COURBES PROJECTIVES ET LE THÉORÈME DE HASSE

TIANYANG WANG

Table des matières

Remerciements 2
1. Courbes Projectives Lisses Irréductibles 3
2. Diviseur et ramification 10
3. Courbes elliptiques 15
4. Points rationnels sur les courbes elliptiques 21

Bibliographie 30
Références 30

Résumé. Ce mémoire aborde le sujet de compter le nombre de points rationnels sur une courbe elliptique. La première partie donne succinctement des préliminaires de variété algébrique où on a montré l'anti-équivalence entre la catégorie de courbes projectives lisses et la catégorie d'extensions de corps de type fini de degré de transcendance 1. Dans la deuxième partie, on étudie le phénomène de ramification et son relation avec le degré du morphisme et les genres des courbes à savoir le formule de Hurwitz, ce qui nous permet de transformer le nombre de points rationnels en le degré du morphisme. Ensuite on énonce le théorème de Riemann-Roch qui nous donne l'information de fonctions rationnelles sur une courbe elliptique quelconque. Cette information nous aide à écrire une courbe elliptique sous la forme d'une équation de Weierstrass. Après, en étudiant isogénie duale, on constate que le fonction degré est une forme quadratique, ce qui nous permet d'utiliser l'inégalité de Cauchy-Schwartz pour achever l'estimation de nombre de points rationnels. Finalement, on introduit les outils accouplement de Weil de module de Tate pour réinterpréter ce problème avec la fonction zêta.

Date: 29 mai 2024.

Remerciements

Je remercie M. Cyril Demarche pour m'encadrer et m'offrir un sujet intéressant qui m'a fait comprendre les phénomènes de géométrie algébrique plus concrètement. Il a répondu à mes questions de manière patiente et détaillée, ce qui m'a aidé à résoudre de nombreuses confusions. Je remercie également M. Jean-François Dat pour ses notes de style fluide sur variétés algébriques et courbes elliptiques.

Notion. Dans les chapitres 1 et 2, k est toujours supposé d'être algébriquement clos tandis que dans les chapitres 3 et 4, il désigne un corps parfais.

1. Courbes Projectives Lisses Irréductibles

Définition 1.1. *(Faisceau de fonctions, espace k-annelé) Soit X un espace topologique.*

Un faisceau de fonctions $\mathcal{A}$ sur X à valeur dans k est la donnée, pour chaque ouvert $U \subset X$, d'une sous-k-algèbre $\mathcal{A}(U) \subset k^U$, de sorte que pour tout recouvrement ouvert $U = \bigcup_{i\in I} U_i$ et toute fonction $f \in k^U$, on a

$$f \in \mathcal{A}(U) \Leftrightarrow \forall i \in I, f|_{U_i} \in \mathcal{A}(U_i).$$

Le couple est appelé un espace k-annelé. Un morphisme d'espace k-annelé entre $(X,\mathcal{O}_X)$ et $(Y,\mathcal{O}_Y)$ est une application continue $\varphi : X \to Y$ telle que pour tout ouvert U de Y, et toute fonction $f \in \mathcal{O}_Y(U)$, la fonction composée $f \circ \varphi : \varphi^{-1}(U) \to k$ appartient à $\mathcal{O}_X(\varphi^{-1}(U))$. On obtient ainsi un morphisme de k-algèbre $\varphi_U^* : \mathcal{O}_Y(U) \to \mathcal{O}_X(\varphi^{-1}(U))$ pour tout ouvert U de Y. On en déduit un morphisme entre germes de fonctions : $\varphi_x^* : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$.

Définition 1.2. *(Variété algébrique affine)*

Soit k un corps. Rappelons que un sous-ensemble algébrique de k^n est un sous-ensemble de k^n sous la forme

$$V(S) := \{(x_1, \cdots, x_n) \in k^n : \forall f \in S, f(x_1, \cdots, x_n) = 0\}$$

et que sa topologie de Zariski est la topologie où les fermés sont les sous-ensembles algébriques.

On va définir une faisceau $\mathcal{O}_V$ de fonction sur un sous-ensemble algébrique quelconque. Posons d'abord

$$\mathcal{O}(V) := \{f \in k^V : \exists P \in k[T_1, \cdots, T_n], \text{tel que } f = P|_V\}.$$

Pour $f \in k^U$, disons f est régulière en P si $\exists$ son voisinage ouvert U', $\exists g,h \in \mathcal{O}(V)$, tels que $h(x) \neq 0$ et $f|_{U'} = \frac{g|_{U'}}{h|_{U'}}$. Pour tout ouvert U de V, posons

$$\mathcal{O}_V(U) := \{f \in k^U : f \text{ est régulière en tout point de } U\}.$$

On peut vérifier que cela satisfait l'hypothèse de faisceau.

Un morphisme de variété algébrique est un morphisme d'espaces k-annelés.

Lemme 1.3. *Soient $V \subset k^n$ et $W \subset k^m$ deux sous-ensemble algébriques. Notons $App.Pol(V,W)$ l'ensemble de fonctions qui sont les restriction à V d'une application polynomiale dans tous les n coordonnées. On a deux bijections*

$$App.Pol(V,W) \xrightarrow{\sim} Hom_{k-alg}(\mathcal{O}(W),\mathcal{O}(V)) \xrightarrow{\sim} Hom_{esp.k-ann.}((V,\mathcal{O}_V),(W,\mathcal{O}_W)).$$

Démonstration. Cf [1, Prop. 1.5.2] et [1, Lemme 1.7.1]. □

Définition 1.4. *(Variété algébrique) Une variété algébrique (sur k) est un espace k-annelé $(X,\mathcal{O}_X)$ qui admet un recouvrement ouvert fini $X = \bigcup_{i=1}^n U_i$ tel que $(U_i,\mathcal{O}_X|_{U_i})$ soit une variété algébrique affine (sur k). Un morphisme de variété algébrique est un morphisme d'espaces k-annelés.*

Définition 1.5. *(L'espace projectif) Notons $\mathbb{P}^n(k)$ le quotient $(k^{n+1}\backslash\{0\})/k^\times$. La classe d'un point $\tilde{P} = (x_0,\cdots,x_n) \in \mathbb{A}^{n+1}$ se note $P := [x_0 : \cdots : x_n]$ dans $\mathbb{P}^n(k)$. Observons qu'il y a un recouvrement*

$$\mathbb{P}^n(k) = \bigcup_{i=0}^n U_i, \text{ où } U_i := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k) : x_i \neq 0\}$$

tel que pour tout $i = 0,\cdots,n$ on a une bijection

$$\psi_i : U_i \xrightarrow{\sim} k^n, [x_0 : \cdots : x_n] \mapsto (\frac{x_0}{x_i},\cdots,\frac{x_n}{x_i}) \in k^n.$$

On peut alors transporter par ψ_i^{-1} la topologie et le faisceau de fonctions de l'espace affine $\mathbb{A}^n$ et faire ainsi de $\mathbb{P}^n(k)$ une variété algébrique. (cf [1, Lemme. 1.7.10]*).*

Définition 1.6. *(Variété projective) Une variété projective est une sous-variété fermée d'un espace projectif. On peut l'écrire sous la forme*

$$V(S) := \{[x_0,\cdots,x_n] \in \mathbb{P}^n : f_i([x_0,\cdots,x_n]) = 0 (\forall f_i)\}$$

où les f_i sont des polynômes homogènes dans $k[T_0,\cdots,T_n]$.

Définition 1.7. *(Fonction rationnelle)*

(i) Soit V une variété algébrique. Posons

$$k(V) := \{(U,f) : U \subset V \text{ ouvert dense et } f \in \mathcal{O}_V(U)\}/\sim$$

où $\sim$ désigne la relation d'équivalence définie par $(U,f) \sim (U',f')$ si et seulement si il existe $U'' \subset U \cap U'$ ouvert dense tel que $f|_{U''} = f'|_{U''}$. Notons que $k(V)$ est un k-algèbre, on l'appelle le corps de fonction de V, les éléments dans $k(V)$ sont appelés fonctions rationnelles sur V.

(ii) Soient V, W deux variétés irréductibles, une application rationnelle est une classe d'équivalence de couples (U,φ) formés d'un ouvert non vide U de V et d'un morphisme $\varphi : U \to W$, où $(U,\varphi) \sim (U',\varphi')$ si et seulement si il existe $U'' \subset U \cap U'$ ouvert dense tel que $\varphi|_{U''} = \varphi'|_{U''}$. En outre, une telle application rationnelle φ induit un morphisme de k-algèbres $\varphi^* : k(W) \hookrightarrow k(V)$.

