Isogénies, échange de clé SIDH et attaque par le lemme de Kani

Travail de fin d'étude, Magistère de Mathématiques

RANGUIS Célian encadré par **IEZZI Annamaria**

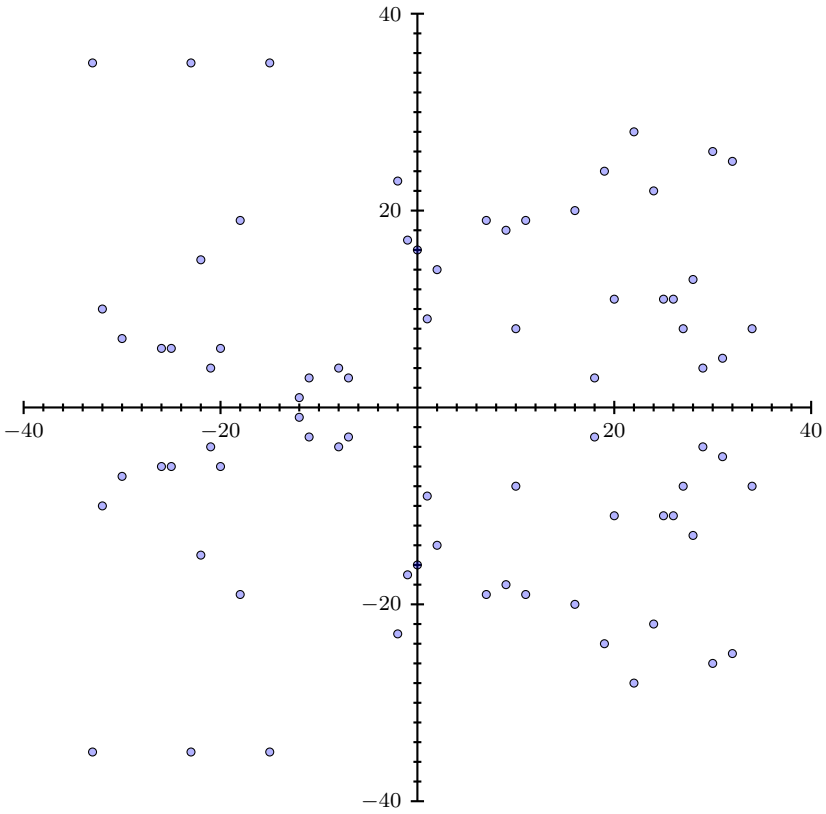


FIGURE 1 – Points $\mathbb{F}_{71}$-rationnels de $Y^2 = X^3 + 37X + 43$

Email : mail@rangu-cel.fr

Institut FOURIER

Magistère de mathématiques et applications

Table des matières

1 Introduction aux variétés algébriques **2**
- 1.1 Variétés algébriques . . . 2
  - 1.1.1 Dans le monde affine . . . 2
  - 1.1.2 Dans le monde projectif . . . 6
- 1.2 Applications entre variétés . . . 13
  - 1.2.1 Applications entre courbes . . . 15

2 Courbes elliptiques **16**
- 2.1 Équation de Weierstrass et loi de groupe . . . 16
- 2.2 Isogénies . . . 19
  - 2.2.1 Forme standard, degré et séparabilité . . . 21
  - 2.2.2 Multiplication par n et torsion . . . 27
  - 2.2.3 Isogénie associée à un noyau . . . 29
  - 2.2.4 Isogénie duale . . . 30
- 2.3 Classe d'isomorphisme et j-invariant . . . 34

3 Application cryptographique : SIDH **38**
- 3.1 Protocole . . . 38
- 3.2 Aspects effectifs . . . 40
  - 3.2.1 Calcul d'isogénies . . . 40
  - 3.2.2 Choix de p . . . 41
  - 3.2.3 Calcul d'une base de $E[l^e]$ . . . 42
- 3.3 Attaque par le lemme de Kani . . . 42
  - 3.3.1 Variétés abéliennes, lemme de Kani et autres outils . . . 43
  - 3.3.2 Déroulement de l'attaque . . . 49

A Notions complémentaires **51**
- A.1 Degré de transcendance . . . 51
- A.2 Extensions séparables . . . 53

Note: *A cause du début de mon année de préparation à l'agrégation, je n'ai pas eu le temps de boucler certains points de ce rapport. Ils seront signalés par des notes comme celles-ci.*

Dans tout ce qui suit, on évitera souvent certains outils et certaines preuves par manque de temps lors du stage. Le but final étant de faire de la cryptographie, j'ai fait le choix de passer à côté de certaines notions pour me concentrer sur cet aspect. Cependant, il y aura dès que possible une référence pour le lecteur souhaitant approfondir.

Introduction et remerciements

Depuis la publication de l'algorithme de Shor, la cryptographie doit s'adapter à l'attaquant quantique. L'une des théories menant à des cryptosystèmes conjecturés robustes face à celui-ci est celle des isogénies entre courbes elliptiques.

Dans ce rapport, nous commençons par des rudiments de géométrie algébrique afin de définir proprement la notion de courbes elliptiques. Nous employons ensuite le formalisme simplifié d'Andrew Sutherland pour comprendre plus en détail ces objets et notamment leurs structures de groupe ainsi que les 'morphismes' qui les relient (les isogénies). Nous expliquons ensuite l'un des premiers cryptosystèmes basés sur celles-ci (SIDH : Jao et De Feo [7]). Nous détaillons également certains aspects effectifs de celui-ci. Enfin, nous introduisons brièvement la théorie des variétés abéliennes et notament des produits de courbes elliptiques afin d'aboutir au lemme de Kani. Celui-ci nous permettra de casser SIDH.

Je tiens à remercier mon encadrante Annamaria Iezzi pour m'avoir offert ce stage ainsi que pour sa grande bienveillance tout au long de celui-ci. Je remercie également l'équipe CAS^{3}C^3 dans son ensemble pour son acceuil chaleureux et les repas partagés ensemble. Aussi, je remercie Antoine De Tarlé pour le temps qu'il a passé à répondre à mes nombreuses questions (même si ses réponses contenaient parfois un peu trop de schémas...). Enfin, je remercie Sara Checcoli pour m'avoir mis en contact avec Annamaria et pour son accompagnement tout au long de l'année.

1 Introduction aux variétés algébriques

Dans tout ce qui suit, on fixe un corps de base K et une clôture algébrique $\overline{K}$ de ce corps.
Commençons par énoncer la définition de courbe elliptique :

Définition 1.0.1: *Courbe elliptique*

Un courbe elliptique sur K est une **variété algébrique projective** de **dimension 1** (une courbe algébrique) sur K, **lisse**, de **genre** 1 et possédant un **point** K**-rationnel** O.

Nous allons maintenant définir les termes en gras afin de comprendre cette définition.

Nous ne traiterons pas la notion de genre car celle-ci nécessite l'introduction de nombreux outils qui dépassent le cadre de ce mémoire. Le lecteur intéressé peut se référer à Silverman [13, II.5.4].

1.1 Variétés algébriques

1.1.1 Dans le monde affine

Définition 1.1.1: *Ensemble algébrique affine*

Un ensemble algébrique affine est une partie de $\overline{K}^n$ de la forme $V_I := \{P \in \overline{K}^n \mid \forall f \in I,\ f(P) = 0\}$ où $I \subset \overline{K}[X_1, \dots, X_n]$ est un idéal.
Soit $V \subset \overline{K}^n$ un ensemble algébrique, l'idéal associé à V est $I(V) := \{f \in \overline{K}[X_1, \dots, X_n] \mid \forall P \in V,\ f(P) = 0\}$.

Remarque 1.1.2:

D'après le théorème de la base de Hilbert, $\overline{K}[X_1, \dots, X_n]$ est un anneau noethérien. C'est-à-dire que tout idéal de $\overline{K}[X_1, \dots, X_n]$ peut être engendré par un nombre fini de polynômes.
Par conséquent, pour tout ensemble algébrique V, il existe des polynômes $f_1, \dots, f_r \in \overline{K}[X_1, \dots, X_n]$ tels que $V = \{P \in \overline{K}^n \mid f_1(P) = \dots = f_r(P) = 0\}$.
Soit f un polynôme de $\overline{K}[X_1, \dots, X_n]$, on notera souvent V_f plutôt que $V_{(f)}$ pour alléger les notations.

Définition 1.1.3:

Soit V un ensemble algébrique affine. On dit que V est défini sur K, et on note V/K, si $I(V)$ peut être engendré par des polynômes de $K[X_1, \dots, X_n]$.

Notation : Soit A un anneau commutatif et $S \subset A$. On note $SA := \left\{ \sum_{i=0}^{n} s_i a_i \;\middle|\; n \in \mathbb{N},\ \forall i\ (s_i, a_i) \in S \times A \right\}$ l'idéal engendré par S dans A

Remarque 1.1.4:

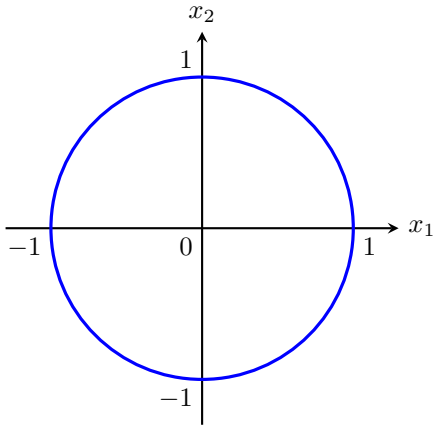
Soit V un ensemble algébrique affine et notons $I(V/K) := \{f \in K[X_1, \dots, X_n] \mid \forall P \in V,\ f(P) = 0\}$, l'idéal des polynômes à coefficients dans K qui s'annulent sur V.
Alors, V est défini sur K si et seulement si $I(V) = I(V/K)\overline{K}[X_1, \dots, X_n]$.

Définition 1.1.5:

Soit V un ensemble algébrique affine. On appelle points K-rationnels de V l'ensemble $V(K) = V \cap K^n$.

Exemple 1.1.6:

Le cercle $\mathbb{S}^1 = \{(x, y) \in \overline{K}^2 \mid x^2 + y^2 = 1\}$ est un ensemble algébrique défini sur K. On le représente ci-dessous pour $K = \mathbb{R}$ (on représente ses points $\mathbb{R}$-rationnels puisque $\overline{\mathbb{R}} = \mathbb{C} \neq \mathbb{R}$).



Remarque 1.1.7:

Soient V un ensemble algébrique affine et J un idéal. Alors $V_{I(V)} = V$ et $I(V_J) \supset J$.
L'inclusion $I(V_J) \subset J$ est fausse en général. Soit, par exemple, $f \in \overline{K}[X]$ un polynôme à racines simples. Alors, puisque pour tout $x \in \overline{K}$, $f(x) = 0 \iff f(x)^2 = 0$, on a $V_{(f^2)} = V_{(f)}$. Il suit que $I(V_{(f^2)}) = I(V_{(f)}) = (f) \not\subset (f^2)$.

Preuve :

Soient J un idéal et $V = V_J$ l'ensemble algébrique associé (par définition on décrit ainsi tous les ensembles algébriques).

Inclusion $I(V_J) \supset J$ **:** Soit $f \in J$, par définition de V, $\forall P \in V,\ f(P) = 0$. Alors, par définition de $I(V)$, $f \in I(V)$. Il suit que $J \subset I(V_J)$.

Égalité $V_{I(V)} = V$ **:** Soit $P \in V$. Par définition de $I(V)$: $\forall f \in I(V),\ f(P) = 0$. C'est-à-dire $P \in V_{I(V)}$ d'où $V \subset V_{I(V)}$.
Soit $P \in V_{I(V)}$. Par définition, $\forall f \in I(V),\ f(P) = 0$. Or, on a montré dans le paragraphe précédent que $J \subset I(V)$. Il suit que pour tout $f \in J$, f est aussi un élément de $I(V)$ donc $f(P) = 0$. Or ceci donne exactement $P \in V$ d'où $V_{I(V)} \subset V$.
□

Définition 1.1.8: *Variété algébrique affine*

Une variété algébrique affine est un ensemble algébrique affine V tel que $I(V)$ est un idéal premier de $\overline{K}[X_1, \ldots, X_n]$.

Définition 1.1.9:

Soit V/K une variété affine (on rappelle que V/K veut dire que V est définie sur K). On appelle anneau de coordonnées de V sur K l'anneau quotient $K[V] = K[X_1, \ldots, X_n]/I(V/K)$.
Puisque V est une variété, c'est un anneau intègre et on peut considérer $K(V) = \mathrm{Frac}(K[V])$ appelé le corps de fonctions de V.

Preuve :

> Il faut s'assurer que $I(V/K)$ est bien un idéal premier de $K[X_1, \ldots, X_n]$.
> Soient $f, g \in K[X_1, \ldots, X_n]$ tels que $fg \in I(V/K)$. Alors, voyant $f, g \in \overline{K}[X_1, \ldots, X_n]$ on a
>
> $$fg \in I(V/K) \implies fg \in I(V/K)\overline{K}[X_1, \ldots, X_n] = I(V)$$
>
> Or $I(V)$ est premier par hypothèse donc f ou g appartient à $I(V)$, disons f quitte à les échanger. Puisque $f \in K[X_1, \ldots, X_n]$, on a $f \in I(V) \cap K[X_1, \ldots, X_n] = I(V/K)$ qui est alors bien un idéal premier.
> □

Remarque 1.1.10:

Il ne faut pas confondre l'ensemble des points K-rationnels $V(K)$ et le corps de fonctions $K(V)$.

Les éléments de ce corps de fonctions seront la base de la construction des applications dite rationnelles entre variétés (Section 1.2). Pour l'instant, on donne simplement la définition suivante :

Définition 1.1.11:

Soient V une variété algébrique affine et $P \in V$. Notons :

$$\overline{K}[V]_P := \{F \in \overline{K}(V) \mid F \text{ a un représentant } f/g \text{ t.q. } g(P) \neq 0\} \subset \overline{K}(V)$$

Si $F \in K[V]_P$, on dit que F est définie en P, car alors l'évaluation $F(P)$ est possible.

Le corps de fonctions permet également de définir la dimension d'une variété :

Définition 1.1.12: *Dimension*

Soit V une variété algébrique affine. La dimension de V est $\dim V := [\overline{K}(V) : \overline{K}]_{\mathrm{tr}}$: le degré de transcendance de $\overline{K}(V)/\overline{K}$. Celle-ci est toujours finie puisque $K(V) = K(X_1 \mod I(V), \ldots, X_n \mod I(V))$.

Si la notion de degré de transcendance n'est pas connue, une courte présentation en est faite en Annexe A.1.

Lemme 1.1.13:

Soit $f \in \overline{K}[X_1, \ldots, X_n]$ un polynôme irréductible. Alors, $\dim(V_f) = n - 1$.

Preuve :

> Rappelons que $\overline{K}(V_f) = \mathrm{Frac}(\overline{K}[X_1, \ldots, X_n]/I(V)) = \overline{K}(X_1 \mod f, \ldots, X_n \mod f)$.
> Fixons i tel que $\deg_{X_i} f > 0$. Puisque $f(X_1 \mod f, \ldots, X_n \mod f) = 0$, $(X_i \mod f)$ est algébrique sur $\overline{K}(X_1 \mod f, \ldots, \widehat{X_i} \mod f, \ldots, X_n \mod f)$.
>
> Reste à voir que $\{X_1 \mod f, \ldots, \widehat{X_i} \mod f, \ldots, X_n \mod f\}$ est algébriquement indépendante.
> Supposons par l'absurde qu'il existe $g \in \overline{K}[X_1, \ldots, \widehat{X_i}, \ldots, X_n]$, non nul, tel que $g(X_1 \mod f, \ldots, \widehat{X_i} \mod f, \ldots, X_n \mod f) = 0$. Alors $g = 0 \mod f$ donc $f | g$ puis $0 = \deg_{X_i} g \geq \deg_{X_i} f$, ce qui contredit notre choix de i.
> □

En particulier, le cercle de l'Exemple 1.1.6 est une variété de dimension 1.

On va maintenant définir le caractère lisse d'une variété.

Définition 1.1.14:

Soit V une variété algébrique donnée par $I(V) = (f_1, \dots, f_m)$ (on rappelle que $V_{I(V)} = V$).
On dit que V est non singulière (ou lisse) au point $P \in V$ si la matrice

$$J_{f_1,\dots,f_n}(P) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(P) & \frac{\partial f_1}{\partial X_2}(P) & \cdots & \frac{\partial f_1}{\partial X_n}(P) \\ \frac{\partial f_2}{\partial X_1}(P) & \frac{\partial f_2}{\partial X_2}(P) & \cdots & \frac{\partial f_2}{\partial X_n}(P) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1}(P) & \frac{\partial f_m}{\partial X_2}(P) & \cdots & \frac{\partial f_m}{\partial X_n}(P) \end{pmatrix}$$

est de rang $n - \dim V$.
Si V est non singulière en tous points on dit qu'elle est non singulière (ou lisse).

Cette définition ne dépend du choix des générateurs de $I(V)$. En effet, le théorème I.5.1 de Hartshorne [6] donne une définition équivalente qui n'en dépend pas.

Exemple 1.1.15:

Soit $f \in \overline{K}[X_1, \dots, X_n]$ un polynôme irréductible, alors V_f est lisse en P si et seulement si :

$$\operatorname{rang} \begin{pmatrix} \frac{\partial f}{\partial X_1} & \cdots & \frac{\partial f}{\partial X_n} \end{pmatrix} = n - (n-1) = 1$$

C'est-à-dire si et seulement si : $\dfrac{\partial f}{\partial X_i} \neq 0$ pour au moins un i.
En particulier le cercle de l'Exemple 1.1.6 est lisse.

Proposition 1.1.16:

Soit V une variété affine non vide, de dimension $\dim V \geq 1$. Alors, V est infinie.

Pour démontrer cela on utilise quelques lemmes :

Lemme 1.1.17:

Soient V_I, V_J des ensembles algébriques affines. Alors, $V_I \cup V_J = V_{IJ}$ où

$$IJ = \{fg \mid f \in I,\ g \in J\}\overline{K}[X_1, \dots, X_n] = \left\{ \sum_{i=1}^{m} f_i g_i \;\middle|\; m \in \mathbb{N} \setminus \{0\},\ \forall i\ (f_i, g_i) \in I \times J \right\}$$

De plus, supposons que V_I et V_J sont des variétés et que $I(V_I) = I, I(V_J) = J, I(V_{IJ}) = IJ$. Alors, $V_I \cup V_J$ est une variété si et seulement si $I = IJ$ ou $J = IJ$.

Preuve :

On commence par montrer que $V_{IJ} = V_I \cup V_J$.

Montrons que $V_I \cup V_J \subset V_{IJ}$ **:** Soit $P \in V_I$. Alors, pour tout $f \in I, g \in J$, $f(P) = 0$ et donc $f(P)g(P) = 0$. Par conséquent, $P \in V_{IJ}$. Idem pour $P \in V_J$.

Montrons que $V_I \cup V_J \supset V_{IJ}$ **:** On procède par contraposé, soit $P \notin V_I \cup V_J$. Par définition, ceci signifie qu'il existe $f \in I,\ g \in J$ tels que $f(P), g(P) \neq 0$. Mais alors $fg \in IJ$ puis $P \notin V_{IJ}$.

Cas ou V_{IJ} **est une variété :** Supposons maintenant que $I = I(V_I)$ et $J = I(V_J)$ et qu'ils soient premiers (et donc que V_I,V_J soient des variétés). Si $I = IJ$ ou $J = IJ$ (disons $IJ = I$), alors $IJ = I$ est un idéal premier. De plus, $I(V_{IJ}) = I(V_I) = I = IJ$ puis V_{IJ} est une variété.
Pour l'autre implication, procédons par contraposé et supposons que $I \neq IJ$ et $J \neq IJ$. Puisque $IJ \subset I \cap J$, il existe $f \in I \setminus IJ$ et $g \in J \setminus IJ$. Mais alors, $fg \in IJ$ qui n'est a fortiori pas un idéal premier. Il suit que $I(V_{IJ}) = IJ$ n'en est pas un non plus et que V_{IJ} n'est pas une variété.

□

Corollaire 1.1.18:

Toute variété non vide finie est réduite à un point.

Preuve :

Soit V une variété finie, alors on peut écrire $V = \bigcup_{i=1}^{n} \{P_i\}$ avec P_i des points distincts. Or, chaque $\{P_i\}$ est une variété algébrique. En effet, fixons i, notons $P_i = (x_1, \dots, x_n)$ et posons $I_i = (X_1 - x_1, \dots, X_n - x_n)$. Alors,

$$(y_1, \dots, y_n) \in V_{I_i} \iff y_1 - x_1 = \cdots = y_n - x_n \iff (y_1, \dots, y_n) = (x_1, \dots, x_n) = P$$

c'est-a-dire $\{P_i\} = V_{I_i}$. De plus, $f(P_i) = 0 \iff f \in (X_1 - x_1, \dots, X_n - x_n) = I_i$, donc $I(\{P_i\}) = I_i$. Ceci va nous permettre d'employer le Lemme 1.1.17. Il nous faut juste vérifier que $I(P_i, P_j) = I_i I_j$ pour tout $i \neq j$, or c'est bien le cas.

Fixons $i \neq j$ et supposons par l'absurde que $I_i I_j = I_i$. Alors $\{P_i\} \cup \{P_j\} = V_{I_i I_j} = V_{I_i} = \{P_i\}$ ce qui contredit $P_i \neq P_j$.
Par conséquent, $\{P_i\} \cup \{P_j\}$ n'est pas une variété ce qui implique $n = 1$ et V est un singleton.
□

On peut maintenant prouver la Proposition 1.1.16 :
Preuve :

D'après le Corollaire 1.1.18, il suffit de montrer qu'un singleton est de dimension 0. Or, si $P = (x_1, \dots, x_n)$ est un point alors $I(\{P\}) = (X_1 - x_1, \dots, X_n - x_n)$. Par conséquent, $\overline{K}[X_1, \dots, X_n]/I(\{P\}) \simeq \overline{K}$ puis $\overline{K}(\{P\}) = \overline{K}$ d'où dim{P}=0.
□

1.1.2 Dans le monde projectif

Rappelons que nous avons défini une courbe elliptique comme une variété **projective**, nous allons maintenant définir ce que cela veut dire.

Définition 1.1.19:

L'espace projectif de dimension n sur K est l'ensemble quotient $\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = (\overline{K}^{n+1} \setminus \{0\})/\sim$ avec

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \in \overline{K}^{\times} \text{ t.q. } (y_0, \dots, y_n) = (\lambda x_0, \dots, \lambda x_n)$$

Il est en bijection naturelle avec les droites vectorielles du $\overline{K}$-e.v. $\overline{K}^{n+1}$.
On note $[x_0 : \cdots : x_n]$ la classe de $(x_0, \dots x_n)$.
On appelle points K-rationnels l'ensemble $\mathbb{P}^n(K) = \{[x_0 : \dots, x_n] \mid (x_0, \dots, x_n) \in K^{n+1}\}$

Pour définir une variété de manière analogue au cas affine, il nous faut considérer des polynômes où la notion de racine dans l'espace projectif fait sens. Si on considère par exemple le polynôme $f(X, Y) = X^2 - Y \in \mathbb{Q}[X, Y]$, alors $f(2, 4) = 0 \neq f(1, 2)$. Cependant, $[2 : 4] = [1 : 2]$. On voit donc que la notion de racine de f dans $\mathbb{P}^1(\mathbb{Q})$ n'est pas bien définie.

Définition 1.1.20:

Un polynôme $f \in \overline{K}[X_0, \dots, X_n]$ est dit homogène de degré d si l'une des conditions équivalente suivante est satisfaite :

- $f(YX_0, \dots, YX_n) = Y^d f(X_0, \dots, X_n)$ dans $\overline{K}[X_0, \dots, X_n, Y]$.
- $f = \sum_{k_0 + \cdots + k_n = d} c_k X_0^{k_0} \cdots X_n^{k_n}$ c'est-a-dire f n'a que des monômes de degré total d.

On note $K^{\text{hom}}[X_0, \dots, X_n]$ l'ensemble des polynômes homogènes en $n + 1$ variables et à coefficients dans K.

Preuve :

Ces deux définitions sont bien équivalentes :
Supposons $f(YX_0, \dots, YX_n) = Y^d f(X_0, \dots, X_n)$ dans $\overline{K}[X_0, \dots, X_n, Y]$. Alors, si $f = \sum_{k_0,\dots,k_n} c_k X_0^{k_0} \cdots X_n^{k_n}$, on a :

$$f(YX_0, \dots, YX_n) = \sum_{m \geq 0} \underbrace{\left(\sum_{k_0+\cdots+k_n=m} c_k X_0^{k_0} \cdots X_n^{k_n} \right)}_{f_m} Y^m = Y^d f(X_0, \dots, X_n)$$

Voyant cette égalité dans $(K[X_0, \dots, X_n])[Y]$, on voit que $\forall m \neq d,\ f_m = 0$ et f a bien la forme voulue.

Supposons $f = \sum_{k_0+\cdots+k_n=d} c_k X_0^{k_0} \cdots X_n^{k_n}$, un simple calcul donne bien $f(YX_0, \dots, YX_n) = Y^d f(X_0, \dots, X_n)$.

□

L'intérêt de cette notion est que l'ensemble $\{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid f(x_0, \dots, x_n) = 0\}$ est bien défini puisque pour tous $P \in \mathbb{P}^n, \forall \lambda \in \overline{K}^\times$ on a $f(\lambda P) = 0 \iff \lambda^d f(P) = 0 \iff f(P) = 0$.

Définition 1.1.21:

Un idéal I de $\overline{K}[X_0, \dots, X_n]$ est dit homogène s'il peut être généré par des polynômes homogènes. À tout tel idéal, on associe :

$$V_I = \{P \in \mathbb{P}^n \mid \forall f \in I,\ f \text{ homogène},\ f(P) = 0\}$$

Définition 1.1.22:

Un ensemble algébrique projectif est toute partie de $\mathbb{P}^n$ de la forme V_I. A un tel ensemble, on associe un idéal homogène

$$I(V) = \{f \in \overline{K}[X_0, \dots, X_n] \mid f \text{ homogène t.q. } \forall P \in V\ f(P) = 0\}\overline{K}[X_0, \dots, X_n]$$

On dit que V est défini sur K si $I(V)$ peut être engendré par des polynômes homogènes à coefficients dans K.

La Remarque 1.1.7 du cas affine se maintient :

Remarque 1.1.23:

Soit V un ensemble algébrique projectif et J un idéal homogène. Alors $V_{I(V)} = V$ et $I(V_J) \supset J$.

Preuve :

Soient J un idéal homogène et $V = V_J$ l'ensemble algébrique associé (par définition on décrit ainsi tous les ensembles algébriques).

Inclusion $I(V_J) \supset J$: Soit $f \in J$ un polynôme homogène, par définition de V, $\forall P \in V,\ f(P) = 0$¿ Alors, par définition de $I(V)$, $f \in I(V)$. Il suit que $J \subset I(V_J)$.

