ et alors

$$\mathbb{Q} = \underbrace{L^{H_n} \subset L^{H_{n-1}}}_{\text{d}^\circ\ 2} \subset ... \subset \underbrace{L^{H_1} \subset L^{H_0}}_{\text{d}^\circ\ 2} = L,$$

avec $\alpha \in L$, ce qui montre bien que α est constructible. □

1.3 Théorème de Gauss

Nous pouvons maintenant démontrer le **Théorème de Gauss**. Énonçons-le tout d'abord précisément :

Théorème 1.3.1 (de Gauss) *Un polygone régulier à n cotés est constructible à la règle et au compas si et seulement si n est de la forme 2^α, $\alpha \geq 2$, ou $2^\alpha p_1 p_2 ... p_k$ où $\alpha \in \mathbb{N}$ et où les p_i, pour $i \in \{1, ..., k\}$, sont des nombres de Fermat premiers et distincts.*

Preuve. Nous allons nous servir de la caractérisation qui fait intervenir la théorie de Galois. Il est clair que le problème revient à chercher tous les $\zeta_n = e^{i\frac{2\pi}{n}}$ constructibles, pour $n \geq 3$.

On sait que $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ est galoisienne, et $\mathrm{Gal}\left({}^{\mathbb{Q}(\zeta_n)}/_{\mathbb{Q}}\right)$ est isomorphe à $\left({}^{\mathbb{Z}}/_{n\mathbb{Z}}\right)^*$ donc est d'ordre $\varphi(n)$. Si

$$n = \prod_{i=0}^{k} p_i^{\alpha_i}$$

est la décomposition élémentaire de n, on voit que n convient si et seulement si

$$\varphi(n) = \prod_{i=0}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

est une puissance de 2, ce qui est le cas si et seulement si

$$\forall i \in \{0, ..., k\}, p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i - 1}(p_i - 1)$$

en est une, i.e. soit $p_i = 2$ et α_i est quelconque (le cas $\alpha_i = 0$ revient à dire que $p_i \not| n$), soit $p_i \neq 2$, $\alpha_i = 1$ et p_i est de la forme $2^{m_i} + 1$.

Mais comme les seuls nombres premiers de la forme $2^m + 1$ sont des nombres de Fermat (car si m admet un facteur impair q, alors $2^m + 1 = (2^{\frac{m}{q}})^q - (-1)^q$ se factorise par $2^{\frac{m}{q}} + 1$ d'après Bernoulli) et, compte tenu de la condition $n \geq 3$, on a bien le résultat annoncé. □

Nous nous intéressons maintenant à une seconde preuve qui peut sembler plus compliquée à première vue, mais qui sera utile pour la suite, car nous démontrerons le **Théorème d'Abel** en suivant le même schéma.

Preuve. Soit $C = \{(x,y) \in \mathbb{R}^2,\ x^2+y^2=1\}$ le cercle unité de $\mathbb{R}^2$, et

$$\xi : \begin{array}{ccc} \mathbb{R}/2\pi\mathbb{Z} & \to & C \\ t & \mapsto & (\cos t, \sin t) \end{array}$$

Il est clair que ξ est bijective, et on bénéficie donc d'une structure de groupe sur C par transfert de celle de $\mathbb{R}/2\pi\mathbb{Z}$. Concrètement, $(\cos x, \sin x) + (\cos y, \sin y) = (\cos(x+y), \sin(x+y))$, c'est-à-dire en utilisant les formules d'addition pour sin et cos,

$$(a,b) + (c,d) = (ac - bd, ad + bc),$$

le neutre de C étant $\xi(0) = (1,0)$.

Par une récurrence immédiate, on voit qu'il existe des fonctions polynômiales f_n et g_n dans $\mathbb{Z}[x,y]$ telles que $n(x,y) = (f_n(x,y), g_n(x,y))$ ($f_{n+1}(x,y) = xf_n(x,y) - yg_n(x,y)$ et $g_{n+1}(x,y) = yf_n(x,y) + xg_n(x,y)$). Ainsi l'ensemble

$$C_n = \{(x,y) \in C, f_n(x,y) = 1 \text{ et } g_n(x,y) = 0\}$$

des points du cercle d'ordres divisant n est isomorphe à

$$C_n \approx \frac{1}{n}\mathbb{R}/2\pi\mathbb{Z} \approx \left(\frac{2\pi}{n}\mathbb{Z}\right)/2\pi\mathbb{Z} \approx \mathbb{Z}/n\mathbb{Z}.$$

En particulier C_n est fini. Soit maintenant $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ un automorphisme de $\mathbb{C}$ laissant $\mathbb{Q}$ invariant, alors

$$\sigma\left(f_n(x,y)\right) = f_n\left(\sigma(x), \sigma(y)\right) \qquad \text{et} \qquad \sigma\left(g_n(x,y)\right) = g_n\left(\sigma(x), \sigma(y)\right),$$

donc

$$\sigma_{|C_n} : C_n \to C_n.$$

Mais comme C_n est fini, si $(a,b) \in C_n$, alors l'ensemble

$$\Sigma_a = \{\sigma(a), \sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})\}$$

est fini ; c'est donc que a est algébrique sur $\mathbb{Q}$, car il est annulé par

$$\prod_{\sigma \in \Sigma_a} (X - \sigma(a)) \in \mathbb{Q}[X],$$

et de même b l'est aussi.

On peut donc considérer l'extension galoisienne

$$\mathbb{Q} \subseteq K_n,$$

où

$$K_n = \mathbb{Q}(a_1, a_2, ...a_n, b_1, ..., b_n),$$

en appelant (a_i, b_i) les éléments de C_n, ainsi que $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$.

Alors G_n agit sur C_n en préservant la structure de groupe de C_n car la loi est définie à partir de fonctions polynômiales à coefficients rationnels, donc on a un morphisme

$$\varphi : \begin{array}{ccc} G_n & \to & \mathrm{Aut}(C_n) \\ \sigma & \mapsto & ((a,b) \mapsto (\sigma(a), \sigma(b))) \end{array}$$

De plus, il est clair que φ est injectif car $\sigma \in \mathrm{Ker}(\varphi)$ doit fixer tous les a_i et tous les b_i donc K_n ; c'est donc que $\sigma = \mathrm{id}$. Ainsi

$$G_n \approx \varphi(G_n) \leq \mathrm{Aut}(C_n) \approx \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \approx (\mathbb{Z}/n\mathbb{Z})^*,$$

et on conclut de la même façon que lors de la preuve précédente. □

Chapitre 2

Fonctions elliptiques

Nous avons besoin des fonctions elliptiques pour résoudre notre problème ; nous en ferons ici une brève présentation[1].

2.1 Définitions et généralités

2.1.1 Réseaux et classes de résidus

On s'intéresse aux sous-groupes discrets de $\mathbb{C}$, ce sont les sous-groupes additifs Ω de $\mathbb{C}$ dont tous les éléments non nuls sont uniformément minorés, i.e.

$$\exists \delta > 0 / \forall \omega \in \Omega \backslash \{0\}, |\omega| \geq \delta.$$

On a alors trois types de sous-groupes discrets, le sous-groupe trivial $\{0\}$, les sous-groupes cycliques, de la forme $< \omega >= \omega\mathbb{Z}$ avec $\omega \neq 0$, et les sous-groupes que l'on appelle *réseaux*, de la forme $< \omega_1, \omega_2 >= \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ où $\{\omega_1, \omega_2\}$ est libre sur $\mathbb{C}$, c'est-à-dire $\omega_1 \neq 0$ et $\frac{\omega_2}{\omega_1} \in \mathbb{C}\backslash\mathbb{R}$.

C'est ce troisième type de sous-groupes qui est le plus intéressant. Notons déjà que ses générateurs ω_1 et ω_2 ne sont pas uniques. En effet, $a\omega_1 + b\omega_2$ et $c\omega_1 + d\omega_2$ conviennent aussi dans le cas où $ad - bc = \pm 1$.

Définition 2.1.1 *Deux réseaux sont dits* semblables *si l'un est le produit de l'autre par un complexe non nul. La relation de similitude est clairement une relation d'équivalence, dont les classes sont appelées* formes de réseaux.

Par la suite, on notera $\bar{\Omega}$ l'ensemble des conjugués de Ω, c'est-à-dire $\bar{\Omega} = \{\bar{\omega}, \omega \in \Omega\}$. Nous définissons maintenant quelques types remarquables de réseaux.

Définition 2.1.2 *On dit que le réseau Ω est* réel *si $\bar{\Omega} = \Omega$.*

Les réseaux réels sont donc
– les réseaux de la forme $< \omega_1, \omega_2 >$ où $\omega_1 \in \mathbb{R}$ et $\omega_2 \in i\mathbb{R}$
– les réseaux de la forme $< \omega, \bar{\omega} >$ avec $\omega \notin \mathbb{R} \cup i\mathbb{R}$

Définition 2.1.3 *On appelle réseau* carré *un réseau de la forme $< \omega, i\omega >$.*

Définition 2.1.4 *On appelle réseau* triangulaire *un réseau de la forme $< \omega, j\omega >$.*

Le point à noter sur ces réseaux est que ce sont les seuls pour lesquels il existe $\alpha \in \mathbb{C}\backslash\{-1, 1\}$ tel que $\Omega = \alpha\Omega$.

Définition 2.1.5 *Un réseau Ω est dit* à multiplication complexe *si le sous-anneau de $\mathbb{C}$,*

$$\{\alpha \in \mathbb{C}, \alpha\Omega \subseteq \Omega\}$$

contient strictement $\mathbb{Z}$.

De façon plus informelle, un réseau à multiplication complexe est tel qu'il existe des homothéties d'angle distinct de 0 mod. π qui envoient le réseau à l'intérieur de lui-même.

[1] Pour une présentation plus détaillée, voir par exemple [2] ou [6].

Remarque. Par exemple, les réseaux carrés et triangulaires sont à multiplication complexe.

On se donne à présent un réseau Ω.

Définition 2.1.6 *On appelle* classe de résidus modulo Ω *ou plus simplement* classe de résidus *un ensemble de la forme* $z+\Omega = \{z+\omega, \omega \in \Omega\}$. *Les classes de résidus forment un groupe abélien pour l'addition*

$$(z+\Omega)+(z'+\Omega) = (z+z')+\Omega$$

Notation Pour plus de commodité, on notera la classe de résidus de z,

$$(z) = z+\Omega$$

Il est maintenant logique de définir les *régions fondamentales*. Si le réseau est $< \omega_1, \omega_2 >$, les classes de résidus sont les translatés du réseau et les régions fondamentales sont des parallélogrammes

$$z + \{u\omega_1 + v\omega_2, u, v \in \mathbb{R}, 0 \leq u < 1, 0 \leq v < 1\}$$

où $z \in \mathbb{C}$ ou encore d'une des trois formes similaires avec l'inégalité large de l'autre coté. Le plus simple des domaines fondamentaux, et le plus pratique, étant bien entendu

$$\{u\omega_1 + v\omega_2, u, v \in \mathbb{R}, 0 \leq u < 1, 0 \leq v < 1\}.$$

Dans toute la suite, pour $f : \mathbb{C} \to \mathbb{C}$, nous introduisons la notation

$$\sum_{\omega \in \Omega}{}' f(\omega)$$

pour la somme

$$\sum_{\omega \in \Omega \setminus \{0\}} f(\omega)$$

Lorsque le réseau ne portera aucune ambiguïté, nous noterons cette somme simplement $\sum' f(\omega)$, ainsi que $\sum f(\omega) = \sum_{\omega \in \Omega} f(\omega)$.

Proposition 2.1.1 *Pour tout réseau* Ω *et tout entier* $n \geq 3$, *la série* $S_n(\Omega) = \sum' \omega^{-n}$ *converge absolument.*

Remarque. Ce résultat semble assez proche de celui concernant les séries de RIEMANN $\sum_{k=1}^{\infty} \frac{1}{k^n}$ pour $n \geq 2$, mais la condition $n \geq 3$ ici se comprend bien car on somme sur un réseau en dimension deux plutôt qu'en dimension un.

Preuve. Comme le suggère la remarque, nous allons utiliser le résultat suivant,

$$s_n = \sum_{k=1}^{\infty} \frac{1}{k^n}$$

converge absolument pour tout $n \geq 2$.

Notons $\Omega =< \omega_1, \omega_2 >$, et regroupons les termes par paquets de $8r$ éléments situés sur le "parallélogramme"

$$P_r = \{u\omega_1 + v\omega_2, u, v \in \mathbb{Z}, |u| \leq r, |v| \leq r, \max\{|u|, |v|\} = r\}.$$

Si l'on appelle

$$\Sigma_r = \sum_{\omega \in P_r} \omega^{-n},$$

on a

$$S_n(\Omega) = \sum_{r=1}^{\infty} \Sigma_r.$$

Soit maintenant

$$h = \inf\{u\omega_1 + v\omega_2, u, v \in \mathbb{R}, |u| \leq r, |v| \leq r, \max\{|u|, |v|\} = r\},$$

alors $h > 0$ et tous les éléments $\alpha \in P_r$ vérifient $|\alpha| \geq r.h$, ainsi

$$\Sigma_r \leq \frac{8r}{rh^n}$$

et

$$S_n(\Omega) \leq 8h^{-n}s^{n-1}$$

d'où le résultat. □

Remarque. Par un simple changement de variable, on remarque que pour tout $\alpha \in \mathbb{C}$,

$$S_n(\alpha\Omega) = \alpha^{-n} S_n(\Omega)$$

En particulier, dans le cas d'un réseau carré, on a $\Omega = i\Omega$ donc $S_n(\Omega) = 0$ pour tout $n \notin 4\mathbb{N}$ et si Ω est triangulaire, $\Omega = j\Omega$ donc $S_n(\Omega) = 0$ pour tout $n \notin 6\mathbb{N}$ (car on sait déjà que c'est le cas si $n \notin 2\mathbb{N}$).