Remarque 1.8. *Soit V une variété projective irréductible sur k avec anneau gradué $S(V)$, alors son corps de fraction*

$$k(V) = Frac(S(V))_0$$
$$:= \{\frac{\bar{f}}{\bar{g}} : f,g \in k[T_0,\cdots,T_n], f \text{ et } g \text{ sont homogeneous de même degré, et } g \notin I(V)\}.$$

Lemme 1.9. *(Classe birationnelle d'une variété irréductible est déterminée par son corps de fonction) En utilisant les notations au-dessus, on a une bijection*

$$App.rat.dom.(V,W) \simeq Hom_{k-alg}(k(W),k(V)).$$

En outre, on a une anti-équivalence entre les deux catégories :

$$\left[\begin{array}{c} \text{Objets : extensions de } k \text{ de type fini} \\ \text{Morphismes : extensions de corps} \end{array}\right] \leftrightsquigarrow \left[\begin{array}{c} \text{Objets : variétés irréductibles} \\ \text{Morphismes : applications rationnelles} \end{array}\right]$$

Démonstration. Prenons U_2 un ouvert affine de W, et U_1 un ouvert affine contenu dans $f^{-1}(U_2) \subset V$. On remplace V avec U_1 et W avec U_2 puisque les deux variétés sont irréductibles et alors les deux ensembles de morphismes ne changent pas (en particulier, les corps de fonctions ne changent pas par la densité de U_1 et U_2 dans les variétés irréductibles). Soit $\psi : k(U_2) \to k(U_1)$ un morphisme de k-algèbre. La type-finitude du k-algèbre $\mathcal{O}(U_2)$ nous assure l'existence de $h \in \mathcal{O}(U_1)$ tel que

$$\psi(\mathcal{O}(U_2)) \subset \mathcal{O}(U_1)[h^{-1}] \subset k(U_1).$$

On en déduit par 1.3 un morphisme de variétés $\varphi : (U_1)_h \to U_2$ où $(U_1)_h$ est l'ouvert principal de U_1 défini par $h \neq 0$. La classe d'équivalence de $((U_1)_h,\varphi)$ ne dépend pas du choix de h et définit donc une application rationnelle (unique) $\phi : V \to W$ telle que $\phi^* = \psi$. □

Lemme 1.10. *Soit C un ouvert de C_K et $v \in C$. Tout morphisme d'espace k-annelé $\varphi : C\backslash\{v\} \to Y$ vers une variété projective Y admet un unique prolongement à C.*

Démonstration. Quitte à composer avec une immersion fermée $Y \subset \mathbb{P}^n$, on peut supposer que $\varphi(C\backslash\{v\})$ n'est pas contenu dans $\cup_{i=0}^n U_i$. Notons U le complémentaire qui est affine et $\mathcal{O}_{\mathbb{P}^n}(U)$ contient tous les fonctions $X_i X_j^{-1}$ pour $0 \leq i,j \leq n$. Soient $f_{ij} \in \mathcal{O}_C(\varphi^{-1}(U)) \subset K$ obtenues par composition avec φ. Supposons k tel que $v(f_{k0}) = min_{0\leq i\leq n}\{v(f_{i0})\}$. Alors pour tout i, on a $v(f_{ik}) = v(f_{i0}f_{k0}^{-1}) \geq 0$ donc $f_{ik} \in \mathcal{O}_C(\varphi^{-1}(U) \cup \{v\})$. Il y a donc unique morphisme donné par $v' \mapsto [f_{0k}(v') : \cdots : f_{nk}(v')]$ (remarquons que $f_{kk} = 1$) qui est bien défini et régulier sur v. Sa restriction en $\varphi^{-1}(U)$ coïncide avec φ, par la densité de $\varphi^{-1}(U)$ dans $C\backslash\{v\}$, ils s'accordent sur $C\backslash\{v\}$. □

Corollaire 1.11. *(Complétude de variétés projectives) Soit $f : C \dashrightarrow Y$ une application rationnelle entre une courbe lisse quelconque et une variété projective. Alors f est un morphisme.*[1]

Définition 1.12. *(Courbe) Une courbe est une variété de dimension* 1.

Théorème 1.13. *On a une anti-équivalence entre les deux catégories :*

$$\left[\begin{array}{c}\textit{Objets : extensions de } k \textit{ de type fini}\\ \textit{et de degré de transcendance 1}\\ \textit{Morphismes : extensions de corps}\end{array}\right] \leftrightsquigarrow \left[\begin{array}{c}\textit{Objets : courbes projectives lisses}\\ \textit{Morphismes : morphismes dominants}\end{array}\right]$$

Démonstration. « $\rightsquigarrow$ ». Juste prenons le corps de fonctions.

L'autre coté : Soit K/k une extension de type finie et de degré de transcendance 1. Supposons

$$C_K := \{\textit{valuation de } K/k\ v : K^\times \twoheadrightarrow \mathbb{Z}\}$$

muni de la topologie cofinie (complémentaire d'un ensemble fini). (Rappelons que une valuation(discrète) de K/k est une valuation discrète $v : K^\times \twoheadrightarrow \mathbb{Z}$ telle que $\forall x \in k^\times$, $v(x) = 0$.) Pour $v \in C_K$, notons $\mathcal{O}_v$ son anneau de valuation, $\mathfrak{m}_v$ l'idéal maximal et $k_v = \mathcal{O}_v/\mathfrak{m}_v$ le corps résiduel, et appelons $t \in \mathcal{O}_v$ une uniformisante de $\mathcal{O}_v$ si elle est un générateur de $\mathfrak{m}_v$. On va achever la preuve par quelques lemmes. On va démontrer d'abord que le foncteur est essentiellement surjectif. Pour cela, on va donner une structure d'espace k-annelé sur C_K.

Lemme 1.14. *C_K est infini. En plus :*
(i) Pour tout valuation $v \in C_K$, on a $k_v = k$.
(ii) Pour tout $f \in K^\times$, l'ensemble de zéros de f, i.e. $\{v \in C_K : v(f) > 0\}$ est fini.

Démonstration. (i) Puisque v est non-trivial, il existe $f \in K$ tel que $v(f) > 0$. Puisque v est nulle sur k, l'élément f est transcendant sur k et alors engendre une k-algèbre isomorphisme à $k[T]$. Soit A la clôture intégrale de $k[f]$ dans K. Alors il est de dimension 1 et de corps de fonctions K. Puisque l'anneau de valuation $\mathcal{O}_v$ est intégralement clos, $k[f] \subset \mathcal{O}_v$ implique que $A \subset \mathcal{O}_v$. En plus, l'idéal $\mathfrak{m} := \{a \in A : v(a) > 0\}$ est le tiré en arrière de $\mathfrak{m}_v \subset \mathcal{O}_v$ dans A, est alors premier. Puisque A est de dimension 1 et $\mathfrak{m} \neq 0$, l'idéal est maximal. On a des plongements de corps

$$k \hookrightarrow A/\mathfrak{m} \xrightarrow{\sim} A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} \hookrightarrow \mathcal{O}_v/\mathfrak{m}_v = k_v$$

1. Dans cet article, on appelle cette propriété « complétude » de variétés projectives. Notons que il y a une autre définition de la complétude, et elles sont équivalentes cf. [1, Définition 3.3.1 et Théorème 3.3.2].

Observons que $A_{\mathfrak{m}}$ est intégralement clos, il est alors un anneau de valuation discret contenu dans $\mathcal{O}_v$ et dans K, on a donc $A_{\mathfrak{m}} = \mathcal{O}_v$. D'où la bijectivité du deuxième plongement. Puisque f est transcendant sur k, $K/k(f)$ est une extension finie, par [1, 2.6.3], A est de type fini. Puisque k est algébriquement clos, le Nullstellensatz nous assure la bijectivité du premier injection.

(ii) Choisissons $f \in K\backslash k$ et donc transcendant sur k (qui est algébriquement clos). D'après la preuve de (i), fixons f et A. Pour tout v' tel que $v'(f) > 0$, on a de même $k[f] \subset \mathcal{O}_{v'}$ alors $A \subset \mathcal{O}_{v'}$. Le tiré en arrière nous donne toujours un idéal maximal $\mathfrak{m} \in Spm(A)$ tel que $f \in \mathfrak{m}$. Autrement dire, on a une bijection

$$\{v \in C_K : v(f) > 0\} \xrightarrow{\sim} \{\mathfrak{m} \in Spm(A) : f \in \mathfrak{m}\}.$$

L'ensemble à droite est fini. En effet, $A/(f)$ est de dimension 0 et de type fini sur k, il est donc un anneau artinien qui possède un nombre fini d'idéaux maximaux.

