UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

ÉCOLE DOCTORALE : SCIENCES, TECHNOLOGIES ET INGÉNIERIE

UFR SCIENCES ET TECHNOLOGIES
DÉPARTEMENT DE MATHÉMATIQUES

THÈSE

DOMAINE :	SCIENCES ET TECHNOLOGIES
MENTION :	MATHÉMATIQUES ET APPLICATIONS
SPÉCIALITÉ :	MATHÉMATIQUES PURES
OPTION :	GÉOMÉTRIE ALGÉBRIQUE

Présentée par :

Moustapha CAMARA

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

Sujet de la thèse :

Application de la finitude du groupe de Mordell-Weil et du théorème de Chevalley-Weil sur la détermination des points algébriques de degré donné sur certaines courbes planes lisses

Directeur de thèse :	Oumar SALL	Professeur titulaire UASZ
Rapporteurs :	Mamadou SANGHARE	Professeur titulaire UCAD
	Amadou Lamine FALL	Professeur assimilé UCAD
	Marie Salomon SAMBOU	Professeur titulaire UASZ

Soutenue publiquement à l'UASZ le 02 Mars 2024 devant le jury composé de :

Président :	Mamadou SANGHARE	Professeur titulaire UCAD
Rapporteurs :	Marie Salomon SAMBOU	Professeur titulaire UASZ
	Amadou Lamine FALL	Professeur assimilé UCAD
	Mamadou SANGHARE	Professeur titulaire UCAD
Examinateurs :	Amoussou Thomas GUEDENON	Professeur assimilé UASZ
	Moussa FALL	Maître de Conf. titulaire UASZ
Directeur :	Oumar SALL	Professeur titulaire UASZ

Thèse effectuée au sein du Laboratoire de Mathématiques et Applications (LMA)
de l'UFR Sciences et Technologies de l'Université Assane Seck de Ziguinchor
BP : 523-Ziguinchor-Sénégal

Remerciements

C'est pour moi un immense plaisir d'exprimer ici toute ma gratitude et toute ma reconnaissance à tous ceux, de près ou de loin, qui ont contribué à l'aboutissement de cette thèse.

Je tiens tout d'abord à exprimer très sincèrement toute ma reconnaissance à l'endroit de mon Directeur de thèse le Professeur Oumar SALL, pour l'encadrement dont j'ai bénéficié de sa part depuis mon mémoire de Master 2 et tout au long de cette thèse. Il a su me guider avec une grande disponibilité et j'ai beaucoup appris à ses côtés. La réalisation de ce travail de recherche n'a été possible que grâce à ses explications claires, sa rigueur scientifique, sa patience et ses précieux conseils. Je le remercie infiniment.

Je suis honoré par la présence du Professeur Mamadou SANGHARE d'avoir bien voulu accepter de rapporter ma thèse et de présider le jury. J'exprime ma profonde gratitude aux Professeurs Marie Salomon SAMBOU et Amadou Lamine FALL pour avoir accepté d'être rapporteurs. Je les remercie pour leur lecture attentive et pour leurs remarques et suggestions qui m'ont aidé à clarifier et à mieux présenter les idées développées dans cette thèse.

Mes remerciements vont également à l'endroit du Professeur Amoussou Thomas GUEDENON et du Docteur Moussa FALL pour avoir accepté de participer au jury de ma thèse en qualité d'examinateurs. Je tiens à vous exprimer toute ma reconnaissance pour la qualité des échanges à chaque fois que je vous retrouve dans vos bureaux. Je suis vraiment honoré que vous fassiez partie des membres de jury de ma thèse.

J'adresse mes vives remerciements à 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, particulièrement aux Pr. Salomon SAMBOU, Pr. Oumar SALL, Pr. Amoussou Thomas GUEDENON, Pr. Diène NGOM, Pr. Edouard DIOUF, Pr. Clément MANGA, Dr. Daouda Niang DIATTA, Dr. Moussa FALL, Dr. Timack NGOM, Dr. Mansour SANE, Dr. Emmanuel Nicolas CABRAL et Dr. Mamadou Eramane BODIAN. Je n'oublie pas les professeurs de l'Université Cheikh Anta DIOP de Dakar particulièrement le Pr. Diaraf SECK et le Pr. Bacary MANGA.

Je souhaite remercier mes collègues du Laboratoire de Mathématiques et Applications de l'UASZ. C'était pour moi un immense plaisir d'exposer et d'assister aux différents exposés portant sur des sujets riches et variés. Merci à Souhaibou SAMBOU, Chérif Mamina COLY, Christophe Lopez NANGO, Seny DIATTA, Abdoulaye DIOUF, Papa BADIANE, Kang-Rang Seth KOUMLA, Pape Modou SARR, El Hadji SOW, Boubacar Sidy BALDE, Mohamadou Mor Diogou DIALLO, Nestor DJINTELBE, Ibrahima SANE, Jonathan DJELLA, Guillaume Itbadio

SADIO, Gorgui GACKOU, Modou NDOUR, Dieynaba SAMB, LALA DIEME, Fatou DIENG, Mamadou Korca BA, Aliou BA, Saliou DIAW, Seydi Diamil DIOUF, Lamine MANE etc. .

J'exprime aussi ma gratitude au Pr. Oumar SY du département de Géographie de l'UASZ et au Dr. Mamadou Lamine MBAYE du département de Physique de l'UASZ qui m'ont été d'une aide remarquable.

J'ai eu la chance de bénéficier des explications de Cécile ARMANA et de Christian MAIRE Professeurs à l'Université de Franche-Comté de France et de Tony EZOME Professeur à l'Ecole Normale Supérieure du Gabon. Qu'il me soit permis de les remercier pour les discussions que j'ai pu avoir avec eux mais aussi pour leur disponibilité, leurs conseils et leur gentillesse.

Mes remerciements à Monsieur Alassane TAMBOURA et à toute son équipe de m'avoir donné l'opportunité de mener nos travaux de reherches dans leur locaux. Je voudrais remercier aussi la famille SADIO et la famille FOFANA depuis Castor pour leur contribution remarquable.

Mes remerciements s'adressent aussi à mes amis dont les encouragements m'ont permis de ne pas dévier de mon objectif final. Merci à Ibrahima MBALLO, Raymond DIATTA, Lamine SAMBOU, David SAGNA, Fallou NGOM, Thierno SECK, Amadou DIOUF, Youssouph BADJI, Amadou DIEYE, Lamine TOURE, Abdoulaye SABALY, Hameth BA, Ousmane NDIAYE, Aboubacry LY, Amadou LY.

Pour terminer, je voudrais exprimer ma gratitude et ma reconnaissance à ma famille. Je remercie ma mère, ma femme, mes frères et sœurs pour leur patience, leur compréhension et leurs prières qui ont accompagné toutes ces années d'étude et de recherche.

Merci à toutes et à tous pour votre contribution à ma modeste personne !

Dédicace

J'ai une pensée particulière à des personnes qui me sont très chères, mais qui malheureusement nous ont quitté. Qu'Allah leur fasse miséricorde et leur accorde le plus haut degré du paradis. Ce modestre travail vous est entièrement dédié :

Mariame Samba GAYE
Alseyni CAMARA
Ibrahima CAMARA
Aldiouma Diallo CAMARA

Table des matières

Application de la finitude du groupe de Mordell-Weil et du théorème de Chevalley-Weil sur la détermination des points algébriques de degré donné sur certaines courbes planes lisses

Résumé.

Étant donné une courbe $\mathcal{C}$ plane lisse définie sur $\mathbb{Q}$ d'équation affine $f(x, y) = 0$. Nous nous sommes intéressés dans cette thèse à la détermination des points algébriques de degré donné sur $\mathcal{C}$. Les résultats obtenus peuvent être vus comme une paramétrisation des points de la courbe étudiée. Les travaux reposent sur deux méthodes. En effet, la première concerne les courbes dont le groupe de Mordell-Weil est fini, et la seconde celles dont l'hypothèse de la finitude du groupe de Mordell-Weil n'est pas envisagée. Dans cette dernière situation, on applique le théorème de Chevalley-Weil. Antérieurement, l'hypothèse de la finitude du groupe de Mordell-Weil semblait être une contrainte ; mais on a constaté que le théorème de Chevalley-Weil permet de contourner cette contrainte dans certains cas.
La finitude du groupe de Mordell-Weil nous a permis d'étendre les travaux de :

- Mulholland et Bruni qui décrivaient l'ensemble des points de degré 1 sur les courbes hyperelliptiques d'équations affines $y^2 = x^5+n^2$, avec $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Notre contribution a consisté à la détermination des points algébriques de degré au plus d sur les mêmes courbes.
- van der Heiden, Evink et Top qui ont donné l'ensemble des points de degré 1 sur les courbes hyperelliptiques d'équations affines $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$, avec $n \in \{1, 2, 3, q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Notre résultat principal décrit l'ensemble des points de degré au plus 3.
- Tzermias (resp. Sall) sur la septique de Fermat d'équation projective $X^7 + Y^7 + Z^7 = 0$ qui a décrit l'ensemble des points de degré au plus 5 (resp. au plus 10). Dans ce travail, nous avons donné l'ensemble des points de degré au plus 14.

