UNIVERSITÉ 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 de mémoire :

Le Théorème d'Abel- Jacobi

Présenté par : **Awa BARRY**

sous la direction de : **Professeur Oumar SALL**

Soutenu publiquement le Samedi 05 Novembre 2022 à l'université Assane SECK de Ziguinchor.
devant le jury ci-aprés :

PRÉNOM(S) ET NOM	Grade	Qualité	Université
SALOMON SAMBOU	Professeur Titulaire	Président du Jury	UASZ
AMOUSSOU THOMAS GUEDENON	Professeur Assimilé	Examinateur	UASZ
MANSOUR SANE	Maître de conférences Titulaire	Examinateur	UASZ
MOUSSA FALL	Maître de conférences Titulaire	Examinateur	UASZ
OUMAR SALL	Professeur Titulaire	Directeur	UASZ

Année universitaire : 2021-2022

Table des matières

Remerciements

Tout d'abord je rends grâce à Dieu de m'avoir donné la force, la motivation et le courage de vaincre toutes les épreuves que j'ai traversées tout au long de ce travail et surtout de m'avoir accordé une bonne santé afin d'aboutir à mes recherches.

C'est sans doute et avec plaisir que mes remerciements se dirigent en premier lieu vers mon directeur de mémoire, le Professeur Oumar SALL. Son talent scientifique et son engagement en tant qu'encadreur m'ont aidé à évoluer sur mes recherches. Je salue ses pertinentes remarques et surtout ses précieux conseils m'ont toujours aidé à avancer dans mes travaux. C'est à travers la clarté de ses explications et de ses connaissances transmises que j'ai aimé et choisi son domaine qui n'est rien d'autre que la géométrie algébrique. **MERCI INFINIMENT PROFESSEUR OUMAR SALL !**
Je suis honorée par la présence du Professeur Salomon SAMBOU qui a accepté de présider le jury de ce mémoire, je le remercie sincèrement.

Je remercie également le Professeur Amoussou Thomas GUEDENON, le Docteur Moussa FALL et le Docteur Mansour SANE pour avoir accepté d'être membres du jury.

Je tiens à exprimer une profonde gratitude envers tous les professeurs du département de mathématiques de l'Université Assane Seck de Ziguinchor, pour la qualité de l'enseignement qu'ils nous ont dispensé ; leur vision des mathématiques reste sans hésitation un modèle pour nous. Sans oublier le Professeur Diaraf SECK de l'Université Cheikh Anta Diop de Dakar et le Docteur Omar DIOP de l'Université Virtuelle du Sénégal. Un grand merci à vous !

J'exprime un remerciement particulier au Docteur Souhaibou SAMBOU, Docteur à l' UASZ, qui a beaucoup participé à la réalisation de ce mémoire, de par son aide, son soutien et surtout ses conseils.
Je remercie très chaleureusement les responsables de ZIP, mention spéciale à Monsieur Alassane TAMBOURA, pour m'avoir permis d'effectuer mes recherches documentaires dans leurs locaux et aussi de m'avoir assuré le transport. Merci encore !
Je profite de l'occasion pour remercier tous mes promotionnaires de classe. Ces remerciements s'adressent en particulier à Marie FAYE, Dieynaba SAMB, Fatou DIENG, Amadou SEYDI, Daouda DIACK, Abdourahmane BA, Abdoulaye SAGNA, Yaya COULIBALY, Mamadou Nazir DIALLO, Azize MANGA, Mamadou Korka BA, Alioune BA, Doudou MANE, Mouhamed NIAMBA, Saliou DIAW, Seydi Diamil DIOUF , Amadou BALDE et Ibrahima DIOP ceux avec qui j'ai partagé le cycle de master. Sans oublier Boubacar DIOP et Sadioba SAMATE.

J'ai eu la chance d'échanger avec nos docteurs et doctorants, j'ai pu profiter de leurs divers points de vue et connaissances et surtout ils sont toujours là pour nous. Je les remercie à cet égard. En particulier, je remercie Docteur Pape Modou SARR, Docteur Chérif Mamina COLY, Docteur Abdoulaye

DIOUF et Papa BADIANE Doctorant à l'UASZ.
Je remercie également toute la première, la deuxième et la troisième promo MPI.

J'en profite pour exprimer toute ma gratitude à mon très cher mari Monsieur Amadou DIALLO qui n'a pas hésité à me soutenir dans mes études et surtout il n'arrête pas de m'encourager VRAIMENT MERCI DE TA COMPREHENSION et à ma fille chérie Fatoumata Binta DIALLO. Mention spéciale à ma belle sœur chérie Madame Salimata DIALLO DIOP qui m'a soutenu moralement et financièrement sans rien y attendre et son mari Monsieur Cheikhna DIOP, à ma chérie à moi Madame kadidiatou DIALLO BA et sa belle famille depuis Joal mais aussi à mes belles mères pour avoir assisté ma fille pour que je puisse terminer ce travail.
Je remercie chaleureusement mon père Monsieur BOUBACAR DIALLO un père pas comme les autres, grâce à lui je n'ai jamais senti l'absence de mon père biologique qui est décédé paix à son âme, une page entière ne suffira pas pour le remercier, je te laisse avec Dieu, seul lui peut te payer tes bonnes actions envers moi et mon frère Mamadou Alpha BARRY **MERCI INFINIMENT PAPA BOUBACAR DIALLO**.
J'en profite pour exprimer ma reconnaissance envers mon ami Monsieur Amadou SEYDI qui n'a pas hésité en aucun cas pour satisfaire mes besoins **Merci frérot** ! sans oublier sa famille, son père Ibrahima SEYDI et sa sœur Binta SEYDI.

J'adresse mes sincères remerciements à toute ma famille, surtout ma maman chérie Aïssatou BARRY, pour le soutien et les encouragements qu'elle ne cesse de renouveler. Je suis infiniment reconnaissante envers mes parents pour l'éducation, les soutiens permanents et leurs encouragements qu'ils m'ont donnés. Je remercie également mes frères et mes sœurs. En particulier, Mariama DIALLO, Binta DIALLO, Mamadou Alpha BARRY, Seydou BA,Mamadou Saliou DIALLO, Seydou DIALLO, Lamine DIALLO, Aïssatou DIALLO, Adama Awa DIALLO, Oumou DIALLO et Fatoumata Korka BA pour la confiance aveugle qu'ils ont en moi et je salue leurs encouragements.
J'en profite pour remercier tous les membres de ma large famille : ma tante Binta BARRY, la famille BARRY à Tanaff, mon beau frére Mr DIEDHIOU, mon amie d'enfance Alimatou DIALLO et sa famille, ma tante Yama CISSE et sa famille à Alwar, ma soeurette Rokhéya SANE et sa famille, mes amis : Bassirou THIAM ; Ismaïla DIATTA ; Marcel MENDY ; Binta DIEME et la famille DABO.
Je profite de l'occasion pour remercier mes enseignants du moyen secondaire qui ont été les premiers à me faire aimer les matières scientifiques.

Dédicaces

Je dédie ce modeste travail :

A la prunelle de mes yeux et la raison de ma vie, ma Mère et mon Père, mon mari pour leur confiance, amour et surtout leurs conseils précieux durant toutes mes années d'études ;

A Papa Boubacar DIALLO un père pas comme les autres ;

A mes frères et mes sœurs ;

A mes tantes et leurs familles, mes oncles ;

A mes belles sœurs et leurs familles ;

A ma fille, mes nièces et mes neuveux ;

A tout l'entourage familial ;

A tous mes amis qui se connaissent eux même sans citer leurs noms, sans oublier tout ce qui tenaient à moi ;

Et bien sur à moi -même.

Résumé

Le travail de ce mémoire porte essentiellement sur le théorème d'Abel-Jacobi dont l'objectif est d'énoncer le théorème, de rappeler les outils nécessaires pour la compréhension de la démonstration du théorème et d'en donner un exemple d'application. L'application donnée dans ce mémoire conserne la détermination explicite des points algébriques de degré donné sur un cas particulier d'une courbe algébrique.