Puisque $Spm(A)$ est un ensemble infini, C_K l'est aussi. □

Pour un ouvert U de C_K, posons

$$\mathcal{O}_K(U) := \{f \in K | \forall v \in U, v(f) \geq 0\} = \bigcap_{v \in U} \mathcal{O}_v.$$

D'après le (i) du lemme précédent, on a une application

$$\mathcal{O}_K(U) \to k^U, f \mapsto (v \mapsto \bar{f} \in k_v = k).$$

Cette application est injective par (ii). En effet, si les images de f_1 et f_2 sont égales dans k_U, $f_1 - f_2$ s'annule sur U qui est un ensemble infini, et par (ii), $f_1 - f_2 = 0$. Ainsi $\mathcal{O}_K(U)$ se voit comme un sous-k-algèbre de k_U. D'où la structure de k-annelé.
Par [1, Théorème 3.4], $(C_K, \mathcal{O}_K)$ est isomorphe à une courbe projective lisse. D'où la surjectivité essentielle.

Lemme 1.15. *(Pleinement fidèle) Soit une extension $K' \subset K$ entre extensions de k de type fini de degré de transcendance 1. Alors il correspond (par le foncteur) à un unique morphisme dominant entre C_K et $C_{K'}$.*

Démonstration. Par 1.9, on a une unique application rationnelle dominante $f : C_K \dashrightarrow C_{K'}$ correspondu. Par la complétude de $C_{K'}$ et la lissité de C_K, f se prolonge en un unique morphisme sur C_K. (Rappelons que un ouvert de C_K est un ensemble cofini.) □

On a une équivalence des catégories. □

Remarque 1.16. *Par complétude, un morphisme $\varphi : C \to C'$ entre deux courbes projectives lisses est non constant si et seulement si il est dominant si et seulement si il est surjectif. En effet, par la complétude de C, $im(\varphi)$ est fermée, alors soit fini soit C'. Si $im(\varphi)$ est fini, par la connexité de C, elle constitue d'un point. Alors φ est constant.*

Définition 1.17. *(Degré) Soit $\varphi : C \to C'$ un morphisme dominant. On définit son degré $deg(\varphi) := [k(C) : k(C')]$, et son degré séparable $deg_s(\varphi) := [k(C)_{sep} : k(C')] = [k(C) : k(C')]_s$.*

Proposition 1.18. *Soit K un corps de caractéristique $p > 0$, $q = p^r$, C/K une courbe, et $\phi_q : C \to C^{(q)}$ l'endomorphisme de Frobenius. Alors on a*

(i) $\phi_q^* k(C^{(q)}) = k(C)^q$ et ϕ_q est purement inséparable;

(ii) $deg\, \phi_q = q$.

Démonstration. (i) Notons que des éléments dans $\phi_q^* K(C^{(q)})$ peuvent s'écrire sous la forme

$$\phi_q(\frac{f}{g}) = \frac{f(T_0^q, \cdots, T_n^q)}{g(T_0^q, \cdots, T_n^q)}$$

où $g \notin I(C^{(q)})$. Alors que des éléments dans $K(C)^q$ peuvent s'écrire sous la forme

$$\frac{f(T_0, \cdots, T_n)^q}{g(T_0, \cdots, T_n)^q} = \frac{f^{(q)}(T_0^q, \cdots, T_n^q)}{g^{(q)}(T_0^q, \cdots, T_n^q)}$$

où $g \notin I(V)$. Puisque k est parfait, l'endomorphisme $\phi_q : k \to k$ est surjectif, ce qui implique que les deux ensemble coïncide. L'inséparabilité se résulte de la définition.

(ii) Cf [2].

□

Corollaire 1.19. *Tout morphisme $\psi : C \to C'$ entre deux courbes sur un corps de caractéristique $p > 0$ se factorise en*

$$C \overset{\phi_q}{\to} C^{(q)} \overset{\psi_s}{\to} C'$$

où $q = deg_i(\psi)$, ϕ_q est l'endomorphisme de Frobenius et ψ_s est séparable.

Démonstration. On identifions tous les corps comme sous-corps de $k(C)$. Choisissons la clôture séparable $k(C')_{sep}$ du $k(C')$ dans $k(C)$, alors

$$[k(C) : k(C')_{sep}] = [k(C) : k(C')]_i = deg_i(\varphi) = q.$$

Par la proposition précédente, $[k(C) : k(C^{(q)})]_i = q$. Donc $k(C^{(q)})/k(C')$ est séparable, et $k(C^{(q)}) \subset k(C')_{sep}$. En comparant les degrés, on a $k(C^{(q)}) = k(C')_{sep}$ et donc $k(C_{(q)})$ contient $k(C')$. Voyons les courbes correspondues des extensions $k(C)/k(C^{(q)})/k(C')$, on a le résultat désiré. □

2. Diviseur et ramification

Définition 2.1. *(Diviseur) Soit C une courbe lisse. Notons $Div(C)$ le groupe abélien libre de base C. Si $D = \sum_P a_P[P]$ est un diviseur, son degré $deg(D)$ est l'entier $\sum_P a_P$. Soit D,D' deux diviseur, on dit que $D \leq D'$ si pour tout point $P \in C$, le coefficient de D est inférieur ou égale à celui de D'. On dit que D est effectif si $D \geq 0$. En outre, 1.14 (ii) permet de définir une application*

$$div : k(C)^\times \to Div(C), f \mapsto \sum_P v_P(f)[P].$$

Notons l'entier $\ell(D)$ la dimension du k-espace vectoriel

$$\mathcal{L}(D) := \{f \in k(C) : div(f) + D \geq 0\}.$$

Observons que pour le zéro diviseur, $\mathcal{L}_0 = k$ lorsque C est projective.

Lemme 2.2. *Soit $\varphi : C \to C'$ un morphisme entre deux courbes projectives lisses, on a pour tout $Q \in C'$,*

$$deg(\varphi) = \sum_{P \in \varphi^{-1}(Q)} e_P(\varphi)$$

Démonstration. □

Corollaire 2.3. *Soit $\varphi : C \to C'$ un morphisme entre deux courbes projectives lisses, on a pour tout $D \in Div(C')$,*

$$deg(\varphi^*(D)) = deg(\varphi)deg(D)$$

Corollaire 2.4. *Soit C une courbe projective. Si $\exists P \in C$ tel que $\ell_{[P]} = 2$, alors $C \simeq \mathbb{P}^1$.*

Démonstration. Choisissons $f \in \mathcal{L}_{[P]} - \mathcal{L}_0$ et $\varphi_f : C \to \mathbb{P}^1$ le morphisme associé. On a $\varphi_f^*([\infty]) = [P]$, alors par 2.2, $deg(f) = 1$. Il s'ensuit que $k(C) = k(\mathbb{P}^1)$, utilisons 1.13.

□

Lemme 2.5. *Soit B un k-algèbre, $\mathfrak{m} \subset B$ un idéal maximal avec corps de résidu k. Notons $\Omega_{B/k}$ le module différentiel (cf par exemple* [1, 2.3.2]*). Alors on a une isomorphism entre les deux k-espaces vectoriels*

$$\mathfrak{m}/\mathfrak{m}^2 \simeq \Omega_{B/k} \otimes_B k.$$

Notons que la gauche est facile à calculer et avec une signification géométrique : espace cotangent (cf la définition dans [1, 2.4]).

Proposition 2.6. *(i) Soit K un corps de fonctions de courbe sur k, v un point de C_K et t une uniformisante en v. Alors $\Omega_{\mathcal{O}_v/k} \simeq \mathcal{O}_v$ comme $\mathcal{O}_v$-modules et dt est un générateur.*

(ii) Soit $K' \subset K$ est une extension fini et t' est une uniformisante de $v' = v|_{K'}$, alors on a

$$\Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \simeq (\mathcal{O}_v/\frac{dt'}{dt}\mathcal{O}_v)dt.$$

En plus,

$$length(\Omega_{\mathcal{O}_v/\mathcal{O}_{v'}}) = e_v - 1, \text{ si la ramification est modérée}$$
$$length(\Omega_{\mathcal{O}_v/\mathcal{O}_{v'}}) > e_v - 1, \text{ si la ramification est sauvage.}$$

(Rappelons que une ramification est dite modérée si $car(k)|e_P$, et sinon, elle est dite sauvage.)

