UNIVERSITE ASSANE SECK DE ZIGUINCHOR

U.F.R DES SCIENCES ET TECHNOLOGIES

DÉPARTEMENT DE MATHÉMATIQUES

Mémoire de Master

DOMAINE : Sciences et Technologies
MENTION : Mathématiques et Applications
SPÉCIALITÉ : Mathématiques Pures
OPTION : Géométrie Algébrique

Théme :

Isogénie entre courbes elliptiques

Présenté par : Souleymane DIEDHIOU

Sous la direction de : Professeur Oumar SALL

Date : 28 Août 2020

Devant le jury ci-après :

Prénom(s) et Nom	Grade	Qualité	Établissement
Salomon SAMBOU	Professeur titulaire	Président du jury	UASZ
Amoussou Thomas GUEDENON	Maître de conférences	Examinateur	UASZ
Moussa FALL	Assistant	Examinateur	UASZ
Oumar SALL	Professeur titulaire	Directeur	UASZ

Année universitaire : 2019-2020

Remerciements

Tout d'abord, je tiens à exprimer ma gratitude à mon directeur de mémoire,
Monsieur Oumar SALL, pour l'encadrement dont j'ai bénéficié de sa part tout au long de ce travail de mémoire. Je salue ses pertinentes remarques qui sont très enrichissantes ses, "re cadrages" et ses précieux conseils m'ont toujours aidé à avancer dans mes travaux.
Je suis honoré par la présence de Monsieur Salomon SAMBOU qui a accepté de présider le Jury de mon mémoire, je vous remercie du fond de mon coeur.
Je remercie Monsieur Amoussou Thomas GUEDENON et Monsieur Moussa FALL pour avoir accepté de faire partie du Jury.
Nos remerciements vont à l'endroit de tous les professeurs du département de Mathématiques de l'université Assane SECK de Ziguinchor, pour la qualité des enseignements qu'ils nous ont dispensés, particulièrement à Salomon SAMBOU, Amoussou Thomas GUEDENON,
Alassane DIEDHIOU, Diéne NGOM, Timack NGOM, Clément MANGA, Daouda Niang DIATTA, Mansour SANE et Moussa FALL.
Je n'oublie pas les professeurs de l'université Cheikh Anta DIOP de Dakar particulièrement à Diaraf SECK et Bacary MANGA.
Merci encore !
Je dis merci à ma femme Adama Awa DIALLO, mon fils Arouna DIEDHIOU et mes parents pour leurs soutiens permanents et encouragements incessants.
Mes remerciements s'adressent à mes camarades de promotion, mes amis et mes collègues dont les encouragements m'ont permis de ne pas dévier de mon objectif final. Merci à Moustapha CAMARA, Papa BADIANE , Nestor DJINTELBE, Winnie Ossete INGOBA, Kang-rang SETH KOUMLA$\cdots$
Mes remerciements s'adressent également à docteur Mbaye Diagne MBAYE, docteur Lat-Grand NDIAYE, docteur Souhaibou SAMBOU et docteur chérif Mamina COLY pour divers services qu'ils m'ont rendus.

Table des matières

Résumé

Depuis le milieu des années 1980, les variétés abéliennes ont été abondamment utilisées en cryptographie à clé publique : le problème du logarithme discret et les protocoles qui s'appuient sur celles-ci permettent le chiffrement asymétrique, la signature, l'authentification. Dans cette perspective, les courbes elliptiques constituent l'un des exemples les plus intéressants de variétés abéliennes principalement les variétés abéliennes polarisées.
Ce travail a permis de revoir la construction de lois d'addition complète sur les courbes elliptiques.
Finalement nous présentons des isogénies entre variétés abéliennes.
La majorité des résultats de ce mémoire sont valides pour des variétés abéliennes de genre quelconque. Nous nous sommes cependant concentrés sur les variétés abéliennes de genre 1 (c'est à dire les courbes elliptiques) ce qui est plus intéressant en pratique.

Introduction

La géométrie algébrique est un domaine des mathématiques qui s'intéresse à l'étude des variétés algébriques qui sont des ensembles définis par l'annulation d'un ou plusieurs polynômes. Le présent mémoire est intitulé *Isogénie entre courbes elliptiques* qui est un morphisme surjectif et de noyau fini entre variétés abéliennes. Ce sont des objets fondamentaux dans l'étude de ces variétés, et donc des courbes algébriques en général.
Les isogénies sont les flèches non triviales dans la catégorie des courbes elliptiques sur un corps k donné, ce sont des quasi-isomorphismes dans certain sens.
les isogénies sont aussi étroitement liées aux sous-groupes de torsions sur les courbes elliptiques.
L'objectif de ce travail de mémoire est double d'une part de mettre en place l'ensemble des outils nécessaires pour la compréhension du sujet et d'autre part de donner quelques applications

Ce document est organisé comme suit :
Dans un premier temps, on expose le matériel nécessaire (ensembles algébriques, courbes algébriques, courbes elliptiques, variétés abéliennes, morphismes, isomorphismes...) qui permet d'aborder le sujet, et enfin on s'intéresse à des applications.

Chapitre 1

Ensembles algébriques

Dans la totalité de ce cours, on considère un corps commutatif k et $\overline{k}$ sa clôture algébrique. la géométrie algébrique s'intéresse aux ensembles définis par des équations polynomiales, c'est à dire les parties $\mathcal{P}$ de k^n définies par l'annulation d'une famille de polynômes de $k[X_1, \ldots, X_n]$. Par exemple :

$$\mathcal{P}_1 = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 + 1 = 0\} \tag{1.1}$$
$$\mathcal{P}_2 = \{(x, y) \in \mathbb{C}^2; x^2 + y^2 + 1 = 0\} \tag{1.2}$$
$$\mathcal{P}_3 = \{(x, y) \in \mathbb{Q}^3; x^2 + y^2 + 1 = 0\}(n \geqslant 1) \tag{1.3}$$

1.1 Ensembles algébriques affines

Définitions 1.1.1 *1. On appelle espace affine de dimension n, et on note $\mathbb{A}^n(k)$ ou encore $\mathbb{A}^n$, l'ensemble k^n, produit cartésien itéré n fois du corps k.*

2. Les éléments de l'espace affine sont appelés points.

3. $\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite et plan affine.

4. Un point a de $\mathbb{A}^n$ est dit zéro de $P \in k[X_1, \ldots, X_n]$ si $P(a) = 0$.

Définition 1.1.2 *Soit S une partie quelconque de $k[X_1, \ldots, X_n]$. On pose :*

$$\mathcal{V}(S) = \{a \in \mathbb{A}^n | \ \forall \ P \in \mathcal{S}, \ P(a) = 0\} \tag{1.4}$$

de sorte que les $a \in \mathcal{V}(S)$ sont les zéros communs à tous les polynômes de S. On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S.
On notera souvent, dans un ensemble fini $\mathcal{V}(P_1, \ldots, P_r)$ au lieu de $\mathcal{V}(\{P_1, \ldots, P_r\})$.
Soit $S = (P_i)_{i \in \mathcal{I}}$ une famille d'éléments de $k[X_1, \ldots, X_n]$; On note $\mathcal{V}(S) = \cap_{i \in I} \mathcal{V}(P_i)$.

Définition 1.1.3 *On appelle hypersurface définie par $f \in k[X_1, \ldots, X_n]$, l'ensemble des zéros de f (pour f non constant et k algébriquement clos) et l'on note $\mathcal{V}(f)$.*

Exemples 1.1.1

1. *Le vide et l'espace tout entier sont des ensembles algébriques affines. En effet, on a : $\mathcal{V}(1) = \varnothing$, car le polynôme le constant 1 ne s'annule jamais et $\mathcal{V}(0) = k^n$, car le polynôme constant 0 est identiquement nul.*
2. *Si $n = 1$ et si S n'est pas réduit à 0, $\mathcal{V}(S)$ est un ensemble fini : les ensembles algébriques affines de la droite affine sont la droite et les ensembles finis.*

Remarques 1.1.1

1. *Soit* $\mathcal{V}(S) = \{a \in \mathbb{A}^n \mid \forall\ P \in S,\ P(a) = 0\}$
   Si deux polynômes P_1 *et* P_2 *s'annulent sur* $\mathcal{V}(S)$*, il en sera de même pour* $P_1 + P_2$ *et* λP_1 *pour tout* $\lambda \in k$*. Ainsi, au lieu d'une famille quelconque de polynômes, on s'intéresse aux idéaux de* $k[X_1, \ldots, X_n]$*.*

2. *L'application* $\mathcal{V}$ *est décroissante : si* $S_1 \subset S_2$ *alors* $\mathcal{V}(S_2) \subset \mathcal{V}(S_1)$ *.*
3. *Si* $S \subset k[X_1, \ldots, X_n]$*, notons* $\langle S \rangle$ *l'idéal engendré par* S *:*
   $\langle S \rangle = \{P \mid P = \sum_{i=1}^{r} \lambda_i P_i,\ \text{avec } P_i \in S \text{ et } \lambda_i \in k\}$.
   Alors, par décroissance de $\mathcal{V}$*, on a* $\mathcal{V}(\langle S \rangle) \subset \mathcal{V}(S)$ *. Réciproquement, si* $a \in \mathcal{V}(S)$*, il annule les polynômes* $P_i \in S$*, ce qui montre que les polynômes* $P \in \langle S \rangle$ *.*
   Ainsi, on a $\mathcal{V}(\langle S \rangle) = \mathcal{V}(S)$ *; on peut donc, pour étudier les ensembles algébriques affines, se limiter aux* S *qui sont des idéaux, ou, au contraire, aux générateurs de ceux-ci.*
4. *Comme* $k[X_1, \ldots, X_n]$ *est noethérien, tout idéal* $\mathfrak{I}$ *est de type fini* $\mathfrak{I} = (P_1, \ldots, P_r)$

Propositions 1.1.1

1. *Un point de* k^n *est un ensemble algébrique affine.*

2. *Une intersection quelconque d'ensembles algébriques affines est un ensemble algébrique affine :*
$$\cap_i \mathcal{V}(S_i) = \mathcal{V}(\cup_i S_i)$$

3. *Une réunion finie d'ensembles algébriques affines est un ensemble algébrique affine.*

Preuve :

1. Si $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$, on a $\{a\} = \mathcal{V}(X_1 - a_1, \ldots, X_n - a_n)$
2. On a

$$\begin{aligned} a \in \mathcal{V}(\cup_i S_i) &\iff \forall\ P \in\ \cup_i S_i, P(a) = 0 \\ &\iff \forall\ i, \forall\ P \in S_i, P(a) = 0 \\ &\iff \forall\ i,\ a \in \mathcal{V}(S_i \\ &\iff a \in \cap_i \mathcal{V}(S_i) \end{aligned}$$

3. On a

$$\begin{aligned} a \in \mathcal{V}(S) \cup \mathcal{V}(T) &\iff a \in \mathcal{V}(S)\ ou\ a \in \mathcal{V}(T) \\ &\iff \forall\ P \in S,\ P(a)\ = 0\ ou \forall\ G \in T,\ G(a) = 0 \\ &\iff \forall\ P \in S, \forall\ G \in T, P(a) = 0\ ou\ G(a) = 0 \\ &\iff \forall\ a \in \mathcal{V}(PG,\ P \in S,\ G \in T). \end{aligned}$$

Conséquences 1.1.1

1. *Tout ensemble fini est algébrique.*
   En effet, il suffit d'appliquer 1) *et* 3) *de la proposition précédente.*
2. *Tout sous-ensemble algébrique propre est une intersection d'hypersurfaces.*
   En effet, on a
   $$\mathcal{V}(S) = \mathcal{V}(\cup_{P\in S}(P)) = \cap_{P\in S}\mathcal{V}(P)$$

Puisque $\mathcal{V}(S)$ est non vide, aucun des $P \in S \setminus 0$ n'est constant et les $\mathcal{V}(P)$ sont donc bien des hypersurfaces.

Remarque 1.1.2 *Un ensemble algébrique peut être défini par plusieurs idéaux.*
Par exemple, les idéaux
$$I = \langle X^2 + Y^2, XY^3\rangle et J = \langle X^2, Y^3\rangle$$
de $\mathbb{C}[X, Y]$ définissent tous deux $(0, 0)$ dans $\mathbb{C}^2$

Définition 1.1.4 *Les ensembles algébriques de $\mathbb{A}^n$ définissent une topologie sur $\mathbb{A}^n$, dite topologie de Zariski, dont ils sont les fermés.*

Définition 1.1.5 *On appelle courbe algébrique plane un ensemble des points de $\mathbb{A}^2$ dont les coordonnées (x, y) satisfont l'équation*

$$f(x, y) = 0 \tag{1.5}$$

pour un polynôme $f \in k[X, Y]$. Une telle courbe est appelée courbe affine.
Voilà une définition équivalente à la précédente :

Définitions 1.1.6 *Une courbe affine plane est une hypersurface du plan affine.*
Notons $C_f \subset \mathbb{A}^2$ la courbe affine plane définie par f.
Le degré d'une courbe affine plane est le degré d'un polynôme qui la définit, c'est à dire, $deg(C_f) = deg(f)$.

Définitions 1.1.7

- *Une courbe algébrique plane est dite conique, cubique, quartique, ..., si le degré est respectivement* 2, 3, 4, ...
- *Un hyperplan est une hypersurface définie par f de degré* 1.
- *Une droite est un hyperplan de $\mathbb{A}^2$.*

Définitions 1.1.8 *Soient C une courbe algébrique et $P = (x, y)$ un point de C.*

1. *P est **ordinaire** si C admet en ce point une tangente unique qui ne la traverse pas.*
2. *P est un **point d'inflexion** si C admet en ce point une tangente unique qui la traverse.*
3. *P est un point singulier, si C admet en ce point deux tangentes distinctes.*
4. *P est un point non singulier, **point de rebroussement**, si C admet en ce point deux tangentes confondues.*

1.1.1 Idéal d'un ensemble de points

Définitions 1.1.9 *Soit V une partie de $\mathbb{A}^n$. On appelle idéal de V dans $\mathbb{A}^n$, l'ensemble noté $\mathfrak{I}(V)$ défini par*

$$\mathfrak{I}(V) = \{P \in k[X_1, \ldots, X_n] \mid \forall\ a \in V,\ P(a) = 0\}. \tag{1.6}$$

On voit clairement que $\mathfrak{I}(V)$ est l'ensemble des polynômes nuls sur V. Si $\mathfrak{I}$ est un idéal de V, l'idéal

$$\sqrt{\mathfrak{I}} = \{F \in V \mid \exists\ m \in \mathbb{N}^*,\ F^m \in \mathfrak{I}\} \tag{1.7}$$

est appelé radical de $\mathfrak{I}$. Un idéal premier est radical. Un idéal $\mathfrak{I}$ de V est radical si et seulement si le seul élément nilpotent $V/\mathfrak{I}$ est 0. L'idéal d'une sous-variété affine est radical.
En particulier, on a

$$\sqrt{\mathfrak{I}} \subset \mathfrak{I}(\mathcal{V}(\mathfrak{I})).$$

Considérons des sous-variétés W et F avec $W \subset F$ et A l'anneau $k[X_1, \ldots, X_n]$ des polynômes à n indéterminées à coefficients dans k. On a $\mathfrak{I}(F) \subset \mathfrak{I}(W)$, de sorte que $\mathfrak{I}(W)$ est l'image inverse par la projection $\pi : A \to A(F)$ d'un idéal de $A(F)$, que l'on note $\mathfrak{I}_F(W)$ avec $A(F) = A/\mathfrak{I}(V)$ est dite algèbre quotient de V.

NB 1.1.1 *On montre facilement que $\mathfrak{I}(V)$ est un idéal de $k[X_1, \ldots, X_n]$; c'est même un idéal radical.*
En effet, si $F,\ G \in \mathfrak{I}(V)$ et $a \in V$, alors $(F+G)(a) = F(a) + G(a) = 0$. De même si $F \in k[X_1, \ldots, X_n], G \in \mathfrak{I}(V)$ et $a \in V$, alors $(FG)(a) = F(a)G(a) = 0$.
Enfin, si $F^r \in \mathfrak{I}(V)$ et $a \in V$, alors $F(a)^r = F^r(a) = 0$. Si bien que $F(a) = 0$ et donc $F \in \mathfrak{I}(V)$.

Propositions 1.1.2

i) On a $\mathfrak{I}(\varnothing) = k[X_1,\ \ldots, X_n]$ et $\mathfrak{I}(\mathbb{A}^n) = 0$.
ii) Si $\{A_i\}_{i \in I}$ est un ensemble de parties de $\mathbb{A}^n$, alors $\mathfrak{I}(\cup_i A_i) = \cap_i \mathfrak{I}(A_i)$.
iii) Si $A \subset B \subset \mathbb{A}^n$, alors $\mathfrak{I}(B) \subset \mathfrak{I}(A)$.

Preuve :

i) La condition pour appartenir à $\mathfrak{I}(\emptyset)$ est vide et on a donc $\mathfrak{I}(\emptyset) = k[X_1, \ldots, X_n]$. Aussi, si $P \in \mathfrak{I}(\mathbb{A}^n)$ alors $P(a) = 0, \forall a \in \mathbb{A}^n$; ce qui montre que P est identiquement nul.

ii) On a

$$\begin{aligned} P \in \mathfrak{I}(\cup_i A_i) &\Leftrightarrow \forall\ \ a \in (\cup_i A_i),\ P(a) = 0 \\ &\Leftrightarrow \forall\ i, \forall\ a \in A_i,\ P(a) = 0 \\ &\Leftrightarrow \forall\ i,\ P \in \mathfrak{I}(A_i) \\ &\Leftrightarrow P \in \cap_i \mathfrak{I}(A_i) \end{aligned}$$

(iii) On a

$$\begin{aligned} P \in \mathfrak{I}(B) &\Rightarrow \forall\ b \in B,\ P(b) = 0 \\ &\Rightarrow \forall\ a \in A,\ P(a) = 0 \\ &\Rightarrow\ P \in \mathfrak{I}(A). \end{aligned}$$

Remarques 1.1.3

- ⊙ *Pour toute partie $S \subset k[X_1, \ldots, X_n], S \subset \mathcal{V}(\mathfrak{I}(S))$; mais il n'y a en général pas égalités, même lorsque S est un idéal.*
- ⊙ *Pour toute partie $A \subset \mathbb{A}^n$, $A \subset \mathcal{V}(\mathfrak{I}(A))$; avec égalité si et seulement si A est affine. En fait, $\mathcal{V}(\mathfrak{I}(A))$ est l'adhérence de A (pour la topologie de Zariski).*

1.1.2 Irréductibilité

Définition 1.1.10 *On dit qu'un espace topologique E est irréductible s'il n'est pas vide et il n'est pas réunion de deux fermés distincts de E.*
On montre facilement que si E est non vide, E est irréductible si et seulement si deux ouverts non vides quelconques se rencontrent, c'est à dire si et seulement si tout ouvert non vide est dense.
Un ensemble algébrique est dit irréductible s'il est irréductible pour la topologie de Zariski

Proposition 1.1.3 *Un ensemble algébrique est irréductible si et seulement si son idéal est premier.*

Preuve : Soit A un ensemble algébrique.
C N $\Longrightarrow$) soient $F,\ G \in k[X_1, \ldots, X_n]$ tels que $FG \in \mathfrak{I}(A)$. On a :
$A \subset \mathcal{V}(FG) = \mathcal{V}(F) \cup \mathcal{V}(G)$, d'où
$A = A \cap (\mathcal{V}(F) \cup \mathcal{V}(G)) = (A \cap \mathcal{V}(F)) \cup (A \cap \mathcal{V}(G))$
de sorte que A est la réunion des fermés $(A \cap \mathcal{V}(F))$ et $(A \cap \mathcal{V}(G))$. Comme par hypothèse A est irréductible, l'un de ces fermés est égal à A, par exemple $A = A \cap \mathcal{V}(F)$. Ainsi $A \subset \mathcal{V}(F)$, ce qui montre que F s'annule sur A ; donc $F \in \mathfrak{I}(A)$.
C S $\Longleftarrow$) Raisonnons par absurde . Supposons A réunion de fermés propres A_1 et A_2 : $A = A_1 \cup A_2$. On a :
$A_i \subsetneq A \Rightarrow \mathfrak{I}(A) \subsetneq \mathfrak{I}(A_i)$
$\Rightarrow \exists\ F_i \in \mathfrak{I}(A_i)$ et $F_i \nexists \mathfrak{I}(A)$. Or $(F_1 \in \mathfrak{I}(A_1)\ et\ F_2 \in \mathfrak{I}(A_2)) \Rightarrow F_1F_2 \in \mathfrak{I}(A_1 \bigcup A_2)$
$\Rightarrow F_1F_2 \in \mathfrak{I}(A)$
Ce qui contredit le fait que $\mathfrak{I}(A)$ est premier .