Égalité $V_{I(V)} = V$ Soit $P \in V$. Par définition de $I(V)$: $\forall f \in I(V)$ homogène, $f(P) = 0$. C'est-à-dire $P \in V_{I(V)}$ d'où $V \subset V_{I(V)}$.
Fixons J un idéal homogène tel que $V = V_J$ et soit $P \in V_{I(V)}$. Par définition, $\forall f \in I(V)$ homogène, $f(P) = 0$. Or, on a montré dans le paragraphe précédent que $J \subset I(V)$. Il suit que pour tout $f \in J$ homogène, f est aussi un élément de $I(V)$ donc $f(P) = 0$. Or ceci donne exactement $P \in V$ d'où $V_{I(V)} \subset V$.

□

Définition 1.1.24:

Une variété algébrique est un ensemble algébrique V tel que $I(V)$ est un idéal (homogène) premier de $\overline{K}[X_0, \dots, X_n]$.

À nouveau, on souhaite définir les notions de dimension et de non-singularité. Pour cela, on va se ramener au cas affine.

Définition 1.1.25: *Cartes*

Fixons $n \geq 2$ et $i \in \{0, \dots, n\}$ et notons $U_i = \{[x_0 : \dots, : x_n] \mid x_i \neq 0\}$ (bien défini modulo produit par $K^\times$). On pose la bijection :

$$\begin{aligned} \phi_i : \overline{K}^n &\to U_i \\ (x_0, \dots, \widehat{x}_i, \dots, x_n) &\mapsto [x_0 : \dots : 1 : \dots : x_n] \end{aligned} \qquad \begin{aligned} \phi_i^{-1} : U_i &\to \overline{K}^n \\ [x_0 : \dots : x_n] &\mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right) \end{aligned}$$

Celle-ci fait correspondre chaque classe de U_i avec son unique représentant vérifiant $x_i = 1$ (ou on a par conséquent retiré cette coordonnée).
On voit donc que l'espace projectif $\mathbb{P}^n$ contient des copies de l'espace affine $\overline{K}^n$.

Ayant fixé une coordonnée i, on identifiera $\overline{K}^n$ à U_i et on parlera des points de $\mathbb{P}^n \cap \overline{K}^n$ comme des points affines et des points de $\mathbb{P}^n \setminus \overline{K}^n$ comme des points à l'infini.

Dans tout ce qui suit, hors précisions, on fixe une telle carte ϕ_i.

Notation : Étant donné un vecteur $x = (x_0, \dots, x_n) \in \overline{K}^{n+1}$, on désigne le vecteur de $\overline{K}^n$ obtenu en retirant la i-ième coordonnée de x par $(x_0, \dots, \widehat{x}_i, \dots, x_n)$

On souhaite maintenant comprendre ce qu'il se produit lorsque l'on considère les points affines d'un ensemble algébrique projectif :

Proposition 1.1.26:

Soit $V \subset \mathbb{P}^n$ un ensemble algébrique. Alors, $V \cap \overline{K}^n$ (c'est-à-dire $\phi_i^{-1}(V \cap U_i)$) est un ensemble algébrique affine d'idéal $I(V \cap \overline{K}^n) := \{f(X_0, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n \mid f \in I(V)\}$.

Preuve :

Notons I l'idéal de l'énoncé. Soit $P = (x_0, \dots, \widehat{x}_i, \dots, x_n) \in \overline{K}^n$. Alors,

$$\begin{aligned} P \in \phi_i^{-1}(V \cap U_i) &\iff \phi_i(P) \in V \\ &\iff \forall f \in I(V),\ f(x_0 : \dots : 1 : \dots : x_n) = 0 \\ &\iff \forall f \in I(V),\ f(X_0, \dots, 1, \dots, X_n)(P) = 0 \\ &\iff \forall g \in I,\ g(P) = 0 \end{aligned}$$

Il suit que $V \cap \overline{K}^n = V_I$ est bien un ensemble algébrique.

Reste à voir que $I(V \cap \overline{K}^n) = I$. D'après la Remarque 1.1.23, $I \subset I(V_I) = I(V \cap \overline{K}^n)$.
Démontrons l'inclusion réciproque : soit $f \in I(V \cap \overline{K}^n) \subset \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n]$. Alors, considérons le polynôme $g = X_i f^*$ (f^* désigne le polynôme homogénéisé de f, comme définit dans la Définition 1.1.28) et remarquons que $g(X_0, \dots, 1, \dots, X_n) = f(X_0, \dots, \widehat{X}_i, \dots, X_n)$.
En particulier, pour tout point affine $P = [x_0 : \dots : 1 : \dots : x_n] \in V$, $g(P) = f(x_0, \dots, \widehat{1}, \dots, x_n) = 0$.
Enfin, pour tout point à l'infini $Q = [y_0 : \dots : 0 : \dots : y_n]$, $g(Q) = 0 f^*(y_0, \dots, 0, \dots, y_n) = 0$. Il suit que $g \in I(V)$ et donc que $f \in I$.
□

Remarque 1.1.27:

Puisque $(U_1, \dots, U_n)$ recouvre $\mathbb{P}^n$, tout ensemble algébrique projectif V est recouvert par des ensembles algébriques affines $(V \cap U_1, \dots, V \cap U_n)$

Ce qui précède montre que les points affines d'un ensemble algébrique projectif forment un ensemble algébrique affine. Maintenant, nous allons développer une procédure pour, partant d'un ensemble algébrique affine V, obtenir un ensemble algébrique projectif $\overline{V}$ tel que $\overline{V} \cap \overline{K}^n = V$. Pour cela, on voudrait en quelque sorte inverser l'opération $f \mapsto f(X_0, \dots, 1, \dots, X_n)$.

Définition 1.1.28:

Soit $f \in \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n]$, le polynôme homogénéisé de f selon X_i est

$$f^{*i} := X_i^d f\left(\frac{X_1}{X_i}, \dots, \widehat{1}, \dots, \frac{X_n}{X_i}\right)$$

où d est le plus petit entier tel que $X_i^d f\left(\frac{X_0}{X_i}, \dots, \widehat{1}, \dots, \frac{X_n}{X_i}\right)$ soit un polynôme.

Pour la suite, il sera utile de bien comprendre comment homogénéisation et déshomogénéisation interagissent.

Proposition 1.1.29:

Notons

$$\begin{aligned} \hom_i : K[X_0, \dots, \widehat{X}_i, \dots, X_n] &\to K^{\hom}[X_0, \dots, X_i, \dots, X_n] \\ g &\mapsto g^{*i} \end{aligned}$$

$$\begin{aligned} \mathrm{dehom}_i : \overline{K}^{\hom}[X_0, \dots, X_i, \dots, X_n] &\to \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n] \\ f &\mapsto f(X_0, \dots, 1, \dots, X_n) \end{aligned}$$

Alors, pour tout $f \in \overline{K}^{\hom}[X_0, \dots, X_i, \dots, X_n]$, pour tout $g \in \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n]$:

- $\mathrm{dehom}_i(\hom_i(g)) = g$
- $\hom_i(\mathrm{dehom}_i(f)) = \dfrac{1}{X_i^m} f$ où $m =: v_i(f)$ est la plus grande puissance de X_i divisant f.

Preuve :

- $\mathrm{dehom}_i(\hom_i(g)) = \mathrm{dehom}_i\left(X_i^d g\left(\frac{X_0}{X_i}, \dots, \widehat{1}, \dots, \frac{X_n}{X_i}\right)\right) = 1^d g\left(\frac{X_0}{1}, \dots, \widehat{1}, \dots, \frac{X_n}{1}\right) = g$
- Notons d le degré de f en tant que polynôme homogène et d_i son degré en tant que polynôme de $(\overline{K}[X_1, \dots, \widehat{X}_i, \dots, X_n])[X_i]$. Notons $f = \sum_{k=0}^{d_i} f_k X_i^k,\ f_k \in K[X_1, \dots, \widehat{X}_i, \dots, X_n]$.

  Posons $m = v_i(f)$. Alors, $X^l | f \iff f_0 = \cdots = f_{l-1} = 0 \iff f = \sum_{k=m}^{d_i} f_k X_i^k$ et $f_m \neq 0$. Dans ce cas, $\hom_i(\mathrm{dehom}_i(f)) = \hom_i\left(\sum_{k=m}^{d_i} f_k\right)$. Il nous faut alors, pour calculer $\hom_i$, déterminer la plus petite puissance α_i de X_i qui fait de $(X_i)^{\alpha_i} \sum_{k=m}^{d_i} f_k\left(\frac{X_1}{X_i}, \dots, \widehat{1}, \dots, \frac{X_n}{X_i}\right)$ un polynôme. Remarquons que f_k est nécessairement homogène de degré $d-k$ et donc le degré cherché est $d-m$. Finalement,

$$\begin{aligned} \hom_i(\mathrm{dehom}_i(f)) = \hom_i\left(\sum_{k=m}^{d_i} f_k\right) &= X_i^{d-m} \sum_{k=0}^{d_i} f_k\left(\frac{X_1}{X_i}, \dots, \widehat{1}, \dots, \frac{X_n}{X_i}\right) \\ &= \sum_{k=0}^{d_i} X_i^{d-m-(d-k)} f_k = \sum_{k=m}^{d_i} f_k X_i^{k-m} = \frac{1}{X_i^m} f \end{aligned}$$

□

Remarque 1.1.30:

On a défini dehom sur $\overline{K}^{\hom}[X_0, \dots, X_n]$ pour obtenir la relation sur $\hom \circ \mathrm{dehom}$. Cependant, dehom est parfaitement bien définie sur l'entièreté de $\overline{K}[X_0, \dots, X_n]$.

Définition 1.1.31:

Soit V un ensemble algébrique affine et fixons une inclusion $\phi_i : \overline{K}^n \to U_i$. On définit l'idéal $I = \{f^{*i} \mid f \in I(V)\}\overline{K}[X_0, \ldots, X_i, \ldots, X_n]$. Alors, la clôture projective de V est définie comme l'ensemble algébrique $\overline{V} = V_I$. De plus, $I(\overline{V}) = I$.

Preuve :

Vérifions que $I(\overline{V}) = I$.

On sait déjà que $I \subset I(\overline{V})$, reste à voir l'autre inclusion. Soient $f \in I(\overline{V})$ et $P \in V$.
Alors, $\phi_i(P) \in \overline{V}$. En effet, $\forall g \in I, \exists \widetilde{g} \in I(V)$ t.q. $g = \hom(\widetilde{g})$, puis $g(\phi_i(P)) = \mathrm{dehom}(g)(P) = \mathrm{dehom}(\hom(\widetilde{g}))(P) = \widetilde{g}(P) = 0$.
Par conséquent, $f(\phi_i(P)) = \mathrm{dehom}(f)(P) = 0$ donc $\mathrm{dehom}(f) \in I(V)$.
Finalement, $f = X_i^{v_i(f)}\hom(\mathrm{dehom}(f)) \in I$.
□

Proposition 1.1.32:

1. Soit V une variété (resp. un ensemble algébrique) affine. Alors, $\overline{V}$ est une variété (resp. un ensemble algébrique) projective et $V = \overline{V} \cap \overline{K}^n$.
2. Soit V une variété projective. Alors $V \cap \overline{K}^n$ est une variété affine et $V \cap \overline{K}^n = \emptyset$ ou $V = \overline{V \cap \overline{K}^n}$.
3. Si une variété affine (resp. projective) V est définie sur K alors $\overline{V}$ (resp. $V \cap \overline{K}^n$) l'est aussi.

Preuve :

1. Vérifions que si $I(V)$ est premier, $I(\overline{V})$ l'est également. C'est-à-dire que si V est une variété, alors $\overline{V}$ aussi.
   Soient $f, g \in \overline{K}[X_0, \ldots, X_n]$ tels que $fg \in I(\overline{V})$.
   Alors, par définition de $I(\overline{V})$, $fg = \sum_j h_j^* u_j$ avec $u_j \in \overline{K}[X_0, \ldots, X_n]$ et $h_j \in I(V)$.
   Mais alors, $\mathrm{dehom}(fg) = \mathrm{dehom}(f)\mathrm{dehom}(g) = \sum_j h_j \mathrm{dehom}(u_j) \in I(V)$ et, puisque $I(V)$ est premier, $\mathrm{dehom}(f) \in I(V)$ ou $\mathrm{dehom}(g) \in I(V)$. On suppose, quitte à les échanger, que $\mathrm{dehom}(f) \in I(V)$.
   Mais alors, utilisant la Proposition 1.1.29, $X_i^{v_i(f)} \underbrace{\hom(\mathrm{dehom}(f))}_{\in I(\overline{V})} = f \in I(\overline{V})$ donc $I(\overline{V})$ est bien premier et $\overline{V}$ est une variété.

   Montrons maintenant que $V = \overline{V} \cap \overline{K}^n$: soit $P = (x_0, \ldots, \widehat{x}_i, \ldots, x_n) \in \overline{K}^n$. Alors,

$$\begin{aligned} P \in \overline{V} \cap \overline{K}^n = \phi_i^{-1}(\overline{V} \cap U_i) &\iff \phi_i(P) \in \overline{V} \\ &\iff \forall f \in I(\overline{V}),\ f \text{ homogène}, f(x_0, \ldots, 1, \ldots, x_n) = 0 \end{aligned}$$

   Montrons alors que ceci équivaut à $\forall g \in I(V),\ g(x_0, \ldots, \widehat{x}_i, \ldots, x_n) = 0$ (c'est-à-dire $P \in V$).
   Le sens direct est clair puisque les homogénéisés des pôlynomes de $I(V)$ sont des polynômes homogènes de $I(\overline{V})$.
   Passons au sens réciproque. Soit $f \in I(\overline{V})$ homogène , on peut écrire $f = \sum_j g_j^* h_j$ avec pour tout j, $g_j \in I(V)$ et $h_j \in \overline{K}[X_0, \ldots, X_n]$. Mais alors :

$$f(x_0, \ldots, 1, \ldots, x_n) = \sum_j \underbrace{g(x_0, \ldots, \widehat{x}_i, \ldots, x_n)}_{0} h_j(x_0, \ldots, 1, \ldots, x_n) = 0$$

   d'où le sens direct (on a utilisé la Proposition 1.1.29).

   On obtient finalement que $P \in V \iff P \in \overline{V} \cap \overline{K}^n$
2. Vérifions que, si $I(V)$ est premier, $I(V \cap \overline{K}^n)$ est premier également. C'est-à-dire que si V est une variété, alors $V \cap \overline{K}^n$ aussi.

Soient $f, g \in \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n]$ tels que $fg \in I(V \cap \overline{K}^n)$. Par définition, $fg = \text{dehom}(h)$ pour un $h \in I(V)$. Il suit que $X_i^{v_i(h)}\text{hom}(f)\text{hom}(g) = h \in I(V)$ (Proposition 1.1.29). Puisque $I(V)$ est premier, on est dans l'un des deux cas suivants :

- $X_i^{v_i(h)} \in I(V)$: si c'est le cas, alors tout point $[x_0 : \cdots : x_n] \in V$ doit vérifier x_i=0. C'est-à-dire $V \cap \overline{K}^n = \emptyset$ et dans ce cas $I(V \cap \overline{K}^n) = \overline{K}[X_0, \dots, \widehat{X}_i, \dots, X_n]$ est un idéal premier.
- $\text{hom}(f)\text{hom}(g) \in I(V)$: alors, puisque $I(V)$ est premier, $\text{hom}(f)$ ou $\text{hom}(g)$ est dans $I(V)$. Quitte à les échanger, on suppose $\text{hom}(f) \in I(V)$. Il suit que $f = \text{dehom}(\text{hom}(f)) \in I(V \cap \overline{K}^n)$ qui est bien un idéal premier.

Montrons alors que si $V \cap \overline{K}^n \neq \emptyset$, $V = \overline{V \cap \overline{K}^n}$. L'équivalence suivante va nous être utile.

$$V \cap \overline{K}^n = \emptyset \iff \forall [x_0 : \cdots : x_n] \in V,\ x_i = 0 \iff X_i \in I(V)$$

Supposons maintenant que $V \cap \overline{K}^n \neq \emptyset$. Alors,

$$I(\overline{V \cap \overline{K}^n}) = \{f^* \mid f \in I(V \cap \overline{K}^n)\} = \{f^* \mid f = \text{dehom}(g),\ g \in I(V)\}$$

Par conséquent, $f \in I(\overline{V \cap \overline{K}^n}) \iff \exists g \in I(V)$ t.q. $f = \text{hom}(\text{dehom}(g)) = X_i^{-m} g$ où $m = v_i(g)$ d'après la Proposition 1.1.29.

Mais alors, pour $f \in I(\overline{V \cap \overline{K}^n})$ et avec les notations précédentes, on a $fX_i^m = g \in I(V)$. Or, $I(V)$ est premier et $X_i \notin I(V)$ donc $f \in I(V)$. Il suit que $I(\overline{V \cap \overline{K}^n}) \subset I(V)$.

De plus, pour $f \in I(V)$, $\text{hom}(\text{dehom}(f))X^{v_i(f)} = f$ (Proposition 1.1.29) et $\text{hom}(\text{dehom}(f)) \in I(\overline{V \cap \overline{K}^n})$ (en effet $I(\overline{V \cap \overline{K}^n}) = \{f^* \mid f = \text{dehom}(g),\ g \in I(V)\}$) , donc $f \in I(\overline{V \cap \overline{K}^n})$.

En conséquence, $I(V) = I(\overline{V \cap \overline{K}^n})$ puis $V = \overline{V \cap \overline{K}^n}$ en utilisant la Remarque 1.1.23.

3. Soient V/K une variété projective et $f_1, \dots, f_n \in \overline{K}^n$ des générateurs homogènes de $I(V)$. Montrons que $V \cap \overline{K}^n$ est définie sur K.
   Soit $g \in I(V \cap \overline{K}^n)$. Alors, il existe $f \in I(V)$ tel que $g = \text{dehom}(f)$.
   Or, il existe $\lambda_1, \dots, \lambda_n \in \overline{K}[X_0, \dots, X_n]$ tels que $f = \sum_k \lambda_k f_k$. Par conséquent,

$$g = \text{dehom}(\sum_k \lambda_k f_k) = \sum_k \text{dehom}(\lambda_k)\text{dehom}(f_k)$$

   et $I(V \cap \overline{K}^n)$ est engendré par les polynômes $\text{dehom}(f_1), \dots, \text{dehom}(f_n) \in K[X_0, \dots, \widehat{X}_i, \dots, X_n]$.
   Note: *La même stratégie ne marche pas (ou pas immédiatement) vu que hom se comporte mal avec la somme.*

□

À partir de cela, il est possible de transporter des notions définies pour les variétés affines aux variétés projectives.

Définition 1.1.33:

Soient V une variété projective et un choix de i tel que $V \cap \overline{K}^n = \phi_i^{-1}(V \cap U_i) \neq \emptyset$.

- L'anneau de coordonnée de V est $\overline{K}[V] = \overline{K}[V \cap \overline{K}^n]$, le corps de fonctions de V est $\overline{K}(V) = \overline{K}(V \cap \overline{K}^n)$.
- La dimension de V est celle de $V \cap \overline{K}^n$
- V est non singulière en P affine si $V \cap \overline{K}^n$ y est non singulière.
- Si P est un point affine, on note $\overline{K}[V]_P = K[V \cap \overline{K}^n]_P$ et un élément de $\overline{K}(V)$ est défini en P s'il appartient à $K[V \cap \overline{K}^n]_P$, l'évaluation en P fait alors sens.

Remarque 1.1.34:

Cette définition ne dépend pas du choix de U_i

Preuve :

Il suffit de voir que le premier point ne dépend pas du choix de U_i. Or la Remarque 1.1.35 ci-après le donne puisqu'elle fournit une caractérisation qui ne dépend pas de U_i.
□

Remarque 1.1.35:

On peut aussi voir $\overline{K}(V)$ comme le corps des fractions de la forme $f(X)/g(X)$ avec f, g homogènes de même degré et $g(X) \notin I(V)$, dans lequel on identifie f/g et f'/g' si $fg' - f'g \in I(V)$.

Preuve :

Notons $K(V)$ cette nouvelle définition et montrons que ce corps est canoniquement isomorphe à la définition donnée précédemment (Définition 1.1.33).

$$\begin{aligned} \Phi : K(V) &\to \overbrace{\mathrm{Fr}\left(K[X_0, \dots, \widehat{X}_i, \dots, X_n]/I(V \cap \overline{K}^n)\right)}^{=:F} \\ f/g &\mapsto \frac{\mathrm{dehom}(f)}{\mathrm{dehom}(g)} \end{aligned}$$

Φ est bien définie : Il faut vérifier deux points :

— Indépendance du représentant : soient $f/g, f'/g'$ tels que $fg' - f'g \in I(V)$. Alors,

$$\begin{aligned} \Phi(f'/g') = \Phi(f/g) &\iff \frac{\mathrm{dehom}(f')}{\mathrm{dehom}(g')} = \frac{\mathrm{dehom}(f)}{\mathrm{dehom}(g)} \\ &\iff \mathrm{dehom}(f)\mathrm{dehom}(g') - \mathrm{dehom}(f')\mathrm{dehom}(g) \in I(V \cap K^n) \end{aligned}$$

Or, $\mathrm{dehom}(f)\mathrm{dehom}(g') - \mathrm{dehom}(f')\mathrm{dehom}(g) = \mathrm{dehom}(\underbrace{fg' - f'g}_{\in I(V)}) \in I(V \cap K^n)$.

— $\mathrm{dehom}(g) \notin I(V \cap K^n)$: pour cela on va montrer que $\mathrm{dehom}(g) \in I(V \cap K^n) \iff g \in I(V)$.
Le sens indirect est immédiat par définition de $I(V \cap \overline{K}^n)$. Supposons que $\mathrm{dehom}(g) \in I(V \cap \overline{K}^n)$, alors $\widetilde{g} = \mathrm{hom}(\mathrm{dehom}(g)) \in I(\overline{V \cap \overline{K}^n}) = I(V)$ et puisque $\widetilde{g}|g$ (Proposition 1.1.29) on a le résultat.

Φ est un morphisme : Car dehom en est un.

Noyau de Φ : $f/g \in \ker \Phi$ si et seulement si $\mathrm{dehom}(f) \in I(V \cap \overline{K}^n)$. Or on a vu ci avant que $\mathrm{dehom}(f) \in I(V \cap \overline{K}^n)$ si et seulement si $f \in I(V)$. C'est-à-dire $\ker \Phi$ est trivial.

Surjectivité Soit $f/g \in F$, notons $f^* = \mathrm{hom}(f)$, $g^* = \mathrm{hom}(g)$ et $d = \max\{\deg f^*, \deg g^*\}$. Supposons que $d = \deg f$ (on procède idem avec g si ce n'est pas le cas), notons $\widetilde{f} = f^*$, $\widetilde{g} = g^* X_i^{d - \deg g^*}$ de sorte que $\widetilde{f}, \widetilde{g}$ soient des polynômes homogènes de même degré. On a de plus $\mathrm{dehom}(\widetilde{f}) = \mathrm{dehom}(\mathrm{hom}(f)) = f$ et $\mathrm{dehom}(\widetilde{g}) = \mathrm{dehom}(\mathrm{hom}(g) X_i^{d - \deg g^*}) = g$ donc $\Phi(\widetilde{f}/\widetilde{g}) = f/g$ et Φ est surjective.

Conclusion : Finalement, on a bien construit un isomorphisme Φ.
□

Proposition 1.1.36:

Comme dans le cas affine (Proposition 1.1.16), toute variété de dimension au moins 1 est infinie.

Preuve :

Soient V une telle variété et ϕ_i un choix d'inclusion tel que $V \cap \overline{K}^n \neq \emptyset$. Alors, par définition, $V \cap \overline{K}^n$ est une variété affine de dimension 1 et est donc infinie. Puisque les points de $V \cap \overline{K}^n$ sont en bijection avec les points affines de V, on obtient que V est également infinie.
□

1.2 Applications entre variétés

Définition 1.2.1: *Application rationnelle*

Soient $V_1 \subseteq \mathbb{P}^m, V_2 \subseteq \mathbb{P}^n$ des variétés algébriques projectives.
Une application rationnelle $f : V_1 \longrightarrow V_2$, définie sur K, est un $(n+1)$-uplet projectif sur le corps $K(V_1)$: $[f_0 : \cdots : f_n] \in \mathbb{P}^n(K(V_1))$, vérifiant $\forall P \in V_1$ tel que chaque f_i est définie en P, $[f_0(P) : \cdots : f_n(P)] \in V_2$.

On dit que f est définie en P s'il existe un représentant $[f_0, \cdots, f_n]$ tel que :

- $f_1, \ldots, f_n$ sont définies en P
- il existe i tel que $f_i(P) \neq 0$.

Si f est définie en tous points de V_1 on dit que f est un morphisme de variétés.

Remarque 1.2.2:

La valeur de $[f_0(P) : \cdots : f_n(P)]$ ne dépend ni du choix du représentant pour P, ni de celui pour $[f_0 : \cdots : f_n]$ (à condition que l'évaluation fasse sens pour ce représentant).

Il existe une définition alternative des applications rationnelles.
Rappelons (Remarque 1.1.35) qu'un élément $F \in K(V)$ peut être vu comme un quotient de polynômes homogènes de même degré.
En multipliant par le produit des dénominateurs (qui est un polynôme homogène), on peut représenter une application rationnelle f comme $(\psi_0, \cdots, \psi_n)$ avec $\psi_0, \ldots, \psi_n$ des polynômes homogènes de même degré, non tous dans $I(V)$.

Définition 1.2.3: *Applications rationnelles bis*

Considérons l'ensemble des $(n+1)$-uplets de polynômes homogènes de même degré, non tous dans $I(V_1)$, modulo la relation d'équivalence

$$(\psi_0, \ldots, \psi_n) \sim (\phi_0, \ldots, \phi_n) \iff \forall i, j,\ \phi_i\psi_j = \psi_i\phi_j \mod I(V_1)$$

. On note $[\psi_0 : \cdots : \psi_n]$ la classe de $(\psi_0, \ldots, \psi_n)$.
Une application rationnelle est alors une telle classe d'équivalence $[\psi_0 : \cdots : \psi_n]$ telle que $\forall f \in I(V_2),\ f(\psi_0, \ldots, \psi_n) \in I(V_1)$. Elle est définie en un point P s'il existe un représentant $(\phi_0, \ldots, \phi_n)$ tel que pour tout i, ϕ_i est définie en P et $\exists j$ t.q. $\phi_j(P) \neq 0$.

Remarque 1.2.4:

La condition :

$$[\psi_0, \ldots, \psi_n] \text{ telle que } \forall f \in I(V_2),\ f(\psi_0, \ldots, \psi_n) \in I(V_1)$$

ne dépend pas du représentant choisit.