Démonstration. (i) Utilisons 2.5 en prenant $B = \mathcal{O}_v$, $\mathfrak{m} = \mathfrak{m}_v$ et $k = k$, on a

$$\mathfrak{m}_v/\mathfrak{m}_v^2 \simeq \Omega_{\mathcal{O}_v/k} \otimes_{\mathcal{O}_v} k.$$

Puisque $\mathcal{O}_v$ est un k-module, on a

$$\mathfrak{m}_v/\mathfrak{m}_v^2 \otimes_k \mathcal{O}_v \simeq \Omega_{\mathcal{O}_v/k} \otimes_{\mathcal{O}_v} k \otimes_k \mathcal{O}_v \simeq \Omega_{\mathcal{O}_v/k}.$$

Il suffit d'observer que $\mathfrak{m}_v/\mathfrak{m}_v^2$ est un k-espace vectoriel engendré par l'image de t.

(ii) La suite exacte [3, 2.3.2 (v)] nous donne ici

$$\Omega_{\mathcal{O}_{v'}/k} \otimes_{\mathcal{O}_{v'}} \mathcal{O}_v \to \Omega_{\mathcal{O}_v/k} \to \Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \to 0.$$

Par (i), elle peut s'écrire

$$\mathcal{O}_v \cdot dt' \to \mathcal{O}_v \cdot dt \to \Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \to 0.$$

D'où l'isomorphisme. Pour le *length*, c'est pas difficile à vérifier que

$$length(\mathcal{O}_v/\frac{dt'}{dt}\mathcal{O}_v) = v(\frac{dt'}{dt}).$$

Notons $t' = ut^{e_v}$, calculons que

$$v(\frac{dt'}{dt}) = v(t^{e_v}\frac{du}{dt} + e_v t^{e_v - 1}).$$

Alors si la ramification est modéré, l'ordre est égale à $v(e_v t^{e_v-1}) = e_v - 1$; sinon, l'ordre est $v(t^{e_v}\frac{du}{dt}) \geq e_v$. □

Définition 2.7. *(Diviseur de ramification) Soit $\varphi : C \to C'$ un morphisme dominant séparable de courbes lisses. On définit le diviseur de ramification de φ :*

$$R_\varphi := \sum_{P \in C} length(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})[P].$$

(D'après le corollaire suivant, le somme est finie, alors le diviseur est effectivement bien-défini.)

Corollaire 2.8. *Sous les hypothèses de la définition, le lieu de ramification est fini.*

Démonstration. Identifions $k(C')$ à un sous-corps de $k(C)$ via φ^*. Par 2.6 (ii), $e_P(\varphi) > 1 \Leftrightarrow \Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}} \neq 0$. Soit t' une uniformisante en $\varphi(P)$, A' la normalisation de $k[t']$ dans $k(C')$ et A sa normalisation dans $k(C)$. Par la commutativité des différentielles avec la localisation, on a $\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}} = \mathcal{O}_P \otimes_A \Omega_{A/A'}$, donc P est dans le support de $\Omega_{A/A'}$. Puisque $\Omega_{A/A'}$ est un A-module de type fini, donc $supp(\Omega_{A/A'}) = V(Ann(\Omega_{A/A'}))$ est fermé □

Proposition 2.9. *(Différentielle méromorphe sur une courbe lisse) Soit C une courbe lisse. On note $\Omega_C := \Omega_{k(C)/k}$, appelé espace des différentielles méromorphes sur C.*

(i) Ω_C est un $k(C)$-espace vectoriel de dimension 1.

(ii) Soit $\varphi : C \to C'$ un morphisme non constant de courbes elliptiques. L'extension $\varphi^* : k(C') \to k(C)$ induit une application $k(C')$-linéaire

$$\Omega_{C'} \to \Omega_C, \sum f_i dx_i \mapsto \sum (\varphi^* f_i) d(\varphi^* x_i).$$

Cette application est non-nulle (ssi injective) si et seulement si φ est séparable.

(iii) Pour tout point $P \in C$ et toute différentielle $\omega \in \Omega_C$, l'entier

$$v_P(\omega) := v_P(\omega/dt)$$

ne dépend pas du choix de l'uniformisante $t \in k(C)$ en P.

(iv) Pour tout différentielle $\omega \in \Omega_C$, i'ensemble $\{P \in C : v_P(\omega) \neq 0\}$ est fini. On peut donc définir

$$div(\omega) := \sum_P v_P(\omega)[P] \in Div(C).$$

Démonstration. Pour (i) and (ii), il suffit d'utiliser (i) de la proposition précédente et un résultat pour différentielles [3, 2.3.2 (viii)].

Pour (iii), soit t' une autre uniformisante en P. Le (ii) de la proposition précédente nous dit que $dt' \in \mathcal{O}_P dt$ et $dt \in \mathcal{O}_P dt'$. Donc on a $dt \in \mathcal{O}_P^\times dt'$.

(iv) Puisque $v_P(f\omega) = v_P(f) + v_P(\omega)$, on peut supposer $\omega = dt$ où t est une uniformisante en un point Q. Soit $\varphi_t : C \to \mathbb{P}^1$ le morphisme défini par t (l'extension correspondue est $k(t) \subset k(C)$) qui induit une application

$$\varphi_t^* : \Omega_{\mathbb{P}^1} \to \Omega_C, dt \mapsto dt$$

non-nulle. Il s'ensuit que φ_t est séparable et $\Omega_{k(C)/k(t)} = 0$ par la suite exacte [3, 2.3.2 (v)].

Pour tout point $P \in \varphi_t^{-1}(\mathbb{A}^1)$, écrivons $\varphi_t(P) = [t(P) : 1]$ avec $t(P) \in k$. La fonction $t - t(P)$ est alors une uniformisante au lieu où φ_t est non ramifié. En un tel point, on a $v_P(dt) = v_P(d(t - t(P))) = 0$. Mais par le corollaire précédent, le lieu de ramification est fini, ce qui achève la preuve. □

Théorème 2.10. *(Formule de Hurwitz) Soit $\varphi : C \to C'$ un morphisme séparable entre deux courbes (lisse). Alors on a l'inégalité*

$$deg(K_C) = deg(\varphi) deg(K_{C'}) + deg(R_\varphi).$$

On a de plus $deg(R_\varphi) \geq \sum_{P \in C}(e_P(\varphi) - 1)$, avec égalité si les indices de ramification sont partout premiers à $car(k)$.

Démonstration. Soit $\omega' \in \Omega_{C'}$. Il suffit de montrer que

$$div(\varphi^*\omega') = \varphi^*(div(\omega')) + R_\varphi,$$

autrement dire,

$$v_P(\varphi^*(\omega')) = e_P(\varphi) v_{\varphi(P)}(\omega') + length(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$$

pour tout $P \in C$. Soit $t' \in k(C')$ une uniformisante en $\varphi(P)$ et $t \in k(C)$ une uniformisante en P. Notons $e := e_P(\varphi)$, il existe $u \in \mathcal{O}_P^\times$ telle que $t' = u \cdot t^e$. Écrivons $\omega' = f dt'$, on a par définition $v_{\varphi(P)}(\omega') = v_{\varphi(P)}(f)$. Calculons que

$$\varphi^*\omega' = f d(ut^e) = (et^{e-1} + t^e \frac{du}{dt}) f dt,$$

donc

$$v_P(\varphi^*\omega') = v_P((et^{e-1} + t^e \frac{du}{dt}) f) = v_P(f) + length(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$$

d'après la preuve de 2.6 (ii). L'inégalité provient aussi de la preuve de 2.6 (ii). □

On définit le genre d'une courbe complète C l'entier $g := \ell(K_C)$.[2] Par le Riemann-Roch au-dessous, on a $2g - 2 = deg(K_C)$

Corollaire 2.11. *Pour tout morphisme non-constant entre deux courbes $C \to C'$, on a $g(C) \geq g(C')$.*

Démonstration. Au cas où φ est séparable, raisonnons par l'absurde. Supposons $g(C) < g(C')$, alors $g(C') \geq 1$. Appliquons la formule de Hurwitz, on a

$$2g(C') - 2 > 2g(C) - 2 \geq deg(\varphi)(2g(C') - 2).$$

Alors $deg(\varphi) < 1$, ϕ est donc constant.

