

# ① le morphisme de Frobenius

Rappels: Soit  $\varphi: C \rightarrow C'$  un morphisme de courbes projectives lisses sur  $K$ . Alors  $\varphi$  est ou bien constant (et on pose  $\deg \varphi = 0$ ) ou bien surjectif et  $K(C)/\varphi^* K(C')$  est une extension finie. Si  $\varphi$  n'est pas constant, on a la tour d'extensions

$$\deg \varphi \left[ \begin{array}{c} K(C) \\ \cup \\ K(C)_{\text{sep}} \\ \cup \\ \varphi^* K(C') \end{array} \right] \begin{array}{l} \deg_i \varphi \\ \deg_s \varphi \end{array}$$

Si  $K(C) = K(C)_{\text{sep}}$ , on dit que  $\varphi$  est séparable (autrement: in séparable). Si  $K(C)_{\text{sep}} = \varphi^* K(C')$ , on dit que  $\varphi$  est purement in séparable.

Pour chaque  $P \in C(K)$ , l'indice de ramification de  $\varphi$  en  $P$  est

$$e_{\varphi}(P) = \text{ord}_P(\varphi^* t_{\varphi(P)}),$$

où  $t_{\varphi(P)}$  est une uniformisante en  $\varphi(P)$ .

Proposition: Pour tout  $Q \in C'(\bar{K})$ ,

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

Pour prouver tout  $Q \in C'(\bar{K})$ ,

$$|\bar{\varphi}^{-1}(Q)| = \deg_s \varphi$$

Introduisons le diviseur de ramification

$$\begin{aligned} R_{\varphi} &= \sum_{P \in C} \dim_K (\Omega_{\mathcal{O}_P / \mathcal{O}_{\varphi(P)}}) \cdot [P] \\ &\geq \sum_{P \in C} (e_{\varphi}(P) - 1) [P] \end{aligned}$$

(avec égalité  $\Leftrightarrow e_{\varphi}(P) \neq 0$  dans le corps  $K$  pour tout  $P \in C(\bar{K})$ ).

Proposition (formule de Hurwitz)

Si  $\varphi: C \rightarrow C'$  est séparable, alors

$$\begin{aligned} \deg(K_C) &= \deg(\varphi) \deg(K_{C'}) \\ &\quad + \deg(R_{\varphi}) \end{aligned}$$

Soient  $p$  un nombre premier et  $k$  un corps parfait de caractéristique  $p$ . Soit  $q$  une puissance de  $p$ . Pour  $f \in k[X_0, \dots, X_n]$ , on note

$$f^{(q)} = \sum a_{\mathbf{I}}^q x^{\mathbf{I}} \in k[X_0, \dots, X_n]$$

le polynôme obtenu en prenant les puissances  $q$ -ièmes de chaque coefficient.

Soit  $C$  une courbe projective lisse définie sur  $k$  d'idéal homogène

$$I(C) = \text{l'idéal engendré par}$$

$$f \in k[X_0, \dots, X_n] \text{ homogène tel que } f(P) = 0 \text{ pour tout } P \in C(k)$$

Définition.  $C^{(q)}$  est la courbe projective lisse définie sur  $k$  d'idéal homogène

$$I(C^{(q)}) = \text{l'idéal engendré par } f^{(q)} \text{ pour } f \in I(C).$$

Il y a un morphisme de Frobenius

$$\varphi_f: C \longrightarrow C^{(f)}$$

$$[x_0: \dots: x_n] \mapsto [x_0^f: \dots: x_n^f]$$

En effet, pour tout  $P = [x_0: \dots: x_n] \in C(K)$   
 et tout  $f \in I(C)$  homogène,

$$f^{(f)}(\varphi_f(P)) = f^{(f)}([x_0^f: \dots: x_n^f])$$

$$= f([x_0: \dots: x_n])^f$$

caractéristique  
de  $K = p \quad = 0$

Proposition:

$$(a) \quad \varphi_f^* K(C^{(f)}) = K(C)^f$$

$\uparrow \{f^f \mid f \in K(C)\}$

(b)  $\varphi_f$  est purement inséparable

$$(c) \quad \deg \varphi_f = f$$

Démonstration (a) Rappelons que  $K(C)$

est l'ensemble des  $\frac{f}{g}$ ,  $f, g \in K[x_0, \dots, x_n]$

(3)

homogènes du même degré,  $g \notin I(C)$  et

$$\frac{f}{g} = \frac{f'}{g'} \text{ comme éléments de } K(C)$$

$$\Leftrightarrow fg' - f'g \in I(C)$$

On a donc:

$$\begin{aligned} \varphi_g^* K(C^{(q)}) &= \left\{ \frac{f(x_0^q, \dots, x_n^q)}{g(x_0^q, \dots, x_n^q)} \right\} \\ &= \left\{ \frac{f^{(q)}(x_0^q, \dots, x_n^q)}{g^{(q)}(x_0^q, \dots, x_n^q)} \right\} \\ &= \left\{ \frac{f(x_0, \dots, x_n)^q}{g(x_0, \dots, x_n)^q} \right\} \\ &= K(C)^q \end{aligned}$$

$K$  est parfait,  
donc tout polynôme  
est de la forme  
 $f^{(q)}$

(b) Une caractérisation équivalente des extensions purement inséparables d'un corps de caractéristique  $p$  est que pour tout élément  $\alpha \in E$ , il existe un entier  $n$  tel que  $\alpha^{p^n} \in F$ . Ce qu'on a vu dans (a) donne alors directement

que l'extension  $K(C)/K(C^q)$  est purement inséparable.

(c) Soit  $P$  un point de  $C$  et  $t$  une uniformisante en  $P$ . On a alors

$$\begin{array}{ccc}
 & K(C) & \text{purement} \\
 & | & \text{inséparable} \\
 \text{séparable} & K(C)^{\frac{1}{q}}(t) & \\
 \swarrow & & \searrow \\
 K(t) & & K(C)^{\frac{1}{q}} = \varphi^* K(C^{\frac{1}{q}})
 \end{array}$$

d'où  $K(C) = K(C)^{\frac{1}{q}}(t)$  car autrement

l'extension  $K(C)/K(C)^{\frac{1}{q}}(t)$  serait en même temps séparable et purement inséparable. On a donc :

$$\begin{aligned}
 \deg \varphi_q &= [K(C) : K(C^{\frac{1}{q}})] \\
 &= [K(C)^{\frac{1}{q}}(t) : K(C)^{\frac{1}{q}}]
 \end{aligned}$$

Comme  $t^{\frac{1}{q}} \in K(C)^{\frac{1}{q}}$ ,  $\deg \varphi_q \mid q =$  puissance de  $p$  et il suffit de montrer que  $t^{\frac{1}{p}}$  n'appartient pas à  $K(C)^{\frac{1}{q}}$ . En effet,

si  $x^{q/p} = f^q$  pour un  $f \in K(C)$ , alors

$$\frac{q}{p} = \text{ord}_p(x^{q/p}) = q \text{ ord}_p(f),$$

ce qui est absurde □

Corollaire. Tout morphisme  $\Psi: C_1 \rightarrow C_2$  entre courbes projectives lisses sur un corps de caractéristique  $p > 0$  se factorise comme

$$\begin{array}{ccccc} C_1 & \xrightarrow{\varphi_q} & C_1^{(q)} & \xrightarrow{\lambda} & C_2 \\ & & & \nearrow & \\ & & & \Psi & \end{array}$$

où  $q = \deg_i(\Psi)$  et  $\lambda$  est séparable.