Introduction

La géométrie algébrique est un domaine des mathématiques qui s'intéresse à l'étude des ensembles algébriques, c'est-à-dire ceux qui sont définis par l'annulation d'un ou de plusieurs polynômes. L'attention particulière est accordée aux variétés algébriques. Il existe deux types de catégories essentielles de variétés algébriques, celles qui sont affines et celles qui sont projectives. Dans ce présent mémoire on s'est intéressé au théorème d'Abel-Jacobi.

L'objectif de ce travail de mémoire est d'énoncer le théorème, de rappeler les outils necessaires pour la compréhension de la démonstration du théorème et d'en donner un exemple d'application, le théorème est énoncé comme suit :

Théorème 1. *(Abel-Jacobi)*
Soit C une courbe lisse projective de genre $g \geqslant 1$. Il existe une variété abélienne $Jac(C)$, appelée la jacobienne de C, et une injection $j : C \longrightarrow Jac(C)$ ayant les propriétés suivantes :

1. *Si l'on étend j linéairement au groupe des diviseurs sur C, on obtient un isomorphisme*
$$Pic^0(C) \cong Jac(C).$$
2. *Pour tout $r \geq 0$, on définit une sous-variété $W_r \subset Jac(C)$ par*
$$W_r = j(C) + ... + j(C) \ \ (r \ copies).$$
Alors $dim(W_r) = min(r, g)$, $W_g = Jac(C)$ et $dim(Jac(C)) = g$.
3. *Soit $\theta = W_{g-1}$. Alors θ est un diviseur irréductible et ample de $Jac(C)$.*

Ce mémoire comprend deux chapitres et est structuré comme suit :
Dans le premier chapitre, nous introduisons les notions de base essentielles pour la compréhension du sujet abordé ainsi que les définitions et notations qui concerneront tout le reste du manuscrit. Les propositions et théorèmes utilisés pour ces notions considérées comme rappels ne sont pas en général démontrés. Parmi ces notions de base on privilégie les ensembles algébriques affines, les ensembles algébriques projectifs, les diviseurs et la loi de groupe sur une courbe elliptique. Ce chapitre rassemble des propriétés essentielles qui seront beaucoup utilisées dans la suite. Pour les preuves, on peut se référer par exemple à [5] ou à [6].

Le deuxième et dernier chapitre qui est le cœur du sujet, est consacré à l'étude du théorème d'Abel-Jacobi qui est facilité par les notions comme la jacobienne d'une courbe, le genre d'une courbe

et le théorème de Riemann-Roch. Nous allons présenter à la fin un exemple d'application pouvant intéresser des chercheurs dans leurs domaines à travers plusieurs branches des mathématiques.

Chapitre 1

Préliminaires

Dans ce chapitre nous présentons d'abord les variétés (les variétés affines, les variétés projectives et les diviseurs) qui sont des éléments essentiels de la géométrie algébrique, le lecteur pourra consulter [5] pour plus d'informations ; et en fin la loi de groupe sur une courbe elliptique (définitions et construction de la loi de groupe sur l'ensemble des points d'une courbe elliptique) ; voir [6].

1.1 Variétés

1.1.1 Variétés affines

1.1.1.1 Ensemble algébrique affine

On considère un corps K commutatif.
Donnons quelques exemples d'ensembles définis par l'annulation d'un polynôme.

$$\mathcal{P}_1 = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2+1=0\},$$
$$\mathcal{P}_2 = \{(x,y) \in \mathbb{C}^2 \mid x^2+y^2+1=0\},$$
$$\mathcal{P}_3 = \{(x,y,z) \in \mathbb{Q}^3 \mid x^n+y^n=z^n\} \quad (n \geq 1).$$

Définition 1.

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

Les éléments de l'espace affine sont appelés points.
$\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite et plan affine.
Un point a de $\mathbb{A}^n$ est dit zéro de $P \in K[X_1,\ldots,X_n]$ si $P(a)=0$.

Définition 2.

Soit S une partie quelconque de $K[X_1,\ldots,X_n]$. L'ensemble noté $\mathcal{V}(S)$ défini par

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

est appelé l'ensemble algébrique affine défini par S.

Remarque 1. *On remarque que $\mathcal{V}(S)$ est l'ensemble des zéros communs à tous les polynômes de S.*

On notera souvent, dans le cas d'un ensemble fini, $\mathcal{V}(P_1, \ldots, P_r)$ au lieu de $\mathcal{V}(\{P_1, \ldots, P_r\})$.

Soit $S = (P_i)_{i \in I}$ une famille d'éléments de $K[X_1, \ldots, X_n]$; on a $\mathcal{V}(S) = \bigcap_{i \in I} \mathcal{V}(P_i)$.

Définitions 1.

1. *On appelle hypersurface définie par P, et on note $\mathcal{V}(P)$, l'ensemble des zéros de P (pour P non constant et K algébriquement clos). Le degré de $\mathcal{V}(P)$ est le degré de P.*
2. *Une courbe algébrique plane est une hypersurface du plan affine.*
3. *Une courbe algébrique plane est dite conique, cubique, quartique,... si le degré est respectivement $2, 3, 4, \ldots$*
4. *Un hyperplan est une hypersurface définie par P de degré 1. Une droite est un hyperplan de $\mathbb{A}^2$.*

Remarque 2. *Tout ensemble algébrique affine peut être défini par l'annulation d'un nombre fini de polynômes.*

Proposition 1.

1. *Le vide et l'espace tout entier sont des ensembles algébriques affines.*
2. *Une intersection quelconque d'ensembles algébriques affines est un ensemble algébrique affine.*
3. *Une réunion finie d'ensembles algébriques affines est un ensemble algébrique affine.*

De cette proposition on peut conclure l'existence d'une topologie sur $\mathbb{A}^n(K)$ dont les fermés sont des ensembles algébriques affines : cette topologie est appelée topologie de Zariski.

1.1.1.2 Irréductibilité

Définition 3.

On dit qu'un espace topologique E est irréductible s'il n'est pas vide et s'il n'est pas la réunion de deux fermés distincts de E.

Définitions 2.

1. *Un ensemble algébrique est irréductible s'il est irréductible pour la topologie de Zariski.*
2. *On appelle variété algébrique affine tout ensemble algébrique affine irréductible.*

Définition 4.

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

$$\mathfrak{I}(A) = \{P \in K[X_1, \ldots, X_n] \mid \forall\, a \in A,\ P(a) = 0\}.$$

On voit que $\mathfrak{I}(A)$ est l'ensemble des polynômes nuls sur A.

Théorème 2.

Tout ensemble algébrique non vide A se décompose de façon unique (à permutation prés) en une réunion finie d'ensembles algébriques irréductibles $A_1, \ldots, A_r$ non contenus l'un dans l'autre.
Les $A_1, \ldots, A_r$ sont appelés les composantes irréductibles de A.

Démonstration.

Existence

Nous allons raisonner par l'absurde. Pour cela supposons que A ne peut pas se décomposer en une réunion finie d'ensembles algébriques irréductibles non contenus l'un dans l'autre. Soit $(A_i)_i$ la famille des ensembles algébriques non vides qui ne se décomposent pas en une réunion finie d'ensembles algébriques irréductibles non contenus l'un dans l'autre. Puisque $K[X_1, \ldots, X_n]$ est noethérien, la famille $(\mathfrak{I}(A_i))_i$ possède un élément maximal c'est-à-dire $\exists\ j = 1, ..., r, \forall\ i = 1, ..., r;$ on a

$$\mathfrak{I}(A_i) \subset \mathfrak{I}(A_j).$$

Ainsi,

$$\exists\ j = 1, ..., r, \forall\ i = 1, ..., r\ A_j \subset A_i.$$

Donc $(A_i)_i$ admet un élément minimal V qui est forcément réductible.
On peut écrire $V = V_1 \cup V_2$, avec V_i fermé non vide distinct de V. Par minimalité V_i est réunion finie d'irréductibles, d'où la contradiction.