Au cas où φ est purement inséparable,

En général, utilisons la factorisation d'après 1.19 :

$$\varphi : C \overset{\phi_q}{\to} C^{(q)} \overset{\varphi_s}{\to} C'$$

où φ_s est séparable et l'endomorphisme de Frobenius ϕ_q est purement inséparable, ce qui achève la preuve. □

Théorème 2.12. *(Théorème de Riemann-Roch) Soit C une courbe (projective lisse). Alors pour tout $D \in Div(C)$, on a*

$$\ell(D) - \ell(K_C - D) = deg(D) + 1 - g(C).$$

2. Au cas de variétés complexes, cette définition de genre coïncide avec celle par triangulation dans la théorie de surfaces de Riemann

3. Courbes elliptiques

Définition 3.1. *(Courbe elliptique) Une courbe elliptique sur k est un pair (E,O) où E est une courbe projective lisse E de genre 1 définie sur k et O un point $k-$rationnel.*

Remarque 3.2. *Observons que $deg(K_C) = 0$ pour une courbe elliptique. En utilisant Riemann-Roch, on va obtenir la relation entre le nombre $\ell(D)$ d'un diviseur et son degré $deg(D)$ comme le formulaire au-dessous.*

$deg(D)$:	$\cdots$	-2	-1	0	1	2	3	$\cdots$
$\ell(D)$:	$\cdots$	0	0	0 ou 1	1	2	3	$\cdots$

C'est-à-dire, $\ell(D)$ est décidé par $deg(D)$ sauf si $deg(D) = 0$. Mais quand $deg(D) = 0$, $\ell(D) = 1$ si D est principal, et $\ell(D) = 0$ sinon.

Proposition 3.3. *Soit (E,O) une courbe elliptique, alors l'application d'Abel-Jacobi*

$$E \to Pic^0(E), P \mapsto \overline{[P] - [O]}$$

est une bijection G_k-équivariante.

Démonstration. Application est G_k-invariante puisque O est $k-$rationnel, alors fixé par G_k.

Injectivité : Raisonnons par l'absurde. Supposons deux points distincts $P_1, P_2 \in E$ tels que $\overline{[P_1] - [P_2]} = 0$, i.e. $\exists f \in k(E)$ tel que $div(f) = [P_1] - [P_2]$. Observons que $f \in \mathcal{L}_{[Q]} - \mathcal{L}_0$, on a alors $\ell_{[Q]} \geq 2$. Par **??**, $E \simeq \mathbb{P}^1$, ce qui est contradictoire au fait que $g(E) = 1$ mais $g(\mathbb{P}^1) = 0$.

Surjectivité : Soit D un diviseur de degré 0. Par le théorème de Riemann-Roch, $\ell_{[O]+D} = 1$. Supposons $f \in \mathcal{L}_{[O]+D}$ non nulle, on a $deg(div(f)+[O]+D) = 1$ et $div(f) + [O] + D \geq 0$. Cela implique que $div(f) + [O] + D = [P]$ pour quelque $[P] \in E$, autrement dire, $\overline{D} = \overline{[P] - [O]}$ dans $Pic^0(E)$. □

Définition 3.4. *(Loi de groupe) Puisque $Pic^0(E)$ est un groupe abélien, via la bijection d'Abel-Jacobi, E est donné une structure de groupe abélien compatible avec l'action de Galois, i.e. $P+Q$ est le seul point tel que $[P+Q] \sim [P]+[Q]-[O]$.*

Remarque 3.5. *Via l'application d'Abel-Jacobi, on constate que un diviseur de degré 0 est principal si et seulement si la somme des points par le loi de groupe est O.*

Théorème 3.6. *(Équation de Weierstrass) Soit (E,O) une courbe elliptique sur k. Il existe un plongement $\iota : E \hookrightarrow \mathbb{P}^2$ défini sur k dont l'image est la courbe définie par une équation de Weierstrass*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Démonstration. Puisque O est un point k-rationnel, le diviseur $3[O]$ est défini sur k. D'après le corollaire 3.2 du Riemann-Roch, on a $\ell(2[O]) = 2$, $\ell(3[O]) = 3$. On peut trouver $x \in \mathcal{L}(2[O])\backslash\mathcal{L}([O])$, et $y \in \mathcal{L}(3[O])\backslash\mathcal{L}(2[O])$. Alors $\{1,x,y\}$ forme une k-base de $\mathcal{L}(3[O])$ qui fournit un plongement $\iota : E \to \mathbb{P}^2$ par **??**. Afin de calculer une équation, remarquons que la famille de 7 fonctions $\{y^2,x^3,yx,x^2,y,x,1\}$ vit dans $\mathcal{L}(6[O])$ dont la dimension est 6. Il s'ensuit que la famille est k-linéairement liée. Par ailleurs, observons que les ordres de pôle en O de ces fonctions sont respectivement 6,6,5,4,3,2,0, les familles obtenue en retirant y^2 ou x^3 sont libres. Donc les deux termes apparaissent forcément dans l'équation. Après une multiplication raisonnable, on peut arranger l'équation sous la forme où les coefficients de y^2 et x^3 sont 1. Ainsi $\iota(E)$ est inclus dans une équation de Weierstrass C. Par 1.16, on a le résultat désiré. □

Remarque 3.7. *Pour comprendre la preuve plus concrètement, considérons la courbe elliptique sur $\mathbb{C}$ de la forme $\mathbb{C}/\Lambda$ avec $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ un réseau de $\mathbb{C}$. La fonction de Weierstrass*

$$p(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^*} [\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}]$$

est une fonction méromorphe sur $\mathbb{C}/\Lambda$ avec $div(p) = -2[0] + [z_1] + [z_2]$. On a $p'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z+\omega)^3}$ aussi méromorphe, avec $div(p') = -3[0] + [\frac{1}{2}] + [\frac{\tau}{2}] + [\frac{1+\tau}{2}]$ (cf [4, Chapitre 9, 1.2]*). Puisque*

$$\frac{p'^2}{(p - p(\frac{1}{2}))(p - p(\frac{\tau}{2}))(p - p(\frac{1+\tau}{2}))}$$

ne possède pas de pôle sur la surface de Riemann compact, on a une équation

$$p^2 = 4(p - p(\frac{1}{2}))(p - p(\frac{\tau}{2}))(p - p(\frac{1+\tau}{2})). \tag{1}$$

Dans cet exemple, p est la fonction x dans la preuve au-dessus, p′ est la fonction y, $[p : p' : 1]$ est le plongement dans $\mathbb{P}^2$, et l'équation 1 est l'équation de Weierstrass.

Lemme 3.8. *Soit $\varphi : E_1 \to E_2$ un morphisme de variété non constant entre deux courbes elliptiques. Alors si φ est non-constant, on a :*

(i) $deg_i(\varphi) = e_P(\varphi)$ ne dépend pas de P.

(ii) $deg_s(\varphi) = \#\varphi^{-1}(Q)$ pour tout $Q \in E_2$.

Démonstration. (i) Au cas où φ est séparable, la formule de Hurwitz nous assure que $deg(R_\varphi) = 0$. Mais le diviseur de ramification R_φ est effectif, il est donc nul i.e. $e_P = 0$ partout. En général, en utilisant 1.19, on peut factoriser $\varphi = \psi \circ \phi_q$ où $q = deg_i(\varphi)$. On a donc

$$e_P(\varphi) = e_P(\phi_q) = deg(\phi_q) = deg_i(\varphi).$$

(ii) Utilisons 2.2 et (i), on a

$$deg_s(\varphi)deg_i(\varphi) = deg(\varphi) = \#\varphi^{-1}(Q) \cdot deg_i(\varphi).$$

D'où l'égalité.

□

Corollaire 3.9. *Sous les hypothèses du lemme précédent, si φ est de plus séparable, alors il est non ramifié. En plus, $\#\ker\varphi = deg(\varphi)$.*

Lemme 3.10. *Soit $\varphi : E \to E'$ un morphisme de variétés non constant entre deux courbes elliptiques. Alors si $\varphi(O) = O'$, on a φ est un morphisme de groupes.*

Définition 3.11. *(Isogénie) Un morphisme de variété $\varphi : E \to E'$ entre courbes ellipiques satisfaisant $\varphi(O) = O'$ est appelé un morphisme de courbes elliptiques. Si il est de plus non constant, on l'appelle une isogénie. Remarquons que les morphismes forment un groupe abélien $Hom(E,E')$ via l'addition sur E', et les endomorphismes forment un anneau $End(E)$ où le produit est la composition.*

Exemple 3.12. *Pour un entier m, on définit une isogénie de la multiplication par m :*

$$[m] : E \to E, P \mapsto P + P + \cdots + P(m \text{ termes})$$

(si m est négatif, $[m]P := [-m](-P)$).

