Rapport de stage 2A

Courbes cubiques projectives et tores complexes

Aude Le Gluher
Encadrant : M. Stéphane Lamy

16 mai 2016 — 26 juin 2016

Table des matières

Introduction 3
1. Courbes elliptiques 3
1.1. Définitions 3
1.2. Simplification d'une courbe elliptique 4
1.3. Loi de groupe 9
1.4. j-invariant et courbes isomorphes 10
2. Fonctions elliptiques 11
2.1. Définition et quelques propriétés 11
2.2. La fonction $\wp$ de Weierstrass 13
2.3. Propriétés de la fonction $\wp$ de Weierstrass 14
3. Du réseau à la courbe 16
3.1. Où l'on découvre une utilité à $\wp$ 16
3.2. Holomorphie de la réciproque 18
3.3. Application : loi de groupe sur une courbe elliptique 20
4. De la courbe au réseau 21
4.1. j-invariant d'un réseau 21
4.2. Encodage des réseaux de $\mathbf{C}$ 24
4.3. Tout complexe est le j-invariant d'un réseau 29
Conclusion 33
Références 34

Je tiens à remercier M. Dominique Cerveau et M. Stéphane Lamy ; le premier pour m'avoir mise en contact avec le second et le second pour avoir eu la patience de m'encadrer durant ce mois et demi de stage. Merci également à Laura Brillon pour l'aide dans les démarches permettant d'accéder à la cantine et à Kévin François pour m'avoir accueillie dans son bureau.

Introduction

Ce travail s'intéresse à certaines courbes projectives ; à savoir les courbes elliptiques. Son but est d'établir des liens - dont la nature est explicitée ci-après - entre l'ensemble des courbes elliptiques sur $\mathbf{C}$ et celui des quotients de $\mathbf{C}$ par un réseau. Une fois ces liens établis, on espère qu'ils aideront à traduire les problèmes compliqués dans l'un des domaines en des problèmes plus simples dans l'autre.

1. Courbes elliptiques

Dans toute cette partie, $\mathbf{K}$ est un corps. On suppose connue la construction de plan projectif $\mathbf{P}^2(\mathbf{K})$, la notion de coordonnées homogènes et le théorème de Bézout.

1.1. **Définitions.**

Définition 1.1. *(Courbe projective)*

On définit une courbe projective plane comme étant un élément de l'ensemble suivant : $\bigcup_{d\in\mathbf{N}^\star} \mathbf{K}_d[X,Y,Z]/\sim$ *où* $\mathbf{K}_d[X,Y,Z]$ *est l'ensemble des polynômes homogènes de degré* d *en trois variables et* $\sim$ *est une relation d'équivalence sur cet ensemble telle que* $F \sim G \Leftrightarrow \exists\lambda \in \mathbf{K}^\star, F = \lambda G$.

Autrement dit, une courbe projective est la donnée d'un polynôme homogène non constant en trois variables, en considérant que deux polynômes proportionnels représentent la même courbe.

Remarques :

- Dans la suite, on confond "courbe projective" et "polynôme homogène non constant en trois variables" (autrement dit, on confond classe d'équivalence et représentant de cette classe)
- Si $F \in \mathbf{K}_d[X,Y,Z]$ est une courbe projective, le degré de cette courbe est celui de F, à savoir d. Dans la suite, on s'intéresse aux courbes projectives de degré trois qu'on nommera aussi cubiques projectives.
- On définit de même une courbe affine plane comme étant un polynôme non constant de $\mathbf{K}[X,Y]$.
- Pour passer d'une courbe affine F à sa version projective, on homogénéise F en $\tilde{F}(X,Y,Z) = Z^{\deg(F)}F(\frac{X}{Z},\frac{Y}{Z})$. Réciproquement, pour passer d'une courbe projective $\tilde{F}$ à la courbe affine sous-jacente, on déshomogénéise $\tilde{F}$ en $F(X,Y) = \tilde{F}(X,Y,1)$. Grâce à ces procédés, les définitions (projectives) suivantes ont toutes leur pendant affine.

Définition 1.2. *(Points d'une courbe)*

Soit $F \in \mathbf{K}_d[X,Y,Z]$ *une courbe projective. L'ensemble des* $\mathbf{K}$*-points de* F *est* $F(\mathbf{K}) = \{[x:y:z] \in \mathbf{P}^2(\mathbf{K}) | F(x,y,z) = 0\}$

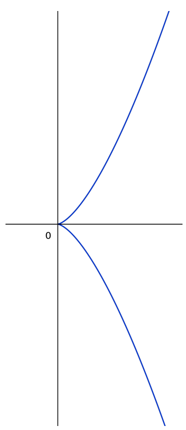
Remarque : Cet ensemble est bien défini. En effet, si (x,y,z) et $(\lambda x,\lambda y,\lambda z)$ (où $\lambda \in \mathbf{K}^\star$) sont deux représentants du même point projectif, comme P est un polynôme homogène, $F(x, y, z) = 0 \Leftrightarrow F(\lambda x, \lambda y, \lambda z) = 0$. De plus, cet ensemble ne dépend pas non plus du représentant choisi pour F.

Définition 1.3. *(Point singulier)*
Soit $F \in \mathbf{K}_d[X, Y, Z]$ une courbe projective et $P = [x_0 : y_0 : z_0] \in F(\mathbf{K})$ un $\mathbf{K}$-point sur cette courbe. On dit que P est un point singulier si et seulement si $\operatorname{grad}(F)(P) = 0$. *Sinon, on dit que P est non singulier et la tangente à F en P est la droite (courbe projective de degré 1)*

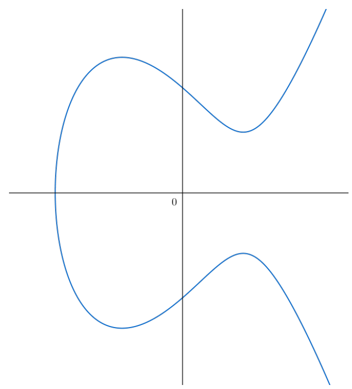
$$L = \frac{\partial F}{\partial X}(P)(X - x_0) + \frac{\partial F}{\partial Y}(P)(Y - y_0) + \frac{\partial F}{\partial Z}(P)(Z - z_0)$$

Si tout point de $F(\overline{\mathbf{K}})$ est non singulier, alors on dit que la courbe F est lisse. Sinon, on dit qu'elle est singulière.

Exemples



La courbe affine $y^2 - x^3$ est singulière.



La courbe affine $y^2 - x^3 + 3x - 3$ est lisse.

Il est important de considérer la clôture algébrique de $\mathbf{K}$ dans la définition d'une courbe singulière. En effet, pour $F = X^3 - 6XZ^2 + 6YZ^2 - Y^3$, un rapide calcul du gradient montre que $F(\overline{\mathbf{Q}}) = \{[\sqrt{2} : \sqrt{2} : 1]\}$. Donc, sur $\mathbf{Q}$, F n'admet aucun point singulier ; pourtant, cette courbe est singulière.

Définition 1.4. *(Courbe elliptique)*
Une courbe elliptique sur $\mathbf{K}$ est une cubique projective lisse.

1.2. **Simplification d'une courbe elliptique.**

1.2.1. *Mise sous forme de Weierstrass.*

Définition 1.5. *(Point d'inflexion)*
Soit F une courbe projective de degré plus grand que deux et $P \in F(\mathbf{K})$ un point non singulier de F. Le point P est un point d'inflexion si et seulement si $\det(H(F))(P) = 0$ *où $H(F)$ est la matrice hessienne associée à F.*

Proposition 1.1. *(Existence d'un point d'inflexion)*

Soit F une courbe projective de $\mathbf{K}$ algébriquement clos, lisse et de degré strictement supérieur à 2. Alors F admet au moins un point d'inflexion.

Démonstration : Comme F est non singulière en tout point de $F(\mathbf{K})$, la définition précédente assure que les points d'inflexion $[x : y : z]$ sont les solutions du système
$$\begin{cases} F(x, y, z) = 0 \\ \det(H(F))(x, y, z) = 0 \end{cases}$$
Comme F est de degré strictement plus grand que 2, $\det(H(F))$ est un polynôme homogène de degré au moins 1 (*ie* une courbe projective de degré au moins 1). Comme $\mathbf{K}$ est algébriquement clos, le théorème de Bézout assure que les deux courbes projectives F et $\det(H(F))$ admettent exactement $\deg(F)\deg(\det(H(F)))$ points d'intersection comptés avec multiplicité. Ici, $\deg(F) > 2$ et $\deg(\det(H(F))) \geqslant 1$ donc nos deux courbes admettent au moins un point d'intersection. Cela veut dire que F admet un point d'inflexion.

Remarques :

- En particulier, toute cubique lisse de $\mathbf{K}$ admet un point d'inflexion.
- On peut en fait montrer que toute cubique lisse sur un corps algébriquement clos admet exactement 9 points d'inflexion distincts.

Proposition 1.2. *Soit F une cubique lisse de $\mathbf{K}$. Alors il existe un automorphisme φ de $\mathbf{P}^2(\mathbf{K})$ (ie un élément de $\mathrm{PGL}_3(\mathbf{K})$) tel que la courbe $F \circ \varphi^{-1}$ est la même que la courbe projective*
$$Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

Cette forme est appelée forme de Weierstrass de la cubique F.

Reformulée autrement, cette proposition dit : toute courbe elliptique peut-être mise sous forme de Weierstrass.

Démonstration : Le plan est le suivant : on envoie un point d'inflexion de F (qui existe) sur le point à l'infini $[0 : 1 : 0]$ et on constate que cette opération transforme notre courbe de la façon voulue.

La forme générale de notre cubique F est $aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3$. Comme F est une cubique lisse, la proposition 1.1 assure que F admet un point d'inflexion $P = [x_p : y_p : z_p]$. On note L la tangente à F en P. Comme P est un point d'inflexion, la multiplicité d'intersection de L et F en P vaut 3.

Choisissons un point $Q = [x_q : y_q : z_q] \in L \backslash F$. Les vecteurs colonnes $\begin{pmatrix} x_p \\ y_p \\ z_p \end{pmatrix}$ et $\begin{pmatrix} x_q \\ y_q \\ z_q \end{pmatrix}$ sont linéairement indépendants puisque P et Q sont deux points distincts du plan projectif. On complète ces deux vecteurs en une base de $\mathbf{K}^3$ par un vecteur colonne C. On obtient alors une matrice inversible $\alpha = \begin{pmatrix} x_q & x_p & \\ y_q & y_p & C \\ z_q & z_p & \end{pmatrix}$ et α^{-1}, tout aussi inversible, permet de passer des coordonnées (X, Y, Z) aux coordonnées (U, V, W) et envoie P sur le point $[0:1:0]$ et Q sur le point $[1:0:0]$. De cette façon, on envoie la tangente à P sur la droite projective Z (car par deux points projectifs passe une unique droite projective).

On obtient alors $G = F \circ \alpha^{-1} = kU^3 + lU^2V + mUV^2 + nV^3 + pU^2W + qUVW + rV^2W + sUW^2 + tVW^2 + uW^3$ et trois conditions :

(1) $\mathcal{O} = [0:1:0] \in G(\mathbf{K})$

(2) La tangente L' à G en $\mathcal{O}$ est W

(3) La multiplicité d'intersection de G et L' en $\mathcal{O}$ est 3 (comme la multiplicité d'intersection de F et L en P)

La première condition impose $n = 0$.

La tangente à G en $\mathcal{O}$ est $\frac{\partial G}{\partial U}(\mathcal{O}) \times U + \frac{\partial G}{\partial V} \times (V-1) + \frac{\partial G}{\partial W} \times W$, c'est à dire après calcul $mU + rW$. On en déduit que $m = 0$ et que $r \neq 0$.

Les points d'intersection entre G et L' sont ceux dont les coordonnées $[u:v:w]$ vérifient $\begin{cases} G(u,v,w) = 0 \\ w = 0 \end{cases}$ c'est à dire ceux tels que $ku^3 + lu^2v = 0$ (après calcul et en utilisant le fait que $n = m = 0$). Or, la troisième condition impose que le seul point d'intersection de G et L' est $\mathcal{O}$ donc on doit avoir une solution triple à l'équation précédente. Cela impose que $l = 0$ et $k \neq 0$.

Puisque une courbe projective est un polynôme modulo multiplication par un facteur non nul, on choisit comme représentant de G celui ayant un coefficient 1 devant U^3 (ce qui est possible car le coefficient devant U^3 est $k \neq 0$). Les observations précédentes montrent alors que

$$G(U, V, W) = U^3 + pU^2W + qUVW + rV^2W + sUW^2 + tVW^2 + uW^3$$

Enfin, puisque $r \neq 0$, on peut faire un nouveau changement de coordonnées et passer de (U, V, W) à $(U, V, \frac{-W}{r})$. Le polynôme obtenu est alors une forme de Weierstrass.

1.2.2. *Mise sous forme de Weierstrass réduite.*

Dans la suite de cette partie, le corps $\mathbf{K}$ est algébriquement clos et de caractéristique différente de 2 ou 3.

Proposition 1.3. *Soit $F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ une courbe elliptique mise sous forme de Weierstrass. Alors il existe un automorphisme φ de $\mathbf{P}^2(\mathbf{K})$ tel que $F \circ \varphi^{-1}$ est la même courbe que $Y^2Z - X^3 - aXZ^2 - bZ^3$.*

Démonstration :

Elle repose sur des changements successifs de coordonnées. On commence par faire le changement de coordonnées :

$$\begin{cases} X & \leftarrow & X \\ Y & \leftarrow & Y - \frac{a_1X}{2} - \frac{a_3Z}{2} \\ Z & \leftarrow & Z \end{cases}$$

ce qui est possible puisque $\mathrm{car}(\mathbf{K}) \neq 2$. Cette opération symétrise la courbe par rapport à l'axe des abscisses lorsqu'on l'observe dans le plan affine.

Après calcul, la forme de Weierstrass initiale devient alors :

$$Y^2Z - X^3 - (\frac{a_1^2}{4} + a_2)X^2Z - (\frac{3a_1a_2}{4} + a_4)XZ^2 - (\frac{a_3^2}{4} + a_6)Z^3$$

En renommant les constantes, on montre donc qu'il existe $(a, b, c) \in \mathbf{K}^3$ tels que la forme devienne :

$$Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3$$

Puis, le changement de coordonnées (loisible puisque car$(\mathbf{K}) \neq 3$)

$$\begin{cases} X & \leftarrow & X - \frac{aZ}{3} \\ Y & \leftarrow & Y \\ Z & \leftarrow & Z \end{cases}$$

permet de montrer qu'il existe $(a, b) \in \mathbf{K}^2$ tels qu'on obtienne une forme de Weierstrass réduite :

$$Y^2Z - X^3 - aXZ^2 - bZ^3$$

Remarques :

- Intéressons nous aux points sur la droite à l'infini d'une courbe elliptique $F = Y^2Z - X^3 - aXZ^2 - bZ^3$. Soit P un tel point et $[x : y : 0]$ ses coordonnées homogènes. Ces dernières doivent vérifier l'équation $x^3 = 0$, donc $x = 0$. De plus, comme $[0 : 0 : 0]$ n'est pas un point du plan projectif, on a nécessairement $y \neq 0$. En divisant les coordonnées de P par y, on obtient finalement que P a pour coordonnées $[0 : 1 : 0]$. Ce point est effectivement à l'infini et dans $F(\mathbf{K})$. On nomme ce point $\mathcal{O}$ et on l'appelle point à l'infini de F.
- On en déduit qu'un point de $F(\mathbf{K})$ est soit $\mathcal{O}$, soit un point dont les coordonnées affines (x, y) vérifient l'équation $y^2 = x^3 + ax + b$.
- On connaît très bien le comportement de $\mathcal{O} \in F(\mathbf{K})$: c'est un point non singulier, d'inflexion et la tangente à F en ce point est la droite à l'infini (vu dans la mise sous forme de Weierstrass). C'est pourquoi on se concentre dans la suite aux points de $F(\mathbf{K})$ qui ne sont pas à l'infini ; ce qui permet de travailler avec la forme de Weierstrass réduite affine : $Y^2 - X^3 - aX - b$.