Démonstration. Considérons

$$\begin{array}{ccc} K(C_1) & & \\ \text{deg } \Psi \downarrow & \nearrow & \\ \Psi^* K(C_2) & \nearrow & F = \text{la plus grande} \\ & & \text{sous-extension} \\ & & \text{séparable} \end{array}$$

Alors  $K(C_1)/_F$  est purement inséparable de degré  $q$ , d'où  $K(C_1)^q \subset F$ . Mais

$$K(C_1)^{\mathbb{F}} = \varphi_{\mathbb{F}}^* K(C_1^{\mathbb{F}}) \Rightarrow F = \varphi_{\mathbb{F}}^* K(C_1)$$

$$[K(C_1) : K(C_1^{\mathbb{F}})] = \mathbb{F}$$

d'où une tour d'extensions

$$\begin{array}{c} K(C_1) \\ | \\ \varphi_{\mathbb{F}}^* K(C_1^{\mathbb{F}}) \\ | \\ \psi^* K(C_2) \end{array}$$

qui par la correspondance entre courbes et corps de fractions induit

$$\begin{array}{ccccc} C_1 & \xrightarrow{\varphi_{\mathbb{F}}} & C_1^{\mathbb{F}} & \xrightarrow{\lambda} & C_2 \\ & & & \searrow & \\ & & & \psi & \end{array}$$

avec  $\lambda$  séparable car d'extension  
 $\varphi_{\mathbb{F}}^* K(C_1^{\mathbb{F}}) / \psi^* K(C_2)$  est séparable  $\square$

## ② Isogénies

Lemme: Soient  $(E, 0)$  et  $(E', 0)$  des courbes elliptiques définies sur  $K$ , et soit



⑤

$\varphi: E \rightarrow E'$  un morphisme de courbes projectives lisses. Alors

(a) Si  $\varphi$  est un constant, pour tout  $P$

$$e_{\varphi}(P) = \deg_i \varphi$$

(b) Si  $\varphi(0) = 0'$ , alors  $\varphi$  est un morphisme de groupes.

Démonstration: (a) Si  $\varphi$  est séparable, la formule de Hurwitz donne

$$\deg(K_E) = (\deg \varphi) \deg(K_{E'}) + \deg R_{\varphi},$$

$\begin{array}{c} \parallel \\ 0 \end{array}$ 
 $\begin{array}{c} \parallel \\ 0 \end{array}$

donc  $\deg R_{\varphi} = 0$ , mais comme le diviseur de ramification est effectif, cela implique  $R_{\varphi} = 0$  et donc  $e_{\varphi}(P) = 1$  en tout point  $P \in E(\bar{K})$ .

En général, on factorise  $\varphi = \lambda \circ \varphi_f$  avec  $\lambda$  séparable et  $\varphi_f: E \rightarrow E'$  le morphisme de Frobenius et on calcule

$$e_{\varphi}(P) = e_{\lambda}(P) e_{\varphi_{\lambda}}(P) = 1,$$

qui est aussi  $\deg_i \varphi$

(b) la morphisme  $\varphi$  induit un morphisme de groupes abéliens

$$\begin{aligned} \varphi_* : \text{Div}(E) &\longrightarrow \text{Div}(E') \\ [P] &\longmapsto [\varphi(P)] \end{aligned}$$

qui passe au quotient par les diviseurs de fonctions à cause de la relation

$$\varphi_* \text{div}(f) = \text{div}(N_{K(E)/K(E')} f)$$

et induit donc

$$\varphi_* : \text{Pic}^0(E) \longrightarrow \text{Pic}^0(E')$$

En utilisant l'isomorphisme

$$\begin{aligned} AJ : E(K) &\longrightarrow \text{Pic}^0(E) \\ P &\longmapsto [P] - [O] \end{aligned}$$

on obtient

$$\varphi_* ([P+Q] - [O]) \stackrel{\varphi(O)=O'}{\downarrow} = [\varphi(P+Q)] - [O']$$

d'un côté et

⑥

$$\begin{aligned}\varphi_* ([P+Q] - [O]) &= \varphi_* ([P] + [Q] - 2[O]) \\ &= [\varphi(P)] + [\varphi(Q)] - 2[O']\end{aligned}$$

d'où  $\varphi(P+Q) = \varphi(P) + \varphi(Q)$  par définition  
de la loi de groupe sur  $E'(\overline{k})$   $\square$

Définition. Un morphisme de courbes elliptiques est un morphisme de courbes projectives lisses  $\varphi: E \rightarrow E'$  tel que  $\varphi(O) = O'$ . Une isogénie est un morphisme non constant de courbes elliptiques.

