Plan du chapitre VI – Fonctions Elliptiques

Perrine Jouteur

Pour le 18 novembre 2020

Table des matières

1 Introduction

Ce document a été rédigé en s'appuyant sur les références suivantes : Ahlfors [1], Audin [2], Lang [4], Fermat-Wiles [3], et Wikipédia [5].

Définition 1.1 Un sous-groupe additif $\Omega \subset \mathbb{C}$ est un réseau si

1. Ω est discret,
2. Ω engendre $\mathbb{C}$ sur $\mathbb{R}$.

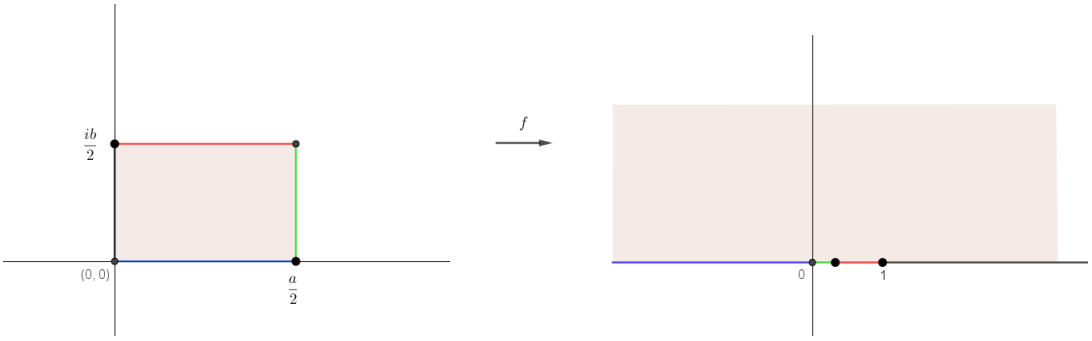
Définition 1.2 Soit Ω un réseau de $\mathbb{C}$. Une fonction méromorphe $f \in \mathrm{Mer}(\mathbb{C})$ est elliptique de périodes Ω lorsque $\forall \omega \in \Omega,\ f(z+\omega) = f(z)$.

Remarque 1.1 L'ensemble des fonctions elliptiques de période Ω est un sous-corps de $\mathrm{Mer}(\mathbb{C})$.

Remarque 1.2 Si $f \in \mathrm{Mer}(\mathbb{C})$ alors l'ensemble des périodes de f forme un sous-groupe discret de $(\mathbb{C}, +)$.

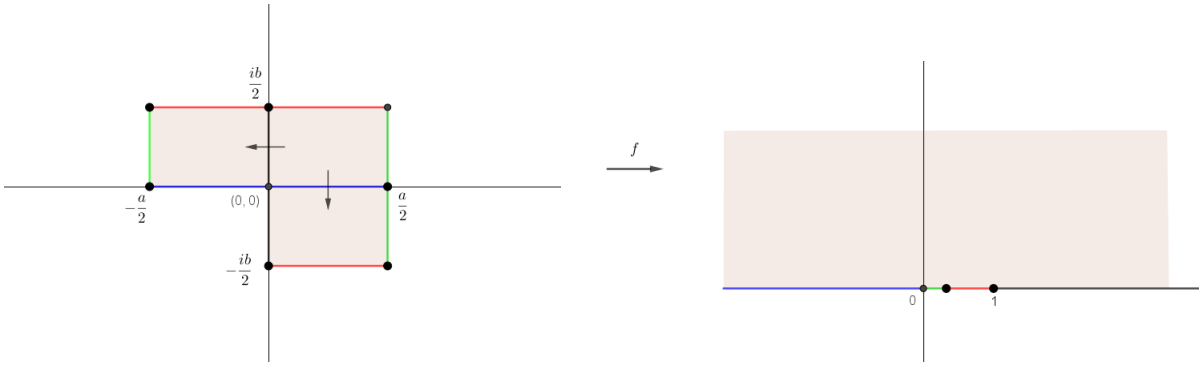
Exemple 1.1 *Reprendre la construction d'une fonction elliptique de périodes $a\mathbb{Z} + ib\mathbb{Z}$ avec $a, b \in \mathbb{R}^*$ faite lors du cours précédent à partir du théorème de représentation conforme et du principe de réflexion de Schwarz.*

Soient a,b deux réels. On pose $\Omega = a\mathbb{Z} + ib\mathbb{Z}$ un réseau. Considérons le rectangle R suivant, et son uniformisation f au demi-plan (un rectangle est bien un domaine simplement connexe) :



(a) rectangle R (b) demi plan $\mathcal{H}$

D'après le principe de réflexion de Schwarz, on peut étendre f aux symétriques du rectangle par rapport à chacun de ses côtés :



(c) prolongements (d) demi plan $\mathcal{H}$

Il manque seulement un lemme pour pouvoir conclure :

Lemme 1.1 Deux réflexions distinctes commutent si et seulement si leurs axes sont perpendiculaires.

Démonstration Soient deux réflexions s_1 et s_2, d'axes respectivement dirigés par les droites affines D_1 et D_2 (distinctes). On choisit $\overrightarrow{u}$ et $\overrightarrow{v}$ des vecteurs directeurs unitaires de D et D' tels que la base $(\overrightarrow{u}, \overrightarrow{v})$ soit directe.
Si D_1 et D_2 sont parallèles, alors $s_1 \circ s_2$ est une translation, de vecteur $2\,\mathrm{dist}(D, D')\overrightarrow{w}$, avec $\overrightarrow{w}$ un vecteur unitaire dirigeant une perpendiculaire à D, orienté de D vers D'. De même, $s_2 \circ s_1$ est une translation de vecteur $-2\,\mathrm{dist}(D, D')\overrightarrow{w}$. Donc s_1 et s_2 commutent si et seulement si $\mathrm{dist}(D, D') = 0$ ce qui n'est pas le cas.
Si D_1 et D_2 sont sécantes, en un point O, alors $s_1 \circ s_2$ est une rotation de centre O et d'angle $2\langle \overrightarrow{u}, \overrightarrow{v} \rangle$.
Comme l'angle d'une rotation la caractérise, les réflexions s_1 et s_2 commutent si et seulement si $\langle \overrightarrow{u}, \overrightarrow{v} \rangle = \langle \overrightarrow{v}, \overrightarrow{u} \rangle$, si et seulement si $\langle \overrightarrow{u}, \overrightarrow{v} \rangle = 0$ si et seulement si les axes sont perpendiculaires. ■

Ce lemme assure que f est définie de manière unique, quel que soit l'ordre choisi pour l'étendre par symétrie. On peut ainsi itérer les symétries pour paver le plan complexe et étendre f à $\mathbb{C}$ entier.

De plus, comme la composée de deux réflexions d'axes parallèles est une translation, on a bien :

$$\forall z \in R, f(z+a) = f(z) \text{ et } f(z+b) = f(z)$$

On a bien construit une fonction elliptique de périodes Ω.

Remarque 1.3 D'après les formules de Schwarz-Christoffel, si f est la fonction elliptique de l'exemple ci-dessus alors sa fonction réciproque est

$$f^{-1}(z) = \int_0^z \frac{dw}{\sqrt{w(w-1)(w-\lambda)}}$$

pour une valeur λ dépendant de a et b. Ce type d'intégrale apparait dans le calcul de la longueur d'un arc d'ellipse. L'étude de ces intégrales commence avec Kepler et se poursuit avec Gauss, Jacobi, Abel et continue encore aujourd'hui.

Exemple 1.2 La série $\sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}$ définie une fonction elliptique de périodes Ω.

Exemple 1.3 Soit $\wp(z) = \sum_{\substack{\omega \in \Omega \\ \omega \neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{w^2}$. Sa dérivée $\wp'(z)$ est elliptique de périodes Ω ce qui implique que pour $\omega \in \Omega$, $\wp(z+\omega) - \wp(z)$ est constante, en posant $z = -\frac{\omega}{2}$ et en utilisant la parité de $\wp$ on montre que cette constante est nulle : $\wp$ est elliptique de périodes Ω.

2 Les réseaux de $\mathbb{C}$

Théorème 2.1 Si G est un sous groupe discret de $(\mathbb{C}, +)$ alors $G = \{0\}$, $G = \omega\mathbb{Z}$ $(\omega \neq 0)$ ou $G = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ $(\omega_1 \neq 0$ et $\frac{\omega_2}{\omega_1} \notin \mathbb{R})$.

Ces derniers sont les réseaux.