La seconde méthode nous a permis de déterminer l'ensemble des points de petit degré sur $\mathbb{Q}$ sur les courbes d'équations affines $x^p + y^{pq} = 1$ avec p et q deux nombres premiers tels que $p \in \{5, 7, 11\}$ et $q \geq 5$.

Mots-clés : Points algébriques, degré d'un point algébrique, théorème de Mordell-Weil, théorème d'Abel-Jacobi, courbes hyperelliptiques, 2−descente, courbes de Fermat, théorème de Chevalley-Weil.

Application of the finiteness of the Mordell-Weil group and the Chevalley-Weil theorem on the determination of algebraic points of given degree on some smooth plane curves

Abstract.

Given a smooth plane curve $\mathcal{C}$ defined over $\mathbb{Q}$ by the affine equation $f(x, y) = 0$. In this thesis, we were interested in the determination of algebraic points of given degree on $\mathcal{C}$. The results obtained can be seen as a parameterization of the points of the studied curve. The work is based on two methods. Indeed, the first concerns curves for which the Mordell-Weil group is finite, and the second those for which the hypothesis of the finiteness of the Mordell-Weil group is not considered. In this last situation, we apply the Chevalley-Weil theorem. Previously, the hypothesis of the finiteness of the Mordell-Weil group seemed to be a constraint ; but we have found that the Chevalley-Weil theorem makes it possible to circumvent this constraint in some cases.

The finiteness of the Mordell-Weil group allowed us to extend the work of :

- Mulholland and Bruni who described the set of points of degree 1 on the hyperelliptic curves of affine equations $y^2 = x^5+n^2$, with $n \in \{4,\ 5,\ 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Our contribution consisted of determining the algebraic points of degree at most d on the same curves.
- van der Heiden, Evink and Top who gave the set of points of degree 1 on the hyperelliptic curves of affine equations $y^2 = x(x^2-n^2)(x^2-4n^2)$, with $n \in \{1,\ 2,\ 3, q$ a prime number and $q \equiv 7 \pmod{24}\}$. Our main result describes all the points of degree at most 3.
- Tzermias (resp. Sall) on Fermat's septic of projective equation $X^7 + Y^7 + Z^7 = 0$ who described the set of points of degree at most 5 (resp. at most 10). In this work, we have given the set of points of degree at most 14.

The second method allowed us to determine the set of points of small degree over $\mathbb{Q}$ on the curves of affine equations $x^p + y^{pq} = 1$ with p and q two prime numbers such that $p \in \{5, 7, 11\}$ and $q \geq 5$.

Keywords. Algebraic points, degree of an algebraic point, Mordell-Weil theorem, Abel-Jacobi theorem, hyperelliptic curves, 2−descent, Fermat curves, Chevalley-Weil theorem.

Introduction

La géométrie algébrique est une branche des mathématiques qui s'intéresse à l'étude des variétés algébriques, c'est-à-dire toutes celles qui sont définies par l'annulation d'un ou de plusieurs polynômes. Une équation diophantienne est une équation polynômiale

$$f(x, y) = 0,$$

à deux indéterminées à coefficients entiers dont on recherche les solutions rationnelles $(x, y) \in \mathbb{Q}^2$. L'étude des équations diophantiennes représente l'une des plus fortes attractions de la géométrie algébrique. Du point de vue géométrique, cela se traduit par la recherche des points rationnels appartenant à la courbe algébrique plane d'équation $f(x, y) = 0$. On remarque aisément que le problème est plus intéressant lorsqu'on remplace $\mathbb{Q}$ par un corps de nombres K. Les travaux de Hilbert et Hurwitz [HH90] semblent être les premiers résultats généraux concernant l'étude des points rationnels sur les courbes algébriques. En particulier, ils montrent que le bon paramètre pour étudier les points rationnels est le genre de la courbe et non le degré du polynôme définissant la courbe. Ils résolvent le cas des courbes de genre 0, c'est-à-dire celles qui sont birationnelles à la droite projective ou affine.

Poincaré [Poi01] traite le genre 1 (i.e., les courbes elliptiques), en expliquant le procédé de construction de solutions à partir de cordes ou tangentes : considérons une cubique plane lisse ; si P, Q sont deux points sur la cubique à coordonnées rationnelles, alors la droite passant par P et Q (si $P = Q$, on prend la tangente à la courbe) recoupe la cubique en un troisième point dont les coordonnées sont aussi rationnelles. En 1922, Mordell [Mor22] a démontré, dans son article consacré aux solutions rationnelles des équations du troisième ou quatrième degré à deux indéterminées, que toutes les solutions rationnelles sur la cubique peuvent se déduire d'un nombre fini d'entre elles par le procédé de cordes ou tangentes. Plus précisément, il a démontré que le groupe des points rationnels d'une courbe elliptique est un groupe abélien de type fini. Dans le même l'article, il a énoncé sa célèbre conjecture : une courbe projective lisse irréductible de genre $g \geq 2$ possède un nombre fini de solutions dans un corps de nombres donné.

Le mathématicien André Weil [Wei29] a généralisé dans sa thèse le théorème de Mordell en considérant une courbe de genre $g \geq 1$ définie sur un corps de nombres K. Autrement dit, si on note $J_{\mathcal{C}}$ la jacobienne d'une courbe $\mathcal{C}$ de genre $g \geq 1$ définie sur K, Weil a montré que le groupe $J_{\mathcal{C}}(K)$ des points rationnels de $J_{\mathcal{C}}$ est un groupe abélien de type fini. Toutefois, il n'a pas pu démontrer la conjecture de Mordell. Cette conjecture fut prouvée pour la première fois par Faltings [Fal83] en 1983.

Le genre d'une courbe est un invariant fondamental et l'une de ses fonctions est qu'il permet de classer les courbes algébriques. En effet, considérons $\mathcal{C}$ une courbe projective lisse irréductible

définie sur K de genre g. On note $\mathcal{C}(K)$ l'ensemble des points $K-$rationnels sur $\mathcal{C}$: il s'agit des points de la courbe $\mathcal{C}$ à coordonnées dans K. On a

- Si $g = 0$, alors $\mathcal{C}$ est isomorphe à $\mathbb{P}^1$; donc soit l'ensemble $\mathcal{C}(K)$ est vide, soit égal à $\mathbb{P}^1(K)$.
- Si $g = 1$, soit $\mathcal{C}(K)$ est vide, soit en fixant $P_0 \in \mathcal{C}(K)$, alors $(\mathcal{C}, P_0)$ est une courbe elliptique. Le théorème de Mordell [Mor22] dit que si $\mathcal{C}(K)$ est non vide, c'est un groupe abélien de type fini.
- Si $g \geq 2$, alors la situation se simplifie comme en atteste le théorème de Faltings qui affirme que l'ensemble $\mathcal{C}(K)$ est fini.

  Lorsque $g = 2$, $\mathcal{C}$ est une courbe hyperelliptique.

