Extensions abéliennes de corps quadratiques imaginaires

Piotr P. Karwasz, Yashonidhi Pandey

30 décembre 2003

Table des matières

1 Introduction **2**

2 Remarques sur le plan projectif $\mathbb{P}^2(K)$ **2**

3 Courbes elliptiques **3**

4 $E(\mathbb{C})$ **5**

5 Les Fonctions Elliptiques **9**

6 Applications Analytiques et Algébriques **14**

7 Uniformisation **17**

8 Points Algébriques sur une Courbe Cubique **19**

9 Représentation Galoisienne **21**

10 Multiplication Complexe **21**

11 Le module de Tate **22**

12 Extension abélienne de $\mathbb{Q}(i)$ **23**

1 Introduction

Le but de cet exposé est de construire des extensions galoisiennes abéliennes de corps quadratiques imaginaires $\mathbb{Q}(\sqrt{-d})$.

Kronecker espérait construire une fonction f holomorphe telle que toute extension K galoisienne abélienne de F soit contenue dans le corps $F(f(a_1), f(a_2), \ldots, f(a_n))$ qui soit bien une extension galoisienne abélienne elle-même et les valeurs $a_1, \ldots, a_n$ soient connues. De plus, il espérait que pour tout $\sigma \in Gal(F(f(a_1), f(a_2), \ldots, f(a_n)))$, on pourrait décrire $\sigma(f(a_i))$ d'une manière explicite comme les valeurs de la fonction f pris aux points de $\mathbb{C}$ déterminé par σ et K.

Le Jugendtraum de Kronecker est vrai pour $\mathbb{Q}$. On prend $f(z) = e^{2i\pi z}$ et les $a_k = k/n$ où n est un entier tel que K soit contenu dans $\mathbb{Q}(\zeta_n)$ engendré par une racine n-ème primitive de l'unité. Tel corps, qui est une extension galoisienne abélienne, existe grâce au théorème de Kronecker-Weber.

Dans cet exposé on étudie le cas de $F = \mathbb{Q}(i)$, en considérant la courbe elliptique $y^2 = 4x^3 - 4x$. Nous construisons des extensions galoisiennes abéliennes de $\mathbb{Q}(i)$ engendrées par les coordonnées de points de n-torsion sur $y^2 = 4x^3 - 4x$. Elles ont la forme $\mathbb{Q}(i)(\wp_\Gamma(\frac{k_1\omega_1+k_2\omega_2}{n}), \wp'_\Gamma(\frac{k_1\omega_1+k_2\omega_2}{n}))$ où Γ est un réseau associé à $y^2 = 4x^3 - 4x$, ω_1, ω_2 sont ses périodes et $\wp_\Gamma$ est la fonction de Weierstrass associé à Γ. Ils contiennent toutes telles extensions de $\mathbb{Q}(i)$ mais nous ne le démontrons pas.

Nous expliquons au passage que toute courbe elliptique et $\mathbb{C}/\Gamma$ admet un structure de surface de Riemann pour Γ un réseau de $\mathbb{C}$. Pour expliquer pourquoi on s'attend que le Jugendtraum de Kronecker est vrai, c'est à dire l'existence de fonction f holomorphe et l'existence de points connus, nous démontrons en utilisant la théorie de Weierstrass que toute courbe elliptique est isomorphe à $\mathbb{C}/\Gamma$ pour Γ un réseau de $\mathbb{C}$, unique à homothétie près, comme un groupe et que l'isomorphisme et son inverse sont analytiques.

Il est remarquable que les fonctions transcendantes $\wp_\Gamma$ et $\wp'_\Gamma$ pris aux points de $\mathbb{Q}(i)$ nous donne des nombres algébriques.

2 Remarques sur le plan projectif $\mathbb{P}^2(K)$

Définition 2.0.1 Soient K un corps et $X = K^3\backslash\{0\}$. On introduit sur X la relation d'équivalence :

$$x, y \in X, \quad x \sim y \Leftrightarrow \exists \lambda \in K^\star : \ y = \lambda x.$$

Le plan projectif, noté $\mathbb{P}^2(K)$, est le quotient de X par cette relation d'équivalence.

On note π l'application canonique de X dans $\mathbb{P}^2(K)$. Les points P de $\mathbb{P}^2(K)$ se représentent par $[X : Y : Z]$ où X, Y et Z sont les coordonnées d'un point de $\pi^{-1}(P)$ dans X. Évidemment cette représentation n'est pas unique : chaque point peut être représenté par plusieurs triplets qui diffèrent seulement par la multiplication de $\lambda \in K^\star$.

On a une bijection $\phi : \{[X, Y, Z] \in \mathbb{P}^2(K) | Z \neq 0\} \to K^2$

$$\phi([X : Y : Z]) = (X/Z, Y/Z).$$

Soit $P \in K[x, y]$. L'ensemble de ses zéros s'injecte à l'aide de ϕ^{-1} dans $\mathbb{P}^2(K)$.
Au polynôme P de degré n, on peut associer un polynôme P_h de $K[X, Y, Z]$, unique à multiplication scalaire près, avec les propriétés suivantes :

1. $P_h(tx) = t^n P_h(x)$.
2. P_h est un polynôme homogène. Si x est un zéro de P_h, alors tx l'est aussi et si $P_h(x) \neq 0$, $P_h(tx) = t^n P_h(x) \neq 0$ où n est le degré de P_h et $t \neq 0$. Donc on peut diviser par $\sim$ la relation $x \sim_1 y \Leftrightarrow P_h(x) = 0$ *et* $P_h(y) = 0$ *ou* $P_h(x) \neq 0$ *et* $P_h(y) \neq 0$ et définir les zéros de P_h sur $\mathbb{P}^2(K)$.
3. $\{z \in \mathbb{P}^2(K) \,|\, P_h(z) = 0\} \cap im(\phi) = \phi(\{z \in K^2 \,|\, P(z) = 0\})$

On trouve P_h de la manière suivante : si n est le degré de P et $P(x, y) = \sum_{i+j\leq n} a_{ij} x^i y^j$ alors on définira P_h comme $P_h(X, Y, Z) = \sum_{i+j\leq n} a_{ij} X^i Y^j Z^{n-i-j}$. On trouve aussi l'inverse de cette transformation qui associe à chaque polynôme homogène P_h un polynôme inhomogène P avec la même relation sur les zéros. En effet si le degré de $P_h = n$ et $P_h(X, Y, Z) = \sum_{i+j+k=n} a_{ij} X^i Y^j Z^k$

alors $P(x,y) = \sum_{i+j\leq n} a_{ij}x^i y^j$ nous convient. Dans la partie suivante on passera souvent d'un polynôme P sur K^2 à son correspondant homogène P_h sur $\mathbb{P}^2(K)$. Ce procédé s'appelle homogénéisation et déshomogénéisation et peut se faire selon une variable différent de Z.

3 Courbes elliptiques

Soit $P(x,y)$ un polynôme du troisième degré en deux variables sur le corps K. On étend P à $\mathbb{P}^2(K)$ comme dans la section précédente.

Le lieu des zéros de la fonction associée à P_h s'appelle **courbe cubique** sur K.

Si la courbe cubique a au moins deux points, on peut l'intersecter avec une droite projective passant par deux points. Après une manipulation algébrique on voit que les points appartenant à l'intersection s'écrivent comme les zéros d'un polynôme homogène du troisième degré. Puisque les coordonnées des deux points satisfont ce polynôme il y a un autre point dans $\mathbb{P}^2(K)$ qui la vérifie. Ce point n'est pas nécessairement distinct des deux autres.

Définition 3.0.2 Pour un point $[X : Y : Z]$ dans une courbe cubique définie par P_h on déhomogenise le polynôme P_h pour obtenir P par rapport à une des trois variable X, Y, Z qui est non-nulle sur le point. Ce point est dit lisse ou non-singulier si le gradient de la fonction induite par P est non nul. Dans le cas où plusieurs variables sont non-nulles, le choix de variable n'est pas important. Une **Courbe Elliptique** (C, P) est une courbe cubique C lisse à tous les points munie d'un point marqué P. Souvent on écrit juste C pour la courbe elliptique. Une **Forme de Weierstrass** d'une courbe elliptique est une équation telle que le point à l'infini est $(0 : 1 : 0)$ et d'inflexion.

On admet que pour un point P lisse on peut définir la tangente à la courbe en P et voir qu'il y a aussi un troisième point d'intersection entre la courbe et la tangente.

Si la courbe n'est pas vide et contient un point P lisse, on peut la transformer en une cubique de cette forme :

$$f(X,\, Y,\, Z) = ZY^2 - 4X^3 - aXZ^2 - bZ^3$$

à l'aide de la proposition suivante.

Proposition 3.0.1 (Forme de Weierstrass) *Chaque cubique non vide sur un corps K de caractéristique $\neq 2, 3$ et contenant un point lisse $\mathcal{O}$ se peut mettre sous la forme :*

$$y^2 = 4x^3 - g_2 x - g_3$$

en utilisant des changements de variables rationnels, c.à.d. des changements où les nouvelles variables sont fonctions rationnelles des anciennes à coefficient dans K.

Démonstration : On a deux cas selon que $\mathcal{O}$ soit un point d'inflexion ou pas.

1. $\mathcal{O}$ n'est pas un point d'inflexion. Choisissons $Z = 0$ tangent à la courbe en $\mathcal{O}$, $X = 0$ tangent au troisième point d'intersection entre la courbe et $Z = 0$ et $Y = 0$ passant par $\mathcal{O}$.
2. $\mathcal{O}$ est un point d'inflexion. On prend $Y = 0$ et $Z = 0$ comme dans le cas précédent et pour $X = 0$ n'importe quelle droite qui ne passe pas par $\mathcal{O}$.

En homogénéisant le résultat on obtient :

$$xy^2 + (ax + b)y = cx^3 + dx^2 + ex.$$

Il suffit de multiplier par x, changer de coordonnées avec $y' = xy$ et on obtient :

$$y^2 + (ax + b)y = \text{“polynôme de degré 3 en x, dans K[x]”}$$

Le changement de variables $y' = y - \frac{1}{2}(ax + b)$ enlève le terme linéaire en y. Or il suffit d'éliminer le terme quadratique en x avec la substitution $x' = x - \frac{1}{3}a_2$ où a_2 est le coefficient du terme quadratique.

On est donc arrivé à :

$$y^2 = cx^3 + dx + e$$

Enfin $x' = 4cx$ et $y' = 4c^2y$ donnent la forme voulue.

□

Fonction rationnelles sur la courbe elliptique :

Une fonction rationnelle sur la courbe elliptique C de polynôme P est un élément du corps de fractions de l'anneau suivant :

$$K[C] = \frac{K[X,Y]}{(P)}.$$

La condition qu'on a donnée sur les racines garantit que P est irréductible, donc $K[C]$ est intègre. L'ensemble des fonctions elliptiques se note $K(C)$.

On définit une structure de groupe canonique d'élément neutre $\mathcal{O} = [0:1:0]$ pour une courbe elliptique considérée sous sa forme de Weierstrass.

Loi de groupe :

La courbe intersecte trois fois la droite à l'infini $(X, Y, 0)$ dans le point $[0:1:0]$ qu'on appellera souvent $\mathcal{O}$. En coordonnés homogènes la courbe s'écrit :

$$ZY^2 = X^3 + aZ^2X + Z^3$$

dont le résultat en intersectant la courbe avec $Z = 0$.

Définissons la structure de groupe sur $C(K)$. Soient P, Q deux points de la courbe. La courbe intersecte exactement trois fois la droite projective passant par P et Q. On note $P * Q$ le troisième point d'intersection, qui appartient à $C(K)$ (voir début de section). Un calcul direct nous montre que le point cherché a comme coordonnées des fonctions rationnelles des coordonnées de P et Q qui ne dépendent pas du choix de P et Q, elles seront données par la suite.

On définit $P + Q$ par $(P * Q) * \mathcal{O}$. On vérifie que cette définition met une structure de groupe abélien sur $C(K)$:

1. $\mathcal{O}$ est l'élément neutre et la loi est commutative par définition.
2. Pour l'associativité on admettra le lemme suivant :

Lemme 3.0.1 *Soient C_1, C_2, C trois courbes cubiques. Si C passe par huit points d'intersection de C_1 avec C_2, alors elle passe aussi par le neuvième.*

Si P, Q, R $\in C(K)$, pour démontrer l'égalité $(P + Q) + R = P + (Q + R)$ on peut démontrer un passage en arrière, cela veut dire que $(P + Q) * R = P * (Q + R)$.

On a deux cubiques dégénérées $C1$ et $C2$: les droites $(P+Q, R)$ et $(P, Q+R)$ dans la figure qui s'intersectent dans un point A. Les points $\mathcal{O}$, P, Q, R, $P*Q$, $P+Q$, $Q*R$, $Q+R$, A appartiennent à deux cubiques dégénérées, donc d'après le lemme A est dans $C(K)$ et il est égal à $(P + Q) * R$ et à $P * (Q + R)$.