Démonstration Supposons que G ne soit pas réduit à $\{0\}$: soit $\omega \in G$, $\omega_1 \neq 0$. Comme G est discret, il existe un nombre fini d'éléments dans G de module inférieur à ω_1, donc on peut choisir ω_1 de module minimal dans G. De plus, G est stable par addition, donc pour tout $n \in \mathbb{Z}$, $n\omega_1 \in G$. Si $G = \omega_1\mathbb{Z}$, on a fini. Sinon :

• Étape 1 : Supposons qu'il existe $\omega_2 \in G$ sur la droite réelle $\mathbb{R}\omega_1$. Alors $\{a + b\frac{\omega_1}{\omega_2} \mid (a,b) \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{R}, +)$, donc ou bien il est de la forme $\mathbb{Z}\alpha$ pour $\alpha > 0$ ou bien il est dense dans $\mathbb{R}$. Comme G est discret, le deuxième cas est impossible, donc il existe $\alpha > 0$ tel que $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \alpha\omega_1\mathbb{Z}$. Enfin, par stabilité de G, on a $\alpha\omega_1 - \lfloor\alpha\rfloor\omega_1 \in G$ donc, par minimalité de $|\omega_1|$:

$$|\alpha\omega_1 - \lfloor\alpha\rfloor\omega_1| \geqslant |\omega_1|$$
$$(\alpha - \lfloor\alpha\rfloor) \geqslant 1$$
$$\alpha \geqslant \lfloor\alpha\rfloor + 1$$

Cela signifie que $\alpha = \lfloor\alpha\rfloor + 1$ donc que $\alpha \in \mathbb{Z}$, ce qui se traduit par $\alpha\omega_1\mathbb{Z} \subset \omega_1\mathbb{Z}$.

• Étape 2 : Supposons qu'il existe $\omega_2 \in G$, $\omega_2 \notin \mathbb{R}\omega_1$. Comme G est discret, il existe un nombre fini d'éléments de G de module inférieur à $|\omega_2|$, donc quitte à changer ω_2, on peut le choisir de module minimal parmi les éléments de G qui ne sont pas dans $\mathbb{Z}\omega_1$. Montrons que $G = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. On a déjà l'inclusion réciproque par stabilité de G par addition.
Pour l'inclusion directe, soit $\omega_3 \in G$.
Remarquons que la famille (ω_1, ω_2) est libre dans $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel, et de cardinal 2, donc elle forme une base de $\mathbb{C}$. Ainsi il existe des réels a_1, a_2 tels que $\omega_3 = a_1\omega_1 + a_2\omega_2$. Posons $n_i = \min(a_i - \lfloor a_i\rfloor, \lfloor a_i\rfloor + 1 - a_i)$ pour $i = 1, 2$. G est stable par addition, donc $\omega_3 - n_1\omega_1 - n_2\omega_2$ est encore un élément de G. Or par inégalité triangulaire, et définition des n_i, on a :

$$|\omega_3 - n_1\omega_1 - n_2\omega_2| \leqslant |a_1 - n_1||\omega_1| + |a_2 - n_2||\omega_2|$$
$$|\omega_3 - n_1\omega_1 - n_2\omega_2| \leqslant \frac{|\omega_1|}{2} + \frac{|\omega_2|}{2} \leqslant |\omega_2|$$

Par minimalité de $|\omega_2|$, on doit avoir égalité dans ces inégalités, donc en particulier,

$$|(a_1 - n_1)\omega_1 + (a_2 - n_2)\omega_2| = |a_1 - n_1||\omega_1| + |a_2 - n_2||\omega_2|$$

D'après le cas d'égalité dans les inégalités triangulaires, soit $(a_1-n_1)\omega_1$ est multiple réel de $(a_2-n_2)\omega_2$, soit $(a_2-n_2)\omega_2$ est nul. Comme ω_1 n'est pas multiple réel de ω_2, on est dans le deuxième cas : $(a_2-n_2)\omega_2 = 0$, donc $\omega_3 - n_2\omega_2 = a_1\omega_1 \in \mathbb{R}\omega_1 \cap G$. Mais on a vu dans l'étape 1 que $\mathbb{R}\omega_1 \cap G = \mathbb{Z}\omega_1$, donc finalement il existe $n \in \mathbb{Z}$ tel que $\omega_3 - n_2\omega_2 = n\omega_1$, et on a montré l'inclusion directe. ■

Remarque 2.1 Si Ω est un réseau et $\lambda \in \mathbb{C}^*$ alors $\lambda\Omega$ est un réseau.

Définition 2.1 Une similitude de Ω_1 dans Ω_2 est une application $z \to \lambda z$ qui envoie Ω_1 dans Ω_2.
• Un endomorphisme du réseau Ω est une similitude de Ω dans Ω (une similitude qui préserve Ω).
• Un automorphisme du réseau Ω est un endomorphisme bijectif de Ω, dont l'inverse est encore un endomorphisme de Ω.

Remarque 2.2 On peut montrer que les seules similitudes qui préservent tous les réseaux sont les similitudes de rapport entier.

Notation 2.1 On note $\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^4 : |ad-bc| = 1 \right\}$ et $\mathrm{SL}_2(\mathbb{Z})$ son sous-groupes des matrices de déterminant 1.

Théorème 2.2 Si (ω_1, ω_2) et $(\tilde{\omega}_1, \tilde{\omega}_2)$ sont deux bases d'un réseau Ω alors $(\omega_1, \omega_2) = (\tilde{\omega}_1, \tilde{\omega}_2)A$ avec $A \in \mathrm{GL}_2(\mathbb{Z})$.
De plus, si $\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)\mathrm{Im}\left(\frac{\tilde{\omega}_2}{\tilde{\omega}_1}\right) > 0$ alors $A \in \mathrm{SL}_2(\mathbf{Z})$.

Démonstration Comme $\tilde{\omega_1} \in \Omega$, il existe $a, c \in \mathbb{Z}$ tels que $\tilde{\omega_1} = a\omega_1 + c\omega_2$. De même, il existe $b, d \in \mathbb{Z}$ tels que $\tilde{\omega_2} = b\omega_1 + d\omega_2$. Ainsi on a $(\tilde{\omega_1}, \tilde{\omega_2}) = (\omega_1, \omega_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

De plus, on peut faire le même raisonnement pour montrer qu'il existe une matrice $\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$ telle que $(\omega_1, \omega_2) = (\tilde{\omega_1}, \tilde{\omega_2})\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}$. Ainsi, on a la relations suivantes :

$$\begin{aligned} \tilde{\omega_1} &= a\omega_1 + c\omega_2 \\ &= a(\tilde{a}\tilde{\omega_1} + \tilde{c}\tilde{\omega_2}) + c(\tilde{b}\tilde{\omega_1} + \tilde{d}\tilde{\omega_2}) \\ &= (a\tilde{a} + c\tilde{b})\tilde{\omega_1} + (a\tilde{c} + c\tilde{d})\tilde{\omega_2} \end{aligned}$$

Or $(\tilde{\omega_1}, \tilde{\omega_2})$ est une base de Ω donc on déduit de l'égalité précédente que

$$a\tilde{a} + c\tilde{b} = 1 \text{ et } a\tilde{c} + c\tilde{d} = 0$$

De même, avec $\tilde{\omega_2}$, on obtient :

$$\tilde{a}b + \tilde{b}d = 0 \text{ et } \tilde{c}b + \tilde{d}d = 1$$

Cela se reformule en :

$$\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

En particulier, par propriété de morphisme du déterminant :

$$(\tilde{a}\tilde{d} - \tilde{c}\tilde{b})(ad - bc) = 1$$

Donc $|\tilde{a}\tilde{b} - \tilde{b}\tilde{c}| = 1$ et $A := \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \in GL_2(\mathbb{Z})$.

Enfin, supposons que $\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)\mathrm{Im}\left(\frac{\tilde{\omega}_2}{\tilde{\omega}_1}\right) > 0$.

Posons $\tau = \dfrac{\omega_2}{\omega_1}$ et $\tilde{\tau} = \dfrac{\tilde{\omega_2}}{\tilde{\omega_1}}$. On a :

$$\begin{aligned} \mathrm{Im}(\tilde{\tau}) &= \mathrm{Im}\left(\frac{b\omega_1 + d\omega_2}{a\omega_1 + c\omega_2}\right) \\ &= \mathrm{Im}\left(\frac{b + d\tau}{a + c\tau}\right) \\ &= \frac{1}{|a + c\tau|^2}\mathrm{Im}((b + d\tau)(a - c\overline{\tau})) \\ &= \frac{1}{|a + c\tau|^2}(ad - bc)\,\mathrm{Im}(\tau) \end{aligned}$$

■

Comme les parties imaginaires de τ et $\tilde{\tau}$ sont de même signe, on doit avoir $ad - bc > 0$, donc $ad - bc = 1$ et $\tilde{a}\tilde{d} - \tilde{b}\tilde{c} = 1$.

Exercice 1 : Bases et aires

Énoncé : *Montrer que deux éléments $\mathbb{R}$-linéairement indépendants ω_1, ω_2, d'un réseau Ω de $\mathbb{C}$ forment une base de Ω si et seulement si le parallélogramme P de sommets 0, ω_1, $\omega_1+\omega_2$, ω_2 ne contient que ces 4 éléments de Ω.*

Sens direct : Supposons que (ω_1, ω_2) forme une base du réseau Ω.
Soit $z \in \Omega$. Comme (ω_1, ω_2) est une base du réseau, il existe un unique couple d'entiers (a_1, a_2) tel que $z = a_1\omega_1 + a_2\omega_2$. Si $z \in P$, alors $0 \leqslant a_1 \leqslant 1$ et $0 \leqslant a_2 \leqslant 1$, par définition de P. Mais a_1 et a_2 sont entiers, donc z est l'un des quatre points 0, ω_1, ω_2, $\omega_1+\omega_2$.