En 1989, une deuxième preuve de la conjecture de Mordell a été trouvée par Vojta [Voj91]. Ces preuves permettent de donner une borne supérieure à la cardinalité de l'ensemble $\mathcal{C}(K)$. Mais, elles sont inefficaces dans la mesure où elles ne peuvent pas être utilisées pour déterminer rigoureusement l'ensemble $\mathcal{C}(K)$. Néanmoins, il existe d'autres méthodes qui, jusqu'à présent n'ont pas réussi à prouver la conjecture de Mordell dans toute sa généralité. Ces méthodes ont tout de même réussi à déterminer dans de nombreux exemples l'ensemble $\mathcal{C}(K)$. Le premier résultat se trouve dans le travail de Chabauty [Cha41] qui a démontré la conjecture de Mordell dans le cas où le rang de la jacobienne est strictement inférieur au genre de la courbe. Puis, Coleman [Col85] a montré que la preuve de Chabauty peut être raffinée pour donner une borne supérieure explicite pour le nombre de points dans $\mathcal{C}(K)$ (voir [HS00, p. 426]). Dans certains cas, les estimations de Coleman sont suffisamment précises pour permettre de déterminer complètement $\mathcal{C}(K)$.

Soit $\mathcal{C}$ une courbe projective lisse irréductible définie sur $\mathbb{Q}$ de genre $g \geq 2$. Étant donné un corps de nombres K, on sait que depuis Faltings l'ensemble $\mathcal{C}(K)$ est fini. On note $\bigcup_{[K:\mathbb{Q}]\leqslant d} \mathcal{C}(K)$ l'ensemble des points $K-$rationnels sur $\mathcal{C}$ de degré au plus d. Le degré d'un point algébrique R sur $\mathcal{C}$ est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire, la dimension de $\mathbb{Q}(R)$ en tant que $\mathbb{Q}-$espace vectoriel. Lorsque $\dim_{\mathbb{Q}} \mathbb{Q}(R) = 1$ (resp. 2, 3, 4, ...), on dit que R est rationnel (resp. quadratique, cubique, quartique, ...) sur $\mathbb{Q}$.

Dans cette thèse, nous nous intéressons à la description explicite de l'ensemble

$$\bigcup_{[K:\mathbb{Q}]\leqslant d} \mathcal{C}(K),$$

pour certaines courbes planes lisses $\mathcal{C}$.

Cette thèse comprend trois chapitres et est organisée comme suit :

Le chapitre 1 présente des objets essentiels de notre sujet d'étude et leurs propriétés. Il est consacré, essentiellement, aux rappels sur des extensions de corps, des variétés algébriques, des diviseurs, des variétés abéliennes et des isogénies.

Le chapitre 2 est consacré à l'étude des points algébriques sur des courbes hyperelliptiques de genre 2. Il contient deux contributions. En effet, dans un premier temps, nous nous intéressons à la description explicite de l'ensemble des points algébriques de degré au plus d sur les courbes hyperelliptiques d'équations affines

$$y^2 = x^5 + n^2,$$

avec $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Ce travail étend les travaux de Mulholland [Mul06] et Bruni [Bru15] qui ont décrit l'ensemble des points $\mathbb{Q}-$rationnels sur les mêmes courbes. Cette première contribution représente une note publiée aux Annales Universitatis Paedagogicae Cracoviensis Studia Mathematica [CFS23a].

Le résultat principal est donné par le théorème suivant :

Théorème 0.0.1. Soit $n \in \{4,5,8,10,12,16,20,27,36,144,162,216,400,432,625,648,1250,1296,5000\}$. Soit la courbe

$$\mathcal{C}_{n^2} : y^2 = x^5 + n^2.$$

Alors

1. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 2 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(2)}(\mathbb{Q}) = \left\{ \left(x, \pm\sqrt{x^5+n^2} \right) \,:\, x \in \mathbb{Q}^* \right\}.$$
2. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 3 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(3)}(\mathbb{Q}) = \left\{ (x, \pm n - \lambda x^2) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } x^3 - \lambda^2 x^2 \pm 2\lambda n = 0 \right\}.$$
3. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 4 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(4)}(\mathbb{Q}) = \mathcal{A}_0^n \cup \mathcal{A}_1^n \cup \mathcal{A}_2^n$$
avec
$$\mathcal{A}_0^n = \left\{ \left(x, \pm\sqrt{x^5+n^2} \right) : [\mathbb{Q}(x):\mathbb{Q}] = 2 \right\};$$
$$\mathcal{A}_1^n = \left\{ \begin{array}{l} \left(x, \pm n - \lambda x - \mu x^2 \right) \,:\, \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ et } x \text{ racine de} \\ x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 \pm 2\mu n)x \pm 2\lambda n = 0 \end{array} \right\};$$
$$\mathcal{A}_2^n = \left\{ \begin{array}{l} \left(x, \pm n - \lambda x^2 - \mu x^3 \right) \,:\, \lambda,\, \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \mu^2 x^4 + (2\lambda\mu - 1)x^3 + \lambda^2 x^2 \mp 2\mu n x \mp 2\lambda n = 0 \end{array} \right\}.$$
4. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré au plus d avec $d \geq 5$ sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{d}(\mathbb{Q}) = \mathcal{D}_0^n \cup \mathcal{D}_1^n \cup \mathcal{D}_2^n \cup \mathcal{D}_3^n$$
avec
$$\mathcal{D}_0^n = \left\{ \left(x, \pm\sqrt{x^5+n^2} \right) : [\mathbb{Q}(x):\mathbb{Q}] \leq \frac{d}{2} \text{ si } d \text{ est pair} \right\};$$
$$\mathcal{D}_1^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\leq i\leq \frac{d}{2}} a_i x^i}{\sum\limits_{0\leq j\leq \frac{d-5}{2}} b_j x^j} \right) \,:\, a_{\frac{d}{2}} \neq 0 \text{ et } \exists\, b_j \neq 0 \text{ si } d \text{ est pair, } b_{\frac{d-5}{2}} \neq 0 \text{ si } d \\ \text{est impair et } x \text{ racine de } \Big(\sum\limits_{i=0}^{\frac{d}{2}} a_i x^i \Big)^2 - \Big(\sum\limits_{j=0}^{\frac{d-5}{2}} b_j x^j \Big)^2 (x^5+n^2) = 0 \end{array} \right\};$$
$$\mathcal{D}_2^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\leq i\leq \frac{d+1}{2}} a_i x^i}{\sum\limits_{0\leq j\leq \frac{d-4}{2}} b_j x^j} \right) \,:\, a_0 = \pm n b_0, a_{\frac{d+1}{2}} \neq 0 \text{ si } d \text{ est impair, } b_{\frac{d-4}{2}} \neq 0 \text{ si } d \\ \text{est pair et } x \text{ racine de } \Big(\sum\limits_{i=0}^{\frac{d+1}{2}} a_i x^i \Big)^2 - \Big(\sum\limits_{j=0}^{\frac{d-4}{2}} b_j x^j \Big)^2 (x^5+n^2) = 0 \end{array} \right\};$$
$$\mathcal{D}_3^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\leq i\leq \frac{d+2}{2}} a_i x^i}{\sum\limits_{0\leq j\leq \frac{d-3}{2}} b_j x^j} \right) \,:\, a_0 = \pm n b_0, a_1 = \pm n b_1, a_{\frac{d+2}{2}} \neq 0 \text{ si } d \text{ est pair, } b_{\frac{d-3}{2}} \neq 0 \\ \text{si } d \text{ est impair et } x \text{ racine de } \Big(\sum\limits_{i=0}^{\frac{d+2}{2}} a_i x^i \Big)^2 - \Big(\sum\limits_{j=0}^{\frac{d-3}{2}} b_j x^j \Big)^2 (x^5+n^2) = 0 \end{array} \right\}.$$

Dans un second lieu, nous étudions les points algébriques de degré au plus 3 sur les courbes hyperelliptiques d'équations affines

$$y^2 = x(x^2 - n^2)(x^2 - 4n^2),$$

avec $n \in \{1, 2, 3, q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Notre contribution étend les travaux de Heiden [Hei98], Evink [Evi20] et Evink et al. [EHT21] qui ont donné les points $\mathbb{Q}-$rationnels. Notre seconde contribution acceptée pour publication dans le proceedings of the Third Edition NLAGA-BIRS Symposium [CFS23c] s'énonce comme suit :

