UNIVERSITE ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES
Département de Mathématiques

MÉMOIRE DE MASTER
Domaine : Sciences et Technologies
Mention : Mathématiques et Applications
Spécialité : Mathématiques Pures
Option : Géométrie Algébrique

Sujet :

VARIÉTÉS ABÉLIENNES

---

présenté le 11 Mars 2017

par

MOHAMADOU MOR DIOGOU DIALLO
diogou_mor@ymail.com

Sous la direction de
OUMAR SALL

Devant le jury :

Prénom(s) et Nom	**Grade**	**Qualité**	**Établissement**
Alassane DIEDHIOU	Maître de conférences	Examinateur	UNIV. A.S.Z
Amoussou Thomas GUEDENON	Chargé d'enseignement	Examinateur	UNIV. A.S.Z
Clément MANGA	Chargé d'enseignement	Examinateur	UNIV. A.S.Z
Marie Salomon SAMBOU	Professeur	Président	UNIV. A.S.Z
Oumar SALL	Professeur	Directeur	UNIV. A.S.Z

11 mars 20017

TABLE DES MATIÈRES

Remerciements

C'est une grande chance et un honneur de pouvoir effectuer son travail de mémoire sous la direction du Professeur **Oumar Sall**. Ses méthodes de travail sont pour moi une référence et un modèle. Je lui suis très sincèrement et infiniment reconnaissant pour le problème qu'il m'a proposé et je lui suis très aimable d'avoir partagé ses idées avec moi et je lui renouvelle mes plus profondes admirations. Je le remercie chaleureusement pour sa patience et pour sa très grande disponibilité, pour son enthousiasme et pour ses conseils. Je tiens à insister sur le rôle inestimable, tant sur le plan professionnel que personnel, de toutes les connaissances et les valeurs mathématiques qu'il m'a transmises.

Je tiens à exprimer ma gratitude à monsieur **Amoussou Thomas GUEDENON** (UASZ) pour m'avoir transmis ses connaissances en algèbre, qui ont été indispensables tout le long de mon travail.

Je remercie tous ceux qui ont bien voulu accepter de faire partie du jury avec tout ce que cela implique comme temps et changement de timing. Je vous remercie infiniment.

Je remercie également les personnes sans lesquelles, je n'aurais jamais eu les capacités requises pour faire tout le boucle de ces deux niveaux (Licence et Master). Je me permettrais de citer les noms : monsieur **Marie Salomon SAMBOU** (UASZ) dont le savoir m'a permis de comprendre le lien entre la géométrie et l'analyse, monsieur **Edouard DIOUF** (UASZ), monsieur **Alassane DIEDHIOU** (UASZ), monsieur **Ndiéne NGOM** (UASZ), monsieur **Clément MANGA** (UASZ), monsieur **Cheikh Mbacké DIOP** (UCAD), monsieur **Abdoulaye SENE** (UCAD), monsieur **Diaraf SECK** (UCAD), monsieur **Gorgu M. SAMB**, monsieur **Guy MBATCHOU** (UASZ), monsieur **Khalifa GAYE** (UASZ), monsieur **Cheikh Tidiane DIENG** (UASZ), monsieur **Mbaye Diagne MBAYE** (UASZ), monsieur **Magatte CAMARA** (UASZ), monsieur **Bomol Ali SOW** (UASZ), monsieur **Modou TINE** (UASZ), monsieur **Diouma KOBOR** (UASZ), monsieur **Moctar CAMARA** (UASZ), monsieur **Lat Grand NDIAYE** (UASZ) et monsieur **CAMARA** (Université de METZ). Je leur suis très profondément reconnaissant.

Je remercie ma mère et mon père pour lesquels j'ai gardé et je garderai de bonnes pensées. Mes remerciements vont aussi à mes grands frères **Abdoulaye Diallo** et **Youssouph Diallo**, à ma petite sœur **Jeynab Diallo** et à tous mes petits frères. Je ne saurais vous oublier, pour tout le soutien psychologique, moral et encouragement que vous m'avez apportés durant toutes ces années.

Mes pensées vont aussi à mes amis : **Ousseynou Sarr**, **Baboucar Diatta**, **Amadou Seikou Diallo**, **Assane Sarr**, **Tidiane Mballo**, **Cherif Mamina Coly**, **Raphael Diatta**, **Seny Diatta**, **Mor Ndiaye**, **Moctar Diallo**, **Binté Diallo**, **Aliou Diallo**, à tous les camarades de promotion et à tous ceux ayant eu une bonne intention à mon égard.

Ce mémoire a bien sûr été un passionnant parcours intellectuel, l'occasion d'approfondir mes connaissances en géométrie algébrique et de découvrir de nouveaux problèmes

mathématiques fascinants et de goûter aux plaisirs et aux exigences de l'initiation à la recherche.

Ça a été aussi et avant tout une formidable expérience personnelle, tant bien difficile, mais que c'est de ces difficultés qu'on sort avec des connaissances plus approfondies.

Si l'aventure se termine de façon heureuse, c'est en grande partie grâce à vous tous, que DIEU vous accorde son salut, AAMINE.

Introduction

La géométrie algébrique est l'étude des variétés algébriques, définies comme ensembles des zéros d'un ou plusieurs polynômes. L'origine de cette étude remonte à Descartes et de nombreux autres mathématiciens : Abel, Riemann, Poincaré, M. Noether, l'école italienne avec Severi. Plus récemment Weil, Zariski et Chevalley s'y sont illustrés . Dans les années 1950-1960 la géométrie algébrique a connu un développement considérable et a subi un bouleversement gigantesque sous l'impulsion de J.-P. Serre et surtout d'A. Grothendieck.

Aujourdh'ui la géométrie algébrique est l'une des disciplines fondamentales dans de nombreuses parties des mathématiques.

L'objectif de ce mémoire est d'étudier un cas particulier intéressant des variétés algébriques : les variétés abéliennes.

Une variété abélienne est un ensemble possédant une structure de groupe et une structure de variété algébrique projective, ces deux structures étant compatibles. La condition de projectivité est d'une grande utilité et plusieurs propriétés des variétés abéliennes en découlent ; c'est le cas, par exemple, de la proposition suivante connue sous le nom de lemme de rigidité :

Proposition :
Soient $\mathscr{X}$ une variété projective, $\mathscr{Y}$ et $\mathscr{Z}$ deux variétés quelconques, et $f : \mathscr{X} \times \mathscr{Y} \to \mathscr{Z}$ un morphisme. S'il existe un point y_0 de $\mathscr{Y}$ tel que f restreint à $\mathscr{X} \times \{y_0\}$ est constant, alors f est constant sur toute tranche $\mathscr{X} \times \{y\}$.

Si de plus f est constant sur une tranche de la forme $\{x_0\} \times \mathscr{Y}$ alors f est constant sur tout $\mathscr{X} \times \mathscr{Y}$.

La méthodologie utilisée pour réaliser cette étude est basée sur une approche comprenant trois chapitres structurés de la manière suivante :

Le chapitre1 intitulé " Préliminaires" regroupe des notions de base utiles dans les chapitres suivants. Les résultats sont sonvent donnés sans démonstration, mais illustrés par des exemples et par des remarques pour faciliter la compréhension aux lecteurs moins familiarisés avec ces théories.

Le chapitre 2 intitulé " Variétés Abéliennes " qui constitue le coeur du sujet présente quelques propriétés importantes des variétés abéliennes et donne quelques méthodes pour décrire les applications dans une variété abélienne. La reconnaissance de certaines propriétés renseigne sur leurs applications (cryptographie, algorithme de Satoh, algorithme de Kedlaya, etc.).

Pour illustrer cette utilité on a donné comme exemple le théorème de Weil suivant :

Théorème (Weil).

Théorème :
Soient $\mathscr{V}$ une variété projective définie sur le corps de nombres K et D un diviseur sur $\mathscr{V}$ et l'application $h_{\mathscr{V},D} : \mathscr{V} \longrightarrow \mathbb{R}$. Il existe une application

$$h_{\mathscr{V}} : Div(\mathscr{V}) \longrightarrow \{h_{\mathscr{V},D}\}$$

tel que :

1) Normalisation : pour un hyperplan $H \subset \mathbb{P}^n$de codimension 1, on a :

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1); \quad \forall P \in \mathbb{P}^n(\bar{k}).$$

2) Fonctorialité : pour un morphisme de variétés $\phi : \mathscr{V} \longrightarrow \mathscr{W}$ induisant une application $\phi^* : Div(\mathscr{W}) \longrightarrow Div(\mathscr{V})$, et un diviseur $D \in Div(\mathscr{W})$, on a :

$$h_{\mathscr{V},\phi^*D}(P) = h_{\mathscr{V},D}(\phi(P)) + O(1), \quad \forall P \in \mathbb{P}^n(\bar{k}).$$

Pour D,$D' \in Div(\mathscr{V})$ on a :

$$h_{\mathscr{V},D+D'}(P) = h_{\mathscr{V},D}(P) + h_{\mathscr{V},D'}(P), \quad \forall P \in \mathbb{P}^n(\bar{k}).$$

3) Équivalence linéaire : Si D, $D' \in Div(\mathscr{V})$ sont des diviseurs linéairement équivalents, alors

$$h_{\mathscr{V},D} = h_{\mathscr{V},D'} + O(1).$$

4) Positivité : Si D est un diviseur sur $\mathscr{V}$, considérons B un sous-ensemble des points associé au système linéaire $|D|$. Alors :

$$h_{\mathscr{V},D}(P) \geq O(1) \quad P \in (\mathscr{V} \backslash B)(K).$$

5) Propriété de Northcott : Si $D \in Div(\mathscr{V})$ est un diviseur ample, alors pour toute extension fini K' de K et une constante réel M, l'ensemble

$$\{P \in \mathscr{V}(K') \mid h_{\mathscr{V},D}(P) \leq M\}$$

est fini.

$O(1)$ étant une constante ne dépendant que de chacune des données suivantes : les variétés, diviseurs, morphismes ; mais pas du point P.

Le chapitre 3 est intitulé "Développement et Problématiques ", dans cette partie on a présenté quelques exemples d'applications pouvant intéresser des chercheurs dans les domaines à travers plusieurs branches mathématiques.

CHAPITRE 1

PRÉLIMINAIRES

Sauf précision, on suppose que k est un corps commutatif et n un entier naturel non nul. On note $k[X_1,\ldots,X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans k.

1.1 Variétés algébriques

1.1.1 Ensembles algébriques affines, ensembles algébriques projectifs

Définition 1.1.1.1 (***espaces affines, espaces projectifs***)

1. *On appelle* ***espace affine*** *de dimension n l'ensemble k^n produit cartésien itéré n fois k. Cet ensemble est noté $\mathbb{A}^n(k)$(ou $\mathbb{A}^n$).*
2. *On définit sur k^{n+1} la relation d'équivalence $\sim$ suivante : pour tous éléments non nuls $a=(a_0,\ldots,a_n)$ et $b=(b_0,\ldots,b_n)$ de k^{n+1} :*

   $$a\sim b \quad \text{si et seulement si il existe } \lambda\in k^* \text{ tel que } (b_0,\ldots,b_n)=\lambda(a_0,\ldots,a_n).$$

   On appelle ***espace projectif*** *de dimension n et l'on note $\mathbb{P}^n(k)$ (ou $\mathbb{P}^n$ ou $\mathbb{P}(k^{n+1})$) l'ensemble quotient de $k^{n+1}\setminus\{0\}$ par la relation d'équivalence $\sim$ (ie $\mathbb{P}^n=k^{n+1}\setminus\{0\}/\sim$).*

Définition 1.1.1.2 (***Points linéairement indépendants***)
On dit que les points de $\mathbb{P}^n$ sont linéairement indépendants si les droites de k^{n+1} qu'ils représentent sont en somme directe.

Soit $P\in\mathbb{P}^n$ ayant pour représentant (ou vecteur directeur) $(x_0,\ldots,x_n)\in k^{n+1}\setminus\{0\}$, alors P sera noté $P=(x_0:\ldots:x_n)$.

Définition 1.1.1.3 (***Coordonnées homogènes***)
Soit $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n$. On dit que les x_i sont des coordonnées homogènes de P, et que $(x_0 : \ldots : x_n)$ est un système de coordonnées homogènes de P.

Définition 1.1.1.4 (***Sous-ensembles affines***)
Soit $S \subset k[X_1, \ldots, X_n]$. On note $\mathscr{V}(S)$ le sous-ensemble de $\mathbb{A}^n$ formé des zéros communs à tous les éléments de S :

$$\mathscr{V}(S) := \{x \in \mathbb{A}^n \mid F(x) = 0, \forall F \in S\}.\ ^1$$

Les sous-ensembles de ce type sont appelés les ***sous-ensembles algébriques affines*** *de $\mathbb{A}^n$.*

Définition 1.1.1.5 (***Sous-ensembles projectifs***)
Soit $S \subset k[X_0, \ldots, X_n]$ formée des polynômes homogènes. On note $\mathscr{V}(S)$ le sous-ensemble de $\mathbb{P}^n$ formé des zéros communs à tous les éléments de S :

$$\mathscr{V}(S) := \{x \in \mathbb{P}^n \mid F(x) = 0, \forall F \in S\}.$$

Les sous-ensembles de ce type sont appelés les ***sous-ensembles algébriques projectifs*** *de $\mathbb{P}^n$.*

⊛ **Cas particuliers**
⊙ On appelle **hypersurface**, un sous-ensemble algébrique défini par l'annulation d'un seul polynôme.
⊙ Un **hyperplan** est une hypersurface définie par un polynôme de degré 1.
⊙ Une courbe algébrique plane est une hypersurface de $\mathbb{A}^2$ (cas affine) ou de $\mathbb{P}^2$ (dans le cas projectif).

Proposition 1.1.1.1 (*[14] ; page 10*)

i) l'ensemble vide et l'espace tout entier sont algébriques.

ii) Toute intersection de sous-ensembles algébriques est un sous-ensemble algébrique.

iii) Toute union finie de sous-ensembles algébriques est un sous-ensemble algébrique.

Démonstration :

i) 1. L'ensemble vide est un ensemble algébrique. En effet $\emptyset = \mathscr{V}(P)$ ou P est un polynôme constant non nul.
2. L'espace affine $\mathbb{A}^n$ (resp projectif $\mathbb{P}^n$) est algébrique. En effet, chacun de ces espaces peut s'écrire sous la forme $\mathscr{V}(0)$ où 0 désigne le polynôme nul.

ii) Soit $P \in \bigcap_\alpha \mathscr{V}(S_\alpha)$: on a $P \in \bigcap_\alpha \mathscr{V}(S_\alpha)$ ssi $\forall \alpha$, $P \in \mathscr{V}(S_\alpha)$ ssi $\forall F \in (\bigcup_\alpha S_\alpha)$, $F(P) = 0$ ssi $P \in \mathscr{V}(\bigcup_\alpha S_\alpha)$.

iii) Soient S et T deux sous-ensembles algébriques, on a : $P \in \mathscr{V}(S) \bigcup \mathscr{V}(T)$ ssi $P \in \mathscr{V}(S)$ ou $\mathscr{V}(T)$ ssi $P \in \mathscr{V}(FG, F \in S$ et $G \in T)$ qui est bien un ensemble algébrique. La suite se fait par récurrence.

1. **NB** : l'application $\mathscr{V}$ est décroissante.

Exemple 1.1.1.1 (*[14] ; page 10*)
Soient P, $Q \in \mathbb{C}[X,Y]$ définis par $P = X^2+Y^2-1$ et $Q = X+2$. Posons $S = \{P,Q\}$, on a :

$$\mathscr{V}(S) = \{(x,y) \in \mathbb{C}^2 | x^2+y^2-1 = 0 \text{ et } x+2 = 0\} = \{(-2, -i\sqrt{3}),(-2, i\sqrt{3})\}.$$

Remarque 1.1.1.1
$*$ *De la Proposition 1.1.1.1, on peut munir les ensembles algébriques d'une topologie dite topologie de Zariski, dont les fermés sont les ensembles algébriques.*
$*$ *On utilisera cette topologie dans toute la suite.*

1.1.2 Idéal d'un sous-ensemble algébrique

Définition 1.1.2.1 (***idéal d'un sous-ensemble algébrique***)
*Soit V un sous-ensemble de $\mathbb{A}^n$; on appelle **idéal** de V et l'on note $\mathfrak{I}(V)$, l'ensemble des polynômes nuls sur V :*

$$\mathfrak{I}(V) := \{F \in k[X_1,\ldots,X_n] \mid F(x) = 0, \forall x \in V\}$$

Définition 1.1.2.2 (***radical d'un idéal***)
*Soit J un idéal d'un sous-ensemble algébrique V. On appelle **radical** de J et on note $\sqrt{J}$, l'idéal :*

$$\sqrt{J} := \{P \in k[X_1,\ldots,X_n] \mid \exists r \in \mathbb{N}^*, P^r \in J\}$$

Théorème 1.1.2.1 (***Nullstellensatz***) (*[12], page 5*)
Soit J un idéal de $k[X_1,\ldots,X_n]$. Si k est algébriquement clos alors on a : $\mathfrak{I}(\mathscr{V}(J)) = \sqrt{J}$.