Inversement, supposons que P ne contienne que les quatre points 0, ω_1, ω_2 et $\omega_1+\omega_2$. Soit $z \in \Omega$. Comme P contient $\omega_1+\omega_2$, la famille (ω_1, ω_2) est libre dans $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel. Donc il existe des réels a_1 et a_2 tels que $z = a_1\omega_1 + a_2\omega_2$. Par stabilité de Ω par addition, $z - \lfloor a_1 \rfloor \omega_1 - \lfloor a_2 \rfloor \omega_2$ est encore dans le réseau. Et on a $z - \lfloor a_1 \rfloor \omega_1 - \lfloor a_2 \rfloor \omega_2 = (a_1 - \lfloor a_1 \rfloor)\omega_1 + (a_2 - \lfloor a_2 \rfloor)\omega_2$, avec

$$0 \leqslant (a_1 - \lfloor a_1 \rfloor) \leqslant 1 \text{ et } 0 \leqslant (a_2 - \lfloor a_2 \rfloor) \leqslant 1$$

Ainsi $z - \lfloor a_1 \rfloor \omega_1 - \lfloor a_2 \rfloor \omega_2$ est dans P, donc il est égal à l'un des points 0, ω_1, ω_2 ou $\omega_1+\omega_2$, et en particulier a_1 et a_2 sont entiers. Finalement, (ω_1, ω_2) engendre Ω, c'est donc une base du réseau.

Exercice 2 : Endomorphismes de réseaux

Question 1 : *Montrer qu'à une similitude près, un réseau Ω est toujours de la forme $\mathbb{Z} + \tau\mathbb{Z}$ avec $\tau \in \mathbb{H}$.*

Soit (ω_1, ω_2) une base de Ω. Quitte à échanger ω_1 et ω_2, on peut supposer que cette base est directe.

Posons $\lambda = \dfrac{1}{\omega_1}$. Alors la similitude $z \mapsto \lambda z$ envoie Ω sur $\mathbb{Z} + \dfrac{\omega_2}{\omega_1}\mathbb{Z}$. Et par définition de base directe, $\tau := \dfrac{\omega_2}{\omega_1}$ est dans $\mathbb{H}$.

Question 2 : *Montrer que si τ et $\tilde{\tau}$ sont deux complexes de $\mathbb{H}$ tels que $\mathbb{Z} + \tau\mathbb{Z} = \mathbb{Z} + \tilde{\tau}\mathbb{Z}$ alors il existe $h \in \mathrm{PSL}_2(\mathbb{Z})$ tel que $\tau = h\tilde{\tau}$.*

Par définition de réseaux semblables, il existe $\lambda \neq 0$ tel que $\lambda(\mathbb{Z} + \tau\mathbb{Z}) = \mathbb{Z} + \tilde{\tau}\mathbb{Z}$. En particulier, $(\lambda, \lambda\tau)$ est une base de $\mathbb{Z} + \tilde{\tau}\mathbb{Z}$. D'après le théorème 2, il existe une matrice $A = \begin{pmatrix} c & a \\ d & b \end{pmatrix}$ dans $\mathrm{GL}_2(\mathbb{Z})$ telle que $(\lambda, \lambda\tau) = (1, \tilde{\tau})A$, c'est-à-dire :

$$\lambda = c + d\tilde{\tau} \text{ et } \lambda\tau = a + b\tilde{\tau}$$

Or les parties imaginaires de $\tilde{\tau}$ et τ sont strictement positives, donc, toujours par le théorème 2, A est en fait dans $\mathrm{SL}_2(\mathbb{Z})$.
Donc $\tau = \dfrac{a + b\tilde{\tau}}{\lambda} = \dfrac{a + b\tilde{\tau}}{c + d\tilde{\tau}}$.
Notons h l'image de la matrice A par le morphisme de projection de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathrm{PSL}_2(\mathbb{Z})$. On a bien $\tau = h\tilde{\tau}$.

Remarque 2.3 On appelle $\mathrm{PSL}_2(\mathbb{Z})$ le groupe modulaire.

Question 3 : *Soit Ω un réseau et ℓ un automorphisme de réseau de Ω, de rapport λ.*
a) Montrez que λ et $\overline{\lambda}$ sont les deux valeurs propres d'une matrice à coefficients entiers de déterminant 1.

Soit (ω_1, ω_2) une base de Ω. Comme ℓ est un automorphisme de Ω, la famille $(\lambda\omega_1, \lambda\omega_2)$ est encore une base de Ω. D'après la question 2, il existe une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$ telle que $(\lambda\omega_1, \lambda\omega_2) = (\omega_1, \omega_2)A$. Donc λ est valeur propre de A, associée au vecteur propre (ω_1, ω_2). De plus, A est une matrice à coefficients réels donc le conjugué de λ est aussi une valeur propre de A.

b) En déduire que les valeurs possibles pour λ sont $\pm 1, \pm i, \pm\dfrac{1}{2} \pm \dfrac{\sqrt{3}}{2}i$.

Les valeurs propres de A sont les racines de son polynôme caractéristique $X^2 - \mathrm{Tr}(A)X + 1$. Comme A est à coefficients entiers, sa trace est entière. Donc les racines λ_1, λ_2 de ce polynôme vérifient :

$$\lambda_1\lambda_2 = 1 \text{ et } \lambda_1 + \lambda_2 \in \mathbb{Z}$$

Par définition de base de réseau, si λ_1 est réelle, alors $(\lambda_1\omega_1, \lambda_1\omega_2)$ est en fait multiple entier de (ω_1, ω_2) donc $\lambda_1 \in \mathbb{Z}$ et de même $\lambda_2 \in \mathbb{Z}$. Or $\lambda_1\lambda_2 = 1$ et les seuls inversibles de $\mathbb{Z}$ sont ± 1, donc $\lambda = \pm 1$.
Si λ_1 n'est pas réelle, alors $\lambda_2 = \overline{\lambda_1}$ car A est à coefficients réels. On a donc $|\lambda_1| = \lambda_1\lambda_2 = 1$ et $\lambda_1 + \overline{\lambda_1} = \lambda_1 + \dfrac{1}{\lambda_1} \in \mathbb{Z}$.

En examinant les cas possibles, on constate que λ est à prendre parmi $\pm i$ ou $\pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.

c) Donner des exemples de réseaux et d'automorphismes réalisant ces 8 valeurs.

• Dans un réseau Ω de base (ω_1, ω_2), le parallélogramme $[-\omega_1 - \omega_2; -\omega_1; -\omega_2; 0]$ est le symétrique par rapport à l'origine du parallélogramme fondamental du réseau, donc il ne contient que les quatre éléments $-\omega_1-\omega_2, -\omega_1, -\omega_2$ et 0. D'après l'exercice 1, $(-\omega_1, -\omega_2)$ est donc une base de Ω, et ainsi -1 est un automorphisme de Ω, pour Ω quelconque. Clairement, 1 l'est aussi.

• Pour $\pm i$: considérons que le réseau $\mathbb{Z} + i\mathbb{Z}$. Si ℓ est un automorphisme de rapport $\pm i$, alors on a : $\ell(1) = \pm i$, $\ell(i) = \mp 1$ donc ℓ envoie la base $(1, i)$ sur une autre base $(\pm 1, \pm i)$. Ainsi ℓ est bien un automorphisme de $\mathbb{Z} + i\mathbb{Z}$.

• Pour $\pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$: considérons le réseau en nid d'abeille $\mathbb{Z} + \mathbb{Z}j$, avec $j = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Si ℓ est un automorphisme de rapport j, alors on a : $\ell(1) = j$, $\ell(j) = -j - 1$ donc ℓ envoie la base $(1, j)$ sur la base $(j, -j - 1)$ (on vérifie qu'il s'agit bien d'une base grâce à l'exercice 1). Ainsi ℓ est bien un automorphisme de $\mathbb{Z}+j\mathbb{Z}$. De même, si ℓ est de rapport $\overline{j}$, $-j$ ou $-\overline{j}$, il s'agit encore d'un automorphisme de $\mathbb{Z} + j\mathbb{Z}$ grâce à la relation $j^2 + j + 1 = 0$.

3 Généralités sur les fonctions elliptiques

Ω sera un réseau fixé dans $\mathbb{C}$ et (ω_1, ω_2) une base de Ω.
Pour $a \in \mathbb{C}$, on note $\mathcal{P}_a$ le parallélogramme $[a, a + \omega_1, a + \omega_1 + \omega_2, a + \omega_2]$. Pour une fonction elliptique f, on choisira a de telle sorte qu'aucun zéro ni pôle ne soit sur le bord de $\mathcal{P}_a$.

Remarque 3.1 Comme f est méromorphe, elle admet un nombre discret de pôles et de zéros, donc il existe toujours un tel a.

Propriété 3.1 Une fonction elliptique sans pôle est constante.

Démonstration Soit f une fonction elliptique de périodes Ω. Supposons que f n'a pas de pôle.
Ainsi f est une fonction holomorphe sur $\mathbb{C}$ (une fonction entière). De plus, comme f est continue sur le compact $\overline{\mathcal{P}_a}$, elle y est bornée, par un certain M. Par périodicité, on a aussi que pour tout point a de Ω, f est bornée par M sur $\mathcal{P}_a$.
Or les parallélogrammes $\mathcal{P}_a$, pour $a \in \Omega$ pavent le plan (car (ω_1, ω_2) est une base de Ω. Donc f est en fait bornée sur $\mathbb{C}$ tout entier, par M. Par le théorème de Liouville, f est constante. ■

Théorème 3.1 Si f est elliptique alors $\sum_{z \in \mathcal{P}_a} \mathrm{Res}_z(f) = 0$.