Théorème 0.0.2. Soit $n \in \{1, 2, 3, q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Soit la courbe

$$\mathcal{C}_n : y^2 = x(x^2 - n^2)(x^2 - 4n^2).$$

Alors, les points algébriques sur $\mathcal{C}_n$ de degré au plus 3 sur $\mathbb{Q}$ sont donnés par

$$\bigcup_{[K:\mathbb{Q}]\leqslant 3} \mathcal{C}_n(K) = \mathcal{C}_n(\mathbb{Q}) \cup \mathcal{B}^n \cup \mathcal{A}_0^n \cup \mathcal{A}_1^n \cup \mathcal{A}_2^n \cup \mathcal{A}_3^n \cup \mathcal{A}_4^n \cup \mathcal{A}_5^n$$

avec

$$\begin{aligned}
\mathcal{C}_n(\mathbb{Q}) &= \left\{P_0,\, P_n,\, \overline{P_n},\, P_{2n},\, \overline{P_{2n}},\, P_\infty\right\};\\
\mathcal{B}^n &= \left\{\left(x, \pm\sqrt{x(x^2-n^2)(x^2-4n^2)}\right) \,:\, x \in \mathbb{Q}\backslash\{0,\, \pm n,\, \pm 2n\}\right\};\\
\mathcal{A}_0^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ x^3 + (-\lambda^2 \mp n)x^2 + (\mp\lambda^2 n - 4n^2)x \pm 4n^3 = 0\end{array}\right\};\\
\mathcal{A}_1^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm 2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ x^3 + (-\lambda^2 \mp 2n)x^2 + (\mp 2\lambda^2 n - n^2)x \pm 2n^3 = 0\end{array}\right\};\\
\mathcal{A}_2^n &= \left\{\begin{array}{l}\left(x, \lambda x(x^2 - n^2)\right) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ \lambda^2 x^3 - x^2 - \lambda^2 n^2 x + 4n^2 = 0\end{array}\right\};\\
\mathcal{A}_3^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)(x \pm 2n)) : \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ \lambda^2 x^3 + (\pm 3\lambda^2 n - 1)x^2 + (2\lambda^2 n^2 \pm 3n)x - 2n^2 = 0\end{array}\right\};\\
\mathcal{A}_4^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)(x \mp 2n)) : \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ \lambda^2 x^3 + (\mp\lambda^2 n - 1)x^2 + (-2\lambda^2 n^2 \mp n)x + 2n^2 = 0\end{array}\right\};\\
\mathcal{A}_5^n &= \left\{\begin{array}{l}\left(x, \lambda x(x^2 - 4n^2)\right) : \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de}\\ \lambda^2 x^3 - x^2 - 4\lambda^2 n^2 x + n^2 = 0\end{array}\right\}.
\end{aligned}$$

Avant de présenter les contributions dans ce chapitre, nous commençons par introduire des notions de base essentielles sur l'arithmétique des courbes hyperelliptiques de genre 2.

Le chapitre 3 est composé de deux parties :

– La première partie concerne la septique de Fermat. Cette partie est centrée sur la description géométrique des points algébriques sur la septique de Fermat, c'est-à-dire, sur la courbe plane lisse de degré 7 d'équation projective

$$F_7 = \{(X,\, Y,\, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}.$$

Tzermias [Tze98] a déterminé l'ensemble des points algébriques sur F_7 de degré au plus 5 sur $\mathbb{Q}$ et Sall [Sal00a, Sal03] a étendu ces résultats en donnant une description géométrique des points algébriques sur F_7 de degré au plus 10 sur $\mathbb{Q}$. Nous donnons ici une extension de cette

description géométrique des points algébriques de degré au plus 14 sur $\mathbb{Q}$ sur la même courbe. Ce travail a fait l'objet d'une publication dans le Journal of the Nigerian Mathematical Society [FCS23].

Le résultat principal s'énonce de la manière suivante :

Théorème 0.0.3. Considérons la septique de Fermat

$$F_7 = \{(X, Y, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}.$$

1. Les points algébriques sur F_7 de degré 11 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞ et tangente en un des deux autres.
2. Les points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$
      (i) passant par deux des points a, b, ∞ ou par P et $\overline{P}$,
      (ii) tangente à F_7 en un des points a, b, ∞,
   (b) une cubique définie sur $\mathbb{Q}$ ayant a, b et ∞ comme points de contact d'ordre 3 en chacun de ces points,
   (c) une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme points de contact d'ordre 8 en chacun de ces points.
3. Les points algébriques sur F_7 de degré 13 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞,
   (b) une cubique définie sur $\mathbb{Q}$ tangente à F_7 en un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres.
4. Les points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$,
   (b) une cubique définie sur $\mathbb{Q}$
      (i) passant par l'un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres,
      (ii) tangente à F_7 en deux des points a, b, ∞ et ayant un point de contact d'ordre 3 avec l'autre,
   (c) une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme point de contact d'ordre 7 en chacun de ces points,
   (d) une quintique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 5 en un des points a, b, ∞ et d'ordre 8 en chacun des points P et $\overline{P}$,
   (e) une sextique définie sur $\mathbb{Q}$ ayant deux points de contact d'ordre 6 parmi les points a, b, ∞ et d'ordre 8 en chacun des points P et $\overline{P}$.

– La deuxième partie concerne des courbes d'équations affines $x^p + y^{pq} = 1$. Elle est dédiée à l'étude des points algébriques de petit degré sur les courbes d'équations affines

$$x^p + y^{pq} = 1,$$

avec $p \in \{5, 7, 11\}$ et $q \geq 5$. Les outils essentiels utilisés pour ce travail sont le théorème de Chevalley-Weil [HS00, p. 292] et les travaux de Gross et Rohrlich [GR78] qui ont déterminé l'ensemble des points algébriques sur la courbe $F_p : x^p + y^p = 1$ de degré au plus 2 sur $\mathbb{Q}$.

Nous déterminons explicitement l'ensemble des points algébriques sur $x^p + y^{pq} = 1$ de degré au plus 2 sur $\mathbb{Q}$. Ce travail a fait l'objet d'une publication dans le JP Journal of Algebra, Number Theory and Applications [CFS23b].

Le résultat principal s'énonce de la manière suivante :

Théorème 0.0.4. Soient p et q deux nombres premiers tels que $p \in \{5, 7, 11\}$ et $q \geq 5$. Considérons $\mathcal{C}_{p,q}$ la courbe d'équation affine

$$\mathcal{C}_{p,q} : x^p + y^{pq} = 1.$$

Alors

1. Les points $\mathbb{Q}-$rationnels sur $\mathcal{C}_{p,q}$ sont donnés par

$$\mathcal{C}_{p,q}(\mathbb{Q}) = \{a, b, \infty\}.$$

2. Les points algébriques sur $\mathcal{C}_{p,q}$ de degré 2 sur $\mathbb{Q}$ sont donnés par

$$\mathcal{C}^{(2)}_{p,\,q}(\mathbb{Q}) = \begin{cases} \{P, \overline{P}\} & \text{si} \quad q \equiv 1 \pmod 6 \\ \{Q, \overline{Q}\} & \text{si} \quad q \equiv 5 \pmod 6. \end{cases}$$

Chapitre 1

Préliminaires

Dans ce chapitre, nous passons en revue certaines notions fondamentales pour la compréhension de notre sujet d'étude. Le rappel portera essentiellement sur des extensions de corps et des variétés algébriques. Nous introduisons aussi quelques propriétés des courbes algébriques planes, des variétés abéliennes et des isogénies. Les corps considérés sont, sauf mention expresse du contraire, supposés commutatifs. On désigne par K un tel corps. Dans ce chapitre, on désignera par n un entier positif non nul.

1.1 Quelques notions sur la théorie de Galois

Dans cette section, nous nous sommes basés principalement sur [Voi02], [Mil22], [ZS60], [Mil20] et [Aud04].

1.1.1 Extensions et degré d'un corps

Définition 1.1.1. On dit qu'un corps L est une extension du corps K et l'on note L/K si K est un sous-corps de L.

Définitions 1.1.2. Soit L/K une extension de corps.

1. On dit qu'un élément x de L est algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$. Dans le cas contraire, on dit que x est transcendant sur K.
2. L'extension L est dite algébrique si tout élément de L est algébrique sur K.
3. Une clôture algébrique de K est une extension algébrique de K qui est algébriquement close. Un corps est dit algébriquement clos si tout polynôme non constant à coefficients dans ce corps admet une racine dans ce corps.
4. Lorsque qu'un élément x de L est algébrique sur K, il existe un unique polynôme unitaire $P_{\min,x,K} \in K[X]$ vérifiant $P_{\min,x,K}(x) = 0$ et de degré minimal. Ce polynôme est irréductible. Un tel polynôme $P_{\min,x,K}$ est appelé le polynôme minimal de x sur K. Les conjugués de x sont les racines de son polynôme minimal dans une clôture algébrique de K.
5. Soit A une partie de L. On définit l'extension de K engendrée par A comme l'intersection de tous les sous-corps de L qui contiennent à la fois K et A ; on la désigne par $K(A)$. C'est

le plus petit sous-corps de L contenant K et A.
Si $A = \{x_1, \ldots, x_n\}$, on écrit simplement $K(x_1, \ldots, x_n)$ au lieu de $K(\{x_1, \ldots, x_n\})$.