NB 1.1.2 *Si on note $a = k[X_1, \ldots, X_n]$, on peut exprimer la condition de la proposition en demandant que l'algèbre quotient $a(A) = a/\mathfrak{I}(A)$, dite algèbre de A, soit intègre.*

Corollaire 1.1.1 *Si k est infini, $\mathbb{A}^n$ (c'est à dire k^n) est irréductible.*

Preuve :
Puisque k est infini, tout polynôme nul sur k^n est identiquement nul, de sorte que $\mathfrak{I}(\mathbb{A}^n) = 0$, qui est premier.

Théorème 1.1.1 *Tout ensemble algébrique non vide se décompose de façon unique (à permutation près) en une réunion finie de sous-ensembles algébriques irréductibles non contenu l'un dans l'autre.*

Preuve : Existence : Raisonnons par absurde.
Supposons qu'il existe un ensemble algébrique non vide qui ne se décompose pas en une réunion finie d'irréductibles ; soit $(A_i)_i$, la famille des ensembles algébriques non vides qui ne se décomposent pas en une réunion finie d'irréductibles. Comme $k[X_1, \ldots, X_n]$ est noethérien, la famille $(\mathfrak{I}(A_i))_i$ possède un élément maximal, donc $(A_i)_i$ admet un élément minimal V qui est forcément réductible. On peut écrire $V = V_1 \cup V_2$, avec V_i fermé non distinct de V. Par minimalité, V_i est réunion finie d'irréductibles, d'où la contradiction.
Unicité : Supposons qu'on ait deux écritures :
$V = V_1 \cup \ldots \cup V_r = W_1 \cup \ldots \cup W_s$.
On écrit

$$V_i = V \cap V_i = (W_1 \cup \ldots \cup W_s) \cap V_i = (W_1 \cap V_i) \cup \ldots \cup (W_s \cap V_i)$$

.
Comme V_i est irréductible, il existe j tel que $V_i = W_j \cap V_i$; d'où

$$V_i \subset W_j (\star).$$

De même on peut écrire $W_j = V \cap W_j = (V_1 \cup \ldots, V_r) \cap W_j = (V_1 \cap W_j) \cup, \ldots, \cup (V_r \cap W_j)$.
Comme W_j est irréductible, il existe l tel que $W_j = V_l \cap W_j$; d'où
$W_j \subset V_l$ $(\star\star)$ $(\star)$ et $(\star\star)$ montrent que $V_i \subset V_l$ et par hypothèse, ceci impose $i = l$, donc $V_i = V_l$.
Ainsi $V_i \subset W_j \subset V_l = V_i$, ce qui montre que $V_i = W_j$.

Remarque 1.1.4 *Si W est fermé irréductible de V, W est contenu dans une composante irréductible de V. Il en résulte que les composantes irréductibles sont exactement les sous-ensembles fermés irréductibles maximaux de V.*

Définition 1.1.11 *On appelle variété algébrique affine tout ensemble algébrique affine irréductible.*

Théorème 1.1.2 *On suppose que k algébriquement clos. Soit V et W deux variétés affines. L'application $W \to \mathfrak{I}_V(W)$ réalise une bijection décroissante, de réciproque $\mathfrak{I} \to \mathcal{V}(\Pi^{-1}(\mathfrak{I})$ entre*

(a) Les sous-variétés affines de V et les idéaux radicaux de $A(V)$ avec $A(V) = A/\mathfrak{I}(V)$ dite algèbre quotient de V ;

(b) Les sous-variétés affines irréductibles de V et les idéaux premiers de $A(V)$;

(c) Les points de V et les idéaux maximaux de $A(V)$.

Preuve : Soit x un point de V ; l'idéal $\mathfrak{I}_V(x)$(*souvent noté* m_x) des polynômes nuls en x est maximal dans $A(V)$: c'est le noyau du morphisme $A(V) \to k$ qui à $[F]$ associe $F(x)$. Cela démontre une partie de (c). Pour le reste, il suffit de remarquer qu'un idéal $\mathfrak{I}$ *de* $A(V)$ est radical (*resp. premier*) (*resp.maximal*) si et seulement si $\Pi^{-1}(\mathfrak{I})$ l'est, puisque ces propriétés se lisent sur le quotient $A(V)/\mathfrak{I}$, qui est isomorphe à $A/\Pi^{-1}(\mathfrak{I})$.
En particulier, les composantes irréductibles de V correspondent aux idéaux premiers minimaux de $A(V)$, et celles de W aux idéaux premiers minimaux de $A(V)$ contenant $\mathfrak{I}_V(W)$

1.1.3 Applications régulières

Définition 1.1.12 *Soient $V \subset k^n$ et $W \subset k^m$ des sous-variétés affines.*
Une application $V \to W$ est dite régulière si c'est la restriction à V d'une application $k^n \longmapsto W^m$ dont les composantes sont des fonctions polygonales.

Exemples 1.1.2 *Supposons k infini.*

1. *Soit C l'hypersurface plane d'équation $Y = X^2$.*
   L'application

$$\begin{aligned} f : C &\longrightarrow k \\ (x, y) &\longmapsto x \end{aligned}$$

   est régulière et bijective; son inverse $x \longmapsto (x, x^2)$ est régulière : on dit que f est un isomorphisme.

2. *Soit C l'hypersurface plane d'équation $Y^3 = X^2$.*
   L'application

$$\begin{aligned} \mu : k &\longrightarrow C \\ t &\longmapsto (t^3, t^2) \end{aligned}$$

   est régulière et bijective.

3. *On suppose k algébriquement clos de caractéristique $q > 0$.*
   L' application

$$\begin{aligned} \nu : k &\longrightarrow k \\ x &\longmapsto x^2 \end{aligned}$$

   (Dite "de Frobenius") est régulière et bijective.

Définition 1.1.13 *Une application régulière $\mu : V \longmapsto W$ est dite dominante si son image est dense.*

Remarques 1.1.5 *Soient $V \subset K^n$ et $W \subset k^m$ des sous-variétés affines et $\mu : V \longrightarrow W$ une application régulière.*
L'ensemble des fonctions régulières de V dans k s'identifie à l'algèbre $a(V) = a/\mathfrak{I}(V)$. On associe à μ un morphisme de k-algèbres

$$\mu^* : a(W) \longrightarrow a(V)$$

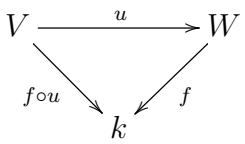
par la règle $f \longmapsto f \circ \mu$

Propositions 1.1.4

i) Une application régulière $\mu : V \longrightarrow W$ est dominante, si et seulement si, μ^* est injective.

ii) Si μ^* est surjective, μ est injective.

Preuve : $\mu^* : a(W) \longrightarrow a(V),\ f \longmapsto f \circ \mu$



(i) C N $\Longrightarrow$) *μ est dominante* $\Longrightarrow$ *$\mu*$ est injective*?.

$$\begin{aligned} f \in ker(\mu^*) &\Longrightarrow \mu^*(f) = 0 \\ &\Longrightarrow f \circ \mu = 0 \\ &\Longrightarrow fs'annule\ sur\ \mu(W) \\ &\Longrightarrow f \in \mathfrak{J}(\mu(V)) \\ &\Longrightarrow f \in \mathfrak{J}(\overline{\mu(V)} \\ &\Longrightarrow f \in \mathfrak{J}(W)\ car\ \overline{\mu(V)} = W\ puisque\ \mu\ est\ dominante \end{aligned}$$

C S $\Longleftarrow$) *μ non dominante* $\Longrightarrow$ *μ^* non injective*?

$$\begin{aligned} \mu\ non\ dominante &\Longrightarrow \mu(V) \neq \overline{\mu(V)} \subset W \\ &\Longrightarrow \mu(V) \neq W \\ &\Longrightarrow \exists\ f :\ W \longrightarrow k\ régulière, nulle\ sur\ \mu(V)\ mais\ pas\ sur\ W \\ &\Longrightarrow f \in ker(\mu^*) \end{aligned}$$

(ii) *μ^* est surjective* $\Longrightarrow$ *μ est injective*?
Soient $x,\ y$ deux points distincts de V. Il existe une fonction régulière $h : V \longrightarrow k$ nulle en x mais pas en y (prendre par exemple une fonction coordonnée).
μ^* est surjective $\Longrightarrow \exists$ une fonction régulière $g :\longrightarrow k, h = \mu^*(g) = g \circ \mu$.
On a

$$\left.\begin{array}{l} h(x) = g \circ \mu(x) = 0 \\ h(y) = g \circ \mu(y) = g(\mu(y)) \neq 0 \end{array}\right\} \Longrightarrow \mu(x) \neq \mu(y)$$

1.2 Ensembles algébriques projectifs

Dans la suite, R désignera l'anneau $k[X_1, \ldots, X_n]$; on garde notre espace affine $\mathbb{A}^n$ de dimension n sur k.

1.2.1 L'espace projectif

Considérons la relation $\Re$ *sur* $k^{n+1} \setminus \{0\}$ définie par : pour tous vecteurs non nuls x et y, on a
$x\Re y$ si et seulement s'ils sont colinéaires, c'est à dire,

$$x\Re y \Leftrightarrow \exists\ \lambda \in k^\star : y = \lambda x$$

On montre que $\Re$ est une relation d'équivalence sur $k^{n+1} \setminus \{0\}$. Ainsi deux vecteurs non nuls sont équivalents s'ils sont colinéaires.

Définitions 1.2.1 *On appelle espace projectif de dimension n sur k, et l'on note* $\mathbb{P}^n$(*ou* $\mathbb{P}^n(k)$) *ou encore* $\mathbb{P}$ *l'ensemble des classes d'équivalence par* $\Re$.
En d'autres termes, $\mathbb{P}^n$ *est l'ensemble des droites vectorielles de* k^{n+1}. *Si un point* $P \in \mathbb{P}^n$ *a pour vecteur directeur (représentant)* $(x_0, \ldots, x_n) \in k^{n+1} - \{0\}$, *on écrit* $P = (x_0 : \ldots : x_n)$; *on dit que* $(x_0 : \ldots : x_n)$ *est un système de coordonnées homogènes de* P *et ils ne sont définis qu'à multiplication par un scalaire non nul près.*
On dit que $\mathbb{P}^1$ *est la droite projective sur* k, *et que* $\mathbb{P}^2$ *est le plan projectif sur* k.
On dit que P *est un zéro de* $F \in k[X_0, \ldots, X_n]$ *si* $F(P) = 0$; *pour tout choix de coordonnées homogènes* $(x_0 : \ldots : x_n)$ *de* P, $F(P) = 0$ *est noté* $F(x_0, \ldots, x_n) = 0$. *On montre qu'un point* $P = (x_0 : \ldots : x_n)$ *est zéro de* F *si et seulement si* $F(\lambda x_0, \ldots, \ldots \lambda x_n) = 0$, *pour tout* $\lambda \in k^*$.
Si E *est un* $k-$*espace vectoriel non nul de dimension finie* n, *on définit de la même manière l'espace projectif associé à* E *noté* $\mathbb{PE}$ (*ou* $\mathbb{P}(E)$) *de dimension* $n-1$. *En particulier,* $\varnothing = \mathbb{P}(\{0\})$ *est un espace projectif de dimension* -1.
Si F *est un sous espace vectoriel non nul de* E, *L'inclusion* $F \setminus \{0\} \subset E \setminus \{0\}$ *induit une inclusion* $\mathbb{P}(F) \subset \mathbb{P}(E)$. *Les sous-ensembles* $\mathbb{P}(E)$ *ainsi obtenus sont appelés sous-ensembles linéaires de* $\mathbb{P}(E)$; *on a* $\mathbb{P}(F) \cap \mathbb{P}(F') = \mathbb{P}(F \cap F')$.
Pour chaque $i = 1, 2 \ldots, n$, *on définit un sous-ensemble* U_i $\mathbb{P}^n$ *par :*

$$U_i = \{P = (x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}.$$

Chacun des U_i *est isomorphe à* $\mathbb{A}^n$:

$$U_i \approx \mathbb{A}^n, (x_0 : \ldots : x_n) = (\frac{x_0}{x_i}, \ldots\ldots, \frac{x_0}{x_i})$$

Les U_i *recouvrent* $\mathbb{P}^n$. *Le complémentaire de* U_i *est l'espace linéaire* $\mathbb{P}(H_i)$; *où* H_i *est l'hyperplan d'équation* $x_i = 0$ *dans* k^{n+1}. $\mathbb{P}^n$ *peut être obtenu à partir de* $\mathbb{A}^n$ *en adjoignant un "hyperplan à l'infini. Par exemple, la droite projective* $\mathbb{P}^1$ *est obtenue en adjoignant à* k *un unique point à l'infini. Plus généralement, le complémentaire dans* $\mathbb{P}^n$ *de n'importe quel hyperplan projectif s'identifie naturellement à* $\mathbb{A}^n$.

Définition 1.2.2 *On dit que des points de* $\mathbb{P}^n$ *sont linéairement indépendants si les droites de* k^{n+1} *qu'ils représentent sont en somme directe. On dit que des points de* $\mathbb{P}^n$ *sont en position générale, si pour tout* $m \leq n+1$, m *quelconques d'entre-eux sont linéairement indépendants.*
La proposition suivante, illustre une des propriétés fondamentales de l'espace projectif : Il n'y a pas de sous-espaces parallèles, ils se rencontrent à «l'infini».

Proposition 1.2.1 *Soient* $\mathbb{P}(F)$ *et* $\mathbb{P}(F')$ *deux sous-espaces linéaires de* $\mathbb{P}^n(k)$ *de dimensions respectives* r *et* r' *vérifiant* $r + r' \geq n$.
Alors l'intersection $\mathbb{P}(F) \cap \mathbb{P}(F') = \mathbb{P}(F \cap F')$ *est un sous-espace linéaire de dimension* $\geq r + r' - n$, *il est en particulier non vide.*

Preuve : Écrivons $\mathbb{P}^n(k) = \mathbb{P}(E)$, *on a* : $dimF = r+1, dimF' = r'+1$ *et* $dimE = n+1$. $dim(F \cap F') = dimF + dimF' - dim(F + F')$; *or* $F + F'$ est un sous-espace vectoriel de E, d'où $dim(F + F') \leq dimE$, *et par suite* $dim(F \cap F') \geq dimF + dimF' - dimE = r + r' - n + 1 \geq r + r' - n$. Ainsi on déduit l'inégalité $dim(F \cap F') \geq r + r' - n$.

1.2.2 Variétés projectives

Définition 1.2.3 *Un élément* F *de* R *est dit homogène de degré* d *si, pour tout* $\lambda \in k^*$, *on a*

$$F(\lambda X_0, \ldots, \lambda X_n) = \lambda^d F(X_0, \ldots, X_n). \tag{1.8}$$

Une conséquence immédiate est que, si F est homogène, on a pour tout $\lambda \neq 0$
$F(x_0, \ldots, x_n) = 0$ si et seulement si $F(\lambda x_0, \ldots, \lambda x_n) = 0$
Tout polynôme se décompose de façon unique en somme de polynômes homogènes.

Définition 1.2.4 *Soit S une partie de $k[X_0, \ldots, X_n]$ formée de polynômes homogènes. On pose :*

$$\mathcal{V}(S) = \{P = (x_0 : \ldots : x_n) \in \mathbb{P}^n \mid \forall\ F \in \mathcal{S},\ F(P) = 0\}, \tag{1.9}$$

de sorte que les $\mathcal{V}(S)$ sont les zéros communs à tous les polynômes de S.
On dit que $\mathcal{V}(S)$ est l'ensemble algébrique projectif défini par S. On notera souvent, dans le cas d'un ensemble fini, $\mathcal{V}(F_1, \ldots, F_r)$ au lieu de $\mathcal{V}(\{F_1, \ldots, F_r\})$.

Définition 1.2.5 *On appelle hypersurface définie par un polynôme F homogène en $n+1$ variables, et on note $\mathcal{V}(F)$, l'ensemble des zéros de F (pour F non constant et k algébriquement clos).*

1.2.3 Courbes projectives planes

Définition 1.2.6 *On appelle courbe algébrique plane un ensemble de points de $\mathbb{P}^2$ dont les coordonnées (X, Y, Z) satisfont l'équation*

$$F(X, Y, Z) = 0 \tag{1.10}$$

pour un polynôme $F \in k[X, Y, Z]$. Une telle courbe est appelée courbe projective plane.
Voilà une définition équivalence à la précédente :

Définition 1.2.7 *Une courbe projective plane est une hypersurface de $\mathbb{P}^2$.*

Définitions 1.2.8

- *Une courbe projective plane est dite conique, cubique, quartique, quintique ... Si le degré est respectivement* 2, 3, 3, 4, 5 ...
- *Un hyperplan est une hypersurface définie par un polynôme homogène de degré* 1.
- *Une droite est un hyperplan de $\mathbb{P}^2$.*
  Notons $C_F \subset \mathbb{P}^2$ la courbe définie par F. Le degré d'une courbe est le degré d'un polynôme homogène qui la définit (c'est à dire $deg(C_F) = deg(F)$).

Définitions 1.2.9

1. *Un polynôme est irréductible lorsqu'il n'est pas factorisable.*
2. *une courbe C est irréductible si le polynôme F est irréductible.*
3. *On dit que deux courbes C_1 et C_2 n'ont pas de composantes communes quand leurs composantes irréductibles sont distinctes.*

Définition 1.2.10 *Un point P d'une courbe $C : F(X, Y, Z) = 0$ est dit singulier si*

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0 \tag{1.11}$$

Définitions 1.2.11 *Une courbe C est lisse en un point $P \in C$ si*

$$(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)) \neq (0,0,0) \tag{1.12}$$

Si tel est le cas alors la droite tangente à C au point P est la droite

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0. \tag{1.13}$$

La courbe C est lisse si elle est lisse en tout point.