Démonstration
Soient f une fonction elliptique de périodes Ω, et a un nombre complexe tel que f n'admette ni zéro ni pôle sur le bord de $\mathcal{P}_a$, que l'on note γ. Comme γ est un lacet simple, que l'on oriente de manière directe, le théorème des résidus assure que :

$$\sum_{z \in \mathcal{P}_a} \mathrm{Res}_z(f) = \frac{1}{2i\pi} \int_\gamma f(\zeta) d\zeta$$

Décomposons γ en quatre chemins correspondant aux quatre côtés de $\mathcal{P}_a$: $\gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ (par exemple, γ_1 suit un côté dirigé par ω_1). Comme f est Ω-périodique, on a : $\forall t \in [0, 1]$,

$$f(\gamma_1(t)) = f(\gamma_3(1 - t)) \text{ et } f(\gamma_2(t)) = f(\gamma_4(1 - t))$$

Ainsi $\int_{\gamma_1} f(\zeta)d\zeta = -\int_{\gamma_3} f(\zeta)d\zeta$, et de même pour γ_2 et γ_4. Finalement $\int_\gamma f(\zeta)d\zeta = 0$, et on a le résultat voulu. ■

Corollaire 3.1 Il n'existe pas de fonction elliptique n'ayant qu'un pôle simple modulo Ω.

Démonstration Le résidu d'une fonction méromorphe en un pôle simple n'est pas nul (sinon le point en question n'est pas un pôle mais une singularité effaçable), donc s'il existait une fonction elliptique f n'ayant qu'un pôle simple z_0 modulo Ω, alors on aurait (pour un a bien choisi) : $res_{z_0}(f) = \sum_{z \in \mathcal{P}_a} \mathrm{res}_z(f) = 0$ ce qui est absurde. ■

Corollaire 3.2 Si f est elliptique alors $\sum_{z \in \mathcal{P}_a} \nu_z(f) = 0$.

Démonstration Avec les mêmes notations que précédemment, le principe de l'argument donne :

$$\frac{1}{2i\pi} \int_\gamma \frac{f'(\zeta)}{f(\zeta)} d\zeta = \sum_{z \in \mathcal{P}_a} \nu_z(f)$$

Or $\dfrac{f'}{f}$ est encore une fonction méromorphe sur $\mathbb{C}$, et Ω-périodique, donc le théorème 3 assure que $\displaystyle\int_\gamma \frac{f'}{f} = 0$, ce qui conclut. ■

Corollaire 3.3 Si f est une fonction elliptique non constante alors pour tout $c \in \hat{\mathbb{C}}$, l'équation $f(z) = c$ a le même nombre de solutions modulo Ω comptées avec multiplicité.

Démonstration
Commençons par le cas où $c = +\infty$. Le nombre de solutions de l'équation $f(z) = c$, comptées avec multiplicité, est alors le nombre de pôles de f modulo Ω (f est méromorphe donc elle n'a pas de singularité essentielle).
Si à présent $c \in \mathbb{C}$, le nombre de solutions de l'équation $f(z) = c$ (comptées avec multiplicité) est égal au nombre de pôles de $g : z \mapsto \dfrac{1}{f(z) - c}$. Mais d'après le corollaire 2, comme g est encore elliptique de période Ω, son nombre de pôles est égal à son nombre de zéros. Or g s'annule exactement sur les pôles de f, donc le nombre de solutions de l'équation $f(z) = c$, comptées avec multiplicité, est égal au nombre de pôles de f. ■

Théorème 3.2 Soit f une fonction elliptique, s'annulant en $a_1, \dots a_d \in \mathcal{P}_a$ et ayant des pôles en $b_1, \dots, b_d \in \mathcal{P}_a$, énumérés avec multiplicité. Alors

$$\sum a_i \equiv \sum b_i \mod \Omega$$

Démonstration On choisit toujours $a \in \mathbb{C}$ tel que f n'aie ni pôles ni zéros sur le bord de $\mathcal{P}_a$, toujours noté γ.
Considérons la fonction $g : z \mapsto \dfrac{zf'(z)}{f(z)}$, et déterminons ses pôles dans P_a.
• Si f a un zéro d'ordre m au point $z_0 \in \mathcal{P}_a$, alors il s'agit d'un pôle de g, d'ordre 1 : en effet, on peut écrire au voisinage de z_0 : $f(z) = (z - z_0)^m \tilde{f}(z)$ avec $\tilde{f}$ holomorphe, donc au voisinage de z_0, $g(z) = z\dfrac{m\tilde{f}(z) + (z - z_0)\tilde{f}'(z)}{(z - z_0)\tilde{f}(z)}$, et ainsi $(z - z_0)g(z) \to mz_0$ quand z tend vers z_0.
• Si f a un pôle d'ordre m au point $z_0 \in \mathcal{P}_a$, on peut écrire au voisinage de z_0 :

$$f(z) = \frac{a_{-m}}{(z - z_0)^m} + ... + \frac{a_{-1}}{(z - z_0)} + \tilde{f}(z)$$

avec $\tilde{f}$ une fonction holomorphe. Ainsi, au voisinage de z_0, $f'(z) = \dfrac{-ma_{-m}}{(z - z_0)^{m+1}} + ... + \dfrac{-a_{-1}}{(z - z_0)^2} + \tilde{f}'(z)$.
Donc z_0 est un pôle d'ordre $m + 1$ de f', et on a $\dfrac{zf'(z)}{f(z)} \xrightarrow[z \mapsto z_0]{} -mz_0$.
Ainsi z_0 est un pôle simple de g.
On peut alors appliquer le théorème des résidus à la fonction g sur le contour γ, simple et bien orienté.

$$\int_\gamma g(\zeta)d\zeta = \sum_{z \in \mathcal{P}_a} \mathrm{Res}_z(g)$$

Or d'après la discussion sur les pôles de g, on a

$$\sum_{z \in \mathcal{P}_a} \mathrm{Res}_z(g) = \sum_{i=1}^{d} a_i - \sum_{j=1}^{d} b_j$$

D'autre part, par périodicité de f, on a :

$$\int_{a+\omega_1}^{a+\omega_1+\omega_2} g(\zeta)d\zeta = \int_{a+\omega_1}^{a+\omega_1+\omega_2} \frac{\zeta f'(\zeta - \omega_1)}{f(\zeta - \omega_1}d\zeta = \int_a^{a+\omega_2} (\zeta + \omega_1)\frac{f'(\zeta)}{f(\zeta)}d\zeta$$

Par le même argument, on a $\displaystyle\int_{a+\omega_2}^{a+\omega_2+\omega_1} g(\zeta)d\zeta = \int_a^{a+\omega_1} (\zeta + \omega_2)\frac{f'(\zeta)}{f(\zeta)}d\zeta$.
Donc

$$\begin{aligned}\int_\gamma g(\zeta)d\zeta &= \int_a^{a+\omega_1} \frac{\zeta f'(\zeta)}{f(\zeta)}d\zeta + \int_{a+\omega_1}^{a+\omega_1+\omega_2} \frac{\zeta f'(\zeta)}{f(\zeta)}d\zeta - \int_{a+\omega_2}^{a+\omega_1+\omega_2} \frac{\zeta f'(\zeta)}{f(\zeta)}d\zeta - \int_a^{a+\omega_2} \frac{\zeta f'(\zeta)}{f(\zeta)}d\zeta \\ &= -\omega_2 \int_a^{a+\omega_1} \frac{f'(\zeta)}{f(\zeta)}d\zeta + \omega_1 \int_a^{a+\omega_2} \frac{f'(\zeta)}{f(\zeta)}d\zeta\end{aligned}$$

Il suffit de montrer que $\dfrac{1}{2i\pi}\displaystyle\int_a^{a+\omega_1} \frac{f'(\zeta)}{f(\zeta)}d\zeta$ et $\dfrac{1}{2i\pi}\displaystyle\int_a^{a+\omega_2} \frac{f'(\zeta)}{f(\zeta)}d\zeta$ sont entiers pour conclure.
Comme f n'a ni pôles ni zéros sur le segment $[a, a + \omega_1]$, par continuité on peut trouver un voisinage V de ce segment sur lequel f n'a ni pôles si zéros. Par un corollaire du théorème de l'application conforme, il existe une fonction holomorphe h sur V telle que $f = \mathrm{e}^h$. Ainsi f'/f est la dérivée de h sur V. Donc :

$$\int_a^{a+\omega_1} \frac{f'(\zeta)}{f(\zeta)}d\zeta = h(a + \omega_1) - h(a)$$

Par périodicité de f, on a : $\mathrm{e}^{h(a+\omega_1)} = \mathrm{e}^{h(a)}$ donc $h(a + \omega_1) - h(a) \in 2i\pi\mathbb{Z}$, ce qui donne bien le résultat voulu. ■

4 La fonction $\wp$ de Weierstrass

Propriété 4.1 Soit Ω un réseau de $\mathbb{C}$. On considère :

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Alors cette série converge uniformément sur tout compact de $\mathbb{C}\setminus\Omega$.

Pour démontrer cette propriété, on commence par montrer le lemme suivant :

Lemme 4.1 Soit Ω un réseau. Alors la série $\displaystyle\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{|\omega|^3}$ est convergente.