Unicité

Supposons qu'on ait deux écritures :

$$V = V_1 \cup \cdots \cup V_r = W_1 \cup \cdots \cup W_e.$$

On écrit

$$V_i = V \cap V_i = (W_1 \cup \cdots \cup W_e) \cap V_i = (W_1 \cap V_i) \cup \cdots \cup (W_e \cap V_i).$$

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

$$V_i \subset W_j. \tag{1.1}$$

De même, on peut écrire

$$W_j = V \cap W_j = (V_1 \cup \cdots \cup V_r) \cap W_j = \left(V_1 \cap W_j\right) \cup \cdots \cup \left(V_r \cap W_j\right).$$

Comme W_j est irréductible, il existe l tel que $W_j = V_l \cap W_j$; d'où

$$W_j \subset V_l. \tag{1.2}$$

Les inégalités (1.1) et (1.2) montrent que $V_i \subset V_l$, ce qui par hypothèse impose que $i = l$. Donc $V_i = V_l$. Par conséquent, $V_i \subset W_j \subset V_l = V_i$, c'est-à-dire $V_i = W_j$.

□

Définition 5. *Soient $V \subset K^n$ et $W \subset K^m$ des sous-variétés affines. Une application $V \to W$ est dite régulière si c'est la restriction à V d'une application $K^n \to K^m$ dont les composantes sont des fonctions polynômiales.*

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

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

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

1.1.2 Variétés projectives

Considérons le corps de base K qui a servi à définir $\mathbb{A}^n = K^n$ et la relation qu'on notera $\mathcal{R}$ définie sur $K^{n+1} \setminus \{0\}$ par : pour tous vecteurs non nuls x, y de K^{n+1}, on a : $x\mathcal{R}y$ si et seulement si, il existe

$$\lambda \in K^* : y = \lambda x.$$

On remarque que $\mathcal{R}$ est une relation de colinéarité qui est une relation d'équivalence. Ainsi, deux vecteurs x et y sont équivalents si et seulement si, ils sont colinéaires.

1.1.2.1 Ensembles algébriques projectifs

Définition 6.

On appelle espace projectif de dimension n sur K et l'on note $\mathbb{P}^n(K)$ ou $\Big(\mathbb{P}(K^{n+1})$ ou encore $\mathbb{P}^n$ s'il n'y a pas risque de confusion sur $K\Big)$, l'ensemble des classes d'équivalences définies par $\mathcal{R}$:

$$\mathbb{P}^n = (K^{n+1} \setminus \{0\})/\mathcal{R}.$$

En d'autres termes $\mathbb{P}^n$ est l'ensemble des droites vectorielles de K^{n+1}. Si un point $P \in \mathbb{P}^n$ a pour vecteur directeur (représentant) $(x_0, ..., x_n) \in K^{n+1} \setminus \{0\}$, on écrit $P = (x_0 : .... : x_n)$.

$\mathbb{P}^1$ et $\mathbb{P}^2$ sont appelés respectivement droite projective et plan projectif sur K.

Définition 7.

Soit S une partie de $K[X_0, \ldots, X_n]$ formée de polynômes homogènes. L'ensemble noté $\mathcal{V}(S)$ défini par

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

est appelé l'ensemble algébrique projectif défini par S.

Remarque 3.

On remarque que $\mathcal{V}(S)$ est l'ensemble des zéros communs à tous les polynômes de S.

Définitions 3.

1) On appelle hypersurface définie par un polynôme F homogène, et on note $\mathcal{V}(F)$, l'ensemble des zéros de F (pour F non constant et K algébriquement clos). Le degré de $\mathcal{V}(F)$ est le degré de F.

2) Une courbe projective plane est une hypersurface du plan projectif.

3) Une courbe projective plane est dite conique, cubique, quartique, quintique, ... si le degré est respectivement $2, 3, 4, 5, \ldots$

4) Un hyperplan est une hypersurface définie par un polynôme homogène de degré 1.

Remarques 1.

1) Les résultats obtenus dans $\mathbb{A}^n$ sont pareils que dans le cadre projectif. On peut en citer quelques uns :

a) Tout $\mathcal{V}(S)$ peut être défini par l'annulation d'un nombre fini de polynômes.

b) L'intersection quelconque et l'union finie d'ensembles algébriques projectifs en est un.

c) Les ensembles $\emptyset$, $\mathbb{P}^n$ sont algébriques projectifs.
Donc on peut définir une topologie de Zariski comme on l'a fait en affine dont les fermés sont des ensembles algébriques projectifs.

2) La notion d'irréductibilité et ses propriétés en affine se comportent de la même façon que dans le cadre projectif.

Définitions 4.

1. *On appelle variété projective, tout ensemble algébrique projectif irréductible.*

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

Remarque 4. *Lorsque nous dirons que X est une variété, il sera toujours sous-entendu que X est quasi-projective.*

Définition 8. *(Application régulière)*

Soient X et Y des variétés quasi-projectives.
On dit qu'une application $u : X \longrightarrow Y$ est régulière si elle est continue et si, pour tout ouvert U de Y et toute fonction régulière $f : U \longrightarrow K$, la composée $f \circ u$ est régulière sur $u^{-1}(U)$.

Définition 9. *(Application rationnelle)*
Soient X et Y des variétés. On considère les couples (u, U) et (v, U), où U et V sont des ouverts denses de X et $u : U \longrightarrow Y$, $v : V \longrightarrow Y$ des applications régulières.
On dit que les couples (u, U) et (v, V) sont équivalents si u et v coïncident sur $U \cap V$.
On appelle application rationnelle de X sur Y, une classe d'équivalence pour cette relation. On note $u : X \dashrightarrow Y$ une application rationnelle de X sur Y.

Remarque 5.

Une application rationnelle n'est pas une application. En particulier, il n'est pas toujours possible de composer des applications rationnelles, ou de les restreindre à des sous-variétés.

1.1.2.2 Courbe lisse, courbe elliptique

Courbe lisse :

Définitions 5.

Considérons une courbe projective plane C définie par l'équation $F(X_1, X_2, X_3) = 0$ et soit $P \in C$.

1. *Un point P de C est dit singulier si*

$$\left(\frac{\partial F}{\partial X_1}(P), \frac{\partial F}{\partial X_2}(P), \frac{\partial F}{\partial X_3}(P)\right) = (0,0,0).$$

2. *On dit qu'un point P de C est lisse (ou non singulier ou régulier) si*

$$\left(\frac{\partial F}{\partial X_1}(P), \frac{\partial F}{\partial X_2}(P), \frac{\partial F}{\partial X_3}(P)\right) \neq (0,0,0).$$

3. *Une courbe C est lisse (ou non singulière ou régulière) si elle l'est en chacun de ses points.*

Courbe elliptique :

Définition 10.

Soit K un corps. Une courbe elliptique est une cubique irréductible, non singulière, définie comme l'ensemble des solutions dans le plan $\mathbb{P}^2(K)$ de l'équation de Weierstrass homogène suivante :

$$\mathbb{E} : Y^2X + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.3}$$

avec $a_i \in K$.

Une courbe elliptique doit être non singulière, c'est-à-dire si on écrit l'équation (1.3) sous la forme d'une équation $F(X,Y,Z) = 0$, alors les dérivées partielles de F ne doivent pas s'annuler simultanément en un point de la courbe.
On remarque qu'une telle courbe admet un unique point de coordonnée Z nulle, le point à l'infini $(0:1:0)$ il sera noté dans la suite par $\mathcal{O}$.
Dans ce qui suit nous utiliserons la représentation affine de l'équation de Weierstrass sur K une telle équation est du type :

$$\mathbb{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.4}$$

avec $a_i \in K$.
Pour $Z \neq 0$ un point $(X : Y : Z)$ solution de l'équation (1.3) correspond à un point $(x,y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right)$ solution de l'équation (1.4). Ainsi, l'ensemble des solutions de l'équation (1.3) correspond à l'union des solutions de l'équation (1.4) et du point $\mathcal{O}$.

1.1.3 Diviseurs

1.1.3.1 Dimension

En général, une variété algébrique ne contient pas d'ouvert non vide isomorphe à un ouvert d'un espace affine.

Définition 11.