6. Une extension L/K est dite simple si $L = K(x)$ pour un certain élément x de L.

Si L/K est une extension de corps, alors L a une structure de $K-$espace vectoriel, où l'addition vectorielle est l'addition dans L et la multiplication par un scalaire $K \times L \longrightarrow L$ est la restriction à $K \times L$ de la multiplication dans L.

Définition 1.1.3. Soit L/K une extension de corps. On définit le degré de L/K comme étant la dimension de L en tant qu'espace vectoriel sur K. On le note par $[L : K]$. On dit que l'extension L/K est finie si le degré $[L : K]$ est fini ; sinon, on dit que l'extension L/K est infinie.

Si L est une extension de K et x un élément de L algébrique sur K, le K-espace vectoriel $K(x)$ a pour base $(1, x, x^2, \ldots, x^{d-1})$, où $d \in \mathbb{N}^*$ qui désigne le degré du polynôme minimal de x.

Voici quelques propriétés des extensions algébriques :

Propriétés 1.1.1.

a) Si L/K est une extension finie, alors L/K est algébrique.

b) Si L/K est une extension finie et x un élément de L, alors le degré du polynôme minimal de x divise le degré $[L : K]$ de l'extension.

c) Si A est une partie finie de L dont tous les éléments sont algébriques sur K, alors $K(A)/K$ est une extension finie.

Démonstration.

a) Soient $[L : K] = d < +\infty$ et $x \in L$. Alors, $1, x, x^2, \ldots, x^d$ sont $d+1$ éléments du $K-$espace vectoriel L et doivent donc être linéairement dépendants sur K. Il existe $a_0, a_1, \ldots, a_d \in K$ non tous nuls tels que
$$a_0 + a_1 x + \ldots + a_d x^d = 0.$$
Par conséquent, x est une racine du polynôme non nul $a_0 + a_1 X + \ldots + a_d X^d \in K[X]$; ce qui montre que x est algébrique sur K.

b) Soit d le degré du polynôme minimal de x. Alors
$$[L : K] = [L : K(x)] \cdot [K(x) : K] = [L : K(x)] \cdot d.$$

c) Par récurrence sur le cardinal de A et par multiplicativité des degrés, il suffit de le vérifier pour A réduit à un élément x. Dans ce cas, l'extension $K(A)/K$ est finie, de même degré que le polynôme minimal de x.

❑

Définitions 1.1.4.

1. Un polynôme à coefficients dans K est dit séparable s'il est premier avec sa dérivée, ou de façon équivalente, s'il n'a pas de racine multiple dans une clôture algébrique de K.
2. Un élément algébrique d'une extension L/K est dit séparable sur K s'il annule un polynôme séparable à coefficients dans K.
3. Une extension algébrique L/K est dite séparable si tous ses éléments sont séparables sur K.
4. On dit que K est parfait si tout polynôme irréductible à coefficients dans K est séparable.
5. Toute extension algébrique d'un corps parfait est séparable.

Définition 1.1.5. Une extension L/K est dite normale si elle est algébrique et si tout polynôme irréductible de $K[X]$ qui a une racine dans L se décompose en produits de polynômes linéaires dans $L[X]$.

Définition 1.1.6. Une extension L/K est dite galoisienne si elle est normale et séparable.

Définition 1.1.7. Soit L/K une extension galoisienne de corps.
L'ensemble des $K-$automorphismes de L forme un groupe pour la composition des applications noté $\mathrm{Gal}(L/K)$ et est appelé le groupe de Galois de l'extension L de K.

Exemples 1.1.1.

- $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ sont des extensions de corps.
- $i \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ car c'est une racine de $X^2+1 \in \mathbb{Q}[X]$.
- Le polynôme minimal de $\sqrt{-2}$ sur $\mathbb{Q}$ est $X^2+2 \in \mathbb{Q}[X]$. Ainsi, les $\mathbb{Q}-$conjugués de $\sqrt{-2}$ sont $\sqrt{-2}$ et $-\sqrt{-2}$.
- L'extension $\mathbb{C}/\mathbb{R}$ est normale. L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale car le polynôme irréductible $X^3-2 \in \mathbb{Q}[X]$ ne se décompose pas en produits de polynômes linéaires dans $\mathbb{Q}(\sqrt[3]{2})[X]$, en effet, le polynôme X^3-2 est irréductible sur $\mathbb{Q}$ mais a exactement une racine dans $\mathbb{Q}(\sqrt[3]{2})$ et les deux autres racines sont complexes.

1.1.2 Degré de transcendance

Définitions 1.1.8. Soient L/K une extension de corps et $\{x_1, \ldots, x_n\}$ une famille d'éléments de L.

1. La famille $\{x_1, \ldots, x_n\}$ est génératrice de L/K si $L = K(x_1, \ldots, x_n)$. Si une telle famille existe et est finie, on dit que L/K est une extension de type fini.
2. On dit que la famille $\{x_1, \cdots, x_n\}$ est algébriquement génératrice de L/K si L est algébrique sur $K(x_1, \cdots, x_n)$.
   On dit que la famille $\{x_1, \cdots, x_n\}$ est algébriquement indépendante sur K, si pour tout polynôme non nul $P \in K[X_1, \cdots, X_n]$, $P(x_1, \cdots, x_n) \neq 0$.
3. Si la famille $\{x_1, \cdots, x_n\}$ est algébriquement génératrice et algébriquement indépendante de L/K, on dit qu'elle est une base de transcendance de L/K.

Soit L/K une extension de type fini. Alors, il existe toujours une base de transcendance de L sur K ; toutes les bases de transcendances de L sur K ont même cardinal.

Définition 1.1.9. Soit L/K une extension de type fini. Le degré de transcendance de L/K est le cardinal d'une base de transcendance de L/K. Il est noté $\deg \mathrm{tr}(L/K)$.

1.1.3 Revêtement galoisien

Définition 1.1.10. Soit B un espace topologique. Un revêtement de B est la donnée d'un espace topologique E et d'une application continue $p : E \longrightarrow B$ ayant la propriété de trivialisation locale suivante : pour tout point b de B, il existe un voisinage V de b dans B, un espace discret non vide F et un homéomorphisme $\Phi : p^{-1}(V) \longrightarrow V \times F$ tels que le diagramme

$$\begin{array}{ccc} p^{-1}(V) & \xrightarrow{\Phi} & V \times F \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle p_1} & \\ & V & \end{array}$$

commute.

On dit que B est la base de p, E l'espace total, $p^{-1}(b)$ la fibre de E au dessus de b, p la projection de E sur B, V un voisinage ouvert trivialisant, Φ une trivialisation locale de p sur V.

Voici quelques propriétés des revêtements :

- La projection d'un revêtement est une application surjective.
- Si E est compact (resp. connexe, connexe par arcs), alors B est compact (resp. connexe, connexe par arcs).

Définition 1.1.11 (**Homomorphismes de revêtements**)**.** Soient $p : E \longrightarrow B$ et $p' : E' \longrightarrow B'$ deux revêtements. On appelle homomorphisme de p dans p' un couple d'applications continues $H : E \longrightarrow E'$ et $h : B \longrightarrow B'$ telles que le diagramme

$$\begin{array}{ccc} E & \xrightarrow{H} & E' \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p'} \\ B & \xrightarrow{h} & B' \end{array}$$

soit commutatif.

Un isomorphisme est un homomorphisme dans lequel H et h sont des homéomorphismes. Lorsque $E = E'$, $B = B'$ et $h = \mathrm{Id}$, on dit que H est un automorphisme. L'ensemble $\mathrm{Aut}(E)$ est l'ensemble des automorphismes de E.