Dans la figure 1 on a montré $\mathcal{O}$ dans un coin. Avec la courbe donnée par un polynôme dans la forme de Weierstrass, le point $\mathcal{O}$ est sur la courbe à l'infini. Dans tel cas on peut expliquer l'addition de deux points de la manière suivante : on trace la droite par P et Q et on prend le symétrique selon l'axe 'x' du troisième point d'intersection de la droite avec la courbe.

Soit C une courbe elliptique sur K de $\text{char}(K) \neq 2, 3$ donnée par l'équation de Weierstrass.

$$C : y^2 = 4x^3 - g_2x - g_3 \text{ avec } g_2, g_3 \in K$$

On va donner des formules explicites pour la somme :

1. Si $P = (x, y) \in C$, alors $-P = (x, -y)$
2. Si $P_1 + P_2 = P_3$ et $P_i = (x_i, y_i)$ on a les cas suivants :

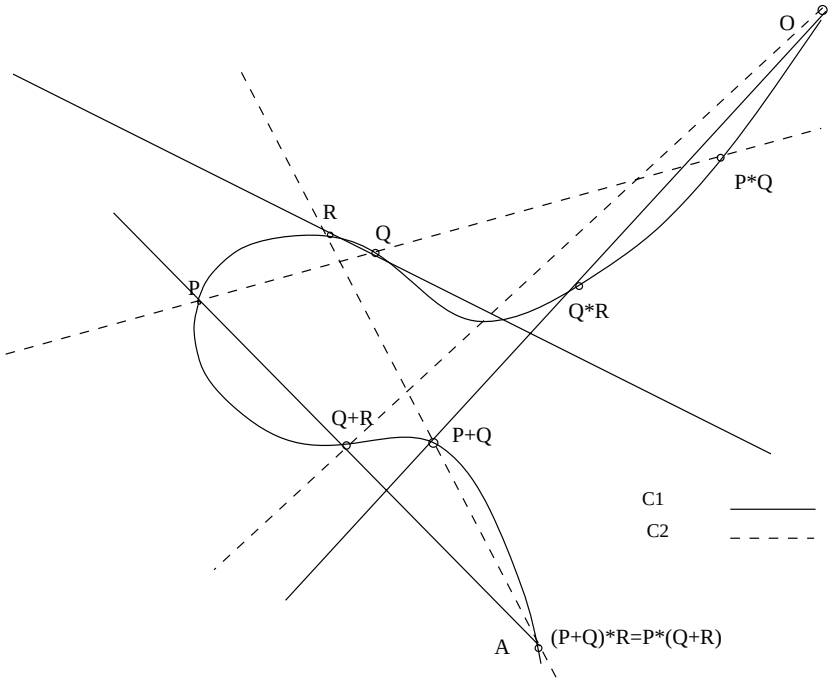

FIG. 1 – Associativité de la loi du groupe.

(a) Si $x_1 = x_2$ et $y_1 = -y_2$, alors :

$$P_1 + P_2 = \mathcal{O}$$

(b) Si $x_1 \neq x_2$ on calcule :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

et $P_3 = P_1 + P_2$ est donné par

$$x_3 = \frac{1}{4}\lambda^2 - x_1 - x_2$$

$$y_3 = -\frac{1}{4}\lambda x_3 - \nu.$$

4 $E(\mathbb{C})$

Le but de ce paragraphe est de démontrer que toute courbe elliptique exprimée comme ci-dessus est isomorphe à $\mathbb{C}$ quotienté par un réseau comme surface de Riemann et réciproquement. On expliquera la terminologie de la phrase précédente.

Définition 4.0.3 On appelle une **surface de Riemann** une variété complexe X de dimension 1. Plus précisément, une surface de Riemann est un espace topologique de Haussdorf et à base dénombrable tel que pour chaque point P dans X il existe V, un voisinage de P et $\phi_V : V \to \mathbb{C}$ un homéomorphisme sur son image tel que si V et V' sont deux ouverts dans X à intersection non vide, alors $\phi_V \circ \phi_{V'}^{-1} : \phi_{V'}(V' \cap V) \to \phi_V(V' \cap V)$ est biholomorphe. L'homéomorphisme ϕ_V de V dans l'ouvert de $\mathbb{C}$ s'appelle une carte.

Définition 4.0.4 Soient A et B deux surfaces de Riemann, une application $f : A \to B$ est **analytique** si pour tout $x \in A$ il existe des voisinages U de x et V de $f(x)$ tel que $f(U) \subset V$ et des cartes $\phi : U \to U' \subset \mathbb{C}$ et $\psi : V \to V' \subset \mathbb{C}$ tels que $\psi \circ f \circ \phi^{-1}$ soit holomorphe.

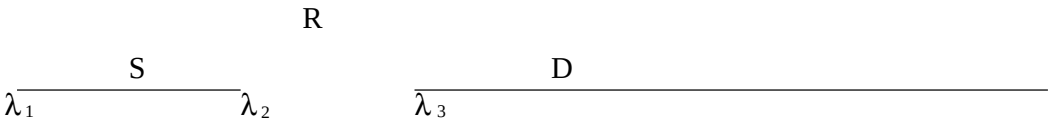

FIG. 2 – Région R.

Définition 4.0.5 On appelle **réseau** de $\mathbb{C}$ un sous groupe discret Γ du groupe additif des nombres complexes, engendré par ω_1 et $\omega_2 \in \mathbb{C}$ tels que ω_1 et ω_2 soient $\mathbb{R}$-linéairement indépendants.

Définition 4.0.6 Le quotient $\mathbb{C}/\Gamma$ est l'espace topologique obtenu en passant au quotient l'action de Γ sur $\mathbb{C}$. En autres termes $\mathbb{C}/\Gamma$ est l'espace obtenu de $\mathbb{C}$ à l'aide de la relation $x \sim y$ si $x - y \in \Gamma$. Cela donne une application canonique $\phi : \mathbb{C} \to \mathbb{C}/\Gamma$. Les ouverts de $\mathbb{C}/\Gamma$ sont les sous-ensembles U tels que $\phi^{-1}(U)$ est un ouvert de $\mathbb{C}$.

Proposition 4.0.2 $\mathbb{C}/\Gamma$ *admet une structure de surface de Riemann telle que la projection* $\pi : \mathbb{C} \to \mathbb{C}/\Gamma$ *soit analytique.*

Démonstration: Puisque Γ est discret, on peut prendre r assez petit de façon à ce que $B(z,r) \cap B(z + a\omega_1 + b\omega_2, r)$ soit vide pour chaque $a, b \in \mathbb{Z}$. Choisissons $P \in \mathbb{C}/\Gamma$ et z tel que $\pi(z) = P$. $\pi(B(z,r)$ nous donne une carte autour P. La compatibilité entre deux cartes φ et ψ est facile à voir, parce que $\varphi \circ \psi^{-1}(z) = z + m\omega_1 + n\omega_2$ pour des $m, n \in \mathbb{Z}$. Donc, les applications "Changements de Cartes" sont des translations donc holomorphe.

□

Les $\mathbb{C}/\Gamma$ sont topologiquement des tores $S^1 \times S^1$. Un homomorphisme peut être donné par :

$$\begin{aligned} f : \mathbb{C}/\Gamma &\to \mathbb{T}^1 \\ \omega_1 x + \omega_2 y &\mapsto (\exp(2\pi i x), \exp(2\pi i y)) \end{aligned}$$

Définition 4.0.7 Un groupe de Lie G est une variété différentielle munie d'une structure de groupe, telle que l'opération de groupe $G \star G \to G$ et le passage à l'inverse (du groupe) soient analytiques.

Définition 4.0.8 Une isogénie entre deux courbes elliptiques est une application non constante qui s'exprime comme fonction rationnelle des coordonnées.

On voit facilement que $\mathbb{C}/\Gamma$ est un groupe de Lie. Il faut juste vérifier les conditions sur l'opération de groupe, qui est une translation dans $\mathbb{C}$.

Après avoir montré qu'une courbe elliptique est elle-même une surface de Riemann, avec la topologie induite de $\mathbb{P}^2(\mathbb{C})$ où elle est contenue, on vérifie facilement que la structure de groupe définie dans la section précédente est en effet un groupe de Lie.

L'introduction de ces définitions est due au fait que les courbes elliptiques sont des surfaces de Riemann et elles sont analytiquement isomorphes à des tores.

Pour une courbe elliptique, on a que $f(x) = x^3 + ax^2 + bx + c$ a des racines $\lambda_1, \lambda_2, \lambda_3$ distinctes dans $\mathbb{C}$. Pour simplifier les arguments on peut supposer que les racines sont sur une droite dans $\mathbb{C}$. Le situation générale est très similaire.

Considérons $\Psi : E(\mathbb{C}) \to \mathbb{C}$, $(x, y) \mapsto x$ cette application est continue. On peut définir une branche analytique de $\sqrt{f(x)}$ sur $\mathbb{C}$ privé du segment S qui joignent λ_1 à λ_2 et d'une demi-droite D passant par λ_3 et allant vers ∞ dans la direction contraire à λ_1. Cette région noté R est illustrée dans Fig. 2.

On a deux fonctions $f_+,\ f_- : R \to E(\mathbb{C})$ $x \mapsto (x, \sqrt{f(x)})$ qui correspondent aux deux choix de $\sqrt{f(x)}$ sur R. Elles sont inverses de Ψ sur R et correspondent aux différents choix de la fonction "argument" comme montré dans Fig 4.