Définition 1.2.12 *Le genre g d'une courbe lisse de degré d est défini par*

$$g = \frac{(d-1)(d-2)}{2} \tag{1.14}$$

Définitions 1.2.13 *Soit C_F une courbe projective plane définie par un polynôme homogène $F \in k[X,Y,Z]$. L'ensemble des points $k-$rationnels de C_F est*

$$C_F(k) = \{(X:Y:Z) \in \mathbb{P}^2 \mid F(X,Y,Z) = 0\}. \tag{1.15}$$

Un point P est $k-$rationnel si ses coordonnées sont dans k.

Théorème 1.2.1 *(faible de Bezout)*
Deux courbes planes de degrés m et n sans composantes communes ont exactement mn points d'intersection.

Définition 1.2.14 *On dit qu'un idéal $\mathfrak{I}$ de R est homogène s'il est engendré par des polynômes homogènes. On note $\mathcal{V}(\mathfrak{I})$ le sous-ensemble de $\mathbb{P}^n$ formé des zéros communs à tous les éléments homogènes de $\mathfrak{I}$.*
Pour qu'un idéal $\mathfrak{I}$ de R soit homogène, il faut et il suffit que pour toute décomposition $F = \sum F_i$ d'un élément F de $\mathfrak{I}$ en somme de polynômes homogènes, on ait $F_i \in \mathfrak{I}$ pour tout i.

Remarques 1.2.1 *On retrouve beaucoup de résultats obtenus dans l'espace affine (mais pas tous !).*

1. *L' application $S \longrightarrow \mathcal{V}(S)$ est décroissante pour l'inclusion*
2. *Si S est formé de polynômes homogènes, l'idéal $\langle S \rangle$ est engendré par S est homogène, et l'on a $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$*

3. *L'anneau R étant noethérien, on vérifie que l'idéal $\langle S \rangle$ est engendré par un nombre fini de polynômes homogènes $F_1, \ldots, F_r$, de sorte que $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle) = \mathcal{V}(F_1, \ldots, F_r)$. En d'autres termes, tout ensemble algébrique projectif peut être défini par un nombre fini d'équations.*

4. *Une intersection quelconque d'ensembles algébriques projectifs est un ensemble algébrique projectif :*
$$\cap_i \mathcal{V}(S_i) = \mathcal{V}(\cup_i S_i)$$

5. *Une réunion finie d'ensembles algébriques projectifs est un ensemble algébrique projectif.*

Définition 1.2.15 *Soit V une partie de $\mathbb{P}^n$. On appelle idéal de V dans $\mathbb{P}^n$, l'ensemble noté $\mathfrak{I}(V)$ défini par*

$$\mathfrak{I}(V) = \{F \in k[X_0, \ldots, X_n] \text{ homogne} \mid \forall\ P \in V,\ F(P) = 0\}$$

On voit clairement que $\mathfrak{I}(V)$ est l'ensemble des polynômes homogènes nuls sur V. On a $\mathcal{V}(\mathfrak{I}(V))$ est l'adhérence de V (pour la topologie des Zariski).
Les résultats sur la décomposition d'un ensemble algébrique affine en composantes irréductibles se transportent tels quels au cadre projectif.

Définition 1.2.16 *Un ensemble algébrique projectif E est dit irréductible s'il est irréductible pour la topologie de Zariski. Comme en affine, E est irréductible si et seulement si $\mathfrak{I}(V)$ est premier. Un tel E est appelé variété projective.*

1.2.4 Applications régulières

Dans ce paragraphe, k désigne un corps algébriquement clos.

Définition 1.2.17 *On appelle variété quasi-projective, tout ouvert (de Zariski) d'une variété projective.*

Remarque 1.2.2 *Lorsque nous dirons que X est une variété, il sera toujours sous-entendu que X est quasi-projective, en revanche, lorsque nous dirons que Y est une sous-variété de X, il sera toujours sous-entendu, sauf mention du contraire, que Y est fermé dans X.*
L'idée de base que si un polynôme, même homogène, ne définit pas de fonction sur $\mathbb{P}^n$, le F/G de polynômes homogènes de même degré définit une fonction sur l'ouvert où G ne s'annule pas.

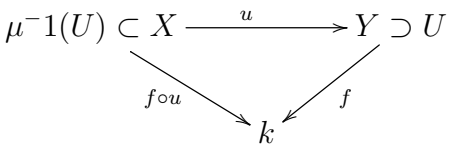
Définition 1.2.18 *Soit X un espace topologique. La dimension de X est le maximum des entiers m pour lesquels il existe des parties irréductibles fermées $X_0 \subsetneq \cdots \subsetneq X_m$.*
La dimension d'un ensemble algébrique est donc un entier positif ou $+\infty$ ou $-\infty$ si X est vide.

Remarque 1.2.3 *Si X est réunion de fermés $X_1, \cdots, X_l$, on a $dim X = max dim X_i$. On constate que la dimension d'un ensemble algébrique est le maximum des dimensions de ses composantes irréductibles.*

Proposition 1.2.2 *Toute variété algébrique est de dimension finie et tout ouvert dense est de même dimension.*
Une variété algébrique est de dimension 0 si et seulement si il existe en un nombre fini non nul de points.

Définition 1.2.19 *Soient X une sous-variété quasi-projective de $\mathbb{P}^n$ et $x \in X$. Une fonction $f : X \longrightarrow k$ est dite régulière en x, s'il existe des polynômes homogènes F et G de même degré avec $G(x) \neq 0$ et $f = F/G$ dans un voisinage de x dans X.*
On dit que f est régulière sur X, si elle est régulière en tout point de X. On note $A(X)$ l'ensemble des fonctions régulières sur X.

Définition 1.2.20 *Soient X et Y des variétés quasi-projectives. On dit qu'une application $\mu : X \longrightarrow Y$ est régulière si elle est continue et si, pour tout ouvert U de Y et toute fonction régulière $f : U \longrightarrow k$, la compose $f \circ \mu$ est régulière sur $\mu^-1(U)$.*



Théorème 1.2.2 *Soit X une sous-variété affine de $\mathbb{A}^n$; toute fonction régulière $f : X \to k$ est définie globalement par un polynôme à n variables.*

Preuve : On supposera pour simplifier que X est irréductible. Comme X est quasi-compact, il existe un nombre fini d'ouverts U_i qui recouvrent X, et des polynômes G_i *et* H_i *tels que* H_i ne s'annule pas sur U_i et que $f = G_i/H_i$ sur U_i. Pour tout i et j, cela signifie que $G_iH_j - G_jH_i$ est nul sur l'ouvert $U_i \cap U_j$ dense dans X, donc sur X. Les H_j n'ayant pas de zéro commun dans X, il existe des fonctions polynomiales a_j sur X telles que $\sum_j a_jH_j = 1$. Notons s la fonction polynomiale $\sum_j a_jG_j$ sur X ; on a

$$H_i s = H_i(\sum_j a_jG_j) = \sum_j a_jG_iH_j = G_i,$$

de sorte que s coïncide avec f sur chaque U_i. Elle est donc égale à f.
Le théorème n'est plus vrai sur un corps quelque (comme le montre l'exemple de la fonction $f : \mathbb{R} \to \mathbb{R}$ *qui a* t *associe* $1/(1+t^2)$.

Exemples 1.2.1
L'application $\mu : \mathbb{P}^1 \longrightarrow \mathbb{P}^3$ $dfinie$ par $\mu(x_0, x_1) = (x_0^3, x_0^2x_1, x_0x_1^2, x_1^3)$ est régulière.
Plus généralement, si on se donne des polynômes homogènes $F_0, \ldots, F_m$ de même degré en $n+1$ variables, l'égalité $\mu(x) = (F_0(x), \ldots, F_m(x))$ définit une application régulière

$$\mu : \mathbb{P}^n - \mathcal{V}(F_0, \ldots, F_m) \to \mathbb{P}^m$$

En particulier, si $F_0, \ldots, F_m$ ne s'annulent simultanément qu'en 0, l'application μ est définie sur tout $\mathbb{P}^n$. C'est sous cette forme plus concrète que l'on rencontre le plus souvent une application régulière.

Exemples 1.2.2 *(Applications de Véronese)*
Soient $M_0, \ldots, M_N$ tous les monômes de degré d en $X_0, \ldots, X_n$. Ils forment un espace vectoriel de dimension C_{n+d}^d donc $N = \mathsf{C}_{n+d}^d - 1$.
On obtient une application régulière injective

$$\mu_d : \mathbb{P}^n \to \mathbb{P}^N$$

La proposition suivante montre qu'une application régulière est toujours définie localement comme dans l'exemple 3

.

Proposition 1.2.3 *Soit X une sous-variété quasi-projective de $\mathbb{P}^n$ et $\mu : X \to \mathbb{P}^n$ une application régulière. Pour tout $x_0 \in X$, il existe un voisinage ouvert U de x_0 dans X et des polynômes homogènes $F_0, \ldots, F_m$ de même degré en $n+1$ variables qui ne s'annulent simultanément en aucun point de U, tels que, pour tout $x \in U$, on ait*

$$(1) \qquad \mu(x) \approx (F_0(x), \ldots, F_m(x))$$

En coordonnées homogènes.

Preuve :
Soit U_i un ouvert standard contenant $u(x_0)$; par définition, on peut écrire pour tout x dans $u^-1(U_i)$, $u(x) = (f_0(x), \ldots, f_n(x))$ où les f_i sont les fonctions régulières avec $f_i = 1$. Par

définition, on peut écrire chaque f_j comme G_j/H_j où G_j *et* H_j sont des polynômes homogènes de même degré,ceci sur voisinage U de x_0 *dans* $u^-1(U_i)$. La proposition s'en déduit facilement. Comme on l'a déjà expliqué, la formule (1) définit une application régulière là où les F_i ne s'annulent pas simultanément. La subtilité est que cette formule peut très bien définir une application régulière sur tout X, sans que celle-ci ait une expression globale de ce type. Il est parfois important de s'en rendre compte à première vue.

Exemple 1.2.3 *Soit C la courbe définie dans $\mathbb{P}^2$ par l'équation $XY = Y^2$.*
L'application $\mu : C \to \mathbb{P}^1$ est définie par $\mu(X,Y,Z) = (X,Y)$ est régulière hors du point $(0,1,0)$. Elle se prolonge en une application régulière sur tout C en posant $\mu(X,Y,Z) = (X,Y)$ hors du point $(1:0:0)$. Il n'existe pas de formule globale pour cette application.

1.2.5 Applications rationnelles

Définition 1.2.21 *Soient X et Y des variétés. On considère les couples (μ, U), où U est un ouvert dense de X et $\mu : U \to Y$ une application régulière.*
On dit que les couples (μ, U) et (ν, V) sont équivalents si μ et ν coïncident sur $U \cap V$
On appelle application rationnelle de X sur Y, une classe d'équivalence pour cette relation. On note $\mu : X \dashrightarrow Y$ une application rationnelle de X sur Y.

Remarque 1.2.4 *Malgré son nom, une application rationnelle n'est pas une application. En particulier, il n'est pas toujours possible de composer des applications rationnelles, ou de les restreindre à des sous-variétés.*

Définition 1.2.22 *On dit qu'une application rationnelle $\mu : X \dashrightarrow Y$ est définie en un point $x \in X$, s'il en existe un représentant régulier défini sur un voisinage dense de x dans X. L'ensemble des points où μ est définie est un ouvert dense de X, que l'on appelle parfois son domaine de définition.*
Une application rationnelle définie en tous les points de X est régulière.
Si X est sous-variété quasi-projective irréductible de $\mathbb{P}^n$, toute application rationnelle

$$\mu : X \to \mathbb{P}^m$$

est définie selon la formule (1) par la donnée de polynômes homogènes $F_0, \ldots, F_m \ldots$ de même degré en $n+1$ variables non tous identiquement nuls sur X. Elle est définie au-moins sur l'ouvert $X - \mathcal{V}(F_0, \ldots, F_m)$, mais son domaine de définition peut être plus grand.

1.3 Diviseurs

Avant de parler de diviseurs, on commence d'abord par la notion d'anneaux.

1.3.1 Anneaux locaux

Soit C une courbe algébrique définie sur un corps de nombres k, et irréductible de sorte que l'anneau de polynômes $k[C]$ est intègre.

Définition 1.3.1 *On appelle corps des fractions de l'anneau $k[C]$ le corps des fonctions rationnelles sur C ; il est noté $k(C)$.*
En d'autres termes, on a

$$k(C) = \{f \mid \exists\ g,\ f \in k[C] \text{ homogène de même degré},\ f = g/h\} \tag{1.16}$$

Définition 1.3.2 *Soient $f \in k[C]$ et $P \in C$. On dit que f est régulière (ou définie) au point P s'il existe $g, f \in k[C]$ avec $h(P) \neq 0$ telle que*

$$f = g/h. \tag{1.17}$$

Définition 1.3.3 *Soit $P \in C$. On appelle anneau local de C en P que l'on note $\mathbf{O_P}(C)$ l'ensemble des fonctions régulières en P.*
En d'autres termes

$$\mathcal{O}_{\mathcal{P}}(C) = \{f \in k(C) \mid f = g/h \text{ avec } h(P) \neq 0\}.$$

L'ensemble des points de C où la fonction rationnelle f n'est pas définie est appelé l'ensemble des pôles de f. Si f est régulière et s'annule en P, on dit que P est un zéro de f. Notons $\mathcal{M}_{\mathcal{P}}(C)$ l'ensemble des fonctions régulières en P et qui s'annulent en P.
Explicitement,

$$\mathcal{M}_{\mathcal{P}}(C) = \{f \in \mathcal{O}_{\mathcal{P}}(C) \mid f(P) = 0\}$$

qui est un idéal maximal.
Les éléments inversibles de $\mathcal{O}_{\mathcal{P}}(C)$ qui n'appartiennent pas à $\mathcal{M}_{\mathcal{P}}(C)$, on les appelle les unités de $\mathcal{O}_{\mathcal{P}}(C)$ et ils forment un groupe multiplicatif.
Si C est définie par l'équation affine $f(x, y) = 0$, alors $\mathcal{M}_{\mathcal{P}}(C)$ pour $p(a, b)$ est engendré par $x - a$ et $y - b$ c'est à dire $\mathcal{M}_{\mathcal{P}}(C) =< x - a, y - b >$

Définition 1.3.4 *On dit que $\mathcal{O}_{\mathcal{P}}(C)$ est un anneau de valuation discrète s'il existe $t \in \mathcal{M}_{\mathcal{P}}(C)$, $t \neq 0$, tel que tout élément non nul $f \in \mathcal{O}_{\mathcal{P}}(C)$ s'écrit de manière unique*

$$f = u\ t^m, u \text{ unté de } \mathcal{O}_{\mathcal{P}}(C),\ m \in \mathbb{N}. \tag{1.18}$$

L'entier m est appelé la valuation (ou l'ordre) de f, notée $ord_P(f)$; il ne dépend pas du choix du paramètre t appelé uniformisante de $\mathcal{O}_{\mathcal{P}}(C)$.
Plus généralement, si $f \in \mathcal{O}_{\mathcal{P}}(C)$, $f \neq 0$ on peut l'écrire sous la forme $u\ t^m$ avec cette fois $m \in \mathbb{Z}$, et on pose $ord_P(f) = m$

Proposition 1.3.1 *Si C est lisse en P, alors $\mathcal{O}_{\mathcal{P}}(C)$ est un anneau de valuation discrète et le corps*

$$\mathcal{O}_{\mathcal{P}}(C)/\mathcal{M}_{\mathcal{P}}(C)$$

est appelé corps résiduel.
La connaissance de la fonction

$$ord_P : f \to ord_P(f)$$

détermine l'anneau discrète
$\mathcal{O}_{\mathcal{P}}(C)$;

$$\mathcal{O}_{\mathcal{P}}(C) = \{f \in k(C) \mid \mathbf{O_P}(C) \geqslant 0\}$$

et $\mathcal{M}_{\mathcal{P}}(C)$:

$$\mathcal{M}_{\mathcal{P}}(C) = \{f \in k(C) \mid ord_P(f) > 0\}.$$

Lorsque une courbe est lisse, alors pour tout point P de C, l'anneau $\mathcal{O}_{\mathcal{P}}(C)$ est un anneau de valuation discrète.

Propriétés 1.3.1 *Soit C une courbe lisse en P.*
Soient f et g deux éléments non nuls de $k(C)$. On a

1. *$ord_P(f) = \infty$ si et seulement si $f = 0$.*
2. *$ord_P(fg) = ord_P(f) + ord_P(g)$.*
3. *$ord_P(\frac{f}{g}) = ord_P(f) - ord_P(g)$.*
4. *$ord_P(f + g) \geqslant min(ord_P(f), ord_P(g))$*
5. *Si f est un pôle de f, alors $ord_P(f) = -ord_P(\frac{1}{f})$.*

1.3.2 Diviseurs

Soit X une variété algébrique.

Définition 1.3.5 (*Diviseur de Weil*)
On appelle diviseur de Weil D sur X une somme formelle finie à coefficients entiers d'hypersurfaces irréductibles de X de codimension 1.
Ainsi, un diviseur de Weil D sur X s'écrit

$$D = \sum m_i Y_i \tag{1.19}$$

où les m_i sont les entiers presque tous nuls et Y_i représentent des hypersurfaces irréductibles de X de codimension 1.

Définition 1.3.6 (*Diviseur de Cartier*)
Un diviseur de Cartier D sur X est la donnée d'un recouvrement de X par des ouverts (U_i), et chaque U_i d'une fonction rationnelle f_i, avec la condition de compatibilité : sur chaque intersection $U_i \cap U_j$, la fonction $f_{ij} = f_i/f_j$ est une fonction à valeurs dans k^* (c'est gravea dire sans zéro ni pôle).
Voici une proposition importante qui nous permet d'identifier les deux diviseurs et ainsi, nous pouvons les écrire de façon simple :

Proposition 1.3.2 *Sur une variété lisse, les notions de diviseurs de Weil et de diviseurs Cartier coïncident.*

Définition 1.3.7 *Soit C une courbe lisse et irréductible. Un diviseur D sur C est une somme formelle de points appartenant à C*

$$D = \sum_{P \in C} n_P P \tag{1.20}$$

où les n_P sont presque tous nuls.
Le degré d'un diviseur est la somme de ses coefficients :

$$deg(\sum_{P \in C} n_P P)) = \sum_{P \in C} n_P.$$

Le support de D est l'ensemble des points $P \in C$ tels que $n_P \neq 0$.
Un diviseur $D = \sum_{P \in C} n_P P$ sur C est effectif (ou positif) et on note $D \geq 0$ si $n_P \geq 0$ pour tout $P \in C$.
L'ensemble des diviseurs sur C est un groupe commutatif noté $Div(C)$, où la loi de groupe est l'addition formelle de points :

$$Si\ D = \sum_{P \in C} n_P P\ et\ D' = \sum_{P \in C} n'_P P\ alors,\ (D + D') = \sum_{P \in C} (n_P + n'_P) P.$$

Manifestement,

$$deg(D + D') = deg(D) + deg(D').$$

Ainsi, on peut définir la relation d'ordre partiel $" \geqslant "$ sur les diviseurs par :

$$D \geqslant D'\ si\ et\ seulement\ si\ D - D' \geqslant 0.$$

Remarque 1.3.1 *Tout diviseur D peut s'écrire sous la forme*

$$D = D_1 - D_2$$

où les D_i sont effectifs et de supports disjoints.
En effet, soit

$$D = \sum_{P \in C} n_P P,\ posons\ D_1 = \sum_{n_P \geqslant 0} n_P P\ D_2 = -\sum_{n_P < 0} n_P P\ alors,\ D = D_1 - D_2.$$

Définition 1.3.8 (*Diviseurs principaux*)
Soient C une courbe lisse et irréductible, f une fonction non nulle de $k(C)$. On associe à f le diviseur noté $div(f)$ défini par :

$$div(f) = \sum_{P \in C} ord_P(f)P. \tag{1.21}$$

Un tel diviseur est appelé diviseur principal.
Comme dans la remarque 1.3.2*, précédente nous pouvons écrire $div(f)$ sous la forme de différence de deux diviseurs positifs :*

$$div(f) = div(f)_0 - div(f)_\infty$$

avec $div(f)_0 = \sum_{ord_P(f) \geqslant 0} ord_P P$ qui est appelé le diviseur de zéro de f et $div(f)_\infty = -\sum_{ord_P < 0} ord_P(f)P$ est le diviseur de pôle de (f).