Les morphismes forment un groupe abélien  
 $\text{Hom}(E, E')$

avec loi d'addition

$$(\varphi_1 + \varphi_2)(P) = \varphi_1(P) + \varphi_2(P)$$

$\uparrow$   $\uparrow$   
 somme dans somme dans  $E'$   
 $\text{Hom}(E, E')$

cas  $E = E'$ ,  $\text{End}(E) = \text{Hom}(E, E)$

forme un anneau avec la composition

comme produit et cet anneau n'a pas de diviseur de zéro, car la composition de deux morphismes non nuls (et donc surjectifs) est surjectif (et donc non nul).

Proposition. Le noyau d'une isogénie est un sous-groupe fini de  $E(\bar{K})$  et tout sous-groupe fini de  $E(\bar{K})$  est le noyau d'une isogénie.

Démonstration. Démonstrons la première partie. Soit  $\varphi: E \rightarrow E'$  une isogénie. Alors  $\text{Ker } \varphi = \varphi^{-1}(0')$ . La relation

$$\deg \varphi = \sum_{P \in \text{Ker } \varphi} e_{\varphi}(P) = \deg_i \varphi \cdot |\text{Ker } \varphi|$$

implique que  $\text{Ker } \varphi$  est un sous-groupe d'ordre  $= \deg_s \varphi$ . Pour démontrer la seconde partie, nous aurons besoin de

Lemme. Soit  $\varphi: E \rightarrow E'$  une isogénie. Pour chaque  $T \in E(K)$ , soit  $\pi_T: E \rightarrow E$

le morphisme de translation par  $T$

$$Z_T(P) = P + T$$

et soit  $Z_T^*$  l'automorphisme induit sur  $\bar{K}(E)$ .

L'application

$$\text{Ker } \varphi \xrightarrow{\sim} \text{Aut}(\bar{K}(E) / \varphi^* \bar{K}(E'))$$

$$T \longmapsto Z_T^*$$

est un isomorphisme de groupes.

Démonstration. Si  $T \in \text{Ker } \varphi$ , alors

$$(\varphi \circ Z_T)(P) = \varphi(P + T) = \varphi(P) + \varphi(T) = \varphi(P)$$

pour tout  $P \in E(\bar{K})$ , d'où

$$Z_T^*(\varphi^* f) = (\varphi \circ Z_T)^* f = \varphi^* f$$

pour tout  $f \in \bar{K}(E')$ , c'est-à-dire l'automorphisme  $Z_T^*$  fixe  $\varphi^* \bar{K}(E')$ . L'application est donc bien définie. Comme

$$Z_S \circ Z_T = Z_{S+T} = Z_T \circ Z_S$$

c'est un morphisme de groupes. Comme

$$|\text{Ker } \varphi| = \deg_S \varphi$$

$$\left| \text{Aut}(\bar{K}(E) / \varphi^* \bar{K}(E')) \right| \leq \deg_S \varphi,$$

↑  
théorème de Galois

il suffit de démontrer que l'application est injective. Soit donc  $T \in \ker \varphi$  tel que  $Z_T^*$  est l'identité sur  $\bar{K}(E_1)$ . Alors pour toute fonction  $f \in \bar{K}(E_1)$ ,

$$f(0) = f(Z_T(0)) = f(T)$$

□

et donc  $0 = T$ .