Démonstration (du lemme)
Soit (ω_1,ω_2) une base de Ω. Pour tout $n\in\mathbb{N}$, soit $P_n := \{a\omega_1 + b\omega_2,\ \sup(|a|,|b|) = n\}$ le parallélogramme centré en 0 de taille $2n$. Notons aussi $d := min\{|z|,\ z\in P_1\cap\Omega\}$. On procède à une sommation par paquets : pour $n\in\mathbb{N}$, on a :

$$\sum_{\omega\in P_n} \frac{1}{|\omega|^3} \leqslant \frac{\text{nb de points dans } P_n}{(\text{module minimal d'un point de } P_n)^3} = \frac{8n}{(dn)^3}$$

Or la série $\sum \frac{1}{n^2}$ converge (série de Riemann), donc par théorème de sommation par paquets, la série $\displaystyle\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{|\omega|^3}$ converge. ■

Démonstration (de la propriété)
Soit $R>0$. On pose $K := \overline{D(0,R)}$ un compact. Comme Ω est discret, il y a un nombre fini de points du réseau dans $D(0,3R)$. De plus, si $\omega\in\Omega$ est tel que $|\omega|\geqslant 3R$, alors la fonction $z\mapsto \dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}$ est holomorphe sur le voisinage $D(0,2R)$ de K, et pour tout $z\in D(0,2R)$, on a :

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \frac{|z|}{|\omega|^3}\frac{|2-z/\omega|}{|1-z/\omega|} \leqslant \frac{2R}{|\omega|^3}\frac{2+2R/|\omega|}{(1-2R/|\omega|)^2} \leqslant \frac{2R}{|\omega|^3}\frac{2R/3}{(2/3)^2} \leqslant \frac{3R^2}{|\omega|^3}$$

D'après le lemme précédent, la série $\displaystyle\sum_{\substack{\omega\in\Omega\\ |\omega|\geq 3R}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$ converge uniformément sur K.

Ainsi la série de fonctions méromorphes $\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \left(\dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}\right)$ converge uniformément sur tout compact. ■

Définition 4.1 Cette fonction est appelée la fonction $\wp$ de Weierstrass associée au réseau Ω.

Propriété 4.2 La fonction $\wp$ est méromorphe sur $\mathbb{C}$, paire, Ω-périodique. Elle n'a qu'un seul pôle double sans résidu modulo Ω. De plus, il existe $g_2, g_3\in\mathbb{C}$ (dépendant de Ω) tels que

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

Démonstration
• On a déjà montré dans la propriété précédente que $\wp$ est méromorphe sur $\mathbb{C}$. Ensuite, comme Ω est symétrique par rapport à l'origine, on a :

$$\forall z\in\mathbb{C}\setminus\Omega,\ \wp(-z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \wp(z)$$

Ainsi $\wp$ est paire.

De même, un changement d'indice dans la somme montre que pour $\omega_1\in\Omega$ et $z\in\mathbb{C}\setminus\Omega$,

$$\wp(z+\omega_1) = \wp(z)$$

Ainsi $\wp$ est Ω-périodique.
• Pour la suite, notons $S(z) = \displaystyle\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$. Pour $\omega\in\Omega$, $\omega\neq 0$, la fonction $z\mapsto \dfrac{1}{(z-\omega)^2} - \dfrac{1}{\omega^2}$ possède un unique pôle double en ω, donc la somme $S(z)$ a ses pôles sur les points non nuls du réseau, et uniquement sur ces

points. Ainsi $\wp$ a un unique pôle modulo Ω, d'ordre 2, qui correspond à sa partie en $1/z^2$. On peut calculer le résidu de $\wp$ en 0 :

$$\mathrm{Res}_0(\wp) = \lim_{z\to 0}\left(\frac{d}{dz}(z^2 wp(z))\right) = \lim_{z\to 0}\left(\frac{d}{dz}\left(1+z^2 S(z)\right)\right)$$

Or la fonction $z \mapsto S(z)$ est holomorphe au voisinage de zéro, donc $\lim_{z\to 0}(\frac{d}{dz}(z^2 S(z))) = 0$. Ainsi $\mathrm{Res}_0(\wp) = 0$.

Calculons à présent la dérivée de $\wp$. D'après la démonstration de la propriété 2, on a que la dérivation de S peut se faire terme à terme :

$$\left(\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)\right)' = -2\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{(z-\omega)^3}$$

Ainsi, $\wp'(z) = -\frac{2}{z^3} + S'(z)$.
De plus, comme S est holomorphe au voisinage de 0, on peut la développer en série entière au voisinage de 0 : $S(z) = a_0 + a_1 z + a_2 z^2 + ...$ Si (ω_1, ω_2) est une base de Ω, on peut expliciter un voisinage pour lequel ce développement est valide : la parallélogramme $\mathcal{P} := \left[-\frac{3}{4}\omega_2 - \frac{3}{4}\omega_1; -\frac{3}{4}\omega_2 + \frac{3}{4}\omega_1; \frac{3}{4}\omega_2 + \frac{3}{4}\omega_1; \frac{3}{4}\omega_2 - \frac{3}{4}\omega_1\right]$. On verra plus loin l'utilité de cette explicitation.
Comme S est paire et $S(0) = 0$, les coefficients impairs ainsi que le terme constant sont nuls : $S(z) = a_2 z^2 + a_4 z^4 + ...$
On obtient ainsi un développement de Laurent de $\wp$ en 0 : $\wp(z) = \frac{1}{z^2} + a_2 z^2 + a_4 z^4 + ...$ On dérive puis on passe au carré :

$$(\wp'(z))^2 = \left(\frac{-2}{z^3} + 2a_2 z + 4a_4 z^3 + ...\right)^2 = \frac{4}{z^6} - \frac{8a_2}{z^2} - 16a_4 + b_2 z^2 + b_4 z^4 + ...$$

Où les b_{2i} sont des complexes. D'autre part, si on élève au cube le développement de Laurent de $\wp$, on obtient :

$$(\wp(z))^3 = \frac{1}{z^6} + \frac{3a_2}{z^2} + 3a_4 + c_2 z^2 + c_4 z^4 + ...$$

Où les c_{2i} sont des complexes. Donc :

$$(\wp'(z))^2 - 4\wp(z)^3 + 20a_2\wp(z) = -28a_4 + d_2 z^2 + d_4 z^4 + ...$$

Avec d_{2i} des complexes. La fonction $(\wp')^2 - 4\wp^3 + 20a_2\wp + 28a_4$ est donc holomorphe sur $\mathcal{P}$, car développable en série entière. De plus, elle conserve la propriété de périodicité de $\wp$. Or on a choisi $\mathcal{P}$ de telle sorte que $\bigcup_{\omega\in\Omega}(\mathcal{P}+\omega) = \mathbb{C}$, ce qui permet d'étendre l'holomorphie de la fonction $(\wp')^2 - 4\wp^3 + 20a_2\wp + 28a_4$ à $\mathbb{C}$ tout entier. Enfin, comme cette fonction est bornée sur $\mathcal{P}$, elle est bornée sur $\mathbb{C}$, donc constante par théorème de Liouville. Elle s'annule en 0 par construction, donc elle est finalement nulle :

$$(\wp')^2 = 4\wp^3 - 20a_2\wp - 28a_4$$

En posant $g_2 = 20a_2$ et $g_3 = 20a_4$, on a le résultat. On peut même calculer a_2 et a_4 :

$$a_2 = \frac{S''(0)}{2} = 3\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^4} \text{ et } a_4 = \frac{S^{(4)}(0)}{4!} = 5\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^6}$$

Ainsi $g_2 = 60\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^4}$ et $g_3 = 140\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^6}$. ■

Notation 4.1 On note $G_2 = \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^4}$ et $G_3 = \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}}\frac{1}{\omega^6}$ puis $g_2 = 60G_2$ et $g_3 = 140G_3$

Remarque 4.1 La fonction doublement périodique que nous avions construit géométriquement en introduction est un cas particulier de la fonction de Weierstrass pour le réseau $a\mathbb{Z} + ib\mathbb{Z}$ avec $a, b \in \mathbb{R}$.

Remarque 4.2 On en déduit que si $f = \wp^{-1}$ alors $f'(w) = \frac{1}{\sqrt{4w^3 - g_2 w - g_3}}$

Théorème 4.1 Le corps des fonctions elliptiques de période Ω est $\mathbb{C}(\wp, \wp')$ où $\wp$ est la fonction de Weierstrass associée au réseau.

Remarque 4.3 La fonction $e^{\wp}$ est Ω-périodique mais pas méromorphe sur $\mathbb{C}$ (cf exercice 2 du TD sur les singularités isolées pour une preuve). Elle n'est donc pas elliptique.

Pour démontrer le théorème, on s'appuie sur les trois lemmes suivants :

Notation 4.2 Soit $z \in \mathcal{P}_0$. On note z^* le représentant modulo Ω de $-z$ dans $\mathcal{P}_0$.

Lemme 4.2 Soit (ω_1, ω_2) une base de Ω.
Les seuls nombres complexes dans $\mathcal{P}_0$ vérifiant $z = z^*$ sont 0, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$.