Preuve :

> Fixons j tel que $\psi_j \notin I(V_1)$. Soit $(\phi_0, \ldots, \phi_n)$ un autre représentant, alors
>
> $$\psi_j^d f(\phi_0, \ldots, \phi_n) = f(\psi_j\phi_0, \ldots, \psi_j\phi_n) = f(\psi_0\phi_j, \ldots, \psi_n\phi_j) = \phi_j^d f(\psi_0, \ldots, \psi_n)$$
>
> Or par hypothèse $f(\psi_0, \ldots, \psi_n) \in I(V_1)$ donc $\psi_j^d f(\phi_0, \ldots, \phi_n) \in I(V_1)$. Cependant, j a été fixé tel que $\psi_j \notin I(V_1)$ et a fortiori, puisque $I(V_1)$ est premier, $f(\phi_0, \ldots, \phi_n) \in I(V_1)$
> □

Remarque 1.2.5:

Cette définition est équivalente à la Définition 1.2.1

Preuve :

Notons A l'ensemble des applications rationnelles selon la Définition 1.2.1 et B celui des applications rationnelles selon la Définition 1.2.3.
Définissons deux applications :

— $\xi : A \to B$ définie par : $\forall \left[\frac{f_0}{g_0} : \cdots : \frac{f_n}{g_n}\right] \in A,\ \xi\left(\left[\frac{f_0}{g_0} : \cdots : \frac{f_n}{g_n}\right]\right) = \left[f_0 \prod_{j\neq 0} g_j : \cdots : f_n \prod_{j\neq n} g_j\right]$

Elle est bien définie. En effet, soient deux représentants $\left[\frac{f'_0}{g'_0} : \cdots : \frac{f'_n}{g'_n}\right] = \left[\frac{f_0}{g_0} : \cdots : \frac{f_n}{g_n}\right]$ et $\frac{u}{v} \in K(V_1)^\times$ tels que pour tout i, $\frac{f'_i}{g'_i} = \frac{u}{v} \times \frac{f_i}{g_i}$ dans $K(V_1)$.
Alors,

$$\begin{aligned}\xi\left(\left[\frac{f'_0}{g'_0} : \cdots : \frac{f'_n}{g'_n}\right]\right) &= \left[uv^n f_0 \prod_{j\neq 0} g_j : \cdots : uv^n f_n \prod_{j\neq n} g_j\right] \\ &= \left[f_0 \prod_{j\neq 0} g_j : \cdots : f_n \prod_{j\neq n} g_j\right] \\ &= \xi\left(\left[\frac{f_0}{g_0} : \cdots : \frac{f_n}{g_n}\right]\right)\end{aligned}$$

De plus, pour tout i, $f_i \prod_{j\neq i} g_j$ est un polynôme de degré $\deg f_i + \sum_{j\neq i} \deg g_j = \sum_j \deg g_j$. Il est de plus homogène car produit de polynômes homogènes. Par conséquent, ξ est bien à valeurs dans B.

— $\chi : B \to A$ définie par $\forall [\psi_0 : \cdots : \psi_n] \in B,\ \chi([\psi_0 : \cdots : \psi_n]) = \left[\frac{\psi_0}{\psi_i} : \cdots : 1 : \cdots \frac{\psi_n}{\psi_i}\right]$ où i est tel que $\psi_i \neq 0 \mod I(V_1)$.

Vérifions que χ est bien définie. Pour cela, commençons par vérifier que le choix de i n'a pas d'importance.
Soient i, j tels que $\psi_i, \psi_j \neq 0 \mod I(V_1)$. Montrons que $\left[\frac{\psi_0}{\psi_i} : \cdots : 1 : \cdots \frac{\psi_n}{\psi_i}\right] = \left[\frac{\psi_0}{\psi_j} : \cdots : 1 : \cdots \frac{\psi_n}{\psi_j}\right]$.
Soit $\lambda = \frac{\psi_j}{\psi_i}$. Alors, pour tout k, $\frac{\psi_k}{\psi_i} = \lambda \frac{\psi_k}{\psi_j}$ d'où l'égalité voulue.
Vérifions alors que l'image ne dépend pas du représentant. Soient deux représentants $[\psi_0 : \cdots : \psi_n] = [\psi'_0 : \cdots \psi'_n]$. Alors, fixons i, j tels que $\psi_i, \psi'_j \neq 0$. Puisque les classes sont égales, $\psi_i \psi'_j = \psi_j \psi'_i \mod I(V_1)$. Or, le membre de gauche est non nul par hypothèse (puisque $K(V_1)$ est un corps donc intègre). A fortiori, le membre de droite aussi et $\psi'_i, \psi_j \neq 0$. Par conséquent, on peut choisir i comme coordonnée pour diviser pour les deux représentants. Alors, puisque pour tout k $\psi_k \psi'_i = \psi'_k \psi_i \mod I(V_1) \implies \frac{\psi_k}{\psi_i} = \frac{\psi'_k}{\psi'_i} \mod I(V_1)$

$$\chi([\psi'_0 : \cdots : \psi'_n]) = \left[\frac{\psi'_0}{\psi'_i} : \cdots : 1 : \cdots : \frac{\psi'_n}{\psi'_i}\right] = \left[\frac{\psi_0}{\psi_i} : \cdots : 1 : \cdots : \frac{\psi_n}{\psi_i}\right] = \chi([\psi_0 : \cdots : \psi_n])$$

Enfin, puisque les ψ_k sont des polynômes homogènes de même degré, χ est bien à valeurs dans A.

Clairement, ces applications sont inverses l'une de l'autre et fournissent une bijection entre A et B. De plus, le sens que l'on donne à l'évaluation des éléments de A et B en un point P donne le même résultat.
□

Définition 1.2.6:

On dit que V_1 et V_2 sont isomorphes s'il existe deux morphismes $\phi : V_1 \to V_2$ et $\psi : V_2 \to V_1$ tels que $\psi \circ \phi$ est l'identité sur V_1 et $\phi \circ \psi$ est l'identité sur V_2.

Proposition 1.2.7:

Soient $V_1 \subset \mathbb{P}^m, V_2 \subset \mathbb{P}^n$ des variétés, $f, g : V_1 \to V_2$ des applications rationnelles définies sur K telles que pour une infinité de points $P \in V_1$, $f(P) = g(P)$. Alors, $f = g$. En particulier, on pourra toujours travailler points par points pour montrer des relations entre applications rationnelles.

Preuve :

Choisissons des représentants $f = [f_0 : \cdots : f_n]$ et $g = [g_0 : \cdots : g_n]$, $f_i, g_i \in K(V_1)$.
Soit i tel que $g_i \neq 0$, un tel i existe nécessairement car sinon g n'est pas une application rationnelle. On pose $\lambda = f_i/g_i \in K(V_1)$.

Soit $j \neq i$. Pour une infinité de points P, $[f_0(P) : \cdots : f_n(P)] = [g_0(P) : \cdots : g_n(P)]$, c'est-à-dire $\exists\gamma$ tel que $(f_0(P), \ldots, f_n(P)) = (\gamma g_0(P), \ldots, \gamma g_n(P))$.
En particulier, si P est tel que :

— $g_i(P) \neq 0$

— f_j, g_j sont définies en P

(donc toujours pour une infinité de P) on a $\gamma = f_i(P)/g_i(P) = \lambda(P)$ soit $f_j(P) = \lambda(P)g_j(P)$.
Mais alors, en simplifiant les dénominateurs, on obtient une égalité entre deux polynômes pour une infinité de P et $f_j = \lambda g_j$.

Finalement, $\forall j,\ f_j = \lambda g_j$ c'est-à-dire $f = [f_0 : \cdots : f_n] = [g_0 : \cdots : g_n] = g$.
□

1.2.1 Applications entre courbes

Définition 1.2.8:

Une courbe algébrique est définie comme une variété projective de dimension 1.

Proposition 1.2.9:

Soient $C_1/K,\ C_2/K$ des courbes et $\alpha : C_1 \to C_2$ une application rationnelle. Alors, si C_1 est non singulière en P, α est définie en P. En particulier, si C_1 est lisse alors α est un morphisme.

Preuve : Silverman [13, II.2.1].

Lemme 1.2.10:

Soient $C_1/K,\ C_2/K$ des courbes et $\alpha : C_1 \to C_2$ une application rationnelle définie sur K. Alors, on a un morphisme de corps :

$$\begin{aligned} \alpha^* : K(C_2) &\to K(C_1) \\ f &\mapsto f \circ \alpha \end{aligned}$$

Théorème 1.2.11:

Soient $E_1/K, E_2/K$ des courbes, $\alpha : E_1 \to E_2$ une application rationelle, alors $[K(C_1) : \alpha^*K(C_2)] < \infty$

Preuve : Silverman [13, II.2.4].

Définition 1.2.12:

Soient $E_1/K, E_2/K$ des courbes, $\alpha : E_1 \to E_2$ une application rationnelle. On appelle degré de α l'entier $\deg \alpha = [K(C_1) : \alpha^*K(C_2)]$. On dit que α est séparable si $K(C_1)/\alpha^*K(C_2)$ l'est. Le degré séparable de α est $[K(C_1) : \alpha^*K(C_2)]_s$.

Si la notion de degré séparable n'est pas connu, elle est expliquée dans la Annexe A.2

2 Courbes elliptiques

Nous allons maintenant nous concentrer sur le cas des courbes elliptiques. Cette section se base fortement sur "18.783 - Elliptic Curves"(Sutherland [14, 2025]), notamment on emploie le même formalisme.
Jusqu'à la fin de ce document (hors annexes), on suppose que la caractéristique du corps K n'est pas 2 ou 3.

Rappelons que nous avons déjà défini la notion de courbe elliptique au début de ce document (Définition 1.0.1).

2.1 Équation de Weierstrass et loi de groupe

Définition 2.1.1:

Une équation de Weierstrass sur K est une équation de la forme $Y^2 = X^3 + AX + B$, où A, B sont des éléments de K.

Théorème 2.1.2:

Notons $f = Y^2Z - X^3 - AXZ^2 - BZ^3 \in K[X, Y, Z]$, le polynôme associé à l'homogénéisation d'une équation de Weierstrass. La variété projective associée est une courbe elliptique si $27B^2 + 4A^3 \neq 0$. Réciproquement, toute courbe elliptique est isomorphe à une variété associée à une équation de Weierstrass où $27B^2 \neq -4A^3$.

Remarque 2.1.3:

La courbe (projective) donnée par V_f est la clôture projective de la courbe affine $V_{(Y^2-X^3-AX-B)}$. Dans ce qui suit, toutes les courbes sont projectives mais on emploiera souvent l'équation affine pour simplifier les notations.

Preuve :

Weierstrass donne CE Notons V l'ensemble algébrique projectif donné par l'équation de Weierstrass $f(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3 = 0$. Montrons qu'il s'agit d'une variété algébrique projective, c'est-à-dire que f est irréductible. Voyant $f \in (K[Y, Z])[X]$ et appliquant le critère d'Eisenstein avec Z comme élément irréductible, on obtient que f est irréductible dans $K(Y, Z)[X]$. Étant unitaire, f est primitif et donc irréductible dans $(K[Y, Z])[X] = K[X, Y, Z]$. C'est-à-dire V est une variété.
De plus, sa dimension est 1 d'après le Lemme 1.1.13 et la définition du corps de fonction pour une variété projective.

Montrons que cette variété est lisse. Soit $P = [x : y : 1]$ un point affine de V, alors $J_f(P) = (-3x^2 - A, 2y) = (0, 0)$ si et seulement si

$$\begin{cases} y^2 - x^3 - Ax - B = 0 \\ 3x^2 + A = 0 \\ 2y = 0 \end{cases} \iff \begin{cases} y^2 - x^3 - Ax - B = 0 \\ x^2 = -\frac{A}{3} \\ y = 0 \end{cases} \iff \begin{cases} \frac{A}{3}x - Ax - B = 0 \\ x^2 = -\frac{A}{3} \\ y = 0 \end{cases}$$

$$\iff \begin{cases} Ax = -\frac{3B}{2} \\ x^2 = -\frac{A}{3} \\ y = 0 \end{cases} \iff \begin{cases} Ax = -\frac{3B}{2} \\ A^2x^2 = \left(-\frac{3B}{2}\right)^2 = \frac{9B^2}{4} \\ x^2 = -\frac{A}{3} \\ y = 0 \end{cases}$$

Or, $\frac{9B^2}{4} = -A^2\frac{A}{3} \iff 27B^2 + 4A^3 = 0$.

Reste à voir les points à l'infini. Soit $[x : y : 0] \in V$ un point à l'infini. L'équation de Weierstrass donne $0 = x^3$ soit $x = 0$ et le seul point à l'infini est $O = [0 : 1 : 0]$.
Vérifions que V est lisse en O. En considérant l'inclusion $(x, z) \mapsto [x : 1 : z]$, on voit que la courbe affine associée est donnée par $Z - X^3 - AXZ^2 - BZ^3 = 0$ et donc est lisse en O (dont on note ici les coordonnées $[x : y : z] = [0 : 1 : 0]$) si et seulement si $(-3x^3 - Az^2, 1 - 2Axz - 3Bz^2) \neq (0, 0)$. Or, $(-3x^3 - Az^2, 1 - 2Axz - 3Bz^2) = (0, 1)$.

Enfin, O est K-rationnel et la courbe admet donc un point K-rationnel
Il resterait à montrer qu'elle est de genre 1, mais cela dépasse le cadre de ce travail. On peut en trouver une preuve dans Silverman [13, III.3.1].
CE est donnée par Weierstrass Ceci fait à nouveau intervenir des outils plus avancé que ceux que nous développons ici. On peut en trouver une preuve dans Silverman [13, III.3.1].
□

En vertu de ce résultat, on confondra maintenant courbes elliptiques et courbes données par une équation de Weierstrass.

Exemple 2.1.4:

Dans la Figure 2, on représente les points K-rationnels de la courbe donnée par l'équation $Y^2 = X^3 - 3X + 3$ pour $K = \mathbb{R}, \mathbb{F}_{17}$. Il apparait clairement que le terme de "courbe" ne correspond forcément à l'intuition que l'on s'en fait usuellement.

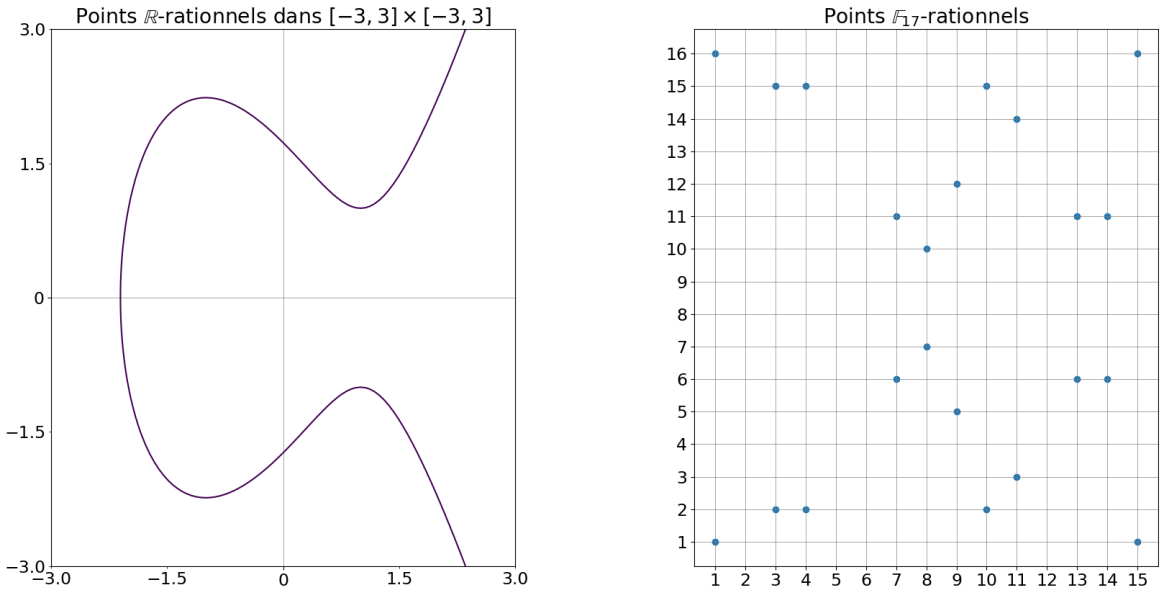


Figure 2 – Points $\mathbb{R}$-rationnels et $\mathbb{F}_{17}$-rationnels de la courbe $Y^2 = X^3 - 3X + 3$

L'un des intérêts principaux des courbes elliptiques est qu'il est possible de les munire d'une loi de groupe. L'idée est que trois points alignés se somment en le neutre (qui sera le point à l'infini). Pour définir cela rigoureusement, il faut travailler sur l'intersection entre des droites et la courbe.

Définition 2.1.5:

Une droite de $\mathbb{P}^2$ est une variété projective associée à un polynôme de la forme $f_{abc} = aX + bY + cZ$ avec $(a, b, c) \neq (0, 0, 0)$ (c'est-à-dire un polynôme homogène de degré 1).

Proposition 2.1.6:

Soient deux points $P, Q \in \mathbb{P}^2$ distincts. Alors, il existe une unique droite passant par ces deux points. On note celle-ci $\mathcal{D}_{PQ}$

Preuve :

Notons $P = [x_1 : y_1 : z_1]$ et $Q = [x_2 : y_2 : z_2]$.

P,Q sont affines ($z_i = 1$) et $x_1 \neq x_2$: Quitte à multiplier par $1/b$, on peut supposer que $b = 1$. Dans ce cas, $P, Q \in V_{f_{abc}} \iff y_i + ax_i + c = 0$. C'est-à-dire si $\widetilde{P} = (x_1, y_1), \widetilde{Q} = (x_2, y_2)$ sont sur la droite affine d'équation $Y + aX + c$. Alors, nécessairement, $a = -\dfrac{y_1 - y_2}{x_1 - x_2}$ et $c = -\dfrac{x_1y_2 - x_2y_1}{x_1 - x_2}$.

P,Q sont affines ($z_i = 1$) et $y_1 \neq y_2$: Idem en inversant les rôles de x et y : $X + bY + cZ = 0$ avec $b = -\dfrac{x_1 - x_2}{y_1 - y_2}$ et $c = -\dfrac{y_1x_2 - y_2x_1}{y_1 - y_2}$. On vérifie qu'il s'agit bien de la même droite que dans le cas $x_1 \neq x_2$ lorsque cette condition est aussi vérifiée.

P,Q sont affines ($z_i = 1$) et $x_1 - x_2 = y_1 - y_2 = 0$: Impossible puisque P, Q sont distincts.

P est affine et Q = O Alors nécessairement $b = 0$ puis $ax_1 + c = 0$ qui fixe complétement la droite (à multiplication près puisqu'on est en projectif). On peut par exemple prendre $X - x_1Z = 0$.
□

Proposition 2.1.7:

Soit E une courbe elliptique sur K donnée par l'équation de Weierstrass $Y^2 = X^3 + AX + B$. Soient $P = [x_1 : y_1 : 1], Q = [x_2 : y_2 : 1] \in E(K)$ affines distincts. Alors, il existe un unique point $R \in E \cap \mathcal{D}_{PQ}$ distinct de P, Q. Ce point est de plus K-rationnel et il est affine si et seulement si P et Q ne sont pas alignés verticalement (c'est-a-dire si $x_1 \neq x_2$).

Preuve :

Cas $x_1 \neq x_2$: Notons $P = [x_1 : y_1 : 1]$, $Q = [x_2 : y_2 : 1]$. Supposons qu'un tel point existe et notons $R = [x_3 : y_3 : z_3]$
D'après la preuve précédente (de la Proposition 2.1.6), on doit avoir $ax_3 + y_3 + cz_3 = 0$ avec $a = -\dfrac{y_1 - y_2}{x_1 - x_2}$ et $c = -\dfrac{x_1y_2 - x_2y_1}{x_1 - x_2}$.
En particulier, R doit être affine et, choisissant son représentant avec $z_3 = 1$, on doit avoir x_3 racine de $g = (aX + c)^2 - X^3 - AX - B$. Dans $\overline{K}$, ce polynôme se factorise en $(X - x_1)(X - x_2)(X - x_3)$ et, d'après les relations coefficients racines, $x_1 + x_2 + x_3 = a^2$ puis $x_3 = a^2 - (x_1 + x_2)$.
Ensuite, nécessairement, $y_3 = -ax_3 - c$.

Cas $x_1 = x_2$: Vu l'équation de Weierstrass, $y_1 = -y_2$ (P, Q distincts). En conséquence, l'équation de droite trouvée dans la preuve précédente (preuve de Proposition 2.1.6) donne $X - x_1Z = 0$. Si $R = [x_3 : y_3 : 1]$ est affine, alors $x_3 - x_1 = 0$. C'est-à-dire $x_3 = x_1$ et donc $R \in \{P, Q\}$. De plus O vérifie clairement l'équation et est par conséquent le troisième point cherché.

Le point obtenu est K-rationnel au vu de l'expression de ses coordonnées dans le premier cas et puisque O l'est dans le second.
□

Remarque 2.1.8:

Pour le cas $P = Q = [x_1 : y_1 : 1]$ avec $y_1 \neq 0$, par analogie avec le cas réel, on définit la pente de la tangente à la courbe en P par $a = \dfrac{3x_1^2 + A}{2y_1}$. L'équation de la tangente (affine) est $y = ax + b$ où $c = y_1 - ax_1$.
Comme précédemment, x_3 doit être racine de $g = X^3 + AX + B - (aX + c)^2$. On vérifie alors que x_1 en est racine double et que la dernière racine est $x_3 = m^2 - 2x_1$. On calcule alors $y_3 = ax_3 + b$. On considère que P est de multiplicité 2 et que R est le troisième point de $E \cap \mathcal{D}_{PP}$.

Si jamais $P = Q = [x_1 : 0 : 1]$, alors $\mathcal{D}_{PP}$ est d'équation $X - x_1Z$ et $[x_3 : y_3 : 1]$ est sur celle-ci si et seulement si $x_3 = x_1$. Mais alors $y_3^2 = x_1^3 + Ax_1 + B = y_1 = 0$ donc $y_3^2 = 0$ et à nouveau P est de multiplicité 2. De plus, O est clairement sur $\mathcal{D}_{PP}$ et il s'agit ainsi du troisième point.

Proposition 2.1.9:

Soit $P = [x_1 : y_1 : 1] \in E(K)$, alors il existe un unique point $R \in E \cap \mathcal{D}_{PO}$ distinct de P et O. Ce point est de plus K-rationnel et affine car donné par $[x_1 : -y_1 : 1]$.

Preuve :

Rappelons que l'équation de $\mathcal{D}_{PO}$ est $X - x_1 Z = 0$ (voir preuve de Proposition 2.1.6). Par conséquent, un point affine $R = [x_3 : y_3 : 1]$ vérifiera nécessairement $x_3 = x_1$. A fortiori, d'après l'équation de Weierstrass, $y_3^2 = y_1^2$ donc $y_3 = \pm y_1$. Le cas $y_3 = y_1$ donne P, l'autre donne R : le troisième point.
□

Remarque 2.1.10:

Pour le cas $P = O$, on utilise la carte $[x : 1 : z] \mapsto (x, z)$. Alors, l'équation de Weierstrass devient $BZ^3 + AXZ^2 - Z + X^3 = 0$ dont la tangente en $(0, 0)$ (qui correspond à O) est $Z = 0$. Injectant dans l'équation de Weierstrass, on obtient $X^3 = 0$ et O est le seul point de $\mathcal{D}_{OO}$. Il est de multiplicité 3.

Définition 2.1.11:

On définit une loi interne sur $E(K)$. Pour $P = [x_1 : y_1 : z_1], Q = [x_2, y_2, z_2]$: si $R = [x_3 : y_3 : z_3]$ est le troisième point de $E \cap \mathcal{D}_{PQ}$, $P + Q = [x_3 : -y_3 : z_3]$.

Proposition 2.1.12:

Ceci muni $E(K)$ d'une structure de groupe abélien de neutre O. L'inverse de $[x : y : z]$ est $[x : -y : z]$.

Preuve :

Toutes les expressions trouvées pour les différentes construction étant des fonctions rationnelles en des éléments de K, le point $P + Q$ est bien K-rationnel.

Vérifions que O est un neutre pour celle-ci. D'après la Proposition 2.1.9, si on note $P = [x_1 : y_1 : 1], Q = O = [0 : 1 : 0]$, alors $R = [x_1 : -y_1 : 1]$ donc $P + Q = [x_1 : y_1 : 1] = P$.

On ne détaille pas ici l'associativité. Il est possible de l'obtenir purement algébriquement en utilisant les formules trouvées pour les coordonnées de la somme de deux points. Il existe également une preuve utilisant le théorème de Riemann-Roch dans Silverman [13, III.3.4].

La commutativité est claire par construction (inverser P et Q ne change pas la droite obtenue pour construire R).

Reste à voir l'inverse.
Soient $P = [x : y : 1] \in E(K)$, $Q = [x : -y : 1]$. Notons $P + Q = [x' : -y' : z']$.

Si $y \neq 0$ **:** Alors $P \neq Q$ et, d'après la Proposition 2.1.7 $[x' : y' : z'] = O$ donc $P + Q = O$.

Si $y = 0$ **:** Alors, d'après la Remarque 2.1.8, $[x' : y' : z'] = O$ et $P + Q = O$.
□

2.2 Isogénies

Puisque nous avons ajouté une structure de groupe sur les courbes elliptiques, on voudrait une notion de morphisme qui préserve cette strucure en plus de la structure de courbe algébrique.

Définition 2.2.1: *Isogénie*

Soient $E_1/K, E_2/K$ deux courbes elliptiques. Une isogénie est un morphisme de courbe $\alpha : E_1 \to E_2$, surjectif et qui induit un morphisme de groupe $E_1(\overline{K}) \to E_2(\overline{K})$.

Une définition équivalente dans le cas des courbes elliptiques (pas dans le cadre général des variétés abéliennes) est :

Définition 2.2.2: *Isogénie bis*

Soient $E_1/K, E_2/K$ deux courbes elliptiques. Une isogénie est une application rationnelle $\alpha : E_1 \to E_2$, non constante et qui envoie le point à l'infini de E_1 sur celui de E_2.

L'équivalence de ces définitions découle des propriétés suivantes :

Propriétée 2.2.3:

- Tout morphisme de variétés abéliennes qui préserve le neutre induit un morphisme de groupe. Ceci est une application directe de Milne [9, I.1.2]. En effet, la translation mentionnée dans celui-ci est forcément l'identité lorsque le neutre est préservé.
- Tout morphisme de courbes projectives non constant est surjectif. (Hartshorne [6, I.6.8]).
- Une application rationnelle sur une courbe projective lisse, est un morphisme (Proposition 1.2.9).

Définition 2.2.4:

Soient $E_1/K, E_2/K$ des courbes elliptiques, soient $\alpha_1 : E_1 \to E_2$ et $\alpha_2 : E_2 \to E_1$ des isogénies. Si $\alpha_1 \circ \alpha_2 = \mathrm{id}_{E_2}$ et $\alpha_2 \circ \alpha_1 = \mathrm{id}_{E_1}$, on dit que α_1, α_2 sont des isomorphismes de courbes elliptiques et que E_1, E_2 sont isomorphes.

Remarque 2.2.5:

Dans la suite, un isomorphisme désignera toujours (hors précision) un isomorphisme de courbes elliptiques.

Exemple 2.2.6:

Considérons une courbe E/K donnée par l'équation de Weierstrass $Y^2 = X^3 + AX + B$.

Inverse L'application $[x : y : z] \mapsto [x : -y : z]$ qui à un point associe son inverse est une isogénie. En effet, il s'agit clairement d'une application rationnelle et $O \mapsto O$. De plus, elle est son propre inverse et est par conséquent un automorphisme.

Multiplication par 2 Au vu des calculs que nous avons faits précédemment, $P \mapsto P + P$ est clairement une application rationnelle. De plus, $O + O = O$ donc il s'agit bien d'une isogénie.