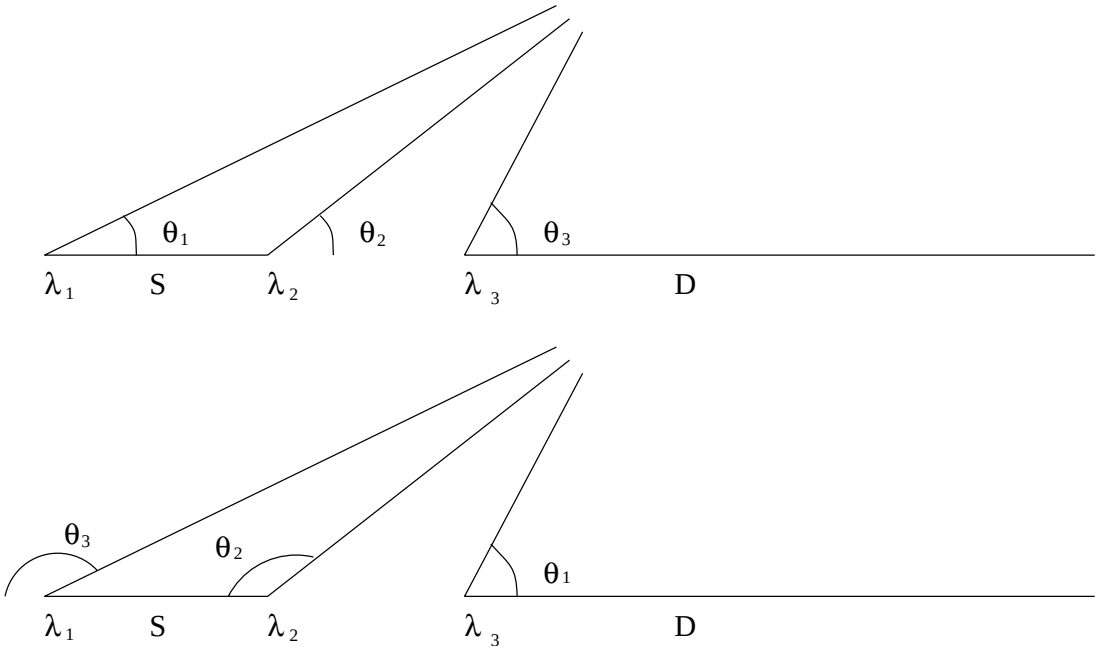

FIG. 3 – Deux différent choix d'argument

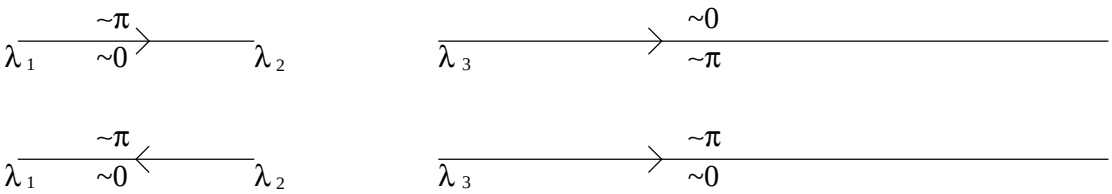

FIG. 4 – Approximations des arguments

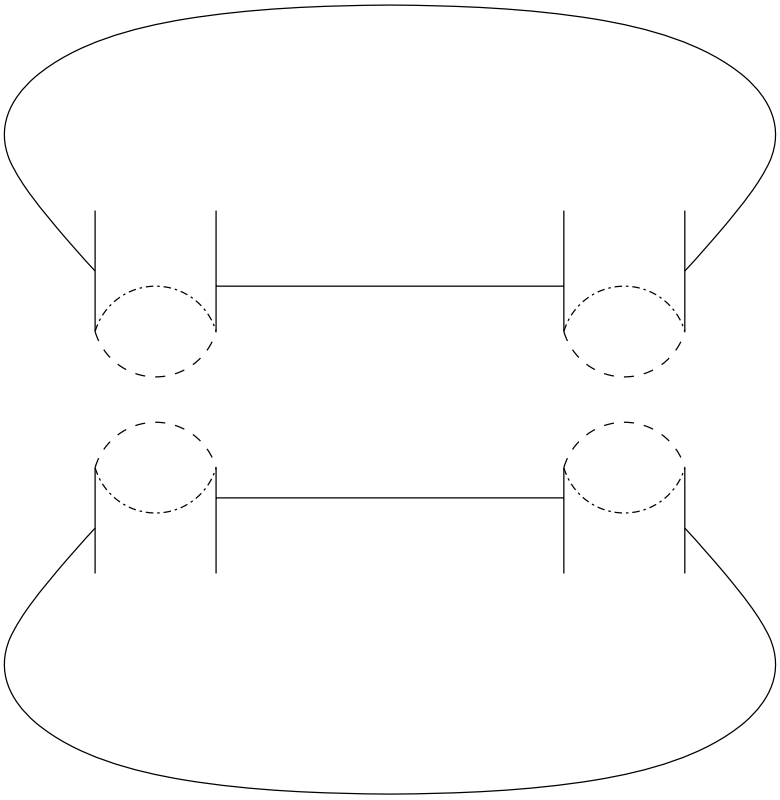

FIG. 5 – Les images de f_+ et f_-

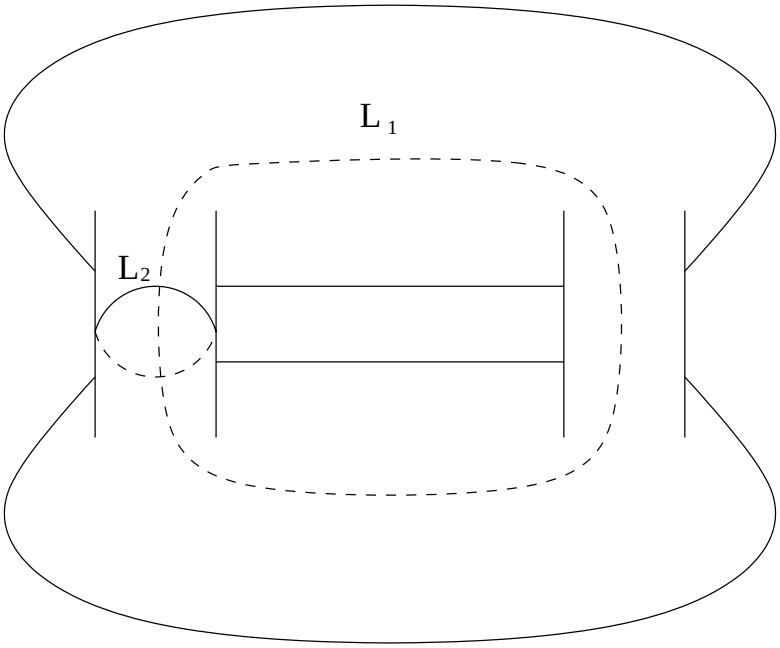

FIG. 6 – Les lacets générateurs du π_1

f_+ et f_- sont holomorphes comme fonction de $\mathbb{C}$ dans $\mathbb{C}$ de dérivée partout non-nulle car $f(x)$ est non-nulle dans R. Notons X_+ (resp X_-) les images de R par f_+ et f_-. Alors X_+, X_- sont des ouverts difféomorphes à R dans $E(\mathbb{C})$. Voir Fig 5.

Pour x près du segment S ou de la D demi-droite, les approximations des arguments de $f_+(x)$ et $f_-(x)$ sont illustrées dans la Fig 4.

On étend f_+, noté $\tilde{f_+}$ sur S (resp. D) en prenant l'argument pour les racines carrées de ces points comme π (resp. 0). De même, on étend f_- sur S resp. (D) en prenant comme l'argument 0 (resp.. π). Les images de f_+ et f_- sont notés dans Fig 5. Sauf λ_1, λ_2, λ_3 et ∞ tous les points ont deux préimages par Ψ. Si on colle les deux figures comme montré dans Fig 5 on voit que $\tilde{f_+}$ et $\tilde{f_-}$:

1. envoient $\mathbb{C}$ dans $E(\mathbb{C})$
2. elles sont égaux dans 4 points mentionnés au-dessus
3. les applications f_+ et f_- sont des homéomorphismes entre

$$\mathbb{C}\backslash\{x \notin S \bigcup D\} et \{z \in E(\mathbb{C}) | \Psi(z) \notin S \bigcup D\}$$

   et Ψ est la leur inverse.
4. si on choisit l'image d'un point $x \in E(\mathbb{C})$ tel que $\Psi(x) \notin S \bigcup D$ en envoyant x par $f_+ \circ \Psi$ on peut prolonger cette application de manière continue partout sur la courbe.

Ceci montre que $E(\mathbb{C})$ est homéomorphe à la réunion que l'on voit facilement est un tore. Un tore est homéomorphe à $\mathbb{C}$ quotienté par un réseau.

Pour définir une structure de surface de Riemann sur $E(\mathbb{C})$ on peut prendre f_+^{-1} et f_-^{-1} comme cartes et faire une autre branche analytique, qui, cette fois joint λ_1 à l'infini et λ_2 à λ_3 et on obtient g_+ et g_-. Les g_+^{-1} et g_-^{-1}, définis dans une façon similaire seront le deuxième couple de cartes. Elles sont compatibles, avec f_+^{-1} et f_-^{-1}, car l'intersection des domaines des deux cartes, une "de type f" et une "de type g", est envoyé dans un demi plan complexe H, obtenu en coupant $\mathbb{C}$ selon la droite passant par $\lambda_1, \lambda_2, \lambda_3$. Les fonctions $f_\pm$ et $g_\pm$ sont par définition les racines carrées de f. Sur le demi plan complexe H il existe un point pour lequel leur valeur coïncide, donc elles sont identiques, étant H simplement connexe.

Soient (x, y) les coordonnées des points sur la courbe. On admettra que dx/y est non nulle sur toute la courbe, alors en particulier dans le quatre points λ et ∞ on peut aussi localement définir une carte.

5 Les Fonctions Elliptiques

Définition 5.0.9 Une fonction méromorphe f sur $\mathbb{C}$ s'appelle fonction elliptique si, étant donné un réseau Γ la fonction vérifie :

$$f(z) = f(z + \omega) \quad \forall \omega \in \Gamma.$$

Pour $a \in \mathbb{C}$, on appelle parallélogramme fondamental l'ensemble $D = \{a + \omega_1 t_1 + \omega_2 t_2 \quad 0 \leq t_1, t_2 < 1\}$.

L'ensemble des fonctions elliptiques noté $\mathbb{C}(\Gamma)$ forme un corps.

Proposition 5.0.3 *Une fonction elliptique holomorphe est constante.*

Démonstration : La propriété de périodicité nous donne que la fonction est bornée sur $\mathbb{C}$ car elle est bornée sur la fermeture d'un parallélogramme fondamental, qui est compacte. Par le théorème de Liouville la fonction est constante. □

Proposition 5.0.4 *Si $f \in \mathbb{C}(\Gamma)$:*

1.

$$\sum_{\omega \in \mathbb{C}/\Gamma} res_w(f) = 0$$

2.

$$\sum_{\omega\in\mathbb{C}/\Gamma} ord_w(f) = 0$$

3.

$$\sum_{\omega\in\mathbb{C}/\Gamma} ord_w(f)w = 0 \ dans\ \mathbb{C}/\Gamma$$

Démonstration :

Si f est elliptique, alors f' l'est aussi. Pour les deux premiers points de la proposition, on intègre f et $\frac{f'}{f}$ sur le bord d'un parallélogramme qui ne contient pas de pôle de la fonction (qui car les pôles sont discrets, donc en nombre fini sur un compact) et on applique le théorème des résidus.

Pour le troisième point on intègre la fonction $\frac{zf'(z)}{f(z)}$. On obtient :

$$\begin{aligned}\sum_{\omega\in\mathbb{C}/\Gamma} ord_w(f) &= \frac{1}{2\pi i}\int_{\partial D}\frac{zf'(z)}{f(z)}d\ z \\ &= \frac{1}{2\pi i}(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a})\frac{zf'(z)}{f(z)}d\ z\end{aligned}$$

Avec le changement de variable $z \leftarrow z-\omega_1$ (resp. $z \leftarrow z-\omega_2$) dans la deuxième (resp. troisième) intégrale on trouve :

$$\sum_{\omega\in\mathbb{C}/\Gamma} ord_w(f)w = -\frac{\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}dz + \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2}\frac{f'(z)}{f(z)}dz$$

$\frac{1}{2\pi i}\int_a^b \frac{f'(z)}{f(z)}dz$ est le nombre de lacet autour de 0 du chemin :

$$[0,1] \to \mathbb{C}, \quad t \mapsto f((1-t)a+tb))$$

et donc comme $f(a) = f(b)$ alors le chemin est fermé et l'intégral et un entier. On conclure que la somme appartient à Γ.

□

Définition 5.0.10 On appelle **degré** de la fonction elliptique le nombre de ses pôles ou zéros comptés avec multiplicité.

Définition 5.0.11 Le groupe des **diviseur** d'une surface de Riemann est le groupe abélien libre engendré par les points de la surface. On le note : $\sum_g n_i(g)$ où g est un point de la surface.

Définition 5.0.12 On appelle **diviseur** de $f \in \mathbb{C}(\Gamma)$ le nombre $div(f) = \sum ord_w(f)(w)$.

Définition 5.0.13 Soit Γ un réseau dans $\mathbb{C}$. La fonction $\wp$ associée à Γ est la fonction définie par :

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Gamma,\,\omega\neq 0}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}).$$

On appelle fonctions de Eisenstein les fonctions suivantes :

$$G_{2k} = \sum_{\omega\in\Gamma,\,\omega\neq 0}\frac{1}{\omega^{2k}}$$

avec $k \in \mathbb{N}$.

On rappelle des résultats connus sur la fonction $\wp$ de Weierstrass.

Proposition 5.0.5 *1. La fonction $\wp$ converge uniformément sur chaque compact de $\mathbb{C}$ Gamma. Elle est paire et elliptique.*

2. Les fonction G_{2k} convergent uniformément sur chaque compact de $\mathbb{C}$, pour tout $k > 1$

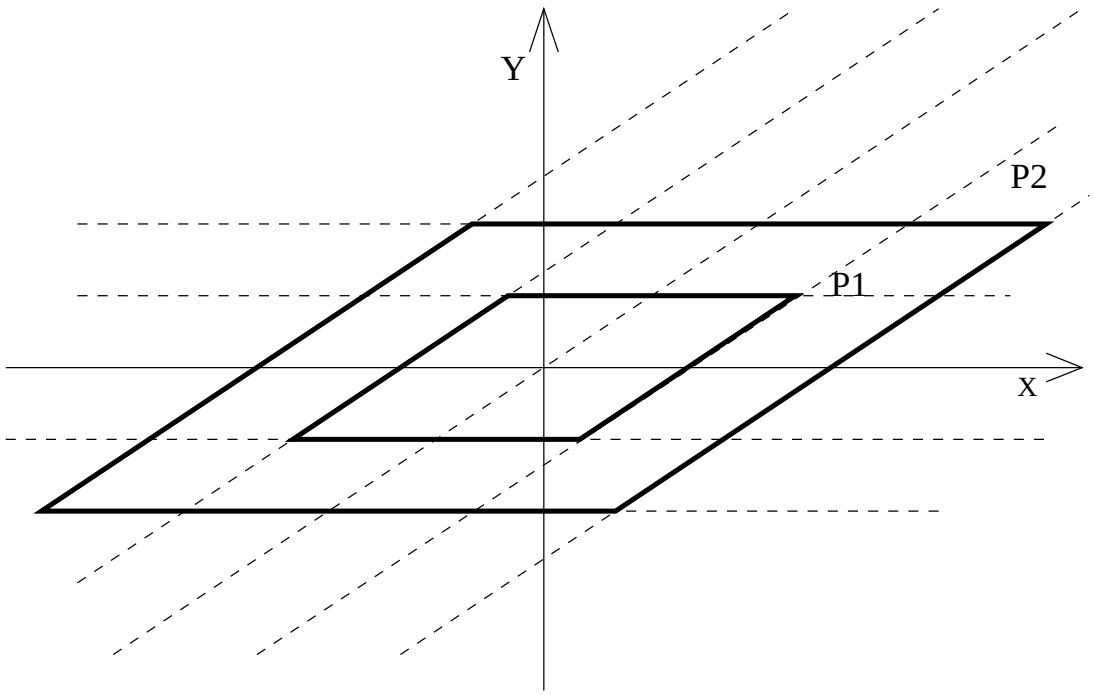

FIG. 7 – Convergence de la série de Eisenstein.