2.1.2 Fonctions elliptiques

Définition 2.1.7 *On appelle* fonction elliptique *une fonction f méromorphe sur $\mathbb{C}$ doublement périodique, c'est-à-dire qu'il existe un réseau Ω tel que*

$$\forall z \in \mathbb{C}, \forall \omega \in \Omega, f(z+\omega) = f(z).$$

Cela revient à dire que f ne dépend que des classes de résidus modulo Ω.

En particulier, les zéros d'une fonction elliptique non identiquement nulle sont isolés, d'après le principe des zéros isolés, car $\mathbb{C}$ est simplement connexe.

Il est alors légitime de se demander si de telles fonctions non constantes existent, ce que nous ferons dans la section suivante ; mais en attendant, établissons quelques généralités sur les fonctions elliptiques.

Proposition 2.1.2 *Une fonction elliptique sans pôle est constante.*

Preuve. En effet, cela découle immédiatement du **Théorème de Liouville** car une fonction elliptique est entière et bornée sur tout compact donc sur $\mathbb{C}$ par périodicité. □

Corollaire. Deux fonctions elliptiques qui ont le même réseau de périodes, les mêmes pôles et zéros aux mêmes ordres, sont proportionnelles.

Preuve. Si l'une est nulle, les deux le sont.

Sinon, soient f et g ces deux fonctions, alors le quotient $\frac{f}{g}$ est une fonction elliptique qui ne peut avoir des pôles qu'en les pôles de f et en les zéros de g. Or les ordres des zéros et pôles de f et g étant les mêmes, $\frac{f}{g}$ n'a pas de pôles, et on conclut avec la proposition 2.1.2. □

Proposition 2.1.3 *L'ensemble des fonctions elliptiques de réseau de périodes Ω, noté $\mathcal{M}(\mathbb{C}/\Omega)$ forme un corps.*

Preuve. Cela résulte notamment du fait que $\mathbb{C}$ est connexe, donc l'ensemble des fonctions méromorphes sur $\mathbb{C}$ est un corps[2]. □

Remarque. D'un autre point de vue, $\mathcal{M}(\mathbb{C}/\Omega)$ est le corps des fonctions méromorphes sur la surface de Riemann ${}^{\mathbb{C}}/_{\Omega}$, ce qui justifie la notation.

Rappelons maintenant quelques résultats classiques de la théorie de l'analyse complexe :

Proposition 2.1.4 *Soient U un ouvert simplement connexe délimité par un contour fermé C et f une fonction continue sur $\bar{U}$, méromorphe sur U sans zéros ni pôles sur C. Soient $a_1, ..., a_j$ ses zéros d'ordres respectifs $m_1, ..., m_j$ et $b_1, ..., b_k$ ses pôles d'ordres $n_1, ..., n_k$ dont les résidus sont notés $r_1, ..., r_k$. Alors on a :*

i.

$$\int_C f = 2i\pi \sum_{l=1}^{k} r_l$$

[2] Il s'agit d'un résultat classique découlant du principe des zéros isolés (si une fonction méromorphe n'est pas identiquement nulle, ses zéros sont isolés donc son inverse est méromorphe).

ii.

$$\int_C \frac{f'}{f} = 2i\pi(\sum_{l=1}^{j} m_l - \sum_{l=1}^{k} n_l)$$

iii.

$$\int_C z\frac{f'(z)}{f(z)}dz = 2i\pi(\sum_{l=1}^{j} m_l a_l - \sum_{l=1}^{k} n_l b_l)$$

Ce que nous appliquons aux fonctions elliptiques :

Proposition 2.1.5 *Soit f une fonction elliptique non constante de réseau de périodes Ω. On appelle $(a_1), ..., (a_j)$ ses classes de zéros d'ordres respectifs $m_1, ..., m_j$ et $(b_1), ..., (b_k)$ ses classes de pôles d'ordres $n_1, ..., n_k$ dont les résidus sont notés $r_1, ..., r_k$. Alors on a :*

i. $\sum_{l=1}^{k} r_l = 0$

ii. $\sum_{l=1}^{j} m_l = \sum_{l=1}^{k} n_l$

iii. $\sum_{l=1}^{j} m_l a_l = \sum_{l=1}^{k} n_l b_l \ (mod\ \Omega)$

Preuve. On applique la proposition 2.1.4 à un contour

$$C = z + \partial\{u\omega_1 + v\omega_2 | (u,v) \in [0,r]^2\}$$

choisi de telle façon que, sur ce contour, f n'ait ni zéros ni pôles, ce qui est possible car ses zéros et pôles sont en quantité dénombrable.

On a alors

$$\int_C f = \int_{[z,z+\omega_1]} (f(u) - f(u+\omega_2))du + \int_{[z,z+\omega_2]} (f(u+\omega_1) - f(u))du = 0,$$

d'où *i.*

De même

$$\int_C \frac{f'}{f} = 0$$

car $\frac{f'}{f}$ est aussi elliptique, donc on a *ii.*

Pour *iii*, on calcule de la même façon, et en notant $g : z \mapsto z\frac{f'(z)}{f(z)}$, on a

$$g(u) - g(u+\omega_2) = -\omega_2 \frac{f'(u)}{f(u)}$$

et

$$\int_{[z,z+\omega_1]} (g(u) - g(u+\omega_2))du = -\omega_2 \int_0^1 \frac{f'(z+t\omega_1)}{f(z+t\omega_1)}dt$$

Et comme $\varphi : t \mapsto f(z+t\omega_1)$ est C^1 et ne s'annule pas sur $[0,1]$, on peut la relever en e^{ϕ}. Alors $e^{\phi(0)} = e^{\phi(1)}$, de plus $\frac{\varphi'}{\varphi} = \phi'$ donc

$$\int_0^1 \frac{f'(z+t\omega_1)}{f(z+t\omega_1)}dt = \phi(1) - \phi(0) \in 2i\pi\mathbb{Z}.$$

On obtient alors

$$\int_{[z,z+\omega_1]} (g(u) - g(u+\omega_2))du \in 2i\pi\omega_2\mathbb{Z}$$

et de même

$$\int_{[z,z+\omega_2]} (g(u+\omega_1) - g(u))du \in 2i\pi\omega_1\mathbb{Z}$$

d'où

$$\int_C z\frac{f'(z)}{f(z)}dz \in 2i\pi\Omega,$$

ce qui est le résultat voulu. □

2.1.3 Ordre d'une fonction elliptique

Proposition 2.1.6 *Soit f une fonction elliptique non constante et $z \in \mathbb{C}$, alors $f - z$ admet un nombre n de classes de zéros (comptées avec leur ordre de multiplicité) indépendant de z. De plus, la somme de ces n zéros ne dépend pas non plus de z (mod Ω).*

Preuve. Cela résulte de la proposition 2.1.5 (*ii* et *iii*). En effet, f et $f - z$ ont les mêmes pôles aux mêmes ordres donc autant de classes de zéros (comptées avec leur ordre de multiplicité), et la somme de ces zéros est la même (modulo Ω), ce qui permet de conclure. □

Définition 2.1.8 *Le nombre n de la proposition 2.1.6 est appelé* ordre *de la fonction elliptique.*

Remarques.

i. L'ordre d'une fonction elliptique est ainsi son nombre de classes de zéros, ou encore son nombre de classes de pôles (comptés avec multiplicité).

ii. L'ordre d'une fonction elliptique dépend du réseau de référence. En effet une fonction de réseau de périodes Ω d'ordre n est d'ordre $4n$ si elle est considérée comme fonction elliptique de réseau de périodes 2Ω. On veillera donc à considérer le réseau constitué de toutes les périodes de la fonction pour parler de son ordre.

La proposition 2.1.5 montre ainsi qu'il n'existe pas de fonctions elliptiques d'ordre 1. En effet, une telle fonction aurait une unique classe de pôles, d'ordre 1, dont le résidu est nul, ce qui n'est pas possible.

De même, les fonctions elliptiques d'ordre 2 ne peuvent être que de deux types :

i. Soit elles ont une classe de pôles, d'ordre 2, de résidu nul.

ii. Soit elles ont deux classes de pôles, d'ordre 1, dont les résidus sont opposés.

Proposition 2.1.7 *Soit f une fonction elliptique d'ordre n. Alors il n'y a qu'un nombre fini de complexes z tels que $f - z$ admette des zéros d'ordre supérieur à 2.*

Preuve. Les seuls points où $f - z$ peut avoir un zéro au moins double sont les zéros de f' qui sont en nombre fini car f' est elliptique. Il y a donc moins de z qui conviennent que de zéros de f'. La proposition en résulte. □

2.2 La fonction $\wp$ de Weierstrass

Nous nous intéressons maintenant à l'existence de fonctions elliptiques, en introduisant la fonction $\wp$ de Weierstrass, et nous montrons que toute fonction elliptique s'écrit simplement en fonction de cette dernière.

2.2.1 Définition de $\wp$

Dans toute la suite, nous noterons $f(\cdot|\Omega)$ lorsqu'une fonction elliptique est définie en fonction d'un réseau Ω mais nous l'omettrons lorsqu'il n'y aura aucune ambiguïté.

Définition 2.2.1 *Soit Ω un réseau et $\wp(\cdot|\Omega)$ la fonction*

$$z \mapsto \wp(z|\Omega) = \frac{1}{z^2} + \sum_{\omega\in\Omega}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Cette fonction est appelée fonction de Weierstrass.

Proposition 2.2.1 *Pour tout réseau Ω, la fonction $\wp(\cdot|\Omega)$ converge uniformément sur les compacts de la forme*

$$\mathcal{D}(0,R)\backslash \bigcup_{\omega\in\Omega} \mathcal{D}(\omega, r)$$

où $\mathcal{D}(a,d)$ est le disque de centre $a \in \mathbb{C}$ et de rayon $d \in \mathbb{R}^+$.

Preuve. On écrit que

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})^2} - 1\right) = \frac{z}{\omega^3}\frac{1}{(1-\frac{z}{\omega})^2}\left(2 - \frac{z}{\omega}\right).$$

Ensuite, si $|z| < R$, et $|\omega| > 2R$, $|2 - \frac{z}{\omega}| < \frac{5}{2}$ et $|1 - \frac{z}{\omega}| > \frac{1}{2}$, donc

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} < \frac{10R}{\omega^3}$$

Or il n'y a qu'un nombre fini N de $\omega \in \Omega$ tels que $|\omega| \leq 2R$, donc, en appelant ω_0 celui de plus petit module, on a uniformément en u,

$$|\wp(u|\Omega)| \leq N\left(\frac{1}{k^2} + \frac{1}{|\omega_0|^2}\right) + 10R\sum{}'\frac{1}{\omega^3} < \infty,$$

d'où la proposition. □

La fonction de WEIERSTRASS est une fonction clairement méromorphe, elliptique, en faisant le changement $\omega \mapsto \omega + \alpha$ dans la somme qui définit $\wp$, où $\alpha \in \Omega$.

On a ainsi une fonction non triviale, bien définie, dans $\mathcal{M}(\mathbb{C}/\Omega)$. On remarque que $\wp(\cdot|\Omega)$ est paire[3], d'ordre 2, car elle n'a qu'une classe de pôles, à savoir Ω, et ces pôles sont doubles.

Comme la série

$$\sum_{\omega\in\Omega}(z-\omega)^{-3}$$

converge uniformément sur les compacts $\mathcal{D}(0,R)\backslash\bigcup_{\omega\in\Omega}\mathcal{D}(\omega,r)$ [4], on peut dériver terme à terme la série qui définit $\wp(\cdot|\Omega)$ et on trouve

$$\wp'(.|\Omega) = -2\sum_{\omega\in\Omega}(.-\omega)^{-3}.$$

Cette expression montre facilement que $\wp'(.|\Omega)$ est d'ordre 3, avec une seule classe de pôles, tous triples, Ω.

Remarque. On peut ainsi continuer et une récurrence triviale montre que pour tout $n \geq 3$, on a

$$\wp^{(n)}(.|\Omega) = (-1)^n(n+1)!\sum_{\omega\in\Omega}(.-\omega)^{-n-2}$$

et que $\wp^{(n)}(.|\Omega)$ est d'ordre $n+2$, et possède une unique classe de pôles, tous d'ordre $n+2$, Ω.

2.2.2 Équation différentielle satisfaite par $\wp$

On se donne un réseau Ω et on définit $\delta = \min(|\omega|, \omega \in \Omega\backslash\{0\})$. On notera simplement $\wp$ la fonction $\wp(\cdot|\Omega)$ dans toute cette section, ainsi que $S_n = {\sum}'\omega^{-n}$.

Notons encore $g_2 = g_2(\Omega) = 60S_4$ et $g_3 = g_3(\Omega) = 140S_6$.