Corollaire. Si  $\varphi$  est séparable, alors l'extension  $\bar{K}(E)/\varphi^*\bar{K}(E')$  est galoisienne.

Démonstration. Si  $\varphi$  est séparable, alors  $|\ker \varphi| = \deg \varphi = [\bar{K}(E) : \varphi^*\bar{K}(E')]$  et donc  $|\text{Aut}(\bar{K}(E)/\varphi^*\bar{K}(E'))| = [\bar{K}(E) : \varphi^*\bar{K}(E')]$  □

Démonstration de la seconde partie

Soit  $E$  une courbe elliptique et soit  $\Gamma \subset E(\bar{K})$  un sous-groupe fini. Chaque point  $T \in \Gamma$  induit une automorphie de  $Z_T^*$  de  $\bar{K}(E)$ . Soit

$$\bar{K}(E)^\Gamma \subset \bar{K}(E)$$

le sous-corps fixe par tous les éléments

de  $\Gamma$ . Alors  $\bar{k}(E)$  est une extension galoisienne de  $\bar{k}(E)^\Gamma$  avec groupe de Galois  $\Gamma$ . Par la correspondance entre courbes et corps de fonctions, il existe une unique courbe  $C$  sur  $\bar{k}$  et un morphisme  $\varphi: E \rightarrow C$  tel que  $\varphi^* \bar{k}(C) = \bar{k}(E)^\Gamma$ .

Soit  $P \in E(\bar{k})$  et  $T \in \Gamma$ . Pour toute fonction  $f \in \bar{k}(C)$ ,

$$\begin{aligned} f(\varphi(P+T)) &= (z_T^* \circ \varphi^*) f(P) \\ &\stackrel{\substack{z_T^* \text{ fixe} \\ \varphi^* \bar{k}(C)}}{=} (\varphi^* f)(P) = f(\varphi(P)) \end{aligned}$$

donc  $\varphi(P+T) = \varphi(P)$ . Soient maintenant  $Q \in C(\bar{k})$  et  $P \in E(\bar{k})$  tel que  $\varphi(P) = Q$ .

Alors  $\varphi^{-1}(Q) \supset \{P+T \mid T \in \Gamma\}$ , mais

$|\varphi^{-1}(Q)| \leq \deg \varphi = |\Gamma|$ , donc  $|\varphi^{-1}(Q)| = \deg \varphi$ ,

ce qui veut dire que  $e_\varphi(P) = 1$  pour

tout  $P \in \varphi^{-1}(Q)$  et donc pour tout  $P$

car  $Q$  était quelconque.

Appliquons alors la formule de Hurwitz

$$2g(E) - 2 = (\deg \varphi)(2g(C) - 2)$$

car  $R\varphi = 0$ , ce qui donne  $g(C) = 1$ . On  
monte  $C$  du point  $\varphi(0)$  et alors  $C$   
est une courbe elliptique et  $E \xrightarrow{\varphi} C$   
est une isogénie séparable.  $\square$

Exemple: Soit  $n$  un entier. On note  
 $[n]: E \rightarrow E$  la « multiplication par  
 $n \gg$  dans la courbe elliptique  $E$ . Si  
 $n$  est non nul, c'est une isogénie.

Comme  $[m] \circ [n] = [mn] = [n] \circ [m]$ ,  
il suffit de démontrer que  $[n]$  est  
non constante pour  $n$  premier. Suppo-  
sons qu'on connaisse l'existence d'un  
point d'ordre 2, c'est-à-dire  $P \neq 0$   
tel que  $[2]P = 0$ . Alors  $[2] \neq 0$  et,  
pour tout  $n$  impair,  $[n]P = P$ , donc  
 $[n]$  est aussi non nulle.