Démonstration :

Commençons par le point 2. On divise Γ en des parallélogrammes concentriques P_n centrés en zéros comme en Figure 7. Sur chaque parallélogramme il y a $8n$ points et la distance de chaque point à l'origine est $\geq cn$ pour un certain $c \in \mathbb{R}$. On estime donc la fonction de Eisenstein.

$$\sum_{\omega\in\Gamma,\,\omega\neq 0} \frac{1}{|\omega|^{2k}} = \sum_{n\geq 1}\sum_{\omega\in P_n} \frac{1}{|\omega|^{2k}} \leq \sum_{n\geq 1} \frac{8n}{|cn|^{2k}} \leq \sum_{n\geq 1} \frac{8n}{cn^3}$$

et cette dernière série converge.

Pour démontrer le point 1 on se sert de ce résultat suivant. On voit que pour $|\omega| > 2|z|$:

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{10|z|}{|\omega^3|}.$$

Donc pour chaque compact de $\mathbb{C}/\Gamma$ on casse la somme qui nous donne $\wp$ en une somme finie et une somme absolument convergente, dans cette dernière on met les ω tq $|\omega| > 2\sup_{z\in K}|z|$.

Donc en dehors de Γ, $\wp$ converge sur chaque compact. Elle est paire : il suffit de changer $z \leftarrow -z$ $\omega \leftarrow -\omega$ dans la somme. On a :

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

Évidemment $\wp'$ est périodique. La fonction

$$c(z) := \wp(z+\omega_1) - \wp(z)$$

est méromorphe partout, elle est holomorphe hors de Γ. Comme au-dessus on voit que son dérivée converge uniformément sur chaque compact ne rencontrant pas Γ, alors on peut interchanger l'ordre de la sommation et on voit que son dérivé est nulle. Donc la fonction est constante hors de Γ et donc partout.

Si on prend $z = \frac{\omega}{2}$ on trouve $c(\omega) = 0$.

□

On voit que $\wp$ est d'ordre 2, car elle a des pôles uniquement sur Γ et d'ordre 2. $\wp'$ a les pôles aussi sur Γ, mais son expression de somme nous montre qu'elle est de degré 3.

Proposition 5.0.6 *Soit Γ un réseau, on a :*

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

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

Démonstration : Pour démontrer le point 1 écrivons :

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}[(1-\frac{z}{\omega})^{-2} - 1] = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}$$

Pour la convergence absolue de $\wp$ en dehors Γ on peut substituer la formule ci-dessus dans la définition de $\wp$ et changer l'ordre de la somme obtenue. On a démontré 1.

Pour 2 on calcule les développements de Laurent des fonctions $\wp$ et $\wp'$ à l'aide de la formule ci-dessus et on a :

$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \dots$$
$$\wp(z)^3 = z^{-6} - 9G_4z^{-2} + 15G_6 + \dots$$
$$\wp(z) = z^{-2} + 3G_4z^2 + \dots$$

La fonction $g(z) := \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$ est holomorphe autour de 0 et elle tends vers 0 lorsque z tends vers 0. Pour la Proposition 5.0.5 et comme $\wp'$ converge uniformément sur chaque compacte de $\mathbb{C}\backslash\Gamma$, on voit qu'elle est holomorphe en dehors Γ. Par le développement on voit qu'elle est holomorphe en 0 de donc on tout point de Γ, c'est à dire elle est holomorphe partout. Elle tend vers zéro pour z tendant vers 0. Elle est donc nulle par la Proposition 5.0.3

On a donc que les points $P \in \mathbb{C}$ de coordonnées $(\wp'(z),\ \wp(z)) \in C\ \forall z \in \mathbb{C}/\Gamma$, où C est la courbe elliptique, d'équation :

$$y^2 = 4x^3 - 60G_4x - 140G_6.$$

On notera par la suite $g_2 = 60G_4$ et $g_3 = 140G_6$.

Exemple 5.0.1 Prenons $\Gamma = \mathbb{Z}[i]$, alors on peut calculer explicitement g_2 et g_3. En fait :

$$G_6 = \sum_{\omega\neq 0}\frac{1}{\omega^6} = \sum_{\omega\neq 0}\frac{1}{(i\omega)^6} = -\sum_{\omega\neq 0}\frac{1}{\omega^6}$$

Le premier passage est un changement d'ordre dans la somme. On voit donc $G_6 = 0$. Par 6.3 on voit que G_4 n'est pas nulle. Il est réel car la somme qui donne G_4 est invariante pas conjugaison. Posons $\lambda := \sqrt[4]{15G_4}$, le réseau $\Gamma' = \lambda\mathbb{Z}[i]$ donne $y^2 = 4x^3 - 4x$ - forme de Weierstrass de la courbe qui nous intéresse dans cet exposé. On pourrait prouver que λ est un nombre transcendant.

Proposition 5.0.7 *Soit Γ un réseau de $\mathbb{C}$. Soit $\wp_\Gamma(z)$ et $\wp'_\Gamma(z)$ les fonctions de Weierstrass associées à Γ. Toute fonction elliptique dans $\mathbb{C}(\Gamma)$ s'écrit comme fonction rationnelle de $\wp_\Gamma(z)$ et $\wp'_\Gamma(z)$.*

Démonstration: On considère pour commencer le cas d'une fonction f elliptique *paire*. On note $a_1, \dots, a_k$ l'ensemble de ses zéros et $b_1, \dots, b_k$ l'ensemble de ces pôles avec multiplicité. Si quelque $w = a_i$ parmi eux a la propriété que $2w \in \Gamma$ alors $f(z) = f(-z)$ nous donne :

$$f^{(i)}(w) = (-1)^i f^{(i)}(-w) = (-1)^i f^{(i)}(w)$$

donc $f^{(i)}(w) = 0$ pour tout i impair et w est d'ordre pair.

Les autres a_i sont en couples, car si w est un zéro alors $-w$ l'est aussi. On peut donc écrire $a_1, \dots, a_k$ comme $a_1, \dots, a_n, -a_1, \dots, -a_n$. En regardant la fonction $\frac{1}{f}$ on peut écrire de la même façon les pôles, $b_1, \dots, b_n, -b_1, \dots, -b_n$.

Considérons la fonction :

$$\prod_{i=1}^{k} \frac{\wp(z) - \wp(a_i)}{\wp(z) - \wp(b_i)}.$$

Le diviseur de $\wp(z) - \wp(a_i)$ étant égal à $(a_i) + (-a_i) - 2(0)$, le produit a les mêmes pôles et zéros que f. Ainsi leur rapport est holomorphe, donc constant.

Considérons une fonction elliptique quelconque f. Elle peut s'écrire comme :

$$f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}(f(z) - f(-z))$$

Donc elle est somme d'une fonction paire et impaire. En multipliant et divisant la deuxième fonction par $\wp'$ on trouve :

$$f(z) = p_1(z) + p_2(z)\wp'(z)$$

avec p_1 et p_2 paires. On applique le premier cas. □

Définition 5.0.14 Soit Γ un réseau sur $\mathbb{C}$. La fonction σ de Weierstass est la fonction :

$$\sigma(z) = z \prod_{\omega \in \Gamma\, \omega \neq 0} (1 - \frac{z}{\omega}) \exp^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2}$$

Lemme 5.0.2 *1. σ est une fonction holomorphe avec tout ses zéros dans Γ et d'ordre un. En plus on a :*

$$\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z) \quad \forall z \in \mathbb{C}/\Gamma.$$

2. Pour chaque $\omega \in \Gamma$ il existe a et $b \in \mathbb{C}$ tels que

$$\sigma(z + \omega) = \exp^{(az+b)} \sigma(z) \quad \forall z \in \mathbb{C}.$$

Démonstration: La convergence de σ suit des propriétés des produits de Weierstrass et des critères de convergence.

En chaque point $z \notin \Gamma$ on peut faire localement le logarithme de la fonction. On obtient :

$$\log \sigma(z) = \log\, z + \sum [\log(1 - \frac{z}{\omega}) - \frac{z}{\omega} - \frac{1}{2}(\frac{z}{\omega})^2]$$

$$\frac{d}{dz} \log \sigma(z) = \frac{1}{z} + \sum [\frac{-1}{\omega - z} - \frac{1}{\omega} - \frac{z}{(\omega)^2}]$$

La dérivé deuxième est la fonction voulue.

(2) La fonction $\wp$ est elliptique, donc $\wp(z + \omega) = \wp(z)$. Si on intègre deux fois on obtient :

$$\log \sigma(z + \omega) = \log \sigma(z) + az + b$$

est le résultat est démontré. □

On utilisera ce lemme pour le théorème suivant :

Proposition 5.0.8 *Si $n_1 \dots n_r \in \mathbb{Z}$ et $z_1 \dots z_r \in \mathbb{C}$ vérifient :*

$$\sum_i n_i = 0 \quad \sum_i n_i z_i \in \Gamma$$

alors il existe une fonction elliptique f telle que :

$$div(f) = \sum n_i(z_i).$$

Démonstration : Si $\sum_i n_i z_i = \omega$ on change $n_1(z_1) + \cdots + n_r(z_r)$ avec $n_1(z_1) + \cdots + n_r(z_r) + 1(0) - 1(\omega)$. Les propriétés de ce diviseur ne changent pas, mais $\sum n_i z_i = 0$.

On prend la fonction :

$$f(z) = \prod \sigma(z - z_i)^{n_i}.$$

Or pour chaque $\omega \in \Gamma$ on a :

$$\frac{f(z+\omega)}{f(z)} = \prod \exp^{(a(z-z_i)+b)n_i} = \exp^{(az+b)\sum n_i - a\sum n_i z_i} = 1$$

□

On a besoin de la proposition suivante dont la démonstration nous emmènerait trop loin du but de cet exposé. Nous la citerons donc en omettant sa démonstration.

Proposition 5.0.9 *Si E est une courbe elliptique et $D = \sum n_P(P)$ est un diviseur de la courbe, alors D est le diviseur d'une fonction rationnelle f si et seulement si $\sum n_P$ et $\sum n_P P = 0$.*

6 Applications Analytiques et Algébriques

La théorie de Weierstrass nous donne un lien entre les courbes elliptiques et l'étude des $\mathbb{C}/\Gamma$. On renforce le lien entre $\mathbb{C}$ et $\mathbb{C}/\Gamma$ avec :

Définition 6.0.15 Soient A et A' deux espaces topologiques. On dit que (A', π) est un **revêtement** de A, si l'application $\pi : A' \to A$ est continue, et telle que pour chaque point P de A il existe un voisinage V de P tel que $\pi^{-1}(V)$ soit une réunion disjointe d'ouverts $\coprod V_i'$ de A', et $\pi|_{V_i'} : V_i' \to V$ soit un homéomorphisme.

Définition 6.0.16 (A', π) est un **revêtement universel** si de plus A' est simplement connexe et connexe.

On admet la proposition suivante de topologie algébrique.

Proposition 6.0.10 *Soient (A_1', π_1) et (A_2', π_2) deux revêtements universels d'un espace topologique A. Alors, il existe un homéomorphisme $\theta : A_1' \to A_2'$ tel que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} A_1' & \xrightarrow{\theta} & A_2' \\ \pi_1 \downarrow & & \downarrow \pi_2 \\ A & \xrightarrow{id} & A \end{array}$$

Si A admet une structure de surface de Riemann, on peut donner canoniquement une structure de surface de Riemann à A' en utilisant les homéomorphismes entre ouverts de A et ouverts de A'.

Par la suite on admettra un théorème sur les revêtement :

Théorème 6.1 *Soient A et B deux espaces topologiques. Soient (A', π_A) et (B', π_B) leurs revêtements universels, alors chaque $\varphi : A \to B$ continue peut se relever en $\tilde{\varphi} : A' \to B'$ continue. C'est à dire, il existe $\tilde{\varphi}$ continue rendant commutatif le diagramme suivant.*

$$\begin{array}{ccc} A' & \xrightarrow{\tilde{\varphi}} & B' \\ \pi_A \downarrow & & \downarrow \pi_B \\ A & \xrightarrow{\varphi} & B \end{array}$$

Si de plus A et B ont une structure de surface de Riemann et si φ est analytique alors $\tilde{\varphi}$ est analytique pour les structures de surfaces de Riemann naturelles sur A' et B'.

Proposition 6.1.1 *$\pi : \mathbb{C} \to \mathbb{C}/\Gamma$ est le revêtement universel de $\mathbb{C}/\Gamma$.*

Démonstration : Γ est discret. Pour chaque point $P \in \mathbb{C}$, prenons un voisinage V de P tel que V n'intersecte pas $g+V, \quad g \in \Gamma, g \neq 0$. On voit que V est homéomorphe à $\pi(V)$, par la définition de espace topologique quotient.