Démonstration (du lemme 2)
On a $0 = -0$, $-\frac{\omega_i}{2} = \frac{\omega_i}{2} - \omega_i$ donc il est clair que 0, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$ sont égaux au représentant de leur opposé dans $\mathcal{P}_0$.
Inversement, si $z \in \mathcal{P}_0$ vérifie $z = z^*$, alors il existe $n_1, n_2 \in ZZ$ tels que $2z = n_1\omega_1 + n_2\omega_2$, et comme $2z$ est dans le parallélogramme $[0, 2\omega_1, 2\omega_2, 2\omega_1 + 2\omega_2]$, on doit avoir $0 \leq n_1 \leq 1$ et $0 \leq n_2 \leq 1$, donc z est parmi 0, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$. ■

Lemme 4.3 Les nombres $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$ sont les zéros d'ordre 1 de la fonction $\wp'$ modulo Ω.

Démonstration (du lemme 3)
Par périodicité de $\wp'$ puis imparité, on a : $\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(-\frac{\omega_1}{2}\right) = -\wp'\left(\frac{\omega_1}{2}\right)$. Ainsi $\frac{\omega_1}{2}$ annule $\wp'$, et le même argument est valable pour $\frac{\omega_2}{2}$ et $\frac{\omega_1+\omega_2}{2}$.
Enfin, si on se place sur le parallélogramme $\mathcal{P} := \left[-\frac{\omega_1}{4} - \frac{\omega_2}{4}; \frac{3\omega_1}{4}; \frac{3\omega_2}{4}; \frac{3\omega_1}{4} + \frac{3\omega_2}{4}\right]$, alors la fonction $\wp'$ n'a ni zéros ni pôles sur le bord de $\mathcal{P}$ et on peut lui appliquer le corollaire 2. Dans ce parallélogramme, $\wp'$ a un unique pôle d'ordre 3, en 0, et les trois zéros que nous avons exhibé. Nécessairement, ces trois zéros sont d'ordre 1, et ce sont les seuls modulo Ω. ■

Lemme 4.4 Soit f une fonction elliptique paire de période Ω. Alors, pour tout $z \in \mathcal{P}_0$,

- $f(z) = f(z^*)$ et $\nu_z(f) = \nu_{z^*}(f)$
- Si $z = z^*$, alors $\nu_z(f)$ est paire.

Démonstration (du lemme 4)
• Comme f est paire, $f(z) = f(-z)$ et comme f est périodique, $f(-z) = f(z^*)$. Par transitivité, $f(z) = f(z^*)$.
De plus, comme f est holomorphe au voisinage de z (car $z \in \mathcal{P}_0$), on peut écrire, pour w assez proche de z :

$$f(w) = a_0 + a_1(w-z) + a_2(w-z)^2 + ... + a_{n-1}(w-z)^{n-1} + a_n(w-z)^n + ...$$

avec $a_0 = ... = a_{n-1} = 0$ et $a_n \neq 0$ (i.e. n est la valuation de f en z).
Comme f est paire, on a (pour w assez proche de z) : $f(-w) = f(w) = a_0 + a_1(w-z) + a_2(w-z)^2 + ... + a_{n-1}(w-z)^{n-1} + a_n(w-z)^n + ... = a_0 - a_1(-w+z) + a_2(-w+z)^2 + ... + (-1)^{n-1}a_{n-1}(-w+z)^{n-1} + (-1)^n a_n(-w+z)^n + ...$ Donc on a identifié le développement analytique de f au voisinage de $-z$, et par périodicité, il s'agit du même développement que celui de f en z^*. Donc la valuation en $-z$ et celle en z^* sont égales à n, la valuation en z.

• Supposons que $z = z^*$. Alors, pour w assez proche de z (donc de z^*) :

$$a_0 + a_1(w-z) + a_2(w-z)^2 + ... + a_{n-1}(w-z)^{n-1} + a_n(w-z)^n + ... = a_0 - a_1(w-z) + a_2(w-z)^2 + ... + (-1)^{n-1}a_{n-1}(w-z)^{n-1} + (-1)^n a_n($$

Par unicité du développement en série entière, $a_i = (-1)^i a_i$ pour tout $i \in \mathbb{N}$, et en particulier, tous les coefficients impairs sont nuls, donc la valuation de f en z est paire. ■

Démonstration (du théorème)
Soit f une fonction elliptique de période Ω. On peut se ramener au cas où f est paire, en remarquant qu'on peut séparer f en une partie paire f_p et une partie impaire f_i, qui devient paire lorsqu'on la multiplie par $\wp'$. Supposons donc que f soit paire.
On note $a_1, a_2, ..., a_d$ les zéros de f dans $\mathcal{P}_0$ et $b_1, ..., b_d$ ses pôles dans $\mathcal{P}_0$.
Pour tout $i \in [\![1, d]\!]$, si $a_i = a_i^*$ (resp. $b_i = b_i^*$) on note r_i (resp. s_i) la valuation de f en a_i (resp. en b_i) divisée par 2, et si $a_i \neq a_i^*$ (resp. $b_i \neq b_i^*$), on note r_i (resp. s_i) la valuation de f en a_i (resp. en b_i). Ce sont des entiers d'après le lemme 4.
Posons

$$g(z) = \frac{\prod_{i=1}^d (\wp(z) - \wp(a_i))^{r_i}}{\prod_{i=1}^d (\wp(z) - \wp(b_i))^{s_i}}$$

La fonction g est elliptique de période Ω. De plus, si $a_i = a_i^*$, d'après les lemmes 2 et 3, la fonction $z \mapsto \wp(z) - \wp(a_i)$ a un zéro d'ordre 2 en a_i, donc la fonction g a un zéro d'ordre $2 \times r_i = \nu_{a_i}(f)$ en a_i. Et si $a_i \neq a_i^*$, la fonction

$z \mapsto \wp(z) - \wp(a_i)$ a un zéro d'ordre 1 en a_i, donc g a un zéro d'ordre $r_i = \nu_{a_i}(f)$ en a_i. De même, g a exactement les mêmes pôles que f, avec les mêmes ordres. Ainsi, f/g est une fonction elliptique qui n'a pas de pôle sur $\mathcal{P}_a$: en effet, ses pôles potentiels seraient les zéros de g et les pôles de f, mais les zéros de g sont annihilés par les zéros de f et les pôles de f sont annihilés par les pôles de g... D'après la propriété 1, f/g est constante égale à un certain c.
On vient de montrer que $f = cg$ donc que f est bien une fraction rationnelle en $\wp$. ■

5 interprétation géométrique

La fonction $\wp$ a des propriétés semblables aux fonctions circulaires (exp, cos etc.)

L'équation différentielle du cosinus permet de voir que l'application $\theta \to (\cos\theta, \sin\theta)$ paramètre le cercle. L'équation différentielle de la fonction $\wp$ s'interprète de la manière suivante :

La fonction

$$\begin{array}{rccc} \Psi : \mathbb{C} - \Omega & \to & \mathbb{C}^2 \\ z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

prend ses valeurs dans la cubique :

$$\mathscr{C} = \{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2 x - g_3\}$$

Lemme 5.1 La cubique est lisse si et seulement si $g_2^3 - 27g_3^2 \neq 0$

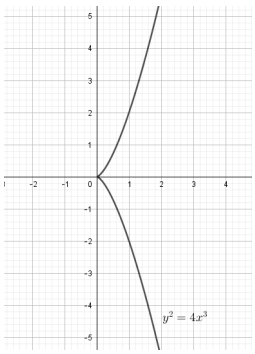
Démonstration La cubique est lisse si et seulement si elle ne possède pas de singularité. Or une singularité est un point (x, y) de la courbe qui annule les dérivées partielles premières du polynôme définissant la courbe, ici $P = Y^2 - 4X^3 + g_2 X + g_3$. Si (x, y) est une singularité de $\mathscr{C}$, alors :

$$\begin{cases} y^2 = 4x^2 - g_2 x - g_3 \\ 2y = 0 \\ -12x^2 + g_2 = 0 \end{cases}$$

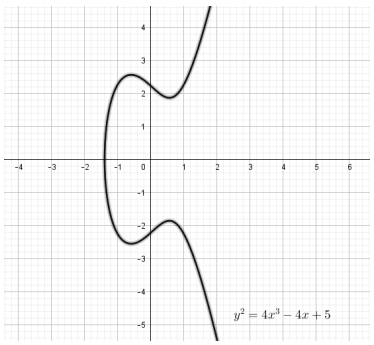
Ainsi $y = 0$ et x est racine double de $4X^3 - g_2 X - g_3$. Inversement, tout couple (x, y) vérifiant ces conditions est une singularité de la courbe $\mathscr{C}$. Donc la courbe n'a pas de singularité si et seulement si le polynôme $4X^3 - g_2 X - g_3$ n'a que des racines simples, si et seulement si son discriminant $\Delta = g_2^3 - 27g_3^2$ est non nul.
Finalement, $\mathscr{C}$ est lisse si et seulement si $\Delta \neq 0$. ■

Pour différentes valeurs réelles de g_2 g_3, dessinez (à la main ou avec votre logiciel préféré) la trace réelle de la courbe :

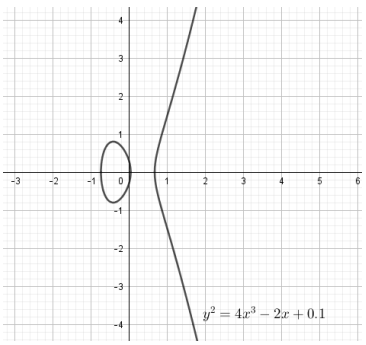
$$\mathbb{R}\mathscr{C} = \{(x, y) \in \mathbb{R}^2 : y^2 = 4x^3 - g_2 x - g_3\}$$



(e) $g_2 = 0$ et $g_3 = 0$



(f) $g_2 = 4$ et $g_3 = -5$



(g) $g_2 = 2$ et $g_3 = -0.1$

Théorème 5.1 Soit Ω un réseau de fonction $\wp$ et de cubique $\mathscr{C}$. Alors $\mathscr{C}$ est lisse, l'application Ψ définie plus haut induit une identification $(\mathbb{C} - \Omega)/\Omega$ avec $\mathscr{C}$ et $\mathbb{C}/\Omega$ avec $\hat{\mathscr{C}}$.