Définition 1.1.12 (**Revêtement galoisien**)**.** Un revêtement $p : E \longrightarrow B$ est galoisien si E est connexe par arcs et si le groupe $\mathrm{Aut}(E)$ opère transitivement sur les fibres de E. Le revêtement est alors dit galoisien de groupe $\mathrm{Aut}(E)$.

Considérons maintenant K un corps parfait. Nous noterons $\overline{K}$ une clôture algébrique de K et $G_K = \mathrm{Gal}(\overline{K}/K)$ le groupe de Galois de $\overline{K}$ sur K.

1.2 Variétés algébriques

Il existe deux types de variétés algébriques, celles qui sont affines et celles qui sont projectives. Dans cette section et dans les deux sections suivantes, nous nous sommes basés essentiellemnt sur [HS00], [Per95], [Sil86], [Har77], [CLO15], [Sha94], [Mil06] et [Vel71].

1.2.1 Variétés algébriques affines

Définition 1.2.1 (**Espace affine**)**.** On appelle espace affine de dimension n sur $\overline{K}$ que l'on note par $\mathbb{A}^n$ ou encore $\mathbb{A}^n(\overline{K})$ l'ensemble

$$\mathbb{A}^n = \{x = (x_1, \cdots, x_n) \,|\, x_i \in \overline{K}\}.$$

Les espaces $\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite et plan affine. Un point a de $\mathbb{A}^n$ est dit zéro de $f \in \overline{K}[X_1, \ldots, X_n]$ si $f(a) = 0$. L'ensemble des points $K-$rationnels de $\mathbb{A}^n$ est l'ensemble

$$\mathbb{A}^n(K) = \{x = (x_1, \cdots, x_n) \,|\, x_i \in K\}.$$

Le groupe de Galois G_K agit sur $\mathbb{A}^n$ en agissant sur les coordonnées : pour tout $\sigma \in G_K$ et $x = (x_1, \cdots, x_n) \in \mathbb{A}^n$, on a

$$x^\sigma = (x_1^\sigma, \cdots, x_n^\sigma).$$

Alors $\mathbb{A}^n(K)$ peut être caractérisé par

$$\mathbb{A}^n(K) = \{x \in \mathbb{A}^n : x^\sigma = x \text{ pour tout } \sigma \in G_K\}.$$

Définition 1.2.2. Soit $S \subseteq \overline{K}[X_1, \ldots, X_n]$. On pose

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

On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S. On notera dans le cas d'un ensemble fini, $\mathcal{V}(f_1, \ldots, f_r)$ au lieu de $\mathcal{V}(\{f_1, \ldots, f_r\})$.

Définition 1.2.3. Soit $f \in \overline{K}[X_1, \ldots, X_n]$ non constant. On appelle hypersurface définie par f, et l'on note $\mathcal{V}(f)$, l'ensemble des zéros de f. Explicitement, on a

$$\mathcal{V}(f) = \{a \in \mathbb{A}^n \mid f(a) = 0\}.$$

Lorsque f est de degré d, on dit que l'hypersurface $\mathcal{V}(f)$ est de degré d.

Cas particuliers d'hypersurfaces :

- Si $n = 2$, on obtient $\mathcal{V}(f) = \{a \in \mathbb{A}^2 \mid f(a) = 0\}$, une telle hypersurface est appelée courbe affine plane.
  Une courbe affine plane est dite conique, cubique, quartique, quintique ... si le degré de f est respectivement 2, 3, 4, 5 ...
- Si $\deg(f) = 1$, l'hypersurface $\mathcal{V}(f) = \{a \in \mathbb{A}^n \mid f(a) = 0\}$ est appelée hyperplan affine.

Pour tout $S \subset \overline{K}[X_1, \ldots, X_n]$, on désigne $\langle S \rangle$ l'idéal engendré par S défini par

$$\langle S \rangle = \Big\{ \sum_{i=1}^{r} h_i f_i \,|\, f_i \in S \text{ et } h_i \in \overline{K}[X_1, \ldots, X_n] \Big\}.$$

Alors, on a $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$. Ainsi, l'étude des ensembles algébriques affines se ramène à l'étude des idéaux de $\overline{K}[X_1, \ldots, X_n]$; or ce dernier étant neothérien, tout idéal est de type fini. Donc, tout ensemble algébrique affine est défini par un nombre fini d'équations : $\mathcal{V}(S) = \mathcal{V}(f_1, \ldots, f_r)$, où $f_i \in S$.

Proposition 1.2.1.

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

Cette proposition nous permet d'énoncer la définition suivante :

Définition 1.2.4. Les ensembles algébriques affines de $\mathbb{A}^n$ définissent une topologie sur $\mathbb{A}^n$, dite topologie de Zariski, dont ils sont les fermés.

Soient $f \in \overline{K}[X_1, \ldots, X_n]$ et $\mathcal{V}(f)$ l'hypersurface définie par f. L'ensemble

$$D(f) = \mathbb{A}^n - \mathcal{V}(f) = \{a \in \mathbb{A}^n \mid f(a) \neq 0\}$$

est un ouvert de Zariski de $\mathbb{A}^n$, dit ouvert standard. Les ouverts standards forment une base d'ouverts pour la topologie de Zariski ; plus précisément, tout ouvert est réunion finie d'ouverts standards.

La topologie de Zariski sur une partie V de $\mathbb{A}^n$ est la topologie induite par la topologie de Zariski sur $\mathbb{A}^n$ dont les fermés sont les $V \cap \mathcal{V}(S)$. En particulier, si V est un ensemble algébrique affine, alors les fermés sont les ensembles algébriques affines contenus dans V. Toutefois, la topologie de Zariski est très différente des topologies usuelles. Pour simplifier, disons que les fermés y sont très petits : dans $\mathbb{A}^3$ les fermés sont les surfaces, les courbes ou les points (comparer aux boules fermés des topologies usuelles). Au contraire, les ouverts sont très gros, ainsi, deux ouverts non vides se rencontrent ; il s'ensuit que la topologie de Zariski sur $\mathbb{A}^n$ n'est pas séparée.

Définitions 1.2.5. Soit E un espace topologique non vide. On dit que E est irréductible s'il n'est pas réunion de deux fermés distincts de E. Autrement dit,

$$E \text{ irréductible } \Leftrightarrow [E = F_1 \cup F_2 \ (F_i \text{ fermé de } E) \Rightarrow E = F_1 \text{ ou } E = F_2]$$

On vérifie que si E est non vide, E est irréductible si, et seulement si deux ouverts non vides quelconques se rencontrent, c'est-à-dire si, et seulement si tout ouvert non vide est dense. Un ensemble algébrique affine est dit irréductible s'il est irréductible pour la topologie de Zariski. Si un ensemble algébrique affine n'est pas irréductible, on dit qu'il est réductible et donc on peut le décomposer en composantes irréductibles comme ci-dessous.

Théorème 1.2.1. Tout ensemble algébrique affine non vide V se décompose de façon unique (à permutation près) en une réunion finie d'ensembles algébriques affines irréductibles $V_1, \ldots, V_p$, non contenus l'un dans l'autre. Les $V_1, \ldots, V_p$ sont appelés les composantes irréductibles de V.

Définition 1.2.6. On appelle variété algébrique affine tout ensemble algébrique affine irréductible.

1.2.2 Idéal d'un ensemble algébrique affine et Nullstellensatz de Hilbert

Dans cette section, nous allons explorer la coorespondance entre l'algèbre des polynômes (i.e., les idéaux de $\overline{K}[X_1, \ldots, X_n]$) et la géométrie (i.e., les ensembles algébriques de $\mathbb{A}^n$). Cette coorespondance établit un dictionnaire permettant de traduire les propriétés algébriques en propriétés géométriques et inversement. Commençons par définir une application $\mathfrak{I}$, essentiellement duale de $\mathcal{V}$, qui associe à un ensemble de points un idéal de l'anneau de polynômes.

Définition 1.2.7 (**Idéal d'un ensemble de points**)**.**
Soit V une partie de $\mathbb{A}^n$. On appelle idéal de V dans $\mathbb{A}^n$, l'ensemble noté $\mathfrak{I}(V)$ défini par

$$\mathfrak{I}(V) = \{f \in \overline{K}[X_1, \ldots, X_n] \ : \ \forall\, a \in V,\ f(a) = 0\}$$

qui est un idéal de $\overline{K}[X_1, \ldots, X_n]$. On dit qu'un ensemble algébrique affine V est défini sur K si $\mathfrak{I}(V)$ peut être engendré par des polynômes à coefficients dans K.