□

Si Γ_1 et Γ_2 sont deux réseaux sur $\mathbb{C}$ et $\alpha \in C$ tel que $\alpha\Gamma_1 \subset \Gamma_2$ alors

$$\phi_\alpha : \mathbb{C}/\Gamma_1 \to \mathbb{C}/\Gamma_2 \quad \phi_\alpha(z) = \alpha z (mod\, \Gamma_2)$$

sont des morphismes analytiques entre les deux surfaces de Riemann. On a de plus :

Théorème 6.2 *Soient Γ_1, Γ_2 deux réseaux dans $\mathbb{C}$.*

1. $$\begin{array}{ccccc} \{\lambda \in \mathbb{C},\ \lambda\Gamma_1 \subset \Gamma_2\} & \to & \{\phi \in \mathrm{Hom}_{analytiques}(\mathbb{C}/\Gamma_1, \mathbb{C}/\Gamma_2) \text{ avec } \phi(0) = 0\} \\ \alpha & \mapsto & \phi_\alpha \end{array}$$
   est une bijection.
2. *En particulier chaque homomorphisme de ce type est un homomorphisme d'un groupe où la structure de groupe sur $\mathbb{C}/\Gamma_1$ et sur $\mathbb{C}/\Gamma_2$ sont les structures héritées de $\mathbb{C}$.*
3. $\{\varphi \in \mathrm{End}_{analytique}(\mathbb{C}/\Gamma) \mid \varphi(0) = 0\} \leftrightarrow \{\lambda \in \mathbb{C} \mid \lambda\Gamma \subset \Gamma\}$ *est une bijection.*
4. $\mathbb{C}/\Gamma_1 \simeq \mathbb{C}/\Gamma_2$ *ssi* $\exists \lambda \in \mathbb{C}^*$ *tel que* $\lambda\Gamma_1 = \Gamma_2$

Démonstration:

1. Si $\vartheta : \mathbb{C}/\Gamma_1 \to \mathbb{C}/\Gamma_2$ est un homomorphisme analytique avec $\vartheta(0) = 0$ alors par le théorème 6.1 on peut remonter ϑ en un homomorphisme $\tilde{\vartheta} : \mathbb{C} \to \mathbb{C}$ tel que $\tilde{\vartheta}(0) = 0$ (quitte à faire une translation).
   Pour chaque $\omega \in \Gamma_1$, $\tilde{\vartheta}(z+\omega) = \tilde{\vartheta}(z) mod(\Gamma_2)$ et le fait que la fonction $z \mapsto \tilde{\vartheta}(z+\omega) - \tilde{\vartheta}(z)$ soit continue à valeurs dans un ensemble discret implique qu'elle est indépendante de z.
   Donc :
   $$\tilde{\vartheta}'(z) = \tilde{\vartheta}'(z+\omega)$$
   pour chaque $\omega \in \Gamma_1$. C'est une fonction holomorphe et bornée sur $\mathbb{C}$, donc constante. Cela implique que :
   $$\tilde{\vartheta}(z) = \alpha z + \gamma \quad \alpha, \gamma \in \mathbb{C}$$
   mais on avait $\tilde{\vartheta}(0) = 0$ et cela nous donne $\tilde{\vartheta} = \phi_\alpha$. L'application du théorème est donc surjective.
   Pour l'injectivité, on raisonne ainsi : si $\theta_\alpha = \theta_\beta$ alors pour chaque $z \in \mathbb{C}$ on a $\alpha z \equiv \beta z (mod\, \Gamma_1)$. La fonction $z \mapsto (\alpha - \beta)z$ renvoie $\mathbb{C}$ dans Γ_2 et elle est continue, donc constante, parce que Γ_2 est discret.
2. Les fonctions considérées sont toutes linéaires, elles préservent donc la structure de groupe.
3. Conséquence directe de 1 avec $\Gamma_1 = \Gamma_2$.
4. Si on peut trouver un tel λ alors ϕ_λ est inversible et a comme inverse $\varphi_{\lambda^{-1}}$, où φ sont les fonctions de la correspondance $\mathbb{C}/\Gamma_2 \to \mathbb{C}/\Gamma_2$

□

Étant donnée une structure de groupe sur la courbe elliptique et ayant sur $\mathbb{C}/\Gamma$ une structure de groupe héritée de $\mathbb{C}$ on peut parler d'homomorphismes isomorphismes analytiques entre les deux : c'est un isomorphisme de groupes tel que l'isomorphisme et son inverse soient holomorphes.

Il y a en effet des isomorphismes entre les surfaces $\mathbb{C}/\Gamma$ et les courbes elliptiques. Le but de cette section d'en montrer l'existence.

Théorème 6.3 *(a) Soit Γ un réseau. Soit g_2 et g_3 les séries associés à Γ. Le discriminant de $y^2 = 4x^3 - g_2 x - g_3$ est non nul. Donc c'est l'équation d'une courbe elliptique :*

$$\Delta = g_2^3 - 27 g_3^2 \neq 0$$

où Δ est le discriminant du polynôme de droite.

(b) Si $C(\mathbb{C})$ est la courbe elliptique définie par $y^2 = 4x^3 - g_2x - g_3$, alors l'application :

$$\begin{array}{rccc} \Phi : & \mathbb{C}/\Gamma & \to & C(\mathbb{C}) \\ & z & \mapsto & [\wp(z) : \wp'(z) : 1] \end{array}$$

est un isomorphisme analytique de surfaces de Riemann et un isomorphisme de groupes.

Démonstration :

(a) $\wp'$ est une fonction elliptique impaire. Soient ω_1 et ω_2 des générateurs du réseau Γ et $\omega_3 = \omega_1 + \omega_2$. On a $\wp'(\omega_i/2) = -\wp'(-\omega_i/2) = -\wp'(\omega_i/2)$, donc $\wp'$ a ses trois zéros (elle est de degré 3) en les points $\omega_i/2$.

Si les valeurs de $\wp$ en ces trois points sont différentes, le discriminant sera non nul. On considère pour chaque i, $\wp(z) - \wp(\omega_i/2)$: c'est une fonction paire et elle a un zéro double en $\omega_i/2$, sa dérivé étant $\wp'(z)$. La fonction considérée est comme $\wp(z)$ de degré 2, donc $\omega_i/2$ est son unique zéro. Les $\wp(\omega_i/2)$ sont distincts.

(b) Φ est évidemment bien définie, car l'image de $\mathbb{C}/\Gamma$ est dans la courbe elliptique. La fonction est surjective : prenons $(x, y) \in C(\mathbb{C})$, $\wp(z) - x$ n'est pas constante, donc elle a un zéro en a. On a $\wp'(a)^2 = y^2$ qui implique, comme $\wp$ est paire on peut éventuellement changer a par $-a$ pour avoir $wp'(a) = y$.

Injectivité : si $\Phi(z_1) = \Phi(z_2)$, on considère deux cas.

(i) $2z_1 \in \Gamma$, alors $\wp(z) - \wp(z_1)$ a un zéro double en z_1 comme montré dans la démonstration de (a). z_2 doit alors être congru à z_1 modulo Γ, parce que la fonction est d'ordre deux.

(ii) $2z_1 \notin \Gamma$, la même fonction $\wp(z) - \wp(z_1)$ a des zéros en z_1, $-z_1$ et z_2 donc $z_1 \equiv \pm z_2$. La fonction $\wp'$ nous donne le résultat, en effet :

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$$

et on sait que $2z_1 \notin \Gamma$ implique que $\wp'(z_1) \neq 0$.

Écrivons $\Phi = (x, y)$ en considérant son image dans $\mathbb{C}^2$. Si on regarde l'effet de la fonction Φ sur l'espace cotangent à $\mathbb{C}/\Gamma$ (l'espace des 1-formes), on a :

$$\Phi^\star(\frac{dx}{y}) = \frac{d\wp(z)}{\wp'(z)} = dz$$

Donc elle n'est jamais nulle sur $\mathbb{C}/\Gamma$. Aussi $\frac{dx}{y}$ n'est jamais nulle sur $C(\mathbb{C})$, comme démontré dans la section dédiée à $C(\mathbb{C})$. Le domaine et codomaine de Φ sont des variétés de dimension 1 (complexe), donc le résultat précédent sur Φ nous donne qu'elle est un isomorphisme local, en plus injectif et surjectif, donc elle est un isomorphisme analytique.

Passons à l'isomorphisme de groupes. Soit z_1, $z_2 \in \mathbb{C}$, alors existe une fonction f avec :

$$div(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)$$

par la proposition 5.0.8. Par la proposition 5.0.7, $f(z) = F(\wp(z), \wp'(z))$ avec F rationnelle. On a

$$div(F) = (\Phi(z_1 + z_2)) - (\Phi(z_1)) - (\Phi(z_2)) + (\Phi(0))$$

Par la proposition 5.0.9 :

$$\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2)$$

□

Théorème 6.4 *Soient E_1 et E_2 des courbes elliptiques correspondant aux réseaux Λ_1 et Λ_2 comme dans 6.3.*

1. *L'inclusion naturelle*

   $$\{ \text{ isogénies } \phi : E_1 \to E_2\} \to \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ applications holomorphes t. q. } \phi(0) = 0\}$$

   est une bijection.

2. *De plus, E_1 et E_2 sont isomorphes sur $\mathbb{C}$ ssi Λ_1 et Λ_2 sont homothétiques. ($\Lambda_1 = \alpha\Lambda_2$ pour un $\alpha \in \mathbb{C}^*$)*

Démonstration: Un isogénie ϕ est donnée localement par des fonctions rationnelles définies partout, c'est donc un morphisme de courbe elliptique. Alors l'application induite sur les tores complexes sera holomorphe. Le diagramme suivant commutatif :

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \to & \mathbb{C}/\Lambda_2 \\ \Phi_{\Lambda_1} \downarrow & & \downarrow \Phi_{\Lambda_2} \\ E_1 & \stackrel{\phi}{\to} & E_2 \end{array}$$

Alors l'application :

$$Hom(E_1, E_2) \to \ \ Application\ \ Holomorphe\ (\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) \text{ telque } 0 \mapsto 0$$

est bien définie. Aussi, il est évident, grâce à la commutativité du diagramme ci-dessus, qu'elle est injective.

Surjectivité : Par 1 il suffit de considérer une application de la forme ϕ_α, où α satisfait $\alpha\Lambda_1 \subset \Lambda_2$. La commutativité du diagramme ci-dessus montre que l'application induite sur les équations de Weierstrass est donnée par

$$\psi : E_1 \to E_2$$

$$[\wp(z, \Lambda_1), \wp'(z, \Lambda_1), 1] \to [\wp(\alpha z, \Lambda_2), (\wp'(\alpha z, \Lambda_2), 1].$$

Comme $\alpha\Lambda_1 \subset \Lambda_2$, on voit que pour tout $\omega \in \Lambda_1$,

$$\wp(\alpha(z + \omega), \Lambda_2) = \wp(\alpha z + \alpha\omega, \Lambda_2) = \wp(\alpha z, \Lambda_2).$$

De même on a :

$$\wp'(\alpha(z + \omega), \Lambda_2) = \wp'(\alpha z + \alpha\omega, \Lambda_2) = \wp'(\alpha z, \Lambda_2).$$

Alors $\wp(\alpha z, \Lambda_2)$ et $\wp'(\alpha z, \Lambda_2)$ sont dans $\mathbb{C}/\Lambda_1$. Comme $\mathbb{C}(\Lambda_1) = \mathbb{C}(\wp(z, \Lambda_1), \wp'(z, \Lambda_1))$ par 5.0.7 on peut exprimer $\wp(\alpha z, \Lambda_2)$ et $\wp'(\alpha z, \Lambda_2)$ par des fonctions rationnelles de $\wp(z, \Lambda_1)$ et $\wp'(z, \Lambda_1)$. Ceci implique que ψ est un isogénie.

Si E_1 et E_2 sont isomorphes, il existe $\phi_{12} : E_1 \to E_2$, $\phi_{21} : E_2 \to E_1$ isogénies telles que $\phi_{12} \circ \phi_{21} = id|_{E_2}$ et $\phi_{21} \circ \phi_{12} = id|_{E_1}$. ϕ_{12} et ϕ_{21} nous donnent par la bijection démontrée ci-dessus deux applications holomorphes qui envoient 0 à 0 entre $\mathbb{C}/\Lambda_1$ et $\mathbb{C}/\Lambda_2$. Ces applications sont inverses l'une de l'autre grâce encore à la commutativité du diagramme ci-dessus. Par 1 ces applications nous donnent α_{12} et α_{21} tels que $\alpha_{12}\Lambda_1 \subset \Lambda_2$ et $\alpha_{21}\Lambda_2 \subset \Lambda_1$ et $\alpha_{12}\alpha_{21} = 1$. Donc $\alpha_{21}\alpha_{12}\Lambda_1 \subset \alpha_{21}\Lambda_2 \subset \Lambda_1$. Alors les inclusions sont des égalités. C'est à dire que Λ_1 et Λ_2 sont homothétiques.