Un argument possible pour l'existence



de points d'ordre 2 en caractéristique  $\neq 2$   
 est d'appliquer la formule de Hurwitz  
 au morphisme  $x: E \rightarrow \mathbb{P}^1$ , où  $x \in \mathcal{L}(2[0])$   
 est une constante. C'est un morphisme  
 séparable de degré 2 et si car  $K \neq 2$ ,  
 le diviseur de ramification est

$$R_x = \sum_{P=-P} [P]$$

$$\text{d'où} \quad 2g(E) - 2 = (\deg x)(2g(\mathbb{P}^1) - 2) + \deg R_x,$$

c'est-à-dire  $\deg R_x = 4$  et il existe  
 4 points  $P$  tels que  $[2]P = 0$ .

Remarque: le fait que  $[m]$  soit une  
 isogénie pour tout  $m$  nous permet d'équivaloir  
 à l'injectivité du morphisme d'anneau  
 $\mathbb{Z} \rightarrow \text{End}(E)$ .

### ③ L'Isogénie duale

Sont  $\varphi: E \rightarrow E'$  une isogénie entre

courbes elliptiques. Rappelons que  $\varphi$  induit un morphisme de groupes abéliens

$$\varphi^*: \text{Pic}^0(E') \longrightarrow \text{Pic}^0(E)$$

$$[Q] \longmapsto \sum_{\varphi(P)=Q} e_{\varphi(P)} [P]$$

qui est linéaire défini par  $\varphi^*(\text{div } f)$  est égal à  $\text{div}(\varphi \circ f)$ .

on considère l'application

$$\hat{\varphi}: E'(\bar{k}) \xrightarrow[\sim]{AJ} \text{Pic}^0(E') \xrightarrow{\varphi^*} \text{Pic}^0(E) \xrightarrow[\sim]{AJ^{-1}} E(\bar{k})$$

qui envoie un point  $Q \in E'(\bar{k})$  sur le point  $\hat{\varphi}(Q)$  de  $E(\bar{k})$  caractérisé uniquement par

$$[\hat{\varphi}(Q)] - [O_E] = \varphi^*([Q] - [O_{E'}])$$

But: montrer que  $\hat{\varphi}$  est une isogénie

Soit  $P \in E(\bar{k})$  tel que  $\varphi(P) = Q$ .

Alors la préimage de  $Q$  est l'ensemble

(10)

$$\{P+R \mid R \in \ker \varphi\}$$

où  $\ker \varphi \subset E(\mathbb{K})$  est un sous-groupe  
d'ordre  $\deg_S \varphi$ . On a alors:

$$\begin{aligned} \varphi^*([Q] - [0_E]) &= \sum_{\varphi(T)=Q} e_\varphi(T) [T] \\ &\quad - \sum_{\varphi(R)=0_E} e_\varphi(R) [R] \end{aligned}$$

$$= \sum_{R \in \ker \varphi} \deg_i \varphi ([P+R] - [R])$$

Comme par ailleurs  $[P+R] - [R] = [P] - [0_E]$   
dans  $\text{Pic}^0(E)$ , on trouve

$$\varphi^*([Q] - [0_E]) = \deg_i \varphi \sum_{R \in \ker \varphi} ([P] - [0_E])$$

$$= \deg_i \varphi |\ker \varphi| ([P] - [0_E])$$

$$= \deg \varphi \cdot ([P] - [0_E])$$

Par conséquent,

$$\hat{\varphi}(Q) = [\deg \varphi](P)$$

Théorème. Soit  $\varphi: E \rightarrow E'$  une isogénie de degré  $m$ . Il existe une unique isogénie  $\hat{\varphi}: E' \rightarrow E$  telle que

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

De plus, cette isogénie satisfait à

- $\varphi \circ \hat{\varphi} = [m]_{E'}$
- $\widehat{\Psi \circ \varphi} = \hat{\varphi} \circ \hat{\Psi}$  pour toute isogénie  $\Psi: E' \rightarrow E''$ .

Démonstration: D'abord l'unicité.