Proposition 2.2.2 *La fonction $\wp$ satisfait à l'équation différentielle*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \tag{2.1}$$

Preuve. Reprenons dans l'expression qui définit $\wp$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})^2} - 1\right),$$

et remarquons que si $|z| < \delta$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\sum_{p=1}^{\infty}(p+1)\left(\frac{z}{\omega}\right)^p.$$

On obtient ainsi, toujours pour $|z| < \delta$,

$$\wp(z) = \frac{1}{z^2} + {\sum_{\omega\in\Omega}}'\frac{1}{\omega^2}\sum_{p=1}^{\infty}(p+1)\left(\frac{z}{\omega}\right)^p,$$

i.e., car la famille est sommable, et que les S_{2k+1} sont tous nuls,

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)S_{2k+2}\,z^{2k}.$$

La série des dérivées convergeant uniformément sur $\mathcal{D}(0,\delta)$, on obtient,

$$\wp'(z) = -\frac{2}{z^3} + \sum_{k=1}^{\infty}2k(2k+1)S_{2k+2}\,z^{2k-1}.$$

L'idée consiste maintenant à annuler les puissances négatives pour se ramener à une fonction elliptique entière. Pour cela, donnons les expressions aux premiers ordres, pour $z \in \mathcal{D}(0,\delta)$,

$$\wp(z) = \frac{1}{z^2} + 3S_4z^2 + 5S_6z^4 + O(z^6)$$
$$\wp'(z) = -\frac{2}{z^3} + 6S_4z + 20S_6z^3 + O(z^5)$$

[3] En faisant $\omega \mapsto -\omega$ dans la somme qui la définit.

[4] On procède de façon similaire. Il n'y a qu'un nombre fini de ω tels que $\omega \leq 2R$ et si $\omega > 2R$, $|z-\omega| > |\omega|$.

Ainsi,

$$\wp^3(z) = \frac{1}{z^6} + \frac{9S_4}{z^2} + 15S_6 + O(z^2)$$
$$\wp'^2(z) = \frac{4}{z^6} - \frac{24S_4}{z^2} - 80S_6 + O(z^2)$$

Et enfin,

$$\wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3 = O(z^2).$$

On voit sur le membre de gauche que la fonction ainsi trouvée est elliptique, de réseau de périodes Ω. De plus, comme $\wp$ et $\wp'$, elle ne peut avoir de pôle qu'en 0, et le membre de droite, qui est son développement au voisinage de l'origine, montre qu'elle n'en a pas. On conclut à l'aide du **Théorème de Liouville**[5] qu'elle est constante, et nulle, car elle l'est en 0. □

On peut alors explicitement calculer les sommes S_i en remarquant d'une part que les S_{2p+1} sont toutes nulles et que les expressions des S_{2p} se trouvent en écrivant que les coefficients du développement précédent sont tous nuls.

Sinon, il peut être plus commode d'utiliser le fait que $\wp'' = 6\wp^2 - \frac{1}{2}g_2$. Par récurrence, il est immédiat que les S_{2p}, pour $p \geq 2$, s'expriment polynômialement en g_2 et g_3, mais ce qui est le plus remarquable, c'est que les coefficients, rationnels, sont indépendants de Ω.

On a de plus que la donnée de g_2 et g_3 détermine entièrement la fonction $\wp$, car c'est le cas pour tous les points de

$$\bigcup_{\omega\in\Omega} \mathcal{D}(\omega, \delta) = \mathbb{C},$$

ainsi que Ω qui est l'ensemble de ses pôles.

Enfin, la donnée de g_2^3/g_3^2 détermine la forme du réseau puisque si

$$\frac{g_2^3(\Omega)}{g_3^2(\Omega)} = \frac{g_2(\Omega')^3}{g_3(\Omega')^2},$$

alors il existe $\alpha \in \mathbb{C}$ tel que $\alpha^4 = g_2(\Omega)/g_2(\Omega')$, et donc $g_2(\Omega') = \alpha^{-4}g_2(\Omega) = g_2(\alpha\Omega)$ et de même $g_3(\Omega') = g_3(\alpha\Omega)$, donc au final $\Omega = \alpha\Omega$.

Il sera donc souvent utile de calculer les coefficients g_2 et g_3, et compte tenu de la remarque sur les réseaux carrés et triangulaires, on sait déjà que $S_6 = 0$ donc $g_3 = 0$ si on a un réseau carré, et $S_4 = 0$ donc $g_2 = 0$ pour le réseau triangulaire.

2.2.3 Quelques propriétés usuelles

On considère toujours un réseau $\Omega =< \omega_1, \omega_2 >$.

On commence à remarquer que, pour $\alpha \in \mathbb{C}^*$ et $n \in \mathbb{N}$, on a

$$\wp^{(n)}(\alpha \cdot |\alpha\Omega) = \alpha^{-n-2}\wp^{(n)}(\cdot|\Omega),$$

ce qui est immédiat lorsqu'on écrit les expressions[6].

Ceci sera utile notamment lorsqu'on utilise des réseaux carrés, auquel cas

$$\wp(i\cdot) = -\wp(\cdot) \quad \text{et} \quad \wp'(i\cdot) = i\wp'(\cdot)$$

ou des réseaux triangulaires,

$$\wp(j\cdot) = j\wp(\cdot) \quad \text{et} \quad \wp'(j\cdot) = \wp'(\cdot).$$

On connaît les pôles de $\wp$ et $\wp'$, qui sont situés sur les points du réseau, et sont d'ordre respectivement 2 et 3, et on s'intéresse aux zéros.

On sait, d'après la proposition 2.1.5, que pour tout complexe α, il y a exactement deux classes (éventuellement confondues) de points z tels que $\wp(z) = \alpha$ et la somme de ces deux classes est nulle (c'est-à-dire égale au réseau lui-même). En d'autres termes, pour tout $a \in \mathbb{C}$,

$$\{z \in \mathbb{C} \,|\, \wp(z) = \wp(a)\} = (a) \cup (-a),$$

où on rappelle la notation $(a) = a + \Omega$.

[5] Voir la proposition 2.1.2.

[6] Voir la dernière remarque de la section "Définition de $\wp$".

Remarques.

i. Compte tenu de la proposition 2.1.5, il n'est pas nécessaire de distinguer le cas $a \in \Omega$, les points tels que $\wp(z) = \infty$ étant simplement les pôles de $\wp$.

ii. Ce résultat est bien en accord avec la parité de $\wp$.

On voit ainsi que dans le cas $(a) = (-a)$, $a \notin \Omega$, i.e.

$$(a) \in \left\{ \left(\frac{\omega_1}{2}\right), \left(\frac{\omega_2}{2}\right), \left(\frac{\omega_3}{2}\right) \right\},$$

avec $\omega_3 = -\omega_1 - \omega_2$, on a un point stationnaire de $\wp$, et en conséquence un zéro de $\wp'$. Or nous avons trouvé trois classes distinctes de zéros de $\wp'$ qui est d'ordre 3, donc on les a tous.

Notons, pour $i \in \{1, 2, 3\}$,

$$e_i = \wp\left(\frac{\omega_i}{2}\right),$$

on a alors les propriétés suivantes :

- Les e_i sont tous distincts, encore parce que $\wp$ est d'ordre 2, donc on a aussi $g_2^3 \neq 27 g_3^2$ en regardant le discriminant.
- Les e_i sont racines de
$$4x^3 - g_2 x - g_3$$
en évaluant (2.1) en ω_i.
- On a les relations entre coefficients et racines, en particulier $e_1 + e_2 + e_3 = 0$.

On passe aux formules d'addition et duplication qui joueront un rôle essentiel par la suite.

Proposition 2.2.3 (Formule d'addition) *Soient $z_1, z_2 \in \mathbb{C}\backslash\Omega$ tels que $(z_1) \neq (\pm z_2)$. Alors on a*

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \tag{2.2}$$

Preuve. On considère la fonction elliptique d'ordre 3

$$f = \wp' - a\wp - b$$

où les nombres a et b sont choisis de telle manière que f s'annule sur (z_1) et (z_2), ce qui est possible en prenant

$$a = \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)} \quad \text{et} \quad b = \frac{\wp(z_1)\wp'(z_2) - \wp(z_2)\wp'(z_1)}{\wp(z_1) - \wp(z_2)}$$

car la condition $(z_1) \neq (\pm z_2)$ revient exactement à la condition $\wp(z_1) \neq \wp(z_2)$.

En remplaçant dans (2.1) $\wp' = f + a\wp + b$, il vient

$$(f + a\wp + b)^2 = 4\wp^3 - g_2\wp - g_3.$$

Évaluons ceci en z tel que $f(z) = 0$, on trouve

$$4\wp(z)^3 - a^2\wp(z)^2 - (2ab + g_2)\wp - (b^2 + g_3) = 0.$$

Ainsi, les racines du polynôme $4X^3 - a^2X^2 - (2ab + g_2)X - (b^2 + g_3)$ sont les valeurs de $\wp(z)$ pour z dans une classe de zéro de f. Or ces trois classes sont (z_1), (z_2) et $(-z_1 - z_2)$, car leur somme doit être nulle, étant donné que la somme des pôles l'est.

Enfin, la somme de ces racines, $\wp(z_1) + \wp(z_2) + \wp(z_1 + z_2)$, est égale à $\frac{1}{4}a^2$, d'où le résultat. □

Proposition 2.2.4 (Formule de duplication) *Soit $z \in \mathbb{C}\backslash\Omega$, alors on a*

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 \tag{2.3}$$

Preuve. La preuve est quasiment la même ; on considère encore la fonction elliptique

$$f = \wp' - a\wp - b$$

où les nombres a et b sont choisis de telle manière que f et f' s'annulent sur (z), ce qui est possible en prenant

$$a = \frac{\wp''(z)}{\wp'(z)} \quad \text{et} \quad b = \frac{\wp'(z)^2 - \wp(z)\wp''(z)}{\wp'(z)}.$$

Les racines du polynôme $4X^3 - a^2X^2 - (2ab + g_2)X - (b^2 + g_3)$ sont toujours les valeurs de $\wp(z)$ pour z dans une classe de zéros de f. Ces trois classes étant (z), (z) et $(-2z)$, la somme des racines, $2\wp(z) + \wp(2z)$, est égale à $\frac{1}{4}a^2$.

On peut aussi appliquer (2.2) à z et $z + \epsilon$ et faire tendre ϵ vers 0. □

Remarque. On peut trouver des formules similaires pour $\wp'$ en dérivant (2.2) et (2.3).

Si on définit à présent

$$E = \{(x,y) \in \mathbb{C}^2 / y^2 = 4x^3 - g_2 x - g_3\} \cup \{\infty\}$$

alors

Proposition 2.2.5 *L'application*

$$\begin{array}{ccc} \mathbb{C}/\Omega & \to & E \\ \xi : z \neq 0 & \mapsto & (\wp(z), \wp'(z)) \\ 0 & \mapsto & \infty \end{array}$$

est bijective

Preuve. On remarque que ξ est injective, car si $(z_1) \neq (z_2)$, $(z_1), (z_2) \neq (0)$ et $\wp(z_1) = \wp(z_2)$, alors $(z_1) = (-z_2)$ et finalement $\wp'(z_1) = \wp'(z_2)$ implique que

$$(z_1) \in \left\{ \left(\frac{\omega_1}{2}\right), \left(\frac{\omega_2}{2}\right), \left(\frac{\omega_3}{2}\right) \right\},$$

ce qui est contradictoire.

Il est par ailleurs clair que ξ est surjective, car si $(x,y) \in E \backslash \{\infty\}$, il existe $z \in \mathbb{C}$ tel que $x = \wp(z)$ et on a alors $y = \pm \wp'(z)$ à cause de (2.1), et quitte à changer z en $-z$, on a le résultat. □

Par suite, E peut être muni d'une loi de groupe par transfert de structure, c'est-à-dire

$$(\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)),$$

ce qu'on peut explicitement exprimer à l'aide des formules (2.2) et (2.3).

Remarquons que le neutre de E est $\xi(0)$, c'est-à-dire ∞.

Grâce à cette bijection, on peut facilement trouver les points dont l'ordre divise $n \in \mathbb{N}^*$ donné. En effet, en appelant E_n le sous-groupe des éléments dont l'ordre divise n de E, on a, comme

$$E \approx {}^{\mathbb{C}}/_{\Omega},$$

$$E_n \approx {}^{\frac{1}{n}\Omega}/_{\Omega} \approx^{\Omega} /_{n\Omega}$$

donc $\#E_n = n^2$.

Plus explicitement, en faisant la convention

$$(\wp(0), \wp'(0)) = \xi(0) = \infty,$$

$$E_n = \left\{ \left(\wp\left(\frac{a\omega_1 + b\omega_2}{n}\right), \wp'\left(\frac{a\omega_1 + b\omega_2}{n}\right)\right), a, b \in \{0, ...n-1\} \right\}.$$

Par exemple,

$$E_2 = \{\infty; (e_1, 0); (e_2, 0); (e_3, 0)\},$$

en reprenant les notations introduites en début de section.