Démonstration
Montrons que $\Psi : \mathbb{C} - \Omega \to \mathscr{C}$ est surjective. Comme $\wp$ est elliptique et admet un pôle d'ordre 2 modulo Ω, d'après le corollaire 3, l'équation $\wp(z) = c$ admet deux solutions modulo Ω pour tout $c \in \mathbb{C}$. Donc si $(x, y) \in \mathscr{C}$, il existe $z \in \mathbb{C}$ tel que $\wp(z) = x$. De plus, d'après la propriété 3, $\wp'(z)$ est une racine carrée de $4x^3 - g_2 x - g_3$, donc $\wp'(z) = \pm y$. Si $\wp'(z) = y$, on a montré la surjectivité. Si $\wp(z) = -y$, on utilise l'imparité de $\wp'$: $\wp'(-z) = y$, et on a aussi $\wp(-z) = \wp(z) = x$, d'où la surjectivité de Ψ.
De plus, Ψ est Ω-périodique, donc elle induit une application surjective $\tilde{\Psi}$ entre $(\mathbb{C} - \Omega)/\Omega$ et $\mathscr{C}$. Montrons que $\tilde{\Psi}$ est injective : soient $z_1, z_2 \in \mathbb{C} - \Omega$ tels que $\tilde{\Psi}(\overline{z_1}) = \tilde{\Psi}(\overline{z_2})$ (où $\overline{z}$ désigne la classe d'équivalence de z dans $(\mathbb{C} - \Omega)/\Omega$). En particulier, $\wp(z_1) = \wp(z_2)$, donc z_1 est solution de l'équation $\wp(z) = \wp(z_2)$. Mais deux solutions évidentes de cette

équation sont z_2 et $-z_2$ (ce sont d'ailleurs les deux seules solutions modulo Ω d'après le corollaire 3). Si $z_2 = -z_2$ modulo Ω, alors on obtient $\overline{z_1} = \overline{z_2}$ donc $\tilde{\Psi}$ est injective. Si $z_2 \neq -z_2$ modulo Ω, on utilise la deuxième équation provenant de l'égalité $\tilde{\Psi}(\overline{z_1}) = \tilde{\Psi}(\overline{z_2})$: on a en effet $\wp'(z_1) = \wp'(z_2)$. Si z_1 était égal à $-z_2$ modulo Ω, on aurait alors : $\wp'(z_1) = -\wp'(z_2)$ par imparité de $\wp'$, donc $-\wp'(z_2) = \wp'(z_2)$, puis $\wp'(z_2) = 0$. D'après le lemme 4, $z_2 \in \left\{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\right\}$. Mais d'après le lemme 3, on devrait donc avoir $z_2 = -z_2$ modulo Ω. Ainsi $\overline{z_1} = \overline{z_2}$ et $\tilde{\Psi}$ est injective.

Par conséquent, l'application $\tilde{\Psi}$ identifie la courbe $\mathscr{C}$ à $(\mathbb{C} - \Omega)/\Omega$. Il suffit ensuite de compactifier $\mathscr{C}$ pour autoriser l'envoi des points de Ω sur l'infini et prolonger l'identification à $\mathbb{C}/\Omega$ vers $\hat{\mathscr{C}}$.

Montrons enfin que $\mathscr{C}$ est lisse. D'après le lemme précédent, il suffit de montrer que pour tout réseau Ω, on a $g_2^3 - 27g_3^2 \neq 0$, avec $g_2 = 60 \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{\omega^4}$ et $g_3 = 140 \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{\omega^6}$.
Soit Ω un réseau de base (ω_1, ω_2). Notons $\omega_3 = \omega_1 + \omega_2$. On a vu dans le lemme 4 que les $\frac{\omega_i}{2}$, pour $i \in \{1,2,3\}$ sont les zéros modulo Ω de $\wp'$. Posons alors $e_i = \wp\left(\frac{\omega_i}{2}\right)$. Les fonctions $z \mapsto \wp(z) - e_i$, pour $i \in \{1,2,3\}$, ont donc un zéro d'ordre 2 en $\frac{\omega_i}{2}$. Considérons la fonction

$$f : z \longmapsto 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Cette fonction a trois zéros d'ordre 2 modulo Ω, et elle est elliptique, donc par le théorème 4, elle doit avoir 6 pôles modulo Ω (comptés avec multiplicité). Or comme $\wp$ a un pôle d'ordre 2 en zéro, la fonction f possède un pôle d'ordre $3 \times 2 = 6$ en zéro, qui est donc son seul pôle.
Ainsi la fonction f possède les mêmes zéros et les mêmes pôles que $(\wp')^2$ modulo Ω. Ces deux fonctions ne diffèrent donc que d'une constante :

$$(\wp')^2(z) = 4c(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Donc les racines de $4X^3 - g_2X - g_3$ sont les e_i. Enfin, d'après le corollaire 3, l'équation $\wp(z) = e_1$ possède 2 solutions modulo Ω comptées avec multiplicité (en effet $\wp$ a un unique pôle d'ordre 2 modulo Ω). Or $\frac{\omega_1}{2}$ est déjà une solution d'ordre 2 pour cette équation, donc c'est la seule solution, ce qui implique que e_1 est distinct de e_2 et $_3$, et de même e_2 est distinct de e_3 donc les racines du polynôme $4X^3 - g_2X - g_3$ sont simples, ce qui implique que la courbe est lisse.■

L'application $(\cos, \sin)$ réalise le quotient de $\mathbf{R}$ (ou $\mathbb{C}$) par $2\pi\mathbf{Z}$; c'est un morphisme de groupe dont l'image est $\mathbb{S}^1$ (ou $\mathbb{C}^*$). De manière analogue, le théorème précédent dit que le compactifié d'Alexandrov de $\mathscr{C}$: $\hat{\mathscr{C}} = \mathscr{C} \cup \{\infty\}$ a une structure de groupe dont l'élément neutre est ∞.

Cette loi de groupe a une interprétation géométrique.

Nous dirons que les droites complexes verticales $x = cst$ passent par ∞.

Lemme 5.2 Une droite complexe de $\mathbb{C}^2$ coupe la cubique en au plus trois points. Si elle coupe $\mathscr{C}$ en deux points seulement alors soit elle est tangente à $\mathscr{C}$, soit elle passe par ∞ . Si elle coupe $\mathscr{C}$ en un seul point alors soit ce point est un point d'inflexion de $\mathscr{C}$ soit la droite est une tangente passant par ∞.

Démonstration
• Soit D une droite affine du plan complexe $\mathbb{C}^2$. Montrons que cette droite coupe la courbe $\mathscr{C}$ en au plus trois points. (C'est une conséquence du théorème de Bézout sur les courbes algébriques, mais on va donner ici une démonstration "à la main" beaucoup plus élémentaire). Supposons donc que la droite D intersecte $\mathscr{C}$ en deux points A et B. Notons $\alpha x + \beta y + \delta = 0$ une équation de la droite D. Comme A (resp. B) est sur la courbe $\mathscr{C}$, paramétrisée par la fonction Ψ, il existe $z_1 \in \mathbb{C}$ (resp. $z_2 \in \mathbb{C}$) tel que $A = \Psi(z_1) = (\wp(z_1), \wp'(z_1))$ (resp. $B = \Psi(z_2) = (\wp(z_2), \wp'(z_2))$).
Les nombres z_1 et z_2 sont donc des zéros de la fonction $\alpha\wp + \beta\wp' + \delta$. Or cette fonction est elliptique et possède un unique pôle d'ordre 3 en zéro modulo Ω, d'après l'étude de la fonction de Weierstrass à la section 4. Donc elle possède trois zéros (avec multiplicité) modulo Ω, c'est-à-dire qu'il existe au plus un autre point $C \in \mathbb{C}^2$ qui soit sur la droite D et sur la courbe $\mathscr{C}$.

• Précisons un peu : avec les mêmes notations, supposons que la droite D coupe la courbe $\mathscr{C}$ en deux points distincts exactement, A et B. Supposons que cette droite ne passe pas par l'infini (c'est-à-dire que dans l'équation de la droite, $\beta \neq 0$). Comme il faut tout de même que la fonction $\alpha\wp + \beta\wp' + \delta$ ait trois zéros modulo Ω pour compenser son pôle en 0 (en effet, $\beta \neq 0$ donc le pôle en zéro est un pôle triple), l'un des deux points est un zéro d'ordre 2, prenons par exemple z_1. Ainsi la restriction de la cubique à la droite D possède un zéro d'ordre 2 en A, donc D est tangente à la courbe au point A.
Donc si la droite coupe la courbe en deux points distincts, alors elle est soit tangente à la courbe, soit elle passe par l'infini.