Si  $\hat{\varphi}'$  est une autre isogénie avec la même propriété, alors

$$\begin{aligned} (\hat{\varphi} - \hat{\varphi}') \circ \varphi &= \hat{\varphi} \circ \varphi - \hat{\varphi}' \circ \varphi \\ &= [m]_E - [m]_E \\ &= 0, \end{aligned}$$

d'où  $\hat{\varphi} = \hat{\varphi}'$  car

- Si  $\hat{\varphi}$  existe, alors

$$\varphi \circ \hat{\varphi} \circ \varphi = \varphi \circ [m]_E = [m]_{E'} \circ \varphi$$

d'où  $\varphi \circ \hat{\varphi} = [m]_{E'}$  après simplification du facteur  $\varphi$ .

- Si  $\hat{\varphi}$  et  $\hat{\psi}$  existent, alors

$$\begin{aligned} (\hat{\varphi} \circ \hat{\psi}) \circ (\psi \circ \varphi) &= \hat{\varphi} \circ \underbrace{(\hat{\psi} \circ \psi)}_{[\deg \psi]_{E'}} \circ \varphi \\ &= \hat{\varphi} \circ \varphi \circ [\deg \psi]_E \\ &= [\deg \varphi]_E \circ [\deg \psi]_E \\ &= [\deg (\varphi \circ \psi)]_E \end{aligned}$$

d'où la relation  $\hat{\psi} \circ \varphi = \hat{\varphi} \circ \hat{\psi}$  par l'unicité.

- Au m de la compatibilité à la composition, après avoir factorisé

$$\begin{array}{ccccc} E & \xrightarrow{\varphi_f} & E^{(q)} & \xrightarrow{\lambda} & E' \\ & & & & \uparrow \\ & \underbrace{\hspace{10em}}_{\varphi} & & & \end{array}$$

il suffit de traiter le cas où  $\varphi$  est séparable et où  $\varphi = \text{Frobenius}$ .

- Cas  $\varphi$  séparable:  $m$  a alors

$$|\ker \varphi| = m$$

d'où  $\ker \varphi \subset \ker([m])$ . Par ailleurs,

$\bar{\kappa}(E)$  est galoisienne de groupe  
|  
de Galois

$$\varphi^* \bar{\kappa}(E')$$

$$\ker \varphi \simeq \text{Gal}(\bar{\kappa}(E) / \varphi^* \bar{\kappa}(E'))$$

on en déduit des inclusions

$$\bar{\kappa}(E) \supset \varphi^* \bar{\kappa}(E') \supset [m]^* \bar{\kappa}(E)$$

et à ces morphismes correspondent

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ & \searrow \varphi & \nearrow \hat{\varphi} \\ & E' & \end{array}$$

Comme  $\hat{\varphi}(0_{E'}) = \hat{\varphi}(\varphi(0_E)) = [m]_E(0) = 0_E$

le morphisme  $\hat{\varphi}$  est une isogénie.

- Cas où  $\varphi$  est le Frobenius  $\varphi_f$

Si  $\varphi = p^e$ , alors  $\varphi_f = \varphi_p \circ e$  et il

suffit donc de démontrer l'existence de  $\hat{\varphi}_p$ . L'application  $[p]_E$  est une isogénie irréductible (exercice), donc  $[p]$  se décompose comme

$$[p] = \psi \circ \varphi_p^f$$

avec  $\psi$  séparable et  $f \geq 1$  et il suffit alors de définir  $\hat{\varphi}_p = \psi \circ \varphi_p^{f-1}$   $\square$

Définition. Soit  $\varphi: E \rightarrow E'$  une isogénie. L'isogénie duale est  $\hat{\varphi}: E' \rightarrow E$ .

Théorème. Soient  $\varphi, \psi: E \rightarrow E'$  des isogénies. Alors

$$\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}.$$

On admet ce résultat pour l'instant.

Corollaire. Soit  $m \geq 1$  un entier.