Soit X un espace topologique. La dimension de X est le maximum des entiers n pour lesquels il existe des parties irréductibles fermées $X_0, ..., X_n$ vérifiant $X_0 \subsetneq ... \subsetneq X_n$. La dimension de X est donc un entier positif, ou $+\infty$, ou $-\infty$ si X est vide.

Remarque 6.

Si X est réunion de fermés $X_1, ..., X_l$, on a $dim(X) = max(dim(X_i))$. On voit donc que la dimension d'un ensemble algébrique est le maximum des dimensions de ses composantes irréductibles.

Proposition 2.

Un ensemble algébrique est de dimension 0 si et seulement si il consiste en un nombre fini de points.

Démonstration.

Soit x un ensemble algébrique de dimension 0. Tout fermé irréductible contenant un point est réduit à ce point, donc les composantes irréductibles de X sont des points. □

Définition 12.

On dit qu'un ensemble algébrique est de dimension pure n, ou équidimensionnelle de dimension n, si chaque composante irréductible est de dimension n.

Si x est un point de X, on appelle dimension de X en x, et l'on note $dim_x X$, le maximum des dimensions des composantes irréductibles de X passant par x.

Exemples 1.

1. *$dim\mathbb{A}^n = n$; $dim\mathbb{P}^n = n$.*
2. *Le produit $\mathbb{P}^n \times \mathbb{P}^m$ contient un ouvert dense isomorphe à $\mathbb{A}^n \times \mathbb{A}^m$, donc à $\mathbb{A}^{n+m}$, il est alors de dimension $n + m$.*

1.1.3.2 Diviseurs de Weil, diviseurs de Cartier

Soit X une variété.

Diviseurs de Weil :

Définition 13. *(Diviseur de Weil)*
On appelle diviseur de Weil sur X une somme formelle finie à coefficients entiers d'hypersurfaces irréductibles de X.

Ainsi, un diviseur de Weil D sur X s'écrit $D = \sum_i m_i Y_i$ où les m_i sont des entiers presque tous nuls et les Y_i représentent des hypersurfaces irréductibles de X.
Diviseurs de Cartier :

Définition 14. *(Diviseur de Cartier)*
Un diviseur de cartier sur X est la donnée d'un recouvrement (U_i) de X par des ouverts, et sur chaque U_i on définit une fonction rationnelle f_i, avec la condition de compatibilité : pour tout U_i, $U_j \in (U_i)$ si $U_i \cap U_j \neq \emptyset$ alors la fraction $f_{ij} = f_i / f_j$ est une fonction à valeurs dans K^* (C'est-à-dire sans zéro ni pôle).

De ces deux notions, on obtient une proposition qui nous permet d'identifier les deux diviseurs. Ainsi, nous pouvons les écrire de façon simple.

Proposition 3.

Sur une variété lisse les notions de diviseurs de Weil et diviseur de Cartier coïncident.

Cette proposition nous permet de conclure qu'un diviseur sur une courbe lisse est la somme formelle finie de points affectés de coefficients entiers.

1.1.3.3 Diviseurs principaux et diviseurs canoniques

Diviseurs principaux :
Dans cette sous-partie on va supposer que la courbe est affine et irréductible de manière à avoir un anneau $K[C]$ intègre.
Soit C une courbe plane affine irréductible de sorte que l'anneau des polynômes $K[C]$ est intègre.

Définition 15.

Le corps des fractions de l'anneau $K[C]$ est appelé le corps des fonctions rationnelles sur C ; il est noté $K(C)$.

Remarque 7.

Tout polynôme, de degré supérieur ou égal à 1, appartenant à $K[C]$ possède un diviseur irréductible.

Définitions 6.

Soit C une courbe plane affine irréductible, $f \in K(C)$ et $P \in C$.

1. *On dit que f est régulière (ou est définie) au point P s'il existe $g, h \in K[C]$ avec $h(P) \neq 0$ telle que $f = \frac{g}{h}$.*
   L'ensemble des fonctions régulières en P est noté $\mathbf{O}_P(C)$ et appelé l'anneau local de C en P.
2. *L'ensemble des points de C pour lesquels f n'est pas régulière est appelé l'ensemble des pôles de f.*
   Si f est régulière au point $P \in C$ et $f(P) = 0$, on dit que P est un zéro de f.
3. *L'ensemble des fonctions régulières en P et qui s'annulent en P est noté $\mathcal{M}_P(C)$ est appelé l'idéal maximal de C en P.*

Si $P = (a, b)$ alors $\mathcal{M}_P(C) = \{f \in \mathbf{O}_P(C) \mid f(P) = 0\}$ est de la forme $\langle x - a, y - b\rangle$: c'est l'idéal engendré par $x - a$ et $y - b$. Les éléments inversibles de $\mathbf{O}_P(C)$ sont ceux qui n'appartiennent pas à $\mathcal{M}_P(C)$, on les appelle les unités de $\mathbf{O}_P(C)$ et ils forment un groupe multiplicatif.

Définition 16.

On dit que $\mathbf{O}_P(C)$ est un anneau de valuation discrète s'il existe un $t \in \mathbf{O}_P(C)$, $t \neq 0$, $t \in \mathcal{M}_P(C)$, tel que tout élément non nul $f \in \mathbf{O}_P(C)$ s'écrit de manière unique $f = u.t^n$, u unité de $\mathbf{O}_P(C)$, $n \in \mathbb{N}$.
L'entier n est appelé la valuation ou l'ordre de f noté $ord_P(f)$; il ne dépend pas du choix de t qu'on appelle uniformisante.

Définition 17.

Soit C une courbe projective lisse et irréductible, f une fonction non nulle de $K(C)$. On associe à f le diviseur noté $div(f)$ défini par :

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

Un tel diviseur est appelé diviseur principal.

Diviseurs canoniques :
Considérons une variété algébrique X de dimension n. Essayons d'introduire les formes différentielles régulières.

Définition 18.

Une p-forme différentielle w régulière sur X est une forme qui dans un voisinage de chaque point $x \in X$ s'écrit

$$w = \sum_{|I|=p} f_I dg_I$$

où $I = (i_1, ..., i_p)$ est un multi-indice d'entiers avec $1 \leq i_1 < i_2 < .... < i_p \leq n$, $f_I = f_{i_1 ....i_p}$ et $g_I = \{g_{i_1}, ..., g_{i_p}\}$; f_I et g_I sont des fonctions régulières en x et $dg_I = dg_{i_1} \wedge dg_{i_2} \wedge .... \wedge dg_{i_p}$.

Une n-forme différentielle w régulière s'écrit $w = f dg_{i_1} \wedge dg_{i_2} \wedge .... \wedge dg_{i_n}$

Définition 19.

Une p-forme différentielle rationnelle sur X est la donnée d'une p-forme régulière w sur un ouvert de X, modulo la relation d'équivalence " $\simeq$ " définie comme suit :

$$(w, U) \simeq (w', u') \ \ si \ \ et \ \ seulement \ \ si \ \ w = w' \ \ \ sur \ \ U \cap U'.$$

Aprés avoir défini les formes différentielles on peut donc pouvoir définir un diviseur canonique. Pour cela on doit considérer notre X comme étant une variété projective lisse de dimension n.

Définition 20. *(Diviseur canonique)*
Un diviseur canonique sur X est un diviseur d'une n-forme différentielle rationnelle sur X.

Un tel diviseur est noté K_X ou simplement K.

Proposition 4.

Si w et w' sont deux n-formes différentielles rationnelles sur X alors

$$K \equiv K'.$$

Autrement dit, il existe une fonction rationnelle non nulle telle que $w = fw'$.
De cette proposition on peut dire que les diviseurs des formes différentielles rationnelles non nulles forment une seule classe de diviseurs, appelée classe canonique. Ainsi, sur X tous les diviseurs canoniques ont le même degré. De ce fait intéressons nous au cas d'une courbe.

Définition 21.