Propriétés 1.3.2 *Soient f et g deux éléments non nuls de $k(C)$. On a :*

1. $div(fg) = div(f) + div(g)$;
2. $div(\frac{1}{f}) = -div(f)$;
3. $div(f) = 0$ *si et seulement si* $f \in k^*$;
4. $div(f) = div(g)$ *si et seulement s'il existe* $\lambda \in k^*$:

$$f = \lambda g.$$

Définition 1.3.9 (*Espace vectoriel associé*).
Pour chaque diviseur $D \in Div(C)$, associe le sous-espace de fonctions

$$\mathfrak{L}(D) = \{f \in \overline{k}(C)^* : \ div(f) \ \geq \ -D\} \cup \{0\} \tag{1.22}$$

Proposition 1.3.3 *Pour tout diviseur D, $\mathfrak{L}$ est un espace vectoriel sur $\overline{k}$ de dimension fini noté $l(D)$.*

Théorème 1.3.1 (*théorème de Riemann − Roch*)
Soient C une courbe lisse et K_C un diviseur canonique de C. Alors, il existe un entier $g \in \mathbb{Z}$ nommé le genre de C tel que, pour tout diviseur D, on a :

$$l(D) - l(K_C - d) = deg(D) - g + 1 \tag{1.23}$$

Chapitre 2

Courbes elliptiques

Les courbes elliptiques sont à priori parmi les objets les plus simples de la géométrie algébrique. Une courbe elliptique est une courbe projective plane cubique non-singulière. Les courbes elliptiques sont un sujet très à la mode en mathématiques. Elles sont à la base de la démonstration du grand théorème de Fermat par Andrew Wiles. Elles sont aussi à l'origine de nouveaux algorithmes de cryptographie très sûrs, et on entrevoit les prémices de leur utilisation pour la factorisation de grand nombres entiers.

2.1 Équations de Weierstrass

On appelle équation de Weierstrass (*forme projective*) sur un corps k une équation plane de la forme :

$$Y^2Z + a_1XYZ + a_3YZ^3 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.1}$$

où les a_i sont dans le corps de base k.

• Si $Z = 0$, alors l'équation (2.1) donne $0 = x^3$ *d'où* $X = 0$.

Ainsi $[X : Y : Z] = [0 : Y : 0] = Y[0 : 1 : 0]$. On note $O = [0 : 1 : 0]$ que l'on appelle point à l'infini.

• Si $Z \neq 0$, on peut écrire $x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$, l'équation de Weierstrass (2.1) devient (forme affine)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

avec $a_i \in k$.

• Si la caractéristique de k est différente de 2, l'équation de Weierstrass peut s'écrire :

$$y^2 = x^3 + a'_2x + a'_4x + a'_6,$$

• Si la caractéristique de k est différente de 2 et de 3, l'équation peut s'écrire :

$$E : y^2 = x^3 + ax + b,$$

• Si la caractéristique de k est 2, l'équation peut s'écrire :

$$y^3 + xy = x^3 + ax^2 + b$$

ou bien

$$y^3 + ay = x^3 + bx + c$$

• Si la caractéristique est 3, l'équation peut s'écrire :

$$y^3 = x^3 + ax^2 + b$$

ou bien

$$y^3 = x^3 + ax + b$$

Lemme 2.1.1 *Soit k un corps de caractéristique $p > 3$.*
Il existe des changements de variables permettant de simplifier (2.2) *en une équation plus simple appelée* ***équation courte de Weierstrass ou équation réduite de Weierstrass***

Preuve :

$$(i) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

avec $a_i \in k$.
Si le corps k est de caractéristique différente de 2 alors l'équation (i) devient

$$(ii) \qquad y^2 + 2y(\frac{a_1x}{2} + \frac{a_3}{2}) = x^3 + a_2x^2 + a_4x + a_6.$$

En ajoutant à chaque membre de l'équation (ii) l'expression suivante $(\frac{a_1x}{2})^2 + (\frac{a_3}{2})^2 + \frac{a_3}{2}x$, on aura :

$$y^2 + 2y(\frac{a_1x}{2} + \frac{a_3}{2}) + (\frac{a_1x}{2})^2 + (\frac{a_3}{2})^2 + \frac{a_3}{2}x = x^3 + a_2x^2 + a_4x + a_6 + (\frac{a_1x}{2})^2 + (\frac{a_3}{2})^2 + \frac{a_3}{2}x$$

$$y^2 + (\frac{a_1x}{2})^2 + (\frac{a_1}{2})^2 + 2y(\frac{a_1}{2}) + 2y(\frac{a_3}{2}) + \frac{a_1a_3}{2} = x^3 + a_2x^2 + a_4x + a_6 + (\frac{a_1x}{2})^2 + (\frac{a_3}{2})^2 + \frac{a_1a_3}{2}x$$

$$(iii) \qquad (y + \frac{a_1x}{2} + \frac{a_3}{2})^2 = x^3 + (\frac{a_2 + a_1^2}{4})x^2 + (\frac{a_4 + a_1a_3}{2})x + a_3^2 + a_6$$

En posant $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$, $a' = a_2 + \frac{a_1^2}{4}$, $b' = a_4 + \frac{a_1a_3}{2} etc' = \frac{a_3^2}{4} + a_6$, alors l'équation (iii) devient :

$$y_1^2 = x^3 + a'x^2 + b'x + c' \qquad (*)$$

Si le corps k est de caractéristique différente de 3, alors en divisant par 3, on a :

$$(x + \frac{a'}{3})^3 = x^3 + a'x^2 + 3(\frac{a'}{3})^2x + (\frac{a'}{3})^2$$
$$x^3 + a'x^2 = (x + \frac{a'}{3})^3 - 3(\frac{a'}{3})^2x - (\frac{a'}{3})^3$$

et en remplaçant $x^3 + a'x^2$ par $(x + \frac{a'}{3})^3 - 3(\frac{a'}{3})^2x - (\frac{a'}{3})^3$ dans $(*)$, nous obtenons enfin :

$$y_1^2 = (x + \frac{a'}{3})^3 - 3(\frac{a'}{3})^2x - (\frac{a'}{3})^3 + b'x + c'$$
$$y_1^2 = (x + \frac{a'}{3})^3 + (b' - 3(\frac{a'}{3})^2)x + (c' - (\frac{a'}{3})^3)$$

$y_1^2 = x_1^2 + Ax + B$ *avec* $x_1 = x + \frac{a'}{3}$; $A = b' - 3(\frac{a'}{3})^2$ $etB = c' - (\frac{a'}{3})^2$.
Comme les variables sont muettes, alors $y^2 = x^3 + ax + b$.
Ces équations de Weierstrass permettent de définir les courbes elliptiques.

Définition 2.1.1 *Une courbe elliptique est une paire (E, O) où :*
- E est une cubique irréductible non-singulière de genre 1 ;
- $O \in E$.

Définition 2.1.2 *Une courbe elliptique est définie sur un corps k si :*
- E est une courbe sur k (c'est à dire donnée par l'annulation d'un polynôme de $k[X, Y]$) ;
- O est un point de la courbe dont les coordonnées sont dans k.

Définition 2.1.3 *Une courbe elliptique E définie sur un corps k de caractéristique $p > 3$ est une courbe d'équation affine :*

$$y^2 = x^3 + ax + b. \tag{2.3}$$

avec a et b dans k tels que $4a^3 + 27b^2 \neq 0$, à laquelle on rajoute le point $O = [0 : 1 : 0]$.

Définition 2.1.4 *Le **discriminant** d'une courbe elliptique définie sur un corps k par l'équation affine réduite* (2.3) *est la quantité*

$$\Delta(E) = -16(4a^3 + 27b^2). \tag{2.4}$$

Définition 2.1.5 *Le **j-invariant** d'une courbe elliptique définie sur un corps k par l'équation affine réduite* (2.3) *est la quantité*

$$j = -1728\frac{(4a)^3}{\Delta(E)} = \frac{6912a^3}{4a^3 + 27b^2}. \tag{2.5}$$

Remarque 2.1.1 *Du point de vue algébrique, le $j-$invariant est une quantité très importante qui permet de caractériser les courbes elliptiques. Le $j-$invariant d'une courbe elliptique est toujours défini.*

Définition 2.1.6 *Une courbe elliptique est dite super-singulière lorsque son $j-$invariant est nul, c'est à dire $j = 0$.*

Remarques 2.1.2 *Le signe du discriminant $\Delta(E)$ peut nous permettre de dire si la courbe elliptique est composée de deux composantes ou d'une seule composante.*
- Si $\Delta(E) > 0$, alors le graphe de la courbe elliptique possède deux composantes.
Le polynôme $x^3 + ax + b$ possède trois racines qui correspondent aux abscisses des points d'intersection de la courbe avec l'axe des abscisses.
-Si $\Delta(E) < 0$, alors le graphe de la courbe elliptique possède une seule composante.
Le polynôme $x^3 + ax + b$ possède une seule racine qui correspond à l'abscisse du point d'intersection de la courbe avec l'axe des abscisses.
- Si $\Delta(E) = 0$, alors nous ne pouvons pas parler de courbe elliptique d'où la nécessité d'avoir $\Delta(E) \neq 0$.

Exemples 2.1.1
- Soit E la courbe elliptique définie par l'équation de Weierstrass $y^2 = x^3 - x$.
$\Delta(E) = -16(4a^3 + 27a^2) = 64$ et $\Delta(E) > 0$ donc le polynôme $x^3 - x$ a exactement trois racines réelles distinctes. $x^3 - x = x(x-1)(x+1)$.
De plus, l'invariant modulaire $j = \dfrac{-1728(4a)^3}{\Delta E} = \dfrac{-1728(-4)^3}{64} = 1728$.
La courbe elliptique E n'est donc ni singulière, ni super-singulière.
- Soit $E : y^2 = x^3 - x + 1$ une courbe elliptique.
$\Delta(E) = -368$ et $\Delta(E) < 0$ donc le polynôme $x^3 - x + 1$ a exactement une racine réelle.

Théorème 2.1.1 *Soit E une courbe elliptique définie par l'équation réduite de Weierstrass* (2.3). *E est non singulière si et seulement si $\Delta(E) \neq 0$.*

Preuve :
Montrons d'abord que le point à l'infini $O = [0 : 1 : 0]$ n'est pas singulier.
Considérons par exemple la courbe E de $\mathbb{P}^2$ donnée par son équation :

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ - bZ^2 = 0.$$

On a :

$$\frac{\partial F}{\partial X} = -3X^2 - aZ^2.$$
$$\frac{\partial F}{\partial X}(O) = 0.$$
$$\frac{\partial F}{\partial Y} = 2YZ.$$
$$\frac{\partial F}{\partial Y}(O) = 0.$$
$$\frac{\partial F}{\partial Z} = Y^2 - 2aXZ - 3bZ^2.$$
$$\frac{\partial F}{\partial Z}(O) = 1^2 - 2(a)(0)(0) - 3(b)(0)^2 = 1$$
$$\frac{\partial \partial F}{\partial Z}(O) \neq 0$$

Les dérivées partielles en $O = [0 : 1 : 0]$ ne sont pas simultanément nulles.
Par suite, O n'est pas singulier.
Pour les autres points, considérons la définition de la courbe E donnée par son équation réduite de Weierstrass $E : f(x, y) = y^2 - x^3 - ax - b = 0$.
La courbe est singulière en un point $P_0 = (x_0, y_0) \in E$ si et seulement si :
$\frac{\partial f}{\partial x}(x_0, y_0) = -3x_0^2 - a = 0$ *et* $\frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0$
$-3x_0^2 = a$ *et* $y_0 = \frac{0}{2}$
$x_0^2 = \frac{-a}{3}$ *et* $y_0 = 0$, *car* $2 \neq 0$ *et* $3 \neq 0$.
Comme P_0 est un point de la courbe, alors $y_0^2 = 0 = x_0^3 + ax_0 + b$.
$x_0^3 + ax_0 + b = 0$
$(x^2)x_0 + ax_0 + b = 0$
$\frac{-a}{3}x_0 + ax_0 + b = 0$ *car* $x_0^2 = \frac{-a}{3}$
$\frac{2ax_0}{3} = -b$
$x_0 = \frac{-3b}{2a} \Rightarrow x_0^2 = \frac{9b^2}{4a^2} \Rightarrow \frac{9b^2}{4a^2} = \frac{-a}{3}$. Par suite $-(27b^2 + 4a^3) = 0$, soit $\Delta = 0$.
Finalement, E est non singulière si et seulement si $\Delta \neq 0$.

Théorèmes 2.1.2

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

$$Y^2Za_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

et qui envoie le point O sur le point $[0 : 1 : 0]$.

ii) Tout autre plongement s'obtient en composant i avec un changement de coordonnées linéaires $\mathbb{P}^2 \to \mathbb{P}^2$ donné par la matrice de la forme

$$\begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$$

. En d'autres termes, deux équations de Weierstrass définissent des courbes elliptiques isomorphes si et seulement si elles se déduisent l'une de l'autre par un changement de coordonnées

$$x' = u^2x + r,\ y' = u^3y + u^2sx + t.$$

iii) Pour $P, Q, R \in E$, on a $P + Q + R = O$ si et seulement si il existe une droite $L \subset \mathbb{P}^2$ telle que $[L \cap i(E)] = [i(P)] + [i(Q)] + [i(R)]$. ($Ici$ $[L \cap i(E)]$ désigne le diviseur des points d'intersection de L et $i(E)$ comptés avec multiplicités).

Preuve :

i) Puisque O est un point $k - rationnel$, le diviseur $3[O]$ est défini sur k. Son degré $deg(3[O]) = 3$ étant $\geq 2g + 1$, on sait que tout choix de $k - base$ de $\mathcal{L}_{3[O]}$ fournit un plongement dans $\mathbb{P}^{\mathbf{L}_{3[o]-1}}$. Or, d'après Riemann- Roch on a $\mathcal{L}_{3[O]} = 3$ et aussi $\mathcal{L}_{2[O]} = 2$. Choisissons une $k - base$ $\{1, x, y\}$ de $\mathcal{L}_{3[O]}$ telle que $1, x$ soit une base de $\mathcal{L}_{2[O]}$. On a donc une immersion fermée $i_{x,y} : E \to \mathbb{P}^2$. Pour en calculer une équation, on remarque que la famille de 7 fonctions $\{y^2, x^3, yx, x^2, y, x, 1\}$ vit dans $\mathcal{L}_{6[O]}$ qui est de dimension 6. Cette famille est donc $k - linairement$ liées. Par ailleurs, les familles obtenues en retirant y^2 *ou* x^3 sont libres, puisque ayant des pôles d'ordre distinct en O. Toute relation de dépendance linéaire non triviale doit donc avoir un coefficient non nul en y^2 et x^3. En remplaçant x et y par des multiples convenables, on obtient une relation de dépendance sous forme de Weierstrass. Ainsi $i_{x,y}(E)$ est contenue dans une cubique de Weierstrass C. Comme $i_{x,y}(E)$ ne peut pas être une conique ni une droite ($genre$ 0), on doit avoir $i_{x,y}(E) = C$. Enfin, remarquons que O est envoyé sur un pôle de $x = X/Z$ *et* $y = Y/Z$, donc sur un point de la droite $\{Z = 0\}$, mais $[0 : 1 : 0]$ est le seul point de $C \cap \{Z = 0\}$.

ii) Réciproquement si $i : E \to \mathbb{P}^2$ est un plongement sur une cubique de Weierstrass envoyant O sur $[0 : 1 : 0]$, alors les fonctions $x' = i^*(X/Z)$ *et* $y' = i^*(Y/Z)$ forment une autre base $\{1, x', y'\}$ de $\mathcal{L}_{3[O]}$ telle que $x' \in \mathcal{L}_{2[O]}$. On peut donc écrire $x' = \lambda x + r$ *et* $y' = \mu y + sx + t$. Pour que les coefficients de x'^3 *et* y'^3 soient égaux, on doit avoir $\mu^2 = \lambda^3$ et donc $\mu = u^3$ *et* $\lambda = u^2$ *pour* $u = \mu\lambda^-1$.

iii) Supposons $P+Q+R = O$. Alors il existe $f \in \overline{k}(E)^*$ telle que $[p]+[Q]+[R]-3[O] = div(f)$. Une telle fonction f s'annule en P, Q, R et est dans $\mathcal{L}_{3[O]}$ donc s'écrit $f = ax + by + c$. Soit alors $L \subset \mathbb{P}^2$ la droite d'équation $aX + bY + cZ = 0$. On constate sur les définitions qu'elle intersecte C avec multiplicité m en le point $i(S)$ si et seulement si f s'annule en S avec ordre m ($c'est\ à\ dire\ v_S(f) = m$). Il s'en suit que l'intersection $L \cap i(E)$ vue comme diviseur est égale à $[i(P)] + [i(Q)] + [i(R)]$. Réciproquement, si L a pour équation $aX + bY + cZ = 0$ *et* $L \cap i(E) = [i(P)] + [i(Q)] + [i(R)]$ alors le diviseur des zéros de $f := ax + by + c$ est $[p] + [Q] + [R]$. Par ailleurs son seul pôle possible est en O et le fait que le $deg(f) = 0$ implique que $div(f) = [p] + [Q] + [R] - 3[O]$, d'*où* $P + Q + R = O$

2.2 Équations de Weierstrass minimales

Soit E une courbe elliptique sur k. On aimerait lui associer une courbe $\overline{E}$ canonique sur $\overline{k}$ et une application de réduction. Si on voit E comme une cubique $E = C_f \subset \mathbb{P}^2$, alors la courbe C_f dépend en général du choix de f.

Définition 2.2.1 *On dit qu'une équation de Weierstrass est minimale si ses coefficients sont entiers et son discriminant est de valuation minimale parmi toutes les équations de Weierstrass à coefficients entiers qui définissent la même courbe.*

Définitions 2.2.2 *On dit que E a*
- *bonne réduction si $\overline{E}$ est non-singulière.*
- *réduction multiplicative si $\overline{E}$ a un point de croisement.*
- *réduction additive si $\overline{E}$ a un point de rebroussement.*

Il est clair que E a bonne réduction si et seulement si elle admet une équation de Weierstrass à coefficients dans $\mathbb{R}$ et avec $\nu(\Delta) = 0$ tel que $\nu(x) = \{\sigma \in G_k,\ \forall\ x\ \in \overline{k},\ \nu(\sigma(x))\}$. Voici un résultat clef pour la preuve du théorème de Mordell.