Proposition 2.2.7: *Frobenius*

Soient K un corps de caractéristique p et E/K est une courbe elliptique donnée par $Y^2 = X^3 + AX + B$. Pour toute puissance $q = p^n$, on appelle q-Frobenius l'application suivante :

$$\begin{aligned} \pi_n : E &\to E^{(q)} \\ [x : y : z] &\mapsto [x^q : y^q : z^q] \end{aligned}$$

où $E^{(q)}$ est la courbe donnée par l'équation $Y^2 = X^3 + A^q X + B^q$.
Alors, π_n est une isogénie.

Preuve :

Vérifions que π_n est bien définie. Soit $[x : y : z] \in E$, injectons $\pi_n(x : y : z)$ dans l'équation de $E^{(q)}$:

$$(y^q)^2 z^q - (x^q)^3 - A^q x^q (z^q)^2 - B^q (z^q)^3 = (y^2 z - x^3 - Axz^2 - Bz^3)^q = 0^q = 0$$

Par conséquent, π_n est bien définie.

Il s'agit clairement d'une application rationnelle non constante. Reste à voir l'image de $O : [0^q : 1^q : 0^q] = O$, il s'agit donc bien d'une isogénie.
□

2.2.1 Forme standard, degré et séparabilité

Pour la suite, nous allons montrer que l'on peut mettre toute isogénie sous une forme particulière que nous appellerons forme standard. Elle nous permettra de donner une autre caractérisation des notions de degré et séparabilité vu dans la Section 1.2.1.

Dans tout ce qui suit, on fixe deux courbes $E_1/K, E_2/K$ définies respectivement par les équations de Weierstrass $Y^2 = f_1(X)$ et $Y^2 = f_2(X)$.

Remarque 2.2.8:

Soit $\alpha = [\alpha_x : \alpha_y : \alpha_z] : E_1 \to E_2$ une isogénie. Puisque O est le seul point à l'infini de E_1 et que son image est nécessairement O, il suit que α est complètement caractérisé par l'application affine

$$\widetilde{\alpha}(X,Y) = \left(\frac{\alpha_x(X,Y,1)}{\alpha_z(X,Y,1)}, \frac{\alpha_y(X,Y,1)}{\alpha_z(X,Y,1)}\right)$$

En effet, $\left[\dfrac{\alpha_x(X,Y,1)}{\alpha_z(X,Y,1)} : \dfrac{\alpha_y(X,Y,1)}{\alpha_z(X,Y,1)} : 1\right]$ et $[\alpha_x : \alpha_y : \alpha_z]$ coïncident sur tous les points affines ou $\alpha_x, \alpha_y, \alpha_z$ sont définies et $\alpha_z \neq 0$: une infinité de points (Proposition 1.2.7).
De plus, soit $[x : y : 1] \in E(\overline{K})$, alors :

$$[x : y : 1] \in \ker \alpha \iff \alpha_z(x,y,1) = 0 \iff \frac{\alpha_y(X,Y,1)}{\alpha_z(X,Y,1)} \text{ à un pole en } (x,y)$$

En effet, si $\alpha_z(x,y,1) = 0$, alors l'équation de Weierstrass pour E_2 donne $\alpha_x(x,y,1) = 0$ et donc $\alpha_y(x,y,1) \neq 0$.
On appellera $\widetilde{\alpha}$ la forme affine de α. Dans la suite, on confondra souvent α et $\widetilde{\alpha}$.

Lemme 2.2.9:

Soit $\alpha : E_1 \to E_2$ une isogénie, alors on peut la mettre sous la forme affine $\alpha(X,Y) = \left(\dfrac{u(X)}{v(X)}, \dfrac{s(X)}{t(X)}y\right)$ avec $u, v, s, t \in K[X]$, $u \perp v$ et $s \perp t$.

Ici, $u \perp v$ désigne "u et v sont premiers entre eux".
Preuve :

Supposons que α soit donnée comme une application rationnelle $[\alpha_x : \alpha_y : \alpha_z]$, elle est alors complètement caractérisée par l'application affine $(r_1(X,Y), r_2(X,Y))$ où

$$r_1(X,Y) = \frac{\alpha_x(X,Y,1)}{\alpha_z(X,Y,1)} \quad \text{et} \quad r_2(X,Y) = \frac{\alpha_y(X,Y,1)}{\alpha_z(X,Y,1)}$$

Utilisant l'équation de Weierstrass donnant E_1 pour remplacer toute instance de Y^2 par $f_1(X)$, on peut supposer que le numérateur et le dénominateur de $r_1(X,Y)$ sont de degré 1 en Y et donc écrire $r_1(X,Y) = \dfrac{p_1(X) + p_2(X)Y}{p_3(X) + p_4(X)Y}$. Alors,

$$r_1(X,Y) = \frac{p_1(X) + p_2(X)Y}{p_3(X) + p_4(X)Y} \times \frac{p_3(X) - p_4(X)Y}{p_3(X) - p_4(X)Y} = \frac{q_1(X) + q_2(X)Y}{q_3(X)}$$

où on a à nouveau utilisé l'équation de Weierstrass pour simplifier le Y^2 du dénominateur.

Nous allons maintenant utiliser le fait que α est un morphisme de groupe : pour tout point $P \in E$, $\alpha(-P) = -\alpha(P)$ ce qui se traduit par

$$\begin{cases} r_1(X,-Y) = r_1(X,Y) \\ r_2(X,-Y) = -r_2(X,Y) \end{cases}$$

En particulier, $q_2(X) = 0$ et $r_1(X,Y) = \dfrac{q_1(X)}{q_3(X)}$. Divisant par $\gcd(q_1, q_3)$ on obtient la forme voulue.

Pour $r_2(X,Y)$, on procède de la même manière pour obtenir $r_2(X,Y) = \dfrac{\widetilde{q}_1(X) + \widetilde{q}_2(X)Y}{\widetilde{q}_3(X)}$. Cette fois, la condition donnée par le fait que α est un morphisme donne cette $q_1(X) = 0$. Divisant idem par le pgcd on obtient à nouveau la forme voulue.
□

Remarque 2.2.10:

Cette forme représente une isogénie comme un point $[\alpha_x : \alpha_y : \alpha_z] \in \mathbb{P}^2(K(E_1))$ tel que $\alpha_z = 1$. Par conséquent, α_x, α_y sont uniquement déterminés en tant qu'éléments de $k(E_1)$. Pour qu'ils soient complétement déterminés comme fractions rationnelles on demande de plus :

- Les numérateurs et dénominateurs de α_x doivent être homogènes de même degré (comme polynômes de $K[X,Z]$) et premiers entre eux dans $K[X,Z]$
- Les numérateurs et dénominateurs de α_y doivent être homogènes de même degré (comme polynômes de $K[X,Y,Z]$), premier entre eux dans $K[X,Y,Z]$. Le numérateur doit être de la forme $g(x,z)y$.

Si on suppose de plus que u, v, s, t sont unitaires alors ils sont aussi uniquement déterminés.

Définition 2.2.11:

On appelle cette forme la forme standard de l'isogénie α.

Proposition 2.2.12:

Gardant les notations précédentes, $v^3 | t^2$ et $t^2 | v^3 f_1$. De plus, v et t ont les mêmes racines dans $\overline{K}$.

Preuve :

Substituant les coordonnées de la forme standard dans l'équation de E_2 donne

$$\frac{s^2}{t^2}Y^2 = \frac{s^2}{t^2}f_1 = f_2\left(\frac{u}{v}\right) \implies v^3 s^2 f_1 = t^2 w$$

où on a posé $w = v^3 f_2(u/v)$, qui est un polynôme vu l'expression de f_2.
Puisque $t \perp s$, le lemme de Gauss donne $t^2 | v^3 f_1$.
De plus, $u \perp v$ implique $v \perp w$. En effet, si q est un diviseur irréductible de v, alors $w = Bv^3 + Auv^2 + u^3 = u^3 \mod q$. Or puisque $u \perp v$, q ne divise pas u donc $u \neq 0 \mod q$. En particulier, $w \neq 0 \mod q$ et q est premier avec w. Par conséquent, employant le lemme de Gauss, $v^3 | t^2$.

Puisque $v^3 | t^2$, toute racine de v est clairement racine de t. Soit maintenant x_0 une racine de t. Alors, x_0 est racine double de $v^3 f_1$. Mais puisque la courbe est non singulière, f_1 n'a que des racines simples et x_0 est racine de v.
□

Ceci nous donne une caractérisation intéressante du noyau de α :

Corollaire 2.2.13:

Toujours avec les mêmes notations, un point affine $[x_0 : y_0 : 1] \in E$ est dans le noyau de α si et seulement si x_0 est racine de v (ou de manière équivalente de t).

Preuve :

Si $v(x_0) \neq 0$, alors $t(x_0) \neq 0$ et $\alpha(x_0 : y_0 : 1) = \left[\dfrac{u(x_0)}{v(x_0)} : \dfrac{s(x_0)}{t(x_0)} : 1\right] \neq O$.
Par conséquent, $[x_0 : y_0 : 1] \in \ker \alpha \implies v(x_0) = 0$.

Réciproquement, supposons que $v(x_0) = 0$. Suivant la preuve de la surjectivité dans la preuve de la Re-

marque 1.1.35, on peut écrire α sous la forme projective :

$$\left[\frac{\widetilde{u}(X,Z)}{\widetilde{v}(X,Z)} : \frac{\widetilde{s}(X,Z)}{\widetilde{t}(X,Z)}Y : 1\right]$$

où $\widetilde{u}, \widetilde{v}, \widetilde{s}, \widetilde{t}$ sont les homogénéisés de u, v, s, t potentiellement multipliés par une puissance de Z.
En multipliant par $\widetilde{v}\widetilde{t}$ dans celle-ci on obtient :

$$\alpha = [\widetilde{u}\widetilde{t} : \widetilde{s}\widetilde{v}Y : \widetilde{v}\widetilde{t}]$$

où les trois coordonnées sont des polynômes homogènes de même degré.

Supposons $y_0 \neq 0$ **:** D'après la Proposition 2.2.12, $\widetilde{v}(x_0, 1) = v(x_0) = 0 \iff \widetilde{t}(x_0, 1) = t(x_0) = 0$ et puisque $v^3|t^2$, la multiplicité de $(x_0, 1)$ comme racine de $\widetilde{t}$ est strictement plus grande que sa multiplicité comme racine de $\widetilde{v}$.
Par conséquent, on peut normaliser par une puissance de $X - x_0Z$ de sorte que α_x et α_z s'annulent, mais pas α_y (on a également utilisé le fait que x_0 ne peut être racine de u et s). Ceci donne exactement $[x_0 : y_0 : 1] \in \ker \alpha$.
Pour normaliser on a utilisé l'équivalence suivante : pour $f \in K^{\hom}[X, Z]$, $f(x_0, 1) = 0 \iff X - x_0Z|f$. Le sens indirect est clair.
Pour le sens direct, on a $f(X, 1) = g(X)(X - x_0) + r$ avec $Q \in K[X]$ et $r \in K$. Mais alors, $0 = f(x_0, 1) = r$ donc $f(X, 1) = \text{dehom}(f) = g(X)(X - x_0)$ puis $f = X^{-v_i(f)}\text{hom}(\text{dehom}(f)) = X^{-v_i(f)}\text{hom}(g)(X - x_0Z)$. Il suit le sens direct.

Si maintenant $y_0 = 0$ **:** Alors, d'après l'équation de Weierstrass, $f_1(x_0) = 0$. Puisque la courbe est non singulière il s'agit d'une racine simple. On multiplie alors par YZ et on utilise l'équation de Weierstrass pour replacer Y^2Z par $f_1^*(X, Z)$ donnant

$$\alpha = [\widetilde{u}\widetilde{t}YZ : \widetilde{v}\widetilde{s}f_1^*(X, Z) : \widetilde{v}\widetilde{t}YZ]$$

Puisque, à nouveau, f_1 n'a que des racines simples et $v^3|t^2$, la multiplicité de $(x_0, 1)$ comme racine de $\widetilde{v}f_1^*$ est inférieure ou égale à sa multiplicité comme racine de t.
On conclut alors comme dans le cas précédent en utilisant de plus $Y|\alpha_x, Y|\alpha_z$ et $y_0 = 0$.

□

Grâce à ce corollaire, dès que l'on manipule une isogénie en forme standard, si on rencontre un point ou elle n'est pas définie, c'est nécessairement qu'il appartient au noyau et il n'y a pas besoin de faire plus de calculs. Cette forme permet donc de calculer facilement (au sens ou il n'y aura pas besoin de changer de représentant) la valeur d'une isogénie en un point.

On peut en tirer un résultat supplémentaire :

Corollaire 2.2.14:

Le noyau d'une isogénie $\alpha : E_1 \to E_2$ est un sous-groupe fini de $E_1(K)$

Preuve :

On met α sous forme standard avec les mêmes notations que précédemment.
Si $(x_0 : y_0 : 1)$ est un élément du noyau, alors x_0 est racine de v. Or, pour une coordonnée x_0 fixée, il y a au plus deux points affines ayant cette coordonnée (équation de degré 2 en y). Combinant ces deux affirmations, on a bien que le noyau est fini.
□

À partir de cette forme standard, on peut redéfinir les notions de degré et de séparabilité.

Définition 2.2.15:

Soit $\alpha : E_1 \to E_2$ une isogénie sous forme standard $\alpha = \left(\frac{u}{v}, \frac{s}{t}Y\right)$. Le degré de α est $\deg \alpha = \max\{\deg u, \deg v\}$. On dit que α est séparable si $\left(\frac{u}{v}\right)' \neq 0$.

Proposition 2.2.16:

Ces définitions sont équivalentes à celles données dans la Section 1.2.1

Preuve :

Pour le degré, Galbraith [5, 9.6.13].

Pour la séparabilité, on réalise un analogue de la preuve de Silverman [13, III.5.5].
La différentielle invariante est $\omega = \frac{dx}{2y}$ (Silverman [13, III.5 début]). Il est mentionné dans la preuve de Silverman [13, III.5.5] que $\alpha = (r_1(x), r_2(x)y)$ est séparable si et seulement si $\alpha^*\omega = 0$. Or,

$$\alpha^*\omega = \alpha^*\left(\frac{1}{2y}\right) d(\alpha^* x) = \frac{1}{2r_2(x)y} d(r_1(x))$$

Ceci vaut 0 si et seulement si $r_1'(x) = 0$ d'où l'équivalence des définitions
□

Exemple 2.2.17: *Frobenius*

Fixons $q = p^n$ et $E/\mathbb{F}_q$ une courbe elliptique donnée par $Y^2 = f(X)$. Étudions alors le q-Frobenius π_n.
En forme affine, celui-ci devient (X^q, Y^q). Utilisant l'équation de Weierstrass pour remplacer Y^2 par $f(X)$, on obtient la forme standard $(X^q, f(X)^{(q-1)/2}Y)$. On voit alors que π_n est inséparable de degré q.

Lemme 2.2.18:

Supposons que K est de caractéristique p et soit $\alpha : E_1 \to E_2$ une isogénie inséparable. Alors, on peut mettre α sous la forme affine

$$\widetilde{\alpha} = (a(X^p), b(X^p)Y^p)$$

pour des fractions rationnelles $a, b \in K(X)$.

Pour prouver cela, on énonce d'abord le lemme suivant :

Lemme 2.2.19:

Soient $u, v \in K[X]$ des polynômes premiers entre eux non tous deux constants. Alors :

- Si $\mathrm{car}(K) = 0$: $\left(\frac{u}{v}\right)' \neq 0$, en particulier toute isogénie est séparable.
- Si $\mathrm{car}(K) = p$: $\left(\frac{u}{v}\right)' = 0 \iff u' = v' = 0 \iff u = \widetilde{u}(X^p)$ et $v = \widetilde{v}(X^p)$ pour $\widetilde{u}, \widetilde{v} \in K[X]$

Preuve :

Rappelons d'abord que $\left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2}$ donc $\left(\frac{u}{v}\right)' = 0 \iff u'v = v'u$.

Caractéristique 0 : Si $u'v = v'u$, puisque $u \perp v$, le lemme de gauss donne $v | v'$. Or, c'est impossible puisque v' est non nul.

Caractéristique p : Si c'est le cas, alors comme ci-dessus $v|v'$ et $u|u'$ ce qui n'est possible que si $u' = v' = 0$. Or, ceci implique que $u = \widetilde{u}(X^p)$ et $v = \widetilde{v}(X^p)$ pour des polynômes $\widetilde{u}, \widetilde{v} \in K[X]$. Enfin, utilisant ces expressions dans le quotient initial et calculant la dérivée on trouve bien 0 ce qui termine l'équivalence.
□

On peut maintenant prouver le Lemme 2.2.18 :
Preuve :

Considérons la forme standard $\alpha(X,Y) = \left(\frac{u(X)}{v(X)}, \frac{s(X)}{t(X)}Y\right)$

Au vu du Lemme 2.2.19 et puisque α est supposé inséparable, on a clairement $\frac{u(X)}{v(X)} = a(X^p)$. Il faut donc montrer que $\frac{s(X)}{t(X)}Y$ peut se mettre sous la forme $b(X^p)Y^p$.

Comme dans la preuve de la Proposition 2.2.12, on met les coordonnées de α dans l'équation de Weierstrass et on obtient $v^3s^2f_1 = t^2w$ avec $w = v^3f_2\left(\frac{u}{v}\right) \in K[X]$. Puisque α est inséparable $u' = v' = 0$ donc $w' = 0$ et $(w/v^2)' = (s^2f_1/t^2)' = 0$.
Par conséquent, $s(X)^2f_1(X) = g(X^p)$ et $t(X)^2 = h(X^p)$ pour des polynômes $g, h \in K[X]$.

Soit x_0 une racine de f_1. Alors, x_0^p est racine de g. A fortiori, $(X - x_0^p)|g$ puis $(X^p - x_0^p) = (X - x_0)^p$ divise $g(X^p)$.
Puisque f_1 est à racines simples, $f_1(X)^p|g(X^p)$. Or, $f_1(X)^p$ est un polynôme en X^p (puisque le Frobenius est un morphisme) donc $g(X^p) = g_1(X^p)f_1(X)^p$ puis $s(X)^2f_1(X) = g_1(X^p)f_1(X)^p$ et $s(X)^2 = g_1(X^p)f_1(X)^{p-1}$.

Rappelons que p est impair donc $p-1$ est pair et f_1^{p-1} n'a que des facteurs irréductibles de multiplicités paires. Idem pour s^2 et donc également pour $g_1(X^p)$. Il suit que $g_1(X^p)$ est un carré. Notons $g_1(X^p) = h_1(X)^2$. Alors, $(g_1(X^p))' = (h_1^2)' = 2h_1h_1' = 0$ car $g_1(X^p)$ est un polynôme en X^p. A fortiori, $h_1' = 0$ et $h_1 = g_2(X^p)$.
Utilisant l'équation de Weierstrass, on obtient maintenant que

$$(s(X)Y)^2 = s(X)^2f_1(X) = g_2(X^p)^2f_1(X)^p = (g_2(X^p)Y^p)^2$$

ce qui permet d'écrire $\left(\frac{s(X)}{t(X)}Y\right)^2 = (r(X^p)Y^p)^2$ où $r = g_2/h$. On a donc $\frac{s(X)}{t(X)}Y = b(X^p)Y^p$ avec $b = \pm r$ ce qui conclut.
□

Corollaire 2.2.20:

Toujours pour $\mathrm{car}(K) = p$, on peut écrire toute isogénie α comme

$$\alpha = \alpha_{\mathrm{sep}} \circ \pi^n$$

avec α une isogénie séparable, $n \in \mathbb{N}$, et $\pi : (x : y : z) \mapsto (x^p : y^p : z^p)$ le p-Frobenius.
De plus, $\deg \alpha = p^n \deg \alpha_{\mathrm{sep}}$

Preuve :

Le cas α séparable est clair avec $n = 0$ et $\alpha_{\mathrm{sep}} = \alpha$.
Supposons que α n'est pas séparable. D'après le Lemme 2.2.18, on peut mettre α sous la forme affine $\alpha(X,Y) = (a(X^p), b(X^p)Y^p)$ et alors $\alpha = \alpha_1 \circ \pi$ avec $\alpha_1 = (a, bY)$.

Ici, α_1 est une isogénie. En effet, il s'agit bien d'une application rationnelle et $O = \alpha(O) = \alpha_1(O^p) = \alpha_1(O)$.
Si elle est séparable, on a bien la forme voulue. Sinon, on lui réapplique le même raisonnemment.
Ce procédé termine bien puisque le degré diminue à chaque étape d'un facteur p.
Disons que ceci termine sur $\alpha_{\mathrm{sep}} := \alpha_n = \left(\frac{u}{v}, \frac{s}{t}Y\right)$, alors $\alpha(X,Y) = \left(\frac{u(X^{p^n})}{v(X^{p^n})}, \frac{s(X^{p^n})}{t(X^{p^n})}Y^{p^n}\right)$ de degré $p^n \deg \alpha_{\mathrm{sep}}$.
□

Théorème 2.2.21:

Soit $\alpha = \alpha_{\mathrm{sep}} \circ \pi^n$ une isogénie. Alors, son noyau a pour cardinal $\#\ker\alpha = \deg\alpha_{\mathrm{sep}}$.

Preuve :

Puisque
$$\pi(x,y,z) = O \iff (x^p : y^p : z^p) = (0:1:0) \iff x, z = 0$$
on a que $\ker\alpha = \ker\alpha_{\text{sep}}$. On peut donc se restreindre au cas ou α est séparable.

Mettons α sous forme standard : $\alpha(X,Y) = \left(\frac{u(X)}{v(X)}, \frac{s(X)}{t(X)}Y\right)$. Soit alors un point $(a:b:1) \in \alpha(E_1(\overline{K}))$ avec $a, b \neq 0$ et $a \neq \frac{\text{dom}(u)}{\text{dom}(v)}$. Un tel point existe puisque $\alpha(E_1(\overline{K})) = E_2(\overline{K})$ est infini (Proposition 1.1.36). Considérons l'ensemble

$$S(a,b) = \{(x:y:1) \in E_1(\overline{K}) \mid \alpha(x:y:1) = (a:b:1)\}$$

Puisque α est un morphisme de groupes, $\#S(a,b) = \#\ker\alpha$. Soient $(x,y) \in S(a,b)$, alors

$$\frac{u(x)}{v(x)} = a, \qquad \frac{s(x)}{t(x)}y = b$$

Puisque α est non nulle en (x,y), on doit avoir $v(x), t(x) \neq 0$ (Corollaire 2.2.13). Puisque $b \neq 0$, on doit avoir $s(x) \neq 0$. Il suit que $y = \frac{t(x)}{s(x)}b$ est uniquement déterminé par le choix de x.
Il suffit donc de compter le nombre de valeurs de x qui apparaissent dans $S(a,b)$.

Notons $g = u - av$ de sorte que $\alpha\left(x, \frac{t(x)}{s(x)}b\right) = (a,b) \iff g(x) = 0$. Vu notre choix de a, on doit avoir $\deg(g) = \deg\alpha$. On cherche donc le nombre de racines distinctes de g.
Or, x est racine multiple de g si et seulement si $g(x) = g'(x) = 0$. C'est-a-dire $av(x) = u(x)$ et $av'(x) = u'(x)$. Multipliant ces deux conditions entre elles donne $u'(x)v(x) = v'(x)u(x)$.

Puisque α est séparable, $u'v - v'u$ est non nul donc possède un nombre fini de racines. Or, $S(a,b)$ est fini donc on peut supposer que notre choix initial de (a,b) est tel que $uv' - v'u$ ne s'annule pas sur $S(a,b)$. Alors, g est à racines simples donc $\#\ker\alpha = \#S(a,b) = \deg g = \deg\alpha$ ce qui conclut.
□

Définition 2.2.22:
On appelle degrés séparables et inséparables de α les quantités $\deg_s\alpha = \deg\alpha_{\text{sep}}$ et $\deg_i\alpha = p^n$. On a $\deg\alpha = (\deg_s\alpha)(\deg_i\alpha)$

Remarque 2.2.23:
- Cette notion de degré séparable correspond à celle de la Définition 1.2.12 (Silverman [13, III.4.10.a] ; en effet, l'auteur définit le degré séparable de la même manière que la Définition 1.2.12)
- Elle est bien défini puisque si $\alpha = \beta\circ\pi^n = \gamma\circ\pi^m$ avec β, γ séparables, alors $\deg\beta = \deg\gamma = \#\ker\alpha$. De plus, $\deg\alpha = p^n\deg\beta = p^m\deg\gamma$ donc $n = m$.

Corollaire 2.2.24:
Pour tout triplet d'isogénies β, γ et $\alpha = \beta\circ\gamma$, on a :
$$\deg\alpha = (\deg\beta)(\deg\gamma), \qquad \deg_s\alpha = (\deg_s\beta)(\deg_s\gamma), \qquad \deg_i\alpha = (\deg_i\beta)(\deg_i\gamma)$$

Preuve :

Les deux dernières égalités impliquent la première, il suffit donc de les démontrer.
Puisque γ est un morphisme surjectif, $\#\ker\alpha = (\#\ker\beta)(\#\ker\gamma)$. En effet, $\ker\alpha = \bigcup_{y\in\ker\beta}\gamma^{-1}(y)$ avec les $\gamma^{-1}(y)$ tous non vides (γ surjectif) et de cardinal $\#\ker\gamma$ (γ morphisme).
Ceci, donne d'après le Théorème 2.2.21, que $\deg_s\alpha = (\deg_s\beta)(\deg_s\gamma)$.
Utilisant le Corollaire 2.2.20 :
$$\alpha_{\text{sep}}\circ\pi^a = \beta_{\text{sep}}\circ\pi^b\circ\gamma_{\text{sep}}\circ\pi^c$$
Considérons l'isogénie $\delta = \pi^b\circ\gamma_{\text{sep}}$, celle-ci a le même noyau et donc le même degré séparable que γ_{sep}. On

peut donc l'écrire $\delta_{\text{sep}} \circ \pi^d$ avec $\deg \delta_{\text{sep}} = \deg \gamma_{\text{sep}}$. Or,

$$\begin{cases} \deg \delta = \deg(\pi^b \circ \gamma_{\text{sep}}) = p^b \deg \gamma_{\text{sep}} \\ \deg \delta = \deg(\delta_{\text{sep}} \circ \pi^d) = p^d \deg \delta_{\text{sep}} \end{cases}$$

donc $d = b$ et

$$\alpha_{\text{sep}} \circ \pi^a = \beta_{\text{sep}} \circ \delta_{\text{sep}} \circ \pi^{bc}$$

Mais alors, puisque une composition d'isogénies séparables est séparable (d'après la dérivée d'une composée), $\deg_i \alpha = a = bc = \deg_i \beta \deg_i \gamma$.
□

Lemme 2.2.25:

Gardant les mêmes notations, α est séparable si et seulement si $\deg_i \alpha = 1$

Preuve :

Sens direct : Par contraposée, si $\deg_i \alpha > 1$, alors d'après le Corollaire 2.2.20 $\alpha = \alpha_{\text{sep}} \circ \pi^k$ avec $k > 0$. Notant $\alpha_{\text{sep}} = (r_1(X), r_2(X)Y)$ en forme standard, on a

$$\alpha = \left(r_1\left(X^{p^k}\right), r_2\left(X^{p^k}\right) Y^{p^k}\right) = \left(r_1\left(X^{p^k}\right), r_2\left(X^{p^k}\right) f_1(X)^{(p^k-1)/2} Y\right)$$

en forme standard.
Immédiatement, α est inséparable.
Sens indirect : Par contraposé à nouveau, application directe du Lemme 2.2.18
□

Lemme 2.2.26:

Une somme d'isogénies inséparables est inséparable.