Soit C une courbe irréductible définie sur K. L'espace des formes différentielles sur C noté $\Omega_C(K)$, est le K-espace vectoriel engendré par les symboles de la forme dx pour $x \in K(C)$ vérifiant les relations usuelles :

1. *$d(x+y) = dx + dy$ pour tous $x, y \in K(C)$,*
2. *$d(xy) = xdy + ydx$ pour tous $x, y \in K(C)$,*
3. *$d\alpha = 0$ pour tout $\alpha \in K(C)$.*

Remarque 8. *L'espace vectoriel $\Omega_C(K)$ est de dimension 1 sur $K(C)$. Si t est une uniformisante en un point lisse de C, alors dt est une base de $\Omega_C(K)$.*

1.2 Loi de groupe sur une courbe elliptique

1.2.1 Définition et construction

La loi de composition interne va être définie à l'aide du théorème suivant :

Théorème 3. *(Règle de la sécante tangente)*
Soient $\mathbb{E}$ *une courbe elliptique et D une droite, toutes deux définies sur un corps K. Si D coupe* $\mathbb{E}$ *en deux points alors D coupe* $\mathbb{E}$ *en trois points.*

De ce théorème une première loi de composition interne que nous noterons $*$ peut être déduite. Elle servira à construire la loi de groupe sur l'ensemble des points d'une courbe elliptique.

Définition 22. *(Loi de composition interne de la sécante tangente)*
Soit $\mathbb{E}$ *une courbe elliptique définie sur un corps K. D'aprés le théorème précédent, puisqu'une courbe elliptique est irréductible et non singulière on a :*

1) *Soient deux points distincts* $P, Q \in \mathbb{E}$, $P \neq Q$, *alors la droite* (PQ) *recoupe la courbe* $\mathbb{E}$ *en un troisième point noté* $P * Q$ *(la règle de la sécante).*
2) *Soit un point* $P \in \mathbb{E}$ *alors on peut définir* $P * P$ *comme le point d'intersection de la courbe* $\mathbb{E}$ *avec sa tangente au point P(règle de la tangente).*

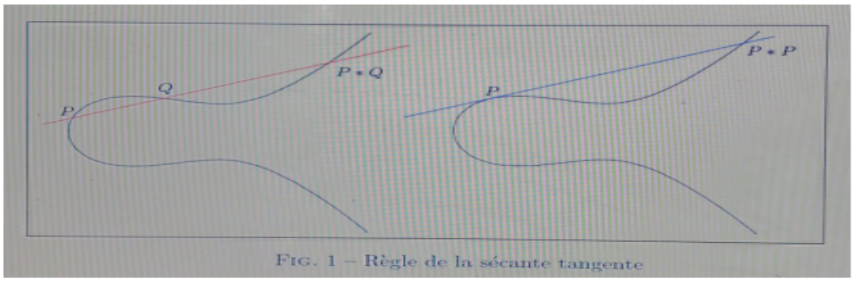

FIG. 1 – Règle de la sécante tangente

Sur la figure ci-dessus on constate qu'une droite verticale coupant la courbe C ne semble pas couper en un troisième point. Ceci est lié à la difficulté de représenter $\mathbb{P}^2$ sur un plan. Ce troisième point existe belle et bien, et appartient à $\mathbb{P}^1$. Pour une courbe elliptique il correspond au point $\mathcal{O}$.

1.2.2 La loi de groupe sur l'ensemble des points d'une courbe elliptique

Proposition 5.

Soient K un corps et $\mathbb{E}$ *une courbe elliptique. Pour tous points* P_1, P_2, Q_1, *et* Q_2 *de* $\mathbb{E}$ *nous avons :*

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2).$$

Pour la preuve voir [1].

Théorème 4.

Soient un corps K et $\mathbb{E}$ *une courbe elliptique définie sur K.*
Soient P et Q deux points de cette courbe.
Alors l'opération $P + Q = \mathcal{O} * (P * Q)$ *définit une structure de groupe commutatif ayant* $\mathcal{O}$ *comme élément neutre.*

Démonstration.

1. La loi $+$ est interne car $P+Q$ est l'intersection d'une droite et d'une cubique, c'est-à-dire un point de la courbe.

2. La loi $+$ est associative .
En effet si P, Q et R sont trois points de la courbe on a :

$$\begin{aligned} P*(Q+R) &= P*(\mathcal{O}*(Q*R)) \\ &= ((P*Q)*Q)*((\mathcal{O}*((Q*R)) \;\; carP = ((P*Q)*Q) \\ &= ((P*Q)*\mathcal{O})*((Q*((Q*R))) \;\; voir\ la\ proposition\ 5 \\ &= (\mathcal{O}*(P*Q)*R) \\ &= (P+Q)*R \end{aligned}$$

d'où l'associativité.
En appliquant $\mathcal{O}$ sur les deux membres de l'égalité, nous trouvons

$$P+(Q+R) = (P+Q)+R.$$

3. L'élément $\mathcal{O}$ est neutre pour la loi $+$. En effet :

$$P+\mathcal{O} = \mathcal{O}*(P*\mathcal{O}) = P$$

et

$$\mathcal{O}+P = \mathcal{O}*(\mathcal{O}*P) = P$$

4. Tout point P possède un inverse pour la loi $+$. Vérifions que le point

$$-P = (\mathcal{O}*\mathcal{O})*P$$

est l'inverse de P :

$$P+(-P) = \mathcal{O}*(P*((\mathcal{O}*\mathcal{O})*P)) = \mathcal{O}*(\mathcal{O}*\mathcal{O}) = \mathcal{O}+\mathcal{O} = \mathcal{O}.$$

De la même manière on montre que $(-P)+P = \mathcal{O}$.

5. Enfin la loi $+$ est commutative. Si P et Q sont deux points de la droite, alors
$P+Q = \mathcal{O}*(Q*P) = Q+P$.

□

Chapitre 2

Application du théorème d'Abel-Jacobi

Dans ce chapitre qui est le but du sujet, nous allons d'abord donner quelques outils pour pouvoir énoncer le théorème, ensuite parler du théorème proprement dit (énoncé, preuve et application).

2.1 Quelques outils

Dans cette section les définitions, théorèmes et propositions font référence à [2].

2.1.1 Jacobienne d'une courbe

Diviseur sur une courbe lisse :
Soit $\mathcal{C}$ une courbe plane lisse.

Définition 23. *Un diviseur D sur C est une somme formelle de points appartenant à C*

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

où les n_P sont des entiers presque tous nuls.

L'ensemble des diviseurs sur C est un groupe commutatif noté $\mathrm{Div}(C)$, où la loi de groupe est l'addition formelle des points :

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

Le degré d'un diviseur est la somme de ses coefficients :

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

Le support de $\sum_{P \in C} n_P P$ est l'ensemble des points $P \in C$ tels que $n_P \neq 0$.
L'application deg définie par

$$\begin{array}{rccc} deg : Div(C) & \longrightarrow & \mathbb{Z} \\ D & \longmapsto & deg(D) \end{array}$$

est un homomorphisme de groupes.
En effet, $Div(C)$ et $\mathbb{Z}$ sont des groupes et de plus si on prend deux diviseurs D et D' dans $Div(C)$ on a :
$deg(D+D') = deg(D) + deg(D')$. D'où deg est un morphisme de groupes.
Le noyau de cet homomorphisme est l'ensemble des diviseurs de degré 0, noté $Div^0(C)$ qui est un sous-groupe de $Div(C)$.
Ainsi, $Div^0(C) = Kerdeg$.

Définition de la jacobienne :

On dit que les diviseurs D_1 et D_2 sont linéairements équivalents, noté $D_1 \sim D_2$, si le diviseur $D_1 - D_2$ est principal.
L'ensemble des diviseurs principaux sur C est un sous-groupe de $Div(C)$ noté $Prin(C)$.

Définition 24.

On appelle groupe de picard de C noté $Pic(C)$ le quotient de $Div(C)$ par $Prin(C)$:

$$Pic(C) = Div(C)/Prin(C).$$

Le quotient de $Div^o(C)$ par $Prin(C)$ sera noté $pic^o(C)$, c'est l'ensemble des classes de diviseurs de degré 0 dans $Pic(C)$.