Démonstration :
Dire que $\mathfrak{I}(\mathscr{V}(J)) = \sqrt{J}$ prouve que $J = k[X_1,\ldots,X_n]$ si et seulement si $\mathscr{V}(J)$ est vide. En effet si $J = k[X_1,\ldots,X_n]$, alors J contient le polynôme constant 1 et $\mathscr{V}(J)$ est vide. Réciproquement si $\mathscr{V}(J)$ est vide, $\mathfrak{I}(\mathscr{V}(J)) = k[X_1,\ldots,X_n]$. Or $1 \in \sqrt{J}$ et donc il existe $r \in \mathbb{N}$ tel que $1 = 1^r \in \sqrt{J}$, c'est-à-dire que $J = k[X_1,\ldots,X_n]$.
Maintenant, on va montrer que si pour tout $m \in \mathbb{N}^*$ et tout idéal propre L de $k[X_1,\ldots,X_n]$, $\mathscr{V}(L)$ n'est pas vide, alors pour tout $n \in \mathbb{N}^*$ et tout idéal J, on a $\mathfrak{I}(\mathscr{V}(J)) = \sqrt{J}$. Soit J un idéal de $k[X_1,\ldots,X_n]$. On a l'inclusion $\mathfrak{I}(\mathscr{V}(J)) \supset \sqrt{J}$ qui est triviale. Soit $P \in k[X_1,\ldots,X_n]\backslash\{0\}$ tel que $P(a) = 0$, lorsque $a \in k^n$ tel que $Q(a) = 0$, alors $Q \in J$. Soit L l'idéal de $k[X_1,\ldots,X_n,y]$ engendré par J et $1-yP$. Alors $\mathfrak{I}(L) = \emptyset$; et notre hypothèse implique que $L = k[X_1,\ldots,X_n,y]$. Il existe par conséquent des polynômes $P_1,\ldots,P_l \in J$ et $R_0,\ldots,R_l \in k[X_1,\ldots,X_n,y]$ tels que $1 = R_0(1-yP)+R_1P_1+\ldots+R_lP_l$.
En posant $y = 1/P$, et en multipliant des deux côtés de l'égalité par une puissance suffisamment grande de P pour éliminer les puissances de P aux dénominateurs des fractions du membre de droite, on obtient l'existence d'un entier r tel que $P^r \in J$.

1.1.3 Irréductibilité

Définition 1.1.3.1 (***irréductibilité***)
*Soit $\mathscr{Z}$ un sous-ensemble algébrique muni de la topologie de Zariski. On dit que $\mathscr{Z}$ est **irréductible** s'il n'est pas réunion de deux fermés propres de $\mathscr{Z}$; ceci équivaut à dire que l'intersection de deux ouverts non vides est non vide, ou encore, que tout ouvert non vide est dense. En d'autres termes*

$$si \quad \mathscr{Z} = \mathscr{Z}_1 \cup \mathscr{Z}_2 \quad avec \quad \mathscr{Z}_1 \ et \ \mathscr{Z}_2 \ des \ fermés \ de \ \mathscr{Z} \ alors \ \mathscr{Z} = \mathscr{Z}_1 \ ou \ \mathscr{Z} = \mathscr{Z}_2.$$

Ce qui implique que tout ouvert non vide de $\mathscr{Z}$ est également irréductible.

Proposition 1.1.3.1 (*[12], page 11*)
Pour un ensemble algébrique (affine ou projectif) $\mathscr{Z}$, les conditions suivantes sont équivalentes :

1) *$\mathscr{Z}$ est irréductible ;*

2) *$\mathfrak{I}(\mathscr{Z})$ est un idéal premier ;*

3) *$k[\mathscr{Z}]$ est un anneau intègre.*

Démonstration :
Cas affine :
1) $\Rightarrow$ 2) Si $\mathscr{Z}$ est irréductible et si $F,G \in k[X_1,\ldots,X_n]$ sont tels que $FG \in \mathfrak{I}(\mathscr{Z})$, alors $\mathscr{Z} = \mathscr{V}(\mathfrak{I}(\mathscr{Z})) \subset \mathscr{V}(FG) = \mathscr{V}(F) \cap \mathscr{V}(G)$ si bien que $\mathscr{V}(FG) \subset \mathscr{V}(F)$(*ou* $\mathscr{V}(G)$) et donc $F \in \mathfrak{I}(\mathscr{V}(F)) \subset \mathfrak{I}(\mathscr{Z})$. On voit donc que $\mathfrak{I}(\mathscr{Z})$ est un idéal premier.
2) $\Rightarrow$ 3) Si $\mathfrak{I}(\mathscr{Z})$ est premier, alors $k[\mathscr{Z}] = k[X_1,\ldots,X_n]/\mathfrak{I}(\mathscr{Z})$ est intègre.
3) $\Rightarrow$ 1) Enfin, si $k[\mathscr{Z}]$ est intègre et si $\mathscr{Z} = \mathscr{W} \cup \mathscr{T}$, alors $0 = \mathfrak{I}(\mathscr{Z}) = \mathfrak{I}(\mathscr{W} \cup \mathscr{T}) = \mathfrak{I}(\mathscr{W}) \cap \mathscr{Z}(\mathscr{T}) \supset \mathfrak{I}(\mathscr{W}) \cdot \mathfrak{I}(\mathscr{T})$ si bien que $\mathfrak{I}(\mathscr{W})$(ou $\mathfrak{I}(\mathscr{T})) = 0$ et donc $\mathscr{W} = \mathscr{V}(\mathfrak{I}(\mathscr{W})) = \mathscr{V}(0) = \mathscr{Z}$.
On voit donc que $\mathscr{Z}$ est irréductible.

Définition 1.1.3.2
*Soit $\mathscr{Z}$ un ensemble algébrique muni de la topologie de Zariski. On dira que $\mathscr{Z}$ est **connexe** s'il ne peut pas s'écrire comme union disjointe de deux fermés propres de $\mathscr{Z}$:*

$$si \;\; \mathscr{Z} = F_1 \bigsqcup F_2 \text{ avec } F_1 \text{ et } F_2 \text{ deux fermés de } \mathscr{Z} \text{ alors } \mathscr{Z} = F_1 \text{ ou } \mathscr{Z} = F_2.$$

*Si $\mathscr{Z}$ n'est pas connexe, on dira que $\mathscr{Z}$ est **disconnexe** ; dans ce cas il s'écrit comme réunion disjointe de deux fermés propres.*

Proposition 1.1.3.2 (*[12], page 12*)
*Si $\mathscr{Z}$ est **irréductible** alors $\mathscr{Z}$ est connexe.*

Démonstration : (voir [12], page 12)

Définition 1.1.3.3 (***Composante irréductible***)
Soit $\mathscr{Z}$ un ensemble algébrique non vide. Il existe $\mathscr{Z}_1,\ldots,\mathscr{Z}_l$ des ensembles algébriques irréductibles, à unique permutation près des indices tels que : $\mathscr{Z}_i \neq \mathscr{Z}_j$, pour $i \neq j$, et $\mathscr{Z} = \mathscr{Z}_1 \cup \ldots \cup \mathscr{Z}_l$. Les ensembles algébriques $\mathscr{Z}_1,\ldots,\mathscr{Z}_l$ sont appelés les composantes irréductibles de $\mathscr{Z}$.

Exemple 1.1.3.1 (*[12], page 12*)
On considère dans $\mathbb{A}^2$ l'ensemble algébrique $V = \mathscr{V}(xy)$. Les propriétés de $\mathscr{V}$ impliquent que $V = \mathscr{V}(x) \cup \mathscr{V}(y)$. De plus, chacun de ces deux termes est irréductible, ce qui entraîne que V s'écrit comme union de deux composantes irréductibles.

Définition 1.1.3.4 (***Variétés, sous-variété et ouvert***)
*Une variété algébrique (**affine ou projective**) est un ensemble **algébrique irréductible**. Une sous-variété (**affine ou projective**) est sous-ensemble **algébrique irréductible**. Un ouvert d'une variété affine (resp. projective) est appelée variété **quasi-affine** (resp. **quasi-projective**).*

Définition 1.1.3.5 (***dimension d'une variété algébrique***)
Soit $\mathscr{V}$ une variété algébrique. La ***dimension*** *de $\mathscr{V}$, notée* $\dim \mathscr{V}$ *est le degré de transcendance de $\bar{k}(V)$ sur $\bar{k}$.*

Exemple 1.1.3.2 (*[15], page 10*)
$\odot$ $\dim \mathbb{A}^n = n$.
$\odot$ *Si $f \in k[X_1,\ldots,X_n]$ non constant alors la dimension de l'hypersurface $\mathscr{V}(f)$ est :* $\dim \mathscr{V}(f) = n-1$.

Définition 1.1.3.6 (***Variété lisse***)
Considérons un élément P d'une variété algébrique $\mathscr{V}$ et $f_1,\ldots,f_m \in k[X_1,\ldots,X_n]$ des générateurs de $\mathfrak{I}(\mathscr{V})$.
On dira que $\mathscr{V}$ est ***lisse*** *en P si la matrice jacobienne $m \times n$*

$$(\partial f_i/\partial X_j(P))_{1\leq i\leq m, 1\leq j\leq n}$$

est de rang $n - \dim(\mathscr{V})$.
Si $\mathscr{V}$ est ***lisse*** *en tout point, alors on dit que $\mathscr{V}$ est lisse.*

Définition 1.1.3.7 (***Fonction polynomiale***)
Soit $\mathscr{V}$ une variété algébrique de k^n. Une ***fonction polynomiale*** *sur $\mathscr{V}$ est une restriction d'une* ***fonction polynomiale*** *dans $k[X_1,\ldots,X_n]$ à $\mathscr{V}$. Si $\mathscr{W}$ est une autre variété algébrique dans k^m, une application $f : \mathscr{V} \longrightarrow \mathscr{W}$ est polynomiale si chacune des applications coordonnées l'est.*

1.1.4 Morphismes et applications

Définition 1.1.4.1 (***morphisme et isomorphisme***)

a) *Un* ***morphisme de variétés*** $\Phi : \mathscr{Z} \longrightarrow \mathscr{W}$ *est un $r-uplet$ $\Phi = (\Phi_1,\ldots\ldots,\Phi_r)$ d'éléments de $k[\mathscr{Z}]$, tel que :*

$$\Phi(x) := (\Phi_1(x),\ldots\ldots,\Phi_r(x)) \in \mathscr{W}; \qquad \forall x \in \mathscr{Z}.$$

b) *Un morphisme de variétés $\Phi : \mathscr{Z} \longrightarrow \mathscr{W}$ est un* ***isomorphisme*** *s'il existe un morphisme $\Gamma : \mathscr{W} \longrightarrow \mathscr{Z}$ tel que : $\Gamma \circ \Phi = id_{\mathscr{Z}}$ et $\Phi \circ \Gamma = id_{\mathscr{W}}$.*

Exemple 1.1.4.1 (***[5], page 13***)

1. *Soit $V \subset \mathbb{P}^2$ une hypersurface de degré 2 (**une conique**) donnée par l'équation $x^2 + y^2 - z^2 = 0$. On a un morphisme $\mathbb{P}^2 \longrightarrow V$, $(u : v) \longmapsto (u^2 - v^2, 2uv, u^2 + v^2)$.*
2. *Soit $k = \mathbb{F}_q$ un corps fini et soit $V \subset \mathbb{P}^n$ une variété projective. On définit le morphisme de Frobenius par $Fr : V \longrightarrow V$, $(x_0 : \ldots : x_n) \longmapsto (x_0^q : \ldots : x_n^q)$.*
3. *Soit $P = (0 : \ldots : 0 : 1) \in \mathbb{P}^n$. Une droite $L \subset \mathbb{P}^n$ qui passe par le point P est l'image d'un morphisme $\mathbb{P}^1 \longrightarrow \mathbb{P}^n$, $[u : v] \longrightarrow (a_0u : a_1u : \ldots : a_{n-1}u : v)$, elle est donc déterminée par la donnée de $(a_0 : \ldots : a_{n-1})$. L'ensemble des droites dans $\mathbb{P}^n$ qui passent par un point donné est donc l'espace projectif de dimension $n-1$.*

NB : Si $\Phi : \mathscr{Z} \longrightarrow \mathscr{W}$ est un morphisme de variétés, alors Φ induit un morphisme de k-algèbres appelé le **comorphisme** de Φ définit par : $\Phi^* : k[\mathscr{W}] \longrightarrow k[\mathscr{Z}]$, $\Phi^*(\varphi) = \varphi \circ \Phi$.

Définition 1.1.4.2 (***Immersion fermée***)
*Soit $f : \mathscr{X} \longrightarrow \mathscr{Y}$ un morphisme de variétés algébriques. On dit que f est une **immersion fermée** si $f(\mathscr{X})$ est un fermé de $\mathscr{Y}$ et que f **induit un isomorphisme** de $\mathscr{X}$ dans $f(\mathscr{X})$.*

Définition 1.1.4.3 (***Application régulière,application régulière dominante***)
Soient $\mathscr{X} \subset k^n$ et $\mathscr{Y} \subset k^m$ des variétés algébriques. Une application $\mathscr{X} \longrightarrow \mathscr{Y}$ est régulière si elle est la restriction à $\mathscr{X}$ d'une application $k^n \longrightarrow k^m$ dont les composantes sont des fonctions polynômiales.
*Elle est **dominante** si son image est dense.*

Définition 1.1.4.4 (***fonction régulière***)
*Soient $\mathscr{U}$ un ouvert d'une variété algébrique et $f : \mathscr{U} \longrightarrow k$ une fonction. La fonction f est dite **régulière** en $a \in \mathscr{U}$ s'il existe un voisinage ouvert $V \subseteq \mathscr{U}$ de a et des polynômes $g, h \in k[X_1, \ldots, X_n]$ avec h ne s'annulant pas sur V tel que $f = \frac{g}{h}$ sur V. La fonction f est dite **régulière sur** $\mathscr{U}$ si elle est régulière en tout point de $\mathscr{U}$.*

Exemple 1.1.4.2 (*[2], page 34*)

1. *Toute application affine est régulière.*
2. *Supposons k infini. Soit $\mathscr{C}$ l'hypersurface plane d'équation $Y = X^2$; on vérifie que le polynôme $X^2 - Y$ est irréductible, ce qui entraîne $\mathfrak{I}(\mathscr{C}) = (X^2 - Y)$, La fonction $f : \mathscr{C} \longrightarrow k$ définie par $f(x, y) = x$ est régulière et bijective. Son inverse $x \longmapsto (x, x^2)$ est aussi régulière : on dit que f est un isomorphisme.*
3. *Supposons toujours k infini. Soit $\mathscr{C}$ l'hypersurface plane d'équation $X^2 = Y^3$ (c'est une cubique à point de rebroussement) ; l'application $u : k \longrightarrow \mathscr{C}$ définie par $u(t) = (t^2, t^3)$ est régulière et bijective.*

Proposition 1.1.4.1 (*[12], page 7*)

1) *Pour qu'une application régulière $\mu : \mathscr{V} \longrightarrow \mathscr{W}$ soit dominante, il faut et il suffit que μ^* soit injectif.*
2) *Si μ^* est surjectif alors μ est injective.*

Proposition 1.1.4.2 *([12], page7)*
Une application régulière est continue.

Démonstration :
Cas affine.
Soient $\mathscr{F}$ un fermé de $\mathbb{A}^1$ et $f : \mathscr{F} \longrightarrow \mathbb{A}^1$ une application régulière Si $\mathscr{F}$ est différent de $\mathbb{A}^1$ et de l'ensemble vide, on a $\mathscr{F} = \{\lambda_1, \ldots, \lambda_n\} \subset k$. Pour montrer que f est continue, il suffit de montrer que $f^{-1}(\lambda_i)$ est fermé pour tout i. Pour un élément $a \in \mathscr{U}$, on a l'existence d'un ouvert V_a et de deux polynômes g_a ; h_a tels que $f = f_a = \frac{g_a}{h_a}$ sur V_a et l'on constate que :

$$f^{-1}(\lambda_i) \cap V_a = \mathscr{V}(g_a - \lambda_i h_a) \cap V_a,$$

qui est un fermé, donc $f^{-1}(\lambda_i)$ est fermé. Ainsi, on montre la continuité de f.

Définition 1.1.4.5 (***anneau local***)
Soit $\mathscr{X}$ une variété algébrique. On note $\mathscr{O}(\mathscr{X})$ l'anneau des fonctions régulières sur $\mathscr{X}$. Pour un élément $x \in \mathscr{X}$, on définit l'anneau local de $\mathscr{X}$ en x, noté $\mathscr{O}_{x,\mathscr{X}}$ ou simplement $\mathscr{O}_x$, l'ensemble des fonctions régulières en x.

Définition 1.1.4.6 (***application rationnelle***)
Pour deux variétés algébriques $\mathscr{X}$ et $\mathscr{Y}$, on définit une relation d'équivalence sur les couples $(\mathscr{U}, \varphi_{\mathscr{U}})$ et $(\mathscr{V}, \psi_{\mathscr{V}})$, où $\mathscr{U}$ et $\mathscr{V}$ sont respectivement des ouverts non vides de $\mathscr{X}$ et $\mathscr{Y}$, et $\varphi_{\mathscr{U}} : \mathscr{U} \longrightarrow \mathscr{Y}$ et $\psi_{\mathscr{V}} : \mathscr{V} \longrightarrow \mathscr{X}$ des morphismes, de la manière suivante :

$$(\mathscr{U}, \varphi_{\mathscr{U}}) \sim (\mathscr{V}, \psi_{\mathscr{V}}) \qquad \Longleftrightarrow \qquad \varphi_{\mathscr{U}}{}_{|_{\mathscr{U}\cap\mathscr{V}}} = \psi_{\mathscr{U}}{}_{|_{\mathscr{U}\cap\mathscr{V}}}.$$

*Une **application rationnelle** est une classe pour cette relation d'équivalence ; une telle application est notée $\rho : \mathscr{X} \dashrightarrow \mathscr{Y}$.*

Définition 1.1.4.7 (***Corps des fonctions, fonction rationnelle***)
Soient $\mathscr{U}$ et $\mathscr{V}$ deux ouverts non vide d'une variété algébrique $\mathscr{X}$ et $f : \mathscr{U} \longrightarrow k$ et $g : \mathscr{V} \longrightarrow k$ des fonctions régulières telles que $(\mathscr{U}, f) \sim (\mathscr{V}, g)$ définie de la façon suivante :

$$(\mathscr{U}, f) \sim (\mathscr{V}, g) \Leftrightarrow f_{|\mathscr{U}\cap\mathscr{V}} = g_{|\mathscr{U}\cap\mathscr{V}}.$$

*Une classe d'équivalence pour cette relation est appelée **fonction rationnelle** sur $\mathscr{X}$. L'ensemble quotient est appelé **corps des fonctions rationnelles** de $\mathscr{X}$ et est noté $k(\mathscr{X})$.*

Remarque 1.1.4.1 (*[12], page 7*)
$\oslash$ $\mathscr{U} \cap \mathscr{V}$ doit être non-vide car $\mathscr{X}$ est irréductible.