1.2.3. *Caractérisation du caractère lisse d'une courbe elliptique.*

Lemme 1.1. *Soit $P \in \mathbf{K}[X]$. P admet une racine multiple si et seulement si P et P' ont une racine commune.*

Démonstration :

Si P a une racine multiple, il existe $\alpha \in \mathbf{K}$ et $Q \in \mathbf{K}$ tels que $P = (X - \alpha)^2Q$. Alors, $P' = 2(X - \alpha)Q + (X - \alpha)^2Q'$ donc $P'(\alpha) = 0$. On en déduit que α est une racine commune à P et P'.

Réciproquement, si il existe α tel que $P(\alpha) = P'(\alpha) = 0$ alors il existe $Q \in \mathbf{K}[X]$ tel que $P = (X - \alpha)Q$. En dérivant cette expression, on obtient $P' = Q + (X - \alpha)Q'$. Mais comme $P'(\alpha) = 0$, $Q(\alpha) = 0$ aussi. Donc il existe $R \in \mathbf{K}[X]$ tel que $Q = (X - \alpha)R$. Par conséquent, $P = (X - \alpha)^2R$ et α est racine multiple de P.

Lemme 1.2. *Soit $a, b \in \mathbf{K}$. Le polynôme $X^3 + aX + b$ admet une racine multiple si et seulement si $4a^3 + 27b^2 = 0$.*

Démonstration :

Le polynôme $P = X^3 + aX + b$ admet une racine multiple si et seulement si P et P' admettent une racine commune par le lemme 1.1. Cette dernière condition est équivalente à la nullité du résultant de P et P'. Or, après calcul, $\mathrm{Res}(P, P') = 4a^3+27b^2$. Ce qui conclut.

Lemme 1.3. *Soit $a, b \in \mathbf{K}$. La courbe affine $f = Y^2 - X^3 - aX - b$ est lisse si et seulement si $4a^3 + 27b^2 \neq 0$.*

Démonstration :

Commençons le raisonnement par équivalence :

$$\begin{array}{rl} & f \text{ est lisse} \\ \Leftrightarrow & \forall (x,y) \in f(\mathbf{K}), \mathrm{grad}(f)(x,y) \neq 0 \\ \Leftrightarrow & \forall (x,y) \in f(\mathbf{K}), (3x^2 + a \neq 0) \text{ ou } (2y \neq 0) \\ \Leftrightarrow & \forall (x,y) \in f(\mathbf{K}), (3x^2 + a \neq 0) \text{ ou } (y \neq 0) \text{ puisque } \mathrm{car}(\mathbf{K}) \neq 2 \end{array}$$

Continuons par double implication :

Supposons que $27b^2 + 4a^3 \neq 0$. Soit $(x, y) \in f(\mathbf{K})$. Si $y \neq 0$, pas de problème. Sinon, $x^3 + ax + b = y^2 = 0$ donc x est racine du polynôme $X^3 + aX + b$. Mais, notre hypothèse et le lemme 1.2 assurent alors que x n'est pas racine double de $X^3 + aX + b$. Le lemme 1.1 implique alors que x n'est pas racine de $3X^2 + a$ donc $3x^2 + a \neq 0$. On a bien :

$$\forall (x,y) \in f(\mathbf{K}), (3x^2 + a \neq 0) \text{ ou } (y \neq 0)$$

Réciproquement, supposons que $\forall (x,y) \in f(\mathbf{K}), (3x^2 + a \neq 0)$ ou $(y \neq 0)$. Par l'absurde, $27b^2+4a^3 = 0$. Par le lemme 1.2, il existe $x \in \mathbf{K}$ qui est racine double du polynôme $X^3 + aX + b$. Alors le point $(x, 0)$ appartient à $f(\mathbf{K})$, et est tel que $3x^2 + a = 0$ et $y = 0$ ce qui est une contradiction. Donc $27b^2 + 4a^3 \neq 0$.

Proposition 1.4. *(Définition équivalente d'une courbe elliptique)*

Soit F une courbe projective sur $\mathbf{K}$, corps algébriquement clos de caractéristique différente de 2 ou 3. Alors, F est une courbe elliptique si et seulement si il existe $a, b \in \mathbf{K}$ tels que $27b^2 + 4a^3 \neq 0$ et F admette la forme de Weierstrass réduite $Y^2Z - X^3 - aXZ^2 - bZ^3$.

Démonstration : Si F est une courbe elliptique, alors elle peut être mise sous forme de Weierstrass réduite (parties précédentes). De plus, comme F est lisse, la courbe affine sous-jacente à F l'est aussi. Le lemme 1.3 assure alors que $27b^2 + 4a^3 \neq 0$.

Réciproquement, si il existe $a, b \in \mathbf{K}$ tels que $27b^2 + 4a^3 \neq 0$ et F admette la forme de Weierstrass réduite $Y^2Z - X^3 - aXZ^2 - bZ^3$, alors F est une cubique. De plus, elle est lisse en tout point de $F(\overline{\mathbf{K}}) = F(\mathbf{K})$ (car $\mathbf{K}$ est algébriquement clos). En effet, $F(\mathbf{K}) = \{[0:1:0]\} \cup \{[x:y:1] | y^2 = x^3 + ax + b\}$ comme vu précédemment. La courbe F est lisse en $[0:1:0]$ car $\mathrm{grad}(F)(0,1,0) = 1 \neq 0$ et comme $27b^2 + 4a^3 \neq 0$, le lemme 1.3 assure que F est lisse en tout point de $\{[x:y:1] | y^2 = x^3 + ax + b\}$. Donc F est une courbe elliptique.

Remarques :

- Cette proposition permet d'utiliser une forme réduite de Weierstrass à chaque fois que l'on veut parler d'une courbe elliptique.
- Si $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ est une courbe elliptique, la quantité $\Delta(F) = 4a^3 + 27b^2$ est appelée discriminant de F.
- Si $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ est une cubique projective, on dispose de trois méthodes permettant d'affirmer qu'il s'agit d'une courbe elliptique :
  - On vérifie que $\mathrm{grad}(F)$ ne s'annule en aucun point de $F(\overline{\mathbf{K}})$.
  - On vérifie que la quantité $4a^3 + 27b^2$ est non nulle.
  - On vérifie que les racines du polynôme $X^3 + aX + b$ sont deux à deux distinctes.

1.3. **Loi de groupe.**

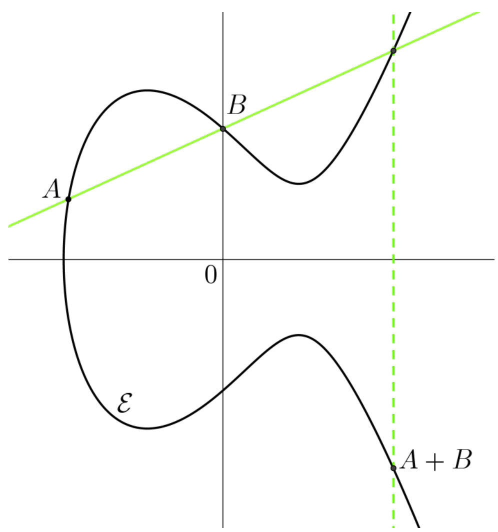
On définit une loi interne sur les points rationnels d'une courbe elliptique F, notée $+$ qui fait de $(F(\mathbf{K}), +)$ un groupe commutatif. Les illustrations s'appuient sur la courbe $Y^2Z - X^3 + 3XZ^2 + 3Z^3$.

Soient A et B deux points de $F(\mathbf{K})$. On note D la droite passant par A et B, en considérant que cette droite est la tangente à F en A si $A = B$. On peut toujours considérer cette droite :

- si $A \neq B$, il existe une unique droite projective passant par A et B
- si $A = B$, la tangente à F en A existe bien car F est lisse par définition

Comme $\mathbf{K}$ est algébriquement clos, on peut utiliser le théorème de Bézout. Ce dernier assure alors que F et D, de degrés respectifs 3 et 1, s'intersectent en exactement 3 points.

Deux d'entre eux sont A et B. On définit la somme de A et B comme étant le symétrique du troisième par rapport à l'axe des abscisses (de façon à ce que le point à l'infini soit neutre). La figure ci-contre illustre le propos.



Remarque : La seule chose "difficile" à prouver est l'associativité de cette loi. On admet (pour l'instant) que $+$ est une loi de groupe. Une preuve de ce fait est donnée juste après le théorème 3.3.

1.4. j**-invariant et courbes isomorphes.**

Définition 1.6. *(Courbes elliptiques isomorphes)*

Soient $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ *et* $F' = Y^2Z - X^3 - a'XZ^2 - b'Z^3$ *deux courbes elliptiques. On dit que* F *et* F' *sont isomorphes si et seulement si il existe* $\mu \in \overline{K}^\star = K^\star$ *tel que* $a = \mu^4 a'$ *et* $b = \mu^6 b'$.

Remarque : Justification de l'appellation "courbes isomorphes".

Si $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ et $F' = Y^2Z - X^3 - \mu^4 a - XZ^2 - \mu^6 bZ^3$, on remarque d'abord que le discriminant de F' est égal à μ^{12} fois celui de F. Donc F est une courbe elliptique si et seulement si F' en est une.

Ensuite on remarque que $\varphi : \left\{ \begin{array}{lcl} F(\mathbf{K}) & \longrightarrow & F'(\mathbf{K}) \\ [x:y:z] & \longmapsto & [\mu^2 x : \mu^3 y : z] \end{array} \right.$ est un isomorphisme de groupes (où on a muni $F(\mathbf{K})$ et $F'(\mathbf{K})$ de la loi de groupe définie précédemment).

En effet,

$$\begin{array}{cl} & [x:y:z] \in F(\mathbf{K}) \\ \Leftrightarrow & y^2 z = x^3 + axz^2 + bz^3 \\ \Leftrightarrow & \mu^6 \times y^2 z = \mu^6 (x^3 + axz^2 + bz^3) \\ \Leftrightarrow & (\mu^3 y)^2 z = (\mu^2 x)^3 + \mu^4 a(\mu^2 xz^2) + \mu^6 bz^3 \\ \Leftrightarrow & [\mu^2 x : \mu^3 y : z] \in F'(\mathbf{K}) \end{array}$$

ce qui permet de définir $\psi : \left\{ \begin{array}{lcl} F'(\mathbf{K}) & \longrightarrow & F(\mathbf{K}) \\ [x:y:z] & \longmapsto & [\mu^{-2} x : \mu^{-3} y : z] \end{array} \right.$ application qui est un inverse pour φ.

Reste à montrer que φ est un morphisme de groupes. Soit P et Q deux points de $F(\mathbf{K})$ et $L = aX + bY + cZ$ la ligne les joignant (qui existe). Le troisième point d'intersection de L avec F est $R = -(P + Q)$. Or, l'image de L par φ est la ligne $L' = \frac{a}{\mu^2}X + \frac{b}{\mu^3}Y + cZ$ et cette dernière intersecte F' en trois points comptés avec multiplicité (par Bézout). Comme $\varphi(P), \varphi(Q)$ et $\varphi(R)$ sont tous trois dans $L'(\mathbf{K}) \cap F'(\mathbf{K})$, les trois points d'intersection en question sont $\varphi(P), \varphi(Q)$ et $\varphi(R)$. On en déduit que $\varphi(P) + \varphi(Q) = -\varphi(R)$ puis que :

$$\varphi(P+Q) = \varphi(-R) \underbrace{=}_{(\star)} -\varphi(R) = \varphi(P) + \varphi(Q)$$

L'égalité $(\star)$ vient de ce que $\varphi(-R) + \varphi(R) = -\varphi(\mathcal{O}) = [0 : -\mu^3 : 0] = [0:1:0] = \mathcal{O}$.

D'où l'appellation "courbes isomorphes".

Définition 1.7. *(j-invariant)*

Soit $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ *une courbe elliptique. Le j-invariant de* F *est défini par* $j(F) = 6912 \times \frac{a^3}{4a^3 + 27b^2}$

Proposition 1.5.

Pour tout $j_0 \in \mathbf{C}$, *il existe une courbe elliptique sur* $\mathbf{C}$ *de* j*-invariant* j_0.

Démonstration : Si $j_0 = 0$ alors $E = Y^2Z - X^3 - Z^3$ convient. Si $j_0 = 1728$ alors $E = Y^2Z - X^3 - XZ^2$ convient.

Sinon, $E = Y^2Z - X^3 - aXZ^2 - bZ^3$ avec $a = 3j_0(1728 - j_0)$ et $b = 2j_0(1728 - j_0)^2$ convient. Comme $4a^3 + 27b^2 = 4 \times 27 \times 1728 j_0^2(1728 - j_0)^3 \neq 0$ car $j_0 \notin \{0, 1728\}$, ceci est bien une courbe elliptique. De plus,

$$j(E) = 4 \times 1728 \frac{27 j_0^3 (1728 - j_0)^3}{4 \times 27 \times 1728 j_0^2 (1728 - j_0)^3} = j_0$$

Proposition 1.6. *(Courbes isomorphes et j-invariant)*
Soient $F = Y^2Z - X^3 - aXZ^2 - bZ^3$ et $F' = Y^2Z - X^3 - a'XZ^2 - b'Z^3$ deux courbes elliptiques. Ces dernières sont isomorphes si et seulement si elles ont même j-invariant.

Démonstration : Si F et F' sont isomorphes, alors il existe $\mu \in \mathbf{K}^\star$ tel que $a' = \mu^4 a$ et $b' = \mu^6 b$. Un calcul direct donne alors $j(F) = j(F')$.

Réciproquement, si $j(F) = j(F') = j$, plusieurs cas se présentent :

- Si $j = 0$ alors $a = a' = 0$. Mais, comme F et F' sont des courbes elliptiques, $\Delta(F)$ et $\Delta(F')$ se doivent d'être non nuls. Cela implique que b et b' sont différents de 0. On peut donc définir μ par $\mu^6 = \frac{b'}{b}$. Il convient.
- Si $j = 1728$ alors $b = b' = 0$, et le même raisonnement que ci dessus impose a et a' non nuls. On définit alors μ par $\mu^4 = \frac{a'}{a}$ et ce dernier convient.
- Si $j \notin \{0, 1728\}$, ni a ni b ne sont nuls. Remarquons que $\frac{j(F)}{j(F)-1728} = \frac{4a^3}{27b^2}$ et $\frac{j(F')}{j(F')-1728} = \frac{4a'^3}{27b'^2}$. Comme $j(F) = j(F')$ alors $\frac{4a^3}{27b^2} = \frac{4a'^3}{27b'^2}$ donc $(\frac{a}{a'})^3 = (\frac{b}{b'})^2$. On définit alors μ par $\mu^2 = \frac{ab'}{a'b}$. On a alors

$$\mu^4 = (\frac{a}{a'})^2 \times (\frac{a}{a'})^{-3} = \frac{a'}{a} \text{ donc } a' = \mu^4 a$$

  et un calcul similaire montre que $b' = \mu^6 b$.