Preuve :

Soient $\alpha, \beta : E \to E'$ des isogénies inséparables. Alors, appliquant le Corollaire 2.2.20, on peut écrire $\alpha = \alpha_{\text{sep}} \circ \pi^a$ et $\beta = \beta_{\text{sep}} \circ \pi^b$ avec $a, b > 1$. On suppose quitte a échanger α et β que $a \geq b$
Mais alors, $\alpha + \beta = \underbrace{(\alpha_{\text{sep}} \circ \pi^{a-b} + \beta_{\text{sep}})}_{\gamma} \circ \pi^b$.
Appliquant à nouveau le Corollaire 2.2.20, $\gamma = \gamma_{\text{sep}} \circ \pi^c$ avec $c \geq 0$.
Finalement, $\alpha + \beta = \gamma_{\text{sep}} \circ \pi^{a-b+c}$ est inséparable puisque $a - b + c \geq a - b > 0$.
□

2.2.2 Multiplication par n et torsion

On va maintenant étudier l'application de multiplication par n. On fixe dans la suite un entier $n \in \mathbb{N}^*$.

Proposition 2.2.27:

Soit E/K une courbe elliptique et considérons l'application

$$\begin{aligned} [n] : E &\to E \\ P &\mapsto [n]P = \underbrace{P + \cdots + P}_{n \text{ fois}} \end{aligned}$$

Alors, $[n]$ est une isogénie.

Preuve :

Il faut tout d'abord montrer que $[n]$ est une application rationnelle. Pour cela, on procède par récurrence sur n.
Clairement [1] en est une (c'est l'identité). Supposons que $[n]$ en soit une, alors $[n+1]P = [n]P + P$ et, puisque $[n]$ est rationnelle, les coordonnées de $[n]P$ sont données par une application rationnelle en les coordonnées de P. Mais alors, sachant que les coordonnées de la somme de deux points sont rationnelles en les coordonnées des points sommés, on a bien que $[n+1]$ est une application rationnelle.

Reste à vérifier que $[n]O = O$, or c'est clairement le cas.
□

Définition 2.2.28:

On note $E[n] = \ker[n]$ le noyau de cette isogénie et on l'appelle le sous-groupe de n-torsion.

Proposition 2.2.29:

L'isogénie $[n]$ est de degré n^2, elle est séparable si et seulement si $\mathrm{car}(K) \nmid n$.

Nous ne prouverons pas ce résultat car très calculatoire. On peut en trouver une preuve dans Sutherland [16].

Dans la suite de cette Section 2.2.2, on suppose que K est de caractéristique p.

Théorème 2.2.30:

Pour tout nombre premier l et tout entier $e \in \mathbb{N}^*$:

$$E[l^e] \simeq \begin{cases} \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z} & \text{si } l \neq p \\ \mathbb{Z}/l^e\mathbb{Z} \text{ ou } \{0\} & \text{si } l = p \end{cases}$$

Preuve :

Supposons $l \neq p$: On sait (Proposition 2.2.29) qu'alors $[l]$ est séparable et $\#E[l] = \deg_s[l] = \deg[l] = l^2$. Les seuls groupes abéliens de ce cardinal sont $\mathbb{Z}/l^2\mathbb{Z}$ et $(\mathbb{Z}/l\mathbb{Z})^2$. Puisque, par définition, tous les éléments de $E[l]$ sont d'ordre l, $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

Puisque $E[l^e]$ est un l-groupe abélien fini (de cardinal l^{2e}), on peut écrire $E[l^e] = \langle P_1\rangle \times \cdots \times \langle P_n\rangle$ où les $P_i \in E(\overline{K})$ sont des points d'ordres divisant l^{2e}, c'est-à-dire que P_i a ordre l^{e_i}.

Mais alors, $E[l] \simeq \prod_i \langle l^{e_i-1}P_i\rangle$.
En effet, si $Q = (a_1 l^{e_1-1}P_1, \ldots, a_n l^{e_n-1}P_n) \in \prod \langle l^{e_i-1}P_i\rangle$, alors $lQ = (O, \ldots, O)$ et donc $Q \in E[l]$. Réciproquement, si $Q \in E[l] \subset E[l^e]$, alors $Q = (b_1P_1, \ldots, b_nP_n)$ et $(O, \ldots, O) = lQ = (lb_1P_1, \ldots, lb_nP_n)$ donc $l^{e_i} | lb_i$ puis $l^{e_i-1} | b_i$ et $Q_i \in \langle l^{e_i-1}P_i\rangle$.

Or, $\langle l^{e_i-1}P_i\rangle \simeq \mathbb{Z}/l\mathbb{Z}$ et $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$ donc $n = 2$ et $E[l^e] \simeq \langle P_1\rangle \times \langle P_2\rangle$. Puisque les éléments de $E[l^e]$ dont d'ordre au plus l^e et que $E[l^e]$ est de cardinal l^{2e}, il suit que $E[l^e] \simeq (\mathbb{Z}/l^e\mathbb{Z})^2$

Supposons $l = p$: Alors, $l^2 = \deg[l] = (\deg_s[l])(\deg_i[l])$ et $\deg_i[l] \neq 0$. Il faut alors distinguer deux cas :
- $\deg_i[l] = l^2$: $\deg_s[l] = 1$ et $E[l] \simeq \{0\}$. Alors, $E[l^e] = \{0\}$.
- $\deg_i[l] = l$: $\deg_s[l] = l$ et $E[l] \simeq \mathbb{Z}/l\mathbb{Z}$. Alors, procédant comme pour le cas précédent, $E[l^e] \simeq \prod \langle P_i\rangle$ puis $E[l] \simeq \prod \langle l^{e_i-1}P_i\rangle \simeq (\mathbb{Z}/l\mathbb{Z})^n$ donc $n = 1$ et $E[l^e] \simeq \mathbb{Z}/l^{e_1}\mathbb{Z}$.
  Finalement, $\#E[l^e] = \deg_s[l^e] = (\deg_s[l])^e = l^e$ donc $E[l] \simeq \mathbb{Z}/l^e\mathbb{Z}$

□

De ce résultat, on tire une définition :

Définition 2.2.31:

Soit E/K une courbe elliptique telle que $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Alors E est dite ordinaire. Sinon ($E[p] \simeq \{0\}$), E est dite supersingulière.

Remarque 2.2.32:

Il existe de nombreuses définitions équivalentes de la supersingularité d'une courbe elliptique. On peut par exemple citer la Proposition 3.2.5.

Lemme 2.2.33:

Pour toute isogénie $\alpha : E_1 \to E_2$, pour tout entier $n \in \mathbb{N}^*$, $\alpha \circ [n] = [n] \circ \alpha$.

Preuve :

> Puisque α est un morphisme de groupes, cette identité tient en tous points de E_1. Alors, la Proposition 1.2.7 conclut.
> □

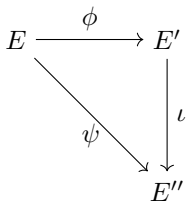
2.2.3 Isogénie associée à un noyau

Clairement, le noyau d'une isogénie est un sous-groupe de $E_1(\overline{K})$. On voudrait maintenant savoir si la réciproque est vraie aussi. C'est-à-dire de savoir si, étant donné un sous-groupe fini de $E_1(\overline{K})$, il est possible de trouver une isogénie dont c'est le noyau.

La réponse est oui, on a même une notion d'unicité :

Théorème 2.2.34:

Soit E/K une courbe elliptique et G un sous-groupe fini de $E(\overline{K})$. Alors, il existe une courbe elliptique E' et une isogénie séparable $\phi : E \to E'$ telle que $\ker \phi = G$. La courbe E' et l'isogénie ϕ sont définies sur une extension finie de K et sont uniques au sens suivant :
Si $\psi : E \to E''$ est une autre isogénie avec les mêmes propriétés, il existe un isomorphisme $\iota : E' \to E''$ tel que le diagramme suivant commute :



Si G est invariant sous l'action de $\mathrm{Aut}_K(\overline{K})$, alors il est possible d'obtenir ϕ et E' définies sur K (Silverman [13, III.4.14]).

Preuve : Silverman [13, III.4.12].

Proposition 2.2.35:

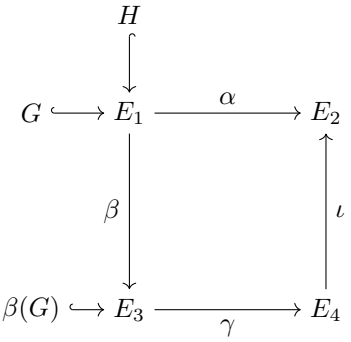
Toute isogénie de degré composé peut s'écrire comme composition d'isogénies de degrés premiers.

Preuve :

> Soit $\alpha : E_1 \to E_2$ une isogénie de degré n. Si on est en caractéristique 0, α est séparable. Sinon, $\alpha = \alpha_{\mathrm{sep}} \circ \pi^r$. Or $\pi^r = \pi \circ \cdots \circ \pi$ est une composition d'isogénies de degrés premiers (p) donc il suffit de vérifier la proposition pour α_{sep}. On suppose par conséquent que α est séparable.
>
> Fixons un nombre premier l divisant n et notons $G = \ker \alpha$. Puisque G est un groupe fini d'ordre n, le théorème de Cauchy donne l'existence d'un sous-groupe $H \subset G$ d'ordre l.
>
> Mais alors, il existe une isogénie séparable $\beta : E_1 \to E_3$ telle que $\ker \beta = H$ et $\deg \beta = \deg_s \beta = \# \ker \beta = \#H = l$.
>
> Considérons maintenant le sous-groupe fini $\beta(G) \subset E_3(\overline{K})$. À nouveau, il existe une isogénie séparable $\gamma : E_3 \to E_4$ telle que $\ker \gamma = \beta(G)$.
>
> Intéressons-nous à la composition $\gamma \circ \beta$. Pour tout $P \in E_1(\overline{K})$:

$$P \in \ker \gamma\circ\beta \iff \beta(P) \in \beta(G) \iff \exists Q \in G \text{ t.q. } \beta(P) = \beta(Q) \iff \exists Q \in G \text{ t.q. } P-Q \in H \iff P \in G$$

On a donc que $\ker \beta \circ \gamma = G$ et, par le Théorème 2.2.34, il existe un isomorphisme $\iota : E_4 \to E_2$ tel que $\iota \circ \gamma \circ \beta = \alpha$.
Les constructions précédentes sont présentées dans le diagramme commutatif ci-dessous (les injections sont placées de sorte à montrer quel sous-groupe est noyau de quelle isogénie).



Or $\deg(\iota \circ \gamma \circ \beta) = \deg(\iota \circ \gamma)\deg(\beta) = \deg(\gamma)p$ et $\deg(\iota \circ \gamma \circ \beta) = \deg \alpha = n$ donc γ est une isogénie de degré n/l. Répétant le processus, on décompose complétement α.

□

Corollaire 2.2.36:

Soit $\alpha : E_1 \to E_2$ une isogénie. Alors α est un isomorphisme si et seulement si elle est de degré 1.

Preuve :

Supposons que α est un isomorphisme : Alors, $1 = \deg \mathrm{id}_{E_2} = \deg(\alpha \circ \alpha^{-1}) = (\deg \alpha)(\deg \alpha^{-1})$. Par conséquent, α et α^{-1} sont de degré 1.
Supposons que α est de degré 1 : Puisque $\deg \alpha = 1$, $\# \ker \alpha = \deg_s \alpha = 1$. De plus, $\deg_i \alpha = 1$ donc α est séparable (Lemme 2.2.25).
Or, id est une isogénie séparable de noyau $\{0\}$ (donnée par (x, y) en forme standard). Le Théorème 2.2.34 donne alors l'existence d'un isomorphisme $\iota : E_2 \to E_1$ tel que $\iota \circ \alpha = \mathrm{id}$ et donc α est un isomorphisme.
□

2.2.4 Isogénie duale

Le but de cette section est de démontrer le théorème suivant et d'étudier quelques propriétés de l'isogénie duale :

Théorème 2.2.37:

Pour toute isogénie $\alpha : E_1 \to E_2$ de degré n, il existe une unique isogénie $\widehat{\alpha} : E_2 \to E_1$ telle que $\widehat{\alpha} \circ \alpha = [n]$.
On appelle $\widehat{\alpha}$ l'isogénie duale de α.

Pour prouver ce théorème, il nous faut d'abord démontrer le lemme suivant. Il nous sera par ailleurs utile à de nombreuses reprises.

Lemme 2.2.38: *Simplification*

Soient $\delta : E_0 \to E_1,\ \alpha, \beta : E_1 \to E_2,\ \gamma : E_2 \to E_3$ des isogénies. Alors,

$$\alpha \circ \delta = \beta \circ \delta \implies \alpha = \beta$$
$$\gamma \circ \alpha = \gamma \circ \beta \implies \alpha = \beta$$

Preuve :

Puisque les isogénies sont surjectives, γ, δ sont en particulier non nulles. Mais alors,

$$\alpha \circ \delta = \beta \circ \delta \implies \alpha \circ \delta - \beta \circ \delta = (\alpha - \beta) \circ \delta = 0 \implies \alpha - \beta = 0$$
$$\gamma \circ \alpha = \gamma \circ \beta \implies \gamma \circ \alpha - \gamma \circ \beta = 0 \implies \gamma \circ (\alpha - \beta) = 0 \implies \alpha - \beta = 0$$

On a utilisé deux choses :

— La composition se distribue sur l'addition car les relations sont vérifiées points par points (puisqu'on manipule des morphismes de groupes)

— La composition de deux morphismes surjectif est surjective et donc non nulle ce qui donne la dernière implication.

□

On peut maintenant prouver le Théorème 2.2.37 :
Preuve :

Commençons par l'unicité. S'il existe deux isogénies duales α_1, α_2, alors $\alpha_1 \circ \alpha = [n] = \alpha_2 \circ \alpha$ et le Lemme 2.2.38 donne $\alpha_1 = \alpha_2$.

Montrons maintenant l'existence, pour cela on procède par récurrence sur le nombre m de facteurs premiers de n, comptés avec multiplicité.
Réalisons d'abord l'étape de récurrence. Supposons que toute isogénie dont le degré a au plus m facteurs ait une isogénie duale. Soit α une isogénie de degré n tel que n ait $m+1$ facteurs. Alors, utilisant la Proposition 2.2.35, on peut écrire $\alpha = \alpha_1 \circ \alpha_2$ avec α_1 et α_2 ayant des degrés avec au plus m facteurs premiers. Elles ont donc des duales par hypothèse de récurrence. Posons alors $\widehat{\alpha} = \widehat{\alpha}_2 \circ \widehat{\alpha}_1$ et vérifions

$$\begin{aligned}\widehat{\alpha} \circ \alpha &= \widehat{\alpha}_2 \circ \widehat{\alpha}_1 \circ \alpha_1 \circ \alpha_2 \\ &= \widehat{\alpha}_2 \circ [\deg \alpha_1] \circ \alpha_2 \\ &= \widehat{\alpha}_2 \circ \alpha_2 \circ [\deg \alpha_1] \\ &= [\deg \alpha_2] \circ [\deg \alpha_1] = [\deg \alpha_2 \deg \alpha_1] = [n]\end{aligned}$$

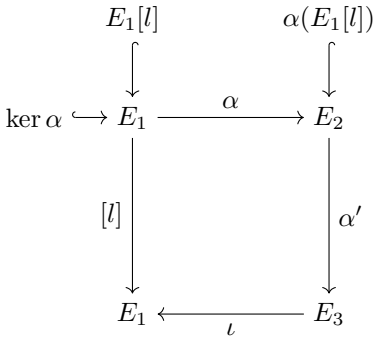
Dans le cas $m = 0$, c'est-à-dire α de degré 1 (car α de degré 0 ne peut être surjective), le Corollaire 2.2.36 donne que α est un isomorphisme. Considérant sa réciproque $\widehat{\alpha}$, on a bien $\widehat{\alpha} \circ \alpha = [1]$.

Reste l'étape $m = 1$. Soit donc α une isogénie de degré premier l, dans le cas ou le corps K est de caractéristique non nulle, on note sa caractéristique p.

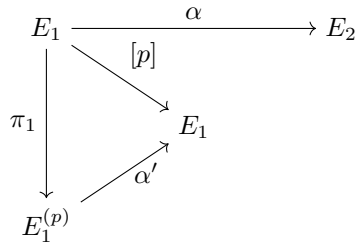
Cas $l \neq p$: Alors, α et $[l]$ sont séparables. En particulier $\#\ker \alpha = \deg \alpha$ et $\#\ker[l] = \deg l = l^2$. Il suit que $\alpha(E_1[l])$ est un sous-groupe de $E_2(\overline{K})$ de cardinal $l^2/l = l$.
Soit alors $\alpha' : E_2 \to E_3$ l'isogénie séparable de noyau $\alpha(E_1[l])$. Alors,

$$P \in \ker \alpha' \circ \alpha \iff \alpha(P) \in \alpha(E_1[l]) \iff \exists Q \in E_1[l] \text{ t.q. } P - Q \in \ker \alpha$$

Or $\#\ker \alpha = l$ donc par le théorème de Lagrange $\ker \alpha \subset E_1[l]$ et $\ker \alpha' \circ \alpha = E_1[l]$. Par conséquent (Théorème 2.2.34), il existe un isomorphisme $\iota : E_3 \to E_1$ tel que $\underbrace{\iota \circ \alpha'}_{\widehat{\alpha}} \circ \alpha = [l]$.
On résume cela sur le diagramme ci-dessous (ou les injections sont placés de manière à montrer quel sous-groupe est noyau de quelle isogénie).



Cas $l = p$ et α séparable : Puisque α est séparable, son noyau est de cardinal p et par Lagrange $\ker\alpha \subset E_1[p]$. D'après le Théorème 2.2.30, $E_1[p] \simeq \mathbb{Z}/p\mathbb{Z}$ ou $\{0\}$ donc ici $\ker\alpha = E_1[p] \simeq \mathbb{Z}/p\mathbb{Z}$. A fortiori, $\deg_s[p] = \#E_1[p] = p$.
Or, $\deg[p] = p^2$ donc $[p] = \alpha' \circ \pi_1$ pour $\alpha' : E_1^{(p)} \to E_1$ une isogénie séparable de degré p et $\pi_1 : E_1 \to E_1$ le p-Frobenius.
On a le diagramme suivant :



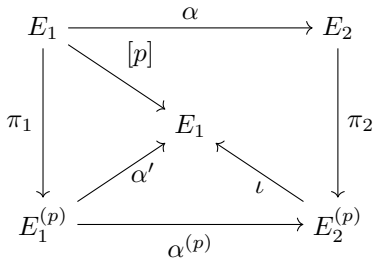
De plus, $\pi_2 \circ \alpha = \alpha^{(p)} \circ \pi_1$ où $\alpha^{(p)} : E_1^{(p)} \to E_2^{(p)}$ est l'isogénie obtenue en remplaçant les coefficients de α par leur puissance p-ième. Cette dernière est séparable puisque

$$\begin{cases} \deg_i(\alpha^{(p)} \circ \pi_1) = p \deg_i(\alpha^{(p)}) = p \\ \deg_i(\alpha^{(p)} \circ \pi_1) = \deg_i(\pi_2 \circ \alpha) = p \deg_i \alpha \end{cases} \implies \deg_i \alpha^{(p)} = 1$$

.
Alors,

$$\ker\alpha^{(p)} = \ker\alpha^{(p)} \circ \pi_1 = \ker\pi_2 \circ \alpha = \ker\alpha = \ker[p] = \ker\alpha' \circ \pi_1 = \ker\alpha'$$

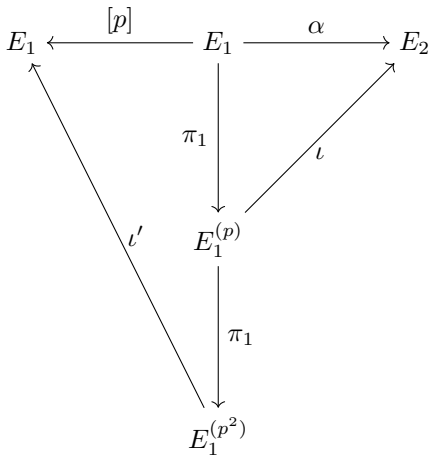
Par conséquent, $\alpha' : E_1^{(p)} \to E_1$ et $\alpha^{(p)} : E_1^{(p)} \to E_2^{(p)}$ sont séparables de même noyau et il existe un isomorphisme $\iota : E_2^{(p)} \to E_1$ tel que $\alpha' = \iota \circ \alpha^{(p)}$.
On complète alors le diagramme précédent :



Finalement, $\underbrace{\iota \circ \pi_2}_{\widehat{\alpha}} \circ \alpha = \iota \circ \alpha^{(p)} \circ \pi_1 = \alpha' \circ \pi_1 = [p]$

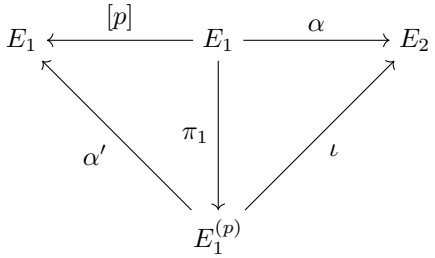
Cas $l = p$ et α n'est pas séparable : Puisque α est de degré premier, $\deg_s \alpha = 1$ et $\alpha = \iota \circ \pi$ pour un isomorphisme $\iota : E_1^{(p)} \to E_2$. Précisons que ι est un isomorphisme par le Corollaire 2.2.36 : $\deg_s \iota = 1$ et ι est séparable donc $\deg_i \iota = 1$ puis $\deg \iota = 1$.
Il y a deux sous-cas :

— Si $E[p] = \{0\}$: alors $[p]$ est idem de la forme $\iota' \circ \pi^2$ pour $\iota : E_1^{(p^2)} \to E_1$ un isomorphisme. On est alors dans la situation du diagramme ci-dessous



Il suit $\underbrace{\iota' \circ \pi_1 \circ \iota^{-1}}_{\widehat{\alpha}} \circ \alpha = \iota' \circ \pi_1 \circ \pi_1 = [p]$

— Si $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$: alors $[p] = \alpha' \circ \pi$ pour $\alpha' : E_1^{(p)} \to E_1$ une isogénie séparable de degré p. On est alors dans la situation suivante :



Il suit $\underbrace{\alpha' \circ \iota^{-1}}_{\widehat{\alpha}} \circ \alpha = \alpha' \circ \pi_1 = [p]$

Ceci termine le cas $m = 1$ et par conséquent la preuve.
□

Il est utile d'étendre la notion d'isogénie duale au morphisme nul en posant $\widehat{[0]} = [0]$.

Définition 2.2.39:

Soient $E_1/K, E_2/K$ des courbes elliptiques et L/K une extension algébrique. On note

$$\mathrm{Hom}_L(E_1, E_2) = \{[0]\} \cup \{\alpha \mid \alpha : E_1 \to E_2 \text{ est une isogénie définie sur } L\}$$

l'ensemble des morphismes de E_1 vers E_2.
En l'absence de précisions $\mathrm{Hom}(E_1, E_2)$ désigne les morphismes définis sur K.

Remarque 2.2.40:

On parle de morphisme (comme pour les variétés algébriques quelconques) mais les éléments de $\mathrm{Hom}(E_1, E_2)$ ne sont pas simplement des morphismes de variétés, ils préservent en plus le neutre. En dehors de [0] qui n'est pas surjectif, ce sont des isogénies.

Lemme 2.2.41:

Soit α un morphisme de degré n ($n = 0$ pour $\alpha = [0]$), alors $\alpha \circ \widehat{\alpha} = [n]$. En particulier, $\widehat{\widehat{\alpha}} = \alpha$.
De plus, $[n] \circ [n] = [n^2] = [\deg[n]]$ donc $\widehat{[n]} = [n]$.

Preuve :

Si $\alpha = [0]$ le résultat est clair. On suppose donc maintenant que α est une isogénie.

$$\alpha \circ \widehat{\alpha} \circ \alpha = \alpha \circ [n] = [n] \circ \alpha$$

Le Lemme 2.2.38 donne alors $\alpha \circ \widehat{\alpha} = [n]$.
□

Lemme 2.2.42:

Soient $E_1/K, E_2/K, E_3/K$ des courbes elliptiques, $\alpha, \beta \in \mathrm{Hom}(E_1, E_2)$ et $\gamma \in \mathrm{Hom}(E_2, E_3)$. Alors :

1. Composition : $\widehat{\gamma \circ \alpha} = \widehat{\alpha} \circ \widehat{\gamma}$
2. Somme : $\widehat{\alpha + \beta} = \widehat{\alpha} + \widehat{\beta}$

Preuve :

On prouve seulement pour la composition, pour la somme voir Silverman [13, III.6.2].

$$(\widehat{\alpha} \circ \widehat{\gamma}) \circ (\gamma \circ \alpha) = \widehat{\gamma} \circ [\deg \alpha] \circ \gamma = \widehat{\gamma} \circ \gamma \circ [\deg \alpha] = [\deg \gamma] \circ [\deg \alpha] = [\deg \gamma \deg \alpha] = [\deg \gamma \circ \alpha]$$

□

Corollaire 2.2.43:

Soit $\alpha \in \mathrm{End}(E)$, alors $\exists n \in \mathbb{Z}$ t.q. $\alpha + \widehat{\alpha} = [n]$.

Preuve :

$$\deg(1 - \alpha) = (1 - \alpha)\widehat{(1 - \alpha)} = (1 - \alpha)(\widehat{1} - \widehat{\alpha}) = 1 - (\alpha + \widehat{\alpha}) + \deg \alpha$$

Le résultat suit pour $n = 1 + \deg \alpha - \deg(1 - \alpha)$
□

Définition 2.2.44:

Soit $\alpha \in \mathrm{End}(E)$, on appelle trace de α l'entier $\mathrm{tr}\, \alpha = \alpha + \widehat{\alpha}$.

Proposition 2.2.45:

Soit $\alpha \in \mathrm{End}(E)$, alors α et $\widehat{\alpha}$ sont racines de $X^2 - (\mathrm{tr}\, \alpha)X + \deg \alpha$

Preuve : $\alpha^2 - (\mathrm{tr}\, \alpha)\alpha + \deg \alpha = \alpha^2 - (\alpha^2 + \widehat{\alpha}\alpha) + \widehat{\alpha}\alpha = 0$. Idem pour $\widehat{\alpha}$.

2.3 Classe d'isomorphisme et j-invariant

Définition 2.3.1:

Soit E/K une courbe elliptique donnée par l'équation de Weierstrass $Y^2 = X^3 + AX + B$. On appelle j-invariant de E l'élément

$$j(E) := 1728 \frac{4A^3}{4A^3 + 27B^2} \in K.$$

On pourra aussi noter $j(A, B)$.