(a)  $\deg([m]_E) = m^2$  et  $\widehat{[m]} = [m]$

(b) Si  $(m, \text{car } K) = 1$ , alors

$$E[m] = \{p \in E(k) \mid [m]p = 0\} \\ \cong (\mathbb{Z}/m\mathbb{Z})^2$$

en tant que groupes abéliens.

(c) si  $\text{car } k = p$ , alors soit

$$E[p^n] = 0 \quad \text{pour tout } n=1, 2, \dots$$

soit  $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$  pour tout  $n=1, 2, \dots$

Définition. Si  $E[p] = 0$ , on dit que  $E$  est super singulière. Sinon, on dit que  $E$  est ordinaire.

Démonstration.

(a) la formule  $\widehat{[m]} = [m]$  est claire pour  $m=1$ , donc

$$\widehat{[m+1]} = \widehat{[m] + [1]} = \widehat{[m]} + \widehat{[1]}$$

par le théorème. Par récurrence sur  $m$  on trouve alors  $\widehat{[m+1]} = [m+1]$ .



Soit  $d = \deg([m])$ . Alors par définition

$$[d] = \widehat{[m]} \circ [m] = [m^2],$$

d'où  $d = m^2$  car la multiplication par un entier non nul est une isogénie.

(b) Si  $(m, \text{car } K) = 1$ , alors  $[m]$  est une isogénie séparable, donc

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

De même, pour tout  $d|m$ , on a

$$|E[d]| = d^2$$

le groupe fini  $E[m]$  est abélien, donc produit de groupes cycliques

$$C_1 \times \dots \times C_r$$

où  $C_i$  est un groupe d'ordre  $p_i^{2k_i}$   
pour chaque  $p_i$  dans  $m = p_1^{k_1} \dots p_r^{k_r}$ .

Il suffit donc de considérer le cas

$m = p^k$ . Si  $k=1$ , les possibilités sont

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad \text{ou} \quad \mathbb{Z}/p^2\mathbb{Z}$$

mais tout élément non nul de  $E[p]$  a ordre  $p$ , donc  $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

Si  $E[p^k] = \langle p_1 \rangle \times \dots \times \langle p_r \rangle$  avec  $p_i$  un point d'ordre  $p^{e_i}$ , alors

$$E[p] = \langle p^{e_1-1} p_1 \rangle \times \dots \times \langle p^{e_r-1} p_r \rangle$$

est isomorphe à  $(\mathbb{Z}/p\mathbb{Z})^r$ , donc  $r=2$ ,

mais alors

$$E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$$

car le plus grand ordre d'un élément est  $p^k$ .

(c) Posons  $p = \text{car } k$  et écrivons  $[p]_E = \hat{\varphi}_p \circ \varphi_p$  où  $\varphi_p: E \rightarrow E^{(p)}$  est l'isogénie de Frobenius. Alors

$$|E[p^n]| = \deg_S([p^n]_E)$$

$$= \deg_S(\hat{\varphi}_p)^n$$

↑ car  $\varphi_p$  est purement isogène

Comme  $\deg \hat{\varphi}_p = \deg \varphi_p = p$ , il y a deux possibilités :

- si  $\hat{\varphi}_p$  est inséparable, alors  $\deg_S \hat{\varphi}_p = 1$  et  $E[p^n] = \{0\}$  pour tout  $n$
- si  $\hat{\varphi}_p$  est séparable, alors  $\deg \hat{\varphi}_p = p$  et  $|E[p^n]| = p^n$ . Pour  $n=1$ , on obtient

$$E[p] \cong \mathbb{Z}/p\mathbb{Z} \cong \langle P \rangle$$

Comme l'isogénie  $[p]: E \rightarrow E$  est surjection, il existe  $Q \in E(\overline{\mathbb{K}})$  avec  $pQ = P$ . Donc  $E[p^2]$  contient un point d'ordre  $p^2$ , et par récurrence

$$E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$$

□