Dans tous les cas, F et F' sont isomorphes.

2. Fonctions elliptiques

2.1. Définition et quelques propriétés.

Définition 2.1. *(Réseau de $\mathbf{C}$)*
Un réseau Γ de $\mathbf{C}$ est un sous groupe (pour l'addition) discret de $\mathbf{R}^2$ tel que le sous espace vectoriel engendré par Γ soit égal à $\mathbf{R}^2$.

Remarque : Une base du réseau Γ est un couple (z_1, z_2) de complexes tel que tout élément de Γ s'écrit comme combinaison linéaire à coefficients entiers de z_1 et z_2. L'existence d'un tel couple est toujours assurée.

Définition 2.2. *(Fonction périodique sur un réseau)*
Une fonction f définie sur $\mathbf{C}$ est dite périodique sur le réseau de $\mathbf{C}$, Γ si pour tout $z \in \mathbf{C}$, pour tout $\gamma \in \Gamma$, $f(z + \gamma) = f(z)$. On dit aussi que f est de période Γ ou que f est Γ-périodique.

Définition 2.3. *(Fonction elliptique)*

Une fonction f est dite elliptique si elle est méromorphe sur $\mathbf{C}$ *et doublement périodique.*

Cette dernière condition signifie qu'il existe deux éléments non colinéaires de $\mathbf{C}$*, u et v tels que pour tout $z \in \mathbf{C}$, $f(z+u) = f(z+v) = f(z)$. Elle est donc équivalente à "f est périodique sur le réseau de base (u, v)"*

Remarque : Toute fonction elliptique et holomorphe est constante.

En effet, soit f une fonction elliptique et holomorphe. Elle est alors périodique sur un réseau de $\mathbf{C}$ de base (u, v). La fonction f est continue donc bornée sur le compact $\{au + bv | a, b \in [0, 1]\}$. Par double périodicité, on en déduit que f est bornée sur $\mathbf{C}$. Le théorème de Liouville assure alors qu'elle est constante.

Remarque : Si Γ est un réseau de base (u, v) et qu'on note $\Pi = \{au + bv | a, b \in [0, 1[\}$ son domaine fondamental, pour tout $\alpha \in \mathbf{C}$, le comportement d'une fonction elliptique de période Γ sur $\alpha + \Pi$ donne celui sur Π (par Γ-périodicité).

Proposition 2.1. *(Zéros et pôles)*

Soit f une fonction elliptique Γ-périodique. On note Π le domaine fondamental de Γ. Si f n'a ni pôle ni zéro sur le bord B d'un parallélogramme $\alpha + \Pi$, que $\{m_i\}_i$ sont les ordres des zéros de f dans $\alpha + \Pi$ et que $\{n_j\}_j$ sont les ordres des pôles de f dans $\alpha + \Pi$, alors $\sum_i m_i = \sum_j n_j$

Démonstration :

Le théorème de l'indice montre que $\frac{1}{2\pi i} \int_B \frac{f'(z)}{f(z)} dz = \sum_i m_i - \sum_j n_j$. Or, $\frac{f'}{f}$ n'a pas de pôle dans B (par hypothèse). La double périodicité de cette fonction montre que $\int_B \frac{f'(z)}{f(z)} dz = 0$. D'où le résultat.

Définition 2.4. *(Ordre d'une fonction elliptique)*

L'ordre d'une fonction elliptique f de période Γ est la somme des ordres des pôles de f situés dans le parallélogramme fondamental de Γ.

Remarques :

- Vu la remarque précédente, l'ordre d'une fonction elliptique est aussi la somme des ordres des pôles de cette fonction situés dans n'importe quel translaté du parallélogramme fondamental.
- La proposition précédente montre que l'ordre d'une fonction elliptique est aussi la somme des ordres des zéros de cette fonction dans n'importe quel translaté du parallélogramme fondamental.

Corollaire 2.1. *Soit Γ un réseau de domaine fondamental Π, $n \in \mathbb{N}$ et f une fonction elliptique relativement à Γ d'ordre n. Alors, pour tout $c, \alpha \in \mathbf{C}$, f prend la valeur c exactement n fois dans $\alpha + \Pi$ en comptant les multiplicités.*

Démonstration : Soit $c \in \mathbf{C}$. Il existe $a \in \mathbf{C}$ tel que le bord de $a + \Pi$ ne contient ni zéro ni pôle de f. On applique alors le résultat de la proposition 2.1 à la fonction elliptique $z \mapsto f(z) - c$. Les pôles de cette fonction sont ceux de f (donc elle est d'ordre n) et ses zéros sont les z tels que $f(z) = c$. D'où le résultat pour $a + \Pi$ puis pour tout translaté de Π par double périodicité.

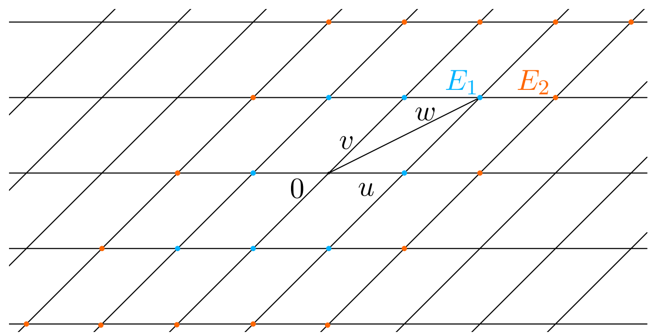
2.2. La fonction $\wp$ de Weierstrass.

Lemme 2.1. *Soit Γ un réseau de* $\mathbf{C}$.

Pour tout $k > 2$, la série $\sum\limits_{\gamma \in \Gamma \backslash \{0\}} \frac{1}{|\gamma|^k}$ *est convergente.*

Démonstration :

On note (u, v) une base du réseau Γ et pour tout $n \in \mathbb{N}^\star$, on note $E_n = \{au + bv | a, b \in \mathbf{Z} \text{ et } \max(|a|, |b|) = n\}$. Ainsi, E_n est l'ensemble des points à coordonnées entières sur P_n, le parallélogramme fondamental dilaté $2n$ fois et centré en 0.



Soit $n \in \mathbb{N}^\star$. On a :

$$\# E_n = \underbrace{2n}_{\substack{\text{longueur} \\ \text{du côté de } P_n}} \times \underbrace{4}_{\substack{\text{nombre} \\ \text{de côtés de } P_n}} - \underbrace{4}_{\substack{\text{on compte deux fois} \\ \text{chaque sommet de } P_n}} = 4(2n - 1)$$

De plus, si $\gamma \in E_n$, $|\gamma| \geqslant dn$ où $d > 0$ est la distance de 0 à E_1 (sur le dessin, $d = \min(u, v, w)$) et on en déduit que $\frac{1}{|\gamma|^k} \leqslant \frac{1}{d^k n^k}$. Donc :

$$\sum_{\gamma \in \Gamma \backslash \{0\}} \frac{1}{|\gamma|^k} = \sum_{n=1}^{+\infty} \underbrace{\sum_{\gamma \in E_n} \frac{1}{|\gamma|^k}}_{\substack{\leqslant \frac{\# E_n}{d^k n^k} \leqslant \frac{4(2n-1)}{d^k n^k} \leqslant \frac{8n}{d^k n^k} = \frac{8}{d^k n^{k-1}} \\ \text{qui est un terme de série convergente puisque } k > 2}}$$

D'où la convergence annoncée.

Dans toute la suite, sauf mention contraire, Γ est un réseau fixé de $\mathbf{C}$ dont une base est (u, v). On note Π le domaine fondamental de Γ.

Proposition 2.2. *(Bonne définition de la fonction $\wp$ de Weierstrass)*

Soit $f_0 : z \mapsto \frac{1}{z^2}$ et pour tout $\gamma \in \Gamma \backslash \{0\}$, $f_\gamma : z \mapsto \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}$. La série de fonctions méromorphes $\sum\limits_{\gamma \in \Gamma} f_\gamma$ converge normalement sur tout compact de $\mathbf{C}$.

La somme de cette série est appelée "fonction $\wp$ de Weierstrass" et est méromorphe sur $\mathbf{C}$.

Remarque : On devrait plutôt appeler cette fonction $\wp_\Gamma$ puisqu'elle dépend du réseau Γ. Dans cette partie, on ne le fera pas.

Démonstration : Soit K un compact de $\mathbf{C}$. Il existe $R > 0$ tel que $K \subset \overline{B(0, R)}$. Comme Γ est discret, il existe un nombre fini d'éléments de Γ dans $\overline{B(0, 2R)}$. Donc tous les $\gamma \in \Gamma$ sauf un nombre fini sont tels que $|\gamma| \geqslant 2R$. On note G l'ensemble des tels γ. En particulier, pour tout $\gamma \in G$, f_γ n'a pas de pôle dans K.

Reste à montrer que $\sum\limits_{\gamma \in G} \sup\limits_{z \in K} |f_\gamma(z)|$ est finie.

Pour $\gamma \in G$ et $z \in K$, on remarque que $|\gamma| \geqslant 2R \geqslant 2|z|$. Donc :

- $\left|2 - \frac{z}{\gamma}\right| \leqslant 2 + \left|\frac{z}{\gamma}\right| \leqslant 2 + \frac{1}{2} = \frac{5}{2}$
- $\left|1 - \frac{z}{\gamma}\right| \geqslant 1 - \left|\frac{z}{\gamma}\right| \geqslant 1 - \frac{1}{2} = \frac{1}{2}$

Alors :

$$\begin{array}{rcl} |f_\gamma(z)| & = & \left|\frac{\gamma^2-(z^2-2\gamma z+\gamma^2)}{(z-\gamma)^2\gamma^2}\right| \\ & = & \left|\frac{2\gamma z - z^2}{\gamma^2(z-\gamma)^2}\right| \\ & = & \frac{\left|z(2-\frac{z}{\gamma})\right|}{|\gamma^3|\left|1-\frac{z}{\gamma}\right|^2} \\ & \leqslant & \frac{10R}{|\gamma|^3} \text{ en utilisant les deux inégalités précédentes} \end{array}$$

Donc $\sum\limits_{\gamma \in G} \sup\limits_{z \in K} |f_\gamma(z)| \leqslant \sum\limits_{\gamma \in G} \frac{10R}{|\gamma|^3} \leqslant 10R \times \sum\limits_{\gamma \in \Gamma} \frac{1}{|\gamma|^3}$ et cette dernière série est convergente grâce au lemme 2.1.

On en déduit que $\sum\limits_{\gamma \in \Gamma} f_\gamma$ est une série de fonctions méromorphes qui converge normalement sur tout compact de $\mathbf{C}$: sa somme est donc méromorphe sur $\mathbf{C}$.

2.3. **Propriétés de la fonction $\wp$ de Weierstrass.**

Proposition 2.3. *(Propriétés de $\wp$)*

(1) *Les pôles de $\wp$ sont exactement les éléments de Γ et sont tous d'ordre deux.*
(2) *La fonction $\wp'$ est impaire et elliptique d'ordre 3.*
(3) *La fonction $\wp$ est paire et elliptique d'ordre 2.*
(4) *Les zéros de $\wp'$ dans Π sont exactement $\frac{u}{2}$, $\frac{v}{2}$ et $\frac{u+v}{2}$.*
(5) *Les seuls $a \in \mathbf{C}$ tels que $z \mapsto \wp(z) - a$ ait un zéro double sont $\wp(\frac{u}{2})$, $\wp(\frac{v}{2})$ et $\wp(\frac{u+v}{2})$. De plus, ces trois nombres sont deux à deux distincts.*

Démonstration :

(1) Pour tout $\gamma \in \Gamma$, la fonction f_γ admet exactement un pôle d'ordre deux ; à savoir γ. Les ensembles de pôles de fonctions f_γ sont donc deux à deux disjoints et leur union forme l'ensemble Γ. Comme $\sum\limits_{\gamma \in \Gamma} f_\gamma$ converge normalement sur tout compact de $\mathbf{C}$ vers $\wp$, on en déduit que l'ensemble des pôles de $\wp$ est Γ et que chacun des pôles de $\wp$ est d'ordre deux.
(2) La convergence normale sur tout compact de la série des f_γ permet d'intervertir somme et dérivation. Comme $f_0' : z \mapsto \frac{-2}{z^3}$ et que pour tout $\gamma \in \Gamma\backslash\{0\}$, $f_\gamma' : z \mapsto \frac{-2}{(z-\gamma)^3}$, on obtient :

$$\forall z \notin \Gamma, \wp'(z) = -2 \sum_{\gamma \in \Gamma} \frac{1}{(z-\gamma)^3}$$

La convergence de la série précédente vers $\wp'$ reste normale sur tout compact d'où le caractère méromorphe sur $\mathbf{C}$ de $\wp'$ et un raisonnement similaire à celui tenu en (1) permet alors d'affirmer que les pôles de $\wp'$ sont les éléments de Γ et sont tous d'ordre trois.

De plus, $\forall z \notin \Gamma, \wp'(-z) = 2 \sum\limits_{\gamma \in \Gamma} \frac{1}{(z+\gamma)^3} = 2 \sum\limits_{\gamma \in \Gamma} \frac{1}{(z-\gamma)^3} = -\wp'(z)$ par changement d'indice $\gamma \leftarrow -\gamma$. D'où l'imparité de $\wp'$.

Un autre changement d'indice montre facilement que $\wp'$ est γ-périodique pour tout $\gamma \in \Gamma$. La fonction $\wp'$ est donc méromorphe et Γ-périodique : elle est elliptique. Comme le seul pôle de $\wp'$ situé dans Π est 0, d'ordre 3, l'ordre de $\wp'$ est 3.

(3) Le même changement d'indice que pour montrer l'imparité de $\wp'$ montre que $\wp$ est paire. On a déjà vu précédemment que $\wp$ est méromorphe. Reste à prouver sa Γ-périodicité : pour ce faire, il suffit de montrer que $\wp$ est u-périodique et v-périodique. Faisons-le pour u :

Soit $f : z \mapsto \wp(z+u)-\wp(z)$. On remarque que f' est nulle sur l'ouvert connexe $\mathbf{C}\backslash\Gamma$ par périodicité de $\wp'$. La fonction f est donc constante sur $\mathbf{C}\backslash\Gamma$. Évaluons f en $\frac{-u}{2} \notin \Gamma$: $f(\frac{-u}{2}) = \wp(\frac{u}{2}) - \wp(\frac{-u}{2}) = 0$ par parité de $\wp$. On en déduit que f est nulle donc que $\wp$ est u-périodique. Ce qui conclut.

La fonction $\wp$ est donc elliptique, et, comme le seul pôle de $\wp$ situé dans Π est 0, d'ordre 2 (par (1)), l'ordre de $\wp$ est 2.

(4) Comme $\wp'$ est d'ordre 3, la somme des ordres des zéros de $\wp'$ situés dans Π vaut 3 aussi (par la proposition 2.1), donc $\wp'$ a au plus trois zéros dans Π. On remarque alors que :

$$\wp'(\frac{u}{2}) \underbrace{=}_{\text{imparité}} -\wp'(\frac{u}{2}) \underbrace{=}_{\text{périodicité}} -\wp'(u - \frac{u}{2}) = -\wp'(\frac{u}{2})$$

Donc $\wp'(\frac{u}{2}) = 0$. On montre de même que $\wp'(\frac{v}{2}) = \wp'(\frac{u+v}{2}) = 0$. Les trois zéros trouvés sont dans Π et deux à deux distincts : ce sont donc exactement les zéros de $\wp'$ dans Π.