Proposition 2.3.2:

Étant donné un élément $j_0 \in K$, il existe une courbe elliptique E/K telle que $j(E) = j_0$. Plus précisément, si $j_0 \neq 0, 1728$, elle est donnée par :

$$Y^2 = X^3 + \underbrace{3j_0(1728 - j_0)}_{A} X + \underbrace{2j_0(1728 - j_0)^2}_{B}.$$

Si $j_0 = 0$, on peut prendre : $Y^2 = X^3 + 1$
Si $j_0 = 1728$, on peut prendre : $Y^2 = X^3 + X$

Preuve :

Vérifions que la courbe spécifiée est bien une courbe elliptique, c'est-à-dire que $4A^3 + 27B^2 \neq 0$.

$$\begin{aligned} 4A^3 + 27B^2 &= 108j_0^3(1728 - j_0)^3 + 108j_0^2(1728 - j_0)^4 \\ &= 108j_0^2(1728 - j_0)^3(j_0 + (1728 - j_0)) \\ &= 1728 \times 108j_0^2(1728 - j_0)^3 \neq 0 \end{aligned}$$

De plus :

$$\begin{aligned} 1728\frac{4A^3}{4A^3 + 27B^2} &= \frac{108j_0^3(1728 - j_0)^3}{1728 \times 108j_0^2(1728 - j_0)^3} \\ &= j_0 \end{aligned}$$

Pour le cas $j_0 = 0$, il faut nécessairement $A = 0$ et alors tout B non nul convient.

Pour le cas $j_0 = 0$ on peut prendre $B = 0$ et alors tout A non nul convient.
□

Théorème 2.3.3:

Soient E_1/K, E_2/K des courbes elliptiques. Alors, E_1 et E_2 sont isomorphes (sur $\overline{K}$) si et seulement si leurs j-invariants sont égaux. Plus précisément elles sont isomorphes sur une extension de K de degré 6, 4 ou 2 selon si leur j-invariant commun vaut 0, 1728 ou autre chose.

On commence par montrer la proposition ci-dessous :

Proposition 2.3.4:

Soient E_1/K, E_2/K des courbes elliptiques données par les équations $Y^2 = X^3 + A_1X + B_1$ et $Y^2 = X^3 + A_2X + B_2$. Alors, E_1 et E_2 sont isomorphes sur K si et seulement s'il existe $\mu \in K^\times$ tel que $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$.

Preuve :

Sens direct Soit $\phi : E_1 \to E_2$ un isomorphisme défini sur K. Notons $(r_1(X), r_2(X)Y)$ sa forme standard. Puisque ϕ est un isomorphisme, son noyau et trivial. D'après le Corollaire 2.2.13, alors, r_1 et r_2 sont des polynômes.
Puisque ϕ est de degré 1 (Corollaire 2.2.36), $r_1(x) = aX + b$ pour des $a, b \in K$, $a \neq 0$.
Substituant dans l'équation de E_2, on obtient :

$$r_2(X)^2Y^2 = (aX + b)^3 + A_2(aX + b) + B_2$$

Puis, utilisant l'équation de E_1 :

$$r_2(X)^2(X^3 + A_1X + B) = (aX + b)^3 + A_2(aX + b) + B_2$$

Comparant les degrés, on obtient que r_2 est constant non nul. Disons $r_2 = c$. Alors,

$$\begin{aligned} & c^2(X^3 + A_1X + B) = (aX + b)^3 + A_2(aX + b) + B_2 \\ \iff & c^2X^3 + c^2A_1X + c^2B = a^3X^3 + 3a^2bX^2 + (3ab^2 + aA_2)X + (b^3 + A_2b + B_2) \end{aligned}$$

Comparant les coefficients devant X^2, on obtient $b = 0$. Comparant ceux devant X^3, on obtient $c^2 = a^3$ puis $a = (c/a)^2$ et $c = (c/a)^3$. Notant $\mu = c/a$ et réinjectant dans l'équation précédente, on obtient :

$$\begin{aligned} & c^2X^3 + c^2A_1X + c^2B = a^3X^3 + aA_2X + B_2 \\ \iff & \mu^6X^3 + \mu^6A_1X + \mu^6B = \mu^6X^3 + \mu^2A_2 + B_2 \end{aligned}$$

Comparant les coefficients, on obtient finalement que $A_2 = \mu^4A_1$ et $B_2 = \mu^6B_1$.
Sens réciproque Soit E_1/K une courbe donnée par l'équation $Y^2 = X^3 + A_1X + B_1$. Soit $\mu \in K^\times$, soient $A_2 = \mu^4A_1$ et $B_2 = \mu^6B_1$. Soit E_2/K donnée par l'équation $Y^2 = X^3 + A_2X + B_2$. Montrons que $E_1 \simeq E_2$ sur K.

On pose l'application :

$$\begin{aligned} \phi : E_1 &\to E_2 \\ [x : y : z] &\mapsto [\mu^2x : \mu^3y : z] \end{aligned}$$

Vérifions que ϕ est bien définie. Si $[x : y : z] \in E_1$, alors, notant $[x' : y' : z']) = \phi([x : y : z])$ et, injectant dans l'équation de E_2, on obtient :

$$\begin{aligned} (y')^2z' = (x')^3 + A_2x'(z')^2 + B_2(z')^3 &\iff \mu^6y^2z = \mu^6x^3 + \mu^2A_2z^2 + B_2z^3 \\ &\iff y^2z = x^3 + \frac{A_2}{\mu^4}xz^2 + \frac{B_2}{\mu^6}z^3 \\ &\iff y^2z = x^3 + A_1xz^2 + B_1z^3 \end{aligned}$$

Or, cette dernière condition est vérifiée puisque $[x : y : z] \in E$ donc ϕ est bien définie.

Montrons que ϕ est une isogénie : il s'agit d'une application rationnelle non constante. De plus, $\phi([0 : 1 : 0]) = [0 : \mu^3 : 0] = O$ donc ϕ est bien une isogénie.

Puisque ϕ est de degré 1 (forme standard (μ^2X, μ^3Y)), c'est un isomorphisme (Corollaire 2.2.36).
□

On peut maintenant prouver le Théorème 2.3.3 :
Preuve :

Sens réciproque Soient $E_1/K, E_2/K$ des courbes isomorphes sur K. Notons $Y^2 = X^3 + A_1X + B_1$ et $Y^2 = X^3 + A_2X + B_2$ des équations pour E_1 et E_2. D'après la Proposition 2.3.4, $A_2 = \mu^4A_1$ et $B_2 = \mu^6B_1$. Alors,

$$j(E_2) = 1728\frac{4A_2^3}{4A_2^3 + 17B_2^2} = 1728\frac{\mu^{12} \times 4A_1^3}{\mu^{12} \times 4A_1^3 + \mu^{12} \times 27B_1^2} = 1728\frac{4A_1^3}{4A_1^3 + 27B_1^2} = j(E_1)$$

Sens direct Soient $E_1/K, E_2/K$ des courbes telles que $j_0 := j(E_1) = j(E_2)$.

— Supposons $j_0 \neq 0, 1728$: Notons, d'après la Proposition 2.3.2, $A_3 = 3j_0(1728 - j_0)$ et $B_3 = 2j_0(1728 - j_0)^2$. Soit alors E_3/K donnée par $Y^2 = X^3 + A_3X + B_3$ de sorte que $j(E_3) = j_0$.

Substituant $j_0 = 1728\frac{4A_1^3}{4A_1^3 + 27B_1^2}$ dans l'expression de A_3 :

$$\begin{aligned} A_3 &= 3 \times 1728 \frac{4A_1^3}{4A_1^3 + 27B_1^2} \times \left(1728 - 1728 \frac{4A_1^3}{4A_1^3 + 27B_1^2}\right) \\ &= 3 \times 1728^2 \frac{4A_1^3}{4A_1^3 + 27B_1^2} \times \left(\frac{27B_1^2}{4A_1^3 + 27B_1^2}\right) \\ &= 3 \times 1728^2 \frac{4 \times 27 A_1^3 B_1^2}{(4A_1^3 + 27B_1^2)^2} \\ &= \left(\frac{2^7 3^5 A_1 B_1}{4A_1^3 + 27B_1^2}\right)^2 A_1 \end{aligned}$$

Idem, on obtient :

$$B_3 = \left(\frac{2^7 3^5 A_1 B_1}{4A_1^3 + 27B_1^2}\right)^3 B_1$$

De manière complètement analogue, on peut utiliser l'expression de j_0 en fonction de A_2, B_2 pour obtenir les mêmes expressions pour A_3, B_3 mais en termes de A_2, B_2.

Notons $u = \left(\frac{2^7 3^5 A_1 B_1}{4A_1^3 + 27B_1^2}\right)\left(\frac{4A_2^3 + 27B_2^2}{2^7 3^5 A_2 B_2}\right)$. Alors, $A_2 = u^2 A_1$ et $B_2 = u^3 B$. Soit alors $L = K(\mu)$ un corps de rupture de $X^2 - u$ ($\mu^2 = u$). On obtient $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$ donc la Proposition 2.3.4 donne E_1 et E_2 isomorphes sur L (extension de degré 2).

— Supposons $j_0 = 0$, alors $A = 0$ donc en considérant $L = K(\mu)$ un corps de rupture de $X^6 B_1 - B_2$ on conclut comme précédemment (puisque $0 = \mu^4 A_1 = A_2$).

— Supposons $j_0 = 1728$, alors $B_1 = B_2 = 0$ et en considérant $L = K(\mu)$ un corps de rupture de $X^4 A_1 - A_2$ on conclut comme avant.

□

Un phénomène intéressant se produit lorsque l'on considère des courbes supersingulières ($E[p] \simeq \{0\}$) en caractéristique p :

Proposition 2.3.5:

Soit K un corps de caractéristique p et E/K une courbe elliptique supersingulière. Alors $j(E) \in \mathbb{F}_{p^2}$.

Preuve :

Notons $[p] = \alpha \circ \pi^k$ avec α une isogénie séparable et $p^k = \deg_i[p]$. Alors,

$$E \text{ supersingulière} \iff \ker[p] = \{0\} \iff \deg \alpha = 0 \iff \alpha \text{ est un isomorphisme}$$

On a utilisé le Théorème 2.2.21 pour la deuxième équivalence et le Corollaire 2.2.36 pour la troisième.

Sachant que $\deg[p] = p^2$ (Proposition 2.2.29), on déduit que E supersingulière $\iff$ $[p] = \alpha \circ \pi^2$ avec α un isomorphisme.

Or, $[p] = \widehat{\pi} \circ \pi$ donc E est supersingulière si et seulement si $\widehat{\pi} = \alpha \circ \pi$ avec $\alpha : E^{(p^2)} \to E$ un isomorphisme.

Notons $Y^2 = X^3 + AX + B$ une équation de E, alors $Y^2 = X^3 + A^{p^2} X + B^{p^2}$ est une équation de $E^{(p^2)}$ et le Théorème 2.3.3 donne :

$$j(E) = j\left(E^{(p^2)}\right) = 1728 \frac{4\left(A^{p^2}\right)^3}{4\left(A^{p^2}\right)^3 + 27\left(B^{p^2}\right)^2} = \left(1728 \frac{4A^3}{4A^3 + 27B^2}\right)^{p^2} = j(E)^{p^2}$$

Par conséquent, $j(E) \in \mathbb{F}_{p^2}$.

□

Cette proposition est utile dans les applications cryptographiques puisqu'elle permet de se restreindre, dès lors que

l'on travail avec des courbes supersingulières, a $\mathbb{F}_{p^2}$: faisable en machine.

3 Application cryptographique : SIDH

Nous allons maintenant présenter l'un des premier protocole à base d'isogénies entre courbes elliptiques : **S**upersingular **I**sogeny **D**iffie-**H**ellman (Jao et De Feo [7]). Rappelons que le but d'un tel échange de clé est d'obtenir, en communiquant par un canal en clair, un secret commun.

Dans tout ce qui suit, on fixe $q = p^2$.

3.1 Protocole

Définition 3.1.1:

Soient $E_1/K, E_2/K$ deux courbes elliptiques et l un nombre premier. On dit que E_1 et E_2 sont l-isogènes s'il existe une isogénie de degré l de E_1 vers E_2.

Remarque 3.1.2:

— Considérant j_1, j_2 deux j-invariant, on peut sans ambiguïtés parler de l'existence d'une l-isogénie entre les classes de courbes elliptiques qu'ils représentent. On parlera donc parfois d'isogénie entre j_1 et j_2. S'il existe une l-isogénie entre j_1 et j_2, on dit que j_1 est l-isogène à j_2.

— S'il existe une l-isogénie de j_1 vers j_2, son isogénie duale donne une l-isogénie de j_2 vers j_1. On peut donc dire que j_1 et j_2 sont l-isogènes.

Définition 3.1.3: *Graphe d'isogénies*

Considérons V_K l'ensemble des j-invariants possibles sur K. Alors, fixant un nombre premier l, on obtient un graphe non orienté $\mathcal{G}_l = (V_K, E_l)$, où E_l contient l'arrête $\{j_1, j_2\}$ si et seulement si j_1 et j_2 sont l-isogène.

L'idée de l'échange de clé SIDH est la suivante :

1. On fixe un j-invariant supersingulier de départ j_0, deux premiers distincts l_A, l_B.
2. Alice marche sur $\mathcal{G}_{l_A}$ et Bob marche sur $\mathcal{G}_{l_B}$ *d'une certaine manière*.
3. Alice et Bob échangent leurs points d'arrivés (et quelques autres informations).
4. Alice marche sur $\mathcal{G}_{l_A}$ en partant du point d'arrivée de Bob. Bob marche sur $\mathcal{G}_{l_B}$ en partant du point d'arrivée d'Alice
5. La manière dont la marche est faite assure qu'Alice et Bob arrivent au même j-invariant qui est leur secret commun

On va maintenant donner cela en plus de détails.

Protocole 3.1.4: *SIDH*

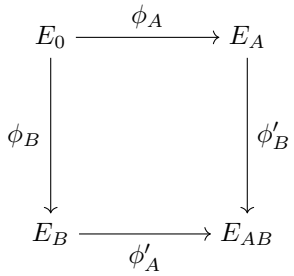
Mise en place, Alice et Bob se mettent d'accord sur :

- Un nombre premier p de la forme $p = f \times l_A^{e_A} l_B^{e_B} \pm 1$ avec $f, e_A, e_B \in \mathbb{N} \setminus \{0\}$ et l_A, l_B deux nombres premiers distincts (souvent 2 et 3 en pratique)
- Une courbe supersingulière de départ $E_0/\mathbb{F}_q$
- Des points $P_A, Q_A, P_B, Q_B \in E_0$ tels que $E_0[l_A^{e_A}] = \langle P_A, Q_A \rangle$ et $E_0[l_B^{e_B}] = \langle P_B, Q_B \rangle$. Ceci est possible d'après le Théorème 2.2.30.

Le protocole se déroule alors comme suit (du point de vue d'Alice, Bob réalise les mêmes actions en parallèle en échangeant les rôles de A et B) :

1. Alice choisit son secret $a \in \{0, 1, \ldots, l_A^{e_A} - 1\}$ et calcule $S_A = P_A + aQ_A$.
2. Elle calcule $\phi_A : E_0 \to E_A$ l'unique isogénie séparable de noyau $\langle S_A \rangle$ (à isomorphisme près, voir Théorème 2.2.34).
3. Elle transmet à Bob le triplet $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
4. À partir du triplet $(E_B, \phi_B(P_A), \phi_B(Q_A))$ que Bob lui a envoyé, elle calcule $\phi'_A : E_B \to E_{BA}$ l'unique isogénie séparable de noyau $\langle \phi_B(P_A) + a\phi_B(Q_A) \rangle = \langle \phi_B(S_A) \rangle$.
5. On montre ci-dessous que E_{BA} ainsi calculée et E_{AB} (calculée par Bob) sont isomorphes et ont donc même j-invariant : ceci donne un secret commun.

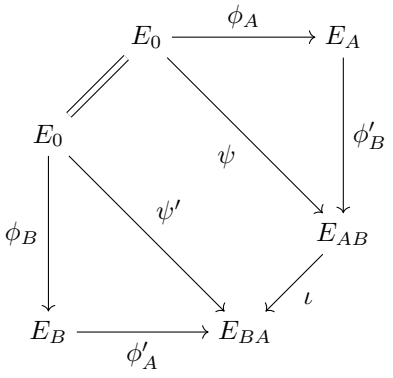
Les différentes isogénies considérées sont représentées sur le diagramme ci-dessous (où on a omis la distinction entre E_{AB} et E_{BA} puisqu'il suffit de composer par un isomorphisme).



Preuve :

Considérons l'isogénie $\psi = \phi'_B \circ \phi_A : E_0 \to E_{AB}$. Soit $P \in E_0$. Alors,

$$\begin{aligned} P \in \ker \psi &\iff \phi_A(P) \in \ker \phi'_B = \langle \phi_A(S_B) \rangle \\ &\iff \exists k \in \mathbb{Z} \text{ t.q. } \phi_A(P) = k\phi_A(S_B) \\ &\iff \exists k \in \mathbb{Z} \text{ t.q. } P - kS_B \in \ker \phi_A = \langle S_A \rangle \\ &\iff \exists k, l \in \mathbb{Z} \text{ t.q. } P - kS_B = lS_A \\ &\iff P \in \langle S_A, S_B \rangle \end{aligned}$$



Idem, considérant $\psi' = \phi'_A \circ \phi_B : E_0 \to E_{BA}$, on trouve que $\ker \psi' = \langle S_B, S_A \rangle = \ker \psi$.

Appliquant le Théorème 2.2.34, on obtient alors l'existence d'un isomorphisme $\iota : E_{AB} \to E_{BA}$.
□

Nous allons voir dans la suite une attaque sur ce protocole donc nous ne parlerons pas de la sécurité de celui-ci, il est cependant intéressant de consulter le papier original (Jao et De Feo [7]) pour y lire les discussions sur la sécurité du protocole avant qu'il ne soit cassé.

Nous allons maintenant détailler quelques aspects effectifs du protocole.

3.2 Aspects effectifs

3.2.1 Calcul d'isogénies

On suppose pour l'instant que tous les points considérés sont $\mathbb{F}_q$-rationnels. La sous-section Section 3.2.2 clarifiera pourquoi cette supposition est valide.

On va employer le lemme suivant :

Lemme 3.2.1:

Soient $E_1/K, E_2/K$ des courbes elliptiques et $\phi : E_1 \to E_2$ une isogénie. Alors, E_2 est supersingulière si et seulement si E_1 l'est.

Preuve :

D'après le Corollaire 2.2.20, on peut écrire $[p]$ comme $[p] = \alpha_{\text{sep}} \circ \pi^k$. Clairement, la courbe est supersingulière si et seulement si α_{sep} est un isomorphisme.

Or, d'après le Lemme 2.2.33, $[p]$ commute avec toute isogénie donc, notant $[p]_i : E_i \to E_i$,

$$\begin{aligned} & [p]_1 \circ \phi = \phi \circ [p]_2 \\ \implies & \deg_i [p]_1 \deg_i \phi = \deg_i \phi \deg_i [p]_2 \\ \implies & \deg_i [p]_1 = \deg_i [p]_2 \end{aligned}$$

D'où le résultat.
□

Proposition 3.2.2:

Soit $E/\mathbb{F}_q$ une courbe elliptique et $P \in E(\mathbb{F}_q)$ un point d'ordre l premier. Soit $\phi : E \to E'$ l'unique isogénie de noyau $\langle P \rangle$. Alors, pour tout $Q \in E$, il est possible de calculer $\phi(Q)$ et une équation de E' en $\widetilde{O}(\sqrt{l})$ opération dans $\mathbb{F}_q$.

Preuve : Bernstein et al. [2].

Soit alors un point $S \in E$ un point d'ordre l^e (l premier et e entier positif). On souhaite calculer l'isogénie $\phi : E_0 \to E'$ de noyau $\langle S \rangle$.
Notons $S_0 = l^{e-1} S$ (d'ordre l) et $\phi_1 : E_0 \to E_1$ l'unique isogénie de noyau $\langle S_0 \rangle$. On pose alors $S_1 = l^{e-2} \phi_1(S)$ (d'ordre l vu le noyau de ϕ_1).
Soit $k < e$ et supposons que pour tous $j \leq k$, $\phi_j : E_{j-1} \to E_j$ de noyau $\langle S_{j-1} \rangle$, est déjà construite. On note pour tout $j \leq k : \psi_j = \phi_j \circ \cdots \circ \phi_1 : E_0 \to E_j$.
Alors, on construit $S_k = 2^{e-k-1} \phi_k \circ \cdot \circ \phi_1(S)$ puis $\phi_{k+1} : E_l \to E_{k+1}$ l'unique isogénie de noyau $\langle S_k \rangle$.

Ainsi, on construit la chaine d'isogénies

$$E_0 \xrightarrow[\langle S_0 \rangle]{\phi_1} E_1 \xrightarrow[\langle S_1 \rangle]{\phi_2} E_2 \dashrightarrow E_{e-1} \xrightarrow[\langle S_{e-1} \rangle]{\phi_e} E_e$$

Pour tout $k \leq e$:

$$\begin{aligned} P \in \ker \psi_k & \iff \psi_{k-1}(P) \in \ker \phi_k = \langle S_{k-1} \rangle \\ & \iff \exists \lambda_k \text{ t.q. } \psi_{k-1}(P) + \lambda_k S_{k-1} = 0 \\ & \iff \exists \lambda_k \text{ t.q. } \psi_{k-1}(P) + \lambda_k l^{e-(k-1)-1} \psi_{k-1}(S) = 0 \\ & \iff \exists \lambda_k \text{ t.q. } P + \lambda_k l^{e-k} S \in \ker \psi_{k-1} \\ & \quad \vdots \\ & \iff \exists \lambda_k, \ldots, \lambda_1 \text{ t.q. } P + (\lambda_k l^{e-k} + \lambda_{k-1} l^{e-(k-1)} + \cdots + \lambda_1 l^{e-1}) S = 0 \\ & \iff P \in \langle l^{e-k} S \rangle \end{aligned}$$

En particulier, $P \in \ker \psi_e \iff P \in \langle S \rangle$.

Par conséquent, ψ_e est l'unique isogénie de noyau $\langle S \rangle$.

Proposition 3.2.3:

Soit $E/\mathbb{F}_{p^2}$ une courbe elliptique et $P \in E(\mathbb{F}_q)$ un point d'ordre l^e, l premier et e entier. Soit $\phi : E \to E'$ l'unique isogénie séparable de noyau $\langle P \rangle$. Alors, pour tout $Q \in E$, il est possible de calculer $\phi(Q)$ et une équation de E' en $\widetilde{O}(e\sqrt{l})$ opération dans $\mathbb{F}_q$. Ici, $\widetilde{O}$ désigne la notation usuelle de O où on néglige les termes logarithmiques.

Preuve :

> Ce qui précède montre qu'il suffit de calculer e isogénies $\phi_1, \ldots, \phi_e$.
>
> Or, pour $k \leq e$, le noyau de ϕ_k est $\langle S_{k-1} \rangle$. Soit $n \in \mathbb{N}$, alors :
>
> $$nS_{k-1} = 0 \iff nl^{e-k-1}\psi_k(S) = 0 \iff nl^{e-k-1}S \in \ker \psi_k = \langle l^{e-k}S \rangle \iff l|n$$
>
> Par conséquent, S_{k-1} est d'ordre l et ϕ_k est de degré l.
>
> Puisque toutes les courbes intermédiaires sont supersingulières, on peut choisir un représentant de leurs classes d'isomorphismes dans $\mathbb{F}_q$ (Proposition 2.3.2) donc toutes les isogénies considérées sont entre courbes sur $\mathbb{F}_q$.
>
> Il faut donc calculer e isogénie de degré premier l entre courbes sur $\mathbb{F}_q$ soit une complexité en $\widetilde{O}(e\sqrt{l})$ opérations dans $\mathbb{F}_q$ d'après la Proposition 3.2.2.
> □

L'échange de clé a donc pour complexité : $\widetilde{O}(e_A\sqrt{l_A})$ pour Alice et $\widetilde{O}(e_B\sqrt{l_B})$ pour Bob.
Détaillons ceci pour Alice :

- Calcul de ϕ_A : considérons que P_A, Q_A sont, à isomorphisme près $(1,0),(0,1) \in (\mathbb{Z}/l_A^{e_A}\mathbb{Z})^2$. Alors, $S_A = (1,a)$ est d'ordre $l_A^{e_A}$ donc ce qui précède donne un coût de $\widetilde{O}(e_A\sqrt{l_A})$.
- Calcul de ϕ'_A : déterminons l'ordre de $\phi_B(S_A)$. Soit $n \in \mathbb{N}^*$, alors : $n\phi_B(S_A) = 0 \iff nS_A \in \langle S_B \rangle \subset E_0[l_B^{e_B}]$. Or, d'après le point précédent, $l_B^{e_B}nS_A = 0 \iff l_A^{e_A}|l_B^{e_B}n \iff l_A^{e_A}|n$ donc $n\phi_B(S_A) = 0 \implies l_Ae_A|n$. L'autre implication étant triviale, $\phi_B(S_A)$ est d'ordre $l_A^{e_A}$ et le calcul de ϕ'_A coûte à nouveau $\widetilde{O}(e_A\sqrt{l_A})$.

3.2.2 Choix de p

Nous n'avons pas encore expliqué pourquoi p est choisi de la forme $fl_A^{e_A}l_B^{e_B} \pm 1$. En fait, ceci permet d'avoir $E[l_A^{e_A}], E[l_b^{e_B}] \subset E(\mathbb{F}_q)$.

Pour démontrer cela, on utilise le théorème de Hasse :

Théorème 3.2.4:

Soit $E/\mathbb{F}_{p^n}$ une courbe elliptique. Alors,

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - t$$

où $t = \operatorname{tr} \pi_n$ avec $\pi_n = (X^{p^n}, Y^{p^n}, Z^{p^n})$ le p^n-Frobenius sur E. De plus, $|t| \leq 2\sqrt{p^n}$

Preuve : Sutherland [17]

Proposition 3.2.5:

Soir $E/\mathbb{F}_{p^n}$ une courbe elliptique, alors E est supersingulière si et seulement si $t = \operatorname{tr} \pi_n \equiv 0 \mod p$.

Preuve :

> Comme dans la preuve de la Proposition 2.3.5, E est supersingulière si et seulement si $\widehat{\pi}$ est de la forme $\iota \circ \pi$ avec ι un isomorphisme.

Sens direct : Utilisant le Corollaire 2.2.24, on obtient que $\deg_i \widehat{\pi_n} = \deg_i \widehat{\pi}^n = p^n$ puis que $\widehat{\pi_n} = \delta \circ \pi^n$ avec δ un isomorphisme. Alors, $\operatorname{tr} \pi_n = \pi_n + \widehat{\pi_n} = (\mathrm{id} + \delta) \circ \pi^n$ est de degré divisible par p.

Sens indirect : Si $t = \operatorname{tr} \pi_n \equiv 0 \mod p$, alors $[t]$ est une isogénie inséparable. Mais alors, $\widehat{\pi_n} = t - \pi_n$ aussi d'après le Lemme 2.2.26.
En particulier, $\widehat{\pi}$ est aussi inséparable et E est supersingulière d'après l'équivalence du début de preuve.
□

Combinant ces résultats, on obtient que, pour une courbe définie sur $\mathbb{F}_p$, $\operatorname{tr} \pi \in [-2\sqrt{p}, 2\sqrt{p}] \cap p\mathbb{Z}$. Or, pour tout $p > 3$ (ce que l'on suppose dans tout ce rapport), ceci contraint $\operatorname{tr} \pi = 0$ (et donc $E(\mathbb{F}_p) = p + 1$).