2.3 Le corps $\mathcal{M}(\mathbb{C}/\Omega)$ des fonctions elliptiques

On a déjà vu précédemment que l'ensemble $\mathcal{M}(\mathbb{C}/\Omega)$ des fonctions elliptiques de réseau de périodes donné Ω formait un corps. C'est donc un sous-corps de $\mathcal{M}(\mathbb{C})$, corps des fonctions méromorphes sur $\mathbb{C}$, contenant les fractions rationnelles en $\wp$ et $\wp'$, c'est-à-dire $\mathbb{C}(\wp, \wp')$. Nous verrons ici plus en détail la structure de ce corps.

2.3.1 Fonctions elliptiques d'ordre 2

Commençons par étudier les fonctions elliptiques d'ordre 2.

Il est assez clair que les fonctions de la forme

$$\frac{a\wp(\cdot - z_0) + b}{c\wp(\cdot - z_0) + d}$$

avec $ad \neq bc$ sont elliptiques d'ordre 2. En effet, si $c = 0$, c'est évident. Sinon, les pôles d'une telle fonction sont les zéros du dénominateur qui ne sont pas zéros du numérateur, car les pôles du numérateur sont "annulés" par ceux du dénominateur. Or la condition $ad \neq bc$ impose que le numérateur et le dénominateur ne s'annulent pas au mêmes points. On sait que $\wp$ est d'ordre 2, donc cette fonction aussi.

Nous nous intéressons maintenant à la réciproque.

Proposition 2.3.1 *Les fonctions elliptiques d'ordre 2 sont les fonctions de la forme*

$$\frac{a\wp(\cdot - z_0) + b}{c\wp(\cdot - z_0) + d}$$

avec $ad \neq bc$.

Preuve. Soit f une fonction elliptique d'ordre 2. Montrons qu'elle est de la forme désirée.

Si la fonction f possède un pôle double, en z_0, alors elle s'annule sur deux classes (éventuellement confondues) du type $(z_0 + \alpha)$, $(z_0 - \alpha)$[7]. Ainsi la fonction elliptique $\wp(\cdot - z_0) - \wp(\alpha)$ possède les mêmes pôles et zéros aux mêmes ordre que f, et on conclut, grâce au **Théorème de Liouville**,[8] que f est proportionnelle à $\wp(\cdot - z_0) - \wp(\alpha)$, le coefficient de proportionnalité étant bien sûr non nul.

Si f possède deux classes distinctes de pôles simples, notées $(z_0 + \beta)$ et $(z_0 - \beta)$, alors elle s'annule sur deux classes (éventuellement confondues) du type $(z_0 + \alpha)$, $(z_0 - \alpha)$[7]. La fonction elliptique

$$\frac{\wp(\cdot - z_0) - \wp(\alpha)}{\wp(\cdot - z_0) - \wp(\beta)}$$

possède les mêmes pôles et zéros aux mêmes ordres que f, donc ces deux fonctions sont proportionnelles.

De plus $\wp(\alpha) \neq \wp(\beta)$ car sinon $(\alpha) = \pm(\beta)$, ce qui permet de conclure. □

2.3.2 Fonctions elliptiques quelconques

Nous cherchons ici un résultat similaire pour les fonctions paires.

Proposition 2.3.2 *Toute fonction elliptique paire s'exprime comme une fraction rationnelle en la fonction $\wp$. La réciproque étant immédiate, l'ensemble des fonctions elliptiques paires de $\mathcal{M}(\mathbb{C}/\Omega)$ est donc $\mathbb{C}(\wp(\cdot|\Omega))$.*

Preuve. On considère une fonction elliptique paire f. Notons $(\pm a_1), ..., (\pm a_j)$ ses classes de zéros d'ordres respectifs $m_1, ..., m_j$ et $(\pm b_1), ..., (\pm b_k)$ ses classes de pôles d'ordres respectifs $n_1, ..., n_k$ différentes de (0). Dans le cas où on a $(a_i) = (-a_i)$ ou $(b_i) = (-b_i)$, c'est-à-dire que a_i ou b_i appartient à $(\frac{1}{2}\Omega) \setminus \Omega$, avec a_i ou b_i d'ordre m, on a m pair et on fait comme si on avait deux classes d'ordre $m/2$.

Si on appelle

$$\sigma = \sum_{i=1}^{j} m_i - \sum_{i=1}^{k} n_i,$$

on a en 0 un pôle d'ordre σ, un zéro d'ordre $-\sigma$ ou ni l'un ni l'autre, suivant que σ est strictement positif, strictement négatif ou nul.

Maintenant, la fonction

$$\frac{\prod_{i=1}^{j}(\wp - \wp(a_i))^{m_i}}{\prod_{i=1}^{k}(\wp - \wp(b_i))^{n_i}}$$

possède les mêmes zéros et pôles aux mêmes ordres, donc, une fois de plus, on conclut à l'aide du **Théorème de Liouville**. □

Nous sommes maintenant en mesure d'étudier toutes les fonctions de $\mathcal{M}(\mathbb{C}/\Omega)$.

Proposition 2.3.3 *Toute fonction elliptique s'écrit comme une fraction rationnelle en $\wp$ et $\wp'$, c'est-à-dire*

$$\mathcal{M}(\mathbb{C}/\Omega) = \mathbb{C}(\wp(\cdot|\Omega), \wp'(\cdot|\Omega)) = \mathbb{C}(\wp(\cdot|\Omega)) + \wp'(\cdot|\Omega)\mathbb{C}(\wp(\cdot|\Omega))$$

ou de façon plus synthétique

$$\mathcal{M}(\mathbb{C}/\Omega) = \mathbb{C}(\wp, \wp') = \mathbb{C}(\wp) + \wp'\mathbb{C}(\wp)$$

[7] Toujours en raison de la proposition 2.1.5.

[8] Voir la proposition 2.1.2.

Preuve. La seconde égalité provient juste de (2.1), car $\wp'$ est de degré 2 sur $\mathbb{C}(\wp)$. Ainsi

$$\mathbb{C}(\wp, \wp') = \mathbb{C}(\wp)(\wp') = \mathbb{C}(\wp) + \wp'\mathbb{C}(\wp).$$

On considère une fonction elliptique f, et on montre qu'il existe $P, Q \in \mathbb{C}(X)$ tels que

$$f = P(\wp) + \wp' Q(\wp).$$

On applique pour cela la proposition 2.3.2 aux fonctions paires

$$f + f(-\cdot) \qquad \text{et} \qquad \frac{f - f(-\cdot)}{\wp'}$$

et on écrit que

$$f = \frac{1}{2}\left(f + f(-\cdot)\right) + \wp' \frac{1}{2}\left(\frac{f - f(-\cdot)}{\wp'}\right)$$

ce qui permet de conclure. □

Proposition 2.3.4 *Toute fonction elliptique vérifie une équation quadratique dont les coefficients sont dans* $\mathbb{C}(\wp)$.

Preuve. On sait qu'il existe $P, Q \in \mathbb{C}(X)$ tels que

$$f = P(\wp) + \wp' Q(\wp).$$

Compte tenu de la proposition 2.2.2, on a

$$(f - P(\wp))^2 = Q(\wp)^2 \left(4\wp^3 - g_2\wp - g_3\right),$$

d'où la proposition. □

Chapitre 3

Théorème d'Abel

Dans ce chapitre, nous nous intéressons au cœur du problème, le **Théorème d'Abel**, que nous exposerons clairement puis démontrerons, ainsi que sa réciproque en fin de chapitre.

3.1 Présentation du problème

3.1.1 La lemniscate

Il existe plusieurs définitions équivalentes de la lemniscate. Géométriquement, on se donne deux points distincts du plan A et B et on définit la lemniscate comme le lieu géométrique des points M dont le produit $AM.BM$ est égal au carré de la demi-distance de A à B.

On peut donc aisément obtenir une équation cartésienne de la lemniscate $\mathcal{L}$; en se plaçant dans un repère orthonormé tel que $A = (-\frac{\sqrt{2}}{2}, 0)$, $B = (\frac{\sqrt{2}}{2}, 0)$ et que la constante soit $\frac{1}{2}$, on obtient :

$$\begin{aligned} M(x,y) \in \mathcal{L} &\Leftrightarrow \sqrt{\left(x-\tfrac{\sqrt{2}}{2}\right)^2 + y^2}\sqrt{\left(x+\tfrac{\sqrt{2}}{2}\right)^2 + y^2} = \tfrac{1}{2} \\ &\Leftrightarrow \left(x-\tfrac{\sqrt{2}}{2}\right)^2\left(x+\tfrac{\sqrt{2}}{2}\right)^2 + y^4 + y^2(2x^2+1) = \tfrac{1}{4} \\ &\Leftrightarrow \left(x^2+y^2\right)^2 = x^2 - y^2 \end{aligned}$$

et de même, on a l'équation polaire de la lemniscate :

$$\rho^2 = \cos(2\theta).$$

La représentation de la lemniscate est la fameuse figure "infini".

3.1.2 La fonction ϕ

Comme nous nous intéressons à la longueur de la lemniscate, il est naturel de considérer l'abscisse curviligne s. On a $ds^2 = d\rho^2 + \rho^2 d\theta^2$ et $\rho.d\rho = -\sin(2\theta).d\theta$, donc $\rho^2 d\rho^2 = (1-\rho^4).d\theta^2$ et enfin

$$ds = \frac{d\rho}{\sqrt{1-\rho^4}}.$$

On peut donc mesurer la longueur de l'arc de lemniscate, de l'origine à un point du premier quadrant,

$$s = \int_0^\rho \frac{dt}{\sqrt{1-t^4}}, \tag{3.1}$$

car s croît avec ρ lorsqu'il décrit $[0,1]$. Ainsi, si on appelle

$$\omega = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}},$$

on voit que la longueur totale de la lemniscate est 2ω, et on peut remarquer que ω correspond, dans le cas de la lemniscate, à π pour ce qui est du cercle.

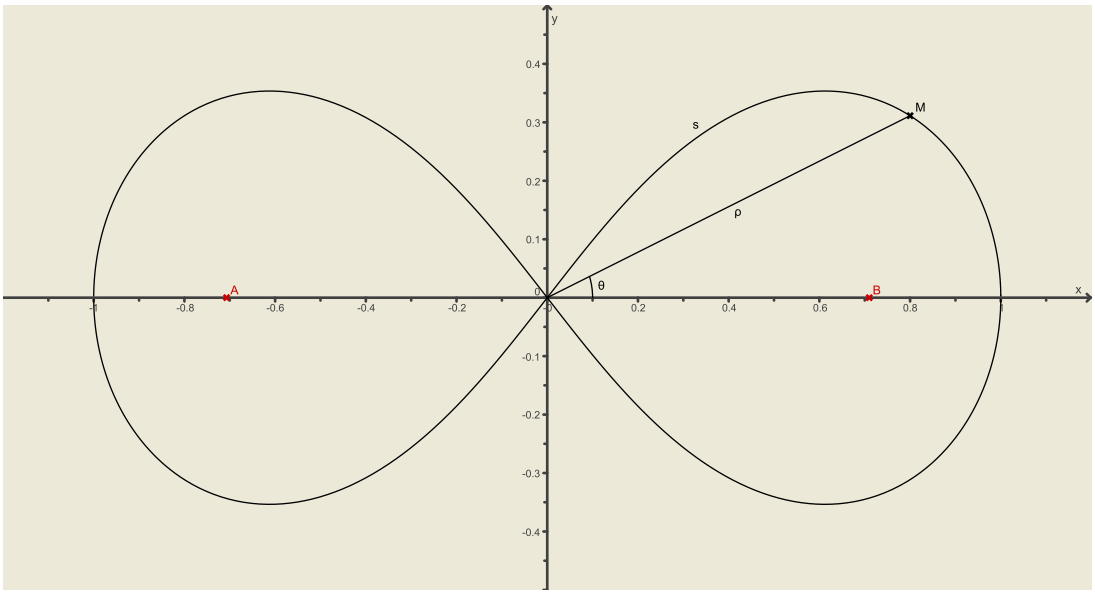

FIG. 3.1 – Représentation de la lemniscate

De plus, il est aussi possible d'exprimer ρ en fonction de s sur $[0, \frac{\omega}{2}]$ car s croît strictement avec ρ sur $[0,1]$. On appellera $\phi : [0, \frac{\omega}{2}] \to [0,1]$ l'application[1] qui à s associe

$$\rho = \phi(s).$$

En considérant la surface de RIEMANN

$$V(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 \mid y^2 = 1 - x^4\}$$

associée à la courbe d'équation $y^2 = 1 - x^4$, on peut considérer (3.1) comme une intégrale sur $V(\mathbb{C})$, à savoir

$$\int \frac{dx}{y},$$

qui est bien définie au moins au voisinage de 0, sur le disque de rayon 1.

La proposition suivante constitue un point primordial.

Proposition 3.1.1 *La fonction ϕ peut être prolongée en une fonction elliptique sur $\mathbb{C}$ de réseau de périodes $< (1+i)\omega, (1-i)\omega >$.*
De plus, ce prolongement, toujours noté ϕ est

$$\phi : z \mapsto z \prod_{\alpha \in \Lambda \cap P} \left(1 - \frac{z^4}{\alpha^4}\right) \prod_{\beta \in \Lambda' \cap P} \left(1 - \frac{z^4}{\beta^4}\right)^{-1},$$

où $\Lambda = \omega\mathbb{Z}[i]$, $\Lambda' = \omega\left(\frac{1+i}{2} + \mathbb{Z}[i]\right)$, et $P = \mathbb{R}_+^* + i\mathbb{R}_+$.