(5) Soit $a \in \mathbf{C}$. Si $z \mapsto \wp(z) - a$ admet un zéro double en z_0, alors $\wp'(z_0) = 0$ et le point (4) assure que $z_0 \in \{\frac{u}{2}, \frac{v}{2}, \frac{u+v}{2}\}$ puis que $a \in \{\wp(\frac{u}{2}), \wp(\frac{v}{2}), \wp(\frac{u+v}{2})\}$. Réciproquement, si $a = \wp(\frac{u}{2})$ alors $z \mapsto \wp(z) - u$ et sa dérivée s'annulent en $\frac{u}{2}$ donc $\frac{u}{2}$ est un double zéro. De même pour $\frac{v}{2}$ et $\frac{u+v}{2}$.

Remarquons d'autre part que pour tout $a \in \mathbf{C}$, $f_a : z \mapsto \wp(z) - a$ est elliptique d'ordre deux, comme $\wp$. La somme des ordres de ses zéros dans Π est donc égale à deux par la proposition 2.1. La fonction f_u admet donc deux zéros simples ou un zéro double. Si $\wp(\frac{u}{2}) = \wp(\frac{v}{2}) = a_0$ (le raisonnement est le même pour les deux autres couples), f_{a_0} admettrait deux zéros doubles différents ($\frac{u}{2}$ et $\frac{v}{2}$), d'où une contradiction. On en déduit que $\wp(\frac{u}{2})$, $\wp(\frac{v}{2})$ et $\wp(\frac{u+v}{2})$ sont deux à deux distincts.

Proposition 2.4. *(Relation fonctionnelle pour $\wp$)*
La fonction $\wp$ vérifie la relation

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

où $g_2 = 60 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^4}$ *et* $g_3 = 120 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^6}$ *dépendent du réseau* Γ.

Remarque : Là encore, on devrait écrire $g_2(\Gamma)$ et $g_3(\Gamma)$ à la place de g_2 et g_3. On sous entend Γ dans cette proposition.

Démonstration :

On considère la fonction $g : z \mapsto \wp(z) - \frac{1}{z^2} = \sum_{\gamma\in\Gamma\setminus\{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}\right)$. Cette fonction est paire, holomorphe au voisinage de zéro, et nulle en zéro.

D'où le début de son développement en série pour z proche de zéro :

$$g(z) = 0 + a_2 z^2 + a_4 z^4 + \mathrm{O}(z^6) \ (\star)$$

La convergence normale sur tout compact de $\sum_{\gamma\in\Gamma\setminus\{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}\right)$ permet d'intervertir somme et dérivation ce qui permet de calculer

$a_2 = \frac{g'(0)}{2} = 3 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^4}$ et $a_4 = \frac{g^{(4)}(0)}{24} = 5 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^6}$.

En reprenant la relation $(\star)$ en isolant $\wp(z)$ et en dérivant puis en mettant au carré, on obtient :

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{8a_2}{z^2} - 16a_4 + \mathrm{O}(z^2)$$

De même, en isolant $\wp(z)$ dans $(\star)$ puis en mettant au cube, on trouve :

$$\wp(z)^3 = \frac{1}{z^6} + \frac{3a_2}{z^2} + 3a_4 + \mathrm{O}(z^2)$$

En ajustant les coefficients utilisés de façon à faire disparaître le pôle en zéro, on en déduit que

$$\wp'(z)^2 - 4\wp(z)^3 + 20a_2\wp(z) + 28a_4 = \mathrm{O}(z^2)$$

Donc la fonction $z \mapsto \wp'(z)^2 - 4\wp(z)^3 + 20a_2\wp(z) + 28a_4$ est holomorphe sur un voisinage de zéro et s'annule en zéro. Par double périodicité, elle est aussi holomorphe au voisinage de chaque point du réseau Γ et est donc holomorphe sur $\mathbf{C}$. Or, on a déjà vu qu'une fonction elliptique et holomorphe est constante. La fonction en question est donc constante sur $\mathbf{C}$ et nulle en zéro donc nulle sur $\mathbf{C}$.

Comme $20a_2 = 60 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^4}$ et $28a_4 = 120 \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^6}$, on conclut.

3. Du réseau à la courbe

3.1. **Où l'on découvre une utilité à $\wp$.**

Théorème 3.1. *L'application* $\varphi : \left\{ \begin{array}{ccc} \mathbf{C}/\Gamma & \longrightarrow & E_\Gamma(\mathbf{C}) \\ z & \longmapsto & \begin{cases} [\wp(z) : \wp'(z) : 1] & si\ z \notin \Gamma \\ [0 : 1 : 0] & si\ z \in \Gamma \end{cases} \end{array} \right.$

où E_Γ *est la cubique dont la forme déshomogénéisée est* $Y^2 - 4X^3 + g_2(\Gamma)X + g_3(\Gamma)$ *(avec* g_2 *et* g_3 *définis comme à la proposition 2.4) est bien définie, bijective et holomorphe (au sens où, pour tout* $z \in \mathbf{C}/\Gamma$, *il existe une carte de* $\mathbb{P}^2(\mathbf{C})$ *telle que dans cette carte, les différentes coordonnées de* φ *sont holomorphes). De plus* E_Γ *est une courbe elliptique.*

Démonstration :

- Bonne définition de φ.

  La double périodicité de $\wp$ et $\wp'$ montrent que φ est bien définie : si z et z' sont conjugués modulo Γ, soit ils appartiennent tous deux à Γ auquel cas ils ont même image par φ, soit aucun de deux n'est dans Γ mais alors $\wp(z) = \wp(z')$ et $\wp'(z) = \wp'(z')$ donc $\varphi(\overline{z}) = \varphi(\overline{z'})$. La relation fonctionnelle que vérifie $\wp$ (établie à la proposition 2.4) montre que l'image de φ est incluse dans $E_\Gamma(\mathbf{C})$.

- E_Γ est une courbe elliptique.

  Il suffit de monter qu'elle est lisse, et pour ce faire, on montre que $G = 4X^3 - g_2(\Gamma)X - g_3(\Gamma)$ voit ses racines dans $\mathbf{C}$ être deux à deux distinctes.

  On remarque que $G(\wp(\frac{u}{2})) = \wp'(\frac{u}{2}) = 0$ (relation fonctionnelle et proposition 2.3). De même, $G(\wp(\frac{v}{2})) = G(\wp(\frac{u+v}{2})) = 0$. On a vu au point (5) de la proposition 2.3 que $\wp(\frac{u}{2})$, $\wp(\frac{v}{2})$ et $\wp(\frac{u+v}{2})$ sont deux à deux distincts et G ne peut avoir plus de trois racines. D'où le résultat.

- Injectivité de φ.

  Soit $\overline{z_1}$ et $\overline{z_2}$ deux éléments de $\mathbf{C}/\Gamma$ tels que $\varphi(\overline{z_1}) = \varphi(\overline{z_2})$.

  Si $\varphi(\overline{z_1}) = \varphi(\overline{z_2}) = [0 : 1 : 0]$, z_1 et z_2 appartiennent nécessairement à Γ donc sont conjugués modulo Γ donc $\overline{z_1} = \overline{z_2}$.

  Sinon, ni z_1, ni z_2 ne sont nuls, et on a $\wp(z_1) = \wp(z_2)$ et $\wp'(z_1) = \wp'(z_2)$. Comme $\wp$ est paire, $\wp(-z_1) = \wp(z_1) = \wp(z_2)$. Comme $\wp$ est d'ordre deux et que $\overline{z_1} \neq \overline{-z_1}$ puisque $z_1 \neq 0$, le corollaire 2.1 assure que : soit $\overline{z_1} = \overline{z_2}$ et on conclut, soit $\overline{z_2} = \overline{-z_1}$.

  Dans ce dernier cas,

  $$\wp'(z_2) = \wp'(-z_1) \underbrace{=}_{\text{imparité de } \wp'} -\wp'(z_1) \underbrace{=}_{\text{hypothèse}} -\wp'(z_2)$$

  ce qui signifie que $\wp'(z_2) = 0$ et on montre de même que $\wp'(z_1) = 0$. Or, la proposition 2.3 donne les zéros de $\wp'$ dans Π : on en déduit que $\overline{z_1}, \overline{z_2} \in \{\overline{\frac{u}{2}}, \overline{\frac{v}{2}}, \overline{\frac{u+v}{2}}\}$. On remarque facilement que $\overline{\frac{u}{2}} = \overline{\frac{-u}{2}}$, $\overline{\frac{v}{2}} = \overline{\frac{-v}{2}}$ et $\overline{\frac{u+v}{2}} = \overline{\frac{-(u+v)}{2}}$. Donc $\overline{z_1} = \overline{-z_1}$ et $\overline{z_2} = \overline{-z_2}$. Donc $\overline{z_2} = \overline{-z_1} = \overline{z_1}$

  Dans tous les cas, $\overline{z_2} = \overline{z_1}$ et l'injectivité de φ est démontrée.

- Surjectivité de φ.

  Soit $[x : y : z] \in E_\Gamma(\mathbf{C})$. On remarque que E_Γ n'a qu'un seul point à l'infini : $[0 : 1 : 0]$, qui a bien un antécédent par φ, à savoir $\overline{0}$. On considère donc désormais que $z = 1$.

  Comme $\wp$ est d'ordre deux, le corollaire 2.1 montre que $\wp$ prend au moins une fois la valeur x : il existe $z \in \mathbf{C}$ tel que $\wp(z) = x$. Comme

  $$\begin{aligned} \wp'(z)^2 &= 4\wp(z)^3 - g_2(\Gamma)\wp(z) - g_3(\Gamma) \text{ (équation fonctionnelle de } \wp) \\ &= 4x^3 - g_2(\Gamma)x - g_3(\Gamma) \\ &= y^2 \text{ car } [x : y : 1] \in E_\Gamma(\mathbf{C}) \end{aligned}$$

  on a $\wp'(z) = \pm y$.

  Si $\wp'(z) = y$, alors $\varphi(\overline{z}) = [x : y : 1]$.

Si $\wp'(z) = -y$, alors $\varphi(\overline{-z}) = [\wp(-z) : \wp'(-z) : 1] = [\wp(z) : -\wp'(z) : 1] = [x : y : 1]$ (parité de $\wp$ et imparité de $\wp'$)

Tout point de $E_\Gamma(\mathbf{C})$ admet donc un antécédent par φ d'où la surjectivité de cette dernière.

- Holomorphie de φ.

  Si $\overline{z} \neq \overline{0}$, plaçons nous dans la carte affine $z = 1$. Dans cette carte, l'image de $\overline{z}$ est $(\wp(z), \wp'(z))$ et $\wp$ et $\wp'$ sont en effet holomorphes dans un voisinage de z puisque les pôles de ces deux fonctions sont les éléments de Γ.

  Sinon, plaçons nous dans la carte affine $y = 1$. Dans cette carte, l'image de $\overline{0}$ est $(0, 0)$, et l'image d'un élément $\overline{z}$ est $(\frac{\wp(z)}{\wp'(z)}, \frac{1}{\wp'(z)})$. Notons $\psi : \quad z \mapsto \begin{cases} \frac{\wp(z)}{\wp'(z)} & \text{si } z \neq 0 \\ 0 & \text{si } z = 0 \end{cases}$ et $\psi' : \quad z \mapsto \begin{cases} \frac{1}{\wp'(z)} & \text{si } z \neq 0 \\ 0 & \text{si } z = 0 \end{cases}$

  Il s'agit de montrer que ψ et ψ' sont holomorphes autour de 0. Faisons le pour ψ. Sur un disque ouvert centré en zéro, de rayon suffisamment petit et épointé en zéro, noté D, $\wp$ est holomorphe et $\wp'$ est holomorphe et ne s'annule pas. Donc ψ est holomorphe sur D. Montrons qu'elle est continue en zéro : pour $z \in D$,

  $\wp(z) = \frac{1}{z^2} + \alpha(z)$ où α est une fonction holomorphe sur $D \cup \{0\}$ et

  $\wp'(z) = -\frac{2}{z^3} + \beta(z)$ où β est une fonction holomorphe sur $D \cup \{0\}$

  On en déduit que pour tout $z \in D$, $\psi(z) = \frac{z+z^3\alpha(z)}{-2+z^3\beta(z)} \underset{z\to 0}{\longrightarrow} 0 = \psi(0)$

  La fonction ψ est holomorphe sur D et continue en 0 donc holomorphe sur $D \cup \{0\}$.

3.2. **Holomorphie de la réciproque.**

On reprend toutes les notations de la sous-partie 3.1. L'objectif ici est de montrer que la réciproque de l'application φ est holomorphe. De façon à ce que cette affirmation ait un sens, on observe d'abord que $E_\Gamma(\mathbf{C})$ est une surface de Riemann. On dira qu'une surface X est une surface de Riemann si pour tout point de X il existe un voisinage ouvert de ce point homéomorphe à un ouvert de $\mathbf{C}$ avec la condition supplémentaire que les changements de cartes sont biholomorphes.

Soit $[x_0 : y_0 : 1] \in E_\Gamma(\mathbf{C})$. Autour de ce point, les points de $E_\Gamma(\mathbf{C})$ sont ceux sur la courbe $e = y^2 - 4x^3 + g_2x + g_3$. Comme $E_\Gamma(\mathbf{C})$ est une courbe elliptique, pour tous $x, y \in \mathbf{C}$, $\text{grad}(e)(x, y) = \begin{pmatrix} \frac{\partial e}{\partial x}(x, y) & \frac{\partial e}{\partial y}(x, y) \end{pmatrix} \neq 0$.

Si $\frac{\partial e}{\partial y}(x_0, y_0) \neq 0$, le théorème des fonctions implicites assure qu'il existe un voisinage U de x_0, un voisinage V de y_0 et une fonction holomorphe f de U dans V tels que $(x \in U, y \in V \text{ et } e(x, y) = 0) \Leftrightarrow (x \in U \text{ et } y = f(x))$. Donc localement autour de $[x_0 : y_0 : 1]$ les points de $E_\Gamma(\mathbf{C})$ sont de la forme $[x : f(x) : 1]$ pour $x \in U$. Une carte autour de $[x_0 : y_0 : 1]$ est $(U, [x : f(x) : 1] \mapsto x)$ (d'inverse $x \mapsto [x : f(x) : 1]$ qui holomorphe).

Si $\frac{\partial e}{\partial x}(x_0, y_0) \neq 0$, on argumente de la même façon et il existe une fonction g, holomorphe sur un voisinage U' de y_0 à valeurs dans un voisinage V' de x_0 telle que localement autour de $[x_0 : y_0 : 1]$ les points de $E_\Gamma(\mathbf{C})$ sont de la forme $[g(y) : y : 1]$ où $y \in U'$. Une carte autour de $[x_0 : y_0 : 1]$ est $(U', [g(y) : y : 1] \mapsto y)$ (d'inverse $y \mapsto [g(y) : y : 1]$ qui est holomorphe).