Exemple 1.1.4.3 (*[12], page 7*)
Les morphismes entre variétés algébriques sont des applications rationnelles.

1.1.5 Produit de variétés

Proposition 1.1.5.1 (*[12], page 19*)
Le produit de deux variétés algébriques irréductibles $\mathscr{V} \times \mathscr{W}$ est irréductible.

Démonstration :
Pour tout $v \in \mathscr{V}$ et $w \in \mathscr{W}$, considérons les applications régulières $\tau_v : \mathscr{W} \longrightarrow \mathscr{V} \times \mathscr{W}$, $x \longmapsto (v,x)$ et $\tau_w : \mathscr{V} \longrightarrow \mathscr{V} \times \mathscr{W}$, $x \longmapsto (x,w)$. Supposons que $\mathscr{V} \times \mathscr{W} = F_1 \cup F_2$ avec F_1 et F_2 des fermés. Alors pour chaque $w \in \mathscr{W}$, on a $\mathscr{V} = \tau_w^{-1}(F_1)$ ou $\mathscr{V} = \tau_w^{-1}(F_2)$. Par conséquent, $\mathscr{W} = W_1 \cap W_2$, où $W_i = \{w \in \mathscr{W} : \tau_w(\mathscr{V}) = F_i\}$. Mais puisque $W_i = \bigcap_{v\in\mathscr{V}} \tau_w^{-1}(F_i)$ donc W_1 et W_2 sont des fermés. Ce qui implique que $\mathscr{W} = W_1$ et donc $\mathscr{V} \times \mathscr{W} = F_1$.

Théorème 1.1.5.1 (*[12], page 20*)
Si $\mathscr{Y}$ est une variété algébrique projective et $\mathscr{X}$ une variété algébrique projective irréductible, alors la projection

$$p : \mathscr{X} \times \mathscr{Y} \longrightarrow \mathscr{X}$$

est fermée.

Démonstration : (voir [12], page 20)

Lemme 1.1.5.1 (*[12], page 35*)
Considérons $\mathscr{U}$, $\mathscr{V}$, $\mathscr{W}$ des variétés algébriques irréductibles et $\mu : \mathscr{U} \times \mathscr{V} \longrightarrow \mathscr{W}$ une application régulière. Si de plus $\mathscr{U}$ est projective et $\mu(\mathscr{U} \times \{v'\})$ ait un seul point avec $v' \in \mathscr{V}$, alors $\mu(\mathscr{U} \times \{v\})$ a un seul point pour tout v de $\mathscr{V}$.

Démonstration :
Soient Γ le graphe de μ et $q : \mathscr{U} \times \mathscr{V} \times \mathscr{W} \longrightarrow \mathscr{V} \times \mathscr{W}$ la projection. Comme $\mathscr{U}$ est projective, donc $q(\Gamma)$ est fermé dans $\mathscr{V} \times \mathscr{W}$; il est aussi irréductible par hypothèse. La projection $q(\Gamma) \to \mathscr{V}$ est surjective, et la fibre de v' est un point, de sorte que $q(\Gamma)$ a même dimension que $\mathscr{V}$ [2]. Soit u' un point de $\mathscr{U}$, la variété $\{(v,\mu(u',v)) \mid v \in V\}$ est fermée dans $q(\Gamma)$ et de même dimension : elles sont égales et pour tout u dans $\mathscr{U}$ et tout v dans $\mathscr{V}$, on a $\mu(u,v) = \mu(u',v)$.

Définition 1.1.5.1 (***variété complète***)
Une variété algébrique $\mathscr{U}$ est complète si pour toute variété algébrique $\mathscr{V}$, la projection $\mathscr{U} \times \mathscr{V} \longrightarrow \mathscr{V}$ est fermée.

Théorème 1.1.5.2 (***Lemme de Rigidité***) (*[8], page 8*)
Considérons une application régulière $\alpha : \mathscr{V} \times \mathscr{W} \longrightarrow \mathscr{U}$ tels que $\mathscr{V}$ soit une variété algébrique complète et $\mathscr{V} \times \mathscr{W}$ soit une variété algébrique irréductible. S'il existe des points $u_0 \in \mathscr{U}$, $v_0 \in \mathscr{V}$ et $w_0 \in \mathscr{W}$ tels que :

$$\alpha(\mathscr{V} \times \{w_0\}) = \{u_0\} = \alpha(\{v_0\} \times \mathscr{W}),$$

alors $\alpha(\mathscr{V} \times \mathscr{W}) = \{u_0\}$.

Démonstration :
Pour la démonstration nous utiliserons le résultat du Lemme 1.1.5.1 et ces deux résultats qui suivent :

(i) Si $\mathscr{X}$ est complète et $\mathscr{Y}$ une variété quelconque, alors la projection $p : \mathscr{X} \times \mathscr{Y} \longrightarrow \mathscr{Y}$ est fermée.

(ii) Si $\mathscr{L}$ est complète et connexe et $\varphi : \mathscr{L} \longrightarrow \mathscr{E}$ une application régulière de $\mathscr{L}$ dans une variété affine $\mathscr{E}$, alors $\varphi(\mathscr{L})$ est une constante.

Soit U_0 un ouvert affine contenant u_0. Par (i) ; $Z \stackrel{def}{=} p(\alpha^{-1}(\mathscr{U} - U_0)$ est fermé dans $\mathscr{W}$. Par définition, Z coïncide avec la seconde coordonne des points de $\mathscr{V} \times \mathscr{W}$ qui ne sont pas dans U_0. Ainsi un point w de $\mathscr{W}$ n'appartient pas à Z si et seulement si $\alpha(\mathscr{V} \times \{w\}) \subset U_0$. En particulier pour w_0 n'appartenant pas à Z, donc $\mathscr{W} - Z$ est non vide. Comme $\mathscr{V} \times \{w\} (\approx \mathscr{V})$ est complète et U_0 est affine, $\alpha(\mathscr{V} \times w)$ est un point de $\mathscr{U}$ lorsque $w \in \mathscr{W} - Z$: en effet ; $\alpha(\mathscr{V} \times \{w\}) = \alpha(\{v_0\} \times \{w\}) = \{u_0\}$. Ainsi α est constante dans le sous-ensemble $\mathscr{V} \times (\mathscr{W} - Z)$ de $\mathscr{V} \times \mathscr{W}$. Puisque $\mathscr{V} \times (\mathscr{W} - Z)$ est non vide et ouvert dans $\mathscr{V} \times \mathscr{W}$ qui est irréductible donc $\mathscr{V} \times (\mathscr{W} - Z)$ est dense $\mathscr{V} \times \mathscr{W}$. Comme $\mathscr{U}$ est séparé, α coïncide avec l'application constante dans l'ensemble $\mathscr{V} \times \mathscr{W}$.

1.2 Espace tangent

Définition 1.2.0.2 (***Dérivations***)
*Soient R un anneau commutatif, A une R-algèbre et M un A-module. Une R-**dérivation** de A dans M est un **morphisme** R-**linéaire**, $\mathfrak{d} : A \longrightarrow M$ tel que :*

$$\mathfrak{d}(ab) = a\mathfrak{d}(b) + b\mathfrak{d}(a)$$

pour tous a, $b \in A$.

2. d'après la proposition 3.22 de ([12], page 35), C'est le théorème sur la dimension des fibrés.

Définition 1.2.0.3 (***Tangentes***)
Soit $\mathscr{X}$ un fermé de $\mathbb{A}^n$ défini par des polynômes $f_1,\dots,f_n \in k[T_1,\dots,T_n]$. Soient $v \in k^n \setminus \{0\}$ et
$L_v := \{x+tv,\ t \in k\}$ la droite passant par $x \in \mathscr{X}$ dirigée par v. On a :

$$L_v \cap \mathscr{X} = \{x+tv : \forall i, f_i(x+tv)\}.$$

Si $v=(v_1,\dots,v_n)$, alors on définit $f_i(x+tv)$ par :

$$f_i(x+tv) = t(\sum_j \partial_j f_i(x) v_j) \mod t^2.$$

*On dira que L_v est **tangente** à $\mathscr{X}$ en x si*

$$(\forall i), \qquad (\sum_j \partial_j f_i(x) v_j = 0).$$

Définition 1.2.0.4 (***Espace tangent de Zariski***)
*Soient $\mathscr{X}$ une variété algébrique et $x \in \mathscr{X}$, on définit l'**espace tangent** de $\mathscr{X}$ en x comme le k-espace vectoriel :*

$$T_x\mathscr{X} := Der_k(\mathscr{O}_x, k_x).$$ [3]

Remarque 1.2.0.1 (*[2], page 44*)
Si $\mathscr{X}$ est affine, alors le morphisme $k[\mathscr{X}] \longrightarrow \mathscr{O}_x$ induit un isomorphisme (de k-espaces vectoriels) :

$$Der_k(\mathscr{O}_x, k_x) \longrightarrow Der_k(k[\mathscr{X}], k)).$$

Définition 1.2.0.5 (***Différentielles***)
Si $f : \mathscr{X} \longrightarrow \mathscr{Y}$ est un morphisme de variétés algébriques, alors f induit un morphisme local : $\mathscr{O}_{x,f(x)} \longrightarrow \mathscr{O}_{\mathscr{X},x}$ et donc une application linéaire :

$$df_{|x} : T_x\mathscr{X} \longrightarrow T_{f(x)}\mathscr{Y}$$

*qu'on appelle la **différentielle** de f en x.*

Remarque 1.2.0.2 (*[2], page 45*)
– Si $f : \mathscr{X} \longrightarrow \mathscr{Y}$, $g : \mathscr{Y} \longrightarrow \mathscr{Z}$ sont des morphismes de variétés algébriques, alors pour tout $x \in \mathscr{X}$,

$$d(g \circ f)_{|x} = dg_{|f(x)} \circ df_{|x}$$

.

1.3 Diviseurs et Groupe de picard

Soit $\mathscr{Z}$ une variété lisse sur le corps k.

3. O_x étant l'ensemble des fonctions régulières en x et k_x le corps k vu comme $k[X]-$module via : $f.z := f(x)z$.

Définition 1.3.0.6 (***Diviseur de Weil, diviseur effectif***)
⊛ *Un* ***diviseur de Weil*** *D sur une variété* $\mathscr{Z}$ *est une somme formelle*

$$D = \sum_i \tau_i \mathscr{C}_i.$$

où les τ_i *sont des entiers presque tous nuls et les* $\mathscr{C}_i$ *sont des sous-variétés de* $\mathscr{Z}$ *de codimension* 1.

⊛ *On dit que* $D = \sum_i \tau_i \mathscr{C}_i$ *est* ***effectif*** *si* $\tau_i > 0 \quad \forall i$.

NB : L'ensemble des diviseurs de Weil sur $\mathscr{Z}$ est un groupe commutatif et est noté $Div(\mathscr{Z})$.

Définition 1.3.0.7 (***Support d'un diviseur***)
Le ***support d'un diviseur*** $D = \sum_i \tau_i \mathscr{C}_i$, *noté* ***supp D*** *est le sous-ensemble fermé de* $\mathscr{Z}$ *défini par :*

$$supp(\sum_i \tau_i \mathscr{C}_i) = \bigcup_{\tau_i \neq 0} \mathscr{C}_i.$$

Définition 1.3.0.8 (***Valuation discrète***)
Une valuation discrète est une application surjective $v : k^* \longrightarrow \mathbb{Z}$ *tel que* $v(x \cdot y) = v(x) + v(y)$ *et* $v(x+y) \geqslant \min(v(x), v(y))$.

Exemple 1.3.0.1 (*[7], page 17*)
Si on voit $k(t)$ *comme* $k(\mathbb{P}^1)$, *alors :*
– *Pour* $P \in \mathbb{A}^1(k) = k$, *la valuation en P est bien l'ordre d'annulation en P de la fraction rationnelle* f (*en particulier, si* f *est un polynôme,* $\upsilon_P(f)$ *est la multiplicité de* $(t-P)$ *dans la décomposition en facteurs irréductibles de* f *et si* $P = 0$, *c'est ce qu'on appelle souvent sans autre précision la valuation d'un polynôme*).
– *Pour* $P = \infty$, *la valuation en* ∞ *d'un polynôme est l'opposé de son degré et la valuation en* ∞ *d'une fraction rationnelle* f *est le degré de son dénominateur moins le degré de son numérateur.*

Définition 1.3.0.9 (***Diviseur Principal***)
Soit f *une fonction rationnelle. Le diviseur de* f *noté* $D(f)$ *ou* (f) *est défini comme suit :*

$$D(f) := \sum_{v_i \in \mathbb{Z}} v_i(f) \mathscr{C}_i.$$

Un tel diviseur est appelé ***diviseur principal****.*
L'ensemble des diviseurs principaux noté $Princ(\mathscr{Z})$ *est un sous-groupe de* $Div(\mathscr{Z})$.

Définition 1.3.0.10 (***Diviseurs linéairement équivalents***)
Deux diviseurs D, $D' \in Div(\mathscr{Z})$ *sont* ***linéairement équivalents****, et l'on note* $D \sim D'$, *si* $D - D'$ *est* ***principal****.*

Notation : L'ensemble des diviseurs effectifs équivalents à D est noté $|D|$.

Définition 1.3.0.11 (***Point base***)
Les ***points base*** *de* $|D|$ *sont les points dans l'intersection des supports de diviseurs dans* $|D|$ *. Si cette intersection est vide, on dit que* $|D|$ *est* ***sans point base****.*

Exemple 1.3.0.2 (*[11], page 4*)
Supposons que D et D' sont deux diviseurs effectifs linéairement équivalents avec des supports disjoints. Alors, par définition, il existe une fonction $f \in k(\mathscr{Z})$ tel que $(f) = D - D'$. Ainsi la fonction f définit une application rationnelle de $\mathscr{Z}$ vers $\mathbb{P}^1$, tel que $f^{-1}(0) = D$ et $f^{-1}(\infty) = D'$.

Définition 1.3.0.12 (***Groupe de Picard***)
*Le **groupe Picard** de $\mathscr{Z}$ noté $Pic(\mathscr{Z})$ est le groupe quotient :*

$$Pic\,\mathscr{Z} = \frac{Div(\mathscr{Z})}{Princ(\mathscr{Z})}.$$

Définition 1.3.0.13 (***Nombre d'intersections***)
Soient D et D' deux diviseurs effectifs sur une variété $\mathscr{X}$, de supports sans composante commune, et soient f et f' définissant des équations locales au voisinage d'un point $x \in \mathscr{X}$. Le nombre

$$\dim \mathscr{O}_x/(f,f')$$

*est appelé le nombre **local d'intersections** de D et D' au point x ; on le note $(D.D')_x$.*

Proposition 1.3.0.2 (*[7], page 9*)
Soient D , D', D'' trois diviseurs, avec D , D' et D , D'' sans composante commune. Alors

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

Démonstration :
Sans perte de généralité, on suppose que les trois diviseurs sont effectifs. Soient f, g des polynômes définissant des équations locales de D' et D. On sait que

$$\dim \mathscr{O}_{x,D}/(fg) = \dim \mathscr{O}_{x,D}/(f) + \dim \mathscr{O}_{x,D}/(g).$$

Or $\dim \mathscr{O}_{x,D}/(fg) = \dim \mathscr{O}_{x,D}/(f)(g) + \dim((g)/(fg))$, et la multiplication par g donne un isomorphisme (th. zéro isolés) $\mathscr{O}_{x,D}/(f) \cong (g)/(fg)$, d'où $\dim \mathscr{O}_{x,D}/(f) = \dim((g)/(fg))$; l'égalité souhaitée en découle.

Définition 1.3.0.14
Soit D un diviseur, on note :

$$\mathscr{L}(D) := \{f \in k^*(X);\ div(f) + D \geq 0\}.$$

NB :
$*$ Notons que $\mathscr{L}(D)$ est un k-**espace vectoriel**.
$*$ On a une bijection entre $\mathbb{P}(\mathscr{L}(D))$ et l'ensemble $|D|$, simplement en remarquant qu'un tel diviseur D' s'écrit $D' = D + (f)$ avec $f \in \mathscr{L}(D)$.

Définition 1.3.0.15 (***système linéaire complet et système linéaire***)
*On dit que $|D|$ est le **système linéaire complet** associé à D.*
*Un sous-espace linéaire de $|D|$ (correspondant à un sous-espace vectoriel de $\mathscr{L}(D)$) est simplement appelé un **système linéaire**.*

Définition 1.3.0.16 (***Dimension d'un diviseur***)
*La **dimension d'un diviseur** D est définie par :*

$$\dim(D) = \dim_k \mathscr{L}(D).$$

Proposition 1.3.0.3 (*[7], page 13*)
Si $D_1 \sim D_2$ alors $|D_1| = |D_2|$ et $\dim \mathscr{L}(D_1) = \dim \mathscr{L}(D_2)$.

