

Les courbes elliptiques sont des groupes, comme on la vu dans le cours précédent. Deux objets fondamentaux:

$E(k) \leftarrow$ le groupe des k -points de E

$\text{End}_k(E) \leftarrow$ endomorphismes de E c'est un anneau!

ex: Sur $\mathbb{C}$: $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$

$\text{End}_{\mathbb{C}}(E) \leftarrow$ déjà évoqué

• Sur $\mathbb{C}$, les points de n -torsion sont donnés par $\frac{1}{n}\Lambda/\Lambda \subset \mathbb{C}/\Lambda$, et donc $E(\mathbb{C})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ (*)

• L'objectif de ce cours est de dire des choses sur $E(k)[n]$ si k est quelconque. En particulier, on va démontrer que (*) reste vraie sur des corps algébriquement clos.

On commence par un lemme général sur les endomorphismes.

LEMME: Soit $(E, \mathcal{O})$ et $(E', \mathcal{O}')$ deux courbes elliptiques sur k , et soit $\varphi: E \rightarrow E'$ un morphisme de variétés.

(i) Si φ est non constant, alors $e_P(\varphi) = \deg_i(\varphi)$ par tout $P \in E$.

(ii) Si $\varphi(\mathcal{O}) = \mathcal{O}'$, alors φ est un morphisme de groupes

Démonstration: (i) On commence par rappeler la formule de Hurwitz: si $\varphi: C \rightarrow C'$ est un morphisme séparable de courbes projectives lisses, alors: $\deg(K_C) = \deg(\varphi) \deg(K_{C'}) + \deg(R_\varphi)$ (effectif)

• Si φ est séparable, la formule de Hurwitz donne $\deg(R_\varphi) \leq 0$ puis R_φ car il est effectif. On en déduit $\deg(\varphi) = 1$

• Sinon, φ se factorise comme $\varphi = \varphi_0 \circ \varphi_1$ avec φ_0 séparable et $\varphi_1: E \rightarrow E^{(p)}$ le morphisme de Frobenius en $q = \deg_i(\varphi)$. Celui-ci est postérieurement d'indice q .

(ii) le morphisme φ induit un morphisme de groupes abéliens

$$\varphi_*: \text{Div } E \rightarrow \text{Div } E', P \mapsto \sum_{\mathbb{P} \in P} e(\mathbb{P}) \cdot [\mathbb{P}]$$

On a vu en exercice que φ_* passe au quotient, et donc induit un morphisme

$$\varphi_*: \text{Pic}(E) \rightarrow \text{Pic}(E')$$

Mais avec l'égalité $\varphi_*([P] - [\mathcal{O}]) = [\varphi_*(P)] - [\mathcal{O}']$ montre que φ est un morphisme de groupes.

DEFINITION: • Un morphisme de courbes elliptiques $(E, \mathcal{O}) \xrightarrow{\varphi} (E', \mathcal{O}')$ est un morphisme de variétés $E \xrightarrow{\varphi} E'$ tel que $\varphi(\mathcal{O}) = \mathcal{O}'$.

• Une isogénie de E vers E' est un morphisme de courbes elliptiques non constant.

• Les morphismes forment un groupe adélin $\text{Hom}(E, E')$, via l'addition

$$(\varphi + \psi)(P) := \varphi(P) +_{E'} \psi(P)$$

Remarque: $\text{End}(E)$ forme un anneau par la composition d'après le lemme précédent. En fait c'est anneau est sans diviseur de zéro car un morphisme non nul est nécessairement séparable.

Le noyau d'une isogénie forme un sous-groupe de $E(k)$. Il s'agit de les dénumérer.

PROPOSITION: le noyau d'une isogénie est un sous-groupe fini de $E(k)$ et tout sous-groupe fini de $E(k)$ est le noyau d'une isogénie.

Démonstration: On commence par montrer la première assertion.

• Soit φ une isogénie et soit $\varphi = \varphi^{-1}(\mathcal{O}')$. Autrement dit $\ker \varphi$ consiste en l'ensemble des points de E au-dessus de $\mathcal{O}'$.

$$\deg(\varphi) = \sum_{\mathbb{P}|\mathcal{O}'} e(\mathbb{P}|\mathcal{O}') f(\mathbb{P}|\mathcal{O}') = \deg_i(\varphi) \sum_{\mathbb{P}|\mathcal{O}'} f(\mathbb{P}|\mathcal{O}')$$

En particulier, si $k = \bar{k}$ est algébriquement clos, $\#\ker(\varphi) = \deg_s(\varphi)$.

Rmq: l'action par translation du groupe $\ker(\varphi)$ sur $\bar{k}(E)$ induit une action par automorphisme de corps sur $\bar{k}(E)$ et $\varphi^*(\bar{k}(E')) \subset \bar{k}(E)^{\ker \varphi}$.