Reste à étudier $[0 : 1 : 0] \in E_\Gamma(\mathbf{C})$. On se place dans la carte $y = 1$. Autour de ce point on définit $\tilde{e}(x, z) = z - 4x^3 + g_2 x z^2 + g_3 z^3$. Comme $\frac{\partial \tilde{e}}{\partial z}(0, 0) = 1 \neq 0$, on utilise à nouveau le théorème des fonctions implicites : il existe U'' voisinage de 0, V'' voisinage de 0 et h holomorphe de U'' dans V'' tels que $(x \in U'', z \in V''$ et $\tilde{e}(x, z) = 0) \Leftrightarrow (x \in U''$ et $z = h(x))$. Une carte autour de $[0 : 1 : 0]$ est $(U'', [x : 1 : h(x)] \mapsto x)$.

Vérifions que les changements de carte sont holomorphes.

- Si un point de $E_\Gamma(\mathbf{C})$ peut s'écrire sous les formes $[x : f(x) : 1]$ et $[g(y) : y : 1]$, les applications de changement de carte sont une restriction de f dans un sens et une restriction de g dans l'autre ; applications qui sont toutes deux holomorphes.
- Si un point de $E_\Gamma(\mathbf{C})$ peut s'écrire sous les formes $[x : f(x) : 1]$ et $[x : 1 : h(x)] = [\frac{x}{h(x)} : \frac{1}{h(x)} : 1]$, les applications de changement de carte sont $t \mapsto \frac{t}{f(t)}$ dans un sens et $t \mapsto \frac{t}{h(t)}$ dans l'autre qui sont toutes deux holomorphes car on considère justement un point où ni f ni h ne s'annulent.
- Si un point de $E_\Gamma(\mathbf{C})$ peut s'écrire sous les formes $[g(y) : y : 1]$ et $[x : 1 : h(x)]$, les applications de changements de carte sont une restriction de $\frac{1}{h}$ dans un sens et $t \mapsto \frac{g(t)}{t}$ dans l'autre, qui sont toutes deux holomorphes au voisinage du point considéré pour la même raison que ci dessus.

Théorème 3.2. *L'application φ^{-1} est holomorphe.*

Démonstration : Elle repose sur le théorème d'inversion locale pour les fonctions holomorphes.

Soit $P = [x_0 : y_0 : w_0]$ un point de $E_\Gamma(\mathbf{C})$. Comme φ est bijective, les coordonnées de ce point sont soit de la forme $[\wp(z_0), \wp'(z_0) : 1]$, soit de la forme $[0 : 1 : 0]$. Montrons que φ^{-1} est holomorphe en P.

- Si $w_0 = 1$ et $y_0 \neq 0$ alors $\frac{\partial e}{\partial y}(x_0, y_0) = 2y_0 \neq 0$ et on peut donc utiliser la carte $c : [x : f(x) : 1] \mapsto x$ localement autour de $[x_0 : y_0 : 1]$. On a ainsi $c \circ \varphi : z \mapsto \wp(z)$ et la dérivée de cette fonction ne s'annule pas en z_0 (puisque $\wp'(z_0) = y_0 \neq 0$). On en déduit que $c \circ \varphi$ est localement inversible autour de z_0. Donc $(c \circ \varphi)^{-1} = \varphi^{-1} \circ c^{-1}$ est holomorphe localement autour de z_0 ce qui est la définition de φ^{-1} est holomorphe en P.
- Si $w_0 = 1$ et $y_0 = 0$ alors $\wp'(z_0) = y_0 = 0$ et par la proposition 2.3, on a nécessairement $z_0 \in \{\frac{u}{2}, \frac{v}{2}, \frac{u+v}{2}\}$. D'autre part, comme vu précédemment, on a aussi $\frac{\partial e}{\partial x}(x_0, y_0) \neq 0$ ce qui permet d'utiliser la carte $c : [g(y) : y : 1] \mapsto y$. On a ainsi $c \circ \varphi : z \mapsto \wp'(z)$ et la dérivée de cette fonction ne s'annule pas en z_0 car $\frac{u}{2}, \frac{v}{2}$ et $\frac{u+v}{2}$ sont des zéros simples de $\wp$. Le théorème d'inversion locale conclut à nouveau que $\varphi^{-1} \circ c^{-1}$ est holomorphe autour de z_0 donc que φ^{-1} est holomorphe en P.
- Si $w_0 = 0$ alors on a forcément $P = [0 : 1 : 0]$. On utilise la carte $c : [x : 1 : h(x)] \mapsto x$ et $c \circ \varphi : z \mapsto \frac{\wp(z)}{\wp'(z)}$. Comme 0 est un pôle d'ordre 2 de $\wp$ et est un

pôle d'ordre 3 de $\wp'$, 0 est un zéro d'ordre 1 de $\frac{\wp}{\wp'}$ On en déduit que la dérivée de $c \circ \varphi$ ne s'annule pas en 0 et le théorème d'inversion locale permet encore de conclure que φ^{-1} est holomorphe en P.

Conclusion des deux parties précédentes : Pour tout réseau Γ de $\mathbf{C}$, il existe une bijection biholomorphe entre $\mathbf{C}/\Gamma$ et une certaine courbe elliptique E_Γ.

3.3. **Application : loi de groupe sur une courbe elliptique.**

Rappels : On sait déjà comment munir une courbe elliptique d'une loi interne qu'on note + dans la suite et on peut facilement montrer que $[0:1:0]$ est neutre pour cette loi. Si Γ est un réseau, on peut bien sûr munir $\mathbf{C}/\Gamma$ d'une loi interne qu'on note aussi + via $\overline{z} + \overline{z'} = \overline{z+z'}$. Cette loi est bien définie et on vérifie rapidement que $\mathbf{C}/\Gamma$ muni de cette loi est un groupe commutatif.

On montre ici que l'application φ étudiée précédemment est un isomorphisme de groupes.

Lemme 3.1.

Soit $f : \mathbf{C}/\Gamma \times \mathbf{C}/\Gamma \to \mathbf{C}/\Gamma$ une fonction continue et telle que pour tout $z \in \mathbf{C}/\Gamma$, $f(z,\cdot)$ et $f(\cdot,z)$ sont holomorphes. Alors il existe $a,b,c \in \mathbf{C}$ tels que pour tous $z,z' \in \mathbf{C}$, $f(z,z') \equiv az + bz' + c \ mod\ \Gamma$.

Démonstration : On note (u,v) une base du réseau Γ. On relève f en une application $F : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ qui reste continue globalement et holomorphe par rapport à chacune de ses variables. On a alors pour tous $z,z' \in \mathbf{C}$, pour tous $m,n \in \mathbf{Z}$, l'existence de deux entiers p et q (dépendant de z,z',m et n) tels que $F(z+nu+mv,z') = F(z,z') + pu + qv \quad (\star)$.

Si on fixe m et n, la continuité de F montre que p et q sont des fonctions continues de z et z', mais comme ces fonctions sont à valeurs entières, cela impose qu'elles sont constantes (en z et z').

Soit $m,n \in \mathbf{Z}$ et $z' \in \mathbf{C}$. Par hypothèse, on peut donc dériver l'égalité $(\star)$ par rapport à z pour obtenir (vu le point précédent) $\frac{\partial F}{\partial z}(z+nu+mv,z') = \frac{\partial F}{\partial z}(z,z')$. En quantifiant universellement en m et n, on obtient que $\frac{\partial F}{\partial z}$ est elliptique par rapport à sa première variable. Comme elle est aussi holomorphe par rapport à sa première variable, elle est constante en z. Le même raisonnement montre qu'elle est constante en z' donc globalement constante égale à a. De même, $\frac{\partial F}{\partial z'}$ est constante égale à b.

Considérons dès lors la fonction $g : (z,z') \mapsto F(z,z') - az - bz'$. Elle est holomorphe par rapport à chacune de ses variables et on constate que $\frac{\partial g}{\partial z} = 0 = \frac{\partial g}{\partial z'}$ donc g est constante en z et constante en z' donc globalement constante égale à c. Ce qui conclut.

Théorème 3.3.

Pour tous $z,z' \in \mathbf{C}/\Gamma$, $\varphi(z+z') = \varphi(z) + \varphi(z')$.

Démonstration : On remarque déjà que $\varphi(0) = [0:1:0] := \mathcal{O}$ qui est le neutre pour l'addition sur une courbe elliptique.

Considérons $f : \begin{cases} \mathbf{C}/\Gamma \times \mathbf{C}/\Gamma & \to \quad \mathbf{C}/\Gamma \\ (z,z') & \mapsto \quad \varphi^{-1}(\varphi(z)+\varphi(z')) \end{cases}$

Cette fonction est bien définie puisque φ est bijective. Elle est holomorphe en chacune de ses variables car φ est un biholomorphisme. Elle est aussi globalement continue. Le lemme 3.1 assure donc l'existence de $a, b, c \in \mathbf{C}$ tels que pour tous $z, z' \in \mathbf{C}$, $f(z, z') \equiv az + bz' + c \bmod \Gamma$. Comme $f(0,0) = \varphi^{-1}(\mathcal{O} + \mathcal{O}) = \varphi^{-1}(\mathcal{O}) = 0$, $c \equiv 0 \bmod \Gamma$. De plus, pour tout $z \in \mathbf{C}/\Gamma$, $f(z, 0) = \varphi^{-1}(\varphi(z) + \mathcal{O}) = \varphi^{-1}(\varphi(z)) = z$. Cela contraint à avoir $a \equiv 1 \bmod \Gamma$ et de même $b \equiv 1 \bmod \Gamma$.

Donc pour tous $z, z' \in \mathbf{C}/\Gamma$, $\varphi^{-1}(\varphi(z) + \varphi(z')) = z + z'$. En appliquant φ à cette égalité, on obtient bien ce qu'on attendait.

Remarque : On déduit du théorème 3.3 et du fait que $(\mathbf{C}/\Gamma, +)$ est un groupe commutatif que $(E_\Gamma, +)$ est aussi un groupe commutatif. On a donc montré que + munit toute courbe elliptique de la forme E_Γ d'une loi de groupe. Une question demeure : si E est une courbe elliptique, existe-t-il un réseau Γ tel que E et E_Γ sont égales ? La partie suivante montre que la réponse à cette question est "oui". On en déduit que pour toute courbe elliptique E, $(E, +)$ est un groupe commutatif (ce qui montre l'affirmation laissée en suspens à la sous-partie 1.3).

4. De la courbe au réseau

On a vu qu'on peut associer à tout quotient de $\mathbf{C}$ par un réseau Γ, une courbe elliptique $E_\Gamma = Y^2Z - 4X^3 + g_2(\Gamma)XZ^2 + g_3(\Gamma)Z^3$ grâce à la fonction $\wp$ de Weierstrass associée au réseau Γ qu'on note désormais $\wp_\Gamma$. On montre ici que pour toute courbe elliptique E, il existe une réseau Γ tel que E et E_Γ sont isomorphes.

4.1. j-invariant d'un réseau.

Définition 4.1. *(j-invariant d'un réseau)*

Soit Γ un réseau de $\mathbf{C}$. On définit le j-invariant de ce réseau par

$j(\Gamma) = 1728\frac{g_2(\Gamma)^3}{g_2(\Gamma)^3 - 27g_3(\Gamma)^2}$ *où* $g_2(\Gamma) = 60 \sum\limits_{\gamma \in \Gamma\setminus\{0\}} \frac{1}{\gamma^4}$ *et* $g_3(\Gamma) = 140 \sum\limits_{\gamma \in \Gamma\setminus\{0\}} \frac{1}{\gamma^6}$

Remarque : Cette définition fait sens. En effet, on a déjà vu que $g_2(\Gamma)$ et $g_3(\Gamma)$ sont bien définis. Reste à montrer que $g_2(\Gamma)^3 - 27g_3(\Gamma)^2 \neq 0$. C'est le cas car c'est le discriminant (à un facteur $\frac{1}{16}$ près) du polynôme $4X^3 - g_2(\Gamma)X - g_3(\Gamma)$ dont on a vu dans la démonstration du théorème 3.1 qu'il a trois racines deux à deux distinctes (d'ailleurs, on les connaît).

Proposition 4.1. *(Lien entre j-invariant d'une courbe et j-invariant d'un réseau)*

Soit Γ un réseau et $E_\Gamma = Y^2Z - 4X^3 + g_2(\Gamma)XZ^2 + g_3(\Gamma)Z^3$ la courbe elliptique qui lui est associée. Alors $j(\Gamma) = j(E_\Gamma)$.

Démonstration : La forme de Weierstrass de E_Γ est $Y^2Z - X^3 - aXZ^2 - bZ^3$ avec $a = -\frac{g_2(\Gamma)}{4}$ et $b = -\frac{g_3(\Gamma)}{4}$ (on divise E_Γ par 4 puis on fait la dilatation $Y \leftarrow 2Y$)

$$\begin{aligned}
\text{Donc } j(\Gamma) &= 1728\frac{g_2(\Gamma)^3}{g_2(\Gamma)^3 - 27g_3(\Gamma)^2} \\
&= 1728\frac{-4^3a^3}{-4^3a^3 - 27 \times 4^2b^2} \\
&= 6912\frac{a^3}{4a^3 + 27b^2} = j(E_\Gamma) \text{ comme prévu.}
\end{aligned}$$

Définition 4.2. *(Réseaux homothétiques)*

Deux réseaux Γ et Γ' sont dits homothétiques s'il existe $\lambda \in \mathbf{C}^\star$ tel que $\Gamma' = \lambda\Gamma$.

Proposition 4.2. *(Déterminons si deux réseaux sont homothétiques)*
Deux réseaux sont homothétiques si et seulement si ils ont même j-invariant.

Remarque : Cette équivalence est à mettre en parallèle avec le fait que deux courbes elliptiques sont isomorphes si et seulement si elles ont même j-invariant. On se sert d'ailleurs de cette propriété dans la

Démonstration :
Si $\Gamma' = \lambda\Gamma$, un changement d'indice dans les sommes définissant $g_2(\Gamma')$ et $g_3(\Gamma')$ montre que $g_2(\Gamma') = \frac{1}{\lambda^4}g_2(\Gamma)$ et $g_3(\Gamma') = \frac{1}{\lambda^6}g_3(\Gamma)$. En remplaçant dans l'expression de $j(\Gamma')$, on trouve que $j(\Gamma') = j(\Gamma)$.

Réciproquement, supposons que $j(\Gamma) = j(\Gamma')$. Comme précédemment, on note $E_\Gamma = Y^2Z - X^3 - aXZ^2 - bZ^3$ (respectivement $E_{\Gamma'} = Y^2Z - X^3 - a'XZ^2 - b'Z^3$) la courbe elliptique associée au réseau Γ (respectivement Γ'). La proposition 4.1 assure que $j(E_\Gamma) = j(E_{\Gamma'})$. Donc E_Γ et $E_{\Gamma'}$ sont isomorphes. Donc il existe $\lambda \in \mathbf{C}^\star$ tel que $a = \lambda^4 a'$ et $b = \lambda^6 b'$. On aimerait monter que $\Gamma' = \lambda\Gamma$ ce qui conclurait.
Comme dans la démonstration de la proposition 4.1, $g_2(\Gamma') = -4a'$ et $g_2(\Gamma) = -4a$. Donc

$$g_2(\Gamma') = -4a' = \frac{-4a}{\lambda^4} = \frac{1}{\lambda^4}g_2(\Gamma) = g_2(\lambda\Gamma)$$

De même, $g_3(\Gamma') = g_3(\lambda\Gamma)$. Pour conclure, montrons les deux lemmes suivants :

Lemme 4.1. *(DSL de $\wp$ en zéro)*
Soit Γ un réseau. Le développement en série de Laurent de $\wp_\Gamma$ au voisinage de zéro est :

$$\wp_\Gamma(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty}(2n+1)G_{2n+2}(\Gamma)z^{2n}$$

où pour tout entier $k > 2$, $G_k(\Gamma) = \sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^k}$ est la série (absolument convergente) d'Eisenstein de poids k.