Démonstration :
Il suffit d'écrire $D_1 = D_2 + (g)$ et de remarquer que $\mathscr{L}(D_1) \longrightarrow \mathscr{L}(D_2)$ est un isomorphisme.
Considérons l'application : $\mathbb{P}(\mathscr{L}(D)) \longrightarrow |D|$, $\overline{f} \longmapsto D + div(f)$, où $\overline{f}$ désigne la classe de f

modulo un élément de k^* ; on a déduit un isomorphisme $\mathbb{P}(\mathscr{L}(D)) \longrightarrow \mathbb{P}^{l(D)-1}$ avec $l(D) = \dim \mathscr{L}(D)$. Soit $f_1, \ldots, f_{l(D)}$ une base de $\mathscr{L}(D)$, on définit le morphisme

$$\varphi_{\mathscr{L}(D)} : \mathscr{X} \longrightarrow \mathbb{P}^{l(D)-1}, \quad z \longmapsto \left(f_1(z) : \cdots : f_{l(D)}(z)\right).$$

Il est bien défini modulo les automorphismes de $\mathbb{P}^{l(D)-1}$ et en dehors des pôles des fonctions f_i et de leurs zéros communs.

Définition 1.3.0.17 (***Diviseur ample***)
*Un diviseur D est dit **très ample** si le morphisme $\varphi_{\mathscr{L}(D)}$ défini ci-dessus est un plongement. Il est dit **ample** si l'un de ses multiples (positifs) est très ample.* [4]

4. On définit pareillement pour un faisceau ample.

CHAPITRE 2

VARIÉTÉS ABÉLIENNES

2.1 Groupes Algébriques

2.1.1 Définitions et Exemples de groupes algébriques

Définitions

Définition 2.1.1.1 (***groupes algébriques***)
*Un **groupe algébrique** sur le corps k est une **variété algébrique** $\mathscr{G}$ sur k, munie d'une **structure de groupe** d'élément neutre $e \in \mathscr{G}$ telles que les applications*

$$m : \mathscr{G} \times \mathscr{G} \longrightarrow \mathscr{G}, \quad (x,y) \longmapsto xy, \qquad \textit{et} \qquad i : \mathscr{G} \longrightarrow \mathscr{G}, \quad x \longmapsto x^{-1} \quad [1]$$

vérifient les axiomes de groupes suivants :

i) $m(e,x) = m(x,e) = x$,
ii) $m(i(x),x) = m(x,i(x)) = e$,
iii) $m(m(x,y),z) = m(x,m(y,z))$.

Définition 2.1.1.2 (***morphismes et isomorphismes de groupes algébriques***)
*Un **morphisme de groupes algébriques** $\Phi : \mathscr{G} \longrightarrow \mathscr{G}'$ est un morphisme de **variétés algébriques** qui est aussi un **morphisme de groupes**.*
*C'est un **isomorphisme** s'il existe un morphisme $\Psi : \mathscr{G}' \longrightarrow \mathscr{G}$ tel que $\Psi \circ \Phi = id_{\mathscr{G}}$ et $\Phi \circ \Psi = id_{\mathscr{G}'}$.*

1. $\mathscr{G}$ est muni d'une loi de composition interne. m est l'application pour la loi de la multiplication et i l'inverse pour

Exemples

Exemple 2.1.1.1 (***Groupe additif***)
Le groupe additif, que l'on note $(\mathbb{G}_a,+)$ *dont les application sont définies par :* $m(a,b) = a+b$ *et* $i(a) = -a$. *On vérifie que les deux applications vérifient les axiomes ci-dessus. On a :*

i) $m(0,b) = 0+b = b+0 = m(b,0) = b$.

ii) $m(i(a),a) = -a+a = 0 \quad et \quad m(a,i(a)) = a+(-a) = a-a = 0$.

iii) $m(m(a,b),c) = m(a,b)+c = a+b+c = a+(b+c) = a+m(b,c) = m(a,m(b,c))$.

Exemple 2.1.1.2 (***Groupe multiplicatif***)
Le groupe multiplicatif noté $(\mathbb{G}_m,\times)$ *dont les applications sont définies par :* $m(a,b) = a\times b$ *et* $i(a) = a^{-1}$. *A nouveau, on vérifie que les deux opérations vérifient les axiomes ci-dessus. On a :*

i) $m(1,b) = 1\times b = b\times 1 = m(b,1) = b$.

ii) $m(i(a),a) = a^{-1}\times a = 1$ *et* $m(a,i(a)) = a\times a^{-1} = a\times a^{-1} = 1$.

iii) $m(m(a,b),c) = m(a,b)\times c = a\times b\times c = a\times(b\times c) = a\times m(b,c) = m(a,m(b,c))$.

Exemple 2.1.1.3 (***Groupe matriciel d'ordre*** $n\times n$)
Le groupe matriciel noté $(\mathbb{G}L_n,\times)$ [2] *dont les applications sont définies par :* $m(A_{n,n},B_{n,n}) = A_{n,n}\times B_{n,n}$ *et* $i(A_{n,n}) = A_{n,n}^{-1}$. *A nouveau, on vérifie que les deux opérations vérifient les axiomes ci-dessus. On a :*

i) $m(Id, A_{n,n}) = Id\times A_{n,n} = A_{n,n}\times Id = m(A_{n,n}, Id) = A_{n,n}$.

ii) $m(i(A_{n,n}), A_{n,n}) = A_{n,n}^{-1}\times A_{n,n} = Id \quad et \quad m(A_{n,n}, i(A_{n,n})) = A_{n\times n}\times A_{n,n}^{-1} = A_{n,n}\times A_{n,n}^{-1} = Id$

iii) $m(m(A_{n,n}, B_{n,n}), C_{n,n}) = m(A_{n,n}, B_{n,n})\times C_{n,n} = A_{n,n}\times B_{n,n}\times C_{n,n} = A_{n,n}\times(B_{n,n}\times C_{n,n}) = A_{n,n}\times m(B_{n,n}, C_{n,n}) = m(A_{n,n}, m(B_{n,n}, C_{n,n}))$.

Propriété 2.1.1.1 (*[2], page 16*)
Soit $\mathcal{G}$ *un groupe algébrique sur le corps* k. *Considérons les morphismes de groupes algébriques ci-dessous :*

$$m : \mathcal{G}\times\mathcal{G} \longrightarrow \mathcal{G} \qquad i : \mathcal{G} \longrightarrow \mathcal{G} \qquad \varepsilon : \{e\} \longrightarrow \mathcal{G}$$

Alors les diagrammes suivants sont commutatifs :

– *Associativité :*
$$\begin{array}{ccc} \mathcal{G}\times\mathcal{G}\times\mathcal{G} & \xrightarrow{m\times id_{\mathcal{G}}} & \mathcal{G}\times\mathcal{G} \\ \downarrow{\scriptstyle id_{\mathcal{G}}\times m} & & \downarrow{\scriptstyle m} \\ \mathcal{G}\times\mathcal{G} & \xrightarrow{m} & \mathcal{G} \end{array}$$

– *élément neutre :*
$$\begin{array}{ccc} \{e\}\times G & \xrightarrow{\varepsilon\times id_G} & G\times G \\ & {\scriptstyle j_1}\searrow \quad \swarrow{\scriptstyle m} & \\ & G & \end{array} \qquad et \qquad \begin{array}{ccc} G\times\{e\} & \xrightarrow{id_G\times\varepsilon} & G\times G \\ & {\scriptstyle j_2}\searrow \quad \swarrow{\scriptstyle m} & \\ & G & \end{array}$$

– *Inversibilités des éléments :*
$$\begin{array}{ccc} G\times\{e\} & \xrightarrow{(i,id_G)} & G\times G \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle m} \\ \{e\} & \xrightarrow{\varepsilon} & G \end{array} \qquad et \qquad \begin{array}{ccc} \{e\}\times G & \xrightarrow{(id_G,i)} & G\times G \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle m} \\ \{e\} & \xrightarrow{\varepsilon} & G \end{array}$$

2. La loi $\times$ est le produit matriciel

2.1.2 Sous-groupes algébriques

Sous-groupes

Propriété 2.1.2.1 (*[2], page 16*)
Soient $\mathscr{G}$ un groupe algébrique et $\mathscr{H}$ une sous-variété de $\mathscr{G}$ qui est aussi un sous-groupe. Alors $\mathscr{H}$ est un groupe algébrique. On dira simplement que $\mathscr{H}$ est un sous-groupe de $\mathscr{G}$.

Démonstration :
Par hypothèse, $\mathscr{H}$ est une sous-variété de $\mathscr{G}$. La restriction $m_{\mathscr{H}}$ de m à $\mathscr{H}$ est un morphisme de $\mathscr{H}\times\mathscr{H}$ dans $\mathscr{H}$. De même, la restriction $i_{\mathscr{H}}$ de i à $\mathscr{H}$ est un morphisme $\mathscr{H}\longrightarrow\mathscr{H}$. Ceci montre que $\mathscr{H}$ est un groupe algébrique, et l'inclusion $\mathscr{H}\subseteq\mathscr{G}$ est un morphisme de groupes algébriques.

Propriété 2.1.2.2 (*[2], page 17*)
Si $\phi:\mathscr{G}'\longrightarrow\mathscr{G}$ est un morphisme de groupes algébriques, alors $\phi(\mathscr{G}')$ est fermé.

Démonstration : voir ([2], page 17)

Théorème 2.1.2.1 (*[2], page 17*)
Soit $\phi:\mathscr{G}'\longrightarrow\mathscr{G}$ un homomorphisme de groupes algébriques. Alors :

1) *le noyau $\mathscr{H}=\ker\phi$ est un sous-groupe algébrique de $\mathscr{G}'$.*
2) *L'image $\mathscr{I}=Im\phi$ est un sous-groupe algébrique de $\mathscr{G}$.*

Démonstration :

1) Puisque $\ker\phi$ est un sous-ensemble algébrique de $\mathscr{G}'$, par le résultat de la théorie des groupes et de la Propriétés 2.1.2.1, on déduit que $\ker\phi$ est sous$-$groupe algébrique.
2) En utilisant le résultat de la Propriétés 2.1.2.2, puisque $\mathscr{H}=\phi^{-1}(0)$ est fermé de $\mathscr{G}'$ (car ϕ est un morphisme). Donc $\mathscr{H}$ est sous groupe algébriques de $\mathscr{G}'$.

2.2 Hauteur

Dans cette partie, K est considéré comme un corps de nombres.

Définition 2.2.0.1 (***hauteur d'un point***)
*Soient $\alpha\in\overline{\mathbb{Q}}$ un nombre algébrique et K une extension finie de $\mathbb{Q}$ contenant α. La **hauteur** de α, notée $H(\alpha)$ est définie par :*

$$H(\alpha):=\prod_{v\in M_K}\max\{1,|\alpha|_v\}^{d_v/d}.$$

Où $d_v:=[K_v:\mathbb{Q}_v]$ et $d:=[K:\mathbb{Q}]$. $[K_v:\mathbb{Q}_v]:=\begin{cases}1 & \text{si } |\cdot|_v \text{ est réelle ,}\\ 2 & \text{si } |\cdot|_v \text{ est complexe}\end{cases}$. et M_K est l'ensembles des classes d'équivalences de valeurs absolues tel que pour tout $x\in K^*$ on a : $\prod_{v\in M_K}|x|_v^{d_v}=1$.

Définition 2.2.0.2 (***Hauteur logarithmique d'un point***)
La ***hauteur logarithmique*** *du point α est définie par :*

$$h(\alpha) := logH(\alpha) = \sum_{v\in M_K} \frac{d_v}{d} log^+ |\alpha|_v,$$

où $\log^+ |\alpha| := \log\ \max\{1, |\alpha|\}$.

Exemple 2.2.0.1 (*[4], page 3*)
Soit un nombre rationnel $\frac{m}{n}$, avec m et n premiers entre eux. Alors :

$$H(\frac{m}{n}) = \prod_{v\in M_{\mathbb{Q}}} \max\{1, \left|\frac{m}{n}\right|_v\} = \max\{|m|_\infty, |n|_\infty\}.$$

En effet, pour p premier on a :

$$max\{1, \left|\frac{m}{n}\right|_p\} = \begin{cases} p^m, & p^m|n. \\ 1, & sinon \end{cases}$$

Donc on constate que

$$\prod_{v\in M_{\mathbb{Q}}} max\{1, \left|\frac{m}{n}\right|_v\} = |n|_\infty.$$

Pour $|\cdot|_\infty$ on a :

$$max\{1, \left|\frac{m}{n}\right|_\infty\} = \begin{cases} |\frac{m}{n}|_\infty, & |m|_\infty > |n|_\infty \\ 1, & si\ non. \end{cases}$$

Ainsi $H(\frac{m}{n}) = \max\{|m|_\infty, |n|_\infty\}$.

Définition 2.2.0.3 (***Hauteur d'un polynôme***)
Considérons un polynôme f défini par :

$$f(X_1,\ldots,X_n) := \sum_i a_i X^i \in K[X_1,\ldots,X_n],$$

on définit sa ***hauteur*** *par :*

$$h(f) := \sum_{v\in M_k} \frac{d_v}{d} log|f|_v,$$

où $|f|_v := \max_i |a_i|_v$.

Exemple 2.2.0.2 (*[4], page 4*)
$h(X+1) = 0\,, \quad h((X+1)^2) = \log\ 2.$

Définition 2.2.0.4 (***Hauteur d'un point projectif***)
Pour un point projectif $P = (x_0(P) : \ldots : x_n(P)) \in \mathbb{P}^n(K)$, sa hauteur est donné par :

$$h(P) := \frac{1}{d} \sum_{v\in M_k} d_v \log \max_{0\le i\le n} |x_i(P)|_v.$$

On définit le plongement de **Segré** par :

$$S_{n,m} : \mathbb{P}^n(K) \times \mathbb{P}^m(K) \longrightarrow \mathbb{P}^N(K) \qquad (\text{ avec } N = (n+1)(m+1)-1).$$
$$(x,y) \longmapsto (x_0y_0 : x_0y_1 : \ldots : x_iy_j : \ldots : x_ny_m)$$

NB : Dans suite de ce paragraphe et celui sur la hauteur dans une variété abélienne (**paragraphe 2.8**), on notera simplement $\mathbb{P}^n$ au lieu de $\mathbb{P}^n(K)$.

Proposition 2.2.0.1 (*[4], page 8*)
Considérons les hyperplans suivants : $H_N = \{(z_0,\ldots,z_N) \in \mathbb{P}^N \mid z_0 = 0\}$, $H_n = \{(x_0,\ldots,x_n) \in \mathbb{P}^n \mid x_0 = 0\}$ *et* $H_m = \{(y_0,\ldots,y_m) \in \mathbb{P}^N \mid y_0 = 0\}$, *on a :*

- $h(S_{n,m}(x,y)) = h(x) + h(y)$,
- *On a :* $S^*_{n,m}H_N = \{(x,y) \in \mathbb{P}^n \times \mathbb{P}^m \mid x_0y_0 = 0\} = H_n \times \mathbb{P}^m + H_m \times \mathbb{P}^n$,
- *Soit* $\phi_d : \mathbb{P}^n \longrightarrow \mathbb{P}^m$ *un d-uplét, on a :* $h(\phi_d(x) = dh(x) \qquad \forall x \in \mathbb{P}^N$.

Démonstration :
• On a :

$$\begin{aligned} h(S_{n,m}(x,y)) &= \sum_{v \in M_k} \frac{d_v}{d} \log \max_{0 \le i \le n} |x_i(P)|_v \\ &= \sum_{v \in M_k} \frac{d_v}{d} \log \max_{0 \le i \le n} |x_i(P)|_v + \sum_{v \in M_k} \frac{d_v}{d} \log \max_{0 \le j \le m} |x_i(P)|_v \\ &= h(x) + h(y). \end{aligned}$$

• Soient $(z_0,\ldots,z_N)$ des coordonnées homogènes de $\mathbb{P}^N$ et H_N, H_n et H_m définis comme ci-dessus. Alors :

$$S^*_{n,m}H_N = S^*_{n,m}\{z \in \mathbb{P}^N \mid z_0 = 0\} = \{(x,y) \in \mathbb{P}^n \times \mathbb{P}^m \mid x_0y_0 = 0\} = H_n \times \mathbb{P}^m + H_m \times \mathbb{P}^n.$$

• Considérons $\phi(x) = (F_0(x),\ldots,F_N(x))$, où les $F_i(x)$ sont des polynômes de degré d à $n+1$ variables. Comme $|F_i(x)|_v \le max_i|x_i|_v^d$, et comme les monômes $x_0^d,\ldots,x_n^d$ sont simples, on déduit que :

$$\max_{0 \le j \le N} |F_j(x)|_v = \max_{0 \le j \le N} |x_j^d|_v.$$

En considérant n_v/d, par la multiplication de $v \in M_k$ et en appliquant le logarithme, on trouve le résultat.