De même, si la droite coupe la courbe en un seul point A, et qu'elle ne passe pas par l'infini, alors la restriction

de la cubique à la droite D possède un zéro d'ordre 3 en A, ce qui signifie que non seulement la droite est tangente à la courbe, mais en plus que le point A est un point d'inflexion de la courbe. Si la droite passe par l'infini, alors il y a zéro d'ordre 2 en A (pour compenser le pôle d'ordre 2 en 0 de la fonction $\alpha\wp + \delta$), donc D est tangente à la courbe en A. ■

Remarque 5.1 Trois points (x_1, y_1), (x_2, y_2), (x_3, y_3) sont alignés si et seulement si

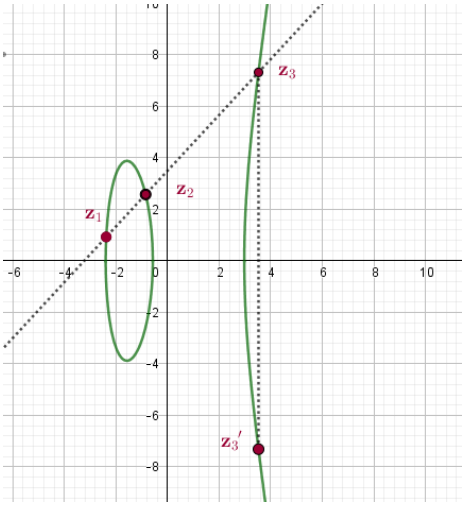
$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ 1 & 1 & 1 \end{vmatrix} = 0$$

Théorème 5.2 (La loi de groupe) Si $z_1, z_2, z_3 \in \mathbb{C} - \Omega$ tels que $z_1 + z_2 + z_3 \equiv 0 \mod \Omega$ alors

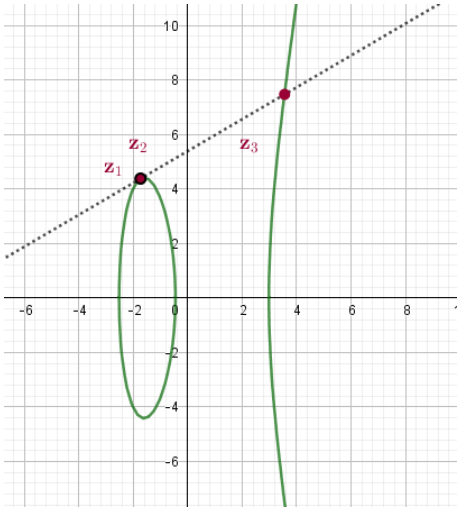
$$\begin{vmatrix} \wp(z_1) & \wp(z_2) & \wp(z_3) \\ \wp'(z_1) & \wp'(z_2) & \wp'(z_3) \\ 1 & 1 & 1 \end{vmatrix} = 0$$

Remarque 5.2 En particulier, $\wp(z_1 + z_2)$ s'exprime rationnellement en fonction de $\wp(z_1), \wp(z_2), \wp'(z_1), \wp'(z_2)$ comme c'est le cas pour $\cos(z_1 + z_2)$ (on le démontre dans l'exercice 5, plus bas).

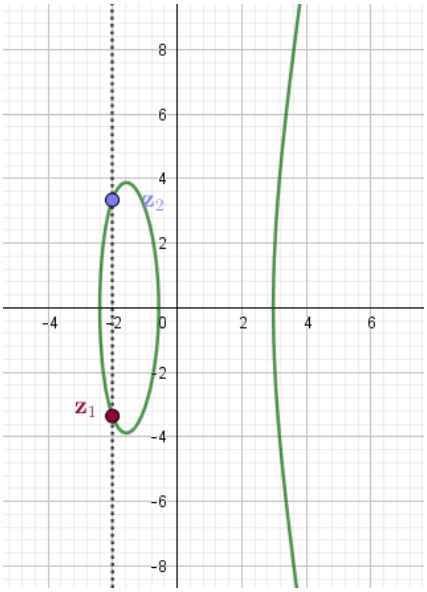
Illustration du théorème d'addition et des cas dégénérés :



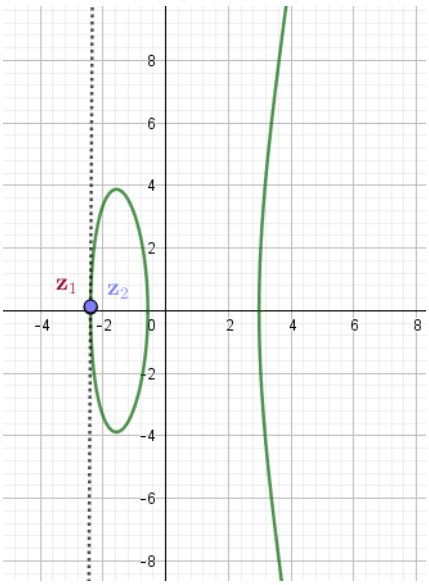
(h) Cas général



(i) $z_1 = z_2$



(j) $z_3 \in \Omega$



(k) $z_1 = z_2$ et $z_3 \in \Omega$

On constate que lorsque $z_1 = z_2$, la droite est une tangente à la courbe. Lorsque $z_3 \in \Omega$, la droite passe par l'infini, et elle ne coupe la courbe qu'en deux points. Lorsque ces deux contraintes sont vérifiées en même temps ($z_1 = z_2$ et $z_3 = \infty$), la droite ne coupe la courbe qu'en un seul point, et elle coïncide avec la tangente en ce point.

Exercice 5 : Formules d'addition et de duplication
Soient trois nombres complexes z_1, z_2 et z_3 tels que $z_1 + z_2 + z_3 \equiv 0[\Omega]$. On note A_i le point $(\wp(z_i), \wp'(z_i))$ pour $i = 1, 2, 3$, et on suppose qu'aucun des z_i n'est sur le réseau Ω de sorte que la droite D passant par A_1, A_2 et A_3 possède une équation réduite $y = ax + b$.
Question 1 : *Montrer que* $4x^3 - a^2x^2 - (2ab + g_2)x - (b^2 + g_3)$ *s'annule en* $\wp(z_1)$, $\wp(z_2)$ *et* $\wp(z_3)$.

Soit $i \in \{1, 2, 3\}$. Comme A_i est à l'intersection de la cubique $\mathscr{C}$ et de la droite D, ses coordonnées (x_i, y_i) vérifient :

$$y_i^2 = 4x_i^3 - g_2x_i - g_3 \text{ et } y_i = ax_i + b$$

En reportant la deuxième égalité dans la première, on obtient :

$$a^2x_i^2 + b^2 + 2abx_i = 4x_i^3 - g_2x_i - g_3$$

Or $x_i = \wp(z_i)$ donc on a le résultat voulu.

Questions 2 et 3 : *En déduire que* $4(\wp(z_1) + \wp(z_2) + \wp(z_3)) = a^2$, *puis que*

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

Les nombres $\wp(z_1)$, $\wp(z_2)$ et $\wp(z_3)$ sont les racines du polynôme unitaire $x^3 - \frac{a^2}{4}x^2 - \frac{(2ab + g_2)}{4}x - \frac{(b^2 + g_3)}{4}$, donc par les relations coefficients-racines, on a bien $\wp(z_1) + \wp(z_2) + \wp(z_3) = \frac{a^2}{4}$.
De plus, par parité de $\wp$, on a $\wp(z_1 + z_2) = \wp(-z_3) = \wp(z_3)$, donc $\wp(z_1 + z_2) + \wp(z_1) + \wp(z_2) = \left(\frac{a}{2}\right)^2$.
La coefficient a est le coefficient directeur de la droite passant par A_1 et A_2 donc il vaut $\frac{y_1 - y_2}{x_1 - x_2} = \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}$, d'où le résultat.

Question 4 : *Déterminer une fraction rationnelle* R *telle que* $\wp(2z) = R(\wp(z))$.

Si on fait tendre z_1 vers z_2, la droite D tend vers la tangente à la cubique $\mathscr{C}$ en A_1 (d'après le lemme 7). À la limite, le coefficient directeur de la droite D coïncide donc avec la pente de la tangente, qui vaut $-\frac{12\wp(z_1) - g_2}{2\wp(z_1)}$. En reportant dans l'équation de la question 3, on obtient :

$$\wp(2z_1) = \frac{1}{16}\frac{(12\wp(z_1) - g_2)^2}{4\wp(z_1)^3 - g_2\wp(z_1) - g_3} - 2\wp(z_1)$$

Références

[1] Lars Ahlfors. *Complex Analysis.* 1979.
[2] Michèle Audin. *Analyse complexe.* Notes de cours, 2012.
[3] Yves Hellegouarch. *Invitation to the Mathematics of Fermat-Wiles.*
[4] Serge Lang. *Complex Analysis.* Springer, 1999.
[5] Wikipédia. *Divers articles, sur les courbes algébriques, la fonction de Weierstrass, le discriminant d'un polynôme de degré 3...*