Démonstration :
On sait que pour tout $x \in \mathbf{C}$ tel que $|x| < 1$, $\frac{1}{(1-x)^2} = \sum_{n=0}^{+\infty}(n+1)x^n$
Notons (u, v) une base du réseau Γ. Alors, pour tout $z \in \mathbf{C}$ tel que $|z| < min(|u|, |v|, |u+v|)$ et pour tout $\gamma \in \Gamma$, on a $\left|\frac{z}{\gamma}\right| < 1$ et donc

$$\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} = \frac{1}{\gamma^2}\left(\frac{1}{(1-\frac{z}{\gamma})^2} - 1\right) = \sum_{n=1}^{+\infty}\frac{(n+1)z^n}{\gamma^{n+2}}$$

Donc pour de tels z,

$$
\begin{aligned}
\wp_\Gamma(z) &= \frac{1}{z^2} + \sum_{\gamma\in\Gamma\setminus\{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}\right) \\
&= \frac{1}{z^2} + \sum_{\gamma\in\Gamma\setminus\{0\}} \sum_{n=1}^{+\infty} (n+1)\frac{z^n}{\gamma^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{+\infty} (n+1)z^n \times \underbrace{\left(\sum_{\gamma\in\Gamma\setminus\{0\}} \frac{1}{\gamma^{n+2}}\right)}_{=G_{n+2}(\Gamma)} \text{ (inversion valide)} \\
&= \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1)G_{2n+2}(\Gamma)z^{2n} \text{ (car } \wp_\Gamma \text{ est paire)}
\end{aligned}
$$

Lemme 4.2. *($g_2(\Gamma)$ et $g_3(\Gamma)$ déterminent Γ)*
Soit Γ et Γ' deux réseaux tels que $g_2(\Gamma) = g_2(\Gamma')$ et $g_3(\Gamma) = g_3(\Gamma')$. Alors $\Gamma = \Gamma'$.

Démonstration : Pour montrer ce résultat, on montre que $\wp_\Gamma$ et $\wp_{\Gamma'}$ ont même développement en série de Laurent sur un voisinage épointé de zéro.

Le lemme 4.1 assure qu'il existe un voisinage de zéro épointé en zéro, noté V, tel que pour tout $z \in V$,

$$\wp_\Gamma(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1)G_{2n+2}(\Gamma)z^{2n} = \frac{1}{z^2} + \sum_{n=1}^{+\infty} a_n z^{2n}$$

Montrons que la connaissance de $g_2(\Gamma)$ et $g_3(\Gamma)$ entraîne la celle de tous les a_n.

On a déjà $g_2(\Gamma) = 60G_4$ par définition et $3G_4 = a_1$ en comparant les coefficients devant z^2 dans le développement ci dessus. Donc $a_1 = \frac{g_2(\Gamma)}{20}$ Un raisonnement similaire montre que $a_2 = \frac{g_3(\Gamma)}{28}$.

D'autre part, $\wp_\Gamma$ vérifie $\wp_\Gamma'(z)^2 = 4\wp_\Gamma^3 - g_2(\Gamma)\wp_\Gamma - g_3(\Gamma)$. Dérivons cette relation pour obtenir $2\wp_\Gamma'(z)\wp_\Gamma''(z) = 12\wp_\Gamma'(z)\wp_\Gamma(z)^2 - g_2(\Gamma)$. Or, les zéros de $\wp_\Gamma'$ sont les multiples de $\frac{u}{2}$, $\frac{v}{2}$ et $\frac{u+v}{2}$ où (u,v) est une base de Γ donc, quitte à réduire V, $\wp_\Gamma'$ ne s'annule pas dans V et pour $z \in V$ on a $\wp_\Gamma''(z) = 6\wp_\Gamma(z)^2 - \frac{g_2(\Gamma)}{2} (\star)$

Les coefficients devant z^{2n} dans l'égalité $(\star)$ se doivent d'être égaux. On en déduit que pour tout $n \geqslant 2$,

$$(2n+3)(2n+2)(2n+1)G_{2n+4}(\Gamma) = 12a_{n+1} + 6\sum_{k=1}^{n-1} a_k a_{n-k}$$

Comme $(2n+3)G_{2n+4}(\Gamma) = a_{n+1}$, on en déduit en isolant a_{n+1} que

$$\text{pour tout } n \geqslant 2, \quad a_{n+1} = \frac{6\sum_{k=1}^{n-1} a_k a_{n-k}}{(2n+1)(2n+2) - 12}$$

Donc on peut calculer tous les a_n pour $n \geqslant 3$ en fonction de $a_1, ..., a_{n-1}$ et comme a_1 et a_2 sont déterminés pas $g_2(\Gamma)$ et $g_3(\Gamma)$ on en déduit par une récurrence rapide qu'il en est de même pour tous les a_n pour $n \geqslant 3$.

Comme $g_2(\Gamma) = g_2(\Gamma')$ et $g_3(\Gamma) = g_3(\Gamma')$, ce dernier résultat montre que $\wp_\Gamma$ et $\wp_{\Gamma'}$ ont même développement en série de Laurent au voisinage de zéro donc que ces deux fonctions sont égales. L'ensemble des pôles de $\wp_\Gamma$, à savoir Γ, est donc égal à l'ensemble des pôles de $\wp_{\Gamma'}$, c'est-à-dire Γ'. Donc $\Gamma = \Gamma'$.

Reprenons la démonstration de la proposition 4.2. Comme $g_2(\Gamma') = g_2(\lambda\Gamma)$ et que $g_3(\Gamma') = g_3(\lambda\Gamma)$, le lemme 4.2 assure que $\Gamma' = \lambda\Gamma$ comme annoncé.

Remarque : Résumons. Si Γ et Γ' sont deux réseaux, les conditions suivantes sont équivalentes :

(1) Γ et Γ' sont homothétiques
(2) $j(\Gamma) = j(\Gamma')$
(3) $j(E_\Gamma) = j(E_{\Gamma'})$
(4) E_Γ et $E_{\Gamma'}$ sont isomorphes

4.2. **Encodage des réseaux de C.**

4.2.1. *Action de $PSL_2(\mathbf{Z})$ sur le demi plan de Poincaré.*

Définition 4.3. *(Action d'un groupe sur un ensemble)*
Soit $(G, \cdot)$ un groupe de neutre e et E un ensemble. Une action de G sur E est une application $\star : G \times E \to E$ telle que :

- $\forall x \in E, e \star x = x$
- $\forall g, g' \in G, \forall x \in E, g' \star (g \star x) = (g' \cdot g) \star x$

Définition 4.4. *(Domaine fondamental)*
Soit G un groupe agissant sur un ensemble E. Un domaine fondamental de l'action de G sur E est une partie D de E telle que :

- $\forall x \in E, \exists g \in G$ *tel que* $gx \in D$ *(on sous entend l'action)*
- $\forall x, x' \in D$, *s'il existe* $g \in G$ *tel que* $x' = gx$ *alors* $x = x'$

Autrement dit, le domaine D contient un et un seul point par orbite sous l'action de G.

Définition 4.5. *(Demi plan de Poincaré)*
On note $\mathcal{H}$ l'ensemble $\{z \in \mathbf{C} | \mathrm{Im}(z) > 0\}$ et on l'appelle demi plan de Poincaré.

Proposition 4.3. *(Action de $SL_2(\mathbf{Z})$ sur $\mathcal{H}$)*
L'application $\star : \left\{ \begin{array}{lcl} SL_2(\mathbf{Z}) \times \mathcal{H} & \longrightarrow & \mathcal{H} \\ (g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) & \longmapsto & g \star z = gz = \frac{az+b}{cz+d} \end{array} \right.$
est bien définie est est une action du groupe $SL_2(\mathbf{Z})$ sur l'ensemble $\mathcal{H}$.

Démonstration :
On remarque que, $\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ et $\forall z \in \mathcal{H}$, on a :

$$\begin{aligned}\mathrm{Im}(gz) &= \mathrm{Im}\left(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}\right)\\ &= \mathrm{Im}\left(\frac{ac|z|^2+(1+bc)z+bc\overline{z}+bd}{|cz+d|^2}\right) \text{ (car } ad-bc=1)\\ &= \frac{\mathrm{Im}(z)}{|cz+d|^2} \text{ (car } ac|z|^2+bc(z+\overline{z})+bd \in \mathbf{R})\end{aligned}$$

Comme $z \in \mathcal{H}$, $\mathrm{Im}(z) > 0$ et donc $\mathrm{Im}(gz) > 0$ aussi ce qui prouve que $gz \in \mathcal{H}$ donc que $\star$ est bien définie. La vérification du fait que $\star$ est bien une action de groupe tient en un petit calcul.

Remarque : Observons l'ensemble $F = \{g \in SL_2(\mathbf{Z}) | \forall z \in \mathcal{H}, gz = z\}$

Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in F$.

Alors, pour tout $z \in \mathcal{H}$, $\frac{az+b}{cz+d} = z$, c'est à dire $cz^2 + (a-d)z + b = 0$

On en déduit que $c = b = 0$ et que $a = d$. Comme $g \in SL_2(\mathbf{Z})$, $ad - bc = ad = 1$. On en déduit donc que $(a, d) = (1, 1)$ ou $(a, d) = (-1, -1)$.

Donc $g = \pm I_2$. Réciproquement, ces deux éléments appartiennent à F.

L'action précédemment décrite passant au quotient, on considère donc l'action de $G = PSL_2(\mathbf{Z}) = SL_2(\mathbf{Z})/\{\pm I_2\}$ (nommé groupe modulaire) sur $\mathcal{H}$.

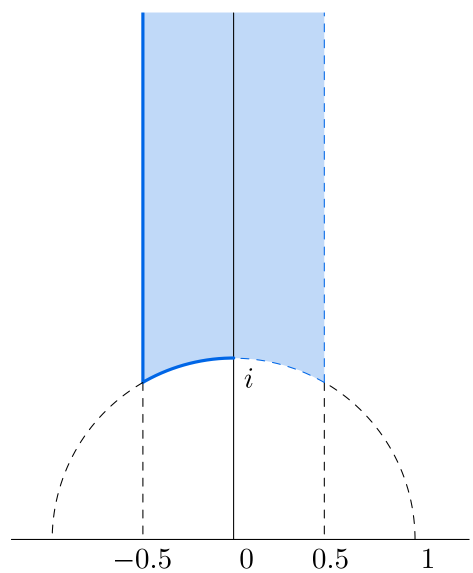
4.2.2. *Domaine fondamental de l'action de $PSL_2(\mathbf{Z})$ sur $\mathcal{H}$.*

Notations :

Dans tout ce qui suit, on note :

$D = \{z \in \mathbf{C} | |z| > 1 \text{ et } -\frac{1}{2} \leqslant \mathrm{Re}(z) < \frac{1}{2}\} \cup \{z \in \mathbf{C} | |z| = 1 \text{ et } \mathrm{Arg}(z) \in [\frac{\pi}{2}, \frac{2\pi}{3}]\}$

Le domaine D correspond au domaine colorié en bleu ci-contre (avec la convention, trait plein = fermé, trait pointillé = ouvert)



On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Remarquons que S correspond à l'application $z \mapsto -\frac{1}{z}$ et que T correspond à la translation $z \mapsto z+1$. On note enfin G' le sous groupe de G engendré par (les classes de) T et S (on confondra les éléments de $SL_2(\mathbf{Z})$ et leurs classes modulo $\pm I_2$)

Lemme 4.3. *(Toute orbite sous l'action de G rencontre D... et même mieux)*

Pour tout $z \in \mathcal{H}$, il existe $g \in G'$ tel que $gz \in D$.

Démonstration :

Soit $z \in \mathcal{H}$.

Il existe $n \in \mathbf{Z}$ (à savoir, $-\mathrm{E}(\mathrm{Re}(z)+\frac{1}{2})$) tel que $T^n z$ voit sa partie réelle être dans $[\frac{-1}{2}, \frac{1}{2}[$. Si $|T^n z| > 1$, $g = T^n$ convient. Si $|T^n z| < 1$ alors $|ST^n z| > 1$ donc $g = ST^n$ convient. Si $|T^n z| = 1$ et que l'argument de $T^n z$ peut être choisi entre $\frac{\pi}{2}$ et $\frac{2\pi}{3}$, $g = T^n$ convient et sinon, l'argument de $ST^n z$ s'y trouve et on conclut encore une fois.

Lemme 4.4. *(Il n'y a qu'un point par orbite dans D)*

Pour tous $z, z' \in D$, s'il existe $g \in G$ tel que $z' = gz$ alors $z = z'$

Démonstration :

Soit $z \in D$ tel qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G'$ vérifiant $z' = gz \in D$.

Il est loisible de supposer $\mathrm{Im}(z') = \mathrm{Im}(gz) \geqslant \mathrm{Im}(z)$ (sinon, $\mathrm{Im}(z) \geqslant \mathrm{Im}(z')$ c'est à dire $\mathrm{Im}(g^{-1}z') \geqslant \mathrm{Im}(z')$ et on applique le raisonnement suivant avec g^{-1} et z' plutôt qu'avec g et z).

Cette inégalité associée au fait que $\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$ implique que

$1 \geqslant |cz+d| \geqslant |c|\mathrm{Im}(z)$. Comme $|z| \geqslant 1$ et que $|\mathrm{Re}(z)| \leqslant \frac{1}{2}$, $\mathrm{Im}(z) \geqslant \sqrt{1-\mathrm{Re}(z)^2} \geqslant \frac{\sqrt{3}}{2}$ et donc $|c| \leqslant \frac{1}{\mathrm{Im}(z)} \leqslant \frac{2}{\sqrt{3}}$. Comme c est un entier, c ne peut donc valoir que $0, 1$ ou -1.

- Si $c = 0$.

  Dans ce cas, $1 \geqslant |cz+d| = |d|$. Donc $d \in \{0, 1, -1\}$. Mais d ne peut valoir 0 sinon $ad - bc = 0 \neq 1$. Donc $d \in \{1, -1\}$.

  (a) Si $d = 1$.

  Alors $ad - bc = 1$ force a à valoir 1 et g est une translation par b, c'est à dire $gz = z + b$. Les conditions sur les parties réelles de gz et de z imposent que :

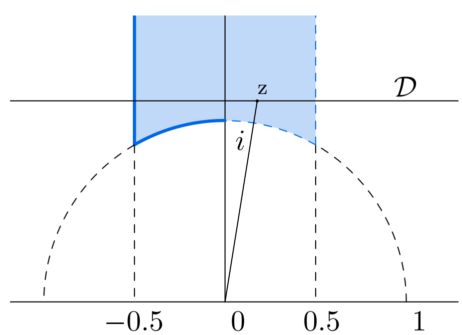
  $$-1 < -\frac{1}{2} - \mathrm{Re}(z) \leqslant b = \mathrm{Re}(gz) - \mathrm{Re}(z) < \frac{1}{2} - \mathrm{Re}(z) \leqslant 1$$

  On en déduit que $b = 0$ puis que $z' = z + 0 = z$.

  (b) Si $d = -1$ alors de même, g est une translation par $-b$ et on applique le même raisonnement qu'au point précédent.