Mais il faut prouver que $[m]$ est non constant. Il suffit de le prouver pour tout m premier. Pour un m impair, supposons que $[m]$ est constant. Si on peut obtenir un point P d'ordre 2, on a $P = [m](P) = [m](O) = O$, un contradiction. On va chercher un point d'ordre 2 au cas où $car(k) \neq 2$. Puisque $\ell(2[O]) = 2$, on a un morphisme $f : E \to \mathbb{P}^1$ associé à $f \in \mathcal{L}(2[O])\backslash\bar{k}$ qui est donc de degré 2.

Alors, pour tout $\lambda \in \mathbb{C} \subset \mathbb{P}^1$, notons son fibré $f^{-1}(\lambda) = \{P_1, P_2\}$, on a $[P_1] + [P_2] - 2[O] = div(f - \lambda)$ un diviseur principal. Par le loi de groupe, $P_2 =$

$-P_1$. Donc $P_1 \in \mathbb{P}^1\backslash\{0\}$ est ramifié si et seulement si $P_1 = -P_1$, i.e. il est d'ordre 2. Observons que f est séparable, appliquons le formule de Hurwitz, on a $degR_\varphi = 4$. Puisque $car(k) \neq 2$, toute ramification de f est modérée. Donc f possède exactement 4 points ramifiés, autrement dire, 4 points d'ordre 2. Cela achève la preuve du cas m impair, et aussi implique le cas $m = 2$. Pour le cas $m = 2$, voyez [3, 3.3.2]. *En bref, on a :*

Proposition 3.13. *Soit E une courbe elliptique. On a une injection d'anneaux*

$$\mathbb{Z} \to End(E), m \mapsto [m].$$

Remarque 3.14. *Si on voit la courbe elliptique sur $\mathbb{C}$ comme $\mathbb{C}/\Lambda$, dans l'exemple précédent, on peut choisir la fonction p comme f. Ses lieux de ramification sont les zéros de p' et 0. Puisque p' est une fonction impair, ce sont les points tels que $P = -P$ i.e. les points d'ordre 2. Alors les quatre points sont 0, $\frac{1}{2}$, $\frac{\tau}{2}$, et $\frac{1+\tau}{2}$.*

Lemme 3.15. *Soit $\varphi : E_1 \to E_2$ une isogénie.*

(i) L'application

$$\ker\varphi \to Aut(k(E_1)/k(E_2)), Q \mapsto \tau_Q^*$$

est un isomorphisme, où τ_Q est l'application translation par Q, et τ_Q^* est l'isomorphisme induit sur les corps de fonctions.

(ii) Supposons de plus que φ est séparable, alors l'extension correspondue $k(E_1)/k(E_2)$ est Galoisinne.

Démonstration. (i) On peut vérifier que τ_Q est un isomorphisme de E_1. Puisque $\varphi(Q) = O$, on a $\varphi \circ \tau_Q = \varphi$. Ainsi $\tau_Q^* \circ \varphi^* = \varphi^*$, autrement dire, $k(E_2)$ est stable sous τ_Q. Pour deux point différents, voyons les images de O, les deux translations correspondues sont différentes. Alors elles induisent deux extensions différentes (par la fidélisation du foncteur dans 1.13). D'où l'injectivité de l'application. Pourtant, d'après la théorie de Galois et 3.8 (i),

$$\#Aut(k(E_1)/k(E_2)) \leq deg_s(\varphi) = \#\ker\varphi.$$

D'où la surjectivité de l'application.

(ii) D'après la preuve de (i), si φ est de plus séparable, on a

$$\#Aut(k(E_1)/k(E_2)) = deg_s(\varphi) = [k(E_1) : k(E_2)].$$

Il s'ensuit que $k(E_1)/k(E_2)$ est une extension Galoisienne. □

Lemme 3.16. *(« Se factoriser ») Soient $\varphi : E_1 \to E_2$ et $\psi : E_1 \to E_3$ deux isogénies. Si φ est séparable et $\ker\varphi \subset \ker\psi$, il existe une isogénie unique $\lambda : E_2 \to E_3$ telle que $\lambda \circ \varphi = \psi$.*

Démonstration. Par (ii) et (i) du lemme précédent, $k(E_1)/k(E_2)$ est Galoisienne et $Gal(E_1/E_2) \subset Aut(E_1/E_3)$. On a

$$k(E_3) \subset k(E_1)^{Aut(E_1/E_3)} \subset k(E_2)^{Gal(E_1/E_2)} = k(E_2).$$

Correspondant à la tour d'extensions $k(E_3) \subset k(E_2) \subset k(E_1)$, on obtient une isogénie unique λ telle que $\lambda \circ \varphi = \psi$. □

Théorème 3.17. *(Isogénie duale) Soit $\varphi : E_1 \to E_2$ une isogénie de degré m. Il existe une isogénie unique*

$$\hat{\varphi} : E_2 \to E_1$$

telle que

$$\hat{\varphi} \circ \varphi = [m].$$

Démonstration. Supposons d'abord que φ est séparable, on a par 3.8

$$\#\ker\varphi = deg(\varphi) = m.$$

Par le théorème de Lagrange, on a

$$\ker\varphi \subset \ker[m].$$

D'après le lemme précédent, $[m]$ se factorise en $E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\hat{\varphi}} E_1$.

Considérons ensuite si φ est un endomorphisme de Frobenius. Quitte à composer, on peut supposer que la puissance de l'endomorphisme de Frobenius est un premier p. D'après **??**, on a $[p]^*\omega = p\omega = 0$, alors $[p]$ est un morphisme inséparable par 2.9. Alors le morphisme de Frobenius ϕ_p apparaît dans une décomposition de $[p]$, i.e. $[p] = \psi_s \circ \phi_p^e$. Posons $\hat{\varphi} := \psi_s \circ \phi_p^{e-1}$.

En général, on prend la factorisation $\varphi = \psi \circ \phi$ où ψ est séparable et ϕ est un endomorphisme de Frobenius. Par les cas au-dessus, on a

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

Posons $\widehat{\varphi} := \hat{\phi} \circ \hat{\psi}$. □

Lemme 3.18. *Soient $\varphi : E_1 \to E_2$, $\psi : E_1 \to E_2$, et $\lambda : E_2 \to E_3$ trois isogénies.*
(i) $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.
(ii) $\widehat{\lambda \circ \varphi} = \hat{\varphi} \circ \hat{\lambda}$.

Démonstration. (i) Consultez [2, III.6.2(b)]. (non-trivial)
(ii) Similaire à la dernière partie de la preuve du théorème précédent. □

Corollaire 3.19. *Soient E_1,E_2 deux courbes elliptiques. Alors l'application*

$$deg : Hom(E_1,E_2) \to \mathbb{Z}$$

est une forme quadratique définie positive.

Démonstration. Il suffit de montrer que

$$< \varphi, \psi >:= deg(\varphi + \psi) - deg(\varphi) - deg(\psi)$$

est bilinéaire. Appliquons l'injection

$$[\,] : \mathbb{Z} \to End(E_1),$$

on a

$$\begin{aligned}
[< \varphi,\psi >] &= [deg(\varphi + \psi)] - [deg(\varphi)] - [deg(\psi)] \\
&= (\widehat{\varphi + \psi}) \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \psi \\
&= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi (\text{par (i) de le lemme précédent}).
\end{aligned}$$