□

7 Uniformisation

On admet le résultat suivant :

Théorème 7.1 (Théorème d'Uniformisation) *Soient $A, B \in \mathbb{C}$ satisfaisant $A^3 - 27B^2 \neq 0$. Alors il existe un unique réseau $\Lambda \subset \mathbb{C}$ tel que $g_2(\Lambda) = A$ et $g_3(\Lambda) = B$.*

Proposition 7.1.1 *Soit $E/\mathbb{C}$ une courbe elliptique. Alors il existe un réseau $\Lambda \subset \mathbb{C}$, unique à homothétie près, et un isomorphisme complexe analytique de groupes de Lie.*

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

$$\phi(z) = [\wp(z, \Lambda), \wp'(z, \Lambda), 1]$$

Démonstration: L'existence découle de 6.3 et du Théorème d'Uniformisation. Il est unique grâce au théorème 2.

□

Théorème 7.2 *Soient α et β les chemins sur $E(\mathbb{C})$ donnant une base de $H_1(E,\mathbb{Z})$. Alors les périodes*

$$w_1 = \int_\alpha \frac{dx}{y} \quad et \quad w_2 = \int_\beta \frac{dx}{y}$$

sont $\mathbb{R}$-linéairement indépendantes.

Démonstration: Par la proposition 7.1.1 et le théorème 6.3 il existe un réseau Λ_1 tel que l'application

$$\phi_1 : \mathbb{C}/\Lambda_1 \to E(\mathbb{C})\ \phi_1(z) : [\wp(z,\Lambda_1), \wp'(z,\Lambda_1,1]$$

soit un isomorphisme complexe analytique. On en déduit que $\phi_1^{-1}\circ\alpha$ et $\phi_1^{-1}\circ\beta$ forment une base de $H_1(\mathbb{C}/\Lambda_1,\mathbb{Z})$. De plus $H_1(\mathbb{C}/\Lambda_1,\mathbb{Z})$ est isomorphe à Λ_1 par l'application $\gamma \mapsto \int_\gamma dz$. Sur $\mathbb{C}/\Lambda_1$ on a,

$$\phi_1^*(dx/y) = d\wp(z)/\wp'(z) = dz.$$

Les périodes

$$\omega_1 = \int_\alpha dx/y = \int_{\phi_1^{-1}\circ\alpha} dz \qquad \omega_2 = \int_\beta dx/y = \int_{\phi_1^{-1}\circ\beta} dz$$

forment une base de Λ_1. Ils sont $\mathbb{R}$-linéairement indépendant.

□

Théorème 7.3 *Soit $\Lambda \subset \mathbb{C}$ un réseau engendré par ω_1 et ω_2. L'application*

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda \qquad F(P) = \int_{\mathcal{O}}^{P} dx/y (mod\Lambda)$$

est un isomorphisme complexe analytique de groupe de Lie. Son inverse est donné par

$$\mathbb{C}/\Lambda \to E(\mathbb{C}) \qquad \phi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1].$$

Démonstration: Par le théorème précédent, le réseau Λ engendré par les périodes de E est précisément celui qui correspond à E par la proposition suivant le théorème d'Uniformisation. La composition $F\circ\phi$ donne une application analytique

$$F\circ : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \qquad z \to \int_{\mathcal{O}}^{(\wp(z),\wp'(z))} dx/y.$$

Puisque $F^*(dz) = dx/y$ et $\phi^*(dx/y) = d\wp(z)/\wp'(z) = dz$, on voit que $(F\circ\phi)^* dz = dz$.

Par théorème 6.2 3) on sait que toute application analytique $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, $\phi(0) = 0$ a la forme $\phi_a(z) = az$ pour un $a \in \mathbb{C}^*$. Comme $\phi_a^*(dz) = a dz$, on a $F\circ\phi(z) = z$ (c'est à dire que $F\circ\phi$ est l'identité). On sait que ϕ est un isomorphisme analytique, donc $F = \phi^{-1}$ l'est aussi.

□

Notons $H_1(E,\mathbb{Z})$ le groupe fondamental de $E(\mathbb{C})$. Comme $E(\mathbb{C})$ est homéomorphe à un tore alors $H_1(E,\mathbb{Z})$ est isomorphe à $\mathbb{Z}\times\mathbb{Z}$ qui est le groupe fondamental d'un tore.

Théorème 7.4 *Il existe une application analytique de $E(\mathbb{C})$ dans $\mathbb{C}$ quotienté par un réseau.*

Démonstration : On vient de voir que $E(\mathbb{C})$ est homéomorphe à un tore. Par Fig 6 on voit que ils existent deux lacets non homotopes sur un tore. Alors abstraitement ils existent deux lacets l_1 et l_2 sur $E(\mathbb{C})$ aussi. Soit $w_i = \int_{l_i} \frac{dx}{y}$ pour $i = 1, 2$.

Fixons $0 \in E(\mathbb{C})$. Considérons

$$\begin{array}{cccc} \phi & E(\mathbb{C}): & \to & \frac{\mathbb{C}}{w_1\mathbb{Z}+w_2\mathbb{Z}} \\ & p & \mapsto & \int_0^p \frac{dx}{y} \end{array}$$

ϕ ne dépend pas sur le chemin choisi : Soit C_1, C_2 deux chemins tels que $C_1(0) = C_2(0) = 0$ et $C_1(1) = C_2(1) = P$. $C_1 - C_2$ est un lacet homotope à une combinaison $\mathbb{Z}$-linéaire de l_1, l_2. Par le théorème de Cauchy l'intégrale de $\frac{dx}{y}$ sur $C_1 - C_2$ est égale à une combinaison Z-linéaire des

intégrales sur l_1 et l_2 c'est à dire que l'intégrale est une combinaison $\mathbb{Z}$-linéaire des intégrales sur w_1 et w_2 qui ne sont pas zéro grâce encore au choix.

ϕ est une application holomorphe. Alors l'image est ouverte.

Puisque le tore est compact et $E(\mathbb{C})$ est homéomorphe à un tore alors elle est compacte aussi. $\frac{\mathbb{C}}{w_1\mathbb{Z}+w_2\mathbb{Z}}$ est séparé et connexe. Alors l'image de $E(\mathbb{C})$ par ϕ est fermé et donc surjective. Alors on a $\frac{\mathbb{C}}{w_1\mathbb{Z}+w_2\mathbb{Z}}$ est compacte. Alors il ne peut être qu'un tore. Donc $w_1\mathbb{Z}+w_2\mathbb{Z}$ noté Γ est bien un réseau.

8 Points Algébriques sur une Courbe Cubique

Soit C une courbe elliptique sur $\mathbb{Q}$ donnée par l'équation de Weierstrass

$$C : y^2 = x^3 + ax^2 + bx + c \text{ avec } a, b, c \in \mathbb{Q}.$$

Soit K un sous corps de $\mathbb{C}$. On rappelle

$$C(K) := (x, y)|x, y \in K, (x, y) \in C \cup \infty$$

Pour $P \in C(K)$ et $\sigma \in Aut_{\mathbb{Q}alg}(\mathbb{C})$, on définit $\sigma(P)$ par

$$\sigma(P) = \begin{array}{c} (\sigma(x), \sigma(y)) \text{ si } P = (x, y) \\ \infty \text{ si } P = \infty \end{array}$$

Considérons $\lambda_n : C(\mathbb{C}) \to C(\mathbb{C}), \lambda_n(P) = nP$. Le noyau de λ_n est un sous groupe de $C(\mathbb{C})$ noté $C[n]$.

Proposition 8.0.1 *Soit C une courbe elliptique définie par ses coefficients dans $\mathbb{Q}$ et soit K une extension galoisienne de $\mathbb{Q}$.*

1. *$C(K)$ est un sous-groupe de $C(\mathbb{C})$.*
2. *Si $P \in C(K)$ alors $\sigma(P) \in C(\sigma(K))$.*
3. *On a une action de $Aut_{\mathbb{Q}alg}(C)$ sur $C(K)$ qui préserve $\mathbb{C}[n]$.*
4. *Pour tout $P, Q \in C(K)$ et tout $\sigma \in Hom_{\mathbb{Q}alg}(\mathbb{C})$,*

   $$\sigma(P + Q) = \sigma(P) + \sigma(Q) \text{ et } \sigma(-P) = -\sigma(P).$$

   Alors $\sigma(nP) = n\sigma(P)$ pour tout $n \in \mathbb{N}$.
5. *Si $P \in C(K)$ a ordre n et si $\sigma \in Gal(K/\mathbb{Q})$ alors $\sigma(P)$ est d'ordre n aussi.*

Démonstration :

1. Les formules de la loi d'addition, qu'on connaît explicitement, sont des fonctions rationnelles des coordonnées. Alors $C(K)$ est fermé pour l'addition, c'est donc bien un sous-groupe de $C(\mathbb{C})$. Aussi on a donc démontré 4.
2. On voit ainsi que $\sigma(P)$ sera envoyé dans $\sigma(K)$ car ses coordonnées sont dans K.
3. Pour tout $P \in C(K)$ et $\sigma, \tau \in Aut_{\mathbb{Q}alg}(C)$,

   $$(\sigma\tau)(P) = \sigma(\tau(P)).$$

   De plus, l'identité agit trivialement. On remarque que $\sigma(nP) = n\sigma(P)$. Cela démontre aussi 5.

□

Proposition 8.0.2 . *En tant que groupe, $C[n] \equiv \frac{\mathbb{Z}}{n\mathbb{Z}} \bigoplus \frac{\mathbb{Z}}{n\mathbb{Z}}$.*

Démonstration : Par 7.1.1 on voit que $C(\mathbb{C})$ est isomorphe à $\mathbb{C}/L$ où $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ est un réseau de $\mathbb{C}$.

$$\mathbb{Z}/n\mathbb{Z} \bigoplus \mathbb{Z}/n\mathbb{Z} \to C[n] \subset \mathbb{C}/L$$

$$(a_1, a_2) \to \frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2$$

est l'isomorphisme recherché. □

Théorème 8.1 *Extension de plongement de corps. Soit K/F une extension de corps. Soit G une sous extension. Soit σ un F- plongement de G dans un corps L algébriquement clos. Alors il existe $\tilde{\sigma}$ un F-plongement de K dans L qui étend σ.*

Lemme 8.1.1 *Soit K une extension séparable du corps F. On suppose qu'il existe un F-plongement de K dans un corps algébriquement clos L. Le nombre de tels prolongements est égal au degré de l'extension de K sur F. En particulier, il est infini quand le degré de l'extension est infini.*

Démonstration: D'abord on suppose que K est une extension primitive de F. Alors $K = F(x)$. Si x est algébrique sur F (dans ce cas on n'a pas besoin de l'hypothèse qu'il existe un F- plongement de K dans L) le degré de K/F est égal au degré du polynôme minimal $P(X)$ de x sur F. Un F-plongement de K dans L renvoie x à une racine de $P(X)$ dans L. Cette image caractérise aussi complètement le plongement. Deux images différents donnent évidemment deux F-plongements différents de K. Alors, le nombre de plongement est égal au degré de $P(X)$ qui est égal au degré d'extension K/F. Si x était transcendant sur F, on renverrait x à y^i où y est un élément de L transcendant sur F et $i \in \mathbb{N}$. Un tel élément existe car par hypothèse, il existe un prolongement de K dans L et l'image de x est transcendant sur F.

Si K/F est une extension finie, comme elle est séparable alors elle est primitive.

On considère deux cas quand K/F est infini.

Cas 1 : L'extension K/F est algébrique - Démontrons le par l'absurde : supposons qu'il existe un nombre fini n de plongements étendant le plongement donné. Prenons une sous-extension G telle que le degré de G/F soit $\geq n$.Le nombre de F-prolongements de G dans L est plus grand que n ci-dessus. Tous ces prolongements s'étendent par le 8.1 au plongement distinct de K dans L. On a une contradiction.

Cas 2 : L'extension K/F n'est pas algébrique - prenons un élément $x \in K \backslash F$ tel que x soit transcendantal sur F. Par ci-dessus $F(x)$ a un nombre infini de F-plongements dans L et tous ces plongement s'étendent au plongements distincts de K dans L. □

Proposition 8.1.1 *Soit C une courbe elliptique donné sous forme de Weierstrass*

$$C : y^2 = x^3 + ax^2 + bx + c \text{ avec } a, b, c \in \mathbb{Q}.$$

1. *Soit $P = (x_1, y_1) \in C$ un point d'ordre fini. Alors x_1 et y_1 sont algébrique sur $\mathbb{Q}$.*
2. *Soit*

$$\{(x_1, y_1), \ldots, (x_m, y_m), \infty\} = C[n]$$

l'ensemble des points dont l'ordre divise n.

$$K_n := \mathbb{Q}(x_1, y_1 \ldots, x_m, y_m)$$

est une extension galoisienne de $\mathbb{Q}$.

Remarque : En général, $Gal(K/\mathbb{Q})$ n'est pas abélien.

Exemple 8.1.1 On considère la courbe C donné sous la forme de Weierstrass $y^2 = x^3 - 2$. Les points d'ordre deux ont coordonné de y nulle. Alors $K_2 = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ qui est bien une extension galoisienne mais pas abélienne ayant Σ_3 comme le groupe de Galois.