Définition 25. *La jacobienne d'une courbe C est le sous - groupe des éléments de degré 0 dans $Pic(C)$.*

2.1.2 Genre d'une courbe et théorème de Riemann-Roch

La complexité d'une courbe est mesurée par un invariant appelé genre et qu'on notera g. Nous verrons que cela s'exprime par le fait que la jacobienne d'une courbe est de dimension g.

Définition 26. *Soit C une courbe projective plane lisse de degré d.*

L'entier $\dfrac{(d-1)(d-2)}{2}$ est appelé le genre de la courbe C que l'on note g.

Ainsi $g = \dfrac{(d-1)(d-2)}{2}$.

Définition 27. *(Système linéaire complet)*
Soit D un diviseur sur C. On appelle système linéaire complet d'un diviseur D noté $|D|$ l'ensemble de tous les diviseurs effectifs linéairement équivalents à D défini par

$$|D| = \{D' \in Div(C) \mid D' \geq 0 \, et \, D \sim D'\}.$$

Soient C une courbe lisse et D un diviseur sur C. On associe à D l'ensemble

$$\mathcal{L}(D) = \{f \in K(C) |\ div(f) + D \geq 0\} \cup \{0\}.$$

$\mathcal{L}(D)$ est un K-espace vectoriel de dimension finie et on note $l(D)$ sa dimension c'est-à-dire $l(D) = dim_K \mathcal{L}(D)$. Le système linéaire complet $|D|$ a une structure naturelle d'espace projectif, et peut être paramétré par $\mathbb{P}(\mathcal{L}(D))$.
Par construction, on a

$$dim(|D|) = dim_K \mathcal{L}(D) - 1$$
$$dim(|D|) = l(D) - 1.$$

Toute partie $|D|$ correspondant à un sous-espace projectif de dimension r est appelée système linéaire de dimension r. Le degré du système linéaire est le degré de ses diviseurs.

Définition 28. *Un point $P \in C$ est dit point base d'un système linéaire s'il apparaît dans chacun de ses diviseurs.*

Théorème 5. *(Riemann-Roch)*
Soit C une courbe lisse projective de genre g. Pour tout diviseur D de $Div(C)$, on a

$$l(D) - l(K_C - D) = deg(D) - g + 1.$$

Corollaire 1. *Soient C une courbe lisse projective de genre g et $D \in Div(C)$.*

1. *$l(K_C) = g$ et $deg(K_C) = 2g - 2$.*
2. *Si $deg(D) < 0$, alors $l(D) = 0$.*
3. *D est ample si et seulement si $deg(D) > 0$.*
4. *Si $deg(D) \geqslant 2g$, alors D est sans point base.*
5. *Si $deg(D) \geq 2g - 1$ alors $l(D) = deg(D) - g + 1$.*

2.1.3 Morphismes

Nous aurons par la suite besoin de la notion de plongement de Segre, donc nous allons d'abord parler des morphismes. Dans notre cas on parle de morphisme entre variétés .

Définition 29.

Soient $X, Y \subset \mathbb{P}^n$ deux variétés. Une application continue $\varphi : X \to Y$ est un morphisme de variétés si pour tout ouvert $V \subset Y$ et toute fonction régulière $f : V \to K$
la fonction $f \circ \varphi : \varphi^{-1}(V) \to K$ est régulière sur $\varphi^{-1}(V)$.

S'il existe un morphisme réciproque $\psi : Y \to X$ tel que $\psi \circ \varphi = id_X$ et $\varphi \circ \psi = id_Y$, on dit que φ est un isomorphisme de variétés.

Proposition 6.

Soient X, Y et $Z \subset \mathbb{P}^n$ des variétés, $\varphi : X \to Y$ et $\psi : Y \to Z$ deux morphismes de variétés. Alors $\psi \circ \varphi : X \to Z$ est un morphisme de variétés.

Définition 30.

Soit $f : Z \longrightarrow X$ un morphisme de variétés algébriques. On dit que f est un plongement fermé si f se factorise à travers une sous variété fermée $Y \subset X$ par un isomorphisme $g : Z \longrightarrow Y$.

Remarque 9. *Soit $f : X \longrightarrow Y$ un morphisme de variétés algébriques. L'image réciproque d'un point $y \in Y$ est une sous-variété fermée de X, qu' On appelle la fibre de f en x.*

Considérons une courbe projective et lisse C et notons $Jac(C)$ sa jacobienne. On désigne par $[D]$ la classe dans $Pic^0(C)$ d'un diviseur D. Choisissons le point base $\infty \in C$ pour définir l'application

$$\begin{array}{rcl} j : C & \longrightarrow & Jac(C) \\ P & \longmapsto & [P - \infty] \end{array}$$

appelée plongement jacobien.

Parlons maintenant du plongement de Segre.

Définition 31. *(Plongement de Segre)*
Le plongement de Segre de degré r et s est :

$$\begin{array}{rcl} \psi_{r,s} : \mathbb{P}^r \times \mathbb{P}^s & \longrightarrow & \mathbb{P}^N \\ (x_0, ..., x_r) \times (y_0, ..., y_s) & \longmapsto & (... : x_i y_j : ...)_{\ 0 \le i \le r,\, 0 \le j \le s} \end{array}$$

où $N = (r+1)(s+1) - 1 = rs + r + s$.

2.2 Théorème d'Abel-Jacobi

Les définitions, théorèmes, propositions et lemmes énumérés dans cette section font référence à [3].

2.2.1 Variétés abéliennes

Définitions 7.

1. *En géométrie algébrique, un point rationnel de variété algébrique peut être défini comme étant un point dont les coordonnées appartiennent à un domaine donné.*
2. *Un groupe algébrique est une variété algébrique munie d'une loi de groupe compatible avec sa structure de variété algébrique.*

Corollaire 2. *Une variété abélienne est un groupe algébrique commutatif.*

Définition 32.

Une variété abélienne est un ensemble possédant une structure de groupe et une structure de variété algébrique projective, ces deux structures étant compatibles.

On notera t_a l'application de translation $(t_a(x) = a + x)$ et $[n]$ l'application de multiplication définie par : $n([n](x) = x + ... + x)$.
Dans une telle situation une variété abélienne est nécessairement lisse car elle contient un ouvert lisse, la translation est un isomorphisme donc on peut recouvrir la variété par des ouverts lisses.

Proposition 7. *(Lemme de rigidité)*
Soit X une variété projective, Y et Z deux variétés quelconques, et $f : X \times Y \longrightarrow Z$ un morphisme. S'il existe un point y_0 de Y tel que f restreint à $X \times \{y_0\}$ est constant, alors f est constant sur toute tranche $X \times \{y\}$.
Si f est de plus constant sur une tranche de la forme $\{x_0\} \times Y$ alors f est constant.

On donne un théorème très utile pour décrire les applications à valeurs dans une variété abélienne.

Théorème 6. *(Weil)*

Une application rationnelle d'une variété lisse dans une variété abélienne s'étend en un morphisme.

En ce qui concerne les applications d'une variété abélienne sur une autre variété, on a la proposition ci-dessous.

Proposition 8.

Soient A une variété abélienne et $f : A \longrightarrow Y$ un morphisme. Alors il existe une sous-variété abélienne B de A telle que pour tout $x \in A$, la composante connexe de $f^{-1}(f(x))$ contenant x soit égal à $B + x$.

Démonstration.

Soit C_x la composante connexe de $f^{-1}(f(x))$ contenant x, et soit $B = C_0$. On considère l'application

$$\begin{array}{rcl} f : A \times C_x & \longrightarrow & Y \\ (a, u) & \longmapsto & f(a + u) \end{array}$$

f est constante sur $\{0\} \times C_x$ donc constante sur toute tranche $\{a\} \times C_x$, ce qui reveint à dire $f(a + C_x) = f(a + x)$.
D'autre part $a - x + C_x$ est connexe et contient a donc, par symétrie $a - x + C_x = C_a$. Pour $a = 0$ cela donne $C_x = x + B$.
Il reste qu'à prouver que B est un sous-groupe de A. Si $b \in B$, alors $C_{-b} = -b + B$ donc $0 \in C_{-b}$ puis $C_{-b} = B$ ou encore $-b + B \subset B$ ce qui termine la preuve. □

Remarque 10. *Une variété abélienne peut être définie comme étant la jacobienne d'une courbe algébrique C. La dimension de la variété $Jac(C)$ est le genre de la courbe C.*

Dans la suite on notera Jac par J.