Définition 2.2.0.5 (***Hauteur dans un espace projectif***)
Pour un morphisme de variétés projectives $\phi : \mathscr{V} \longrightarrow \mathbb{P}^n$, *on définit sa hauteur par :*

$$h_\phi := h(\phi(P)) \qquad pourP \in \mathscr{V}(\overline{\mathbb{Q}}).$$

Théorème 2.2.0.2 (***hauteur de Weil***) (*[4], page 15*)
Soient $\mathscr{V}$ *une variété projective définie sur le corps de nombres K et D un diviseur sur* $\mathscr{V}$ *et l'application* $h_{\mathscr{V},D} : \mathscr{V} \longrightarrow \mathbb{R}$. *Il existe une application*

$$h_{\mathscr{V}} : Div(\mathscr{V}) \longrightarrow \{h_{\mathscr{V},D}\}$$

tel que :

– **NORMALISATION :** *pour un hyperplan $H \subset \mathbb{P}^n$de codimension 1, on a :*

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1); \quad \forall P \in \mathbb{P}^n(\overline{k}).$$

– **FONCTORIALITÉ :** *Pour un morphisme de variétés $\phi : \mathscr{V} \longrightarrow \mathscr{W}$ induisant une application*
$\phi^* : Div(\mathscr{W}) \longrightarrow Div(\mathscr{V})$, et un diviseur $D \in Div(\mathscr{W})$, on a :

$$h_{\mathscr{V},\phi^* D}(P) = h_{\mathscr{V},D}(\phi(P)) + O(1), \quad \forall P \in \mathbb{P}^n(\overline{k}).$$

Pour D,$D' \in Div(\mathscr{V})$ on a :

$$h_{\mathscr{V},D+D'}(P) = h_{\mathscr{V},D}(P) + h_{\mathscr{V},D'}(P), \quad \forall P \in \mathbb{P}^n(\overline{k}).$$

– **ÉQUIVALENCE LINÉAIRE :** *Si D, $D' \in Div(\mathscr{V})$ sont des diviseurs linéairement équivalents, alors*

$$h_{\mathscr{V},D} = h_{\mathscr{V},D'} + O(1).$$

– **POSITIVITÉ :** *Si D est un diviseur sur $\mathscr{V}$, considérons B un sous-ensemble des points associé au système linéaire $|D|$. Alors :*

$$h_{\mathscr{V},D}(P) \geq O(1) \quad P \in (\mathscr{V} \backslash B)(K).$$

– *Propriété de Northcott : Si $D \in Div(\mathscr{V})$ est un diviseur ample, alors pour toute extension fini K' de K et une constante réel M, l'ensemble*

$$\{P \in \mathscr{V}(K') \mid h_{\mathscr{V},D}(P) \leq M\}$$

est fini.

$O(1)$ étant une constante ne dépendant que de chacune des données suivantes : les variétés, diviseurs, morphismes ; mais pas du point P.

Démonstration : (Voir [4], Page 15).

2.3 Applications rationnelles et Diviseurs dans un produit de variétés abéliennes

2.3.1 Applications rationnelles d'un produit de variétés abéliennes

Définition 2.3.1.1 (***Variété abélienne, morphisme de variétés abéliennes***)
⊙ *On appelle **variété abélienne** une variété projective vérifiant une structure de groupe algébrique.*
⊙ *Un **morphisme de variétés abéliennes** est un morphisme de groupes algébriques, qui est aussi un morphisme de variétés algébriques.*

Théorème 2.3.1.1 (*[3], page 7*)
Soient $\mathscr{V}$ une variété algébrique complète, $\mathscr{U}$ et $\mathscr{W}$ deux variétés algébriques et $\phi : \mathscr{U} \times \mathscr{V} \to \mathscr{W}$ un morphisme. S'il existe un point $u_0 \in \mathscr{U}$ tel que $\phi(u_0,v)$ ne dépende pas de $v \in \mathscr{V}$, alors on a pour tout $u \in \mathscr{U}$ et $v \in \mathscr{V}$:

$$\phi(u,v) = \psi(u)$$

où $\psi : \mathscr{U} \longrightarrow \mathscr{W}$ est un morphisme.

Démonstration :
En considérant le Théorème 1.1.5.2, on a pour $v_1,v_2 \in \mathscr{V}$ et $u \in \mathscr{U}$, l'ensemble $\{v_1,v_2\}$ est tels que $\phi(u,v_1) = \phi(u,v_2)$ est un sous-ensemble fermé de $\mathscr{U}$. L'intersection $E = \bigcap_{v_1,v_2}\{v_1,v_2\}$ est donc un sous-ensemble fermé de $\mathscr{U}$. Montrons que c'est aussi ouvert de $\mathscr{U}$. En effet, soit u_1 un point de $\mathscr{U}$, alors le point $w_1 = \phi(u_1,v)$ de $\mathscr{W}$ ne dépend pas de v. Soient S un ouvert affine de $\mathscr{W}$ contenant w_1 et $F = \mathscr{W} - S$ son complémentaire. Comme ϕ est un morphisme alors $\phi^{-1}(F)$ est un fermé de $\mathscr{U} \times \mathscr{W}$, et comme $\mathscr{V}$ est complète donc l'ensemble $G = pr_1(\phi^{-1}(F))$ est un fermé de $\mathscr{U} \times \mathscr{V}$, on a donc $u_1 \in \mathscr{U} - G$. Pour $u \in \mathscr{U} - G$, l'application $\phi_u : \mathscr{V} \to \mathscr{W}$ obtenue en posant $\phi_u(y) = \phi(u,v)$ est un morphisme dont l'image est dans S. Cette image est une sous-variété complète de S,

ce qui implique que c'est une sous-variété affine complète, donc elle est réduite en un point, d'où $\mathscr{U} - G \subset E$, d'où E est un voisinage de u_1. Ainsi on montre que E est ouvert de $\mathscr{U}$. E étant non vide (car $u_0 \in E$) et est à la fois ouvert et fermé dans $\mathscr{U}$, donc E coïncide avec $\mathscr{U}$. Il existe donc une application $\psi : \mathscr{U} \to \mathscr{W}$ telle que $\phi(u,v) = \psi(u)$. En prenant $v = v_0$ fixé, on voit que ϕ est un morphisme.

Théorème 2.3.1.2 (***Chevalley***) (*[3], page 9*)
La loi de groupe dans une variété abélienne $\mathscr{A}$ est commutative.

Démonstration :
En effet, considérons le morphisme $\Phi : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}$ obtenu en posant $\Phi(x,y) = x.y.x^{-1}$. Pour tout $x \in A$, on a $\Phi(x,e) = e$. D'après le Théorème 2.3.1.1, il existe donc un morphisme $\Psi : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}$, tel qu'on ait identiquement $\phi(x, y) = \Psi(y)$. En faisant $x = e$, on obtient $\phi(e,y) = y = \Psi(y)$ quel soit y, d'où $x.y.x^{-1} = y$.

Proposition 2.3.1.1 (*[3], page 14*)
Soient $\mathscr{A}$ et $\mathscr{B}$ deux variétés abéliennes et $\phi : \mathscr{B} \longrightarrow \mathscr{A}$ une application rationnelle. Alors ϕ est la composée d'un morphisme $\phi_0 : \mathscr{B} \longrightarrow \mathscr{A}$ et d'une translation sur $\mathscr{A}$ ie il existe $a \in \mathscr{A}$ tel que $\phi(b) = \phi_0(b) + a$.

Démonstration :
Comme $\mathscr{B}$ est une variété abélienne donc ϕ est un morphisme. Notons e l'élément neutre de $\mathscr{B}$ et posons $\phi_0(b) = \phi(b) - \phi(e)$. En appliquant (le théorème 8, voir [3], page 11) $\psi_0 : \mathscr{B} \times \mathscr{B} \longrightarrow \mathscr{A}$ défini par $\psi_0(b,b') = \phi_0(b,b')$. Il existe des morphismes $\alpha : \mathscr{B} \longrightarrow \mathscr{A}$ et $\beta : \mathscr{B} \longrightarrow \mathscr{A}$ tels qu'on ait $\phi_0(b,b') = \alpha(b) + \beta(b')$. En posant $b' = e$, puis $b = e$, on obtient les relations :

$$\phi_0(b) = \alpha(b) + \beta(e)$$
$$\phi_0(b') = \alpha(e) + \beta(b')$$

En faisant $b = b' = e$,
on obtient la relation $0 = \alpha(e) = \beta(e)$
On a donc $\phi_0(b,b') = \phi_0(b) + \phi_0(b')$.
Ce qui montre donc que ϕ_0 est un morphisme.

2.3.2 Diviseurs dans une variété abélienne

Posons $I = \{1,2,3\}$, on définit une application s_I par :

$$s_I : \mathscr{A} \times \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A} \qquad s_I(x_1,x_2,x_3) = \sum_{i \in J \subset I} x_i.$$

Par exemple $s_{2,3}(x_1,x_2,x_3) = x_2 + x_3$ et $s_1(x_1,x_2,x_3) = x_1$.

Théorème 2.3.2.1 (***théorème du cube***) (*[10], page 120*)
Soit $\mathscr{A}$ une variété abélienne. Pour tout diviseur $D \in Div(\mathscr{A})$, on a la relation d'équivalence dans le produit $\mathscr{A} \times \mathscr{A} \times \mathscr{A}$ suivante :

$$s_{123}^*D - s_{12}^*D - s_{13}^*D - s_{23}^*D + s_1^*D + s_2^*D + s_3^*D \sim 0.$$

Démonstration : (voir [10], page 120)

Corollaire 2.3.2.1 (*[10], page 122*)
Soient $\mathscr{A}$ une variété abélienne , $\mathscr{V}$ une variété abstraite et f, g, h trois morphismes de $\mathscr{V}$ vers $\mathscr{A}$. Alors pour tout diviseur $D \in Div(\mathscr{A})$,

$$(f+g+h)^*D - (f+g)^*D - (f+h)^*D - (h+g)^*D + f^*D + g^*D + h^*D \sim 0.$$

Démonstration :
Soit $\Psi(D)$ le diviseur décrit par le Théorème 2.3.2.1. Alors le diviseur est la restriction du diviseur $\Psi(D)$ par l'application $(f, g, h) : \mathscr{V} \times \mathscr{V} \times \mathscr{V} \longrightarrow \mathscr{A} \times \mathscr{A} \times \mathscr{A}$. Mais $\Psi(D) \sim 0$ en appliquant le théorème du cube on obtient le résultat.

Définition 2.3.2.1 (***Diviseur symétrique, diviseur antisymétrique***)
*Un diviseur D tel que $[-1]^*D \sim D$ est appelé **diviseur symétrique**.*
*Un diviseur D tel que $[-1]^*D \sim -D$ est appelé **diviseur antisymétrique**.*

Corollaire 2.3.2.2 (***Formule de Mumford***) (*[10], page 122*)
Soient D un diviseur dans une variété abélienne $\mathscr{A}$ et $[n] : \mathscr{A} \longrightarrow \mathscr{A}$ la multiplication par n. Alors

$$[n]^*(D) \sim \left(\frac{n^2+n}{2}\right) D + \left(\frac{n^2-n}{2}\right) [-1]^*(D).$$

En particulier,

$$[n]^*(D) \sim \begin{cases} n^2 D & \text{si } D \text{ et symétrique ;} \\ nD & \text{si } D \text{ et antisymétrique.} \end{cases}$$

Démonstration :
La formule est trivialement vraie pour $n = -1$, $n = 0$ et $n = 1$. En appliquant le Corollaire 2.3.2.1 en posant $f = [n]$, $g = [1]$ et $h = [-1]$, on obtient

$$[n+1]^*D + [n-1]^*D - 2[n]^*D \sim D + [-1]^*D.$$

En remplaçant de part et d'autre $n = 0$ on trouve le résultat pour 0.
Le résultat final s'obtient en utilisant le Lemme A. 7.2.6 ([10], page 123).

Lemme 2.3.2.1 (***Principe de See-Saw***) (*[10], page 122*)
Soient $\mathscr{X}$ et $\mathscr{Y}$ deux variétés algébriques, $c \in Pic(\mathscr{X} \times \mathscr{Y})$ et des applications définies par : $i_x(y) = (x,y)$ et $p_1(x,y) = x$.

(*i*) *Si $i_x^*(c) = 0$ dans $Pic(Y)$ pour tout $x \in \mathscr{X}$, alors il existe une classe $c' \in Pic(\mathscr{X})$ telle que $c = p_1^*(c')$.*

(*ii*) *Si de plus la restriction de c à $Pic(\mathscr{X} \times \{y_0\})$ est triviale, alors $c = 0$ dans $Pic(\mathscr{X} \times \mathscr{Y})$.*

Démonstration : Voir ([10], page 123) preuve de **Sketch**.

Théorème 2.3.2.2 (***théorème du carré***) (*[10], page 123*)
Soit $\mathscr{A}$ une variété abélienne et , notons $t_a : \mathscr{A} \longrightarrow \mathscr{A}$ la translation par $a \in \mathscr{A}$, définie par $t_a(x) = x + a$. Alors

$$t^*_{a+b}(D) + D \sim t^*_a(D) + t^*_b(D) \qquad \text{pour tout } D \in Div(\mathscr{A}) \text{ et } b \in \mathscr{A}$$

En d'autres termes, pour toute classe de diviseur $c \in Pic(\mathscr{A})$, l'application

$$\phi_c : \mathscr{A} \longrightarrow Pic(\mathscr{A}), \qquad a \longmapsto t^*_a(c) - c$$

est un morphisme de groupes.

Démonstration : (voir ([10], page 123))

2.4 Dual d'une variété abélienne

Définition 2.4.0.2 (***Classe de diviseur invariant par translation***)
*Soit $\mathscr{A}$ une variété abélienne. On définit le groupe des **classes de diviseurs invariants par translation** noté $Pic^0(\mathscr{A})$ par :*

$$Pic^0(\mathscr{A}) := \{ \quad c \in Pic(\mathscr{A}) \quad | \quad t^*_a c - c = 0 \quad \forall a \in \mathscr{A} \quad \}.$$

*Le quotient noté $NS(\mathscr{A}) := Pic(\mathscr{A})/Pic^0(\mathscr{A})$ est appelé le groupe de **Néron-Severi**.*

Remarque 2.4.0.1 (*[10], page 125*)
Le groupe $Pic^0(\mathscr{A})$ est un sous groupe de $Pic(\mathscr{A})$.

Théorème 2.4.0.3 (*[10], page 127*)
Soient $\mathscr{A}$ une variété abélienne, n un entier naturel non nul, c un élément de $Pic(\mathscr{A})$ et ϕ un morphisme de groupes définie par :

$$\phi_c : \mathscr{A} \longrightarrow Pic(\mathscr{A}), \qquad a \longmapsto t^*_a c - c,$$

on a :

1) *l'image de ϕ_c est dense dans $Pic^0(\mathscr{A})$.*
2) *Si $nc \in Pic^0(\mathscr{A})$ pour un entier $n \neq 0$, alors $c \in Pic^0(\mathscr{A})$.*
3) *Si la classe c est ample, alors $\phi_c : \mathscr{A} \longrightarrow Pic^0(\mathscr{A})$ est surjective et de noyau fini.*

Démonstration :

1) En appliquant le théorème du carré, on obtient :

$$t^*_b(\phi_c(a)) = t^*_b(t^*_a c - c) = t^*_{a+b} c - t^*_b c = t^*_a c - c$$

.

2) De par la définition de ϕ_c, on a $\phi_{c+c'} = \phi_c + \phi_{c'}$, en utilisant (1) et la définition de $Pic^0(\mathscr{A})$, on définit une suite exacte

$$0 \longrightarrow Pic^0(\mathscr{A}) \longrightarrow Pic(\mathscr{A}) \xrightarrow[c \longmapsto \phi_c]{} Hom(\mathscr{A}, Pic^0(\mathscr{A})).$$

Maintenant supposons que $nc \in Pic^0(\mathscr{A})$. Alors on a $\forall a \in \mathscr{A}$,

$$0 = \phi_{nc}(a) = (n\phi_c)(a) = \phi_c([n]a).$$

Mais puisque $[n](\mathscr{A}) = \mathscr{A}$ (ie $\mathscr{A}$ est n-divisible), donc ϕ_c est une application nulle. Ainsi $c \in Pic^0(\mathscr{A})$.

3) Voir Mumford [ii, II.8 théorème 1], page 75.

Proposition 2.4.0.1 (*[10], page 128*)
Soit $c \in Pic(\mathscr{A})$. Les assertions suivantes sont équivalentes :

i) $[-1]^*c = -c$;

ii) $c \in Pic^0(\mathscr{A})$;

iii) $s_{12}^*c - p_1^*c - p_2^*c = 0$, *où* s_{12}, p_2, $p_1 : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}$ *sont des applications telles que* $s_{12}(x,y) = x+y$, $p_1(x,y) = x$ *et* $p_2(x,y) = y$.

Démonstration :
Notons $\Gamma_c = s_{12}^*c - p_1^*c - p_2^*c$. Aussi, pour tout $a \in \mathscr{A}$, notons $i_a : \mathscr{A} \to \mathscr{A} \times \mathscr{A}$ définie par $i_a(x) = (a,x)$. On a $s_{12} \circ i_a(x) = t_a(x)$, $p_1 \circ i_a(x) = a$ et $p_2 \circ i_a(x) = x$. En utilisant ces formules, on obtient la relation suivante

$$i_a^*(\Gamma_c) = i_a^*(s_{12}^*c - p_1^*c - p_2^*c) = t_a^*c - c.$$

iii)⇒ ii). Puisque $\Gamma_c = 0$, donc $t_a^*c - c = i_a^*(\Gamma_c) = 0$. D'où $c \in Pic^0(\mathscr{A})$.
i)⇒ ii). Puisque $t_a^*c - c = 0$ pour tout $a \in \mathscr{A}$, donc $i_a^*(\Gamma_c) = 0$. En outre, Γ_c est clairement triviale si on se restreint à $\mathscr{A} \times \{0\}$, donc en appliquant **le principe de See-saw** on obtient $\Gamma_c = 0$.
ii)⇒ i). Fixons un diviseur symétrique $c_0 \in Pic(\mathscr{A})$. Le théorème 2.4.0.3 permet d'affirmer qu'il existe une élément $a \in \mathscr{A}$ tel que $c = t_a^*c_0 - c_0$ et en appliquant le théorème du carré, on obtient :

$$[-1]^*c = [-1]^*t_a^*c_0 - [-1]^*c_0 = t_{-a}^*c_0 + c_0 = -c$$

i)⇒ ii) Pour une classe arbitraire $c \in Pic(\mathscr{A})$, on peut affirmer que $c - [-1]^*c$ est dans $Pic^0(\mathscr{A})$. En effet :

$$\begin{aligned}
t_a^*(c - [-1]^*c) - (c - [-1]^*c) &= t_a^*c - [-1]^*t_{-a}^*c - c + [-1]^*c && car\ [-1] \circ t_a = t_{-a} \circ [-1] \\
&= (t_a^*c - c) - [-1]^*(t_{-a}^*c - c) \\
&= (t_a^*c - c) - [-1]^*(c - t_a^*c) && \text{par le théorème du carré} \\
&= c' + [-1]^*c' && o\ c' = t_a^*c - c \text{ et note que } c' \in Pic^0(\mathscr{A}) \\
&= 0 && d'o\ ii) \Rightarrow i)
\end{aligned}$$

Maintenant supposons que $[-1]^*c = -c$. Puisque nous avons prouvé que $2c = c - [-1]^*c \in Pic^0(\mathscr{A})$; il en résulte de l'assertion **(2) du théorème 2.4.0.3** que $c \in Pic^0(\mathscr{A})$, ce qui met fin à la démonstration.