Preuve. Notons provisoirement

$$\psi : z \mapsto z \prod_{\alpha \in \Lambda \cap P} \left(1 - \frac{z^4}{\alpha^4}\right) \prod_{\beta \in \Lambda' \cap P} \left(1 - \frac{z^4}{\beta^4}\right)^{-1}.$$

Cette fonction est bien définie et méromorphe sur $\mathbb{C}$. De plus, elle est ω-antipériodique, et on a facilement

$$\psi(-s) = -\psi(s) \qquad \text{et} \qquad \psi(is) = i\psi(s).$$

Comme $\psi((1 \pm i)\omega + s) = -\psi(\pm i\omega + s) = -\psi\left(\pm i(\omega \mp is)\right) = \mp i\psi(\omega \mp is) = \pm i\psi(\mp is) = \psi(s)$, on a bien

$$\psi \in \mathcal{M}(\mathbb{C}/\ < (1+i)\omega, (1-i)\omega >).$$

[1] Il s'agit de la notation utilisée par ABEL, GAUSS préférait la notation sinlemn(s) et on trouve encore parfois sl(s) pour "sine of the lemniscate".

Montrons maintenant qu'il existe $\lambda \in \mathbb{C}$ tel que $\psi'^2 = 1 - \lambda\psi^4$ et alors

$$\phi : z \mapsto \mu\psi\left(\frac{z}{\mu}\right)$$

où $\mu^4 = \lambda$ vérifiera $\phi'^2 = 1 - \phi^4$ donc sera localement inversible, d'inverse $\int \frac{dx}{y}$ ce qui permettra de conclure que ϕ peut être prolongée à $\mathbb{C}$ en une fonction elliptique. Cela est équivalent à voir que

$$\chi := \left(\frac{\psi'}{\psi}\right)^2 - \psi^{-2} + \lambda\psi^2 = 0.$$

Cette fonction est elliptique de réseau de périodes Λ et de pôles les points de $\Lambda \cup \Lambda'$ à l'ordre 2. Mais en fait, comme $\frac{\psi'(z)}{\psi(z)} = \frac{1}{z} + O(z^3)$, χ n'a pas de pôle en 0, et de même en tout point de Λ par périodicité.

Comme $\frac{\psi'}{\psi}$ a un pôle simple en $\frac{1+i}{2}\omega$ dont le résidu est[2] -1, que ψ^{-2} n'a pas de pôle en ce point et que ψ en a un, simple, de résidu qu'on peut noter $i\lambda^{-1}$ car il est non nul, on voit que χ ne peut avoir en $\frac{1+i}{2}\omega$ qu'un pôle simple, ce qui est impossible car ce serait une fonction elliptique d'ordre un. Par suite, la fonction χ est entière, donc constante, et nulle, car en $O(z^2)$ au voisinage de 0.

Il suffit maintenant de montrer que $\lambda = 1$. Mais comme on sait que ϕ est elliptique, il est légitime de faire les calculs qui conduisent à la proposition 3.1.4, grâce à laquelle on voit que ω est un zéro de ϕ. Étant donnée l'expression de ϕ, il est clair qu'elle n'a pas de zéro sur $]0, \frac{\omega}{2}]$. Ses seuls zéros réels sont donc les points de $\omega\mathbb{Z}$. Et comme $\phi(iz) = i\phi(z)$, le réseau de ses zéros est carré, c'est donc que

$$\omega\mathbb{Z}[i] = \frac{\omega}{\mu}\mathbb{Z}[i]$$

donc $\mu = \pm 1$ ou $\mu = \pm i$, ce qu'on cherchait. □

On a donc en particulier :

Proposition 3.1.2 *La fonction ϕ est d'ordre 2. Ses zéros sont les points de $\Lambda = \omega\mathbb{Z}[i]$ et ses pôles sont ceux de $\Lambda' = \omega\left(\frac{1+i}{2} + \mathbb{Z}[i]\right)$.*

Preuve. Étant donnée l'expression de ϕ, il est clair que ses zéros et pôles sont simples et sont les points respectivement Λ et Λ'.

On a donc immédiatement l'ordre de ϕ étant donné que son réseau minimal de périodes est $< (1+i)\omega, (1-i)\omega >$ et qu'il n'y a que deux zéros dans une région fondamentale de ce réseau. □

Essayons maintenant de caractériser un peu mieux la fonction ϕ, en donnant quelques résultats découverts par ABEL.

Proposition 3.1.3 *On a :*

$$\phi\left((1+i)s\right) = \frac{(1+i)\phi(s)}{\sqrt{1-\phi^4(s)}}. \tag{3.2}$$

Preuve. On sait, pour calculer

$$s = \int \frac{dt}{\sqrt{1-t^2}},$$

qu'il est judicieux de poser

$$t = \frac{2x}{1+x^2},$$

car alors

$$1 - t^2 = \left(\frac{1-x^2}{1+x^2}\right)^2.$$

L'idée naturelle est donc d'essayer avec $t = \rho^2$ et $x = u^2$, il vient alors

$$\rho^2 = \frac{2u^2}{1+u^4}, \qquad \rho = \frac{\sqrt{2}u}{\sqrt{1+u^4}} \qquad \text{et} \qquad 1 - \rho^4 = \left(\frac{1-u^4}{1+u^4}\right)^2.$$

Ainsi

$$d\rho = \sqrt{2}\frac{1-u^4}{(1+u^4)^{\frac{3}{2}}}du \qquad \text{donc} \qquad \frac{d\rho}{\sqrt{1-\rho^4}} = \sqrt{2}\frac{du}{\sqrt{1+u^4}}.$$

On retrouve presque la même intégrale, à un facteur près et à un signe près. On pose alors

$$u = \frac{1+i}{\sqrt{2}}v,$$

ce qui permet d'avoir

$$\rho = \frac{(1+i)v}{\sqrt{1-v^4}}, \qquad 1 - \rho^4 = \left(\frac{1+v^4}{1-v^4}\right)^2 \qquad \text{et} \qquad \frac{d\rho}{\sqrt{1-\rho^4}} = (1+i)\frac{dv}{\sqrt{1-v^4}}.$$

[2] Ceci est un résultat général : si une fonction méromorphe f admet un pôle d'ordre k en u, alors on peut l'écrire $f(z) = \frac{g(z)}{(z-u)^k}$ avec g méromorphe sans pôle en u et donc $\frac{f'(z)}{f(z)} = \frac{g'(z)}{g(z)} - \frac{k}{z-u}$.

Ainsi en intégrant, on trouve

$$\int_0^\rho \frac{dt}{\sqrt{1-t^4}} = (1+i)\int_0^v \frac{dt}{\sqrt{1-t^4}},$$

et donc, en appelant

$$s = \int_0^v \frac{dt}{\sqrt{1-t^4}},$$

que $v = \phi(s)$ et

$$\rho = \phi\left((1+i)s\right) = \frac{(1+i)\phi(s)}{\sqrt{1-\phi^4(s)}},$$

ce qui est le résultat attendu. □

Proposition 3.1.4 (formule de duplication de Fagnano) *La fonction ϕ satisfait à*

$$\phi(2s) = \frac{2\phi(s)\sqrt{1-\phi^4(s)}}{1+\phi^4(s)}.$$

Preuve. On procède de la même manière en remplaçant i en $-i$, ce qui n'influence en rien les calculs précédents et il vient

$$\phi\left((1-i)s\right) = \frac{(1-i)\phi(s)}{\sqrt{1-\phi^4(s)}}. \tag{3.3}$$

On applique maintenant successivement (3.2) et (3.3), ce qui donne

$$\phi\left(2s\right) = \phi\left((1+i)(1-i)s\right) = \frac{(1+i)\phi\left((1-i)s\right)}{\sqrt{1-\phi^4\left((1-i)s\right)}},$$

puis comme

$$1-\phi^4\left((1-i)s\right) = 1 - \frac{-4\phi(s)}{(1-\phi^4(s))^2} = \frac{(1+\phi^4(s))^2}{(1-\phi^4(s))^2},$$

$$\phi\left(2s\right) = \frac{2\phi(s)}{\sqrt{1-\phi^4(s)}}\frac{1-\phi^4(s)}{1+\phi^4(s)} = \frac{2\phi(s)\sqrt{1-\phi^4(s)}}{1+\phi^4(s)}.$$

□

On peut aussi montrer plus généralement la formule d'addition suivante[3],

Proposition 3.1.5 (formule d'addition) *La fonction ϕ satisfait, pour s et t complexes, à*

$$\phi(s+t) = \frac{\phi(s)\sqrt{1-\phi^4(t)} + \phi(t)\sqrt{1-\phi^4(s)}}{1+\phi^2(s)\phi^2(t)}.$$

On est donc finalement conduit au problème suivant :

Problème. Pour quels $n \in \mathbb{N}$, les

$$\phi\left(\frac{2k\omega}{n}\right), k \in \{0, ..., n-1\}$$

sont-ils constructibles ?

Remarque. On peut voir que ce problème est très proche de celui traité au premier chapitre, où il s'agissait de chercher tous les $n \in \mathbb{N}$ tels que

$$\sin\left(\frac{2k\pi}{n}\right), k \in \{0, ..., n-1\}$$

soient constructibles.

3.2 Démonstration du théorème

Dans cette section, nous démontrerons le résultat suivant découvert par Abel :

Théorème 3.2.1 (d'Abel) *Il est possible de diviser la lemniscate à la règle et au compas en n parties égales si $n = 2^\alpha$, $\alpha \geq 2$, ou $n = 2^\alpha p_1 p_2 ... p_k$ où $\alpha \in \mathbb{N}$ et où les p_i, pour $i \in \{1, ..., k\}$ sont des nombres premiers de Fermat distincts.*

Par commodité, nous introduisons l'ensemble, noté $\mathcal{N}$, des nombres n de la forme $n = 2^\alpha$, $\alpha \geq 2$, ou $n = 2^\alpha p_1 p_2 ... p_k$ où $\alpha \in \mathbb{N}$ et où les p_i, pour $i \in \{1, ..., k\}$ sont des nombres premiers de Fermat distincts.

[3] Voir [6] pour une démonstration.

Remarque. Ainsi le **Théorème d'Abel** devient : il est possible de diviser la lemniscate en n parties égales si $n \in \mathcal{N}$.

3.2.1 Équation différentielle vérifiée par $\wp$

Nous considérons ici le réseau carré $\Omega =< 2\omega, 2i\omega >$, car nous n'avons pas encore besoin du fait que ϕ est mieux qu'elliptique de réseau de périodes Ω. Appliquons la proposition 2.2.2, en notant $\wp = \wp(\cdot|\Omega)$ la fonction de Weierstrass associée.

Proposition 3.2.1 *La fonction $\wp$ vérifie l'équation différentielle*

$$\wp'^2 = 4\wp^3 - \frac{1}{4}\wp. \tag{3.4}$$

Preuve. Il suffit de montrer que $g_2 = 1/4$ et $g_3 = 0$. Or on a déjà remarqué, en raison de l'invariance du réseau carré par rotation d'angle $\pi/2$, que $g_3 = 0$. Il reste donc à calculer g_2.

Rappelons que

$$g_2 = 60 \sum_{\alpha \in <2\omega, 2i\omega> \setminus \{0\}} \alpha^{-4};$$

Il suffit donc de montrer la proposition suivante :

Proposition 3.2.2 *On a*

$$\sum_{\alpha \in <\omega, i\omega> \setminus \{0\}} \alpha^{-4} = \frac{1}{15}.$$

Pour cela, nous partitionnons le réseau $< \frac{\omega}{2}, i\frac{\omega}{2} >$ en trois, de la façon suivante : notons $\Lambda = \omega\mathbb{Z}[i]$, nous avons

$$\frac{1}{2}\Lambda = \Lambda \cup \underbrace{\left[\left(\frac{\omega + i\omega}{2}\right) + \Lambda\right]}_{\Lambda'} \cup \underbrace{\left[\left(\frac{\omega}{2} + \Lambda\right) \cup \left(\frac{i\omega}{2} + \Lambda\right)\right]}_{\Lambda''}$$

Définissons maintenant $\Sigma = S_4(\Lambda)$, $\Sigma' = S_4(\Lambda')$ et $\Sigma'' = S_4(\Lambda'')$. On a alors

$$16\Sigma = \Sigma + \Sigma' + \Sigma''$$

et comme[4]

$$\frac{1+i}{2}\Lambda' = \Lambda'',$$

il vient $\Sigma'' = -4\Sigma'$, et finalement $\Sigma' = -5\Sigma$.

Pour trouver la dernière relation dont nous avons besoin, nous reprenons l'expression de la fonction ϕ trouvée par Abel,

$$\phi(z) = z \prod_{\alpha \in \Lambda \cap P} \left(1 - \frac{z^4}{\alpha^4}\right) \prod_{\beta \in \Lambda' \cap P} \left(1 - \frac{z^4}{\beta^4}\right)^{-1},$$

où $P = \mathbb{R}_+^* + i\mathbb{R}_+$.