Démonstration :

1. Un homomorphisme de corps de K dans $\mathbb{C}$ est caractérisé par son action sur $C[n]$. Il s'identifie ainsi avec un élément de groupe de permutation des points $P_1, \ldots, P_m$ par 3. Donc le nombre d'homomorphismes est fini. Si un x_i ou y_i n'était pas algébrique sur $\mathbb{Q}$, le degré de K serait infini sur $\mathbb{Q}$. Comme la caractéristique de $\mathbb{Q}$ est zéro alors K_n est un extension séparable de $\mathbb{Q}$. Par le lemme ci-dessus, il y aurait donc un nombre infini d'homomorphismes distincts.
2. L'ordre de $\sigma(P_i)$ divise n par 5. Il est donc l'un des points P_i. Alors les coordonnées de $\sigma(P_i)$, c'est-à-dire, $\sigma(x_i), \sigma(y_i)$ sont déjà dans K. Alors $\sigma(K) \subset K$. Alors K est une extension galoisienne de $\mathbb{Q}$.

□

9 Représentation Galoisienne

Définition 9.0.1 (Représentation d'un groupe G) Soit A un anneau commutatif. Soit M un A-module libre. Un homomorphisme de G dans $Aut_A(M)$ est appelé une représentation de G.

Définition 9.0.2 (Représentation Galoisienne) Une représentation d'un groupe de Galois est appelée représentation galoisienne.

Par 3 on a

$$\phi : Gal(K(C[n])/K) \to Aut(C[n])$$

où K est une extension de $\mathbb{Q}$. On obtient ainsi une représentation galoisienne. Soit $C[n]$, qui est isomorphe à $\mathbb{Z}/n\mathbb{Z} \bigoplus \mathbb{Z}/n\mathbb{Z}$, engendre par P_1 et P_2. Alors $Aut(C[n]) \equiv GL_2(\mathbb{Z}/n\mathbb{Z})$.

Théorème 9.1 (Théorème de représentation de Galois) *Soit C une courbe elliptique donnée par l'équation de Weierstrass avec des coefficients rationnels et soit $n \geq 2$ un nombre entier. Fixons les générateurs P_1 et P_2 de $C[n]$. Alors l'application ϕ est un monomorphisme de groupes.*

Démonstration : Que ϕ est un homomorphisme est clair. Il suffit de démontrer l'injectivité. Si σ fixe P_1 et P_2 alors il fixe tout $P \in C[n]$. Comme $\sigma(x, y) = (\sigma(x), \sigma(y))$, alors σ fixe tous les x et y coordonnées des points de $C[n]$. Ces coordonnées engendrent $K(C[n])$ alors σ fixe le corps entier. C'est à dire que σ est identité. □

10 Multiplication Complexe

Les points complexes sur une courbe elliptique forment un groupe abélien. Pour tout groupe abélien il existe un morphisme, qui est la multiplication par n.

On remarque que comme un isogénie est un endomorphisme, il envoie 0 sur 0. La multiplication par n sur $C(\mathbb{C})$ s'exprime par des fonctions rationnelles. Alors elle est une isogénie.

Définition 10.0.1 (Multiplication Complexe) Soit C une courbe elliptique. On dit que C a une multiplication complexe s'il existe un endomorphisme isogénie ϕ de C qui n'est pas une multiplication par n.

Exemple de Multiplication Complexe On donne deux exemples des fonctions rationnels qui sont des homomorphismes grâce au dernier théorème.

Exemple 10.0.1 La courbe elliptique $C : y^2 = 4x^3 - 4x$ a la multiplication complexe $\phi(x, y) = (-x, iy)$.

Exemple 10.0.2 La courbe elliptique $C : y^2 = x^3 + 1$ a la multiplication complexe $\phi(x, y) = (\frac{-1+\sqrt{(-3)}}{2}x, -y)$.

On remarque que l'ensemble des endomorphismes de $C(\mathbb{C})$ est un anneau abélien. $(\phi_1+\phi_2)(P) = \phi_1(P) + \phi_2(P)$ et $(\phi_1\phi_2)(P) = \phi_1(\phi_2(P))$. Si $C(\mathbb{C})$ n'a pas de multiplication complexe cet anneau est $\mathbb{Z}$. Sinon il est strictement plus large.

Soit E une courbe elliptique avec la multiplication complexe θ. Soit L un réseau obtenu par 7.1.1. Par 1 on obtient un $\phi \in End(\mathbb{C}/L)$ qui renvoie 0 sur 0. Par 1 on obtient c tel que $cL \subset L$. Comme θ est une multiplication complexe alors $c \notin \mathbb{Z}$.

Proposition 10.0.1 *Alors c n'est pas réel.*

Ceci justifie l'appellation multiplication complexe.

Démonstration : Choisissons des générateurs pour L. Disons

$$L = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \{a_1w_1 + a_2w_2 | a_1, a_2 \in \mathbb{Z}\}.$$

Notons que w_1 et w_2 sont linéairement indépendants sur $\mathbb{R}$ car ils engendrent un réseau. Comme $cL \subset L$, $cw_1 \in L$ alors il existe $A, B \in \mathbb{Z}$ tel que

$$cw_1 = Aw_1 + Bw_2.$$

Donc

$$(c - A)w_1 - Bw_2 = 0.$$

Si c était réel, $c - A$ serait zéro, c-a-d $c = A$. Ceci implique que $c \in \mathbb{Z}$. Alors c n'est pas réel. □

11 Le module de Tate

Soit E/K une courbe elliptique. On suppose que l est premier à $Char(K)$.

Définition 11.0.2 (Les entiers $l - adique$)

$$\mathbb{Z}_l = \{(x_n), n \in \mathbb{N} | x_n \in \mathbb{Z}/l^n\mathbb{Z}, x_{n-1} \equiv x_n(l^{n-1})\},$$

Les entiers $l - adique$, $\mathbb{Z}_l$, forment un anneau intègre, local, principal. L'idéal maximal étant $l\mathbb{Z}_l = \{(x_n) \in \mathbb{Z}_l | x_1 = 0\}$. Un idéal non nul quelconque est engendré par l^n dans $\mathbb{Z}_l$.

Définition 11.0.3 (Le module de Tate) Soit E une courbe elliptique et $l \in \mathbb{Z}$ un nombre premier. Le module de Tate $l - adique$ de E est le groupe abélien $T_l(E) = \varprojlim_n E[l^n]$, la limite inverse prise par rapport aux applications canoniques $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$.

Comme chaque $E[l^n]$ est un $\mathbb{Z}/l^n\mathbb{Z} - module$, alors on voit que le module de Tate a une structure naturelle comme un $\mathbb{Z}_l - module$ donné par

$$(a_1, a_2, \dots, a_n, \dots)(P_1, P_2, \dots, P_n, \dots) = (a_1P_1, a_2P_2, \dots, a_nP_n, \dots).$$

Il existe un k tels que $a_i = a_{i-1} + l^{i-1}k$. Comme

$$la_iP_i = a_iP_{i-1} = (a_{i-1} + l^{i-1}k)P_{i-1} = a_{i-1}P_{i-1},$$

on vérifie que la définition est bonne.

Proposition 11.0.2 *Le noyau de la projection naturelle sur la nième coordonné* $(P_1, \dots, P_n) \mapsto P_n$ *de* $T_l(E) \to E[l^n]$ *est* $l^nT_l(E)$.

Démonstration: Il est clair que $l^nT_l(E)$ est contenu dans le noyau car son nième coordonné vaut zéro. Réciproquement, un élément $(P_1, P_2, \dots, P_n, \dots)$ du noyau est égal à $l^n(P_{n+1}, P_{n+2}, \dots)$ par la définition de limite inverse. □

Proposition 11.0.3 $T_l(E)$ *est isomorphe à* $\mathbb{Z}_l \times \mathbb{Z}_l$ *comme un* $\mathbb{Z}_l$ *module.*

Démonstration: Par 8.0.2 $E[l^n]$ est isomorphe à $\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ comme un $\mathbb{Z}/l^n\mathbb{Z}$ module. De plus on a la commutativité du diagramme suivant :

$$\begin{array}{ccc} E[l^{n+1}] & \xrightarrow{[l]} & E[l^n] \\ \downarrow & & \downarrow \\ \frac{\mathbb{Z}}{l^{n+1}\mathbb{Z}} \times \frac{\mathbb{Z}}{l^{n+1}\mathbb{Z}} & \xrightarrow{l \times l} & \frac{\mathbb{Z}}{l^n\mathbb{Z}} \times \frac{\mathbb{Z}}{l^n\mathbb{Z}} \end{array}$$

où les flèches verticales sont des isomorphismes. La commutativité du diagramme implique que

$$T_l(E) \equiv \lim_{\underset{n}{\leftarrow}} E[l^n] \equiv \lim_{\underset{n}{\leftarrow}} (\mathbb{Z}_{l^n} \times \mathbb{Z}_{l^n}) \equiv \mathbb{Z}_l \times \mathbb{Z}_l.$$

□

Proposition 11.0.4 *On a*

$$G_{\frac{\bar{K}}{K}} \to End_{\mathbb{Z}_l}(T_l(E))$$

tels que

$$\sigma \to ((P_1, P_2, \dots, P_n) \to (\sigma(P_1), \sigma(P_2), \dots, \sigma(P_n))).$$

Démonstration: La multiplication par l utilisée pour la limite inverse est donnée par un polynôme pour chaque point de $E[l^n]$. Alors l'action de $G_{\frac{\bar{K}}{K}}$ sur $E[l^n]$ commute avec la multiplication par l. Du coup, $G_{\frac{\bar{K}}{K}}$ agit sur $T_l(E)$.

$$\begin{aligned} \sigma((a_1, a_2, \dots)(P_1, P_2, \dots)) = \sigma(a_1P_1, a_2P_2, \dots) = (\sigma(a_1P_1), \sigma(a_2P_2), \dots) = \\ = (a_1\sigma(P_1), a_2\sigma(P_2), \dots) = (a_1, a_2, \dots)\sigma(P_1, P_2, \dots) \end{aligned}$$

Alors l'action est $\mathbb{Z}_l$ linéaire.

□

Définition 11.0.4 (Représentation l-adique) C'est l'application

$$\rho_l : G_{\frac{\bar{K}}{K}} \longrightarrow Aut(T_{\mathbb{Z}_l}(E))$$

$$\rho_l(g) \times ((x_0, y_0), (x_1, y_1), \dots) \longrightarrow ((g(x_0), g(y_0)), (g(x_1), g(y_1)) \dots).$$

Si on choisit une $\mathbb{Z}_l$ base de $T_l(E)$ on obtient une représentation

$$G_{\frac{\bar{K}}{K}} \longrightarrow GL_2(\mathbb{Z}_l).$$

Soit $\mathbb{Q}_l = Frac(\mathbb{Z}_l)$, c'est un corps de caractéristique zéro. L'inclusion canonique $\mathbb{Z}_l \subset \mathbb{Q}_l$ donne

$$G_{\frac{\bar{K}}{K}} \longrightarrow GL_2(\mathbb{Q}_l).$$

Ainsi on obtient une représentation 2-dimensionnelle de $G_{\frac{\bar{K}}{K}}$ sur $\mathbb{Q}_l$ qui est un corps de caractéristique zéro.

12 Extension abélienne de $\mathbb{Q}(i)$

La courbe elliptique $y^2 = 4x^3 - 4x$ admet la multiplication complexe $\phi(x, y) = (-x, iy)$. On démontrera dans cette section que ses points de n-torsion engendrent une extension galoisienne abélienne de $\mathbb{Q}(i)$.

Soit $K/\mathbb{Q}$ une extension galoisienne de $\mathbb{Q}$ contenant i. Soit $\sigma \in Gal(K/\mathbb{Q})$ et $P \in C(K)$.

Proposition 12.0.5 *ϕ commute avec $Gal(K/\mathbb{Q}(i))$.*

$$\sigma(\phi(P)) = \sigma(-x, iy) = (\sigma(-x), \sigma(iy)) = (-\sigma(x), \sigma(i)\sigma(y)).$$
$$\phi(\sigma(P)) = \phi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)).$$

Comme $\sigma(i) = i$ on a $\sigma(\phi(P)) = \phi(\sigma(P))$ pour tout point $P \in C(K)$. Donc ϕ commute avec tous les éléments de $\sigma \in Gal(K/\mathbb{Q}(i))$. □

Théorème 12.1 *Soit C la courbe elliptique*

$$y^2 = 4x^3 - 4x.$$

Pour tout entier $n \geq 1$, soit

$$K_n = \mathbb{Q}(i)(C[n])$$

le corps engendré par i et les coordonnés de points dans $C[n]$. Alors K_n est une extension galoisienne abélienne de $\mathbb{Q}(i)$.

Démonstration: Les corps $\mathbb{Q}(i)$ et $\mathbb{Q}(C[n])$ sont de Galois sur $\mathbb{Q}$. Alors K_n leur composition est de Galois sur $\mathbb{Q}$. A fortiori K_n est de Galois sur $\mathbb{Q}(i)$.