2.2.2 Variétés jacobiennes

Nous allons avant cela parler des produits symétriques de courbes, non simplement parce que nous en aurons besoin plus loin, mais aussi parce qu'ils interviennent directement dans la preuve de notre théorème.

Lemme 1.

Un produit de variétés projectives peut être canoniquement muni d'une structure de variété projective à l'aide du plongement de Segre.

Définition 33.

Soit E un ensemble. On appelle groupe symétrique de E l'ensemble des applications bijectives de E sur E muni de la composition d'applications (la loi $\circ$), on le note $\mathcal{G}(E)$.

Un cas particulier courant est le cas où E est l'ensemble fini $\{1, 2, ..., n\}$, n étant un entier naturel strictement positif, on note alors $\mathcal{G}_n$ ou S_n le groupe symétrique de cet ensemble. Les éléments de $\mathcal{G}_n$ sont appelés permutations et $\mathcal{G}_n$ est appelé groupe des permutations de degré n ou groupe symétrique d'indice n.

Définition 34.

Soit G un groupe algébrique agissant algébriquement sur une variété algébrique projective X. Un quotient géométrique de X par G est la donnée d'une variété algébrique projective Y et d'un morphisme $\pi : X \to Y$ exposés aux conditions suivantes :

a) $\pi^{-1}(\pi(x)) = G.x$ *pour tout* $x \in X$.

b) Si $f : X \longrightarrow Z$ *est un morphisme* $G-$*équivariant de variétés, il se factorise par* π *en un morphisme* $g : Y \longrightarrow Z$ *tel que* $f = g \circ \pi$.

Cette définition étant, un théorème d'algèbre commutative de Hilbert traduit géométriquement, elle nous assure que les quotients géométriques par des groupes finis existent.
Fixons-nous alors une courbe lisse projective C et prenons sa $r^{\text{ième}}$ puissance. Le lemme précédent nous dit que c'est une variété projective. Le $r^{\text{ième}}$ goupe symétrique S_r agit sur cette variété, et comme il est fini, le théorème de Hilbert nous dit que son quotient géométrique par S_r existe. On note alors

$$Sym^r(C) = (C \times ... \times C)/S_r$$

et est appelé $r^{\text{ième}}$ produit symétrique.

2.2.3 Enoncé, preuve et application du théorème d'Abel-Jacobi

Nous commençons cette sous-section par donner des résultats qui vont nous permettre de démontrer la troisième partie de notre théorème.

Définition 35. *(Diviseur ample)*
Un diviseur est très ample si l'application rationnelle associée au système linéaire $|D|$ est un plongement.
Un diviseur D est ample si un multiple positif de D est très ample.

Le diviseur θ
Le diviseur θ est donné avec la jacobienne et a plusieurs propriétés intéressantes, notamment celle de caractériser, avec la jacobienne, la classe d'isomorphisme de la courbe dont il provient.

Théorème 7. *(Torelli) La courbe C est caractérisée (à isomorphisme prés) de manière unique par le couple (J, θ).*

Aprés avoir donné ces résultats on peut maintenant énoncer le théorème.

2.2.3.1 Enoncé du théorème

Théorème 8. *(Abel-Jacobi)*
Soit C une courbe lisse projective de genre $g \geqslant 1$. Il existe une variété abélienne $J(C)$, appelée la jacobienne de C, et une injection $j : C \longrightarrow J(C)$ ayant les propriétés suivantes :

1. *Si l'on étend j linéairement au groupe des diviseurs sur C, on obtient un isomorphisme*
$$Pic^0(C) \cong J(C).$$
2. *Pour tout $r \geq 0$, on définit une sous-variété $W_r \subset J(C)$ par*
$$W_r = j(C) + ... + j(C) \ \ (r \ copies).$$
Alors $dim(W_r) = min(r, g)$, $W_g = J(C)$ et $dim(J(C)) = g$.
3. *Soit $\theta = W_{g-1}$. Alors θ est un diviseur irréductible et ample de $J(C)$.*

2.2.3.2 Preuve du théorème

Montrons d'abord l'existence d'une variété abélienne $J(C)$ appelée la jacobienne de C.
Considèrons $Sym^n(C)$ pour un certain n, pour cela on va supposer qu'en C on a un point rationnel $P_0 \in C(K)$.
Ensuite, si on choisit un entier $n \geq 2g-1$ de sorte que pour tout diviseur D de degré n, on ait $l(D) = deg(D) - g + 1$. Sur la variété $Sym^n(C)$, dont on identifie les points avec les diviseurs

effectifs de degré n sur C, on pose $D_0 = n(P_0)$, que l'on utilisera comme point base sur $Sym^n(C)$. Soit J l'ensemble de tous les systèmes linéaires de degré n sur C, et π l'application définit par :

$$\begin{aligned} \pi : Sym^n(C) &\longrightarrow J \\ D &\longmapsto |D|. \end{aligned}$$

A ce point J n'est qu'un ensemble et on a les fibres de π sont isomorphes à $\mathbb{P}^{n-g}$, nous pouvons utiliser notre point base D_0 pour définir une application d'addition sur l'ensemble J, cette construction utilise des familles de systèmes linéaires ; soit m cette application définit par :

$$\begin{aligned} m : J \times J &\longrightarrow J \\ (|D_1|, |D_2|) &\longmapsto |D_1 + D_2 - D_0|. \end{aligned}$$

Puisque J est un ensemble et est muni d'une loi de groupe, donc on peut le munir d'une structure d'ensemble algébrique pour laquelle π est un morphisme, et dans ce cas m est aussi un morphisme. $Sym^n(C)$ étant une variété projective et que π est surjective, donc J est aussi une variété projective. Comme les fibres de π sont isomorphes à $\mathbb{P}^{n-g}$, la dimension de J est :

$$dim(J) = dim(Sym^n(C)) - dim(\mathbb{P}^{n-g}) = n - (n-g) = g.$$

Maintenant essayons de montrer que m définit une loi de groupe sur J. Pour cela on va vérifier les propriétés suivantes :

Vérifions l'existence d'un élément neutre et d'un inverse :

On a :

$$m(|D|, |D_0|) = |D + D_0 - D_0| = |D| \tag{2.1}$$

et

$$m(|D_0|, |D|) = |D_0 + D - D_0| = |D|. \tag{2.2}$$

Les relations (2.1) et (2.2) nous montrent l'existence d'un élément neutre qui est $|D_0|$.

$$m(|D|, |2D_0 - D|) = |D + 2D_0 - D - D_0| = |D_0|. \tag{2.3}$$

et

$$m(|2D_0 - D|, |D|) = |2D_0 - D + D - D_0| = |D_0| \tag{2.4}$$

(2.3) et (2.4) montrent l'existence d'un élément inverse qui est $|2D_0 - D|$.

Vérifions l'associativité : On a

$$m(m(|D_1|, |D_2|), |D_3|) = m(|D_1 + D_2 - D_0|, |D_3|) = |D_1 + D_2 - D_0 + D_3 - D_0|.$$

Donc

$$m(m(|D_1|, |D_2|), |D_3|) = |D_1 + D_2 + D_3 - 2D_0|. \tag{2.5}$$

On a aussi

$$m(|D_1|, m(|D_2|, |D_3|)) = m(|D_1|, |D_2 + D_3 - D_0|) = |D_1 + D_2 + D_3 - D_0 - D_0|.$$

Donc

$$m(|D_1|, m(|D_2|, |D_3|)) = |D_1 + D_2 + D_3 - 2D_0|. \tag{2.6}$$

D'aprés les relations (2.5) et (2.6) on voit que

$$m(m(|D_1|, |D_2|), |D_3|) = m(|D_1|, m(|D_2|, |D_3|))$$

d'où l'associativité.