On appelle radical d'un idéal I de $\overline{K}[X_1, \ldots, X_n]$, l'ensemble noté $\sqrt{I}$ défini par

$$\sqrt{I} = \{f \in \overline{K}[X_1, \ldots, X_n] \ : \ \exists\, m \in \mathbb{N}^*,\ f^m \in I\}.$$

Un idéal I est dit idéal radical si $\sqrt{I} = I$. Notons que les idéaux premiers satisfont $\sqrt{I} = I$.

Nous avons deux applications :

$$\mathcal{V} : \Big\{\text{idéaux de } \overline{K}[X_1, \ldots, X_n]\Big\} \longrightarrow \Big\{\text{ensembles algébriques affines de } \mathbb{A}^n\Big\},\ I \longmapsto \mathcal{V}(I)$$

et

$$\mathfrak{I} : \Big\{\text{ensembles algébriques affines de } \mathbb{A}^n\Big\} \longrightarrow \Big\{\text{idéaux de } \overline{K}[X_1, \ldots, X_n]\Big\},\ V \longmapsto \mathfrak{I}(V).$$

Ces deux applications nous donnent une correspondance entre les idéaux et les ensembles algébriques affines. Nous allons analyser cette correspondance. Pour tout ensemble algébrique affine V, on peut vérifier que $\mathcal{V}(\mathfrak{I}(V)) = V$, c'est-à-dire, l'application $\mathfrak{I}$ est injective. Réciproquement, pour tout idéal I, on a $I \subset \mathfrak{I}(\mathcal{V}(I))$, mais en général il n'y a pas égalité. Il y a une obstruction à cela. En effet, deux idéaux différents peuvent donner le même ensemble, par exemple si $n = 2$, $I =< X, Y >$ et $J =< X^2, Y >$, alors $\mathcal{V}(I) = \mathcal{V}(J) = \{(0, 0)\}$.

La relation entre I et $\mathfrak{I}(\mathcal{V}(I))$ est dû à Hilbert appelée Nullstellensatz de Hilbert (où Théorème des zéros de Hilbert).

Théorème 1.2.2 (**Nullstellensatz de Hilbert**). Pour tout idéal I de $\overline{K}[X_1, \ldots, X_n]$.

1) Si I est un idéal propre, alors $\mathcal{V}(I)$ est non vide.
2) Alors, on a $\mathfrak{I}(\mathcal{V}(I)) = \sqrt{I}$.

Dans le Nullstellensatz de Hilbert, si on se restreint aux idéaux radicaux, nous obtenons $\mathfrak{I}(\mathcal{V}(I)) = I$ et par conséquent, les applications $\mathcal{V}$ et $\mathfrak{I}$ deviennent inverses l'une de l'autre et définissent donc une bijection entre les ensembles algébriques affines et les idéaux radicaux. Le Nullstellensatz a donc permis d'établir un dictionnaire entre la géométrie et l'algèbre. Et voici quelques exemples.

1) Les ensembles suivants sont équivalents :
   a) {ensembles algébriques affines irréductibles de $\mathbb{A}^n$} ;
   b) {idéaux premiers de $\overline{K}[X_1, \ldots, X_n]$}.
2) Les ensembles suivants sont équivalents :
   a) {les points de $\mathbb{A}^n$} ;
   b) {idéaux maximaux de $\overline{K}[X_1, \ldots, X_n]$}.

Définition 1.2.8 (**Fonction régulière**). Soit $V \subset \mathbb{A}^n$ un ensemble algébrique affine. Une fonction $f : V \longrightarrow \overline{K}$ est dite régulière (ou polynômiale) s'il existe un polynôme $P \in \overline{K}[X_1, \ldots, X_n]$ tel que $f(x) = P(x)$ pour tout $x \in V$.

Nous soulignons que deux polynômes $P, Q \in \overline{K}[X_1, \ldots, X_n]$ représentent la même fonction régulière si, et seulement si, $P - Q \in \mathfrak{I}(V)$. L'ensemble des fonctions régulières sur V forme un anneau et même une $\overline{K}-$algèbre. Cet anneau est noté $\overline{K}[V]$ et est appelé l'anneau de coordonnées de V.

Considérons l'homomorphisme surjectif d'anneaux suivant

$$\overline{K}[X_1, \ldots, X_n] \longrightarrow \overline{K}[V], \quad f \longmapsto f_{|V}$$

où $f_{|V}$ représente la restriction de f à V dont le noyau est $\mathfrak{I}(V)$. Ainsi, d'après le premier théorème d'isomorphisme, on a

$$\overline{K}[V] \cong \overline{K}[X_1, \ldots, X_n]/\mathfrak{I}(V).$$

Avec cet isomorphisme, on peut traduire les propriétés géométriques exprimées en fonction de $\mathfrak{I}(V)$ en propriétés exprimées en fonction de $\overline{K}[V]$. Nous avons :

1) Les énoncés suivants sont équivalents :
   a) V irréductible ;
   b) $\mathfrak{I}(V)$ premier ;
   c) $\overline{K}[V]$ intégre.
2) Les énoncés suivants sont équivalents :
   a) V est un singleton ;
   b) $\mathfrak{I}(V)$ est maximal ;
   c) $\overline{K}[V] = \overline{K}$.

Définitions 1.2.9. Soit $V \subset \mathbb{A}^n$ une variété affine.
Le corps de fonctions $\overline{K}(V)$ de V est le corps des fractions de $\overline{K}[V]$. La dimension de V, notée $\dim(V)$, est le degré de transcendance de $\overline{K}(V)$ sur $\overline{K}$. La dimension d'un ensemble algébrique affine est le maximum des dimensions de ses composantes irréductibles.

Exemple 1.2.1.

- Si $V = \mathbb{A}^n$, alors $\overline{K}(\mathbb{A}^n) = \overline{K}(X_1, \ldots, X_n)$ et donc $\dim(\mathbb{A}^n) = n$.
- Si $V \subset \mathbb{A}^n$ est donnée par une seule équation polynômiale non constante $f(X_1, \ldots, X_n) = 0$, alors $\dim(V) = n - 1$.
  La variété affine V est une courbe algébrique affine si $\dim(V) = 1$, et une surface algébrique affine si $\dim(V) = 2$.

Définition 1.2.10 (**Application régulière**)**.** Soient $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ des ensembles algebriques affines et $\varphi : V \longrightarrow W$ une application, que l'on peut ecrire $\varphi = (\varphi_1, \ldots, \varphi_m)$ avec $\varphi_i : V \longrightarrow \overline{K}$. On dit que φ est régulière (ou un morphisme) si ses composantes φ_i sont polynomiales (i.e., sont dans $\overline{K}[V]$).

Définition 1.2.11 (**Ensembles algébriques affines isomorphes**)**.** Une application régulière $\varphi : V \longrightarrow W$ est un isomorphisme s'il existe une application régulière $\psi : W \longrightarrow V$ telle que $\psi \circ \varphi = \mathrm{id}_V$ et $\varphi \circ \psi = \mathrm{id}_W$. On dit que deux ensembles algébriques affines sont isomorphes s'il existe un isomorphisme entre eux.

Exemple 1.2.2.

- Soit la parabole $V = \mathcal{V}(y - x^2)$. L'application $f : V \longrightarrow \overline{K}$ définie par $f(x, y) = x$ est régulière. L'application f est bijective ; son inverse $x \longmapsto (x, x^2)$ est aussi régulière. Il en résulte que f est un isomorphisme.
- Soit $V = \mathcal{V}(y^2 - x^3)$ une variété algébrique affine. Considérons l'application suivante $f : \overline{K} \longrightarrow V$ définie par $f(x) = (x^2, x^3)$. L'application f est un morphisme bijectif, mais ce n'est pas un isomorphisme.

1.2.3 Variétés algébriques projectives

La géométrie affine peut se révéler insuffisante pour bien comprendre des problèmes de nature géométrique. Par exemple, on veut que les types d'énoncés suivants soient vrais : deux droites distinctes du plan se rencontrent en un point ; une droite rencontre une conique en deux points (comptés avec multiplicités) etc.. Il est clair que ces affirmations sont fausses dans le plan $\mathbb{A}^2$, puisque les droites parallèles ne se rencontrent jamais. Afin de les rendre vraies, nous introduisons l'espace projectif.