2.3 Courbes elliptiques sur les corps quelconques

Définition 2.3.1 *Une courbe elliptique E définie sur le corps k est une courbe projective plane d'équation*

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{2.6}$$

où a_i sont des éléments de k.
Si l'on définit les éléments d_2, d_4, d_6 et d_8 de k par

$$d_2 = a_1 + 4a_2, d_4 = 2a_4 + a_1a_3, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

on a

$$\Delta_E = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \text{ avec } \Delta_E \neq 0. \tag{2.7}$$

L'équation (2.6) est appelée paramétrisation de Weierstrass de E.
L'ensemble des points d'une courbe elliptique E définie sur corps k est noté

$$E(k) = \{[X : Y : Z] \in \mathbb{P}^2(k),\ Y^2Z + a_1XYZ + a_3Z^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}. \tag{2.8}$$

Propositions 2.3.1 *Avec les notations introduites ci-dessus.*

i) Pour tout $j \in k$, il existe une courbe elliptique E sur k telle que $j(E) = j$;

ii) Si $j(E) = j(E')$ alors E et E' sont isomorphes sur $\overline{k}$;

iii) Si $Aut(E/\overline{k})$ est un groupe fini. Son ordre est donné par le tableau

$j(E)$	$car(k)$	$Aut(E)$
$\neq 0, 1728$		2
1728	$\neq 2, 3$	4
0	$\neq 2, 3$	6
0	3	12
0	2	24

Preuve :

(i) En caractéristique 2 ou 3, c'est clair vu les formules données plus haut.
En caractéristique $\neq 2,3$ et lorsque $j \neq 0, 1728$, on prend E donnée par $y^2 = 4x^3 - \frac{27j}{j-1728}$. De plus, la courbe $y^2 = x^3 + 1$ a pour invariant $j = 0$ et la courbe $y^2 = x^3 + x$ a pour invariant $j = 1728$.

(ii) Si k est de caractéristique $\neq 2, 3$ et E (*resp* E'), donnée par l'équation courte associée à (a_4, a_6) *resp* (a'_4, a'_6), alors on a plusieurs cas :
- Si $a_4 a_6 \neq 0$, on doit avoir $a'_4 a'_6 \neq 0$ et $a_6^2 a_4^{-3} = a_4'^{-3} a_6'^2$. Il suffit alors de changer de coordonnées $x' = u^2 y, y' = u^3 y$ *avec* $u = (a'_4 a_4^{-1})^1/4$.
- Si $a_6 = 0$, alors $a_4 \neq 0$ donc $a'_6 = 0$ et le même changement de coordonnées convient.
- Si $a_4 = 0$, alors $a'_4 = 0$ et suffit de changer de coordonnées avec $u = (a'_6 a_6^{-1})^1/6$.
Lorsque k est de caractéristique 2 ou 3 c'est un peu plus compliqué mais tout aussi élémentaire, voir $|Silverman, appendice A|$.

iii) $\phi_{x,y}$ est un isomorphisme de E sur une cubique de Weierstrass, alors pour tout automorphisme σ de E, $\phi_{x,y} \circ \sigma$ est un autre isomorphisme de E sur la même cubique. D'après *ii*) du théorème 4, on sait que $\phi \circ \sigma$ se déduit de $\phi_{x,y}$ par un changement de coordonnées linéaires sur $\mathbb{P}^2$, et celui-ci doit préserver l'équation de Weierstrass fixée. Il s'agit donc de trouver les changements de coordonnées qui préservent une équation de l'une des formes ci-dessus.
Lorsque k de caractéristique $\neq 2, 3$ et E est donnée par $y^2 = x^3 + a_4 x^2 + a_6$, les seuls automorphismes sont de la forme $(x', y') = (ux, uy)$ avec $u^4 a_4 = a_4$ *et* $u^6 a_6 = a_6$. On en déduit donc que $AutE$ est cyclique d'ordre donné dans l'énoncé.
Calculer l'ordre pour $j = 0$ en caractéristique 2 et 3 est encore élémentaire. Les groupes obtenus ne sont pas abéliens.

Définition 2.3.2 *Soit g un polynôme unitaire à coefficients dans k de degré $n \geq 1$. Soient $\alpha_1, \ldots, \alpha_n$ ses n racines dans $\overline{k}$ comptées avec multiplicités.le déterminant Δ de g est défini par l'égalité*

$$\Delta = \Pi_{i<j}(\alpha_i - \alpha_j). \tag{2.9}$$

C'est un élément de k.
On dit que la courbe elliptique d'équation (2.5) *est définie sur k pour préciser que a et b sont dans k.*

2.3.1 Points rationnels d'une courbe elliptique

Soit L une extension de k dans $\overline{k}$.

Définition 2.3.3 *Soit $P = [x : y : z]$ un point de $\mathbb{P}^2$. On dit que P est rationnel sur L s'il existe $\lambda \in \overline{k}^*$ tel que $\lambda x, \lambda y, \lambda z$ soient dans L. On note $\mathbb{P}^2(L)$ l'ensemble des points de $\mathbb{P}^2$ rationnels sur L.*
Cela justifie la notation $\mathbb{P}^2 = \mathbb{P}^2(\overline{k})$.

Remarque 2.3.1 *Soit $P = [x_1 : x_2 : x_3]$ un point de $\mathbb{P}^2$. Le point P est rationnel sur L s'il existe i tel que x_i soit non nul, et que chaque $\frac{x_j}{x_i}$ appartienne à L.*

Définition 2.3.4 *Soit E une courbe elliptique définie sur k d'équation $y^2z = x^3 + axz^2 + bz^3$. Un point de E est dit rationnel sur L s'il appartient à $E \cap \mathbb{P}^2(L)$. On note $E(L)$ l'ensemble des points de E rationnels sur L.*
En d'autres termes

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\} \cup \{O\} \tag{2.10}$$

2.3.2 Points de torsion d'une courbe elliptique

Considérons une courbe elliptique E définie sur k. Étant donné un entier $n \geq 2$, posons

$$E[n] = \{P \in E(\overline{k}) \mid nP = O\}. \tag{2.11}$$

C'est un sous-groupe de $E(\overline{k})$, qui est l'ensemble des points de E d'ordre divisant n.
Un point $P \in E(\overline{k})$ est dit de $n - torsion$ s'il appartient à $E[n]$. Le groupe $E[n]$ s'appelle le sous-groupe des points de $n - torsion$ de E.

Théorème fondamental

Notons $car(k)$ la caractéristique de k. Nous admettons le résultat essentiel suivant.

Théorèmes 2.3.1 *Soit n un entier supérieur ou égal à 2.*

1) *Supposons que $car(k)$ ne divise pas n (tel est le cas si $car(k) = 0$). Alors, $E[n]$ est un groupe d'ordre n^2 isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

2) *Supposons $car(k) = p$, où p est un diviseur premier de n. Posons $n = p^r n'$, où p ne divise pas n'. Alors, $E[n]$ est isomorphe à l'un des groupes*

$$\mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \text{ et } \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}.$$

En particulier :

Corollaire 2.3.1 *Pour tout $n \geq 2$, le groupe $E[n]$ est fini d'ordre au plus n^2.*
Par ailleurs, si $car(k) = p$, le groupe $E[p]$ est trivial ou est cyclique d'ordre p. On reviendra sur ce point.

Corollaire 2.3.2 *Soit l un nombre premier distinct de $car(k)$. Le groupe $E[l]$ est un $\mathbb{F}_l-$espace vectoriel de dimension 2.*
Pour tout nombre premier l distinct de $car(k)$, si (P_1, P_2) est une base de $E[l]$ sur $\mathbb{F}_l$, tout point $P \in E[l]$ s'écrit ainsi de manière unique sous la forme

$$P = n_1P_1 + n_2P_2,$$

où n_1 et n_2 sont des entiers compris entre 0 et $l - 1$.

Lemme 2.3.1 *Soient α, β, γ les racines dans $\overline{k}$ du polynôme $X^3 + aX + b \in k[X]$. On a*

$$E[2] = \{O, (\alpha, 0), (\beta, 0), (\gamma, 0)\}.$$

En particulier, $E[2]$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Preuve : Soit P un point de E distinct de O. Posons $P = (x, y) \in E(\overline{k})$.
D'après les assertions 3 et 4 du théorème 5, le point P est dans $E[2]$ si et seulement si $y = 0$, d'*où* le résultat, vu que α, β, γ sont distinctes *deux − à − deux* (*corollaire* 2).

Lemme 2.3.2 *Posons* $G = 3X^4 + 6aX^2 + 12bX - a^2 \in k[X]$.

1) Le polynôme G possède quatre racines distinctes dans $\overline{k}$.

2) Soit $P = (x, y)$ un point de $\overline{k}$. On a l'équivalence

$$P \in E[2] \Longleftrightarrow G(x) = 0.$$

En particulier, $E[3]$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Preuve :

1) On vérifie que le discriminant de G est

$$-2^8.3^3(4a^3 + 27b^2).$$

Puisque $car(k) \geq 5$ et que $4a^3 + 27b^2 \neq 0$, il n'est pas nul, d'*où* la première assertion.

2) Supposons que P appartienne à $E[3]$. On a alors $2P = -P$. Par ailleurs, on a $2P \neq 0$ (*car P est par hypothèse distinct de O*), donc y est non nul (*lemme* 4). D'après les assertions 3 et 5 du théorème 5, on obtient

$$(\star)\lambda^2 - 2x = x \text{ avec } \lambda = \frac{3x^2 + a}{2y}.$$

Compte tenu de l'égalité $y^2 = x^3 + ax + b$, il en résulte que $G(x) = 0$.
Inversement, supposons $G(x) = 0$. On vérifie que l'on a

$$(3X^2 + 4a)G - (X^3 + aX + b)(9X^3 + 21aX + 27b) = -(4a^3 + 27b^2).$$

Par suite, G et X^3+aX+b n'ont pas de racines communes. On a donc $x^3+ax+b \neq 0$ c'est à dire y est non nul. L'égalité $G(x) = 0$ entraine alors que la condition $\star$ est satisfaite. L'abscisse de $2P$ est donc celle de P. On a ainsi $2P = \pm P$, puis $2P = -P$ c'est à dire P est dans $E[2]$, d'*où* l'équivalence annoncée.
Par ailleurs, chaque racine de G dans $\overline{k}$ est l'abscisse de deux points distincts de E. Le groupe $E[3]$ est donc d'ordre 9, d'*où* le résultat.

2.4 Loi de groupe

Soit E une courbe elliptique définie sur k. Pour toute extension L de k dans $\overline{k}$, on va munir $E(L)$ d'une structure naturelle de groupe abélien, d'élément neutre le point à l'infini $O = [0 : 1 : 0]$.

2.4.1 Droites de $\mathbb{P}^2$

Définition 2.4.1 *Une droite de $\mathbb{P}^2$ est une partie de $\mathbb{P}^2$ formée des points $[x : y : z]$ tels que*

$$ux + vy + wz = 0$$

, où u, v et w sont des éléments non nuls de $\overline{k}$.
On parle alors de la droite d'équation $ux+vy+wz = 0$. Une droite d'équation $x = \lambda z$, où λ est dans $\overline{k}$, est dite verticale. Une telle droite passe par le point $O = [0 : 1 : 0]$. En fait, toute droite passant par O a une équation de la forme $ux + wz = 0$. On dit souvent que la droite d'équation $z = 0$ est la droite à l'infini. En identifiant la partie de $\mathbb{P}^2$ formée des points $[x : y : z]$ tels que $z \neq 0$ Avec $\overline{k}^2$, le plan projectif s'interprète comme la réunion de $\overline{k}^2$ avec la droite à l'infini.

Lemme 2.4.1 *Soient $P = [a_1 : a_2 : a_3]$ et $Q = [b_1 : b_2 : b_3]$ deux points distincts de $\mathbb{P}^2$. Il existe une unique droite de $\mathbb{P}^2$ passant par P et Q. C'est l'ensemble des points $[x : y : z] \in \mathbb{P}^2$ tels que le déterminant de la matrice*

$$\begin{pmatrix} a_1 & b_1 & x \\ a_2 & b_2 & y \\ a_3 & b_3 & z \end{pmatrix}$$

soit nul. Autrement dit, c'est la droite d'équation $ux + vy + wz = 0$, avec

$$u = a_2b_3 - a_3b_2, \qquad v = a_3b_1 - a_1b_3, \qquad w = a_1b_2 - a_2b_1.$$

Preuve :
Les éléments u, v *et* w ne sont pas tous nuls car P et Q sont distincts. L'équation $ux+vy+wz = 0$ est donc celle d'une droite contenant P et Q. Considérons alors une droite de $\mathbb{P}^2$ passant par P et Q d'équation

$$u'x + v'y + w'z = 0.$$

Soient f *et* g les formes linéaires de $\overline{k}^3 \to \overline{k}$ définies par

$$f(x, y, z) = ux + vy + wz \text{ et } g(x, y, z) = u'x + v'y + w'z.$$

Le noyau de f $(resp\ g)$ est le plan $\overline{k}^3$ engendré par (a_1, a_2, a_3) *et* (b_1, b_2, b_3). En particulier, f *et* g ont le même noyau. Dans le dual de $\overline{k}^3$, l'orthogonal du noyau de f $(resp\ g)$ est une droite engendrée par f $(resp\ g)$. Il existe donc $\lambda \in \overline{k}$ non nul tel que $f = \lambda g$, d'*où* l'assertion d'unicité.

2.4.2 Tangente à E en un point

Notons désormais

$$y^2z = x^3 + axz^2 + bz^3$$

L'équation de E, *où* a *et* b sont dans k. Posons

$$F = Y^2Z - (X^3 + aZX^2 + bZ^3) \in K[X, Y, Z],$$
$$F_X = \frac{\partial F}{\partial X}, F_Y = \frac{\partial F}{\partial Y}, F_Z = \frac{\partial F}{\partial Z}$$

On a

$$F_X = -(3X + aZ^2), \quad F_Y = 2YZ, \quad F_Z = Y^2 - (2aXZ + 3bZ^2)$$

.

Lemme 2.4.2 *Il n'existe pas de point $P \in E$ tel que*

$$F_X(P) = F_Y(P) = F_Z(P) = 0$$

.

Preuve :
Supposons qu'il existe un tel point P. On a $F_Z(O) = 1$, donc P est distinct de O. Posons $P = [x : y : 1]$. La caractéristique de k étant distincte 2, on a $y = 0$. On obtient

$$3x^2 + a = 0 \quad et \quad 2ax + 3b = 0$$

Supposons $a \neq 0$. On a alors $x = -\dfrac{3b}{2a}$, d'*où* $4a^3 + 27b^2 = 0.Si\ a = 0$, vu que la caractéristique de k n'est pas 3, on a $b = 0$. On obtient ainsi une contradiction et le résultat.

Définition 2.4.2 *Pour tout point $P \in E$, la tangente à E en P est la droite d'équation*

$$F_X(P)x + F_Y(P)y + F_Z(P)z = 0.$$

Lemme 2.4.3

1. *L'équation de la tangente à E au point O est $z = 0$.*

2. *Soit $P = [x_0 : y_0 : 1]$ un point de E distinct de O. L'équation de la tangente à E en P est*

$$F_X(P)(x - x_0z) + F_Y(P)(y - y_0z) = 0.$$

Preuve :
Cela résulte des formules $F_X = -(3X + aZ^2),\quad F_Y = 2YZ,\quad F_Z = Y^2 - (2aXZ + 3bZ^2)$ et de l'égalité $y_0^2 = x_0^3 + ax_0 + b$.

Exemple 2.4.1 *Soit α une racine dans $\overline{k}$ du polynôme $X^3 + aX + b$. Le point $P = (\alpha, 0)$ appartient à E. On a $F_X(P) = -(3\alpha^2 + a) \neq 0$ $(lemme3)$ et $F_Y(P) = 0$. La tangente à E en P est donc verticale et a pour équation*

$$x = \alpha z$$

En particulier, elle passe par O.

2.4.3 Loi de composition

On va définir ici une loi de composition interne sur E, qui va s'avérer ne pas être une loi de groupe, mais qu'il suffira de modifier à l'aide d'une symétrie convenable pour obtenir la loi de groupe que l'on a en vue. Pour tout point R de E distinct de O, on notera $R = [x_R : y_R : 1]$.

Proposition 2.4.1 *Soient P et Q des points de E. Soit D la droite de $\mathbb{P}^2$ passant par P et Q si $P \neq Q$, ou bien la tangente à E en P si $P = Q$. On a*

$$D \cap E = \{P, Q, f(P, Q)\},$$

où $f(P, Q)$ désigne le point de E défini par les conditions suivantes.

1. *Supposons $P \neq Q, P \neq O$ et $Q \neq O$.*

1.1) Supposons $x_P \neq x_Q$. Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad et \ \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$f(P,Q) = [\lambda^2 - x_P - x_Q : \lambda(\lambda^2 - x_P - x_Q) + \nu : 1] \tag{2.12}$$

1.2) Si $x_P = x_Q$, on a

$$f(P,Q) = O. \tag{2.13}$$

2. Supposons $P \neq O$ et $Q = O$. On a

$$f(P,O) = [x_P : -y_Q : 1]. \tag{2.14}$$

De même, si $P = O$ et $Q \neq O$, on a $f(O,Q) = [x_Q : -y_P : 1]$

3. Si $P = Q = O$, on a

$$f(O,O) = O. \tag{2.15}$$

4. Supposons $P = Q$ et $P \neq O$.

4.1) Si $y_P = 0$, on a

$$f(P,P) = O. \tag{2.16}$$

4.2) Supposons $y_P \neq 0$. Posons

$$\lambda = \frac{3x_P^3 + a}{2y_P} \quad et \ \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

On a

$$f(P,P) = [\lambda^2 - 2x_P : \lambda(\lambda^2 - 2x_P) + \nu : 1] \tag{2.17}$$

Preuve :

1. Supposons $x_P \neq x_Q$. D'après le lemme 3, l'équation de D est

   $$y = \lambda x + \nu z.$$

   Soit M un point de $E \cap D$. Puisque O n'est pas sur D, il existe x_0 *et* y_0 dans $\overline{k}$ tels que $M = [x_0 : y_0 : 1]$. On a les égalités

   $$y_0 = x_0^3 + ax_0 + b \quad et \quad y_0 = \lambda x_0 + \nu.$$

   Ainsi, x_0 est une racine du polynôme

   $$H = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

   La somme de ses racines est λ^2. On a $H(x_P) = H(x_Q) = 0$ *et* $x_P \neq x_Q$. Par suite, les racines de H sont

   $$x_P, x_Q \ et \ \lambda^2 - x_P - x_Q.$$

Il en résulte que $D \cap E$ est formé de P, Q et du point $f(P,Q)$ définit par la formule (8) Supposons $x_P = x_Q$. Puisque P et Q sont distincts, on a alors $y_P = y_Q$. D'après le lemme, l'équation de D est

$$x = x_P z.$$

Le point O est donc sur $D \cap E$. Soit M un point de $D \cap E$ distinct O. Si $M = [x_0 : y_0 : 1]$, on a $x_0 = x_P$ *puis* $y_0 = \pm y_P$. On a donc $M = P$ *ou* $M = Q$. On en déduit que l'on a $D \cap E = \{P, Q, O\}$, d'*où* l'assertion dans ce cas.