- Si $c = 1$.

  Dans ce cas, $|z+d| \leqslant 1$. Cela veut dire que, comme indiqué sur le dessin ci-contre, $z+d$ se trouve à la fois sur la droite $\mathcal{D}$ et dans le disque unité. Si $|z| > 1$, on aboutit immédiatement à une contradiction. Donc $|z| = 1$.



(a) Si $z \neq e^{\frac{2i\pi}{3}}$ alors $d = 0$ (sinon, on obtient une contradiction avec $|z+d| \leqslant 1$). Comme $ad - bc = 1$, $b = -1$. On a donc $z' = gz = a - \frac{1}{z} = a - \overline{z}$ puisque $|z| = 1$. La condition sur z impose que $\mathrm{Re}(z) \in]-\frac{1}{2}, 0]$ donc que $a = 0$ (sinon $\mathrm{Re}(gz) = a - \mathrm{Re}(\overline{z}) \notin [-\frac{1}{2}, \frac{1}{2}[$ donc $z' \notin D$). On en déduit que $z' = -\overline{z}$. Mais alors $|z'| = 1$ donc pour que z' reste dans D, on doit avoir $\mathrm{Arg}(z') \in [\frac{\pi}{2}, \frac{3\pi}{2}]$. Comme $\mathrm{Arg}(z)$ est compris dans ce même intervalle, on a d'autre part $\mathrm{Arg}(z') = \pi - \mathrm{Arg}(z) \leqslant \frac{\pi}{2}$. On a donc nécessairement $z' = i$. Mais comme $z = -\overline{z'}$, on a aussi $z = i$ et donc on a toujours $z = z'$.

(b) Si $z = e^{\frac{2i\pi}{3}}$ alors $d \in \{0, 1\}$ (sinon, on obtient une contradiction avec $|z+d| \leqslant 1$).
Si $d = 0$, en tenant le même raisonnement qu'au point ci-dessus, $z' = gz = a - \overline{z} = (a + \frac{1}{2}) + \frac{i\sqrt{3}}{2}$. Pour garantir $z' \in D$, on doit avoir $a = -1$ et on retrouve bien $z = z'$.

Si $d = 1$, comme $ad - bc = 1$ alors $a - b = 1$ et

$$z' = gz = \frac{az + b}{z + 1} = \frac{az + a - 1}{z + 1} = \frac{ae^{\frac{2i\pi}{3}} + a - 1}{1 + e^{\frac{2i\pi}{3}}} = a + \frac{1}{1 + e^{\frac{2i\pi}{3}}} = a + e^{\frac{2i\pi}{3}}$$

Comme $z' \in D$, cela implique que $a = 0$. Encore un fois, $z = z'$.

- Si $c = -1$, on travaille avec l'autre représentant de g modulo $\pm I_2$ et on retrouve alors le cas précédent où $c = 1$.

Théorème 4.1. *L'ensemble $\mathcal{H}/PSL_2(\mathbf{Z})$ s'identifie au domaine D.*

Démonstration :
Il s'agit de démontrer que, pour tout $z \in \mathcal{H}$, il existe un unique élément de $g \in PSL_2(\mathbf{Z})$ tel que $gz \in D$. Le lemme 4.3 donne l'existence et le lemme 4.4 donne l'unicité.

4.2.3. *Lien avec les réseaux de* $\mathbf{C}$.
Notations : On note $\mathcal{R}$ l'ensemble des réseaux de $\mathbf{C}$ et $H = \{(z_1, z_2) \in \mathbf{C}^2 | \mathrm{Im}\left(\frac{z_1}{z_2}\right) > 0\} = \{(z_1, z_2) \in \mathbf{C}^2 | \frac{z_1}{z_2} \in \mathcal{H}\}$. On continue de noter D le domaine du demi plan de Poincaré défini dans la section précédente.

Soit Γ un réseau de $\mathbf{C}$ de base (z_1, z_2). Comme (z_1, z_2) est une base, l'un au moins de ces complexes n'est pas réel donc le rapport de ces complexes n'est pas réel non plus. On en déduit que $\mathrm{Im}\left(\frac{z_1}{z_2}\right) \neq 0$. Quitte à changer z_1 en $-z_1$ (ce qui ne modifie pas le réseau Γ), on peut supposer que $\mathrm{Im}\left(\frac{z_1}{z_2}\right) > 0$. Donc, tout réseau de $\mathbf{C}$ admet au moins un élément de H pour base.

Proposition 4.4. *(Action de $SL_2(\mathbf{Z})$ sur H)*
L'application suivante :

$$\bullet \begin{cases} SL_2(\mathbf{Z}) \times H & \longrightarrow \quad H \\ (g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (z_1, z_2)) & \longmapsto \quad g \bullet (z_1, z_2) = g \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (az_1 + bz_2, cz_1 + dz_2) \end{cases}$$

est bien définie est est une action du groupe $SL_2(\mathbf{Z})$ sur l'ensemble H.

De plus, pour tout $g \in SL_2(\mathbf{Z})$, pour tous couples de complexes (z_1, z_2) et (w_1, w_2), si $g \bullet (z_1, z_2) = (w_1, w_2)$ alors $g \star \frac{z_1}{z_2} = \frac{w_1}{w_2}$ où on rappelle que $\star$ est l'action de $SL_2(\mathbf{Z})$ sur $\mathcal{H}$ définie plus haut.

Démonstration :

Le lien avancé entre $\bullet$ et $\star$ se vérifie par le calcul. Il permet ensuite de déduire du fait que $\star$ est une action le fait que $\bullet$ en est une.

Lemme 4.5. *Soit $(z_1, z_2), (w_1, w_2) \in H$. Ces couples sont deux bases du même réseau de $\mathbf{C}$ si et seulement si il existe $g \in SL_2(\mathbf{Z})$ telle que $g \bullet (z_1, z_2) = (w_1, w_2)$.*

Démonstration :

Si (z_1, z_2) et (w_1, w_2) sont deux bases du même réseau de $\mathbf{C}$ alors il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$ tel que $g \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$. Vu le lien entre $\star$ et $\bullet$ souligné en proposition 4.4, cela veut dire que $g\frac{z_1}{z_2} = \frac{w_1}{w_2}$. Pour montrer l'une des implications, il suffit de montrer que $\det(g) = 1$. Comme $g \in GL_2(\mathbf{Z})$, on sait déjà que $\det(g) = \pm 1$. De plus,

$$0 < \mathrm{Im}\left(\frac{w_1}{w_2}\right) = \mathrm{Im}\left(g\frac{z_1}{z_2}\right) = \frac{\det(g)\mathrm{Im}(\frac{z_1}{z_2})}{|c\frac{z_1}{z_2} + d|}$$

par un calcul similaire à celui de la proposition 4.3. Comme $\mathrm{Im}(\frac{z_1}{z_2}) > 0$ aussi, cela contraint $\det(g)$ à être strictement positif donc $\det(g) = 1$.

Réciproquement, s'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ tel que $g \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$, alors $w_1 = az_1 + bz_2$ et $w_2 = cz_1 + dz_2$ avec $a, b, c, d \in \mathbf{Z}$. Donc $\mathbf{Z}w_1 \oplus \mathbf{Z}w_2 \subset \mathbf{Z}z_1 \oplus \mathbf{Z}z_2$. De même, en travaillant avec g^{-1}, $z_1 = dw_1 - bw_2$ et $z_2 = -cw_1 + aw_2$ donc $\mathbf{Z}z_1 \oplus \mathbf{Z}z_2 \subset \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$. Donc (z_1, z_2) et (w_1, w_2) sont deux bases du même réseau.

Proposition 4.5. *(Action sur $\mathcal{R}$)*

L'application $\cdot \begin{cases} \mathbf{C}^\star \times \mathcal{R} & \longrightarrow \quad \mathcal{R} \\ (\alpha, \mathbf{Z}z_1 \oplus \mathbf{Z}z_2) & \longmapsto \quad \mathbf{Z}(\alpha z_1) \oplus \mathbf{Z}(\alpha z_2) \end{cases}$

est une action du groupe multiplicatif $\mathbf{C}^\star$ sur $\mathcal{R}$. La vérification est immédiate.

Remarque : Un élément du quotient $\mathcal{R}/\mathbf{C}^\star$ est un réseau "modulo homothétie".

Théorème 4.2. *Il existe une bijection entre $\mathcal{R}/\mathbf{C}^\star$ et D.*

Démonstration :

Considérons l'application $\varphi : \begin{cases} \mathcal{R}/\mathbf{C}^\star & \longrightarrow \quad \mathcal{H}/PSL_2(\mathbf{Z}) \\ \overline{\mathbf{Z}z_1 \oplus \mathbf{Z}z_2} & \longmapsto \quad \frac{z_1}{z_2} \bmod PSL_2(\mathbf{Z}) \end{cases}$ où $(z_1, z_2) \in H$ (ce qui est toujours possible d'après une remarque précédente)

Montrons que pour tout élément $x \in \mathcal{R}/\mathbf{C}^\star$, $\varphi(x)$ ne dépend ni du représentant r choisi pour x, ni du choix de la base de r du moment qu'elle se trouve dans H :

Si $\mathbf{Z}z_1 \oplus \mathbf{Z}z_2 \in \mathcal{R}$ et $\alpha \in \mathbf{C}^\star$, $\varphi(\mathbf{Z}z_1 \oplus \mathbf{Z}z_2) = \frac{z_1}{z_2} = \frac{\alpha z_1}{\alpha z_2} = \varphi(\mathbf{Z}(\alpha z_1) \oplus \mathbf{Z}(\alpha z_2))$ ce qui assure le premier point.

De plus, si (z_1, z_2) et (w_1, w_2) sont deux éléments de H et bases d'un même réseau, le lemme 4.5 assure qu'il existe $g \in SL_2(\mathbf{Z})$ tel que $(w_1, w_2) = g \bullet (z_1, z_2)$. Donc $\varphi(\mathbf{Z}z_1 \oplus \mathbf{Z}z_2) = \frac{z_1}{z_2} = g \star \frac{w_1}{w_2} = g \star \varphi(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2)$ et les images $\varphi(\mathbf{Z}z_1 \oplus \mathbf{Z}z_2)$ et $\varphi(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2)$

sont conjuguées modulo $SL_2(\mathbf{Z})$ donc sont égales dans $\mathcal{H}/PSL_2(\mathbf{Z})$. Ce qui montre le second point.

Ces deux observations montrent que φ est bien définie.

Soit $\overline{u} \in \mathcal{H}/PSL_2(\mathbf{Z})$ et u un représentant de cette classe. Comme $\mathrm{Im}(u) > 0$, $(1, u)$ est une base de $\mathbf{C}$ donc $\mathbf{Z} \oplus \mathbf{Z}u$ est un réseau de $\mathbf{C}$. De plus $\varphi(\mathbf{Z} \oplus \mathbf{Z}u) = u$: on a trouvé un antécédent à $\overline{u}$ par φ. Cette fonction est donc surjective.

Si $\varphi(\overline{\mathbf{Z}z_1 \oplus \mathbf{Z}z_2}) = \varphi(\overline{\mathbf{Z}w_1 \oplus \mathbf{Z}w_2})$ alors $\frac{z_1}{z_2}$ et $\frac{w_1}{w_2}$ sont dans la même classe de $\mathcal{H}$ modulo $PSL_2(\mathbf{Z})$. Donc il existe $g \in SL_2(\mathbf{Z})$ tel que $\frac{z_1}{z_2} = \pm g \frac{w_1}{w_2}$. Si le signe devant g est $+$, alors le lemme 4.5 assure que (z_1, z_2) et (w_1, w_2) sont deux bases du même réseau. Si le signe devant g est $-$ alors $\frac{z_1}{z_2} = (-g)\frac{-w_1}{-w_2}$ avec $-g \in SL_2(\mathbf{Z})$ et le lemme 4.5 assure que (z_1, z_2) et $(-w_1, -w_2)$ sont deux bases du même réseau. Comme on considère les réseaux modulo les homothéties, on a $\overline{\mathbf{Z}z_1 \oplus \mathbf{Z}z_2} = \overline{\mathbf{Z}w_1 \oplus \mathbf{Z}w_2}$ dans les deux cas ce qui permet d'affirmer que φ est injective.

$\mathcal{R}/\mathbf{C}^\star$ est ainsi en bijection avec $\mathcal{H}/PSL_2(\mathbf{Z})$ et par le théorème 4.1, $\mathcal{H}/PSL_2(\mathbf{Z})$ est en bijection avec D. D'où la conclusion du théorème.

Conclusion

Toute classe de $\mathcal{R}/\mathbf{C}^\star$ est représentée par un unique élément de D. Dit autrement, tout réseau de $\mathbf{C}$ modulo homothétie est encodé par un unique point appartenant à un domaine explicite inclus dans le demi plan de Poincaré.

Proposition 4.6. *Le groupe $G = PSL_2(\mathbf{Z})$ est engendré par S et T.*

Démonstration : Il suffit de montrer que $G \subset G'$ pour conclure. Soit $g \in G$ et notons $z_0 = 2i$ et $z = gz_0$. On a vu plus haut qu'il existe $g' \in G'$ tel que $g'z \in D$. Alors, z_0 et $g'z = g'gz_0$ sont conjugués modulo G et sont tout deux dans D donc sont égaux. Donc $g'g \in \{h \in G | hz_0 = z_0\}$. Or, ce dernier ensemble est réduit à l'identité (c'est en fait le cas pour tous les z_0 de D à l'exception de i et $e^{\frac{2i\pi}{3}}$. La démonstration est très semblable à celle de lemme 4.4). Donc $g = g'^{-1} \in G'$.

4.3. Tout complexe est le j-invariant d'un réseau.

Définition 4.6. *(Fonction j)*

On définit la fonction $j : \mathbb{H} \to \mathbf{C}$ par $\forall z \in \mathbb{H}$, $j(z) = j(\Gamma)$ où Γ est un réseau de base $(1, z)$.

De même, on définit $g_2 : \mathbb{H} \to \mathbf{C}$ et $g_3 : \mathbb{H} \to \mathbf{C}$ par $\forall z \in \mathbb{H}$, $g_2(z) = g_2(\Gamma)$ et $g_3(z) = g_3(\Gamma)$ où Γ est un réseau de base $(1, z)$.

Proposition 4.7. *(Propriétés de j)*

(1) *La fonction j est holomorphe sur $\mathbb{H}$.*
(2) *Pour tout $z \in \mathbb{H}$, $j(z+1) = j(z)$ et $j(\frac{-1}{z}) = j(z)$.*
(3) *Pour tout $\gamma \in PSL_2(\mathbf{Z})$, pour tout $z \in \mathbb{H}$, $j(\gamma z) = j(z)$.*
(4) *Pour tous $z, z' \in \mathbb{H}$, $j(z) = j(z')$ si et seulement si il existe $\gamma \in PSL_2(\mathbf{Z})$ tel que $z' = \gamma z$.*
(5) *$j : D \to \mathbf{C}$ est bijective. (où D est le domaine fondamental pour l'action de $PSL_2(\mathbf{Z})$ qu'on a étudié précédemment)*

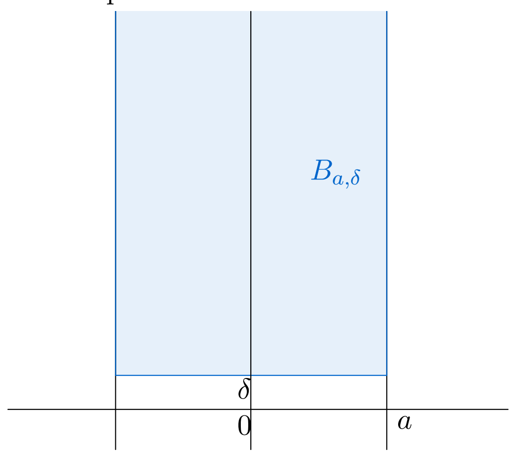
Démonstration :

(1) Par définition du j-invariant d'un réseau, pour tout $z \in \mathbb{H}$, $j(z) = 1728\frac{g_2(z)^3}{g_2(z)^3-27g_3(z)^2}$ et on a montré dans la remarque suivant la définition 4.1 que pour tout $z \in \mathbb{H}$, $g_2(z)^3 - 27g_3(z)^2 \neq 0$. Il suffit donc pour conclure de montrer que g_2 et g_3 sont holomorphes sur $\mathbb{H}$.