On a $\phi \in Aut_{\mathbb{Q}_{alg}}(C)$. Nous avons vu dans 3 que ϕ restreint à $C[n]$ est un élément de $Aut(C[n])$. De plus, son action est $\mathbb{Z}$ linéaire car c'est un endomorphisme. Fixons l un nombre premier. Alors ϕ agit sur $T_l(E)$ aussi.

Le théorème découle des 3 lemmes suivants. Nous les démontrerons d'abord et après nous compléterons la démonstration du théorème.

Lemme 12.1.1 *ϕ n'agit pas sur $T_l(E)$ par homothétie.*

Démonstration: On suppose que ϕ agit sur $T_l(E)$ par homothéties. Comme $\phi(lT_l(E)) \subset lT_l(E)$ et $T_l(E)/lT_l(E)$ est isomorphe à $E[l]$ par 11.0.3, on obtient $\tilde{\phi}$ agissant par homothéties sur $E[l]$. C'est à dire que $\phi : E[l] \to E[l]$ est la multiplication par m pour un $m \in \mathbb{Z}$.

Soit $\tau : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe. On fixe une inclusion de K_n dans $\mathbb{C}$. Comme $\tau \in Gal(K_n/\mathbb{Q})$ par 4 on a $\tau(mP) = m\tau(P)$. Comme $\tau(i) = -i$ on a

$$\tau(\phi(P)) = \tau(-x, iy) = (\tau(-x), \tau(iy)) = (-\tau(x), -i\tau(y)) = -\phi(\tau(P)).$$

pour tout $P \in E(K_n)$. Donc ceci est vrai à fortiori pour tout $P \in E[l]$, on a alors

$$m\tau(P) = \tau(mP) = \tau(\phi(P)) = -\phi(\tau(P)) = -m\tau(P))$$

car $\tau(P)$ est aussi dans $E(l)$.

Donc, $2m\tau(P) = 0$ pour tout $P \in E(l)$. Comme τ ne permute que les éléments de $E(l)$ alors on a $2mP = 0$ pour tout $P \in E(l)$. Si $l|m$ on a $\phi(P) = 0$ pour tout $P \in E(l)$. Mais comme $\phi(\phi(P)) = -P$ alors il est obligatoire que $l = 2$. Dans ce cas on calcule la matrice de ϕ explicitement en prenant $P_1 = (0, 0)$ et $P_2 = (i, 0)$ comme générateurs de $E(2)$. Alors $\phi(P_1) = (0, 0) = P_1$ et $\phi(P_2) = (-i, 0) = P_1 + P_2$. Donc la matrice de $\phi : E(2) \to E(2)$ est $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Cette matrice n'est pas diagonale. Donc on a aussi éliminé le cas $l = 2$.

□

Lemme 12.1.2 *Soit k un corps, si $u \in End_k(k^2)$ n'est pas une homothétie alors*

$$Comm_{End_k(k^2)}(u) = k[u]$$

.

Démonstration: Il est clair que $k[u] \subset Comm_{End_k(k^2)}(u) \subset End_k(k^2)$. On considère le polynôme caractéristique $P(X) \in k(X)$ de u sur k.

Cas 1 : $P(X)$ est irréductible de degré 2. Alors $k[u]$ est un corps et son rang sur k est 2. Le rang de $End_k(k^2)$ sur k est 4. Si le rang de $Comm_{End_k(k^2)}(u)$ sur $k[u]$ est 2 alors il est égal à $End_k(k^2)$.

Il est bien connu que le centre de $End_k(k^2)$ est l'ensemble des homothéties et on a supposé que u ne l'est pas. Alors le rang de $Comm_{End_k(k^2)}(u)$ sur $k[u]$ est 1, c'est-à-dire qu'ils sont égaux.

Cas 2 : $P(X)$ a des racines r_1 et r_2 distinctes. Alors u est conjugué à une matrice diagonale D par une matrice $C \in Gl_2(k^2)$. $Comm_{End_k(k^2)}(u)$ est conjugué à $Comm_{End_k(k^2)}(D)$ par C aussi. Il suffit montrer alors que $Comm_{End_k(k^2)}(D)$ est égal $k[D]$. Il est facile à voir que le commutant d'un matrice diagonale est aussi diagonale et que $k[D]$ est l'ensemble de toutes les matrices diagonale car $r_1 \neq r_2$.

Cas 3 : $P(X)$ a des racines égales. Alors u est conjugué à une matrice $D + N$ où D est une homothétie et N est nilpotent. u n'est pas un homothétie alors il n'est pas conjugué a une matrice diagonale alors N n'est pas zéro. Comme ci-dessus il suffit prouver que le commutant de $D + N$ est $k[D + N]$. Ceci se voit facilement en écrivant les 2×2 matrices.

□

La projection $T_l(E) \to E[l^j]$ nous donne un morphisme de $\theta : Aut_{\mathbb{Z}l}(T_l(E)) \to Aut_{\mathbb{Z}/l^n\mathbb{Z}}(E[l^j])$. Ce morphisme par composition avec ρ_l défini dans 11.0.4 nous donne pour $K = \mathbb{Q}(i)$ une application

$$\rho_l^j : Gal(\tilde{\mathbb{Q}}/\mathbb{Q}(i)) \to Aut_{\mathbb{Z}/l^j\mathbb{Z}}(E[l^j]).$$

Comme $K_{l^j}/\mathbb{Q}(i)$ est une extension galoisienne alors grâce au théorème 8.1 on a une surjection

$$res : Gal((\tilde{\mathbb{Q}}(i))/\mathbb{Q}(i)) \to Gal(K_{l^j}/\mathbb{Q}(i))$$

$$\sigma \longrightarrow \sigma|_{K_{l^j}}$$

Par le théorème 9.1 on a une injection $\rho_{l^j} : Gal(K_{l^j}/\mathbb{Q}(i)) \to Aut_{\mathbb{Z}/l^j\mathbb{Z}}(E[l^j])$. L'action de ρ_l^j se factorise par res car un élément de $Gal((\tilde{\mathbb{Q}}(i)/\mathbb{Q}(i)))$ agit sur $E[l^j]$ coordonnée par coordonnée, alors l'action est complètement déterminée par sa restriction sur K_{l^j} qui est le corps engendré par les coordonnées des éléments de l^j torsion.

Alors on a le diagramme suivant commutatif :

$$\begin{array}{ccc} Gal(\tilde{\mathbb{Q}}(i)/\mathbb{Q}(i)) & \xrightarrow{\rho_l} & Aut_{\mathbb{Z}_l}(T_l(E)) \\ res \downarrow & & \theta \downarrow \\ Gal(K_{l^j}/\mathbb{Q}(i)) & \xrightarrow{\rho_{l^j}} & Aut_{\mathbb{Z}_{l^j}}(E[l^j]) \end{array}$$

Comme l'image de ρ_{l^j} fixe i alors il commute avec ϕ par la proposition 12.0.5. Le lemme 12.1.1 nous dit que ϕ n'est pas un homothétie et le lemme 12.1.2 implique que l'image de ρ_{l^j} tombe dans $\mathbb{Z}_{l^j}(\phi)$. Alors l'image est abélienne. Ceci démontre le théorème quand n est une pure puissance d'un nombre premier.

Dans le cas général considérons pour r, s premiers entre eux,

$$\chi : E[rs] \tilde{\longrightarrow} E[r] \times E[s]$$

$$x \mapsto (sx, rx)$$

Il est clair que ϕ est un morphisme de groupes. Comme $(r, s) = 1$ alors il est aussi injectif. On voit qu'il est surjectif en regardant l'ordre des deux groupes. Alors c'est un isomorphisme.

Lemme 12.1.3

$$\theta : Gal(K_{rs}/\mathbb{Q}(i)) \longrightarrow Gal(K_r/\mathbb{Q}(i)) \times Gal(K_s/\mathbb{Q}(i))$$

$$\sigma \longrightarrow (\sigma|_{K_r}, \sigma|_{K_s})$$

est un monomorphisme de groupe.

Démonstration: Comme $K_r/\mathbb{Q}$ et $K_s/\mathbb{Q}$ sont des extensions galoisiennes de $\mathbb{Q}(i)$ alors K_r et K_s sont envoyés dans eux-même par les éléments de $Gal(K_{rs}/\mathbb{Q}(i))$. Alors θ est un homomorphisme de groupe. Démontrons l'injectivité de θ. L'isomorphisme χ nous donne $\tilde{\chi}$ qui est un isomorphisme entre $Aut(E[rs])$ et $Aut(E[r]) \times Aut(E[s])$. On rappelle que $\rho_{rs} : Gal(K_{rs}/\mathbb{Q}(i) \mapsto Aut_{\frac{\mathbb{Z}}{rs\mathbb{Z}}}(E[rs])$.

Le diagramme suivant est commutatif :

$$\begin{array}{ccccc} Gal(K_{rs}/\mathbb{Q}(i)) & \times E[rs] & \longrightarrow & E[rs] \\ \theta \downarrow & \chi \downarrow & & \chi \downarrow \\ Gal(K_s/\mathbb{Q}(i)) \times Gal(K_s/\mathbb{Q}(i)) & \times E[r] \times E[s] & \longrightarrow & E[r] \times E[s] \end{array}$$

Prenons $\sigma \in Gal(K_{rs}/\mathbb{Q}(i))$ et $(p_x, p_y) \in E[rs]$.

$$\sigma(p_x, p_y) = (\sigma(p_x), \sigma(p_y)) \mapsto (s(\sigma(p_x), \sigma(p_y)), r(\sigma(p_x), \sigma(p_y))) = (s(\sigma(p_x, p_y)), r(\sigma(p_x, p_y)))$$

$$(\sigma|_{K_r}, \sigma|_{K_s})(s(p_x, p_y), r(p_x, p_y)) = (\sigma|_{K_r}(s(p_x, p_y)), \sigma|_{K_s}(r(p_x, p_y))) = (s(\sigma(p_x, p_y)), r(\sigma(p_x, p_y)))$$

Donc, le diagramme suivant est commutatif :

$$\begin{array}{ccc} Gal(K_{rs}/\mathbb{Q}(i)) & \xrightarrow{\rho_{rs}} & Aut(K[rs]) \\ \theta \downarrow & & \tilde{\chi} \downarrow \\ Gal(K_r/\mathbb{Q}(i)) \times Gal(K_s/\mathbb{Q}(i)) & \xrightarrow{\rho_r \times \rho_s} & Aut(K[r]) \times Aut(K[s]) \end{array}$$

Par le théorème 9.1 $\rho_{rs}, \rho_r, \rho_s$ sont des monomorphismes. Si $\theta(\sigma) =$ identité alors $\rho_r \times \rho_s(\theta(\sigma)) =$ identité. La commutativité implique que $\tilde{\chi}(\rho_{rs}(\sigma)) =$ identité. Alors on a $\rho_{rs}(\theta(\sigma))$ identité car $\tilde{\chi}$ est un isomorphisme. ρ_{rs} injective implique que $\sigma =$ identité.

□

Comme $Gal(K_{l^j}/\mathbb{Q}(i))$ sont abéliens, la dernière proposition implique que $Gal(K_n/\mathbb{Q}(i))$ est abélien.

□

Notons $s = \sum_{\omega \in \mathbb{Z}[i] \setminus \{0\}} \omega^{-4}$. Rappelons que le réseau $\Gamma = \sqrt[4]{15s}\mathbb{Z}[i]$ nous donne la courbe E donnée sous forme de Weierstrass par l'équation $y^2 = 4x^3 - 4x$ par théorème 6.3.

L'ensemble des points de n-torsion de $\mathbb{C}/\Gamma$ est noté $\mathbb{C}/\Gamma[n] = \{\frac{k_1 w_1 + k_2 + w_2}{n} | 0 \leq k_1, k_2 \leq n-1\}$.

Par la proposition 7.1.1 l'ensemble des points de n-torsion de E noté

$$E[n] = \{[\wp_\Gamma(P) : \wp'_\Gamma(P) : 1] | P \in \mathbb{C}/\Gamma[n]\}.$$

Comme $K_n = \mathbb{Q}(i)(E[n])$, par le théorème 9.1 un élément de $Gal(K_n/\mathbb{Q}(i))$ est complètement déterminé par son action sur $E[n]$ et donc sur $\mathbb{C}/\Gamma[n]$ qui a une structure explicite.

Conclusion :

On voit que $\wp_\Gamma$ et $\wp'_\Gamma$ sont les fonction méromorphes cherchées dans l'introduction, et les points où on les évalue sont les points appartenant à $\mathbb{C}/\Gamma[n]$. Pour décrire $Gal(K_n/\mathbb{Q}(i))$ il suffit de décrire son action sur $\mathbb{C}/\Gamma[n]$.

Références

[1] Silvermann, Joseph H. *The Aritmetic of Elliptic Curves*, **Springer Verlag 1986**

[2] Silvermann, Joseph H. and Tate John *Rational Points on Elliptic Curves*, **Springer Verlag 1992**