2. Supposons $P \neq O$. La droite D passe par P et O a pour équation

$$x = x_P z.$$

Si $M = [x_0 : y_0 : 1]$ est un point de $D \cap E$, on a donc $x_0 = x_P$ d'*où* $y_0 = \pm y_P$. On a ainsi $D \cap E = \{P, O, f(P,O)\}$, *d'où* $f(P,O)$ est définit par la formule (2.12).

3. La tangente de D à E en O a pour équation $z = 0$ (*Lemme* 2.4.1). Par suite, O est le seul point de $D \cap E$, *d'où* $f(O,O) = O$.

4. On a $P = Q$ *et* $P \neq O$. L'équation de la tangente de D à E en P a donc pour équation

$$F_X(P)(x - x_P z) + F_Y(P)(y - y_P z) = 0.$$

Si$y_P = 0$, on a $F_Y(P) = 0$. Puisque x_P est la racine simple du polynôme $X^3 + aX + b$, on a $F_X(P) \neq 0$. Ainsi, D a pour équation

$$x = x_P z.$$

Le seul point de $D \cap E$ distincts de P est donc le point O, d'*où*$D \cap E = \{P, O\}$ et l'assertion est vérifiée.
Supposons $y_P \neq 0$. L'équation de D est dans ce cas

$$y = \lambda x + \nu z.$$

Le point O n'est pas sur D. Soit $M = [x_0 : y_0 : 1]$ un point de $D \cap E$. On a

$$y_0^2 = x_0^3 + a x_0 + b \quad et \quad y_0 = \lambda x_0 + \nu.$$

Par suite, x_0 est racine du point polynôme

$$G = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

Le polynôme dérivé de G est

$$G' = 3X^2 - 2\lambda^2 X + a - 2\lambda\nu.$$

On a $G(x_P) = 0$, et en utilisant l'égalité $y_P^2 = x_P^3 + a x_P + b$, on vérifie que $G'(x_P) = 0$. Ainsi, x_P est une racine d'ordre au moins 2 de G. Les racines de G sont donc

$$x_P \quad et \quad \lambda^2 - 2x_P.$$

On obtient $D \cap E = \{P, f(P,Q)\}$ *où* $f(P,Q)$ est définit de la formule (2.17), d'*où* le résultat.
On obtient une loi de composition interne sur E, appelée loi de composition des cordes-tangentes, $f : E \times E \to E$ qui a tout couple $(P,Q) \in E \times E$ associe le point $f(P,Q) \in E$ définit dans la proposition. Elle est commutative, mais n'est pas associative.

Exemple 2.4.2 *Soit E une courbe elliptique sur $\mathbb{Q}$ d'équation*

$$y^2 = x^3 + 3x.$$

Les points $P = (1, 2)$, $Q = (0, 0)$ et $R = (\frac{1}{4}, \frac{7}{8})$ sont dans $E(\mathbb{Q})$. On vérifie que l'on a

$$f(P, Q) = (3, 6), \ f(Q, R) = (12, -42).$$

$$f(f(P, Q), R) = (3, 6), \ f(P, f(Q, R)) = (3, -6).$$

Considérons a et b deux éléments de k tels que $4a^3 + 27b^2 \neq 0$ et E la courbe elliptique définie sur k d'équation

$$y^2 = x^3 + ax + b$$

Notons $+$ la loi de composition interne sur E, définie pour tous P et Q dans E par l'égalité

$$P + Q = f(f(P, Q), O). \tag{2.18}$$

Géométriquement $P + Q$ s'obtient à partie de $f(P, Q)$ par symétrie par rapport à l'axe des abscisses. Cette loi de composition est une loi de groupe sur E.

Théorème 2.4.1 *Le couple $(E, +)$ est un groupe abélien d'élément neutre O. La loi interne $+$ est décrite explicitement par les formules suivantes.*
Soient P et Q des points de E distincts de O. Posons $P = (x_P, y_Q)$ et $Q = (x_Q, y_Q)$.

1. *Supposons $x_P = x_Q$. Posons*

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \ \text{ et } \ \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda(\lambda^2 - x_P - x_Q) - \nu). \tag{2.19}$$

2. *Si $x_P = x_Q$ et $P \neq Q$, on a*

$$P + Q = O. \tag{2.20}$$

3. *Supposons $P = Q$ et $y_P \neq 0$. posons*

$$\lambda = \frac{3x_P^2 + a}{2y_P} \ \text{ et } \ \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}$$

On a

$$2P = (\lambda^2 - 2x_P, -\lambda(\lambda^2 - 2x_P) - \nu). \tag{2.21}$$

4. *Si $P = Q$ et $y_P = 0$, on a*

$$2P = O. \tag{2.22}$$

5. *L'opposé de P est le point*

$$-P = -(x_P, y_P) \tag{2.23}$$

Preuve :
Compte tenu de (2.18), les formules (2.19) et (2.21) résultent directement des égalités (2.12), (2.14) et (2.17). Supposons $x_P = x_Q$ *et* $P \neq Q$. D'après l'assertion (1.2) de la proposition 2.4.1, on a $f(P,Q) = O$ *d'où* $P + Q = f(O,O) = O$. Si $P = Q$ *et* $y_P = 0$, on a $f(P,P) = O$ (*assertion* 4.1 *de la proposition* 8), d'*où* $2P = f(O,O) = O$. Cela établit les formules d'addition de P et Q.
Par ailleurs, pour tous R et S de E, on a $f(R,S) = f(S,R)$. La loi + est donc commutative. Le fait que cette loi soit associative peut par exemple se vérifier au cas par cas, en utilisant les formules ci-dessus et un logiciel de calculs. C'est assez long et nous l'admettrons ici. Les assertions 2 et 3 de la proposition 2.4.1 impliquent

$$R + O = f(f(R,O),O) = R;$$

donc O est l'élément neutre. En ce qui concerne la formule (2.23), si $P = (x_P, 0)$, on a $2P = O$ d'après l'assertion 4 établie ci-dessus. Si $y_P \neq 0$, en posant $Q = (x_P, y_P)$, on a $P + Q = O$ d'après l'assertion 2, d'*où* la formule (2.23) du théorème.

Théorème 2.4.2 *Supposons* $k = \mathbb{F}_q$. *Alors* $||E(\mathbb{F}_q| - q - 1| \leq 2\sqrt{q}$.

Preuve : Comme dans le dernier exemple , on a $E^{(q)} = E$ et l'isogénie de Frobenius ϕ_q est donc un endomorphisme de E. De plus, son action sur E est la même que celle d'un générateur de $G_{\mathbb{F}_q}$ donc on a $E(\mathbb{F}_q) = E^{\phi_q} = ker(id - \phi_q)$. Puisque ϕ_q est inséparable, on a $\phi_q^* w = 0$ pour toute différentielle $w \in \Omega_E$, et il s'en suit que $(id - \phi_q)^* w = w$, donc $id - \phi_q$ est une isogénie séparable. En particulier, $|ker(id - \phi_q)| = deg(id - \phi_q)$. Or, le corollaire précédent nous dit que $\varphi \to deg(\varphi)$ est une forme quadratique définie positive sur $End(E)$. Une version de l'inégalité de Cauchy-Schwartz nous dit alors que

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

Les égalités $deg(id) = 1$ *et* $deg(\phi_q) = q$ achève la preuve.

Chapitre 3

Isogénies entre courbes elliptiques

Avant de parler d'isogénies, on commence d'abord par la notion de morphismes, la notion d'isomorphismes, la notion de groupes algébriques et la notion de variétés abéliennes.

3.1 Morphismes d'ensembles algébriques

Définitions 3.1.1
■ *Soit $V \subset k^n$ une variété algébrique. Une fonction sur V à valeurs dans k est dite polynomiale sur V s'il s'agit de la restriction à V d'un élément de $k[X_1, \cdots, X_n]$. L'ensemble des fonctions polynomiales sur une variété algébrique V est une $k-$algébre que l'on note $k[V]$.*
■ *Soient $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques. Une application de V dans W est dite polynomiale si toutes ses coordonnées sont des fonctions polynomiales.*

Définition 3.1.2 *Soient $A \subset k^n$ et $B \subset k^m$ deux variétés algébriques et $\Phi : A \to B$ une application que l'on peut écrire $\Phi = (\Phi_1, \cdots, \Phi_m)$ avec $\Phi_i : A \to k$. On dit que Φ est un morphisme si les composantes Φ_i sont des éléments de $k[A]$. On note $Reg(A, B)$ l'ensemble des morphismes de A dans B.*

Définition 3.1.3 *Soient A et B deux variétés algébriques. Un isomorphisme de A sur B est une application polynomiale f de A dans B telle qu'il existe une application polynomiale g de B dans A vérifiant $g \circ f = Id_A$ et $f \circ g = Id_B$.*

Remarques 3.1.1

1. *Une application bijective n'est pas nécessairement un isomorphisme.*
2. *Lorsqu'une application polynomiale f est un isomorphisme, l'application polynomiale g dans la définition ci-dessus est unique et est appelée inverse de f.*

Exemples 3.1.1
• *Les applications affines bijectives f de k^n dans k^n sont les isomorphismes : Elles correspondent aux polynômes de $deg f$.*
• *Soit $A \subset k^n$. La projection $\Phi : A \to k^P$, $(x_1, \ldots, x_n) \to (x_1, \ldots, x_P)$ est un morphisme.*
• *Soit $A = \mathcal{V}(Y - X^2)$ une parabole. La projection $\Phi : A \to k, (x, y) \to x$ est un isomorphisme de réciproque $x \to (x, x^2)$.*
• *L'application $k \to \mathcal{V}(-X^3+Y^2-X^2), t \to (t^2-1, t)(t^2-1)$ (on coupe V avec la droite $Y = tX$) est un morphisme.*
• *L'application $\Phi : k \to \mathcal{V}(Y^2 - X^3), t \to (t^2, t^3)$ est un morphisme bijectif mais n'est pas un isomorphisme.*

Définition 3.1.4 *Soit $\Phi \in Reg(A,B)$. Pour $f \in k[B]$. On définit le morphisme de $k-$algebre :* $\Phi^* : k[B] \to k[A]$, $\Phi^*(f) = f \circ \Phi$.

Remarque 3.1.2
$(g \circ f)^* = f^* \circ g^*$

Exemples 3.1.2
• *soit $\varphi = (\varphi_1, \ldots, \varphi_m) : A \to B$ un morphisme.Soit η_i la i-ème fonction coordonnée sur B, image de l'indéterminée Y_i dans $k[B]$. Alors $\varphi^*(\eta_i) = \varphi_i$.*
• *si $\varphi : \mathcal{V}(F) \subset k^2 \to k$, $\varphi(x,y) = x$ alors $\varphi^* : k[X] \to k[X,Y]/(F)$, $X \to X$.*

Proposition 3.1.1 *L'application $\gamma : Reg(A,B) \to hom_{k-alg}(k[B], k[A])$ est bijective.*

Preuve : On suppose $A \subset k^n$ *et* $B \subset k^m$ et note η_i les fonctions coordonnées sur B.
Injectivité : Si $\varphi^* = \Psi^*$ *alors* $\varphi_i = \varphi^*(\eta_i) = \Psi^*(\eta_i) = \Psi_i$ *donc* $\varphi = \Psi$.
Surjectivité : Soit $\Theta : k[B] \to k[A]$ un morphisme de k-algèbres. Soit $\varphi_i\Theta(\eta_i) \in k[A]$.
Cela définit $\varphi : A \to k^m$. Il s'agit de montrer que φ est à valeurs dans B et ainsi $\varphi^* = \Theta$.
Soit $F(Y_1, \ldots, Y_m) \in \mathfrak{I}(B)$ *et* $x \in A$. Ainsi $F(\varphi(x)) = F(\Theta(\eta_1)), \ldots, \Theta(\eta_m))(x)$. Or Θ est un morphisme de k-algèbre donc $F(\Theta(\eta_1), \ldots, \Theta(\eta_m)) = \Theta(F(\eta_1), \ldots, F(\eta_m))$. Or $F(\eta_1, \ldots, \eta_m)$ est l'image de $F(Y_1, \ldots, Y_m) \in \mathfrak{I}(B)$ *dans* $k[B]$, donc est nul.

Remarque 3.1.3 *Si A est un ensemble algébrique fini, alors toute application f de A vers une variété algébrique B, est un morphisme.*

Exemples 3.1.3 *Soient A et B deux fermés algébriques de $\mathbb{A}^n$.*
Si $f_1, \ldots, f_n \in k[A]$ et si pour tout $x \in A$, $f_1(x), \ldots, f_n(x) \in B$, alors l'application

$$A \to B, x \to (f_1(x), \ldots, f_n(x))$$

est un morphisme de variétés algébriques. De plus, tous les morphismes de variétés algébriques : $A \to B$ sont de cette forme.
Si $f : A \to B$ est un morphisme de variétés algébriques, on notera

$$f^* : k[B] \to k[A] \text{ le morphisme de } k-\text{algèbres associe à } f.$$

Remarque 3.1.4 *Soient A et B deux variétés algébriques affines. Pour tout morphisme de*

$$k-\text{algèbre } \Phi : k[B] \to k[A],$$

il existe un unique morphisme de variétés algébriques $f : A \to B$ tel que $f^* = \Phi$

Définitions 3.1.5 *Soit $\Phi : A \to B$ un morphisme de variétés algébriques.*
On dit que Φ est dominant si $\Phi(A) = B$.
On dit que Φ est une immersion fermée si $\Phi(A)$ est fermé dans B et que $\Phi : A \to \Phi(A)$ est un isomorphisme.

Proposition 3.1.2 *Soit $\Phi : A \to B$ un morphisme de variétés algébriques.*
Φ est dominant si et seulement si Φ^* injective.

Preuve : $\Rightarrow$) Si $f \in ker\Phi^*$, alors $f \circ \Phi = 0$, c'est à dire, f est nulle sur $\Phi(A)$; par densité f est nulle sur tout X.
$\Leftarrow$) *Si* $\overline{\Phi(A)} \subset B$, alors il existe $f \in k[X]$ non nulle mais nulle sur $\Phi(A)$.
Mézalor(dans la théorie des nombres en 1971) : $\Phi^*(f) = 0 \Rightarrow f = 0$ impossible

Lemme 3.1.1 *Pour* $0 \leq i \leq n$, *soit*

$$\Phi_i : \mathbb{A}^n \to \mathbb{P}^n, (y_1, \ldots, y_n) \to [y_1 : \ldots : y_{i-1} : 1 : y_i : \ldots : y_n]$$

et pose $U_i = \{P = [x_0 : \ldots : x_n] \in \mathbb{P}^n, x_i \neq 0\}$. *On a ainsi un recouvrement* $\mathbb{P}^n = \cup_i U_i$.
On a un homomorphisme :$\Phi_i^{-1} : U_i \to \mathbb{A}^n$ *où* $\mathbb{A}^n$ *est muni de la topologie des Zariski et* U_i *de la topologie induite de la topologie des Zariski sur* $\mathbb{P}^n$

Lemme 3.1.2 (*théorème sur la dimension des fibres*)
Soient k un corps et $f : A \subset k[A] \to B \subset k[B]$ *un morphisme dominant entre variétés sur k. Il existe un ouvert non-vide U de B tel que*

$$\forall\ y \in U :\ dim f^{-1}(y) = dim A - dim B.$$

De plus, f est une application fermée.

Preuve : *voir* [*Har*77] *ou* [*Mum*99] *corollary* 1 *P* . 50

Lemme 3.1.3 *Soit* $f : A \to B$ *un morphisme dominant de variétés affines. Soit* $x \in A$ *tel que* $f^{-1}(f(x))$ *est fini. Alors f est localement fini en x, c'est à dire : il existe un ouvert affine U de B tel que* $f^{-1}(U)$ *soit un ouvert affine et le morphisme restreint :* $f^{-1}(U) \to U$ *soit un morphisme fini.*

3.1.1 Groupes algébriques

Définition 3.1.6
Un groupe algébrique sur le corps k est une variété algébrique G sur k, munie :

i) d'un morphisme de variétés algébriques sur k $m : G \times G \to G,\ (g, h) \mapsto gh$.
ii) d'un morphisme inverse $i : G \to G,\ g \mapsto g^{-1}$;
iii) d'un élément neutre e appartenant à $G(k)$ (*un point rationnel de G*).

3.1.2 Morphismes et isomorphismes de groupes algébriques

Définitions 3.1.7

- *Un morphisme de groupes algébriques* $\Phi : A \to B$ *est un morphisme de variétés algébriques qui est aussi un morphisme de groupes.*
- *C'est un isomorphisme s'il existe un morphisme* $\Psi : B \to A$ *tel que* $\Psi \circ \Phi = idA$ *et* $\Phi \circ \Psi = idB$

Définitions 3.1.8

- *On appelle variété abélienne une variété projective vérifiant une structure de groupe algébrique.*

- *Un morphisme de variété abélienne est un morphisme de groupes algébriques, qui est aussi un morphisme de variétés algébriques.*

Exemples 3.1.4
Les variétés abéliennes de dimension 1 *sont les courbes elliptiques.*
La jacobienne d'une courbe algébrique projective non-singulière géométriquement connexe, de genre g*, est une variété abélienne de dimension* g*.*

3.2 Isogénies

3.2.1 Isogénie entre variétés abéliennes

Définitions 3.2.1 (*Isogénie et Degré d'une isogénie*).
Considérons $I : A \to B$ *un morphisme de variétés abéliennes.*
$\odot$ *Un morphisme de variétés abéliennes* I *est une isogénie, s'il est surjectif et de noyau fini.*
$\odot$ *Le degré d'une isogénie* $I : A \to B$ *sur un corps* k *est le cardinal de son noyau. Il est aussi égal au degré de son extension de corps* $[k(A) : k(B)]$*. Un exemple typique d'isogénie est la multiplication par* n

$$\begin{aligned} n_A : A &\to A \\ a &\mapsto na \end{aligned}$$

Pour tout entier naturel n *(même quand il est divisible par la caractéristique de* k*). Cette isogénie est degré* n^{2g} *si* $g = dimA$*.*

Proposition 3.2.1 *Soit* $f : A \to B$ *un morphisme de variétés abéliennes. Les conditions suivantes sont équivalentes :*

1. f *est une isogénie.*
2. $dimA = dimB$ *et* f *est surjective.*
3. $dimA = dimB$ *et* $ker(f)$ *est fini.*

Preuve :
On utilise le théorème sur la dimension des fibres :
1. $\Rightarrow$ 2. : f est surjective et $dimA - dimB = dimker(f) = 0$.
2. $\Rightarrow$ 3. : $dimA = dimB$ et par surjectivité de f, on en déduit que $ker(f)$ est dimension 0, donc fini.
3. $\Rightarrow$ 1. : L'image continue d'un ensemble irréductible est encore irréductible, donc $f(A)$ est irréductible. Or $dimA = dimB$, donc $f(A) = B$.