Définition 2.4.0.3 (***Dual d'une variété abélienne***)
Soient $\hat{\mathscr{A}}$ et $\mathscr{A}$ des variétés abéliennes et $i_{\hat{a}} : \mathscr{A} \longrightarrow \mathscr{A} \times \hat{\mathscr{A}}$ définie par $i_{\hat{a}}(a) = (a,\hat{a})$ et $i_a : \hat{\mathscr{A}} \longrightarrow \mathscr{A} \times \hat{\mathscr{A}}$ définie par $i_a(\hat{a}) = (a,\hat{a})$ des applications.
*La variété abélienne $\hat{\mathscr{A}}$ est appelée le **dual** de $\mathscr{A}$; s'il existe une classe de diviseurs $\mathscr{P}$ dans $\mathscr{A} \times \hat{\mathscr{A}}$ telles que les applications*

$$\hat{\mathscr{A}} \longrightarrow Pic^0(\mathscr{A}), \qquad \hat{a} \longmapsto i_{\hat{a}}^*(\mathscr{P}),$$

et

$$\mathscr{A} \longrightarrow Pic^0(\hat{\mathscr{A}}), \qquad \hat{a} \longmapsto i_a^*(\mathscr{P}),$$

soient en bijection.

La classe de diviseurs $\mathscr{P}$ est appelée **classe de diviseurs de Poincaré**.

Définition 2.4.0.4 (***morphisme dual de variétés abéliennes***)
*L'application $\phi : \hat{\mathscr{A}} \longrightarrow \hat{\mathscr{A}}$ entre variétés abéliennes est appelée le **morphisme dual**.*

Théorème 2.4.0.4 (*[10], page 129*)
Le dual d'une variété abélienne existe, ainsi que sa classe de diviseurs de Poincaré $\mathscr{P}$ a un unique isomorphisme prés.

Démonstration : (Voir [10], page 129),

Théorème 2.4.0.5 (*[10], page 130*)
Supposons qu'il existe une classe de diviseur $c \in Pic(\mathscr{A})$ tel que $K(c) = 0$, où $K(c) = \{a \in \mathscr{A} \mid t_a^* c = c\}$, alors $\mathscr{A}$ est son propre dual et

$$s_{12}^* c - p_1^* c - p_2^* c \in Pic(\mathscr{A} \times \mathscr{A})$$

est une classe de diviseurs de Poincaré.

Démonstration :
Posons $\mathscr{P} = s_{12}^* c - p_1^* c - p_2^* c$, et pour tout $y \in \mathscr{A}$ posons $i_y : \mathscr{A} \longrightarrow \mathscr{A} \times \mathscr{A}$ définie par $i_y(x) = (x,y)$. Le diviseur $\mathscr{P}$ est clairement symétrique, donc il suffit de montrer que l'application

$$\mathscr{A} \longrightarrow Pic^0(\mathscr{A}), \qquad y \longmapsto i_y^* \mathscr{P},$$

est un isomorphisme. Notons que

$$s_{12} \circ i_y(x) = x + y = t_y(x), \qquad p_1 \circ i_y(x) = x \qquad et \qquad p_2 \circ i_y(x) = y.$$

En utilisant les expressions ci-dessus, on obtient :

$$i_y^* \mathscr{P} = i_y^* \circ s_{12}^* c - i_y^* \circ p_1^* c - i_y^* \circ p_2^* c = t_y^* c - c = \phi_c(y).$$

En d'autres termes, l'application $y \longmapsto i_y^* \mathscr{P}$ est égale à ϕ_c. Notre supposition que $K(c) = 0$ entraîne que ϕ_c est un isomorphisme, donc $\mathscr{P}$ est un diviseurs de Poincaré.

2.5 Isogénies

Considérons $\alpha : \mathscr{A} \longrightarrow \mathscr{B}$ un morphisme de variétés abéliennes.

2.5.1 Définitions et propriétés élémentaires

Définition 2.5.1.1 (***Isogénies et Degré d'une isogénie***)
⊙ *Un morphisme de variétés abéliennes α est une* ***isogénie****, s'il est surjectif et de noyau fini.*
⊙ *Le* ***degré d'une isogénie*** $\alpha : \mathscr{A} \longrightarrow \mathscr{B}$ *sur k est le cardinal de son noyau. Il est aussi égal au degré de son extension de corps $[k(\mathscr{A}) : k(\mathscr{B})]$.* [3]

Théorème 2.5.1.1 (*[8], page 30*)
Soit un homomorphisme $\phi : \mathscr{A} \longrightarrow \mathscr{B}$ de variétés abéliennes, les assertions suivantes sont équivalentes :

1) ϕ *est une isogénie ;*

2) $\dim \mathscr{A} = \dim \mathscr{B}$ *et* ϕ *est surjective ;*

3) $\dim \mathscr{A} = \dim \mathscr{B}$ *et* $\ker(\phi)$ *est fini ;*

Démonstration :
On utilise le théorème sur la dimension des fibrés pour les 3 premières assertions :
– $1) \Rightarrow 2)$. ϕ est surjectif et $\dim \mathscr{A} - \dim \mathscr{B} = \dim \ker(\phi) = 0$.
– $2) \Rightarrow 3)$. $\dim \mathscr{A} = \dim \mathscr{B}$ et ϕ surjective, on en déduit que $\ker(\phi)$ est de dimension 0, donc ϕ est de noyau fini.
– $3) \Rightarrow 1)$. Puisque l'image d'une variété algébrique irréductible par une application continue est irréductible, donc $\phi(\mathscr{A})$ est irréductible ; or $\dim \phi(\mathscr{A}) = \dim \mathscr{A} = \dim \mathscr{B}$, donc $\phi(\mathscr{A}) = \mathscr{B}$.

Lemme 2.5.1.1 (*[6], page 73*)
Soient $\mathscr{A}$, $\mathscr{B}$ et $\mathscr{C}$ des variétés abéliennes et $f : \mathscr{A} \longrightarrow \mathscr{B}$ et $h : \mathscr{C} \longrightarrow \mathscr{B}$ des isogénies de variétés abéliennes sur k. Si $g_1 : \mathscr{B} \longrightarrow \mathscr{C}$ et $g_2 : \mathscr{B} \longrightarrow \mathscr{C}$ sont des morphismes tels que $h \circ g_1 \circ f = h \circ g_2 \circ f$, alors $g_1 = g_2$.

Démonstration :
Sans perte de généralité, posons $k = \overline{k}$. Supposons que $h \circ g_1 \circ f = h \circ g_2 \circ f$. Puisque f un morphisme, d'après le Théorème 2.5.1.1, 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 $\mathscr{B}$ dans le groupe fini $\ker(h)$. Comme $\mathscr{B}$ est connexe et réduit, $g_1 - g_2$ se factorise à travers $\ker(h)^0_{red}$ qui est trivial.

2.5.2 Application de l'isogénie

On définit la multiplication dans $\mathscr{A}$ par $n : [n]_{\mathscr{A}} : \mathscr{A} \longrightarrow \mathscr{A}$ pour un entier $n \neq 0$; on note $\mathscr{A}[n] := \ker([n]_{\mathscr{A}}) \subset \mathscr{A}$.

Proposition 2.5.2.1 (*[6], page 74*)
Soient $\mathscr{A}$ et $\mathscr{B}$ des variétés abéliennes. Si $f : \mathscr{A} \longrightarrow \mathscr{B}$ une isogénie de degré d, alors il existe une isogénie $g : \mathscr{B} \longrightarrow \mathscr{A}$ tels que $g \circ f = [d]_{\mathscr{A}}$ et $f \circ g = [d]_{\mathscr{B}}$.

3. notons que nous avons un homomorphisme $k(\mathscr{B}) \longrightarrow k(\mathscr{A})$ qui est une isogénie qui est surjective

Démonstration :
Si $\deg(f) = d$, alors $\ker(f)$ est un groupe fini de rang d, donc est infini par la multiplication par d. Il s'en suit que $[d]_{\mathscr{A}}$ se factorise comme suit :

$$[d]_{\mathscr{A}} = (\mathscr{A} \xrightarrow{f} \mathscr{B} \xrightarrow{g} \mathscr{A})$$

pour une isogénie $g : \mathscr{B} \longrightarrow \mathscr{A}$.
Alors $g \circ [d]_{\mathscr{B}} = [d]_{\mathscr{A}} \circ g = (g \circ f) \circ g = g \circ (f \circ g)$ en appliquant le Lemme 2.5.1.1 on obtient $f \circ g = [d]_{\mathscr{B}}$.

♠Un exemple important d'une isogénie est la multiplication $[n]_{\mathscr{A}} : \mathscr{A} \longrightarrow \mathscr{A}$ par un entier $n \neq 0$, avec $\mathscr{A}[n] := \ker([n]_{\mathscr{A}}) \subset \mathscr{A}$.

2.6 Polarisation et accouplement de Weil

2.6.1 Polarisation

Définition 2.6.1.1 (***Polarisation***)
*Considérons une variété abélienne $\mathscr{A}$ sur le corps k. Une **polarisation** $\mathscr{A}$ est une isogénie $\alpha : \mathscr{A} \longrightarrow \mathscr{A}^*$ vérifiant l'une des conditions équivalentes suivantes :*

1 : *α est une isogénie symétrique et $\alpha^* \mathscr{P}$ est un faisceau ample.*
2 : *α est une isogénie symétrique et $\alpha^* \mathscr{P}$ est un faisceau effectif.*
3 : *S'il existe une extension de corps k' de k et un faisceau ample $\mathscr{L}$ dans $\mathscr{A}_{k'}$ de sorte que $\alpha_{k'} = \varphi_{\mathscr{L}} : \mathscr{A} \longrightarrow \mathscr{A}^*$.*
4 : *S'il existe une extension de corps fini et séparable k' de k et un faisceau ample $\mathscr{L}$ dans $\mathscr{A}_{k'}$ tel que $\alpha_{k'} = \varphi_{\mathscr{L}} : \mathscr{A} \longrightarrow \mathscr{A}^*$.*

Définition 2.6.1.2 (***Degré d'une polarisation***)
*Le **degré d'une polarisation** est son degré en tant que isogénie.*

Proposition 2.6.1.1 (*[6], page 161*)
Soit $\beta : \mathscr{A} \longrightarrow \mathscr{B}$ une isogénie. Si $\alpha : \mathscr{B} \longrightarrow \mathscr{B}^*$ est une polarisation, alors $\beta^\vee \alpha := \beta^* \circ \alpha \circ \beta$ est une polarisation de $\mathscr{A}$ de degré

$$\deg(\beta^\vee \alpha) = \deg(\beta)^2 \cdot \deg(\alpha)$$

Démonstration :
Il est clair que $\beta^\vee \alpha$ est une isogénie de degré donné. Par hypothèses, il existe une extension de corps k' de k et un faisceau ample $\mathscr{L}$ dans $\mathscr{B}_{k'}$ tel que $\alpha_{k'} = \varphi_{\mathscr{L}}$. Alors $\beta^\vee \alpha_{k'} = \varphi_{\beta^\vee \mathscr{L}}$ et puisque β est finie $\beta^\vee \mathscr{L}$ est un faisceau ample dans $\mathscr{A}_{k'}$.

2.6.2 Accouplement de Weil

Définition 2.6.2.1 (***Accouplement bilinéaire***)
Soit $\beta : \mathscr{A} \longrightarrow \mathscr{B}$ une isogénie de variétés abéliennes sur le corps k. Considérons l'isomorphisme α défini par $\alpha : \ker(\beta^*) \xrightarrow{\sim} \ker(\beta)^D$.

– *Définissons*

$$e_\beta : \ker(\beta) \times \ker(\beta^*) \longrightarrow \mathbb{G}_m$$

*l'**accouplement bilinéaire parfait** (des points) est défini par* $e_\beta(x,y) = \alpha(y)\cdot\beta(x)$. *Notons que si* $\ker(\beta)$ *est annulé par* $n \in \mathbb{Z}$ *(avec* $n \geq 1$*), alors* e_β *est à valeurs dans* $\mu_n \subset \mathbb{G}_m$. *Dans le cas particulier* $\beta = n_{\mathscr{A}} : \mathscr{A} \longrightarrow \mathscr{A}$, *on obtient la relation suivante :*

$$e_n : \mathscr{A}[n] \times \mathscr{A}[n]^* \longrightarrow \mu_n$$

*qui est appelée l'**accouplement de Weil**.*

– *Soit* $\lambda : \mathscr{A} \longrightarrow \mathscr{A}^*$ *un homomorphisme. L'accouplement bilinéaire :*

$$e_n^\lambda : \mathscr{A}[n] \times \mathscr{A}[n] \longrightarrow \mu_n$$

est défini par : $e_n^\lambda(x_1,x_2) = e_n(x_1,\lambda(x_2))$.

2.7 Endomorphismes de variétés abéliennes

2.7.1 Décomposition des variétés abéliennes

Définition 2.7.1.1 (***variété abélienne simple***)
Une variété abélienne $\mathscr{A}$ *est dite **variété abélienne simple** s'il n'existe pas une sous-variété abélienne* $\mathscr{B} \subset \mathscr{A}$ *tel que* $0 \neq \mathscr{B} \neq \mathscr{A}$.

Proposition 2.7.1.1 (*[8], page 42*)
Pour toute variété abélienne $\mathscr{A}$, *il existe des sous-variétés abéliennes simples* $\mathscr{A}_1,\mathscr{A}_2,\ldots \subset \mathscr{A}_n$ *telles que l'application :*

$$\mathscr{A}_1 \times \mathscr{A}_2 \times \ldots \times \mathscr{A}_n \longrightarrow \mathscr{A}, \qquad (a_1,\ldots,a_n) \longmapsto a_1 + \cdots + a_n$$

soit une isogénie.

Démonstration :
Par induction, il suffit de prouver l'assertion suivante : soit $\mathscr{B} \subset \mathscr{A}$ tel que $0 \neq \mathscr{B} \neq \mathscr{A}$; alors il existe une variété abélienne $\mathscr{B}' \subset \mathscr{A}$ tel que l'application

$$\mathscr{B} \times \mathscr{B}' \longrightarrow \mathscr{A} \qquad (b,b') \longmapsto b + b',$$

soit une isogénie.
Considérons l'injection i: $\mathscr{B} \hookrightarrow \mathscr{A}$ et choisissons un faisceau ample $\mathscr{L}$ dans $\mathscr{A}$ et défini dans $\mathscr{A}'$ par la composante connexe du noyau de :

$$i^* \circ \lambda_{\mathscr{L}} : \mathscr{A} \longrightarrow \mathscr{B}^*,$$

contenant l'élément neutre 0. Alors B' est une variété abélienne. On sait que :

$$\dim \mathscr{B}' \geq \dim \mathscr{A} - \dim \mathscr{B}.$$

La restriction du morphisme $\mathscr{A} \longrightarrow \mathscr{A}^*$ à $\mathscr{B}$ est $\lambda_{\mathscr{L}|\mathscr{B}} : \mathscr{B} \to \mathscr{B}^*$, qui admet un noyau fini parce que $\mathscr{L}|\mathscr{B}$ est ample (proposition 8.1, proposition 6.6 b, [8], page 35 et page 31). Ainsi $\mathscr{B} \cap \mathscr{B}'$ est fini, et l'application $\mathscr{B} \times \mathscr{B}' \to \mathscr{A}$, $\quad (b,b\prime) \longmapsto b + b\prime$ est une isogénie.

Remarque 2.7.1.1 (*[8], page 43*)
- *Toute variété abélienne peut se décomposer en produite de variétés abéliennes simples.*
- *On peut conclure de la Proposition 2.7.2.1 que si $\mathscr{A}$ et $\mathscr{B}$ sont deux variétés abéliennes simples et que si $\mathscr{A}$ est isogènes à $\mathscr{B}$, on a :*

$$End^0(\mathscr{A}) \approx Hom^0(\mathscr{A},\mathscr{B}) \approx End^0(\mathscr{B}).^4$$

Plus précisément, $Hom(\mathscr{A},\mathscr{B})$ est un espace vectoriel qui est une $End(\mathscr{A})$-module libre à droite et $End(\mathscr{B})$-module libre à gauche. S'ils ne sont pas isogènes alors $Hom(\mathscr{A},\mathscr{B}) = 0$.