D'où, en considérant les dérivées logarithmiques, et en multipliant par z,

$$z\frac{\phi'(z)}{\phi(z)} = 1 + (\Sigma' - \Sigma)z^4 + O(z^8),$$

puisque la dérivée du terme $\ln\left(1 - \frac{z^4}{\alpha^4}\right) - \ln\left(1 - \frac{z^4}{\beta^4}\right)$ vaut $-4z^3\left(\frac{1}{\alpha^4} - \frac{1}{\beta^4}\right) + O(z^7)$, et que $\Sigma = 4S_4(\Lambda \cap P)$ et $\Sigma' = 4S_4(\Lambda' \cap P)$.

Il s'agit donc de développer $z\frac{\phi'}{\phi}$ pour conclure. Comme on sait que

$$z = \int_0^{\phi(z)} \frac{dt}{\sqrt{1-t^4}},$$

il vient $\phi'^2 = 1 - \phi^4$.

Notons $\phi(z) = z + az^5 + O(z^9)$ au voisinage de l'origine, alors $\phi'(z) = 1 + 5az^4 + O(z^8)$ et en remplaçant dans l'équation différentielle, on trouve $a = -\frac{1}{10}$, et enfin $\Sigma' - \Sigma = -\frac{2}{5}$.

Finalement, $\Sigma = \frac{1}{15}$, ce que l'on cherchait. □

[4] C'est l'ensemble des $\frac{p-q}{2} + i\frac{p+q+1}{2}$, donc bien le réseau indiqué.

3.2.2 propositions préparatoires

Rappelons que, le réseau étant carré, on a les relations

$$\wp(i\cdot) = -\wp(\cdot) \quad \text{et} \quad \wp'(i\cdot) = i\wp'(\cdot)$$

De plus, en appliquant (2.2) à z et iz, pour $z \in \mathbb{C}\backslash\Omega$, il vient

$$\begin{aligned} \wp\left((1+i)z\right) &= -\wp(z) - \wp(iz) + \frac{1}{4}\left(\frac{\wp'(z)-\wp'(iz)}{\wp(z)-\wp(iz)}\right)^2 \\ &= -\frac{i}{8}\left(\frac{\wp'(z)}{\wp(z)}\right)^2 \end{aligned}$$

et finalement, en utilisant l'équation différentielle vérifiée par $\wp$,

$$\wp\left((1+i)z\right) = -\frac{i}{8}\frac{4\wp^2(z) - \frac{1}{4}}{\wp(z)} \tag{3.5}$$

Et de même, on obtient

$$\wp\left((1-i)z\right) = \frac{i}{8}\frac{4\wp^2(z) - \frac{1}{4}}{\wp(z)} \tag{3.6}$$

Proposition 3.2.3 *Si $\wp(\alpha)$ est constructible, il en est de même de $\wp(\alpha/2)$.*

Preuve. Supposons $\wp(\alpha)$ constructible, alors en appliquant (3.5) à $z = \frac{\alpha}{1+i}$, on voit que $\wp\left(\frac{\alpha}{1+i}\right)$ satisfait à une équation quadratique dont les coefficients sont constructibles, donc $\wp\left(\frac{\alpha}{1+i}\right)$ est constructible. On procède de même en faisant $z = \frac{\alpha}{2}$ dans (3.6) en remarquant que $\frac{1-i}{2} = \frac{1}{1+i}$, ce qui permet de conclure de la même manière. □

Proposition 3.2.4 *Pour $\lambda \in \Omega$ et $n \in \mathbb{N}^*$ tels que $\lambda 2^{-n} \notin \Omega$,*

$$\wp\left(\frac{\lambda}{2^n}\right)$$

est constructible.

Preuve. Le résultat est clair si $n = 1$ car $\wp(\omega)$, $\wp(i\omega)$, et $\wp\left((1+i)\omega\right)$ sont les racines de $4X^3 - \frac{1}{4}X$, c'est-à-dire $\pm\frac{1}{4}$ et 0, qui sont, tous les trois, constructibles[5].

Ensuite la proposition précédente permet de conclure à l'aide d'une récurrence élémentaire. □

On peut maintenant relier la fonction ϕ à la fonction $\wp$ grâce à la proposition suivante :

Proposition 3.2.5 *On a*

$$\wp(\alpha) \text{ est constructible si et seulement si } \phi(\alpha) \text{ l'est.}$$

Preuve. ($\Rightarrow$) Les classes de zéros de ϕ sont (0), (ω), $(i\omega)$ et $((1+i)\omega)$ et ses classes de pôles sont $\left(\frac{1+i}{2}\omega\right)$, $\left(\frac{3+i}{2}\omega\right)$, $\left(\frac{1+3i}{2}\omega\right)$ et $\left(\frac{3+3i}{2}\omega\right)$ (cf proposition 3.1.2). Ainsi, si on pose $z_0 = \frac{1+i}{2}\omega$ et $z_1 = \frac{3+i}{2}\omega$, on voit que

$$\psi : z \mapsto \frac{\wp'(z)}{\left(\wp(z) - \wp(z_0)\right)\left(\wp(z) - \wp(z_1)\right)}$$

possède les mêmes zéros et pôles au mêmes ordres, donc ces deux fonctions sont proportionnelles,

$$\phi = \frac{\psi}{\psi\left(\frac{\omega}{2}\right)}.$$

Comme $\wp\left(\frac{\omega}{2}\right)$, ainsi que $\wp(z_0)$ et $\wp(z_1)$ sont constructibles, $\wp'\left(\frac{\omega}{2}\right)$ l'est aussi grâce à l'équation (3.4), donc $\varphi\left(\frac{\omega}{2}\right)$ aussi, ce qui permet de conclure, car $\wp(\alpha)$ constructible implique $\wp'(\alpha)$ constructible, puis $\psi(\alpha)$ et enfin $\phi(\alpha)$ constructibles.

($\Leftarrow$) Comme on l'a vu lors de la proposition 3.1.1, la fonction $\phi \in \mathcal{M}(\mathbb{C}/ < (1+i)\omega, (1-i)\omega >)$. On considère donc le réseau $\widetilde{\Omega} =< (1+i)\omega, (1-i)\omega >$ ainsi que la fonction associée

$$\widetilde{\wp} = \wp(|\widetilde{\Omega}).$$

De $\Omega = (1+i)\widetilde{\Omega}$, on tire

$$\widetilde{\wp} = 2i\wp\left((1+i)\,\cdot\right). \tag{3.7}$$

[5] Voir la dernière remarque précédant la proposition 2.2.

Dans $\widetilde{\Omega}$, ϕ admet pour classes de pôles $\left(\frac{1+i}{2}\omega\right)$ et $\left(\frac{1-i}{2}\omega\right)$ et pour classes de zéros (0) et (ω), ainsi on déduit toujours du corollaire de la proposition 2.1.2 que

$$\phi = A\frac{\widetilde{\wp} - \widetilde{\wp}(\omega)}{\widetilde{\wp}'},$$

avec A constructible en évaluant en $\frac{\omega}{2}$ car $\widetilde{\wp}(\omega)$ et $\widetilde{\wp}\left(\frac{\omega}{2}\right)$ sont constructibles étant donné (3.7).

Posons maintenant $z_2 = \frac{1-i}{2}\omega$. Alors les zéros de $\widetilde{\wp}'$ étant (z_0), (z_2) et (ω), il vient, encore grâce au **Théorème de Liouville** et en évaluant en $\frac{\omega}{2}$,

$$\phi^2 = \frac{A^2}{4}\frac{\widetilde{\wp} - \widetilde{\wp}(\omega)}{\left(\widetilde{\wp} - \widetilde{\wp}(z_0)\right)\left(\widetilde{\wp} - \widetilde{\wp}(z_2)\right)}.$$

On voit alors que, si $\phi(\alpha)$ est constructible, $\widetilde{\wp}(\alpha)$ l'est aussi, ainsi que $\wp(\alpha)$ en reprenant la formule (3.5). □

Grâce à la proposition 3.2.5, on cherche maintenant à résoudre le problème suivant :

Problème. Pour quels $n \in \mathbb{N}$, les

$$\wp\left(\frac{2k\omega}{n}\right), k \in \{0, ..., n-1\}$$

sont-ils constructibles ?

3.2.3 Preuve

On reconsidère à présent

$$E = \{(x, y) \in \mathbb{C}^2 / y^2 = 4x^3 - \frac{1}{4}x\} \cup \{\infty\}$$

ainsi que la bijection

$$\begin{array}{ccc} \mathbb{C}/\Omega & \to & E \\ \xi : z \neq 0 & \mapsto & (\wp(z), \wp'(z)), \\ 0 & \mapsto & \infty \end{array}$$

introduite dans la section 2.2.3, et on va suivre le même schéma que celui utilisé pour la seconde preuve du **Théorème de Gauss**[6].

On rappelle que le sous-groupe des éléments d'ordre divisant n de E,

$$E_n \approx {}^{\Omega}/_{n\Omega}$$

et en particulier, E_n et fini, de cardinal n^2. Si de plus, on convient que $(\wp(0), \wp'(0)) = \xi(0) = \infty$, alors on peut écrire explicitement E_n,

$$E_n = \left\{\left(\wp\left(\frac{a+ib}{n}2\omega\right), \wp'\left(\frac{a+ib}{n}2\omega\right)\right), a, b \in \{0, ...n-1\}\right\}. \tag{3.8}$$

En appliquant les formules d'addition (2.2) et duplication (2.3), on voit qu'on peut là aussi trouver des fonctions rationnelles f_n et g_n dans $\mathbb{Q}(x, y)$ telles que $n(x, y) = (f_n(x, y), g_n(x, y))$.

On considère alors $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ un automorphisme de $\mathbb{C}$ laissant $\mathbb{Q}$ invariant, donc

$$\sigma(E_n) \subseteq E_n,$$

et comme E_n est fini, on voit, comme dans la preuve du **Théorème de Gauss**, que les points de E_n sont à coordonnées algébriques au-dessus de $\mathbb{Q}$ (ou infinies).

On considère ainsi l'extension galoisienne

$$\mathbb{Q} \subseteq K_n,$$

où

$$K_n = \mathbb{Q}(a_1, a_2, ...a_{n^2}, b_1, ..., b_{n^2}),$$

en appelant (a_i, b_i) les éléments de E_n, et $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ son groupe de Galois.

[6] Voir la section 1.3.

Alors G_n agit sur E_n en préservant la structure de groupe de E_n car la loi est définie à partir de fonctions polynômiales à coefficients rationnels, donc on a un morphisme

$$\varphi : \begin{array}{ccc} G_n & \to & \mathrm{Aut}(E_n) \\ \sigma & \mapsto & ((a,b) \mapsto (\sigma(a), \sigma(b))) \end{array}$$

De plus, là encore, φ est injectif car $\sigma \in \mathrm{Ker}(\varphi)$ doit fixer tous les a_i et tous les b_i donc K_n, c'est donc que $\sigma = \mathrm{id}$. Ainsi

$$G_n \approx \varphi(G_n) \leq \mathrm{Aut}(E_n) \approx \mathrm{Aut}\left({}^{\Omega}/_{n\Omega}\right).$$

Or $\Omega = 2\omega\mathbb{Z} + 2i\omega\mathbb{Z} \approx 2\omega\mathbb{Z} \oplus 2\omega\mathbb{Z}$, donc

$${}^{\Omega}/_{n\Omega} \approx {}^{\mathbb{Z}}/_{n\mathbb{Z}} \oplus^{\mathbb{Z}} /_{n\mathbb{Z}},$$

et

$$G_n \approx \varphi(G_n) \leq \mathrm{Aut}(E_n) \approx \mathrm{Aut}\left({}^{\mathbb{Z}}/_{n\mathbb{Z}} \oplus^{\mathbb{Z}} /_{n\mathbb{Z}}\right) \approx \mathrm{GL}_2\left({}^{\mathbb{Z}}/_{n\mathbb{Z}}\right).$$

Hélas, nous ne pouvons pas conclure comme nous l'avions fait dans le cas du **Théorème de Gauss**, car nous ne possédons pas assez d'informations sur $\varphi(G_n)$, et de plus, on sait que l'ordre de $\mathrm{GL}_2\left({}^{\mathbb{Z}}/_{n\mathbb{Z}}\right)$ n'est jamais une puissance de 2...

Mais il reste encore une donnée dont nous ne nous sommes pas servis, à savoir que $\Omega = \mathbb{Z}[i](2\omega)$, et comme $\mathbb{Z}[i]$ est un anneau, Ω possède une structure de $\mathbb{Z}[i]$-module de rang 1, et donc $\mathbb{C}/\Omega$ est aussi un $\mathbb{Z}[i]$-module, et enfin, par transfert de structure via ξ, E devient également un $\mathbb{Z}[i]$-module.

Réutilisant à nouveau les deux relations

$$\wp(i\cdot) = -\wp(\cdot) \quad \text{et} \quad \wp'(i\cdot) = i\wp'(\cdot),$$

on voit que

$$i(x,y) = (-x, iy).$$

On caractérise maintenant E_n en tant que $\mathbb{Z}[i]$-module.