Ainsi, on peut conclure que J est bien une variété abélienne.

Passons maintenant à la démonstration des trois parties du théorème.

1. Démontrons que si on étend linéairement l'application j au groupe des diviseurs sur C, on obtient un isomorphisme entre $Pic^0(C)$ et $J(C)$.

Considèrons l'application

$$\begin{aligned} j : C &\longrightarrow J \\ P &\longmapsto |(P) + (n-1)P_0| \end{aligned}$$

et on l'étend linéairement pour obtenir

$$\begin{aligned} j : Pic^0(C) &\longrightarrow J \\ ([D]) &\longmapsto |D + D_0|. \end{aligned}$$

Montons que $j : Pic^0(C) \longrightarrow J$ est un isomorphisme.

Soit D un diviseur de degré n. A-t-on $j([D - D_0]) = |D|$?

On a $j([D - D_0]) = |D - D_0 + D_0| = |D|$ donc j est surjective.

Supposons maintenant que $j([D]) = D_0$, cela signifie que $|D + D_0| = |D_0|$, ainsi on a : $deg(|D + D_0|) = deg(|D_0|)$, or $deg(|D + D_0|) = deg(|D|) + deg(|D_0|)$ donc $deg(|D|) = 0$ d'où D est un diviseur principal par conséquent j est injective.

Ce qui met fin à la démonstration de la premiére partie.

2. Essayons de prouver que $dim(W_r) = min(r, g)$, $W_g = J(C)$ et $dim(J(C)) = g$, pour tout $r > 0$.

L'ensemble $W_r = j(C) + ... + j(C)$ est l'image dans J de la variété projective $C \times C \times ... \times C$, donc l'ensemble est de dimension au plus r.

Cependant, $W_r \subseteq W_r + j(C) = W_{r+1}$, soient $W_{r+1} = W_r$ et $dim(W_{r+1}) = dim(W_r) + 1$.

Mais s'il existe un r tel que $W_{r+1} = W_r$, il s'ensuit par récurrence que $W_s = W_r$ pour tout $s \geq r$.

En effet,

$*$) Pour $s = r$ on a $W_r = W_r$ c'est vrai au rang $s = r$.

$*$) Supposons que $W_r = W_s$ et montrons que $W_{r+1} = W_{s+1}$,

on a : $W_r = W_s$
$W_r + j(C) = W_s + j(C)$, par suite $W_{r+1} = W_{s+1}$ donc c'est vrai au rang $r+1$ d'où pour tout $s \geq r$ $W_s = W_r$.
Comme l'application $j : Pic^0(C) \longrightarrow J$ est surjectivité, on a $Im(j) = J$ ce qui implique que la réunion des W_r est égale à J, qui est de dimension g. Il en résulte que $dim(W_r) = r$ pour tout $r \leq g$ et que $dim(W_r) = g$ pour tout $r \geq g$. Donc $dim(W_r) = min(r, g)$ et par suite on a : $W_g = J(C)$ et $dim(J(C)) = g$; d'où la preuve de la deuxième partie.

3. D'aprés le théorème (7) on peut conclure que θ est ample.

2.2.3.3 Application du théorème d'Abel-Jacobi

Le théorème d'Abel-Jacobi est beaucoup utilisé dans la détermination des degrés de points algébriques, sur certains courbes.
Par exemple, considèrons la courbe affine

$$C_1(5) : y^5 = x(x-1).$$

Théorème 9.

L'ensemble des points quadratiques sur $C_1(5)$ *est*

$$E = \left\{ \left(\frac{1}{2} \pm \sqrt{y^5 + \frac{1}{4}}, y \right) \mid y \in \mathbb{Q}^* \right\}.$$

Démonstration. Pour plus de détaille le lecteur pourra consulté [4].

Soit $R \in C_1(5)(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$ (le degré), avec $\bar{\mathbb{Q}}$ corps des nombres algébriques. Notons R_1, R_2 les conjugués de Galois de R, et travaillons avec $t = [R_1 + R_2 - 2P_\infty]$ qui est un point de $J_1(5) = \{m_j(P_0),\ 0 \leq m \leq 4\}$; donc $t = m_j(P_0)$ avec $0 \leq m \leq 4$. On remarque que $R \notin \{P_\infty, P_0, P_1\}$.
Pour le cas $m = 0$
$t = 0 \Rightarrow [R_1 + R_2 - 2P_\infty] = 0$, d'aprés le théorème d'Abel-Jacobi, il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + R_2 - 2P_\infty;$$

donc $f \in \mathcal{L}(2P_\infty)$ et par suite $f(x,y) = a_1 + a_2 y$ avec $a_2 \neq 0$ sinon un des R_i devrait être à ∞ .
Aux points R_i, on a $a_1 + a_2 y = 0$, d'où $y = \frac{a_1}{a_2}$. On sait que $y^5 = x(x-1)$, donc $(x - \frac{1}{2})^2 = y^5 + \frac{1}{4}$ et on obtient les solutions

$$\{R_1, R_2\} = \left\{ \left(\frac{1}{2} + \sqrt{-\frac{a_1^5}{a_2^5} + \frac{1}{4}} - \frac{a_1}{a_2} \right), \left(\frac{1}{2} - \sqrt{-\frac{a_1^5}{a_2^5} + \frac{1}{4}} - \frac{a_1}{a_2} \right) \right\}.$$

Pour $m = 1$
$t = j(P_0) \Rightarrow [R_1 + R_2 - 2P_\infty] = j(P_0 = [P_0 - P_\infty] = -j(P_1) = -[P_1 - P_\infty] = [-P_1 + P_\infty]$ donc

$[R_1 + R_2 + P_1 - 3P_\infty] = 0$, d'aprés le théorème d'Abel-Jacobi, il existe une fonction rationnelle ff définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + R_2 + P_1 - 3P_\infty;$$

donc $f \in \mathcal{L}(3P_\infty)$ et comme $f \in \mathcal{L}(2P_\infty) = f \in \mathcal{L}(3P_\infty)$ alors un des R_i devrait être égal à ∞ ce qui est absurde.
Ainsi l'ensemble des points quadratiques sur C est donné par $R_1 \, et \, R_2$.

□

Conclusion

Dans ce mémoire, après avoir défini les outils nécessaires et rappelé leurs propriétés, nous avons abordé la preuve du théorème d'Abel-Jacobi qui est scindée en quatres parties.
Dans la première partie de la preuve, nous avons montré l'existence d'une variété abélienne $J(C)$ appelée la jacobienne de C. Dans la deuxième partie, nous avons montré que si l'on étend linéairement l'application j au groupe des diviseurs sur C, on obtient un isomorphisme entre $Pic^0(C)$ et $J(C)$. Dans la troisième partie, nous avons prouvé que $dim(W_r) = min(r, g)$, $W_g = J(C)$ et $dim(J(C)) = g$, pour tout $r > 0$. Dans la quatrième et dernière partie, la preuve est facilitée par le théorème (7) qui nous a permis de conclure que θ est ample. Nous avons terminé ce document par une application du théorème d'Abel-Jacobi sur la détermination des points quadratiques sur la courbe affine $C_1(5)$: $y^5 = x(x-1)$.

Bibliographie

[1] Blake, I., Seroussi,G., and Nigel SMART. Elliptic Curves in Cryptography Cambrige University Press, 1999.

[2] Hartshorne, R., Algebraic Geometry, Springer-Verlag, New York, 1997, graduate texts in mathématics.

[3] Hindry, M., Silverman, J., Introduction to Diophantine Geometry, Springer-Verlag, New York, (2000), graduate texts mathématics, 201.

[4] Oumar, S., Points algébriques sur les courbes de Fermat (Thése de doctorat), 04 décembre 2000 à Denis Diderot.

[5] Perrin, D., *Géométrie Algébrique, Une introduction*, Savoirs Actuels. 2 ième édition, EDP Sciences/CNRS ÉDITIONS, 2001.

[6] Souad, B., INTRODUCTION AUX COURBES ELLIPTIQUES, souad 2016 introduction, 2016.