De plus, on a alors que π et $\widehat{\pi}$ sont racines de $X^2 + 0X + p$ (Proposition 2.2.45) donc $\pi^2 = \widehat{\pi}^2 = [-p]$ et $\operatorname{tr} \pi^2 = -2p$.
Il suit, supposant $p = f l_A^{e_A} l_B^{e_B} - 1$, que $\#E(\mathbb{F}_q) = q + 1 - (-2p) = (p+1)^2 = f^2 l_A^{2e_A} l_B^{2e_B}$
Le théorème de Lagrange donne alors que $E[l_A^{e_A}], E[l_B^{e_B}] \subset E(\mathbb{F}_q)$.

Cependant, pour dire que $\pi^2 = [-p]$, on a eu besoin que la courbe E soit définie sur $\mathbb{F}_p$. Or, ce n'est a priori pas le cas de toutes les courbes supersingulières. De plus, on a supposé que p n'est pas de la forme $f l_A^{e_A} l_B^{e_B} + 1$

Pour le cas général, Broker [3] fournit un algorithme permettant de construire une courbe supersingulière $E/\mathbb{F}_q$ avec $\operatorname{tr} \pi_2 = \pm 2\sqrt{q}$ (l'algorithme qu'il fournit fonctionne en réalité pour toutes les traces possibles).
Le théorème de Hasse donne alors un cardinal $\#E(\mathbb{F}_q) = q + 1 - (\pm 2\sqrt{q}) = (p \mp 1)^2 = f^2 l_A^{2e_A} l_B^{2e_B}$ donc les torsions sont bien $\mathbb{F}_q$-rationnelles pour la même raison que ci-dessus.

Puisque toutes les isogénies considérées sont définies sur $\mathbb{F}_q$, tous les points manipulés dans la sous-section précédente sont, comme annoncé, $\mathbb{F}_q$-rationnels.

Remarque 3.2.6:
Pour ce choix de p, $E(\mathbb{F}_q) = E[p \mp 1] = E[f l_A^{E_A} l_B^{E_B}] \simeq (\mathbb{Z}/(f l_A^{E_A} l_B^{E_B})\mathbb{Z})^2$.

En effet, le cardinal trouvé précédemment pour $E(\mathbb{F}_q)$ et le théorème de Lagrange donnent $E(\mathbb{F}_q) \subset E[p \mp 1]$. Or, d'après le Théorème 2.2.30, $E[p \mp 1] \simeq (\mathbb{Z}/(f l_A^{e_A} l_B^{E_B})\mathbb{Z})^2$ est un ensemble de même cardinal que $E(\mathbb{F}_q)$ d'où l'égalité.

3.2.3 Calcul d'une base de $E[l^e]$

On s'intéresse maintenant au calcul de P_A, Q_A, P_B, Q_B, nécessaires pour l'instanciation du protocole. On va seulement traiter P_A, Q_A puisque la procédure sera identique pour P_B, Q_B.

La procédure est la suivante :

1. Tirer au hasard un point P dans $E_0(\mathbb{F}_q) \simeq \mathbb{Z}/(p \mp 1)\mathbb{Z}$ (Remarque 3.2.6) de cardinal $(f l_A^{e_A} l_B^{e_B})^2$
2. Le multiplier par $(f l_B^{e_B})^2$, donnant $P' = (f l_B^{e_B})^2 P$ dont l'ordre divise $l_A^{e_A}$. Si P' est d'ordre exactement $l_A^{e_A}$, fixer $P_A = P'$ et continuer. Sinon repartir à l'étape 1.
3. Répéter la même procédure pour obtenir un second point Q' d'ordre $l_A^{e_A}$. Tester si $E[l_A^{e_A}] = \langle P_A, Q' \rangle$. Si oui, fixer $Q_A = Q'$ et terminer. Sinon, répéter cette étape.

Ceci est efficace. En effet, P' est d'ordre $l_A^{e_A}$ avec grande probabilité. Aussi, une fois P_A choisit, la probabilité de choisir $Q \in \langle P_A \rangle$ est faible ($(f l_B^{e_B})^{-1}$). De plus, on peut tester efficacement $E[l_A^{e_A}] = \langle P_A, Q' \rangle$ avec le couplage de Weil, voir Sutherland [15, 23.25].

3.3 Attaque par le lemme de Kani

L'attaque sur SIDH se base sur le lemme de Kani. Celui-ci porte sur des produits de courbes elliptiques. Nous allons donc énoncer quelques résultats sur les variétés abéliennes afin de le comprendre. Je me suis beaucoup basé sur : "Computing the isogeny class-group action on ordinary elliptic curves by going into higher dimensions"(Rueger [11, 2024]) pour cette section.

3.3.1 Variétés abéliennes, lemme de Kani et autres outils

Définition 3.3.1: *Variété abélienne*

Une variété abélienne définie sur K est une variété algébrique V/K, projective, non singulière et munie d'applications rationnelles $+ : V \times V \to V$ et $\text{inv} : V \to V$ (définie sur K) qui induisent une structure de groupe abélien sur $V(\overline{K})$ (où inv est l'opération de passage à l'inverse pour la loi $+$).

Remarque 3.3.2:

— Nous n'avons défini les applications rationnelles qu'entre variétés algébriques. Il faudrait donc montrer que $V \times V$ en est bien une. On peut en trouver une preuve dans Shafarevich [12, 1.5 : début de section].

— Soient V, W des variétés algébriques, alors $\dim(V \times W) = \dim V + \dim W$. On peut trouver une preuve de ceci dans Shafarevich [12, 1.6 : exemple 1.33].

Remarque 3.3.3:

Puisque la somme est définie sur K, pour toute extension algébrique L/K, $+$ induit une loi de groupe sur $V(L)$.

Exemple 3.3.4:

Une courbe elliptique est une variété abélienne de dimension 1.

Il va nous falloir généraliser la notion d'isogénie à ces nouvelles structures. La définition sera cette fois-ci :

Définition 3.3.5:

Soient $A/K, B/K$ des variétés abéliennes. Un morphisme de variétés abéliennes $\phi : A \to B$ est une application rationnelle induisant un morphisme de groupe $A(\overline{K}) \to B(\overline{K})$. Un tel morphisme est une isogénie si les deux conditions suivantes sont vérifiées :

— A et B ont même dimension

— ϕ est surjective

Les noyaux de telles applications se comportent comme dans le cas des courbes elliptiques :

Théorème 3.3.6:

Soient $A/K, B/K$ des variétés abéliennes de même dimension et $\phi : A \to B$ une isogénie. Alors, $\ker \phi$ est un sous-groupe fini de $A(\overline{K})$ (Milne [9, I.7.1]).

Réciproquement, soit A/K une variété abélienne de dimension n et $G \subset A(K)$ un sous-groupe fini. Alors, il existe une variété abélienne B/K de dimension n et $\phi : A \to B$ une isogénie séparable telle que $\ker \phi = G$. De plus, B et ϕ sont uniques à isomorphisme près (Milne [9, I.8.10, I.8.11.e et I.8.12]).

Proposition 3.3.7:

Soit A/K une variété abélienne et $n \in \mathbb{Z} \setminus \{0\}$. Notons $[n] : A \to A$ définie par, pour tout $P \in A$, $[n]P = \underbrace{P + \cdots + P}_{n \text{ fois}}$.

Alors, $[n]$ est une isogénie de degré $n^{2 \dim A}$. De plus, elle est séparable si et seulement si $\text{car}(K) \nmid n$.

Preuve :

> Il s'agit clairement d'une application rationnelle puisque la loi de groupe est rationnelle. Elle préserve clairement la loi de groupe. Les preuves de la surjectivité et du degré sont dans Milne [9, I.7.2].
> On y trouve également que $[n]$ est étale si et seulement si $\text{car}(K) \nmid n$.
> Toujours dans Milne [9], la remarque I.8.12 donne l'équivalence entre étale et séparable pour les variétés abéliennes.
> □

Remarque 3.3.8:

Nous n'avons pas défini le degré d'une isogénie entre variétés abéliennes (seulement pour les applications entre courbes algébriques). La définition est la même que pour les applications entre courbes, il faudrait démontrer que les extensions de corps utilisées sont finies. Cependant, cela nous intéresse peu donc nous n'en traiterons pas ici.

Théorème 3.3.9:

Soient $A/K, B/K$ des variétés abéliennes. Il existe une variété abélienne $A^\vee/K$ appelée variété duale de A. Pour tout morphisme $\phi : A \to B$, il existe un morphisme dual $\phi^\vee : B^\vee \to A^\vee$ ayant même degré que ϕ.
$A^\vee$ et $\phi^\vee$ sont uniquement déterminés par une propriété universelle que nous ne citerons pas (dépasse le cadre de ce stage). Si ϕ est une isogénie alors $\phi^\vee$ aussi.

Voir les sections I.8 et I.9 de Milne [9] pour plus de détails.

Proposition 3.3.10:

Soient $A_1/K, \ldots, A_n/K$ des variétés abéliennes. Alors $(A_1 \times \cdots \times A_n)^\vee = A_1^\vee \times \cdots \times A_n^\vee$.

Note: *Je n'ai pas réussi à trouver une citation pour la preuve de ce résultat.*

Définition 3.3.11:

Soit A/K une variété abélienne. Une polarisation sur A est une isogénie $\lambda : A \to A^\vee$ *d'une certaine forme* (voir Milne [9, I.11]). Si cette isogénie est un isomorphisme, on parle d'une polarisation principale.
Un couple (A, λ), où A est une variété abélienne et λ une polarisation (principale), est appelée une variété abélienne (principalement) polarisée.

Exemple 3.3.12:

Une courbe elliptique est une variété abélienne principalement polarisée.

Note: *Idem, je ne trouve pas de ref à citer. J'ai l'impression que c'est assez clair lorsqu'on a tout le contexte, mais du coup c'est assez dur de trouver un endroit où c'est clairement prouvé.*

Proposition 3.3.13:

Soient $(A_1, \lambda_1), \ldots, (A_n, \lambda_n)$ des variétés abéliennes principalement polarisées. Alors, $A_1 \times \cdots \times A_n$ est principalement polarisée par $(\lambda_1, \ldots, \lambda_n)$.

Preuve : Jordan, Keeton et Poonen [8, début de 3].

Corollaire 3.3.14:

Soient $E_1/K, E_2/K$ des courbes elliptiques, alors $E_1 \times E_2$ est une variété abélienne principalement polarisée.

Définition 3.3.15: *Morphisme renversé*

Soient $(A/K, \lambda_A), (B/K, \lambda_B)$ des variétés abéliennes principalement polarisées. Soit $\phi : A \to B$ un morphisme. On appelle morphisme renversé le morphisme $\widetilde{\phi} = \lambda_A^{-1} \circ \phi^\vee \circ \lambda_B : B \to A$.

Remarque 3.3.16:

Puisque A et B sont principalement polarisées, λ_A et λ_B sont de degrées 1. De plus, $\deg \phi^\vee = \deg \phi$. Par conséquent $\deg \widetilde{\phi} = \deg \phi$.

Ce morphisme va jouer un rôle similaire à celui de l'isogénie duale dans le cas des courbes elliptiques. Cependant, il n'est pas sûr ici que $\phi \circ \widetilde{\phi} \in \mathrm{End}(A)$ soit une multiplication par n.

Définition 3.3.17:

Soient $(A/K, \lambda_A), (B/K, \lambda_B)$ des variétés abéliennes principalement polarisées. Soit $\phi : A \to B$ un morphisme. On dit que ϕ est, pour un entier $N \in \mathbb{Z}$, un N-morphisme si $\widetilde{\phi} \circ \phi = [N]$.

Remarque 3.3.18:

Si $\phi : A \to B$ est une N-isogénie, alors $\phi \circ \widetilde{\phi} = [N]$.

Preuve : Idem que pour le Lemme 2.2.41.

Remarque 3.3.19:

Lorsque ϕ est une isogénie entre courbes elliptiques, il s'agit forcément d'une d-isogénie, où $d = \deg \phi$, d'après le Théorème 2.2.37. Dans le formalisme des variétés abéliennes, l'isogénie duale a été remplacée par l'isogénie renversée.

Proposition 3.3.20:

Soient $E_1/K, \dots, E_n/K, E'_1/K, \dots, E'_m/K$ des courbes elliptiques. Alors, toute isogénie $F : E_1 \times \cdots \times E_n \to E'_1 \times \to \times E'_n$ est donnée par une matrice $(f_{ij})_{i,j}$ où $f_{ij} : E_j \to E_i$ est une isogénie (ou le morphisme nul). L'image de $(P_1, \dots, P_n) \in E_1 \times \cdots \times E_n$ est donnée par $(Q_i)_{i=1,\dots,m}$ où $Q_i = \sum_j f_{ij}(P_j)$.

Preuve :

> Notons $\gamma_i : E_i \to E'_1 \times \cdots \times E'_n$ l'inclusion canonique et $\pi_i : E_1 \times \cdots E_n \to E_i$ la projection canonique. Définissons alors $f_{ij} = \pi_i \circ F \circ \gamma_j$.
> Alors, $((f_{ij})_{ij})(P))_i = \sum_j f_{ij}(P_j) = \sum_j \pi_i(F(0, \dots, P_j, \dots, 0)) = \pi_i(F(P_1, \dots, P_n))$
>
> Reste à voir que les f_{ij} sont des isogénies ou le morphisme nul. Puisque ce sont des applications rationnelles entre courbes elliptiques. Il suffit de vérifier qu'elles fixent le neutre. Or, $f_{ij}(O) = \gamma_i(F(O, \dots, O, \dots, O)) = \gamma_i(O, \dots, O) = O$.
> □

Remarque 3.3.21:

La réciproque est fausse, toute matrice ne donne pas une isogénie. Par exemple, considérons la matrice $F = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et une variété abélienne A/K. Soient $(P, Q) \in A^2$. Alors $F(P, Q) = (P+Q, P+Q)$ donc l'image de F est $\{(P, P) \mid P \in A\} \neq A \times A$ donc F n'est pas surjective. Par conséquent, F n'est pas une isogénie.

Théorème 3.3.22:

Soient $A_1/K, \dots, A_n/K, B_1/K, \dots, B_m/K$ des variétés abéliennes et $F = (f_{ij})_{ij} : A_1 \times \cdots \times A_n \to B_1 \times \cdots \times B_m$ un morphisme. Alors, $F^\vee$ est donnée par $(f^\vee_{ji})_{ij}$, la transposée de la matrice des duales.

Note: Rueger *[11] avance que c'est vrai. Il founit une source pour une preuve dans le cas 2×2 et une pour le cas matrice entière (*Edixhoven, Geer *et* Moonen *[4]). Je n'ai pas trouvé mieux en ligne.*

Corollaire 3.3.23:

Avec les mêmes notations, si les variétés sont principalement polarisées, $\widetilde{F}$ est donnée par $(\widetilde{f_{ji}})_{ij}$.

Preuve :

> On a déjà vu (Proposition 3.3.13) que $A_1 \times \cdots \times A_n$ est polarisé par $(\lambda_1, \dots, \lambda_n)$ qui correspond à la matrice diagonale $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$. Un simple calcul matriciel donne alors le bon résultat (en utilisant le Théorème 3.3.22).
> □

Proposition 3.3.24:

Soient $(A/K, \lambda_A), (B/K, \lambda_B)$ des variétés abéliennes principalement polarisées. Soit $\phi : A \to B$ un N-morphisme. Alors :

- Soit $n \in \mathbb{N} \setminus \{0\}$, $\phi I_n : A^n \to B^n$ est un N-morphisme.
- Si ϕ est une isogénie, son noyau est donné par $\ker \phi = \widetilde{\phi}(B[N])$. En particulier, $\ker \phi \subset A[N]$.

Preuve :

> - Utilisant le Théorème 3.3.22,
>
> $$\widetilde{\phi I_n} \circ \phi I_n = \begin{pmatrix} \widetilde{\phi} & 0 & \cdots & 0 \\ 0 & \widetilde{\phi} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \widetilde{\phi} \end{pmatrix} \begin{pmatrix} \phi & 0 & \cdots & 0 \\ 0 & \phi & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \phi \end{pmatrix} = \begin{pmatrix} N & 0 & \cdots & 0 \\ 0 & N & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & N \end{pmatrix} = NI_n$$
>
> Or, NI_n est la multiplication par N sur A^n.
> - Soit $P \in \ker \phi$. Puisque $\widetilde{\phi}$ est surjective (par définition d'une isogénie), il existe $Q \in B$ t.q. $P = \widetilde{\phi}(Q)$.

Mais alors, $0 = \phi(P) = [N]Q$ donc $Q \in B[N]$. En particulier, $\ker\phi \subset \widetilde{\phi}(B[N])$.
Pour l'autre inclusion, soit $Q \in B[N]$, alors $\widetilde{\phi}(Q)$ est dans $\ker\phi$ puisque $\phi(\widetilde{\phi}(Q)) = [N]Q = 0$.

□

Proposition 3.3.25:
Soient $(A/K, \lambda_A), (B/K, \lambda_B)$ des variétés abéliennes principalement polarisées. Soit $\phi : A \to B$ une N-isogénie. Alors, N est strictement positif.

Preuve :

La preuve de ce résultat va demander d'admettre certaines choses :
- Soit A/K une variété abélienne et $\alpha : A \to A$ une isogénie. Alors, il existe un unique polynome unitaire $P_\alpha \in \mathbb{Z}[X]$ de degré $2\dim(A)$ tel que $\forall r \in \mathbb{Z},\ P_\alpha(r) = \deg(\alpha - r)$ (Milne [9, I.10.9]). L'opposé du coefficient devant X^{2g-1} de ce polynôme est appelé trace de α. On le note $\operatorname{tr}\alpha$. (Milne [9, fin de page 48])
- Soit A/K une variété abélienne principalement polarisée et $\alpha : A \to A$ un endomorphisme (application rationnelle qui préserve la structure de groupe). Alors $\operatorname{tr}(\widetilde{\alpha} \circ \alpha) > 0$ (Milne [9, I.14.3])

Passons à la preuve du résultat. Considérons la variété abélienne principalement polarisée $C = A \times B$. Considérons alors l'endomorphisme $\alpha : C \to C$ donnée par la matrice $\begin{pmatrix} 0 & 0 \\ \phi & 0 \end{pmatrix}$ Alors, $\widetilde{\alpha} = \begin{pmatrix} 0 & \widetilde{\phi} \\ 0 & 0 \end{pmatrix}$ puis $\widetilde{\alpha}\alpha = \begin{pmatrix} [N] & 0 \\ 0 & 0 \end{pmatrix}$
Soit $r \in \mathbb{Z}$, alors $\widetilde{\alpha}\alpha - r = \begin{pmatrix} [N-r] & 0 \\ 0 & [-r] \end{pmatrix}$ est de degré $(N-r)^{2d}r^{2d}$ (d'après Edixhoven, Geer et Moonen [4, 11.28.i]) où $d = \dim A = \dim B$ puisque A et B sont isogènes.
Par conséquent,

$$P_{\widetilde{\alpha}\alpha} = (X^2 - XN)^{2d} = \sum_{k=0}^{2d} \binom{2d}{k} (-1)^k N^k X^{k+2(2d-k)} = \sum_{k=0}^{2d} \binom{2d}{k} (-1)^k N^k X^{4d-k}$$

Ensuite,

$$\operatorname{tr}(\widetilde{\alpha}\alpha) = -\binom{2d}{1}(-1)N = 2dN$$

Or, puisque $\operatorname{tr}(\widetilde{\alpha}\alpha) > 0$ (vu le premier résultat admis en début de preuve), nécessairement $N > 0$.
□

On peut alors se demander quand est-ce qu'une isogénie donnée matriciellement est une N-isogénie. Le cas qui va nous intéresser est le cas des matrices 2×2.

Soient $A_1/K, A_2/K, B_1/K, B_2/K$ des variétés abéliennes et $F = (f_{ij})_{ij} : A_1 \times A_2 \to B_1 \times B_2$ une isogénie. Alors,

$$\widetilde{F}F = \begin{pmatrix} \widetilde{f_{11}} & \widetilde{f_{21}} \\ \widetilde{f_{12}} & \widetilde{f_{22}} \end{pmatrix} \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} = \begin{pmatrix} \widetilde{f_{11}}f_{11} + \widetilde{f_{21}}f_{21} & \widetilde{f_{11}}f_{12} + \widetilde{f_{21}}f_{22} \\ \widetilde{f_{12}}f_{11} + \widetilde{f_{22}}f_{21} & \widetilde{f_{12}}f_{12} + \widetilde{f_{22}}f_{22} \end{pmatrix}$$

Supposons maintenant que f_{ij} est une d_{ij}-isogénie. Ceci se produira par exemple lorsque les variétés considérées sont des courbes elliptiques (et alors $d_{ij} = \deg f_{ij}$). Il suit :

$$\widetilde{F}F = \begin{pmatrix} [d_{11} + d_{21}] & \widetilde{f_{11}}f_{12} + \widetilde{f_{21}}f_{22} \\ \widetilde{f_{12}}f_{11} + \widetilde{f_{22}}f_{21} & [d_{12} + d_{22}] \end{pmatrix}$$

Or ceci est une multiplication par un entier $N \in \mathbb{Z}$ si et seulement si :

1. $d_{11} + d_{21} = d_{12} + d_{22}$

2. $\widetilde{f_{11}}f_{12} + \widetilde{f_{21}}f_{22} = 0$
3. $\widetilde{f_{12}}f_{11} + \widetilde{f_{22}}f_{21} = 0$

Remarque 3.3.26:

On va utiliser $\widetilde{\alpha+\beta} = \widetilde{\alpha} + \widetilde{\beta}$. Une preuve possible est d'utiliser le fait que $\alpha+\beta = \begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$ et appliquer le Corollaire 3.3.23.

Remarque 3.3.27:

— Puisque les conditions 2. et 3. sont le renversé l'une de l'autre, elles sont équivalentes.

— Les conditions 2. et 3. donnent $d_{11}d_{12} = d_{21}d_{22}$. En effet, $\widetilde{f_{11}}f_{12}(\widetilde{f_{12}}f_{11}) = [d_{11}d_{12}]$. De plus, d'après les conditions 2. et 3. :

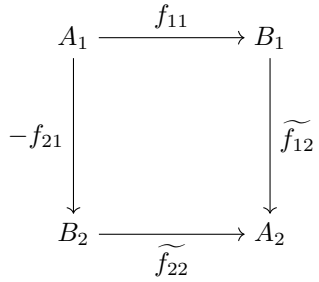
$$\widetilde{f_{11}}f_{12}(\widetilde{f_{12}}f_{11}) = -\widetilde{f_{21}}f_{22}(\widetilde{f_{12}}f_{11}) = -\widetilde{f_{21}}f_{22}(\widetilde{f_{22}}f_{21}) = [d_{21}d_{22}]$$

— Sous ces 3 conditions, $d_{11} = d_{22}$ et $d_{12} = d_{21}$. En effet,

$$0 = d_{11}d_{12} - d_{21}d_{22} = d_{11}(d_{11} + d_{21} - d_{22}) - d_{21}d_{22} = d_{11}^2 + d_{11}d_{21} - d_{11}d_{22} - d_{21}d_{22} = (d_{11} + d_{21})(d_{11} - d_{22})$$

Or, puisque les d_{ij} doivent être positif (Proposition 3.3.25). Il suit $d_{11} = d_{22}$. La condition 1. donne alors immédiatement $d_{21} = d_{12}$.

— La condition 3. se réécrit par la commutativité du diagramme ci-dessous :



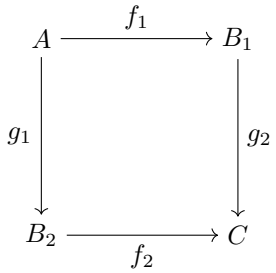
On obtient alors le lemme de Kani :

Lemme 3.3.28: *Kani*

Soient $A/K, B_1/K, B_2/K, C/K$ des variétés abéliennes principallement polarisées et $f_1 : A \to B_1$ $f_2 : B_2 \to C$ des d-isogénies, $g_1 : A \to B_2$ $g_2 : B_1 \to C$ des d'-isogénies.

Notons $F = \begin{pmatrix} f_1 & \widetilde{g_2} \\ -g_1 & \widetilde{f_2}\end{pmatrix}$

Alors, $F : A \times C \to B_1 \times B_2$ est une isogénie si et seulement si le diagramme ci-dessous commute.



On parle alors de carré de Kani et F est une $(d+d')$-isogénie.

On peut de plus obtenir une description plus précise du noyau de l'isogénie F.

Lemme 3.3.29:

Avec les notations précédentes :

— Le noyau de F est

$$\ker F = \{(\widetilde{f}_1(P) - \widetilde{g}_1(Q), g_2(P) + f_2(Q)) \mid P \in B_1[d+d'], Q \in B_2[d+d']\}$$

— Si de plus on suppose $\ker \widetilde{f}_1 \cap \ker g_2 = \{0\}$ et $p \nmid d+d'$, on dit que le carré est orthogonal et

$$\ker F = \{(\widetilde{f}_1(P), g_2(P)) \mid P \in B_1[d+d']\}$$

— Si on suppose que d et d' sont premiers entre eux, $p \nmid d+d'$ et que les isogénies considérées sont séparables. Alors le carré est orthogonal et la description du noyau se simplifie encore plus en :

$$\ker F = \{(dP, g_2 \circ f_1(P) \mid P \in A[d+d']\}$$

Preuve :

— Puisque F est une $(d+d')$-isogénie, son noyau est $\widetilde{F}(B_1 \times B_2[d+d'])$ (Proposition 3.3.24). Or, $B_1 \times B_2[d+d'] = B_1[d+d'] \times B_2[d+d']$ et $\widetilde{F} = \begin{pmatrix} \widetilde{f}_1 & -\widetilde{g}_1 \\ g_2 & f_2 \end{pmatrix}$. Par conséquent,

$$\begin{aligned} \ker F &= \widetilde{F}(B_1[d+d'] \times B_2[d+d']) \\ &= \{(\widetilde{f}_1(P) - \widetilde{g}_1(Q), g_2(P) + f_2(Q)) \mid P \in B_1[d+d'], Q \in B_2[d+d']\} \end{aligned}$$

— Regardons la restriction de $\widetilde{F}$ à $B_1 \times \{0\}$.

$$(P,0) \in \ker \widetilde{F} \iff \widetilde{f}_1(P) = g_2(P) = 0 \iff P \in \ker \widetilde{f}_1 \cap \ker g_2 = \{0\}$$

Par conséquent, $\widetilde{F}$ est injective sur $B_1 \times \{0\}$. Il suit, notant $r = \dim B_1$

$$\begin{aligned} (d+d')^{2r} &= |B_1[d+d'] \times \{0\}| \\ &\overset{(*)}{=} |\widetilde{F}(B_1[d+d'] \times \{0\})| \\ &\leq |\widetilde{F}(B_1[d+d'] \times B_2[d+d'])| \\ &= |\ker F| \\ &= (d+d')^{2r} \end{aligned}$$

La première égalité vient du fait que $p \nmid d+d'$ (donc $[d+d']$ est séparable, Proposition 3.3.7). L'étoile $(*)$ indique l'endroit ou l'injectivité a été utilisée. La dernière égalité provient du fait que F est séparable (puisque $p \nmid d+d' = \deg F$ et Lemme A.2.11) et que $A \times C$ est de dimension $2r$.