Faisons le pour g_2 (le même raisonnement s'applique à g_3).

Par définition, $g_2(z) = 60 \sum\limits_{(n,m)\in\mathbf{Z}\backslash\{(0,0)\}} g_{n,m}$ où $g_{n,m} : z \mapsto \frac{1}{(n+mz)^4}$ est holomorphe sur $\mathbb{H}$ (son seul pôle dans $\mathbf{C}$ est $\frac{-n}{m} \notin \mathbb{H}$). Montrer que $\sum\limits_{(n,m)\in\mathbf{Z}\backslash\{(0,0)\}} g_{n,m}$ converge normalement sur tout compact de $\mathbb{H}$ permettrait de conclure.

Montrons alors que $\sum\limits_{(n,m)\in\mathbf{Z}\backslash\{(0,0)\}} g_{n,m}$ converge normalement sur toute bande $B_{a,\delta} = \{x+iy \in \mathbf{C} | |x| \leqslant a \text{ et } y \geqslant \delta\}$ où $a > 0$ et $\delta > 0$.



Pour ce faire, il suffit de montrer qu'il existe $M > 0$ (dépendant de a et δ) tel que pour tout $z \in B_{a,\delta}$ et tout $(m,n) \in \mathbf{Z}\backslash\{(0,0)\}$, on ait

$$\frac{1}{|m+nz|^4} \leqslant \frac{1}{|m+in|^4} \qquad (1)$$

En effet on aura alors

$$\sum_{n,m} \sup_{z\in B_{a,\delta}} \frac{1}{|m+nz|^4} \leqslant \sum_{n,m} \frac{M}{|m+in|^4} = \sum_{\gamma\in\Gamma\backslash\{0\}} \frac{1}{|\gamma|^4} < +\infty$$

où Γ est un réseau de base $(1,i)$. On remarque que la puissance 4 ici présente peut être remplacée par $k > 2$ sans changer le résultat (en particulier, le raisonnement qui suit marche aussi pour g_3)

Soit $z = x+iy \in B_{a,\delta}$ et $(n,m) \in \mathbf{Z}\backslash\{(0,0)\}$. Pour montrer (1), il suffit de trouver $K > 0$ tel que $|m+nz|^2 > K|m+ni|^2$ c'est-à-dire tel que

$$(m+nx)^2 + (ny)^2 > K(m^2+n^2) \qquad (2)$$

Si $n = 0$, cette inégalité est vraie pour tout $K \in]0,1[$. Sinon, notons $q = \frac{m}{n}$. Montrer (2) revient alors à trouver $K' > 0$ tel que

$$\frac{(q+x)^2+y^2}{1+q^2} > K \qquad (3)$$

Montrons que $K' = \frac{\delta^2}{1+(a+\delta)^2}$ convient :

Si $|q| \leqslant a+\delta$, (3) est immédiat puisque $(q+x)^2 \geqslant 0$ et $y \geqslant \delta$. Si $|\delta| > a+\delta$ alors $\left|\frac{x}{q}\right| < \frac{|x|}{|a+\delta|} \leqslant \frac{a}{a+\delta} < 1$ donc

$$|q+x| = q\left|1+\frac{x}{q}\right| \geqslant q(1-\left|\frac{x}{q}\right|) > q\left(1-\frac{a}{a+\delta}\right) = \frac{q\delta}{a+\delta}$$

Puis :

$$\frac{(q+x)^2+y^2}{1+q^2} > \frac{\delta^2}{(a+\delta)^2} \times \frac{q^2}{(1+q)^2} \underbrace{\geqslant}_{(\star)} \frac{\delta^2}{(a+\delta)^2} \times \frac{(a+\delta)^2}{1+(a+\delta)^2} = K'$$

L'inégalité $(\star)$ est vraie car $x \mapsto \frac{x^2}{(1+x)^2}$ est croissante et on est dans le cas où $|q| > a+\delta$.

En prenant $K = \min(\frac{1}{2}, K')$, on obtient un réel strictement positif vérifiant (2) et on peut conclure.

(2) Soit $z \in \mathbb{H}$. On sait déjà que $\frac{-1}{z} \in \mathbb{H}$ aussi. On remarque que $(1, z)$ et $(1, z+1)$ sont deux bases du même réseau donc $j(z) = j(z+1)$. D'autre part, les réseaux de bases $(1, z)$ et $(1, \frac{1}{z})$ sont homothétiques (de rapport $\frac{1}{z}$) et le réseau de base $(1, \frac{1}{z})$ est le même que celui de base $(1, \frac{1}{z})$. La proposition 4.2 assure alors que $j(z) = j(\frac{-1}{z})$.

(3) Comme $z \mapsto \frac{-1}{z}$ (qui correspond matriciellement à $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$) et $z \mapsto z+1$ (qui correspond matriciellement à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$) engendrent $PSL_2(\mathbf{Z})$, le point (2) permet de conclure que j est invariante sous l'action de $PSL_2(\mathbf{Z})$.

(4) Le sens de la droite vers la gauche est clair vu le point (3). Réciproquement, si $j(z) = j(z')$ alors les réseaux de bases $(1, z)$ et $(1, z')$ sont homothétiques par la proposition 4.2. On en déduit qu'il existe $\lambda \in \mathbf{C}^\star$ tel que le réseau de base $(1, z')$ est aussi celui de base $(\lambda, \lambda z)$. Donc il existe $a, b, c, d \in \mathbf{Z}$ tels que $\begin{cases} z' = a\lambda z + b\lambda \\ 1 = c\lambda z + d\lambda \end{cases}$.

La deuxième équation permet de trouver λ, et, en remplaçant λ dans la première, on trouve que

$$z' = \frac{az+b}{cz+d} = \gamma z \text{ avec } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

En remarquant que $(1, z)$ et $(\frac{1}{\lambda}, \frac{z'}{\lambda})$ sont aussi deux bases d'un même réseau, et en appliquant le même raisonnement que ci dessus, on trouve qu'il existe une matrice $\gamma' \in M_2(\mathbf{Z})$ tel que $z = \gamma' z'$. Donc $z = \gamma'\gamma z$ et comme γ et γ' sont à coefficients entiers, on en déduit que $\det(\gamma) = \pm 1$. Mais comme z et z' sont dans $\mathbb{H}$, nécessairement $\det(\gamma) = 1$. On a donc bien $z' = \gamma z$ avec $\gamma \in SL_2(\mathbf{Z})$.

Remarque : Tout ce qu'on a montré jusqu'ici montre que pour connaître le comportement de la fonction j, il suffit de l'étudier sur un domaine fondamental de l'action de $PSL_2(\mathbf{Z})$ sur $\mathbb{H}$, D par exemple.

(5) On veut montrer que $j : D \mapsto \mathbf{C}$ est bijective. Si $z, z' \in D$ sont tels que $j(z) = j(z')$ alors le point (4) montre qu'il existe $\gamma \in PSL_2(\mathbf{Z})$ tel que $z' = \gamma z$. La définition de domaine fondamental assure alors que $z = z'$. Donc j est injective.

Pour montrer la surjectivité, on montre d'abord que $j(\mathbb{H})$ est ouvert et fermé dans $\mathbf{C}$. Comme $j(\mathbb{H}) \neq \varnothing$ et que $\mathbf{C}$ est connexe, cela assurera que $j(\mathbb{H}) = \mathbf{C}$. Puis, comme j est invariante sous l'action de $PSL_2(\mathbf{Z})$ et que D est un domaine fondamental pour cette action on aura comme attendu $j(D) = \mathbf{C}$.

Soit $z \in \mathbf{C}$. Par définition,

$$g_2(z) = 60 \sum_{(n,m)\in\mathbf{Z}\setminus\{(0,0)\}} \frac{1}{(m+nz)^4} = 60 \left(2\sum_{m=1}^{+\infty} \frac{1}{m^4} + \sum_{\substack{n,m\in\mathbf{Z} \\ n\neq 0}} \frac{1}{(m+nz)^4} \right)$$

La convergence normale montrée au point (1) permet d'échanger sommation et limite lorsque $\mathrm{Im}(z)$ tend vers $+\infty$ dans l'expression ci dessus et comme $\sum_{\substack{n,m\in\mathbf{Z} \\ n\neq 0}} \frac{1}{(m+nz)^4} \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} 0$ on a

$$g_2(z) \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} 120\zeta(4) = \frac{4\pi^4}{3}$$

De même, $g_3(z) \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} 280\zeta(6) = \frac{8\pi^6}{27}$.

On en déduit que $g_2(z)^3 - 27g_3(z)^2 \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} 0$

Puis que $j(z) = 1728\frac{g_2(z)^3}{g_2(z)^3-27g_3(z)^2} \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} +\infty$.

Donc la fonction j est holomorphe et non constante sur $\mathbb{H}$ Le théorème de l'application ouverte conclut que $j(\mathbb{H})$ est un ouvert de $\mathbf{C}$.

Soit $(j(z_n))_{n\in\mathbb{N}}$ convergeant vers $w \in \mathbf{C}$. Comme D est un domaine fondamental et que j est $PSL_2(\mathbf{Z})$ invariante, on peut supposer que tous les z_n sont dans D. Comme $j(z) \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} +\infty$, $(\mathrm{Im}(z_n))_n$ est nécessairement bornée par $B > 1$. Ajouté au fait que les z_n sont dans D, on en déduit que tous les z_n sont dans le compact $K = \{\tau | \mathrm{Re}(\tau) \in [\frac{-1}{2}, \frac{1}{2}], \mathrm{Im}(\tau) \in [\frac{1}{2}, B]\}$. On peut donc extraire de la suite $(z_n)_n$ une sous suite $(z_{\varphi(n)})_n$ qui converge vers $z \in K$. Alors, $j(z_{\varphi(n)}) \underset{n\to+\infty}{\longrightarrow} j(z)$ par continuité de j. Donc $w = j(z)$ et cela montre que $j(\mathbb{H})$ est fermé dans $\mathbf{C}$.

Comme on l'a vu, ça conclut.

Théorème 4.3.
Soit E une courbe elliptique sur $\mathbf{C}$. Il existe un réseau Γ tel que E et E_Γ sont isomorphes.

Démonstration : Par surjectivité de $j : D \to \mathbf{C}$, il existe $z \in D$ tel que $j(z) = j(E)$. Soit dès lors Γ un réseau de base $(1, z)$. On a

$$j(E) = j(z) \underbrace{=}_{\text{par définition de la fonction } j} j(\Gamma) \underbrace{=}_{\text{proposition 4.1}} j(E_\Gamma)$$

Cela montre que E et E_Γ sont isomorphes.

Corollaire 4.1. *(Et même mieux !)*
Soit E une courbe elliptique sur $\mathbf{C}$. Alors il existe un réseau Γ tel que $E = E_\Gamma$.

Démonstration : On sait déjà par le théorème 4.3 qu'il existe un réseau Λ tel que $E = Y^2Z - aX^3 - bXZ^2 - bZ^3$ et $E_\Lambda = Y^2Z - 4X^3 + g_2(\Lambda)XZ^2 + g_3(\Lambda)Z^3$ - dont la forme de Weierstrass est $Y^2Z - X^3 - \left(\frac{-g_2(\Lambda)}{4}\right)XZ^2 - \left(\frac{-g_3(\Lambda)}{4}\right)Z^3$ - sont isomorphes. On en déduit l'existence de $\mu \in \mathbf{C}^\star$ tel que $a = -\mu^4\frac{g_2(\Lambda)}{4}$ et $b = -\mu^6\frac{g_3(\Lambda)}{4}$ $(\star)$.

Vue la proposition 4.2, n'importe quel réseau homothétique à Λ donne une courbe elliptique isomorphe à E. On se demande si parmi tous ces réseaux, l'un d'eux donne exactement E ; c'est à dire s'il existe $\alpha \in \mathbf{C}^\star$ tel que $E_{\alpha\Lambda}$ a pour forme de Weierstrass celle de E. On constate que $\Gamma = \frac{1}{\mu}\Lambda$ convient.

En effet, $E_{\frac{\Lambda}{\mu}} = Y^2Z - 4X^3 + \mu^4 g_2(\Lambda)XZ^2 + \mu^6 g_3(\Lambda)Z^3$ dont la forme de Weierstrass est $Y^2Z - X^3 + \mu^4\frac{g_2(\Lambda)}{4}XZ^2 + \mu^6\frac{g_3(\Lambda)}{4}Z^3 = Y^2Z - X^3 - aXZ^2 - bZ^3$ par $(\star)$.

Conclusion

On a montré ici que tout quotient de $\mathbf{C}$ par un réseau (c'est-à-dire, tout tore complexe) est en bijection biholomorphe avec les $\mathbf{C}$-points d'une courbe elliptique et que réciproquement, toute courbe elliptique sur $\mathbf{C}$ découle d'un quotient de $\mathbf{C}$ par un réseau. D'où l'affirmation suivante (dont le sens précis est éclairé ci-dessus) : une courbe elliptique est un tore complexe et vice versa. Ce résultat permet, comme avancé en introduction et illustré dans la sous-partie 3.3, de traduire les résultats d'un des domaines dans l'autre. Cependant, les liens entre eux peuvent encore être explicités. Par exemple, est-il possible de trouver le réseau sous-jacent à une courbe elliptique donnée ? D'en calculer une base ? Avec quelle efficacité ? Des réponses à ces questions pourraient encore faciliter l'établissement d'un "dictionnaire" entre courbes elliptiques et tores complexes.

Références

[1] Michèle Audin, *Un cours sur les fonctions spéciales* [en ligne ici], 2012

[2] Niels Duif, *Transforming a general cubic elliptic curve equation to Weierstrass form, A Sage implementation* [en ligne ici], 2011

[3] D. Husemöller, *Elliptic curves (2^{nd} edition)*, volume 111 of *Graduate Texts in Mathematics*, Springer-Verlag, 2004

[4] Anthony W. Knapp, *Elliptic curves*, Mathematical notes 40, Princeton University Press, 1992

[5] Jan Nekovár, *Elliptic functions and elliptic curves* [en ligne ici],2004

[6] Sacha Schweiser, *The j-invariant* [en linge ici], 2006

[7] Jean-Pierre Serre, *Cours d'arithmétique*, Presses Universitaires de France, 1970

[8] Lawrence C. Washington, *Elliptic curves : number theory and cryptograhpy (2^{nd} edition)*, Chapman & Hall/CRC, 2008

[9] Notes de cours du MIT numéros 14, 15 et 16, [en ligne ici]