Si φ est séparable, c'est une égalité (comparer les degrés). Dans ce cas $\bar{k}(E)$ est une extension Galoisienne de $\bar{k}(E)^{\ker \varphi}$ de groupe de Galois $\ker(\varphi)$.

• Soit $T \subset E(k)$ un sous-groupe fini. T agit sur E par translation et on obtient un plongement de $T \subset \text{Aut}(\bar{k}(E))$. La théorie de Galois nous dit alors que $\bar{k}(E)$ est Galoisienne sur $\bar{k}(E)^T$ de groupe de Galois T .

Comme c'est un corps de fonctions, il existe une courbe projective lisse C pour laquelle

$$\bar{k}(C) = \bar{k}(E)^T: \text{on obtient un morphisme}$$

$$\varphi: E \rightarrow C \text{ de degré } |T|.$$

On a en particulier $|T| = e_P(\varphi) \cdot f_P(\varphi) \cdot C_P \leftarrow$ Cardinal des fibres.

indice de ramification $\uparrow$ indice d'inertie = 1 (corps alg. clos)

On peut dire que φ est constante sur les T -orbites dans E . En effet si, pour $\gamma \in T$, $\varphi(\gamma + P) \neq \varphi(P)$, alors on peut trouver $f \in \bar{k}(C)$ avec un pôle en $\varphi(P)$ mais pas en $\varphi(\gamma + P)$. Alors f vue dans $\bar{k}(E)$ aurait un pôle en P et pas en $\gamma + P$ ce qui est absurde car f est T -invariante.

En particulier, les fibres sont toutes de même cardinal $= |T|$ (il existe au moins un point de C non ramifié). On obtient alors que φ n'est pas ramifié.

La formule de Hurwitz donne alors $g(C) = g(E)$. En posant $\mathcal{O}' = \varphi(\mathcal{O})$, on obtient que $(C, \mathcal{O}')$ est une courbe elliptique et que donc $\varphi: E \rightarrow C$ est une isogénie de noyau T . $\square$

Exemple: Si $m \neq 0$, alors la multiplication par m est l'exemple fondamental d'une isogénie. On la notera $[m]$ (ou encore $[m]_E$). Encore faut-il démontrer sa non-constance!

Il suffit de le démontrer pour m premier.

• Si m est impair, il suffit de trouver un point P d'ordre 2 (car alors $mP = P$, et donc P et $\mathcal{O}$ sont dans l'image de $[m]$).

Lorsque $\text{car}(k) \neq 2$, $E \rightarrow \mathbb{P}^1$, associé à $a \in \mathcal{L}(2[\mathcal{O}]) \setminus \bar{k}$, de degré 2 dont les fibres sont $\{P, -P\}$. Le morphisme est séparable (car $\text{car}(k) \neq 2$) et ses indices de ramification $\in \{1, 2\}$ sont inversibles. Par Hurwitz, on déduit qu'il y a 4 points de ramification, i.e. 4 points tels que $P = -P$.

• Cela montre aussi que $[2]$ n'est pas constant.

PROPOSITION: Si $\text{car}(k) \neq 2$, alors $[m]$ est une isogénie.

Rmq: c'est encore vrai sans hypothèse de caractéristique.

Exemple: Si E est définie sur $k = \bar{k} = \overline{\mathbb{F}_p}$. Alors $E(\overline{\mathbb{F}_q}) \subset E(\overline{\mathbb{F}_q})$ est un sous-groupe fini. L'isogénie sous-jacente est $\text{id} - \varphi_q$ où φ_q est le q -Frobenius.

En particulier, la torsion de $E(k)$ ainsi que $E(\overline{\mathbb{F}_p})$ s'obtiennent par noyau d'isogénies. Ce sont des sous-groupes dont on aimerait dénumérer la structure et en particulier le cardinal. La question de savoir si une isogénie est séparable devient alors une question importante. Dans cette direction, on a:

THÉORÈME: L'isogénie $[m]$ est séparable si, et seulement si, $(m, \text{car}(k)) = 1$.

Exemple: On a vu que $\#E[2] = 4$. Comme $[2]$ est séparable, elle est non ramifiée et donc de degré 4. Il s'en suit que $[2^n]$ est de degré 4^n et, par conséquent, non ramifiée, $\#E[2^n] = (2^n)^2$. En déduire que $E[2^n] = (\mathbb{Z}/2^n\mathbb{Z})^2$ par récurrence.

III.5.5, III.4.10.c, III.6.3. $\leftarrow$ degré positif gradué form

$\leftarrow m+n \neq 0$ est séparable $\Leftrightarrow p \nmid m$