2.7.2 La représentation de $T_l\mathscr{A}$

Soit $\mathscr{A}$ une variété abélienne de dimension g sur le corps k. Rappelons que pour tout n ne divisant pas la caractéristique de k, $\mathscr{A}_n(k)$ est d'ordre n^{2g}. De plus, si k est séparé (noté k^{sep}), notons

$$\mathscr{A}_n(k) \stackrel{def}{=} \ker(n : \mathscr{A}(k) \longrightarrow \mathscr{A}(k)).$$

Définition 2.7.2.1 (***définition de*** $T_l\mathscr{A}$)
Fixons un nombre premier $l \neq char(k)$. On définit

$$T_l\mathscr{A} = \varprojlim \mathscr{A}_{l^n}(k^{sep}).$$

En termes simples, un élément de $T_l\mathscr{A}$ est une suite finie

$$(a_1,a_2,\ldots,a_n,\ldots\ldots), \qquad a_i \in \mathscr{A}(k),$$

avec $la_n = a_{n-1}$, $la_1 = 0$ (et donc en particulier pour $a_i \in \mathscr{A}_{l^n}(k^{sep})$).

Lemme 2.7.2.1 (*[8], page 44*)
Soient Q un groupe abélien de torsion et Q_n le sous-groupe des éléments d'ordre n. Supposons qu'il existe un entier d tel que $|Q_n| = n^d$ pour tout entier n. Alors $Q \approx (\mathbb{Q}/\mathbb{Z})^d$.

Démonstration :
L'hypothèse implique que pour tout $n \succ 0$, Q_n est un $(\mathbb{Z}/n\mathbb{Z})$-module de rang d. Choisissons une base $e_1,\ldots,e_n$ de Q_n telle qu'on ait un isomorphisme :

$$\begin{array}{ccccc} Q_n & \stackrel{\approx}{\to} & (\mathbb{Z}/n\mathbb{Z})^d & \stackrel{\approx}{\to} & (n^{-1}\mathbb{Z}/\mathbb{Z})^d, \\ \sum a_i e_i & \longmapsto & (a_1,a_2,\ldots) & \longmapsto & (\frac{a_1}{n},\frac{a_2}{n},\ldots). \end{array}$$

Considérons une suite exacte d'entiers positifs $n_1,n_2,\ldots,n_i,\ldots$ tel que n_i divise n_{i+1} successivement et tout entier divise n_i. Choisissons une autre base $e_1,\ldots,e_n$ de Q_{n_1}, alors en considérant une base $e'_1,\ldots,e'_n$ dans Q_{n_2} tel que $\frac{n_1}{n_2}e'_i = e_i$ pour tout i, ainsi de suite ; on obtient donc le résultat.

Proposition 2.7.2.1 (*[8], page 45*)
Pour $l \neq char(k)$, $T_l\mathscr{A}$ est un $\mathbb{Z}$-module de rang $2g$.

Démonstration : (voir ([8], page 45))

4. Avec $\mathrm{End}^0(T) := End(T) \otimes \mathbb{Q}$.

Corollaire 2.7.2.1 (*[8], page 45*)
Pour tout entier premier $l \neq p$ (avec $p \in \mathscr{A}(k^{sep})$), l'application naturelle

$$Hom(\mathscr{A},\mathscr{B}) \longrightarrow Hom_{\mathbb{Z}_l}(T_l\mathscr{A},T_l\mathscr{B})$$

est injective.

Démonstration :
Soit α un homomorphisme tel que $T_l\alpha = 0$. Alors $\alpha(P) = 0$ pour tout $P \in \mathscr{A}(k^{sep})$ tel que $l^n P = 0$ pour un entier n. Considérons une sous-variété abélienne $\mathscr{C} \subset \mathscr{A}$. Le noyau de $\alpha_{|\mathscr{C}}$ n'est pas fini [5]. Ainsi α est zéro d'une sous-variété abélienne simple de $\mathscr{A}$. La Proposition 2.7.2.1 implique qu'il est zéro dans tout $\mathscr{A}$.

2.7.3 La caractéristique polynomiale d'un endomorphisme

Supposons $k = \mathbb{Q}$ et un endomorphisme α de $H_1(\mathscr{A},\mathbb{Q})$ (avec $H_1(\mathscr{A},\mathbb{Q})$ des endomorphisme de $\mathscr{A}$)qui est un espace vectoriel de dimension $2g$ sur $\mathbb{Q}$.

Définition 2.7.3.1 (***Polynôme caractéristique***)
On définit le ***polynôme caractéristique*** P_α *de* α *par :*

$$P_\alpha(X) = \det(\alpha - X \mid H_1(\mathscr{A},\mathbb{Q})).$$

C'est un polynôme minimal de degré $2g$ à coefficients dans $\mathbb{Z}$.
Plus généralement, on définit le ***polynôme caractéristique*** *d'un élément de $End(\mathscr{A}) \otimes \mathbb{Q}$ de la même façon.*

Théorème 2.7.3.1 (*[8], page 46*)
Soit $\alpha \in End(\mathscr{A})$. Il existe un unique polynôme minimal $P_\alpha \in \mathbb{Z}[X]$ de degré $2g$ tel que $P_\alpha(r) = \deg(\alpha - r)$ pour tout entier r.

Démonstration : (Voir [8], page 46)

Remarque 2.7.3.1 (*[8], page 47*)

1. *Pour $\alpha \in End(\mathscr{A})$ et $n \in \mathbb{Z}$, on a :*

$$\deg(n\alpha) = \deg(n_{\mathscr{A}}) \cdot \deg(\alpha) = n^{2g} \cdot \deg(\alpha).$$

2. *Par extension, on définit de la même façon le degré de $End(\mathscr{A}) \otimes \mathbb{Q}$. De plus, $End(\mathscr{A})$ peut s'identifier à un sous-module de $End(\mathscr{A}) \otimes \mathbb{Q}$.*
   Pour $\alpha \in End(\mathscr{A}) \otimes \mathbb{Q}$, on définit :

$$\deg(\alpha) = n^{-2g} \deg(n\alpha)$$

   avec n un entier tel que $n\alpha \in End(\mathscr{A})$. La formule ci-dessus montre que ceci est indépendant du choix de n. De la même manière, en utilisant le théorème 2.7.3.1, on définit

$$P_\alpha(X) = n^{2g} P_{n\alpha}(nX), \quad \text{avec } \alpha \in End(\mathscr{A}) \otimes \mathbb{Q} \quad \text{et} \quad n\alpha \in End(\mathscr{A}).$$

   Alors $P_\alpha(X)$ est un polynôme minimal de degré $2g$ avec des coefficients rationnels, et

$$P_\alpha(r) = \deg(\alpha - r), \quad \text{pour tout} \quad r \in \mathbb{Q}.$$

5. parce qu'il contient $\mathscr{C}_{l^n}$ pour tout n, et donc $\alpha_{|\mathscr{C}} = 0$

Lemme 2.7.3.1 (*[8], page 47*)
Soient V un k-espace vectoriel et $f : V \longrightarrow k$ une fonction tel que pour tous $v, w \in V$ l'application $k \to k, \quad x \mapsto f(xv+w)$ soit polynomiale en x à coefficients dans k, alors f est une fonction polynomiale.

Démonstration : (voir [8], page 47).

Proposition 2.7.3.1 (*[8], page 47*)
La fonction $End(\mathscr{A}) \otimes \mathbb{Q} \longrightarrow \mathbb{Q}, \quad \alpha \mapsto \deg(\alpha)$ est une fonction polynomiale de degré $2g$ dans $End(\mathscr{A}) \otimes \mathbb{Q}$.

Démonstration :
D'après le Lemme 2.7.3.1, pour montrer que le $\deg(\alpha)$ est une fonction polynomiale, il suffit de montrer que $\deg(n\alpha - \beta)$ est polynomial avec α et β des éléments de $End(\mathscr{A}) \otimes \mathbb{Q}$ fixés. Mais nous savons déjà que l'application deg est homogène et de degré égal à $2g$ dans $\mathbb{Q}$,

i.e on a :

$$\deg(n\alpha) = n^{2g} \deg(\alpha),$$

en utilisant ce résultat, il suffit de prouver que $\deg(n\alpha - \beta)$ est un polynôme de degré $\leq 2g$ pour $n \in \mathbb{Z}$ et $\alpha, \beta \in End(\mathscr{A})$. Soient D un diviseur ample dans $\mathscr{A}$ et $D_n = (n\alpha - \beta)^* D$. Alors par (**Algebraic Groupe de J.S Milne** exemple 10.10, page 170)

$$(D_n \cdot \ldots \cdot D_n) = \deg(n\alpha - \beta) \cdot (\underbrace{D \cdot \ldots \cdot D}_{g})$$

et donc il suffit de montrer que $(D_n)^g$ est un polynôme de degré $\leq 2g$. Par le Corollaire 2.3.2.1 appliqué à $(n\alpha + \beta$, avec $\alpha, \beta : \mathscr{A} \to \mathscr{A}$ et le faisceau $\mathscr{L} = \mathscr{L}(D)$ montre que

$$D_{n+2} - 2D_{n+1} + (2\alpha)^* D + D_n + 2(\alpha^* D) \sim 0$$

ie

$$D_{n+2} - 2D_{n+1} + D_n = D', \text{ où } D' = (2\alpha)^* D - 2(\alpha^* D).$$

Par un même raisonnement, on montre que

$$D_n = \frac{n(n-1)}{2} D' + nD_1 - (n-1)D_0,$$

et donc

$$\deg(n\alpha + \beta) \cdot (D^g) = (D_n^g) = (\frac{n(n-1)}{2})^g (D')^g) + \ldots,$$

qui est un polynôme à n variables de degré $\leq 2g$.

2.8 Hauteur dans une variété abélienne

Propriété 2.8.0.1 (***[4], page 27***)
Soit $\mathscr{A}$ une variété abélienne sur un corps de nombres K. Soit $D \in Div(\mathscr{A})$ et pour tout $m \in \mathbb{Z}$, définissons l'application $[m] : P \longmapsto \underbrace{P + \cdots + P}_{m}$ (avec $[m]P := -[-m]P$ pour $m < 0$).

Alors

$$h_{\mathscr{A},D}([m]P) = \frac{m^2+m}{2} h_{\mathscr{A},D}(P) + \frac{m^2-m}{2} h_{\mathscr{A},D}(-P) + O(1),$$

où la constante $O(1)$ ne dépend pas de P.

Démonstration :
C'est une conséquence du théorème du cube. Si f, g, $h : \mathscr{V} \longrightarrow \mathscr{A}$ sont des applications régulières d'une variété algébrique $\mathscr{V}$ dans une variété abélienne $\mathscr{A}$, on a :

$$(f+g+h)^*D-(f-g)^*D-(f+h)^*D-(g+h)^*D+f^*D+g^*D+h^*D\sim 0.$$

Si on pose $f=[m]$, $g=id$, $h=[-1]$, alors on obtient

$$[m]^*D-[m+1]^*D-[m-1]^*D+[m]^*D+D+[-1]^*D\sim 0.$$

En transposant de l'autre côté une partie de l'expression ci-dessus, on obtient :

$$[m+1]^*D\sim 2[m]^*D-[m-1]^*D+D+[-1]^*D. \qquad (*)$$

En introduisant m, cela donne la formule de **Mumford**

$$[m]^*D\sim \frac{m^2+m}{2}D+\frac{m^2-m}{2}2[-1]^*D. \qquad (**)$$

En combinant les propriétés d'additivité, fonctorialité et la linéarisation du théorème de Weil (Théorème 2.2.0.2).
En effet, si on pose $m=1$ dans (*), alors on obtient :

$$[2]^*D\sim 3D+[-1]^*D.$$

Par induction, observons que :

$$\begin{aligned}\frac{(m+1)^2+(m+1)}{2} &= m^2+m-\frac{(m-1)^2+(m-1)}{2}+1,\\ \frac{(m+1)^2-(m+1)}{2} &= m^2-m-\frac{(m-1)^2-(m-1)}{2}+1.\end{aligned}$$

En considérant (**), alors pour $m+1$, on obtient :

$$\begin{aligned}&\tfrac{(m+1)^2+(m+1)}{2}D+\tfrac{(m+1)^2-(m+1)}{2}[-1]^*D\\ &=2\left(\tfrac{m^2+m}{2}D+\tfrac{m^2-m}{2}[-1]^*D\right)-\left(\tfrac{(m-1)^2+(m-1)}{2}D-\tfrac{(m-1)^2-(m-1)}{2}D\right)+D+[-1]^*D\\ &=2[m]^*D-[m-1]^*D+D+[-1]^*D\\ &\sim [m+1]^*D.\end{aligned}$$

Corollaire 2.8.0.1 (***[4], page 28***)
Pour un diviseur Symétrique D, on a :

$$[m]^*D\sim m^2D \quad et \quad h_{A,D}([m]P)=m^2h_{A,D}(P)+O(1).$$

Démonstration :
Pour la preuve on applique (**) de la Propriété 2.8.0.2, combinée au théorème de Weil (Théorème 2.2.0.2).

Proposition 2.8.0.2 (***Loi parallélogramme des Hauteurs***) (***[4], page 28***)
Soit D un diviseur symétrique sur une variété abélienne $\mathscr{A}$. Alors pour tous P,Q $\in \mathscr{A}(\bar{k})$

$$h_{\mathscr{A},D}(P+Q)+h_{\mathscr{A},D}(P-Q)=2h_{\mathscr{A},D}(P)+2h_{\mathscr{A},D}(Q)+O(1).$$

De cette propriété, on voit que $h_{\mathscr{A},D}$ est une forme quadratique.

Démonstration :
Considérons les applications suivantes $\mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}$ définies par :

$$\sigma(P,Q) := P+Q, \quad \delta(P,Q) := P-Q \quad \pi_1(P,Q) := P \quad \pi_2(P,Q) := Q$$

Mais le "**principe de seesaw**", nous conduit à une équivalence $\sigma^*D + \delta^*D \sim \pi_1^*D + 2\pi_2^*D$ dans $\mathscr{A} \times \mathscr{A}$. En appliquant la hauteur de Weil ici, on obtient :

$$h_{\mathscr{A},\sigma^*D}(P,Q) + h_{\mathscr{A},\delta^*D}(P,Q) = 2h_{\mathscr{A},\pi_1^*D}(P,Q) + 2h_{\mathscr{A},\pi_2^*D}(P,Q) + O(1).$$

et la fonctorialité donne le résultat.

Théorème 2.8.0.2 (***Néron-Tate***) (***[4], page 28***)
*Soit $\mathscr{V}$ une variété projective lisse définie sur un corps de nombres K. Soit $\phi : \mathscr{V} \longrightarrow \mathscr{V}$ un morphisme tel que $\phi^*D \sim \alpha D$ avec $\alpha > 1$ pour un diviseur D. Alors il existe une unique fonction hauteur $\hat{h}_{\mathscr{V},\phi,D} : \mathscr{V}(k) \longrightarrow \mathbb{R}$ appelée la hauteur de **Néron-Tate** (ou la **hauteur canonique**) dans $\mathscr{V}$, vérifiant les propriétés suivantes :*

1. $\hat{h}_{\mathscr{V},\phi,D}(P) = \lim_{n\to\infty} \alpha^n h_{\mathscr{V},D}(\phi^n(P)), \quad où \quad \phi^n := \phi \circ \ldots \circ \phi.$
2. $\hat{h}_{\mathscr{V},\phi,D}(P) = h_{\mathscr{V},D}(P) + O(1).$
3. $\hat{h}_{\mathscr{V},\phi,D}(\phi(P)) = \alpha \hat{h}_{\mathscr{V},\phi,D}(P).$

Démonstration :
Pour le 1. de la propriété, puisque toute suite de Cauchy est convergente, il nous suffira de montrer que la suite $\alpha^n h_{\mathscr{V},D}(\phi^n(P))$ pour $n = 1, 2, 3, \ldots$ est de Cauchy.
Comme $\hat{h}_{\mathscr{V},\phi,D}(P) := \lim_{n\to\infty} \alpha^n h_{\mathscr{V},D}(\phi^n(P))$
On a :

$$h_{\mathscr{V},D}(\phi(P)) = \alpha_{\mathscr{V},D}(P) + O(1)$$

comme $h_{\mathscr{V},D}(\phi(P)) - \alpha h_{\mathscr{V},D}(P)$ est bornée, donc

$$|h_{\mathscr{V},D}(\phi(P)) - \alpha h_{\mathscr{V},D}(P) \leq C, \quad \text{pour tout } P.$$

Pour la différence $\alpha^{-n} h_{\mathscr{V},D}(\phi^n(P)) - \alpha^{-m} h_{\mathscr{V},D}(\phi^m(P))$, on a :

$$\begin{aligned} |\alpha^{-n} h_{\mathscr{V},D}(\phi n(P)) - \alpha^{-m} h_{\mathscr{V},D}(\phi^m(P))| &= \left| \sum_{m+1\leq i\leq n} \alpha^{-i} h_{\mathscr{V},D}(\phi^i(P)) - \alpha^{-(i-1)} h_{\mathscr{V},D}(\phi^{i-1}(P)) \right| \\ &\leq \sum_{m+1\leq i\leq n} \alpha^{-i} |h_{\mathscr{V},D}(\phi^i(P)) - \alpha h_{\mathscr{V},D}(\phi^{i-1}(P))| \\ &\leq \sum_{m+1\leq i\leq n} \alpha^{-i} C \\ &\leq \frac{\alpha^{-m} - \alpha^{-n}}{\alpha - 1} C, \end{aligned}$$

ainsi donc la suite est de Cauchy. En faisant $n \to \infty$, on obtient

$$|\hat{h}_{\mathscr{V},D}(P) - h_{\mathscr{V},D}(P)| \leq \frac{C}{\alpha - 1},$$

Ce qui donne le 2. de la propriété.
Pour le 3. de la propriété , notons que

$$\hat{h}_{\mathscr{V},D}(\phi(P)) = \lim_{n\to\infty} \alpha^{-n} h_{\mathscr{V},D}(\phi n(P)) = \lim_{n\to\infty} \frac{h_{\mathscr{V},D}(\phi^{n+1}(P))}{\alpha^{n+1}} = \alpha \hat{h}_{\mathscr{V},\phi,D}(P).$$

$\mathscr{A}$ étant une variété abélienne, en appliquant la loi du parallélogramme pour $h_{\mathscr{A},D}$, on obtient :

$$\alpha^{-n}h_{\mathscr{A},D}(P+Q)+\alpha^{-n}h_{\mathscr{A},D}(P-Q)=\alpha^{-n}2h_{\mathscr{A},D}(P)+\alpha^{-n}h_{\mathscr{A},D}(Q)+\alpha^{-n}O(1).$$

On trouve le résultat en faisant $n\to\infty$.