Proposition 3.2.6 *On a*

$$E_n \underset{\mathbb{Z}[i]-module}{\approx} {}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}$$

Preuve. On reprend la définition de E_n,

$$E_n \underset{\mathbb{Z}[i]-\mathrm{module}}{\approx} \left(\tfrac{1}{n}\Omega\right)/_{\Omega} \underset{\mathbb{Z}[i]-\mathrm{module}}{\approx} {}^{\Omega}/_{n\Omega} = {}^{\mathbb{Z}[i](2\omega)}/_{n\mathbb{Z}[i](2\omega)} \underset{\mathbb{Z}[i]-\mathrm{module}}{\approx} {}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}$$

ce qui est le résultat souhaité. □

Si on appelle à présent $F = \mathbb{Q}(i)$ et $F_n = F(a_1, ..., a_{n^2}, b_1, ..., b_{n^2}) = FK_n$, alors on a les extensions suivantes

$$\underbrace{\mathbb{Q} \subseteq F}_{\mathbb{Z}/2\mathbb{Z}} \quad \text{et} \quad \underbrace{\mathbb{Q} \subseteq K_n}_{G_n},$$

donc d'après la proposition 1.2.2, comme $F \cap K_n = \mathbb{Q}$,

$$F \subseteq F_n$$

est galoisienne de groupe de Galois

$$\mathrm{Gal}({}^{F_n}/_{F}) := \mathcal{G}_n = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times G_n. \tag{3.9}$$

De plus $\mathcal{G}_n$ laisse F fixe donc en particulier i et donc son action sur E_n préserve la structure de $\mathbb{Z}[i]$-module. On a donc un morphisme injectif de $\mathcal{G}_n$ vers

$$\mathrm{Aut}_{\mathbb{Z}[i]}(E_n),$$

le caractère injectif venant toujours de la même raison.

La proposition 3.2.6 permet de voir que

$$\mathrm{Aut}_{\mathbb{Z}[i]}(E_n) \approx \mathrm{Aut}_{\mathbb{Z}[i]}\left({}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}\right) \approx \left({}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}\right)^*.$$

Nous serons en mesure de conclure une fois démontrée la proposition suivante :

Proposition 3.2.7 *Le groupe*

$$\left({}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}\right)^*$$

est un 2-groupe si et seulement si $n \in \mathcal{N}$.

Preuve. Soit $x+iy \in \left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^*$, alors $x-iy \in \left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^*$[7], et donc x^2+y^2 est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Réciproquement, si x^2+y^2 est inversible, $(x+iy)\frac{x-iy}{x^2+y^2}=1$ donc $x+iy$ est inversible.

L'idée est maintenant d'adapter la fonction indicatrice d'Euler à notre cas, posons pour cela

$$\tilde{\varphi}(n) = o\left(\left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^*\right).$$

La fonction $\tilde{\varphi}$ est multiplicative : en effet, soient p et q premiers entre eux, on bénéficie de l'application

$$\begin{array}{ccc} \mathbb{Z}[i]/pq\mathbb{Z}[i] & \to & \mathbb{Z}[i]/p\mathbb{Z}[i] \times^{\mathbb{Z}[i]} /q\mathbb{Z}[i] \\ \overline{x}^{pq}+i\overline{y}^{pq} & \mapsto & (\overline{x}^p+i\overline{y}^p, \overline{x}^q+i\overline{y}^q) \end{array}.$$

Le fait qu'il s'agisse d'un morphisme est clair, le caractère bijectif provient du **Lemme Chinois**, c'est-à-dire du fait que

$$\mathbb{Z}/pq\mathbb{Z} \approx^{\mathbb{Z}} /p\mathbb{Z} \times^{\mathbb{Z}} /q\mathbb{Z}.$$

Ainsi

$$\mathbb{Z}[i]/pq\mathbb{Z}[i] \approx^{\mathbb{Z}[i]} /p\mathbb{Z}[i] \times^{\mathbb{Z}[i]} /q\mathbb{Z}[i],$$

donc

$$\left(\mathbb{Z}[i]/pq\mathbb{Z}[i]\right)^* \approx \left(\mathbb{Z}[i]/p\mathbb{Z}[i]\right)^* \times \left(\mathbb{Z}[i]/q\mathbb{Z}[i]\right)^*,$$

ce qui implique bien

$$\tilde{\varphi}(pq) = \tilde{\varphi}(p)\tilde{\varphi}(q).$$

Il reste donc à calculer $\tilde{\varphi}(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}$. On peut déjà remarquer que pour $\alpha \geq 1$,

$$\tilde{\varphi}(p^\alpha) = p^{\alpha-1}\tilde{\varphi}(p),$$

car x^2+y^2 est inversible modulo p^α si et seulement s'il est inversible modulo p. Les inversibles de $\mathbb{Z}[i]/p^\alpha\mathbb{Z}[i]$ sont donc exactement ceux de $\mathbb{Z}[i]/p\mathbb{Z}[i]$ modulo p et il y en a $p^{\alpha-1}$ pour chaque classe modulo p.

Calculons donc maintenant $\tilde{\varphi}(p)$ pour p premier. x réel est inversible si et seulement si x^2 l'est dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire $x \in (\mathbb{Z}/p\mathbb{Z})^*$. De même, iy est inversible si et seulement si $y \in (\mathbb{Z}/p\mathbb{Z})^*$.[8]

On s'intéresse maintenant aux $x+iy$ avec x et y non nuls. Comme p est premier, $x \in \{1,...,p-1\}$ est inversible, donc

$$\{x+iy \,|\, x,y \in \{1,...,p-1\}\} = \{x(1+ia) \,|\, x,a \in \{1,...,p-1\}\},$$

et $x(1+ia)$ est inversible si et seulement si $1+a^2$ l'est. On a donc

$$\tilde{\varphi}(p) = (p-1)(2+\mathrm{Card}\{a \in \{1,...,p-1\} | \, p \not| 1+a^2\}).$$

Or

$$\mathrm{Card}\{a \in \{1,...,p-1\} | \, p \not| 1+a^2\} = p-1-\underbrace{\mathrm{Card}\{a \in \mathbb{Z}/p\mathbb{Z} \,|\, a^2=-1\}}_{u_p},$$

et comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $u \leq 2$. Si -1 est un carré et $p \neq 2$, c'est-à-dire $p \equiv 1 (\mathrm{mod.}\ 3)$ alors $u_p = 2$, car il y a deux racines opposées distinctes, si -1 n'est pas un carré, $u_p = 0$, et si $p=2$, $u_2 = 1$.

Finalement, si

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

est la décomposition élémentaire de n, alors

$$\tilde{\varphi}(n) = \varphi(n) \prod_{i=1}^{r} (p_i + 1 - u_{p_i}).$$

Il est maintenant clair que si $\tilde{\varphi}(n)$ est une puissance de 2, $\varphi(n)$ aussi et $n \in \mathcal{N}$ d'après ce qu'on a fait dans la preuve du **Théorème de Gauss**.

Réciproquement, si $n \in \mathcal{N}$, $\varphi(n)$ est une puissance de 2 et pour i tel que $p_i \neq 2$, $p_i+1-u_{p_i} = p_i-1$ est bien une puissance de 2 et si $p_i = 2$, $p_i+1-u_{p_i} = p_i = 2$ est encore une puissance de 2, donc $\tilde{\varphi}(n)$ est aussi une puissance de 2. □

Grâce à cette proposition et à la caractérisation des nombres constructibles ayant recours à la théorie de Galois[9], on vient de voir que si $n \in \mathcal{N}$, alors $\mathcal{G}_n$ est un 2-groupe, donc G_n aussi à l'aide de (3.9) et les coordonnées des points de E_n sont constructibles, car incluses dans K_n.

Or c'est exactement dire que les $\wp\left(\frac{a+ib}{n}2\omega\right)$ et $\wp'\left(\frac{a+ib}{n}2\omega\right)$, avec $a,b \in \{0,...n-1\}$ sont constructibles d'après (3.8), et en particulier les

$$\wp\left(\frac{2k\omega}{n}\right), k \in \{0,...,n-1\}$$

sont constructibles, le théorème 3.2.1 est donc démontré.

[7] C'est immédiat en remarquant que si $(x+iy)^{-1} = a+ib$, alors $a-ib = (x-iy)^{-1}$.

[8] On aurait aussi pu simplement dire que si un réel ou un imaginaire pur est inversible, son inverse est du même type.

[9] Voir la proposition 1.2.2.

3.3 Réciproque

Passons maintenant à la réciproque. Nous allons "copier" la preuve de la proposition 1.2.1 comme énoncé à la fin du chapitre 1. Commençons par définir l'ensemble E'_n (correspondant à μ_n) des éléments qui engendrent E_n comme $\mathbb{Z}[i]$-module,

$$E'_n = \{(x,y) \in E_n | < (x,y) >_{\mathbb{Z}[i]-\text{module}} = E_n\}.$$

On sait que

$$\mathcal{G}_n \hookrightarrow \left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^* \approx E'_n$$

et que le groupe

$$\left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^*$$

est un 2-groupe si et seulement si $n \in \mathcal{N}$, d'après la proposition 3.2.7.

On introduit encore

$$A'_n = \{x \,|\, \exists y, (x,y) \in E'_n\}.$$

Il suffit alors de montrer la proposition suivante, car si on peut diviser la lemniscate en n parties égales, alors Γ_n sera un 2-groupe, donc $\left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^*$ aussi et $n \in \mathcal{N}$.

Proposition 3.3.1 *Soit $F = \mathbb{Q}[i]$ et $x \in A'_n$, alors l'extension $F \subseteq F(x^2)$ est galoisienne de groupe de* Galois

$$\Gamma_n := Gal\left(F(x^2)/F\right) \approx \left(\mathbb{Z}[i]/n\mathbb{Z}[i]\right)^* / \{\pm 1, \pm i\}.$$

Nous aurons besoin pour cela de trouver les nombres premiers de $\mathbb{Z}[i]$,

Proposition 3.3.2 *Les nombres premiers de $\mathbb{Z}[i]$ sont :*
- *les nombres $\pm 1 \pm i$*
- *les $a + ib$ avec $a^2 + b^2$ premier dans $\mathbb{Z}$ congru à 1 modulo 4*
- *les $\pm p$ et $\pm ip$ ou p est un nombre premier dans $\mathbb{N}$ congru à 3 modulo 4*

Preuve. On sait déjà que si $z \in \mathbb{Z}[i]$, alors $|z|^2 \in \mathbb{N}$.

Remarquons que les unités de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$ car ce sont bien des unités et si $xy = 1$, alors $|x|^2|y|^2 = 1$ donc $|x|^2$ est inversible dans $\mathbb{Z}$, donc vaut 1.

Ensuite, $\mathbb{Z}[i]$ est factoriel donc ses nombres premiers sont ses irréductibles.

Il est clair que si $|z|^2$ est irréductible dans $\mathbb{Z}$, alors z est irréductible dans $\mathbb{Z}[i]$, car si $z = xy$, $|z|^2 = |x|^2|y|^2$. Ainsi les $a + ib$, tels que $a^2 + b^2$ est premier dans $\mathbb{N}$, sont premiers dans $\mathbb{Z}[i]$. Il y a $\pm 1 \pm i$ et les $a + ib$ avec $a^2 + b^2$ premier dans $\mathbb{Z}$ congru à 1 modulo 4, car si $a \in \mathbb{Z}$, $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$.

Cherchons à présent les nombres premiers p de $\mathbb{Z}[i]$ qui sont dans $\mathbb{N}$. Ils sont premiers dans $\mathbb{N}$ et congrus à 3 modulo 4 car sinon, d'après le **Théorème des deux carrés**[10], on peut trouver a et b tels que $(a + ib)(a - ib) = p$.

Réciproquement, si $p = (a + ib)(c - id)$, avec $a + ib$ et $c - id$ non inversibles, alors $bc = ad$ et $p = ac + bd$, donc $a \wedge b \,|\, p$ et $a \wedge b = 1$ car sinon $p \,|\, a + ib$ et donc $c - id$ est inversible (car de module carré égal à 1). Ainsi d'après le **Lemme de Gauss**, $a \,|\, c$, et de même $c \,|\, a$, donc $a = \epsilon c$ avec $\epsilon = \pm 1$ et par le même raisonnement $b = \epsilon d$ aussi (c'est le "même" ϵ car $bc = ad$). Enfin, $p = \epsilon(a^2 + b^2) = a^2 + b^2$ donc $p = 2$ ou $p \equiv 1 \pmod 4$.

On peut alors conclure, car si $|z|^2$ n'est pas premier, on le décompose dans $\mathbb{N}$ en

$$|z|^2 = p_1 ... p_r . q_1 ... q_s$$

où les p_j sont congrus à 1 ou égaux à 2 et les q_j congrus à 3. On décompose ensuite les p_j en $(a_j + ib_j)(a_j - ib_j)$ et on a alors la décomposition dans $\mathbb{Z}[i]$ car tous ces facteurs sont premiers d'après ce qu'on a déjà fait. Ainsi, si z est premier, il divise $|z|^2$ donc est associé à un des facteurs qui est forcément un q_j, sinon z est associé à $a_j + ib_j$ et $|z|^2 = p_j$ est premier.

Finalement, z est de la troisième forme annoncée, ce qui conclut. □

Nous utiliserons aussi sans démonstration le

Théorème 3.3.1 (de Dirichlet) *Pour tous k et n premiers entre eux dans $\mathbb{Z}[i]$, il existe une infinité de nombres premiers de $\mathbb{Z}[i]$ congrus à k modulo n.*

[10] Un nombre premier de $\mathbb{N}$ s'écrit comme somme de deux carrés si et seulement s'il est égal à 2 ou est congru à 1 modulo 4.
De plus, cette décomposition est unique.