Maintenant, appliquons (i) de le lemme précédent à nouveaux. □

4. Points rationnels sur les courbes elliptiques

Théorème 4.1. *(Hasse) Soit $E/\mathbb{F}_q$ une courbe elliptique définie sur $\mathbb{F}_q$, alors*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Démonstration. D'après 3.6, on peut choisir une équation de Weierstrass pour E avec coefficients dans $\mathbb{F}_q$. Soit ϕ_q l'isogénie de Frobenius. D'après la théorie de Galois, on a $\bar{\mathbb{F}}_q^{\phi_q} = \mathbb{F}_q$, alors pour un point $P \in E(\bar{\mathbb{F}}_q)$, $P \in E(\mathbb{F}_q)$ si et seulement si $\phi_q(P) = P$, qui est équivalent à $P \in \ker(id - \phi_q)$. Prenons une différentielle $\omega \in \Omega_E$ non-nulle quelconque, puisque ϕ_q est inséparable, on a $\phi_q^*\omega = 0$ par 2.9, il s'ensuit que $(id - \phi_q)^*\omega = \omega$. Alors, $(id - \phi_q)^* : \Omega_E \to \Omega_E$ est non-nulle, ce qui implique que $id - \phi_q$ est séparable encore par 2.9. En conséquence, il est non ramifié par 3.9, on a $deg(id - \phi_q) = \#\ker(id - \phi_q)$. Il s'agit de calculer $deg(id - \phi_q)$. En outre, par 3.19, l'application $\varphi \mapsto deg\,\varphi$ est une forme quadratique définie positive sur $End(E)$. Appliquons la version de l'inégalité de Cauchy-Schwartz au-dessous, on a

$$|deg(id - \phi_q) - deg(id) - deg(\phi_q)| \leq 2\sqrt{deg(id)deg(\phi_q)}.$$

Observons que $deg(id) = 1$, et $deg(\phi_q) = q$ par 1.18, l'inégalité désirée se résulte. □

Lemme 4.2. *Soit A un groupe Abélien et $d : A \to \mathbb{Z}$ une forme quadratique définie positive. Alors pour tous ψ,$\varphi \in A$, on a*

$$|d(\psi - \varphi) - d(\psi) - d(\varphi)| \leq 2\sqrt{d(\psi)d(\varphi)}.$$

Démonstration. Notons $L(\psi,\varphi) = d(\psi - \varphi) - d(\psi) - d(\varphi)$ qui est bilinéaire. Puisque d est définie positive, on a pour tous m,$n \in \mathbb{Z}$,

$$0 \leq d(m\psi - n\varphi) = m^2 d(\psi) + mnL(\psi,\varphi) + n^2 d(\varphi).$$

Prenons en particulier $m = -L(\psi,\varphi)$ et $n = 2d(\psi)$, on obtient

$$0 \leq d(\psi)[4d(\psi)d(\varphi) - L(\psi,\varphi)^2].$$

Cela nous assure l'inégalité à condition que $\psi \neq 0$, mais le cas où $\psi = 0$ est trivial. □

Définition 4.3. *(Accouplement de Weil) Soit (E,O) une courbe elliptique et m un entier tel que $pgcd(m,car(k)) = 1$ de sorte que $\#E[m] = m^2$.*

Soit $T \in E[m]$. Par 3.5, il existe une fonction $f \in \bar{k}(E)$ telle que

$$div(f) = m[T] - m[O].$$

Soit $T' \in E$ tel que $[m]T' = T$. Alors il existe une fonction $g_T \in \bar{k}(E)$ telle que

$$div(g_T) = [m]^*([T]) - [m]^*([O])$$

En effet, par 3.5 encore, on a

$$[m]^*([T])-[m]^*([O]) = \sum_{R\in E[m]} ([T'+R]-[R]) \sim \sum_{R\in E[m]} ([T']-[O]) \sim m^2([T']-[O]) \sim 0$$

Ainsi,

$$div(f \circ [m]) = [m]^*(div(f)) = div(g_T^m)$$

donc quitte à une multiplication de une constante, on peut supposer que

$$f \circ [m] = g_T^m. \tag{2}$$

Soit maintenant S un autre point dans $E[m]$. Notons τ_S le morphisme de translation par S. On a

$$(\tau_S^* g_T)^m = \tau_S^*(g_T^m) = g_T^m$$

par 2. Donc il existe une unique racine de l'unité $e_m(S,T) \in \mu_m(\bar{k})$ telle que

$$\tau_S^* g_T = e_m(S,T) g_T.$$

Notons que ce facteur ne dépend pas de choix de g_T. Autrement dire,

$$e_m(S,T) = g(X+S)/g(X),$$

pour $X \in E$ quelconque tel que $g(X+S)$ et $g(X)$ bien-définis et non-zéro.

Proposition 4.4. *L'accouplement de Weil est :*

(i) Bilinéaire :

$$e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T),$$
$$e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2);$$

(ii) Alternatif :

$$e_m(S,T) = e_m(T,S)^{-1};$$

(iii) Non-dégénéré : si $e_m(S,T) = 1$ pour tout $S \in E[m]$, alors $T = O$;

(iv) Compatible avec le morphisme de multiplication : si $S \in E[mm']$ et $T \in E[m]$, alors on a

$$e_{mm'}(S,T) = e_m([m']S,T);$$

(v) Compatible avec dualité : soit $S \in E_1[m]$, $T \in E_2[m]$ et $\varphi : E_1 \to E_2$ une isogénie. Alors on a

$$e_m(S,\hat{\varphi}(T)) = e_m(\varphi(S),T).$$

Démonstration. (i) La première linéarité est simple :

$$e_m(S_1 + S_2,T) = \frac{g(X + S_1 + S_1)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} = e_m(S_2,T)e_m(S_1,T).$$

Pour montrer

$$e_m(S,T_1)e_m(S,T_2)e_m(S,T_1 + T_2)^{-1} = 1,$$

il suffit de montrer que $g_{T_1} g_{T_2} g_{T_1+T_2}^{-1}$ est invariant par translation par $E[m]$. Calculons que

$$div(g_{T_1} g_{T_2} g_{T_1+T_2}^{-1}) = [m]^*([T_1]+[T_2]-[T_1+T_2]-[O]) = [m]^*(div(f)) = div(f \circ [m])$$

pour quelque $f \in \bar{k}(E)^\times$ (par 3.5). Observons que $f \circ [m]$ est stable sous translation par $E[m]$, d'où la linéarité.

Pour les autres, cf [2, III.8.1, III.8.2] □

Définition 4.5. *Soit E une courbe elliptique et $m \in \mathbb{Z}^*$. On définit le m-torsion sous-groupe*

$$E[m] := \{P \in E : [m]P = 0\}.$$

Proposition 4.6. *Soit E une courbe elliptique et $m \in \mathbb{Z}^*$ tel que $pgcd(m,car(k)) = 1$. Alors on a*

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Démonstration. Puisque $[m]$ est séparable, on a

$$\#E[m] = deg([m]) = m^2$$

(cf [2, III.6.2 (d)], pas difficile). De même, on a pour tout d qui divise m la même équation. Pour écrire $E[m]$ comme un produit de groupes cycliques, il y a seulement une possibilité :

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

□

Définition 4.7. *(Module de Tate) Soit E une courbe elliptique et ℓ un nombre premier. On a un système projectif*

$$\cdots \to E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \to \cdots \to E[\ell].$$

Le module (ℓ-adique) de Tate est la limite projective de ce système

$$T_\ell(E) := \varprojlim_n E[\ell^n]$$

qui est naturellement un $\mathbb{Z}_\ell$-module.

Proposition 4.8. *Si $\ell \neq car(k)$, on a*

$$T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Démonstration. Prenons la limite projective dans 4.6. □

Soit $\varphi : E_1 \to E_2$ une isogénie entre deux courbes elliptiques, alors φ induit une application $E_1[\ell^n] \to E_2[\ell^n]$, ainsi une application ($\mathbb{Z}_\ell-$linéaire) entre modules de Tate

$$T_\ell(E_1) \to T_\ell(E_2).$$

On obtient une application

$$Hom(E_1,E_2) \to Hom(T_\ell(E_1),T_\ell(E_2))$$

et en particulier pour une courbe elliptique quelconque,

$$End(E) \to End(T_\ell(E)),\psi \mapsto \psi_\ell$$

qui est en fait un morphisme d'anneaux. Après avoir choisi une $\mathbb{Z}_\ell$-base pour $T_\ell(E)$, on peut écrire ψ_ℓ comme une 2×2 matrice dans $GL_2(\mathbb{Q}_\ell)$.