Proposition 2.8.0.3 (***[4], page 29***)
Soit $\mathscr{A}$ une variété abélienne sur un corps de nombres K. Soit D un diviseur symétrique sur $\mathscr{A}$ tel que $\phi^*D\sim\alpha D$ pour $\alpha>1$. Alors pour tous $P,Q\in\mathscr{A}(\overline{k})$, on a :

$$\hat{h}_{\mathscr{V},\phi,D}(P+Q)+\hat{h}_{\mathscr{V},\phi,D}(P-Q)=2\hat{h}_{\mathscr{V},\phi,D}(P)+2\hat{h}_{\mathscr{V},\phi,D}(Q).$$

Démonstration :
C'est une conséquence directe de la preuve du 3. du Théorème 2.8.0.2, en faisant tendre la limite de n à l'infini.
En effet d'après la preuve du 3. du Théorème 2.8.0.2 on a :

$$\alpha^{-n}h_{\mathscr{A},D}(P+Q)+\alpha^{-n}h_{\mathscr{A},D}(P-Q)=\alpha^{-n}2h_{\mathscr{A},D}(P)+\alpha^{-n}h_{\mathscr{A},D}(Q)+\alpha^{-n}O(1).$$

En appliquant la limite quand $n\to\infty$ on obtient :

$$\hat{h}_{\mathscr{V},\phi,D}(P+Q)+\hat{h}_{\mathscr{V},\phi,D}(P-Q)=2\hat{h}_{\mathscr{V},\phi,D}(P)+2\hat{h}_{\mathscr{V},\phi,D}(Q).$$

Comme $\hat{h}_{V,\phi,D}$ est une forme quadratique dans une variété abélienne $A(\overline{k})$ (toute fonction $h:A\to\mathbb{R}$ satisfaisant la loi de parallélogramme est une forme quadratique).
Quand $\hat{h}_{V,\phi,D}\geq 0$ pour tout $P\in A(\overline{k})$, et caractérisant les points où $\hat{h}_{V,\phi,D}(P)=0$. Pour cela D est un diviseur ample.

Théorème 2.8.0.3 (***[4], page 29***)
Soit $\mathscr{A}$ une variété abélienne sur un corps de nombres K. Comme la Proposition 2.8.0.3, considérons le morphisme $\phi:\mathscr{A}\to\mathscr{A}$ et D un diviseur tel que $\phi^*D\sim\alpha D$ pour $\alpha>1$. Supposons que D est un diviseur ample, alors :

1. $\hat{h}_{\mathscr{V},\phi,D}(P)\geq 0$.
2. $\hat{h}_{\mathscr{V},\phi,D}(P)=0$ *ssi ϕ est* ***pré−périodique*** *en P, signifiant que l'ensemble*

   $$\{P,\phi(P),\phi^2(P),\ldots\}$$

   est fini (*donc les valeurs $\phi^n(P)$ sont* ***pré−périodiques***).
3. *l'ensemble*

   $$\{P\in\mathscr{A}(k)\mid\phi\text{ est pré−périodique en }P\}$$

   est fini.

Démonstration :
Pour 1., notons que $h_{\mathscr{V},D}(Q)\geq O(1)$ puisque D est ample, et $\alpha^{-n}h_{\mathscr{A},D}(\phi^n(P))\geq\alpha^{-n}O(1)$; en faisant $n\to\infty$, on en déduit que $\hat{h}_{\mathscr{V},\phi,D}\geq 0$.
Pour 2., si ϕ est pré-périodique en P, alors $\{\phi^n(P)\}$ est répété et de même l'ensemble des hauteurs $\{h_{\mathscr{A},D}(\phi^n(P))\}$. La hauteur $h_{\mathscr{A},D}(\phi^n(P))$ est bornée, et $\hat{h}_{\mathscr{V},\phi,D}(P)=\lim_{n\to\infty}\alpha^n h_{\mathscr{V},D}(\phi^n(P))=0$ pour tout n. Les points de l'ensemble

$$\{P,\phi(P),\phi^2(P),\ldots\}$$

sont de hauteurs $h_{\mathscr{V},D}(\phi^n(P))$ bornées, puisque $\hat{h}_{\mathscr{V},D}(Q)=h_{A,D}(Q)+O(1)$. Ainsi l'ensemble $\{\phi^n(P)\}$ est fini par la propriété de Northcott.
Pour 3., c'est une application directe de la propriété de Northcott.

Définition 2.8.0.2 (***Point de torsion***)
Considérons l'application $[m] : \mathscr{A} \to \mathscr{A}$ *avec* $m = 2,3,4\ldots$*, vérifiant les hypothèses du Théorème 2.8.0.3 (avec* $\phi = [m]$*), si* $[m]$ *est pré-périodique en P impliquant que* $[m]^s P = [m]^l P$ *pour* $s > l \geq 1$*, on dira que P est un* ***point de torsion****.*

Proposition 2.8.0.4 (***[4], page 30***)
Si $\phi = [m]$ *pour* $m = 2,3,4\ldots$*, alors* $\hat{h}_{\mathscr{V},\phi,D}(P) = 0$ *ssi P est de torsion dans* $\mathscr{A}(k)$*. Ils sont en nombre fini de points.*

Par ailleurs, notons que si $P \in \mathscr{A}(K)$ et $Q \in \mathscr{A}(K)_{tor}$, alors $\hat{h}_{\mathscr{V},\phi,D}(P) = \hat{h}_{\mathscr{V},\phi,D}(P+Q)$.
En effet si $[n]Q = 0$, alors

$$\hat{h}_{\mathscr{V},\phi,D}(P+Q) = \frac{1}{n^2}\hat{h}_{\mathscr{V},\phi,D}([n](P+Q)) = \frac{1}{n^2}\hat{h}_{\mathscr{V},\phi,D}([n]P) = \hat{h}_{\mathscr{V},\phi,D}(P).$$

CHAPITRE 3

DÉVELOPPEMENT ET PROBLÉMATIQUES

3.1 Problématiques

3.1.1 La conjecture de Mordell-Weil

La théorie diophantienne s'est développée après les travaux de Weil dans de multiples directions, une des plus fécondes est ce que l'on appelle la théorie d'Arakelov qui est venue étoffer les analogies entre arithmétique et géométrie chères à Weil. La preuve de la conjecture de Mordell par Faltings (1983) n'utilise à aucun moment le théorème de Mordell-Weil mais repose sur la théorie des variétés abéliennes et des schémas. En fait le théorème fondamental démontré par Faltings est le suivant

Conjecture 3.1.1.1 ***(Faltings 1983, "conjecture de Shafarevic")***
Soient le corps de nombres K, T un ensemble fini de places de K et $g \geq 1$. Il n'existe qu'un nombre fini de variétés abéliennes de dimension g, définies sur K, ayant bonne réduction hors de T, à isomorphisme prés.

Une variété lisse projective a "*bonne réduction*" en une place v si elle possède un modèle que l'on peut réduire modulo v en gardant la licité. Par un théorème de Torelli on déduit le même énoncé avec "courbes de genre g" à la place de "variétés abéliennes". Un argument dû à Parshin permet alors d'en déduire la conjecture de Mordell.
Faltings a utilisé plusieurs domaines de la géométrie algébrique : schémas, schémas en groupes, espaces de modules ; il construit aussi une notion de hauteur intrinsèque d'une variété abélienne inspirée des idées introduites par Arakelov. Il utilise aussi les représentations l-adiques associées à une variété abélienne introduites par Weil ainsi que "*l'hypothèse de Riemann*" démontrée par Weil pour les variétés abéliennes sur un corps fini.

3.1.2 Problème de Lehmer pour les hypersurfaces de variétés abéliennes

On sait depuis les travaux de Philippon, puis Bost, Gillet, Soulé dans le cadre de l'intersection arithmétique, comment définir la hauteur des variétés projectives ; l'idée étant de considérer un point comme une variété de dimension zéro et de généraliser ceci en dimension supérieure. De même que dans le cas des points, on sait pour les variétés abéliennes munies d'un fibré en droites ample et symétrique définir une hauteur particulièrement agréable : la hauteur canonique $\widehat{h}_{\mathscr{L}}$, ou hauteur normalisée. En dimension zéro, il existe un théorème caractérisant les points de hauteur normalisée nulle ; c'est un résultat de Kronecker dans le cas de $\mathbb{G}_m$. Philippon (dans le cas d'un produit de courbes elliptiques) puis Zhang et David-Philippon dans le cas général ont montré comment généraliser ce résultat pour caractériser les sous-variétés de hauteur normalisée nulle : ce sont les translatées d'une sous-variété abélienne par un point de torsion. On dit qu'une telle sous-variété est une sous-variété de torsion. La réponse à cette question revient à résoudre une conjecture de Bogomolov. Ceci étant, on peut se demander comment minorer la hauteur normalisée d'une sous-variété de hauteur non nulle d'une variété abélienne. Dans leur article [1] , David et Philippon ont formulé un problème général contenant cette question. En termes de degré défini ci-dessous, on peut notamment faire ressortir de la discussion suivant la formulation de leur problème l'énoncé suivant :

Conjecture 3.1.2.1 (***David-Philippon***)
Soit $\mathscr{A}$ une variété abélienne définie sur un corps de nombres K, munie d'un fibré ample et symétrique $\mathscr{L}$. Soit $\mathscr{V}$ une sous-variété stricte de $\mathscr{A}$ sur K, irréductible et qui n'est pas réunion de sous-variétés de torsion, alors, on a l'inégalité

$$\frac{\widehat{h}_{\mathscr{L}}(\mathscr{V})}{\deg_{\mathscr{L}}(\mathscr{V})} \geq c(\mathscr{A},\mathscr{L}) \deg_{\mathscr{L}}(\mathscr{V})^{-\frac{1}{s-\dim \mathscr{V}}};$$

où s est la dimension du plus petit sous-groupe algébrique contenant $\mathscr{V}$, et où $c(\mathscr{A},\mathscr{L})$ est une constante ne dépendant que de $\mathscr{A}$ et de $\mathscr{L}$.

Conjecture 3.1.2.2 (***David-Philippon***)
Sous les hypothèses précédentes, et en supposant de plus que $\mathscr{V}$ est un hypersurface de $\mathscr{A}$, on a l'inégalité

$$\widehat{h}_{\mathscr{L}}(\mathscr{V}) \geq c(\mathscr{A},\mathscr{L}),$$

où $c(\mathscr{A},\mathscr{L})$ est une constante ne dépendant que de $\mathscr{A}$ et de $\mathscr{L}$.

3.2 Développement

Dans l'usage moderne de la cryptographie, la cryptographie à clé publique basée sur le protocole *RSA* occupe une place prépondérante. Cependant, l'augmentation des puissances de calcul et l'amélioration des attaques contre *RSA* rendent le besoin d'alternatives pressant. Or les courbes elliptiques et les variétés abéliennes de dimension 2

1. S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes. In Number theory (Tiruchirapalli, 1996) Contemp. Math., Contemp. Math., Amer. Math. Soc., Provi-dence, RI, (1998)., volume 210, pages 333–364, 1996. ratazzi@math.jussieu.fr

permettent d'avoir des niveaux de sécurité équivalents à la taille de clé et coût calculatoire bien moindre. De plus, l'existence d'une forme bilinéaire naturelle (pairing) sur ces structures permet des constructions cryptographiques avancées de plus en plus utilisées chez les constructeurs de protocoles.
L'algorithmique des courbes elliptiques sur les corps finis a été étudiée en profondeur : on dispose d'une arithmétique rapide, on sait calculer efficacement les isogénies, les polynômes de classes de Hilbert, les anneaux d'endomorphismes, et on dispose d'algorithmes efficaces de comptage de points. En revanche, il n'en va pas de même des variétés abéliennes de dimension 2 : si l'arithmétique a été relativement étudiée, les algorithmes plus avancés (comme le calcul d'isogénies, des anneaux d'endomorphismes, ou le comptage de point en grande caractéristique) sont bien plus lents que leurs contreparties sur les courbes elliptiques. De plus, l'utilisation des pairings peut faire intervenir des variétés abéliennes de dimension supérieure (pour des raisons d'efficacité ou pour avoir plus de liberté dans la conception de protocoles).

On peut utiliser les isogénies de variétés abéliennes en cryptographie.
Lorsqu'on utilise une variété abélienne $\mathscr{A}_k$ sur un corps fini k en vue d'applications cryptographiques, il faut faire attention à ce que son cardinal soit divisible par un grand nombre premier. Pour cela, il faut être capable de le calculer rapidement. (Une autre méthode est d'utiliser la théorie de la multiplication complexe pour construire une courbe elliptique avec un nombre de points prescrit.)

On termine en donnant un panorama des algorithmes de comptage de points disponibles. Si F_r est le morphisme de Frobenius de k, il agit sur $\mathscr{A}_k$, et les points fixes de $\sharp\mathscr{A}_k(k)$ par le Frobenius sont exactement les points rationnels $\mathscr{A}_k(k)$. On a donc $\sharp\mathscr{A}_k(k) = \deg(F_r - Id)$.
Il existe deux grandes familles d'algorithmes pour calculer le cardinal de $\mathscr{A}_k$.
La première famille (appelée famille p-adique), consiste à calculer un relevé (canonique avec l'algorithme de Satoh , ou non, avec l'algorithme de Kedlaya utilisant la cohomologie de Monsky-Washnitzer de la variété abélienne $\mathscr{A}_k$ à un anneau p-adique et calculer le polynôme caractéristique du Frobenius sur ce relevé. Cette famille d'algorithmes est surtout efficace lorsque la caractéristique p de k est petite.
L'autre famille (appelée aussi famille l-adique), consiste à calculer l'action du Frobenius sur $\mathscr{A}_k[l]$ (avec l premier à p).

Bibliographie et sitographie

[1] Adrien Douady, VARIÉTÉS ABÉLIENNES, séminaire Claude Chevalley, tome 4 (1958-1959), exp. n°9, p.1-6,http://www.numdam.org/item?id=SCC_1958-1959_4__A9_0.

[2] Alexis TCHOUDJEM ; Introduction aux groupes algébriques, *Institut Camille Jordan ; Université Claude Bernard Lyon I. Boulevard du Onze Novembre 1918 69622 Villeurbanne FRANCE, Villeurbanne*, le 7 janvier 2013, http://math.univ-lyon1.fr/~tchoudjem/ENSEIGNEMENT/M2R/cours-m2.pdf.

[3] André Néron ; VARIÉTÉS ABÉLIENNES,(cours 1965-66,retirage 1979), Université Paris-Sud, Département de Mathématiques.

[4] Fabien Pazuki ; Heights ;Institut de Mathématiques de Bordeaux Université de Bordeaux351, cours de la Libération 33405 Talence ; Spring semester 2014, http://www.math.u-bordeaux.fr/~fpazuki/.

[5] Felice Ronga ; Notes de géométrie algébrique,Genève, MMVI ap. J.-C., http://www.unige.ch/math/folks/ronga/geo_alg_06_07/geo_alg.pdf.

[6] Gerard van der Geer Ben Moonen ;ABELIAN VARIETIES, PRELIMINARY VERSION OF THE FIRST CHAPTERS,http://www.mi.fu-berlin.de/users/elenalavanda/BMoonen.pdf.

[7] Griffith Harris ; *Principles of Algebraic Geometry* ;New york 1978, https://www.amazon.com/Principles-Algebraic-Geometry-Phillip-Griffiths/dp/0471050598.

[8] J.S. Milne ; Abelian Varieties,Version 2.0, March 16, 2008 , www.jmilne.org/math/,http://www.jmilne.org/math/CourseNotes/AV.pdf.

[9] MAT 562 : Introduction à la géométrie algébrique et courbes elliptiques, http://cims.nyu.edu/~pirutka/coursMAT562.pdf.

[10] Marck Hindry et Joseph H. Silverman ; Diophantine Geometry An Introduction,Graduate Texts in Mathematics, With 8 Illustrations,https://www.amazon.com/Diophantine-Geometry-Introduction-Graduate-Mathematics dp.

[11] Martin Bright ; The Picard group, 14 April 2008, http://homepages.warwick.ac.uk/~maseap/arith/notes/picard.pdf.

[12] OLIVIER DEBARRE ; INTRODUCTION À LA GÉOMÉTRIE ALGÉBRIQUE, HTTP://WWW.MATH.ENS.FR/~DEBARRE/DEA99.PDF.

[13] OUMAR SALL ; NOTE DE COURS, (UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR), NOTE DE COURS GÉOMÉTRIE ALGÉBRIQUE NIVEAU MASTER II 2014, HTTP://WWW.UNIV-ZIG.SN.

[14] RAFAEL GUGLIELMETTI ; INTRODUCTION À LA GÉOMÉTRIE ALGÉBRIQUE ; ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, HTTP://RGUG.CH/MEDIAS/MATH/GEOMETRIE_ALGEBRIQUE.PDF.

[15] W. FULTON, **ALGEBRAIC CURVES**, AN INTRODUCTION TO ALGEBRAIC GEOMETRY, JANUARY 28 2008, HTTP://WWW.MATH.LSA.UMICH.EDU/~WFULTON/CURVEBOOK.PDF.