Passons maintenant à la preuve de la proposition 3.3.1.

Tout d'abord, montrons que l'extension $F \subseteq F(x^2)$ est galoisienne.

Lemme 3.3.1 *Les endomorphismes de E sont de la forme*

$$\varphi : (x, y) \mapsto (r(x), ys(x)),$$

où r et s sont des fractions rationnelles.

Preuve. En effet, si $\varphi(x,y) = (r(x,y), s(x,y))$, alors, comme $\varphi(-(x,y)) = \varphi(x,-y) = (r(x,-y), s(x,-y))$ et par ailleurs, $\varphi(-(x,y)) = -\varphi(x,y) = (r(x,y), -s(x,y))$, y n'intervient qu'avec des puissances paires dans l'expression de r et des puissances impaires dans celle de s. On utilise ensuite que $y^2 = 4x^3 - \frac{x}{4}$. □

Maintenant, l'endomorphisme

$$n : (x, y) \mapsto n.(x, y)$$

s'écrit $(r(x), ys(x))$ où r est impaire, car

$$(r(-x), iys(-x)) = n.(-x, iy) = ni.(x, y) = in.(x, y) = (-r(x), iys(x)).$$

Enfin, r^2 est paire, donc est une fonction de X^2 et $F(x^2)$ contient les conjugués de x^2.

À présent, si

$$\Gamma_n \not\approx \left({}^{\mathbb{Z}[i]}/_{n\mathbb{Z}[i]}\right)^* /_{\{\pm 1, \pm i\}},$$

alors on peut décomposer[11]

$$E'_n/_{\{\pm 1, \pm i\}} = E_n^1 \cup E_n^2,$$

avec E_n^1 et E_n^2 non triviaux et Γ_n-invariants.

On introduit à présent, pour $i = 1, 2$, les ensembles[12]

$$A_n^i = \{x^2 \mid \exists y, (x, y) \in E_n^i\},$$

ainsi que les polynômes

$$P_i(X) = \prod_{\alpha \in A_n^i} (X - \alpha) \in F[X] \quad \text{et} \quad P = P_1 P_2 \in F[X].$$

Le fait que les coefficients de ces polynômes soient dans F provient une fois de plus du fait qu'ils sont invariants par Γ_n.

En appelant m_i le ppcm des dénominateurs des coefficients de P_i et $m = m_1 m_2$, on a le polynôme $Q := mP \in \mathbb{Z}[i][X]$ et les polynômes $Q_i := m_i P_i \in \mathbb{Z}[i][X]$, de sorte que

$$Q = Q_1 Q_2.$$

On va maintenant chercher à réduire modulo un certain p, pour aboutir à une contradiction.

On rappelle qu'on bénéficie sur E_n de la loi

$$(a + ib).(x, y) = (f_a(x, y), g_a(x, y)) + (-f_b(x, y), ig_b(x, y)).$$

Lemme 3.3.2 *On peut trouver $a + ib$ premier dans $\mathbb{Z}[i]$ et $\zeta \in E_n^1$ tels que $(a + ib).\zeta \in E_n^2$, avec de plus $p = a^2 + b^2$ supérieur strictement à $md^\circ(P)$, et $a \neq 0$, $b \neq 0$.*

[11] On sépare les orbites qui sont au moins au nombre de deux par hypothèse.

[12] Il est clair que $\infty \notin A_n^i$ car (∞, ∞) n'engendre pas E_n.

Preuve. On prend pour cela $\zeta \in E_n^1$ et $\eta \in E_n^2$, donc il existe $k+il \in \mathbb{Z}[i]$ premier avec n tel que $\eta = (k+il).\zeta$, car $\zeta \in E'_n$. On considère aussi $q \in \mathbb{N}$ premier ne divisant pas n. D'après le **Théorème de Dirichlet**, il existe un complexe $a+ib$ premier dans $\mathbb{Z}[i]$, congru à $k+il$ modulo n, et congru à $1+i$ modulo q, car $n \wedge q = 1$ donc ces deux congruences reviennent à une seule à l'aide du **Théorème Chinois**. On a ainsi encore $(a+ib).\zeta = \eta$ vu que $n.\zeta = \infty$ et a et b non nuls car ils sont tous les deux congrus à 1 modulo q. On peut de plus supposer que $p = a^2+b^2 > \mathrm{d}^\circ(P)$ car on a une infinité de nombres premiers qui conviennent. □

On a donc $p \equiv 1 \pmod 4$, et on se place dans[13]

$$E(\overline{\mathbb{F}_p}) = \left\{(x,y) \in \overline{\mathbb{F}_p}^2 \mid y^2 = 4x^3 - \frac{x}{4}\right\} \cup \{\infty\}.$$

Dans $\mathbb{F}_p$, on note i_p une racine de -1, on choisit $i_p = -ba^{-1}$ (on verra plus tard pourquoi ce choix est judicieux). Son action sur la courbe elliptique est donnée par $i_p.(x,y) = (-x, i_p y)$.

Lemme 3.3.3 *Les endomorphismes de $E(\overline{\mathbb{F}_p})$ sont de la forme*

$$\varphi : (x,y) \mapsto (r(x), ys(x)),$$

où r et s sont des fractions rationnelles.

Preuve. La preuve est exactement la même que celle du lemme 3.3.1. □

Considérons un endomorphisme φ et notons $(X,Y) = \varphi(x,y)$. Alors

$$\frac{dX}{Y} = \frac{r'(x)}{s(x)}\frac{dx}{y}.$$

On note

$$c_\varphi = \frac{r'(x)}{s(x)}.$$

On peut montrer dans le cas général que c_φ ne dépend pas de x mais nous n'en n'aurons pas besoin ici. En revanche, on va montrer :

Lemme 3.3.4 *On a*

$$c_{\alpha+i\beta} = \alpha + i\beta.$$

Preuve. Commençons par montrer que pour φ_1 et φ_2, on a

$$c_{\varphi_1+\varphi_2} = c_{\varphi_1} + c_{\varphi_2}.$$

En effet, si $(x_1,y_1)+(x_2,y_2) = (x_3,y_3)$, alors on a

$$x_3 = \frac{1}{4}u^2 - x_1 - x_2 \qquad \text{et} \qquad y_3 = -y_1 + u(x_1 - x_2),$$

où

$$u = \frac{y_1 - y_2}{x_1 - x_2}.$$

On veut montrer que $\frac{dx_1}{y_1} + \frac{dx_2}{y_2} = \frac{dx_3}{y_3}$, il suffit pour cela de voir que

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1} \qquad \text{et} \qquad \frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}.$$

Or la première condition s'écrit

$$-1 + \frac{u}{4}\left[2\frac{dy_1}{dx_1}(x_1-x_2) - 2(y_1-y_2)\right](x_1-x_2)^{-2} = -1 + \frac{u}{4}[8x_1 + 4x_2 - u^2]y_1^{-1},$$

or $y_i^2 = 4x_i^3 - \frac{1}{4}x_i$ pour $i = 1,2$, donc $2y_1\frac{dy_1}{dx_1} = 12x_1^2 - \frac{1}{4}$ et on obtient alors

$$\left(12x_1^2 - \frac{1}{4}\right)(x_1-x_2) - 2y_1(y_1-y_2) = (8x_1+4x_2)(x_1-x_2)^2 - (y_1-y_2)^2,$$

[13] Comme $p \neq 2$, 4 est bien inversible dans $\mathbb{F}_p$.

et en remplaçant y_i^2 par $4x_i^3 - \frac{1}{4}x_i$ on vérifie bien cette égalité. On procède de même pour montrer l'autre égalité.

Maintenant, $1.(x,y) = (x,y)$ et $i.(x,y) = (-x, iy)$ donc $c_1 = 1$ et $c_i = i$, et par suite,

$$c_{\alpha+i\beta} = \alpha + i\beta.$$

□

On peut considérer une autre notion, celle de degré d'un morphisme $\varphi : (x,y) \mapsto (r(x), ys(x))$ qu'on définit comme le degré de la fraction rationnelle r, c'est-à-dire le maximum des degrés de son numérateur et de son dénominateur si elle est écrite sous forme irréductible.

$$\mathrm{d}^\circ(\varphi) = \mathrm{d}^\circ(r) = \max\{\mathrm{d}^\circ(d), \mathrm{d}^\circ(n)\} \quad \text{si } r = \frac{n}{d} \text{ avec } n \wedge d = 1.$$

C'est donc le nombre d'antécédents d'un point générique, car $\varphi(x,y) = (r(x), ys(x)) = (u,v)$ si et seulement si $u = r(x)$ et $y = \frac{v}{s(x)}$, et comme la valeur de x détermine de façon unique celle de y, il y a bien $\mathrm{d}^\circ(\varphi)$ points qui conviennent.

Lemme 3.3.5 *En particulier*

$$d^\circ(\alpha + i\beta) = \alpha^2 + \beta^2.$$

Preuve. On sait que, sur E, il y a $\alpha^2 + \beta^2$ points (x,y) tels que

$$(\alpha + i\beta).(x,y) = (x_0, y_0)$$

pour (x_0, y_0) générique. Si l'on pose

$$(\alpha + i\beta).(x,y) = (r(x), ys(x)),$$

c'est donc que $r(X) - x_0$ possède $\alpha^2 + \beta^2$ racines. Ainsi r est de degré $\alpha^2 + \beta^2$ et, sur $E(\overline{\mathbb{F}_p})$, si on note

$$(\alpha + i\beta).(x,y) = (\tilde{r}(x), y\tilde{s}(x)),$$

les relations définissant la somme étant les mêmes, $\tilde{r}$ est la réduction de r modulo p, elle est donc aussi de degré $\alpha^2+\beta^2$ car les coefficients dominants du numérateur et du dénominateur de r sont des puissances de 2, étant données les relations (2.2) et (2.3). □

Revenons à notre morphisme

$$a + ib : (x,y) \mapsto (a+ib).(x,y) = (r(x), ys(x)),$$

on a vu que $c_{a+ib} = a + ib = a - b^2a^{-1} = pa^{-1} = 0 \pmod{p}$ et $\mathrm{d}^\circ(a+ib) = p$. Mais dire que $r'(X) = 0 \pmod{p}$ revient à dire que r est une fraction rationnelle en X^p, donc il existe une fraction rationnelle ρ telle que $r(X) = \rho(X^p)$.

Ajoutons à cela le fait que $\mathrm{d}^\circ(r) = p$, on voit qu'il existe des constantes $\kappa, \lambda, \mu, \nu$, avec κ et μ non toutes nulles, telles que

$$r(X) = \frac{\kappa X^p + \lambda}{\mu X^p + \nu}.$$

Mais comme $r(\infty) = \infty$, $\mu = 0$ et on peut supposer que $\nu = 1$ car on travaille à une constante multiplicative près.

Enfin, il y a trois points d'ordre deux sur la courbe, à savoir $(0,0)$ et $\left(\pm\frac{1}{4}, 0\right)$. Comme i_p laisse le premier invariant et échange les deux autres, on a

$$-r(0) = r(0) \quad \text{et} \quad -r\left(\pm\frac{1}{4}\right) = r\left(\pm\frac{1}{4}\right),$$

donc $\lambda = 0$ et $\kappa = \pm 1$.

Compte tenu de ce qu'on sait déjà, le polynôme

$$D := mP_1(X) \wedge P_2(X^p) = mQ_1(X) \wedge Q_2(X^p),$$

de $\mathbb{Z}[i][X]$ (toujours d'après le **Lemme de Gauss**) est non trivial, ainsi que sa réduction $\overline{D}$ modulo p, car $p \wedge m = 1$ donc le coefficient dominant dans $\mathbb{Z}[i][X]$ de sa dérivée est non nul dans $\mathbb{F}_p$.

On peut maintenant conclure de la même manière que dans la preuve de la proposition 1.2.1, car $\overline{Q} = \overline{Q_1 Q_2}$ est séparable[14], mais il existe $x \in \overline{\mathbb{F}_p}$ tel que

$$\overline{Q_1(x^p)} = \overline{Q_1(x)^p} = 0 \qquad \text{et} \qquad \overline{Q_2(x^p)} = \overline{Q_2(\pm x^p)} = 0,$$

ce qui est impossible.

Ceci achève la preuve de la réciproque du **Théorème d'Abel**.

[14] Vu que sa dérivée est non nulle car p est premier avec le degré de P.

Bibliographie

[1] Jean-Claude Carrega. *Théorie des Corps : La Règle et le Compas.* Hermann, 1989.

[2] Patrick Du Val. *Elliptic Functions and Elliptic Curves*, volume 9 of London mathematical society lecture note series. Cambrige University Press, 1973.

[3] Carl Friedrich Gauss. *Disquisitiones Arithmeticae,* traduit par Arthur A. Clarke. Yale University Press, New Haven, 1966.

[4] Serge Lang. *Algebra.* Reading MA : Addison-Wesley, 1971.

[5] Claude Mutifian. *Equations algébriques et théorie de Galois.* Vuibert, 1980.

[6] Jan Nekovář. *Elliptic Functions and Elliptic Curves.* http ://www.math.jussieu.fr/ nekovar/co/ln/el/, 2004.

[7] Michael Rosen. *Abel's Theorem On The Lemniscate*, pages 387–395. American Mathematical Monthly 88, 1981.