Proposition 4.9. *(Accouplement de Weil sur module de Tate) Soit E une courbe elliptique, ℓ un premier tel que $\ell \neq car(k)$. On a un accouplement bilinéaire, alternatif, non-dégénéré, compatible avec le morphisme de multiplication et la dualité (comme 4.4)*

$$T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

Démonstration. Pour tout $n = 1,2,\cdots$, on a

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu(\ell^n).$$

Afin de prendre la limite projective, il suffit de vérifier que l'accouplement de Weil est compatible avec le morphisme $[\ell]$, à savoir

$$e_{\ell^{n+1}}(S,T)^{\ell} = e_{\ell^n}([\ell]S,[\ell]T).$$

Par la linéarité 4.4 (i) on a

$$e_{\ell^{n+1}}(S,T)^{\ell} = e_{\ell^{n+1}}(S,[\ell]T).$$

Appliquons la compatibilité avec le morphisme $[\ell]$ (4.4(iv)). □

Proposition 4.10. *Soit E une courbe elliptique, $\psi \in End(E)$ un endomorphisme. Rappelons que on a un endomorphisme de module de Tate $\psi_\ell \in End(T_\ell[E])$. Alors on a*

$$det(\psi_\ell) = deg(\psi)$$

et

$$Tr(\psi_\ell) = 1 + deg(\psi) - deg(1-\psi).$$

En particulier, $det(\psi_\ell)$ et $Tr(\psi_\ell)$ ne dépend pas de choix de ℓ.

Démonstration. Soit $\{u,v\}$ une $\mathbb{Z}_\ell$-base de $T_\ell(E)$. Écrivons la matrice de ψ_ℓ sous cette base comme

$$\psi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Utilisons l'accouplement de Weil dans la proposition précédente, on peut calculer que

$$\begin{aligned} e(u,v)^{deg(\psi)} &= e([deg(\psi)]u,v)(4.4(i)) \\ &= e(\widehat{\psi_\ell}\psi_\ell u, v) \\ &= e(\psi_\ell u, \psi_\ell v) \text{ (compatibilité avec dualité)} \\ &= e(au+cv,bu+dv) \\ &= e(u,v)^{ad-bc} \, (alternatif) \\ &= e(u,v)^{det(\psi_\ell)}. \end{aligned}$$

Puisque e est non-dégénéré, on conclut que

$$deg(\psi) = det(\psi_\ell).$$

Pour la trace, il suffit d'utiliser le résultat dans l'algèbre linéaire

$$Tr(A) = 1 + det(A) - det(1 - A).$$

□

Proposition 4.11. *Notons $\mathbb{F}_{q^n}$ l'extension de $\mathbb{F}_q$ de degré n, et $E(\mathbb{F}_{q^n})$ les point $\mathbb{F}_{q^n}$-rationnel de E. On a*

$$\#E(\mathbb{F}_{q^n}) = 1 - \alpha^n - \beta^n + q^n$$

où α, $\beta \in \mathbb{C}$ deux nombres complexes conjugués avec norme ordinaire $\sqrt{q}$ dans $\mathbb{C}$.

Démonstration. Notons ϕ le q-puissance morphisme de Frobenius, similaire à la preuve de 4.1, on a

$$\#E(\mathbb{F}_{q^n}) = deg(1 - \phi^n).$$

D'après la proposition précédente, le polynôme caractéristique de ϕ_ℓ

$$det(T - \phi_\ell) = T^2 - Tr(\phi_\ell)T + det(\phi_\ell)$$

possède coeffients dans $\mathbb{Z}$. Écrivons-le avec ses racines En outre, pour un nombre rationnel $\frac{m}{n} \in \mathbb{Q}$, par la proposition précédente on a

$$det(\frac{m}{n} - \phi_\ell) = \frac{1}{n^2} det(m - n\phi_\ell) = \frac{1}{n} deg(m - n\phi) > 0.$$

Il s'ensuit que les deux racines α, β du polynôme caractéristique sont complexes satisfaisant

$$\alpha\beta = det(\phi_\ell) = deg(\phi) = q.$$

Donc on a

$$|\alpha| = |\beta| = \sqrt{q}.$$

Finalement, observons que le polynôme caractéristique de ϕ_ℓ^n est

$$det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n)$$

(considérons ses valeurs propres). On peut calculer que

$$\#E(\mathbb{F}_{q^n}) = deg(1 - \phi^n) = det(1 - \phi_\ell^n) = 1 - \alpha^n - \beta^n + q^n.$$

□

Définition 4.12. *(Fonction zêta) Soit V une variété projective sur $\mathbb{F}_q$. La fonction zêta de V est la série formelle*

$$Z(V/\mathbb{F}_q;T) = exp(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}) \in \mathbb{Q}[[T]],$$

où $exp(F(T))$ désigne la série formelle $\sum_{i=0}^{\infty} F(T)^i/i!$ pour une série formelle sans terme constant.

Remarquons que quand on connaît la fonction zêta d'une variété V, on peut récupérer les nombres $\#V(\mathbb{F}_{q^n})$ par le formule

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n} logZ(V/\mathbb{F}_q;T)\Big|_{T=0}.$$

Exemple 4.13. *Soit $V = \mathbb{P}^m$. Calculons que*

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(m+1)}-1}{q^n-1} = \sum_{i=0}^{m} q^{ni},$$

alors

$$logZ(V(\mathbb{F}_q);T) = \sum_{i=0}^{\infty}(\sum_{i=0}^{m} q^{ni})\frac{T^n}{n} = \sum_{i=0}^{m} -log(1-q^iT).$$

En conséquence, on a

$$Z(V/\mathbb{F}_q;T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^mT)}.$$

Notons que dans ce cas la fonction zêta est rationnelle. En général, on a les théorèmes suivantes.

Théorème 4.14. *(Conjectures de Weil) Soit V une variété projective lisse sur $\mathbb{F}_q$ de dimension n. On a les suivants pour la fonction zêta.*

(i) Rationalité (Dwork 1960)

$$Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T).$$

(ii) Équation Fonctionnelle (M. Artin, Grothendieck, etc.)
Il existe un entier χ (caractéristique d'Euler de V) tel que

$$Z(V/\mathbb{F}_q;\frac{1}{q^nT}) = \pm q^{n\chi/2}T^{\chi}Z(V/\mathbb{F}_q;T).$$

(iii) Hypothèse de Riemann (Deligne 1973)
Il existe une factorisation

$$Z(V/\mathbb{F}_q;T)=\frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$$

avec chaque $P_i(T)\in\mathbb{Z}[T]$, $P_0(T)=1-T$, $P_{2n}(T)=1-q^nT$, *et pour tout* $i=1,\cdots,2n-1$, $P_i(T)$ *se factorise comme*

$$P_i(T)=\prod_j(1-\alpha_{ij}T)\quad avec\quad |\alpha_{ij}|=q^{1/2}.$$

Théorème 4.15. *(Hasse) Soit* E *une courbe elliptique sur* $\mathbb{F}_q$. *Alors il existe* $a\in Z$ *tel que*

$$Z(E/\mathbb{F}_q;T)=\frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

$$Z(E/\mathbb{F}_q;\frac{1}{qT})=Z(E/\mathbb{F}_q;T),\quad et$$

$$1-aT+qT^2=(1-\alpha T)(1-\beta T)\quad avec\quad |\alpha|=|\beta|=\sqrt{q}.$$

Démonstration. Par 4.11, on calcule que

$$\begin{aligned}log Z(E/\mathbb{F}_q;T)&=\sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+q^n)\frac{T^n}{n}\\&=-log(1-T)+log(1-\alpha T)+log(1-\beta T)-log(1-qT).\end{aligned}$$

Cela implique que

$$Z(E/\mathbb{F}_q;T)=\frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

où α, $\beta\in\mathbb{C}$ sont deux nombres complexes conjugués avec norme ordinaire $\sqrt{q}$ dans $\mathbb{C}$ et

$$a=\alpha+\beta=Tr(\phi_\ell)=1+q-deg(1-\phi)\in Z.$$

On peut vérifier que elle est la forme désirée. □

Remarque 4.16. *Prenons un changement de variable* $T=q^{-s}$, *on a pour une courbe elliptique*

$$\zeta(s)=Z(E/\mathbb{F}_q;q^{-s})=\frac{1-aq^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

Par (ii) et (iii) du théorème précédent, on a l'équation fonctionnelle

$$\zeta(1-s) = \zeta(s)$$

et que tout zéro s de la fonction ζ, on a $Re(s) = \frac{1}{2}$, ce qui est similaire à la conjecture de Riemann ordinaire.

Références

[1] Jean-François Dat, *Variétés algébriques* https://webusers.imj-prg.fr/ jean-francois.dat/enseignement/VA/VA.pdf
[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer 2009.
[3] Jean-François Dat, *Introduction aux courbes elliptiques* https://webusers.imj-prg.fr/ jean-francois.dat/enseignement/CourbesEll/CE.pdf
[4] Elias M. Stein, Rami Shakarchi. *Complex Analysis*.