Lemme 3.2.1
Soient A, B, C *des variétés abéliennes et* $f : A \to B$ *et* $h : C \to B$ *des isogénies de variétés abéliennes sur* k*. Si* $g_1 : B \to C$ *et* $g_2 : B \to C$ *sont des morphismes tels que*

$$h \circ g_1 \circ f = h \circ g_2 \circ f, \ alors \ g_1 = g_2.$$

Preuve :
Sans perte de généralité, posons $k = \overline{k}$ avec $\overline{k}$ la clôture algébrique de k. Supposons que $h \circ g_1 \circ f = h \circ g_2 \circ f$. Puisque f est un morphisme, d'après le théorème 16, c'est un épimorphisme, donc il s'en suit que $h \circ g_1 = h \circ g_2$. D'*où* $g_1 - g_2$ est une application de B dans le groupe fini $Ker(h)$. Comme B est connexe et réduit, $g_1 - g_2$ se factorise à travers $Ker(h)^0_{red}$ qui est trivial.

Définition 3.2.2 (*Polarisation*)
Considérons une variété abélienne A sur le corps k.
Une polarisation A est une isogénie $\alpha : A \to A^*$ vérifiant l'une des condition équivalentes suivantes :
1 : α est une isogénie symétrique et $\alpha^* \in \mathcal{F}$ un faisceau ample.
2 : α est une isogénie symétrique et $\alpha^* \in \mathcal{F}$ est un faisceau effectif.
3 : S'il existe une extension k' de k et faisceau ample L dans $A_{k'}$ de sorte que $\alpha_{k'} = \varphi_L : A \to A^*$.
4 : S'il existe une extension de corps fini et séparable k' de k et un faisceau ample L dans $A_{k'}$ tel que $\alpha_{k'} = \varphi_L : A \to A^*$.

Définition 3.2.3 *Le degré d'une polarisation est son degré en tant que isogénie.*

3.2.2 Accouplement de Weil

Définition 3.2.4 (*Accouplement bilinaire*)
On considère une courbe elliptique E définie sur un corps k. Soit un entier $n > 0$, et on suppose que k contient une racine primitive $n-$ième de l'unité, et on note μ_n le groupe cyclique des racines $n-$ièmes de l'unité dans k. Notons enfin les points de n-torsion de la courbe :

$$E[n] = \{P \in E(\overline{k}) \mid [n]P = O\}$$

où $[n]$ est l'application de << multiplication par n >> dans le groupe des points rationnels de la courbe, O est l'élément neutre du groupe (le << point infini >>), et $\overline{k}$ est la clôture algébrique de k. Alors il existe un accouplement :

$$w_n : E[n] \times E[n] \to \mu_n$$

que l'on appelle accouplement de Weil. Cette fonction possède notamment les propriétés suivantes :
• *Bilinéaire : $w_n(P+Q,R) = w_n(P,R) + w_n(Q,R)$.*
• *Alternante : $w_n(P,Q) = w_n(Q,P)^{-1}$ et en particulier, $w_n(P,P) = 1$.*
• *Non-dégénérescence : Si $w_n(P,Q) = 1$ pour tout $Q \in E[n]$, alors $P = O$; de même si $w_n(P,Q) = 1$ pour tout $P \in E[n]$ alors $Q = O$.*
• *Invariance par les opérations du groupe de Galois : pour tout $\sigma \in Gal(\overline{k}/k)$, $w_n(P^\sigma, Q^\sigma) = w_n(P,Q)^\sigma$*

3.2.3 Isogénie entre courbes elliptiques

Définitions 3.2.5 *Soient (E,O) et (E',O) deux courbes elliptiques définies sur le même corps k. Une isogénie de E vers E' est un morphisme non nul $I : E \to E'$ entre deux courbes elliptiques. C'est un morphisme de groupes, mais aussi une application régulière donnée par des fractions rationnelles en x, y. L'ensemble des isogénies de E dans E' est noté $Hom(E,E')$. les endomorphismes forment un anneau $End(E)$ avec pour produit la composition.*
On appelle le degré de l'isogénie I le degré de ces fractions.
L'ensemble des isogénies $Hom(E,E')$ possède une structure de groupe abélien. Une composée d'isogénies est une isogénie.
Il existe une dualité naturelle entre $Hom(E,E')$ et $Hom(E',E)$ associant à une isogénie $I : E \to E'$ une isogénie duale $\tilde{I} : E' \to E$ de même degré (disons n).
Une isogénie définie sur k sera dite $k-$rationnelle ou simplement rationnelle quand il n'y a pas d'ambiguïté.
On relie les isogénies au groupe de torsions.
Il existe un certain c et une fraction rationnelle I_x tel que

$$I(x,y) = (I_x(x), cyI'_x(x))$$

Définition 3.2.6 *Soit k un corps algébriquement clos, I une isogénie définie sur k de E dans E', I est dite séparable ou inséparable selon que l'extension $k(E)/I^*(k(E'))$ l'est ou pas avec pour une isogénie I on peut définir sur les corps de fonctions associés à E et E' l'injection suivante*

$$I^* : k(E') \to k(E), f \to f \circ \phi.$$

On note alors $deg_s I$, $deg_i I$ les degrés de séparabilité et d'inséparabilité de l'extension du corps $k(E)/I^*(k(E'))$.
Nous avons donc $degI = deg_s I.deg_i I$ qui est égal aussi au degré de l'extension de corps $k(E)/I^*(k(E'))$.

Remarques 3.2.1 *Le noyau $Ker(I)$ d'une isogénie séparable $I : E \to E'$ est l'ensemble*

$$Ker(I) = \{P \in E(k) \mid I(P) = 0_{E'}\}$$

c'est un sous groupe de $E(\bar{k})$ d'ordre $deg(I)$ qui est rationnel sur k.
Inversement, tout sous-groupe fini G de $E(\bar{k})$ rationnel su k est le noyau d'un isogénie séparable de degré $|G|$ de E vers une autre courbe $E' = E/G$ définie su k. Le noyau d'une isogénie de degré l sera un sous-groupe de cardinal l.

Définition 3.2.7 *L'isogénie I est normalisée si $c = 1$.*

Exemples 3.2.1
• *Les multiplications scalaires pour $m \in \mathbb{Z}$*

$$[m]_E : E \to E,\ P \mapsto P + \cdots + P,\ m\ fois$$

sont des endomorphismes. L'isogénie $[m]$ est de degré m^2, son noyau est noté $E[m]$, le sous-groupe des points de $n - torsions$ de la courbe. En utilisant la loi de groupe, on peut calculer explicitement un polynôme de degré $m^2 - 1$ s'annulant sur les points de $E[m]$, le polynôme de $n - torsion$ de E.
Cela donne une copie de $\mathbb{Z}$ à l'intérieur de $End(E)$. Ce ne sont pas toujours les seuls endomorphismes, et même jamais lorsque k est un corps fini de cardinal q.
• *Le morphisme de Frobenius*

$$\pi_E : (x, y) \to (x^q, y^q)$$

est un endomorphisme.
• *Si E est une courbe elliptique sur $\mathbb{C}$, on montre que E est isomorphe à un tore complexe :*

$$E \approx \mathbb{C}/\wedge,\ \wedge\ réseau\ de\ \mathbb{C}.$$

La loi de E coïncide avec celle $\mathbb{C}/\wedge$, et l'isogénie devient simplement la multiplication par un nombre complexe : on a une isogénie

$$[m] : \mathbb{C}/\wedge \to \mathbb{C}/\wedge'\ dès\ \alpha \in \mathbb{C}^*\ vérifie\ \alpha\wedge \subset \wedge'.$$

Par exemple, le noyau de la multiplication scalaire $[m]$ est alors $E[m](\mathbb{C}) = \frac{1}{m}\wedge/\wedge$, un groupe isomorphe à $(\mathbb{Z}/m\mathbb{Z})^2$.

Lemme 3.2.2 *Soient (E, O) et (E', O') deux courbes elliptiques, et soit $\phi : E \to E'$ un morphisme de variétés.*
Si $\phi(O) = O'$, alors ϕ est un morphisme de groupes, et $\mu'_E \circ (\phi \times \phi) = \phi \circ \mu_E$.

Lemme 3.2.3 *Soit $\tau \subset E$ un sous-groupe fini. Alors τ est le noyau d'une isogénie $I : E \to E'$.*

Preuve : La théorie de Galois nous dit que $\overline{k}(E)$ est galoisienne de groupe τ sur le sous-corps $\overline{k}(E)^\tau$. En particulier, ce dernier a pour degré de transcendance 1 sur $\overline{k}$, donc est le corps de fonctions d'une courbe projective lisse C. De plus, l'inclusion de corps provient d'un morphisme $\phi : E \to C$ de degré $[\tau]$.
Montrons que ϕ est constant sur les $\tau - orbites$ dans E. En effet, si $\phi(\gamma + P) \neq \phi(P)$ alors on peut trouver $f \in \overline{k}(C)$ avec un pôle en $\phi(P)$ et sans pôle en $\phi(\gamma + P)$. Alors f, vue comme fonction sur E, aurait un pôle en P mais pas en $\gamma + P$, ce qui est absurde puisque f est $\tau - invariante$. Cela implique que les fibres de ϕ sont de cardinal $[\tau]$ et, par conséquent, que ϕ est non ramifiée. Mais alors la formule de Hurwitz assure que $g(C) = 1$. En posant $O' = \phi(O)$, on a donc une courbe elliptique (C, O) munie d'une isogénie $\phi : E \to C$ de noyau τ.

Théorème 3.2.1 *Soit $f : E \to E'$ une isogénie de degré n. Il existe une unique isogénie $\hat{f} : E' \to E$ telle que $\hat{f} \circ f = [n]_E$ et $f \circ \hat{f} = [n]'_E$. On dit que $\hat{f}$ est l'isogénie duale de f.*

Preuve : L'unicité est claire, vu la surjectivité de f. De même, supposant l'existence de $\hat{f}$, l'égalité $f \circ \hat{f} \circ f = f \circ [m]_E = [m]'_E \circ f$ montre que $f \circ \hat{f} = [m]'_E$. Supposons maintenant l'existence de$\hat{f}$ *et* $\hat{g}$ comme dans l'énoncé, alors on a

$$(\hat{f} \circ \hat{g}) \circ (g \circ f) = \hat{f}[degg]'_E \circ f = \hat{f} \circ f[degg]_E = [degf]_E[degg]_E = [deg(f+g)]_E$$

d'*où* l'existence de $\widehat{g \circ f}$ et l'égalité $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$. Cela nous permet de traiter séparément les isogénies séparables et purement inséparables.
Dans le cas *où* f est séparable, on a $f^*(\overline{k}(E')) = \overline{k}(E)^{kerf}$ tandis que $[m]^*_E(\overline{k}(E)) \subset \overline{k}(E)^{ker[m]_E}$. Or $kerf$ est d'ordre $m = degf$, donc contenu dans $ker[m]_E$, et on a donc des inclusions

$$\overline{k}(E) \supset f^*\overline{k}(E') \supset [m]^{*\overline{k}(E)}.$$

On en déduit un morphisme de corps $(f^*)^-1 \circ [m]^* : \overline{k}(E) \to \overline{k}(E')$, auquel correspond un morphisme de variétés $\hat{f} : E' \to E$ tel que $\hat{f} \circ f = [m]_E$. On a nécessairement $\hat{f}(O') = O$, donc $\hat{f}$ est une isogénie.
Dans le cas *où* f est purement inséparable, elle est de la forme $f_q : E \to E'$ avec $q = p^r$ (isogénie de Frobenius), et se décompose en $E \xrightarrow{f_p} E^{(p)} \xrightarrow{f_p^{(p)}} E^{(p^2)} \to \ldots \to E^{(q)}$, donc il suffit de traiter le cas $q = p$. Mais alors le théorème nous dit que $[p]_E$ est inséparable, donc se factorise $[p]_E = g \circ f_p^r$, avec g inséparable, et donc se factorise aussi $[p]_E = g' \circ f_p$ et il n'y a plus qu'à poser $\hat{f}_p := g$.

Exemple 3.2.2 *(Isogénie duale)*
Soit k de caractéristique $\neq 2$. Soient $a, b \in k$ avec $b \neq 0$ et $r = a^2 - 4b \neq 0$. Notons E la courbe d'équation affine $y^3 = x^2 + ax^2 + bx$ et E' celle d'équation affine $y^2 = x^3 - 2ax + rx$. On a alors deux isogénies de degré 2

$$I : E \to E', (x, y) \mapsto (\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2})$$

et

$$\hat{I} : E' \mapsto E, (x, y) \mapsto (\frac{y^2}{4x^2}, \frac{y(r - x^2)}{8x^2})$$

On vérifie par calcul que $\hat{I} \circ I = [2]_E$ et $I \circ \hat{I} = [2]_{E'}$. On en déduit que $I = \hat{I}$ est l'isogénie duale de I.

Propositions 3.2.2 *Les points suivants sont vérifiés.*

(i) Soit $f : E \to E'$ une isogénie. On a $deg(f) = deg(\hat{f})$ et $\hat{\hat{f}} = f$

(ii) Soient $f : E \to E'$ et $g : E' \to E''$ deux isogénies. On a $\widehat{g \circ f} = \hat{f} \circ \hat{g}$

(iii) Soient $f : E \to E'$ et $g : E \to E'$ deux isogénies. On a $\widehat{f + g} = \hat{f} + \hat{g}$

(iv) Pour tout $m \in \mathbb{Z}$. On a $\hat{[m]}_E = [m]_E$ et $deg([m]_E) = m^2$

Preuve :
Admettons le point 3 pour l'instant et prouvons le dernier. On en déduit $\hat{[m]}_E = [m]_E$ par récurrence de n. On a ensuite $[deg(m)] = [m] \circ \hat{[m]} = [m] \circ [m] = [m^2]$, donc $deg(m) = m^2$ puisque $[\bullet] : \mathbb{Z} \to End(E)$ est injective.
Montrons le second point. Soit $r = deg(f)$ *et* $s = deg(g)$. On a $g \circ f \circ \hat{f} \circ \hat{g} = g \circ [r] \circ \hat{g} = [r] \circ g \circ \hat{g}$ car g est un morphisme de groupe donc $g \circ [r] = [r] \circ g$. On trouve donc $g \circ f \circ \hat{f} \circ \hat{g} = [r] \circ [s] = [rs] = [deg(g \circ f)]$ d'*où* $\widehat{g \circ f} = \hat{f} \circ \hat{g}$.
Montrons le premier point. On a $deg(f).deg(\hat{f}) = deg(f \circ \hat{f}) = deg(deg(f)) = deg(f)^2$ d'*où* $deg(f) = deg(\hat{f})$. On a ensuite en notant $m = deg(f) = deg(\hat{f}$ les égalités

$$[m] \circ \hat{f} = f \circ \hat{f} \circ \hat{f} = f \circ [m] = [m] \circ f$$

donc $f = \hat{f}$.
La démonstration du point 3 est authentiquement difficile. Elle demande de considérer des diviseurs sur la surface $E \times kE$, et de considérer la courbe elliptique $E_k(\eta E)$ sur le corps non parfait $k(\eta E)$.

Proposition 3.2.3 *Si $I : E \to E'$ est une isogénie, alors*

$$I(P + Q) = I(P) + I(Q) \text{ pour tout } P,\ Q \in E$$

Théorèmes 3.2.2 *Soit I une isogénie de E dans E', alors :*
• *Pour tout point P de E' on a $|I^{-1}(P)| = deg_S(I)$,*
• *Si I est séparable alors $deg_S(I) = deg(I) = |Ker(I)|$*

Preuve : *Voir* $[sil86, III.4.10]$

Corollaire 3.2.1
Si $car(k) \neq 2$, alors $E[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^2$ pour tout $n > 0$.

Preuve :
On vient de voir que $|E[2]| = 4$. Puisque $[2]_E$ est séparable, elle est non ramifiée et donc de degré 4. Il s'en suit que $[2^n]_E$ est degré 4^n, et puisqu'elle est aussi non ramifiée, on $|E[2^n]| = (2^n)^2$. D'après la théorie des groupes, on déduit par récurrence que $E[2^n] = (\mathbb{Z}/2^n\mathbb{Z})^2$

Corollaire 3.2.2

(i) Si $(m, car(k)) = 1$ alors $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ $m \in \mathbb{N}^*$.

(ii) Si $p = car(k)$ alors soit $E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$ pour tout n, soit $E[p^n] = \{O\}$ pour tout n.

Preuve :

(i) Lorsque $(m, car(k)) = 1$, on a donc $|E[m]| = m^2$. En écrivant $E[m]$ comme produit de groupes cycliques et en utilisant $|E[m']| = (m')^2$ pour $m'|m$, on obtient le i).

(ii) Si $p = car(k)$, écrivons $[p]_E = \hat{\phi}_p \circ \phi_p$ *où* $\phi_{\ p} : E \to E^{(p)}$ est l'isogénie de Frobenius. Si $\hat{\phi}_p$ est séparable, alors $|E[p]| = deg_s([p]_E) = p$ et plus généralement $|E[p^n]| = deg_s([p]_E) = p^n$, *d'où* l'on tire par récurrence que $E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$. Si $\hat{\phi}_p$ est inséparable alors $deg_s([p]_E) = deg([p^n]_E) = 1$ *et* $E[p] = E[p^n] = O$ pour tout n.

Définition 3.2.8
Si $E[p] = \{O\}$, E *est dite super singulière. Sinon, elle est dite ordinaire.*

Corollaire 3.2.3
L'application degré $deg : hom(E, E') \to \mathbb{N}$ *est une forme quadratique définie positive.*

Preuve :
La positivité et le caractère défini sont clairs. Ce qui l'est beaucoup moins est la bilinéarité de l'application $\varphi, \psi) \to deg(\varphi\varphi + \psi) - deg(\varphi) - deg(\psi)$. Regardons cette expression dans $End(E)$, à travers l'injection $\mathbb{Z} \to End(E)$. On a :

$$\begin{aligned}
[deg(\varphi+\psi)]_E - [deg(\varphi)]_E - [deg(\psi)]_E = & \quad (\widehat{\varphi+\psi}) \circ (\varphi+\psi) - \widehat{\varphi} \circ \varphi - \widehat{\psi} \circ \psi \\
= & \quad (\widehat{\varphi} + \widehat{\psi}) \circ (\varphi+\psi) - \widehat{\varphi} \circ \varphi - \widehat{\psi} \circ \psi \\
= & \quad \widehat{\varphi} \circ \psi + \widehat{\psi} \circ \varphi.
\end{aligned}$$

La dernière expression est bien $\mathbb{Z} - bilinaire\ en\ (\varphi, \psi)$

3.3 Applications

Calculer une isogénie $I : E \to E'$ peut avoir plusieurs significations. Dans cette partie, on s'intéresse à deux situations :
• On connait E et $KerI$, et l'on souhaite calculer une équation de E' ainsi que des fractions rationnelles définissant I (*en somme, on souhaite construire un quotient explicitement*).
• On connait E, E' et éventuellement le degré de I, et l'on souhaite retrouver le noyau de I et des fractions rationnelles la définissant. On demande donc de calculer entièrement une isogénie lorsque l'on sait qu'elle existe.
La première question est résolue à l'aide des formules de Vélu, proposées en 1971. De nombreuses méthodes ont vu le jour pour calculer le noyau d'une isogénie, en commençant par la méthode de Stark, publiée en 1972 et qui concerne les endomorphismes d'une courbe elliptique à multiplication complexe.
L'histoire récente commence avec les travaux d'Elkies dans les années 1990 : il s'inspire des travaux de Stark et Vélu pour calculer les fractions rationnelles d'une isogénie, à condition qu'elle soit normalisée. Il fait circuler manuscrit en $1991 - 1992$ (*explicitisogenies*) puis en publie une version étendue en 1998. Dans le même manuscrit, des techniques sont développées par Alkin, sous la forme de mails principalement : on peut trouver certains manuscrits à l'adresse *http* : *//www.lix.polytechnique.fr/labo/franois.Mmorain/*. Ces méthodes ont fait l'objet d'articles au journal de théorie des nombres de Bordeaux.
Il n'existe alors pas d'algorithmes fonctionnant en petite caractéristique. En 1994, Conveignes

publie sa thèse contenant un algorithme à base de groupes formels qui résout ce problème. Cet algorithme est complexe, et cela pousse Lercier à développer en 1996 un algorithme dans le cas de la caractéristique 2 de complexité non prouvée, mais très intéressant en pratique. Ce travail est ensuite généralisé par Conveignes, qui propose un algorithme basé sur l'interpolation de l'isogénie en certains points de la courbe.
Les progrès réalisés depuis prennent surtout la forme d'amélioration et généralisation de méthodes existantes : Bostan, Morain, Salvy et Schost améliorent en 2008 la méthode d'Elkies, pour pouvoir l'utiliser en petite caractéristique, Lairez et Vacon remarquent que la précision $p-adique$ est nécessaire à cette dernière méthode. De Feo, dans sa thèse et des articles ultérieurs développent la méthode de Conveignes.
Cette partie est organisée comme suit ; dans un premier temps, on présente d'abord les formules de Vélu, enfin, on s'intéresse à des méthodes comme la méthode de Stark, la méthode d'Elkies , la méthode de Conveignes .