Puisque $\widetilde{F}(B_1[d+d'] \times \{0\}) \subset \widetilde{F}(B_1[d+d'] \times B_2[d+d'])$ sont des ensembles de même cardinalité $(d+d')^{2r}$, on a $\widetilde{F}(B_1[d+d'] \times \{0\}) = \widetilde{F}(B_1[d+d'] \times B_2[d+d'])$ et on obtient la bonne caractérisation du noyau en procédant comme pour le point précédent.

— Le carré est orthogonal puisque $\ker \widetilde{f}_1 \cap \ker g_2$ est un sous groupe de $\ker \widetilde{f}_1$ (d'ordre d) et de $\ker g_2$ (d'ordre d'). Lagrange donne alors que son cardinal divise le pgcd des ordres qui est 1 par hypothèse.

De plus, f_1 induit une bijection $A[d+d'] \to B_1[d+d']$. En effet, puisque d et d' sont premiers entre eux, d et $d+d'$ le sont aussi. Ceci implique que $\ker f_1 \cap A[d+d'] \subset A[d] \cap A[d+d']$ est trivial et donc que $f_1 : A[d+d'] \to B_1[d+d']$ est injective. Puisque $A[d+d']$ et $B[d+d']$ ont même cardinal, on obtient bien une bijection.

Finalement,

$$\begin{aligned} \ker F &= \{(\widetilde{f}_1(P), g_2(P)) \mid P \in B_1[d+d']\} \\ &= \{(\widetilde{f}_1(f_1(Q)), g_2(f_1(Q))) \mid Q \in A[d+d']\} \\ &= \{(dQ, g_2 \circ f_1(Q)) \mid Q \in A[d+d']\} \end{aligned}$$

□

Remarquons que, si on connait l'isogénie F, on connait également l'isogénie f_1. De plus, partant d'une isogénie f_1 donnée, ce lemme permet de construire des isogénies dont le degré est obtenu en sommant quelque chose au degré de f_1. Ceci va nous permettre d'obtenir un degré friable (c'est-à-dire puissance de petits nombres premiers).

Théorème 3.3.30: *Théorème des quatre carrés*

Tout entier $n \in \mathbb{N}$ peut s'écrire comme $n = a^2 + b^2 + c^2 + d^2$ pour certains entiers $a, b, c, d \in \mathbb{N}$.

Lemme 3.3.31:

Soit A une variété abélienne et $m \in \mathbb{N}$. Alors, il existe une m-isogénie $\alpha : A^s \to A^s$ où $s = 1, 2, 4$ est le nombre minimum de carrés nécessaires pour écrire m comme somme de carrés.

Preuve :

Cas $s = 1$ **:** Alors, $m = a^2$ et $[a]$ est un m-endomorphisme de A.

Cas $s = 2$ **:** Alors, $m = a^2 + b^2$. Considérons la matrice $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Alors, M est un m-endomorphisme. En effet,

$$\widetilde{M}M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & b^2+a^2 \end{pmatrix} = [a^2+b^2] = [m]$$

Cas $s = 4$ **:** Alors, $m = a^2 + b^2 + c^2 + d^2$. Considérons la matrice $M = \begin{pmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{pmatrix}$

Un calcul donne alors $\widetilde{M}M = (a^2 + b^2 + c^2 + d^2)I_4 = [a^2 + b^2 + c^2 + d^2]$.

Pour voir qu'il s'agit bien d'isogénies, on peut se référer à la preuve de la proposition 11.28 de Edixhoven, Geer et Moonen [4]. Dans celle-ci, l'auteur décompose une isogénie donnée par une matrice de déterminant non nul en le produit d'un endomorphisme et d'une matrice diagonale à coefficient non nuls, donnant par conséquent une isogénie. Ici, les déterminants sont :

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 = m \qquad \begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{vmatrix} = (a^2 + b^2 + c^2 + d^2)^2 = m^2$$

□

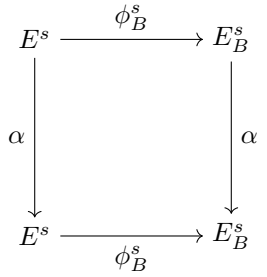
Remarque 3.3.32:

- La variété abélienne A n'entre pas en jeu dans la preuve. Le morphisme sera donné par la même matrice quelle que soit la variété abélienne considérée.
- Le calcul des carrés nécessaires peut se faire avec complexité $O((\log m)^2(\log\log m)^{-1})$ (Pollack et Trevino [10]).

3.3.2 Déroulement de l'attaque

Nous avons maintenant les outils nécessaires pour casser SIDH. On reprend ici les notations du Protocole 3.1.4.

On suppose que $m := l_A^{e_A} - l_B^{e_B} > 0$. Soit α la matrice définissant une m-isogénie donnée par le Lemme 3.3.31. Notons s le nombre de carrés nécessaires pour écrire m comme somme de carrés.
Considérons le diagramme ci-dessous :



Il s'agit d'un carré de Kani (c'est-à-dire qu'il commute) puisque $\phi_B^s = \phi_B I_s$ et que les scalaires commutent avec tout morphisme (α est une matrice de scalaires).

Le Lemme 3.3.28 donne alors la $l_A^{e_A}$-isogénie $F : E^s \times E_B^s \to E_B^s \times E^s$ donnée par la matrice $\begin{pmatrix} \phi_B^s & \widetilde{\alpha} \\ -\alpha & \widetilde{\phi_B}^s \end{pmatrix}$
De plus, ϕ_B^s est une $l_B^{e_B}$-isogénie et α une $(l_A^{e_A} - l_B^{e_B})$-isogénie donc, d'après le troisième cas du Lemme 3.3.29, le noyau de F est :

$$\ker F = \{(l_B^{e_B} P, \alpha\phi_B^s(P)) \mid P \in E^s[l_A^{e_A}]\}$$

Considérons une attaquante Eve qui a accès à toutes les communications entre Alice et Bob. Son but est de récupérer l'isogénie ϕ_B, secret de Bob. Elle va pour cela calculer F.
Or, $E^s[l_A^{e_A}] = E[l_A^{e_A}]^s = \langle P_{A,i}, Q_{A,i} \mid i = 1, \ldots, s\rangle$ où $P_{A,i} = (\delta_{ij} P_A)_{j=1,\ldots,s}$ est connu avec l'initialisation du protocole. A fortiori, le noyau de F l'est également.

De plus, F est de degré friable $l_A^{e_A}$ et il est donc possible de le calculer de manière analogue à la Proposition 3.2.3 en $O(e_A \xi)$ ou ξ représente le coût du calcul d'une isogénie de degré l_A entre deux variétés abéliennes de dimension 2^s.

Eve peut donc calculer efficacement l'isogénie F. Mais alors, elle connait complètement l'isogénie ϕ_B puisque pour tout $P \in E_B$, notant $\overline{P} = (P\delta_{i1})_{i=1,\ldots,n}$, $F(\overline{P}, \overline{O}) = \begin{pmatrix} \overline{\phi_B(P)} & * \\ * & * \end{pmatrix}$.

A Notions complémentaires

A.1 Degré de transcendance

Considérons un corps K ainsi que le corps des fractions rationnelles en une variable $K(X)$. L'extension $K(X)/K$ est clairement transcendante.
Considérons maintenant les fractions en deux variables $K(X,Y)$. À nouveau, $K(X,Y)/K$ est transcendante mais on aurait envie de dire qu'elle l'est "plus" que $K(X)/K$. La notion de degré de transcendance formalise ceci.

Rappelons qu'une partie S d'un corps L/K est dite algébriquement indépendante sur K si pour tout sous-ensemble fini $\{s_1,\dots,s_n\} \subset S$ et pour tout polynôme non nul $f \in K[X_1,\dots,X_n]$, on a $f(s_1,\dots,s_n) \neq 0$. Si $S = \{s_1,\dots,s_n\}$ est algébriquement indépendante,

$$\begin{aligned} K(X_1,\dots,X_n) &\longrightarrow K(s_1,\dots,s_n) \\ P/Q &\mapsto P(s_1,\dots,s_n)/Q(s_1,\dots,s_n) \end{aligned}$$

est un isomorphisme de corps.

Définition A.1.1: *Base de transcendance*

Soit L/K une extension transcendante. Une base de transcendance de L sur K est une partie $S \subset L$, algébriquement indépendante sur K et telle que $L/K(S)$ est algébrique.

Proposition A.1.2:

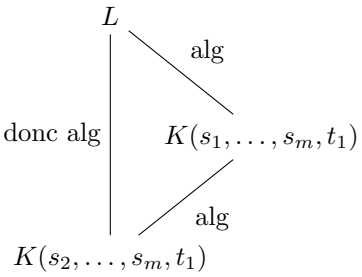
Si L/K admet une base de transcendance finie, alors toutes ses bases de transcendance finies ont même cardinal.

Preuve :

Considérons une base de cardinal minimal $S = \{s_1,\dots s_m\}$ ainsi qu'une autre base $T = \{t_1,\dots,t_n\}$ $(n \geq m)$. Puisque $t_1 \in L$ et $L/K(S)$ est algébrique, il existe un polynôme $P \in K(S)[X]$ tel que $P(t_1) = 0$. Or (puisque S est algébriquement indépendante) les coefficients de ce polynôme sont des fractions rationnelles en $s_1,\dots,s_m$. En multipliant P par le produit de leurs dénominateurs, on obtient un polynôme $\widetilde{P} \in K[Y_1,\dots,Y_m,X]$ tel que $P(s_1,\dots,s_m,t_1) = 0$. En particulier, $\{s_1,\dots,s_m,t_1\}$ est algébriquement dépendant sur K.

Or, au moins l'un des s_i, disons s_1, est algébrique sur $K(s_2,\dots,s_m,t_1)$. En effet, dès lors que $\widetilde{P}$ admet un monôme non nul en Y_i, il induit un polynôme annulateur de s_i dans $K(s_1,\dots,\widehat{s_i},\dots,s_n,t_1)[Y_i]$. Si aucun tel monôme n'existe, alors $\widetilde{P} \in K[X]$ et t_1 est algébrique sur K ce qui est impossible puisque t_1 est supposé transcendant.

A fortiori, l'extension $K(s_1,\dots,s_m,t_1)/K(s_2,\dots,s_m,t_1)$ est algébrique. Or, on sait que $L/K(s_1,\dots,s_m)$ est algébrique donc $L/K(s_1,\dots,s_m,t_1)$ aussi et il suit que $L/K(s_2,\dots,s_m,t_1)$ est algébrique. Ceci est résumé dans le diagramme ci-contre.



Puisque S est supposé de cardinal minimal pour une base de transcendance, $\{s_2,\dots,s_m,t_1\}$ est nécessairement algébriquement indépendant (sinon il contiendrait une base plus petite que S).

Par conséquent, $\{s_2,\dots,s_m,t_1\}$ est une base de transcendance de cardinal minimal et en répétant ceci on obtient que $\{t_1,\dots,t_m\}$ est une base de transcendance. Or alors $m = n$ sinon $\{t_1,\dots,t_n\}$ ne peut être algébriquement indépendant.
□

Définition A.1.3:

Soit L/K une extension qui admet une base de transcendance finie. On appelle degré de transcendance son cardinal (et donc celui de toutes les bases de transcendance finies). On le note $[L:K]_{\mathrm{tr}}$

Proposition A.1.4:

Soient deux extensions L/K et M/L possédant des bases de transcendance finies. Alors, $[M : K]_{\text{tr}} = [M : L]_{\text{tr}} + [L : K]_{\text{tr}}$

Pour prouver cela on emploie le lemme suivant :

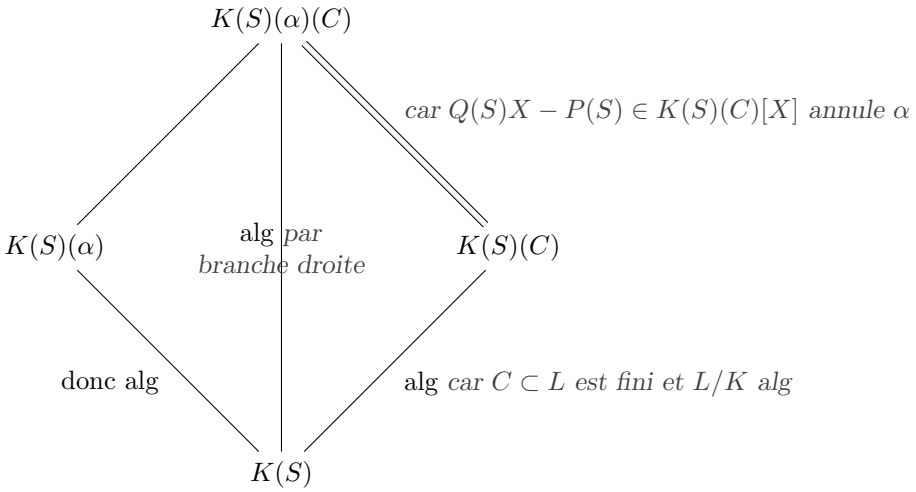
Lemme A.1.5:

Soit L/K une extension algébrique et S une partie finie et algébriquement indépendante sur L d'un surcorps de L. Alors $L(S)/K(S)$ est algébrique.

Preuve :

Soit $\alpha \in L(S)$, on peut écrire $\alpha = \dfrac{P(s_1, \ldots, s_n)}{Q(s_1, \ldots, s_n)}$ avec $P, Q \in L[X_1, \ldots, X_n]$. Notons $C \subset L$ l'ensemble des coefficients de P et Q.
Alors, $g = Q(s_1, \ldots, s_n)X - P(s_1, \ldots, s_n) \in K(S)(C)[X]$ annule α donc $\alpha \in K(S)(C)$.
Or $C \subset L$ et L/K est algébrique donc tous les éléments de C sont algébriques sur $K(S) \supset K$ et puisque C est fini $K(S)(C)/K(S)$ est algébrique.
On déduit de ceci que $K(S)(\alpha)(C)/K(S)$ est algébrique donc $K(S)(\alpha)/K(S)$ l'est également.

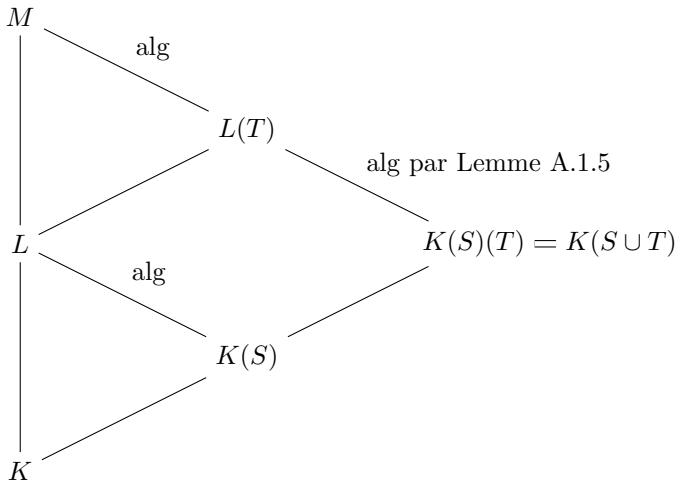
Ce qui précède est résumé dans le diagramme ci-dessous (à lire de droite à gauche).



Ceci nous dit exactement que tout élément de $L(S)$ est algébrique sur $K(S)$ c'est-à-dire $L(S)/K(S)$ est algébrique.
□

On peut maintenant prouver la Proposition A.1.4.
Preuve :

Soit S une base de transcendance pour L/K et T une base de transcendance pour M/L. Montrons que $T \cup L$ est une base de transcendance pour M/K.
On est dans la situation suivante :



Le Lemme A.1.5 nous permet de dire que $M/K(S \cup T)$ est algébrique, reste à montrer que $S \cup T$ est algébriquement indépendant sur K.
Notons $S = \{s_1, \dots, s_n\},\ T = \{t_1, \dots, t_m\}$ et soit $P \in K[X_1, \dots X_n, Y_1, \dots, Y_m]$ tel que $P(S,T) = 0$.
Alors, puisque $S \subset L$, $P(S, Y_1, \dots, Y_m) \in L[Y_1, \dots, Y_m]$ et $P(S,T) = 0$ contredisent que T est algébriquement indépendant dès lors que P a au moins un monôme en $Y_i,\ i \in \{1, \dots, m\}$.
Nécessairement on a donc $P \in K[X_1, \dots, X_n]$ mais cela contredit que S est algébriquement indépendant sur K dès lors que P est non nul. Finalement $P = 0$ et $S \cup T$ est algébriquement indépendant sur K.
□

A.2 Extensions séparables

On fixe ici un corps K et une extension finie L/K.

Définition A.2.1:

- Soit $f \in K[X]$, on dit que f est séparable s'il est à racines simples dans $\overline{K}$.
- Soit $\alpha \in L$, on dit que α est séparable sur K si $\mathrm{Irr}(\alpha, K)$ est séparable.
- On dit que L/K est séparable si tous les éléments de L sont séparables sur K.

Proposition A.2.2:

Si $\mathrm{car}(K) = 0$ ou si le Frobenius est surjectif (en particulier si K est fini), tout polynôme irréductible est séparable. En particulier, toute extension algébrique est séparable.

Preuve :

Supposons que K est de caractéristique 0 et soit $f \in K[X]$ irréductible. Puisque la caractéristique est 0, f' est non nulle et puisque f est irréductible f et f' sont premiers entre eux. Or ceci équivaut à f est séparable.

Si $\mathrm{car}(K) = p$ et le Frobenius est surjectif, le seul cas ou f et f' ne sont pas premier entre eux est le cas $f' = 0$ c'est-à-dire $f = \widetilde{f}(X^p)$. Mais puisque le Frobenius est surjectif, $f = g(X)^p$ ce qui contredit son irréductibilité. Donc f et f' sont premiers entre eux ce qui conclut.
□

Au vu des du résultat précédent, on suppose maintenant que le corps K est de caractéristique positive p et est infini (puisque le cas ou il ne l'est pas sera toujours trivial).

Définition A.2.3: *Degré séparable*

On appelle degré séparable de L/K et on note $[L : K]_s$ le sombre de prolongement à L de $\iota : K \hookrightarrow \overline{K}$ l'injection canonique.

Lemme A.2.4:

Soit $x \in L$ et $f = \mathrm{Irr}(x, K)$, alors :

$$[K(x) : K]_s = \text{nombre de racines distinctes de } f$$

En particulier, x est séparable si et seulement si $[K(x) : K] = [K(x) : K]_s$.

Preuve :

> Un morphisme $\sigma : K(x) \to \overline{K}$ est entièrement déterminé par $\sigma(x)$ et $\sigma_{|K}$. Il y a donc exactement autant de prolongements de ι à $K(x)$ que de racines distinctes de f.
> □

En fait, on a une théorème plus puissant :

Théorème A.2.5:

Nécessairement, $[L : K]_s \leq [L : K]$ et on a égalité si et seulement si L/K est séparable. Dans ce cas, tout morphisme $K \to \overline{K}$ admet excatement $[L : K]_s$ prolongements à L.

Preuve : Berhuy [1] : XXI.1.11

Corollaire A.2.6:

Soit $x \in L$, $K(x)/K$ est séparable sur K si et seulement si x l'est.

Preuve : Théorème A.2.5 et Lemme A.2.4

Proposition A.2.7:

Notons $F = \{x \in L \mid x \text{ est séparable sur } K\}$. Alors, F est un corps appelé clôture séparable de K dans L.

On démontre d'abord le lemme suivant :

Lemme A.2.8:

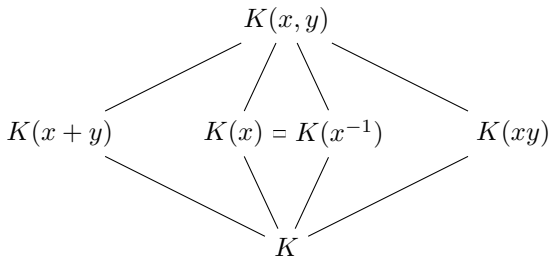
Soit $M/L/K$ une tour d'extensions finies. Si M/K est séparable, alors M/L et L/K le sont.

Preuve :

> Soit $x \in M$, $f = \mathrm{Irr}(x, K)$ et $g = \mathrm{Irr}(x, L)$. Alors, $g|f$ et f est à racines simples dans $\overline{K}$ donc g aussi.
> Soit $x \in L$, soit $f = \mathrm{Irr}(x, K)$. Puisque $x \in M$, f est à racines simples dans $\overline{K}$.
> □

Passons à la preuve de la proposition :

Preuve :

> Soient $x, y \in L$ séparables sur K. On a le diagramme suivant, par conséquent il suffit de montrer que $K(x, y)/K$ est séparable (d'après le Lemme A.2.8).
>
> 
>
>
> Puisque x est séparable sur K, et d'après le Lemme A.2.4, $[K(x) : K]_s = [K(x) : K]$.
> De plus, y est séparable sur $K(x)$. En effet, si P, Q sont les polynômes minimaux de y sur K et $K(x)$ respectivements, alors $Q|P$ (puisque $P \in K(x)[X]$ annule x). En particulier, si P est séparables Q l'est aussi.
> Par conséquent, $[K(x)(y) : K(x)]_s = [K(x)(y) : K(x)]$ et tout morphisme $K(x) \to \overline{K}$ admet $[K(x)(y) : K(x)]$ prolongements à $K(x, y)$.
> Finalement, pour chacun des $[K(x) : K]$ prolongements de $K \hookrightarrow \overline{K}$ à $K(x)$, on a $[K(x, y) : K(x)]_s$

prolongements à $K(x,y)$ (Théorème A.2.5). A fortiori, le nombre de prolongement de $K \hookrightarrow \overline{K}$ à $K(x,y)$ est $[K(x):K][K(x,y):K(x)] = [K(x,y):K]$ et le Théorème A.2.5 donne le résultat.
□

Proposition A.2.9:

Soit $M/L/K$ une tour d'extensions finies. Alors M/K est séparable si et seulement si M/L et L/K le sont

Il nous faut un lemme

Lemme A.2.10:

Soit C une partie de L, alors $K(C)/K$ est séparable si et seulement si chaque élément de C est séparable.

Preuve :

Si $K(C)/K$ est séparable alors tout les éléments de C le sont par définition d'une extension séparable.
Supposons que les éléments de C sont séparables et notons F le corps composé des éléments séparables sur K de L.
Alors, puisque F est un corps contenant K et C, $K(C) \subset F$ c'est-à-dire $K(C)$ est séparable.
□

Preuve :

Le sens direct a déja été vu dans le Lemme A.2.8.

Supposons que M/L et L/K sont séparables et soit $\alpha \in M$. Notons P le polynôme irréductible de α sur L. Notons $C \subset L$ l'ensemble des coefficients de P de sorte que $P \in K(C)[X]$.

Puisque P est irréductible dans $L[X]$, il l'est aussi dans $K(C)[X] \subset L[X]$. A fortiori, α est séparable sur $K(C)$ et le Théorème A.2.5 donne que le nombre de prolongements tout morphisme $K(C) \to \overline{K}$ à $K(C)(\alpha)$ est $[K(C)(\alpha):K(C)]$.

Or, d'après le Lemme A.2.10, $K(C)$ est séparable sur K donc il y a $[K(X):K]$ prolongements de $K \hookrightarrow \overline{K}$ à $K(C)$ (Théorème A.2.5). Ce qui précède donne que chacun d'eux possède $[K(C)(\alpha):K(C)]$ prolongements à $K(C)(\alpha)$.

Finalement, $K \hookrightarrow \overline{K}$ admet $[K(C)(\alpha):K(C)][K(C):K] = [K(C)(\alpha):K]$ prolongements et le Théorème A.2.5 donne la séparabilité de $K(C)(\alpha)/K$ et en particulier celle de α.
□

Lemme A.2.11:

Soit K un corps de caractéristique p et L/K une extension de degré d premier avec p. Alors L/K est séparable.

Preuve :

Soit $x \in L$, et notons f le polynôme minimal de x sur K. Celui-ci est de degré $d'|d$ donc premier avec p. Alors, $f' \neq 0$ donc f et f' sont premiers entre eux et f est séparable.
□

Références

[1] Grégory Berhuy. *Algèbre : le grand combat*. Première édition. Calvage & Mounet, 2018.

[2] Daniel J. Bernstein et al. "Faster computation of isogenies of large prime degree". In : *Open Book Series* 4.1 (2020), p. 39-55. DOI : 10.2140/obs.2020.4.39. URL : https://msp.org/obs/2020/4-1/p04.xhtml.

[3] Reinier Broker. "Constructing supersingular elliptic curves". In : *Frontiers of Combinatorics and Number Theory* (2009).

[4] Bas Edixhoven, Gerard van der Geer et Ben Moonen. *Abelian Varieties*. URL : http://van-der-geer.nl/~gerard/AV.pdf.

[5] Steven Galbraith. "9. Elliptic Curves". In : *Mathematics of Public Key Cryptography*. 2012. URL : https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch9.pdf.

[6] Robin Hartshorne. *Algebraic Geometry*. T. 52. Graduate Texts in Mathematics. Springer, 1977. DOI : 10.1007/978-1-4757-3849-0. URL : http://link.springer.com/10.1007/978-1-4757-3849-0.

[7] David Jao et Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In : *Cryptology ePrint Archive* (2011). URL : https://eprint.iacr.org/2011/506.

[8] Bruce W. Jordan, Allan G. Keeton et Bjorn Poonen. *Unique factorization of principally polarized abelian varieties*. 2016. DOI : 10.48550/arXiv.1602.06811. URL : http://arxiv.org/abs/1602.06811.

[9] J S Milne. *Abelian Varieties*. 2008. URL : https://www.jmilne.org/math/CourseNotes/AV.pdf.

[10] Paul Pollack et Enrique Trevino. *Finding The Four Squares In Lagrange's Theorem*. 2018. URL : https://campus.lakeforest.edu/trevino/finding4squares.pdf.

[11] Ryan Rueger. *Computing the isogeny class-group action on ordinary elliptic curves by going into higher dimensions*. 2024. URL : https://rueg.re/2024-rrueger-msc-ordinary-icga-hd.pdf.

[12] Igor R. Shafarevich. *Basic Algebraic Geometry 1 : Varieties in Projective Space*. Springer, 2013. DOI : 10.1007/978-3-642-37956-7. URL : https://link.springer.com/10.1007/978-3-642-37956-7.

[13] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. T. 106. Graduate Texts in Mathematics. Springer, 1986. DOI : 10.1007/978-1-4757-1920-8. URL : http://link.springer.com/10.1007/978-1-4757-1920-8.

[14] Andrew Sutherland. *18.783 - Elliptic Curves*. 2025. URL : https://math.mit.edu/classes/18.783/2025/lectures.html.

[15] Andrew Sutherland. *23-The Weil pairing.pdf*. 2025. URL : https://math.mit.edu/classes/18.783/2025/LectureNotes23.pdf.

[16] Andrew Sutherland. *5-Isogeny kernels and division polynomials.pdf*. 2025. URL : https://math.mit.edu/classes/18.783/2025/LectureNotes5.pdf.

[17] Andrew Sutherland. *7-Hasse's Theorem, point counting.pdf*. 2025. URL : https://math.mit.edu/classes/18.783/2025/LectureNotes7.pdf.