3.3.1 Les formules de Vélu

Soit E une courbe elliptique sur k donnée sous forme de Weierstrass

$$y^2 = x^3 + ax + b.$$

La question posée par Vélu est la suivante : connaissant un sous-groupe fini G de $E(\overline{k})$, comment déterminer une isogénie dont ce sous-groupe est le noyau ? On supposera $car(G)$ impair pour simplifier.
Afin de déterminer une équation de la courbe elliptique image,
on cherche des fonctions rationnelles x' et y' sur E de degrés respectifs 2 et 3
(comme x, y d'une équation de Weierstrass). On définit ainsi

$$x'(P) = \sum_{g\in G} x(P+g) - \sum_{g\in G\setminus\{0_E\}} x(g), \tag{3.1}$$

$$y'(P) = \sum_{g\in G} y(P+g) - \sum_{g\in G\setminus\{0_E\}} y(g) \tag{3.2}$$

pour tout point $P \in E(\overline{k})$. Pour trouver une équation satisfaite par ces deux fonctions (c'est à dire l'équation de la courbe image), on trouve des fractions rationnelles f, g telles que $x' = f(x)\ et\ y' = yg(x)$: on regroupe les termes $P+g\ etP-g$, on utilise la loi de groupe et on trouve

$$x' = x + \sum_{g\in G\setminus\{0_E\}} [\frac{3x^2(g)+a}{x-x(g)} + 2\frac{x^3(g)+ax(g)+b}{(x-x(g))^2}], \tag{3.3}$$

$$y' = y - y\sum_{g\in G\setminus\{0_E\}} [\frac{3x^2(g)+a}{(x-x(g))^2} + 4\frac{x^3(g)+ax(g)+b}{(x-x(g))^3}]. \tag{3.4}$$

On développe ces expressions et on déduit l'équation

$$y'^2 = x'^3 + a'x' + b'$$

avec

$$a' = a - 5\sum_{g\in G\setminus\{0_E\}} (3x^2(g)+a) \tag{3.5}$$

$$b' = b - 7\sum_{g\in G\setminus\{0_E\}} (5x^3(g)+3ax(g)+2b). \tag{3.6}$$

Le terme constant de x a été ajusté pour trouver une équation réduite. On a ainsi l'équation de la courbe image, et les expressions (3.3) et (3.4) donnent l'isogénie sous forme de fractions rationnelles. Les relations (3.5) *et* (3.6) sont souvent exprimées en fonction des coefficients du polynôme dont $x(g)$ sont les racines.

3.3.2 La méthode de Stark

Stark s'intéresse au calcul d'endomorphisme d'une courbe elliptique E à multiplication complexe par O, définie par exemple sur une extension finie de $\mathbb{Q}$ et donnée par une équation de la forme

$$y^2 = x^3 - ax - b.$$

On a vu qu'il existe un réseau Λ de $\mathbb{C}$ tel que $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Ce paramétrage est donné par

$$z \to (\varrho(z), \frac{\varrho'(z)}{2}) \tag{3.7}$$

pour $z \in \mathbb{C}/\Lambda$, *où* ϱ est la fameuse fonction de Weierstrass associée à Λ. Si $\beta \in O$, on a un endomorphisme $[\beta]_E$ de E qui s'écrit $z \to \beta z$ dans le point de vue du tore complexe.
La question est alors d'exprimer cet endomorphisme du point de vue algébrique plutôt analytiquement, c'est à dire en tant que application rationnelle sur la courbe E. Cela revient à trouver une fraction rationnelle f telle que l'on ait l'égalité de fonctions méromorphes sur $\mathbb{C}$:

$$\varrho(\beta z) = f(\varrho(z)) \tag{3.8}$$

La fraction f donne alors la coordonnée x de l'endomorphisme $[\beta]_E$. En regardant les zéros et les pôles de ces séries de Laurent, on peut savoir que f s'écrit $\frac{p}{q}$, *où* les polynômes p et q sont de degrés respectifs $|\beta|^2$ *et* $|\beta|^2 - 1$.
La quantité $|\beta|^2$ est le degré de cet endomorphisme.
Pour calculer ces deux polynômes, *Stark* utilise un algorithme de décomposition en fraction continue inspiré des nombres réels. Lorsque l'on se donne $\alpha \in \mathbb{Q}$, on définit $\alpha_0 = \alpha$ et pour tout $j \geq 0$,

$$a_j = \lfloor \alpha_j \rfloor, \quad \alpha_{j+1} = \frac{1}{\alpha_j - a_j}$$

et l'on s'arrête lorsque $\alpha_j = a_j$. Le rationnel α est alors égal à

$$\frac{p_j}{q_j} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_j}}}. \tag{3.9}$$

Le principe est exactement le même ici, et cela permet d'écrire facilement $\varrho(\beta z)$ sous forme de fraction rationnelle en $\varrho(z)$.
Bien sûr, on manipule dans cet algorithme uniquement un nombre fini de coefficients des séries de Laurent comme $\varrho(z)$. On connait le degré des polynômes p, q obtenus à la fin de l'algorithme, ce qui permet de contrôler le nombre de coefficients nécessaire au calcul. Ces coefficients sont obtenus à l'aide de l'équation différentielle $\varrho'^2 = 4\varrho^3 + 4a\varrho + 4b$:

$$\varrho(z) = \frac{1}{z^2} + \frac{a}{5}z^2 + \frac{b}{7}z^4 + \dots \tag{3.10}$$

Telle qu'expose ci-dessus, la méthode de *Stark* ne s'applique qu'à des endomorphismes et non à une isogénie.

3.3.3 La méthode d'Elkies

Les calculs proposés par *Elkies* partent de l'idée d'inverser les formules de Vélu.
Soit $I : E \to E'$ une isogénie de degré l, *avec* $l = 2n+1$ impair (on conserve cette simplification ici). On se donne une équation de Weierstrass pour E et E' ; cette donnée est équivalente à celles de formes différentielles w_E *et* $w_{E'}$. On dit que I est normalisée si $I^* w_{E'} = w_E$.
On peut voir que l'isogénie quotient $E \to E/G$ donnée par les formules de Vélu est normalisée.
L'idée d'*Elkies* est alors la suivante : si I est normalisée, alors l'équation de Weierstrass de E' est celle que l'on aurait obtenue en appliquant les formules de Vélu à partir de $KerI$. Si le polynôme $K(X) = \sum(-1)^{n-1}\sigma_{n-1}X^i$ a pour racines les abscisses des éléments de $KerI$, les relations de Vélu fournissent le coefficient σ_2 ainsi qu'une relation linéaire entre σ_1 *et* σ_3.
Comment continuer et calculer les coefficients suivants du polynôme ?
Comme I est normalisée, on peut écrire

$$I(x,y) = (I_x(x), yI'_x(x)), \quad I_x(x) = \frac{N(x)}{D(x)} \tag{3.11}$$

où N et D sont des polynômes de degrés l *et* $l-1$, et $D = K^2$. L'équation de E' donne donc une équation différentielle (notons l'analogie avec les idées de *Stark*) :

$$y^2 I'^2_x(x) = I_x(x)^3 + a' I_x(x) + b' \tag{3.12}$$

où l'on remplace y^2 par $x^3 + ax + b$ et que l'on différencie pour obtenir une équation du second ordre :

$$(3x^2 + a)I'_x + 2(x^3 + ax + b)II''_x = 3I_x^2 + a'. \tag{3.13}$$

On développe ensuite I_x en série de x^-1 :

$$I_x(x) = x + \sum_{i\geq 1}(\frac{h_i}{x^i}.$$

L'équation différentielle (3.13) donne une relation de récurrence liant les coefficients h_i, qui s'initia lise grâce aux relations tirées de (3.5) et (3.6)

$$h_1 = \frac{a - a'}{5}, \qquad h_2 = \frac{b - b'}{7}. \tag{3.14}$$

On peut retrouver les coefficients de K à partir de ceux de I_x, puisque l'on peut réarranger (3.3) et (3.4) en

$$I_x(x) = lx - \sigma_1 - (3x^2 + a)\frac{K'(x)}{K(x)} - 2(x^3 + ax + b)(\frac{K'(x)}{K(x)})'. \tag{3.15}$$

On obtient une relation de récurrence qui permet de déterminer les coefficients de K. Cependant, pour l'utiliser il faut connaître la qualité de σ_1 (la somme des racines de K). On peut parfois la déterminer par d'autres méthodes, mais on ne dispose pas toujours de renseignement.
L'algorithme d'*Elkies* est quadratique en l en termes d'opérations dans le corps de base. Tel qu'expose ci-dessus, il s'applique aux isogénies normalisées pour laquelle on dispose d'un renseignement supplémentaire, et n'est donc pas utilisable directement en général.
Bostan, Morain Salvy et Schoof reprennent cette méthode en 2008 en proposant deux améliorations. La première est l'utilisation d'une itération de Newton afin de résoudre l'équation (3.13) dans les séries formelles ; on passe ainsi d'un algorithme quadratique en l à une complexité

quasi-optimale, linéaire en l à facteurs logarithmiques près. Atteindre cette complexité nécessite de plus, d'utiliser des algorithmes rapides pour la manipulation des polynômes et séries formelles, que l'on peut trouver par exemple dans le livre de Von zur de Gathen et Gerhardt
La seconde idée est de récupérer le polynôme $K(x)$ non pas à partir de la relation (3.15), mais directement à partir de la série formelle $I_x(x) = \dfrac{N(x)}{K(x)}$ à l'aide d'un algorithme dit de reconstruction rationnelle. Cela nécessite de calculer un peu plus de coefficients de I_x, mais connaître la somme des racines de K n'est plus nécessaire. En revanche, on demande toujours une isogénie normalisée.
Remarquons que résoudre les différentes relations de récurrence (ou l'application de la méthode de Newton) nécessite de diviser par beaucoup de petits entiers dans le corps de base. Cet algorithme n'est donc pas utilisable en petite caractéristique. De plus, on ne sait pas normaliser une isogénie en temps quasi-linéaire : proposer un algorithme quasi-linéaire dans tous les cas reste une question ouverte.

3.3.4 L'algorithme de Conveignes

L'algorithme de Conveignes permet de donner une solution au problème de calcul d'isogénie en petite caractéristique. Soit p un nombre premier, $q = p^r$ *et* $E/\mathbb{F}_q$ une courbe elliptique.
L'endomorphisme $[p]$ de E n'est pas séparable : dans la plupart des cas, E est une courbe dite ordinaire, et l'on a pour tout $j \geq 1$

$$E[p^j](\overline{k}) \simeq \mathbb{Z}/p^j\mathbb{Z}. \tag{3.16}$$

L'inséparable se voit bien : il n'y a pas assez de points dans le noyau par rapport au degré.
Lorsque $I : E \to E'$ est une isogénie de degré l premier à p, elle définit une bijection

$$E[p^j](\overline{k}) \to E'[p^j](\overline{k}). \tag{3.17}$$

Pour simplifier, fixons $j \geq 1$ et supposons que les points de $p^j - torsion$ de E sont définis sur $\mathbb{F}_q$. C'est alors vrai sur E' également, puisque ce sont les images par ϕ des points de E. Choisissons deux points P, P' qui engendrent respectivement les groupes cycliques $E[p^j](\overline{k}), E'[p^j](\overline{k})$. Il existe alors un unique $a \in (\mathbb{Z}/p^j\mathbb{Z})^*$ tel que $I(P) = [a]P'$. Comme I est un morphisme de groupes, elle envoie également le point $[m]P$ sur $[am]P'$ pour tout entier m. Conveignes propose donc de choisir un coefficient a et de tenter d'interpoler l'isogénie entre ces points ; si cela échoue, on prend un autre coefficient a jusqu'à trouver le bon !
Afin d'interpoler une fraction rationnelle de degré l, il faut disposer de suffisamment de points : il faut choisir l'entier j tel que $p^j > 4l$. Pour trouver un générateur de $E[p^j](\mathbb{F}_q)$, on calcule un polynôme de division T_j définissant $E[p^j]$ et on en cherche une racine dans $\mathbb{F}_q$, à l'aide de l'algorithme de Cantor-Zassenhaus.
Bien sûr, en général les points de $E[p^j]$ ne sont pas $\mathbb{F}_q - rationels$, et il faut manipuler des extensions du corps $\mathbb{F}_q$. Si T_j se scinde sur$\mathbb{F}_q$ en f facteurs irréductibles de degré d

$$T_j = \prod_{k=1}^{f} U_{kj}, \tag{3.18}$$

il est intéressant de travailler avec les d extensions $\mathbb{F}_q[X]/U_{kj}$ munie d'isomorphismes compatibles, plutôt que dans le gros anneau $\mathbb{F}_q[X]/T_j$. On peut aussi calculer intelligemment des isomorphismes avec les analogues de ces corps que l'on obtient avec la courbe E'. Afin d'obtenir une meilleure complexité, il faut également utiliser des méthodes rapides pour la manipulation de polynômes. Lorsque $l >> p$, on obtient un algorithme de coût essentiellement quadratique

en l en termes de $\mathbb{F}_q - opérations$.
En revanche, le $cô$t est exponentiel en $logp$, puisqu'il faut manipuler des polynômes de degré au moins $p-1$. Pour cette raison, l'algorithme de *Conveignes* n'est pas adapté lorsque $logp$ n'est pas très petit. Pour traiter le cas de la caractéristique intermédiaire (lorsqu'un algorithme de grande caractéristique comme la méthode *d'Elkies* n'est pas applicable du fait de division par zéro sans que p soit petit), on peut étendre l'algorithme de Conveignes en interpolant sur la $n^k - torsion$ pour un premier n distinct de l et p : voir par exemple de Feo, Hugonenq, Pût et Schost.

Conclusion

Dans ce document, nous avons d'abord introduit des outils fondamentaux pour la compréhension d'isogénies entre courbes elliptiques. On remarque de nombreuses applications d'isogénies entre courbes elliptiques comme illustré par quelques exemples donnés dans la dernière partie.

- La méthode de Vélu
- La méthode de Stark.
- La méthode d'Elkies.
- La méthode de Conveignes.

Il existe d'autres applications comme l'algorithme de Schoof, d'Alkin, de SEA$\cdots$

Une attention particulière est accordée aux variétés abéliennes. C'est dans ce cadre qu'on a donné des exemples plus explicites d'isogénies pour lesquelles, on a appliqué le calcul d'isogénies.

Bibliographie

[1] Bostan.A, Morain.F, Salvy.B and Schost.E. Fast algorithms for computing isogenies between elliptic curves. Mathématics of computation, 77(263) : 1755 − 1778, 2008.

[2] Morain.F. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. Journal de théorie des nombres Bordeaux, 7(1) : 255 − 282, 1995.

[3] Robin Hartshorne, Algebraic Geometry, Springer-Verlag, New York, 1977, graduate texts in Mathematics.

[4] Stark.M.H. Class number of complex quadratic field. In W. Kuyk, editor, Modular fonctions of on variable I, pages 153 − 174. Antwerp, 1972.

[5] Conveignes. -M.J. Quelques calculs en théorie des nombres. PhD thesis, 1994.

[6] Conveignes. -M.J. Computing $l-isogenies$ with the $p-torsion$. Algorithms number theory, $ANTSII$, $L.N.C.S.$, 1122 : 59 − 65, 1996.

[7] Conveignes. -M.J. Isomorphisms between Artin-Schreier towers. Maths. Comp., 69(232) : 1625 − 1631, 2000

[8] Nekovar.J, Algebraic theory of elliptic curves, cours de M_2, disponible sur sa page web.

[9] Silvermann.H.J. The arthmetic of elliptic curves 1986.

[10] Silvermann.H.J. Advanced topics in the arithmetic of elliptic curves. Springer, 1994.

[11] Vélu.J. Isogénies entre courbes elliptiques. Comptes-rendus de l'académie des sciences, série I, 273 : 238 − 241, 1971.

[12] Von Zur Gathen.J and Gerhard.J. Modern Computer Algebra. Cambridge University Press, 1999.

[13] De Feo.L, Hugounenq.C, Plût.J, and Schost.E. Explicit isogenies in quadritic times in any characteristic. $LMSJ. Comp. Math.$, 19(A) : 267 − 282, 2016.

[14] De Feo.L. Fast algorithms for towers of finite fields and isogenies. PhD thesis, Ecole Polytechnique, 2010.

[15] Elkies.D.N. Elliptics and modular curves over finite fields and related computational issues, 1997. Preprint.

[16] Lairez.P and Vaccon.T. On $p-adic$ differential equations with separation of variables. In proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '16, *pages* 319 − 323, 2016.

[17] The PARI Group, Univ.Bordeaux. PARI/GP version 2, 9, 0, 2017.
availlable from http : //pari.math.u-bordeaux.fr/.

[18] Lercier.R and Sirvent.T. On Elkies subgroup of $l-torsion$ points in elliptic curves defined over a finite field. Journal de théorie des nombres de Bordeaux, 20(3) : 783 − 797, 2008.

[19] Lercier.R. Computing isogenies in $\mathbb{F}_{2^n}$. Algorithmic Number Theory, *ANTS II*, *L.N.C.S.*, 1122 : 197 − 212, 1996

[20] Schoof.R. Counting points on elliptic curves over finite fields. Jounal de théorie des nombres de Bordeaux, 7(1).

[21] William.C. Waterhouse, Abelian varieties over Funite Fields, Ann. Sci . Ecole Norm. Sup. (4) 2 (1969), 521 − 560.