Considérons la relation $\mathcal{R}$ sur $\mathbb{A}^{n+1} - \{0\}$ définie par : pour tous vecteurs non nuls x et y, nous avons

$$x \mathcal{R} y \iff \exists\, \lambda \in \overline{K}^* : y = \lambda x.$$

La relation $\mathcal{R}$ ainsi définie est une relation d'équivalence sur $\mathbb{A}^{n+1} - \{0\}$.

Définition 1.2.12 (**Espace projectif**)**.** On appelle espace projectif de dimension n sur $\overline{K}$, noté $\mathbb{P}^n$ ou $\mathbb{P}^n(\overline{K})$, l'ensemble des classes d'équivalence par $\mathcal{R}$. En symbole, on a

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

En d'autres termes, $\mathbb{P}^n$ est l'ensemble des droites vectorielles de $\mathbb{A}^{n+1}$. Si $P \in \mathbb{P}^n$, tout représentant de P est un vecteur directeur de P. Si un point $P \in \mathbb{P}^n$ a pour vecteur directeur $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} - \{0\}$, on écrit $P = (x_0 : \ldots : x_n)$; on dit $(x_0 : \ldots : x_n)$ est un système de coordonnées homogènes de P et ils ne sont définis qu'à multiplication par un scalaire non nul près. Les espaces $\mathbb{P}^1$ et $\mathbb{P}^2$ sont appelés respectivement droite projective et plan projectif.

Le groupe de Galois G_K agit sur $\mathbb{P}^n$ en agissant sur les coordonnées : pour tout $\sigma \in G_K$ et $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n$, on a

$$P^\sigma = (x_0^\sigma : \ldots : x_n^\sigma).$$

L'ensemble des points $K-$rationnels de $\mathbb{P}^n$, noté par $\mathbb{P}^n(K)$, est l'ensemble

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n : P^\sigma = P \text{ pour tout } \sigma \in G_K\}.$$

Pour définir les ensembles algébriques projectifs, nous procédons de manière analogue à la définition des ensembles algébriques affines, sauf que dans l'espace projectif, nous utilisons des polynômes homogènes. En effet, la valeur d'un polynôme $F \in \overline{K}[X_0, \ldots, X_n]$ au point $P \in \mathbb{P}^n$ dépend du système de coordonnées homogènes. Un polynôme $F \in \overline{K}[X_0, \ldots, X_n]$ est dit homogène de degré d si pour tout $\lambda \in \overline{K}$, on a

$$F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n).$$

Par suite, le polynôme F s'annule en $P = (x_0 : \ldots : x_n)$ si, et seulement si $F(\lambda x_0, \ldots, \lambda x_n) = 0$ pour tout $\lambda \in \overline{K}^*$. On dit que $P = (x_0 : \ldots : x_n)$ est un zéro de F, et on notera $F(x_0, \ldots, x_n) = 0$.

Définition 1.2.13. Soit S une partie de $\overline{K}[X_0, \ldots, X_n]$ formée de polynômes homogènes. On pose :

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

On dit que $\mathcal{V}(S)$ est l'ensemble algébrique projectif défini par S.

Définition 1.2.14. On appelle hypersurface définie par un polynôme homogène F, notée $\mathcal{V}(F)$, l'ensemble des zéros de F. L'hypersurface $\mathcal{V}(F)$ est de degré d, si F est de degré d.

Cas particuliers d'hypersurfaces : Soit l'hypersurface $\mathcal{V}(F) = \{P \in \mathbb{P}^n \mid F(P) = 0\}$.

- Si $n = 2$, on obtient $\mathcal{V}(F) = \{P \in \mathbb{P}^2 \mid F(P) = 0\}$, une telle hypersurface est appelée courbe projective plane.
  Une courbe projective plane est dite conique, cubique, quartique, quintique ... si le degré de F est respectivement 2, 3, 4, 5 ...
- Si $\deg(F) = 1$, l'hypersurface $\mathcal{V}(F) = \{P \in \mathbb{P}^n \mid F(P) = 0\}$ est appelée hyperplan projectif.

De la même façon que le cadre affine, les ensembles algébriques projectifs définissent une topologie sur $\mathbb{P}^n$, dite de Zariski. Notons aussi les notions d'irréductibilité et des composantes irréductibles des ensembles algébriques projectifs sont définies comme dans le cas affine.

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

$$\mathfrak{I}(V) = \{F \in \overline{K}[X_0, \ldots, X_n] \text{ homogène } :\ \forall\ P \in V,\ F(P) = 0\},$$

qui est un idéal homogène de $\overline{K}[X_0, \ldots, X_n]$, c'est-à-dire engendré par des polynômes homogènes, ou encore, si les composantes homogènes de tout polynôme dans l'idéal est à nouveau dans l'idéal. On dit qu'un ensemble algébrique projectif V est défini sur K si $\mathfrak{I}(V)$ peut être engendré par des polynômes homogènes à coefficients dans K.

La coorespondance entre les ensembles algébriques projectifs et les idéaux homogènes est similaire à la correspondance affine. La différence notable est l'existance d'un idéal irrelevant (ou inconvenant), à savoir l'ideal I_0 engendré par $X_0, \ldots, X_n$. Notons que I_0 définit le sous-ensemble vide de $\mathbb{P}^n$.

Nous avons le théorème suivant.

Théorème 1.2.3 (Nullstellensatz de Hilbert). Soit I un idéal homogène de $\overline{K}[X_0, \ldots, X_n]$.
1) $\mathcal{V}(I) = \emptyset \iff \langle X_0, \ldots, X_n \rangle \subset \sqrt{I}$.
2) Si $\mathcal{V}(I) \neq \emptyset$, alors on a $\mathfrak{I}(\mathcal{V}(I)) = \sqrt{I}$.

Remarque 1.2.1. Soulignons que pour un ensemble algébrique projectif V, les éléments de $\overline{K}[V]$ ne définissent pas des fonctions sur V à valeurs dans $\overline{K}$ même dans le cas le plus simple, c'est-à-dire les polynômes homogènes. Toutefois, si F et H sont des éléments homogènes de $\overline{K}[V]$ de même degré, alors le quotient F/H définit une fonction sur l'ouvert où H ne s'annule pas. Ainsi, seuls les éléments constants de $\overline{K}[V]$ qui sont des fonctions sur V à valeurs dans $\overline{K}$.

Définitions 1.2.16. Soient X une variété projective et x un point de X. Une fonction $f : X \to \overline{K}$ est dite régulière en x, s'il existe des polynômes homogènes F et H de même degré tels que $f = F/H$ avec $H(x) \neq 0$ dans un voisinage de x dans X. On dit que f est régulière sur X, si elle l'est en tout point de X.

Définition 1.2.17. Soient X et Y des variétés projectives. On dit qu'une application $u : X \to Y$ est régulière si elle est continue et si, pour tout ouvert U de Y et toute fonction régulière $f : U \to \overline{K}$, la composée $f \circ u$ est régulière sur $u^{-1}(U)$.

Définition 1.2.18. Soient X et Y deux variétés. On considère les couples (u, U), où U est un ouvert dense de X et $u : U \to Y$ une application régulière. On dit que de tels 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. Une fonction rationnelle sur X est une application rationnelle de X à valeurs dans $\overline{K}$.

Proposition 1.2.2. Soient $\mathcal{C}$ une courbe, $V \subset \mathbb{P}^n$, $P \in \mathcal{C}$ un point lisse et $\phi : \mathcal{C} \to V$ une application rationnelle. Alors ϕ est régulière en P. En particulier, si $\mathcal{C}$ est lisse, alors ϕ est un morphisme.

Théorème 1.2.4. Soit $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ un morphisme de courbes. Alors ϕ est soit constant, soit surjectif.

Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux courbes définies sur K et soit $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ une application rationnelle non constante définie sur K. Alors, la composition avec ϕ induit une injection de corps de fonctions fixant K,

$$\phi^* : K(\mathcal{C}_2) \to K(\mathcal{C}_1), \qquad f \mapsto \phi^*(f) = f \circ \phi.$$

Pour toute application rationnelle ϕ telle que définie précédemment, le corps de fonctions $K(\mathcal{C}_1)$ est une extension de corps finie de $\phi^*(K(\mathcal{C}_2))$, ce qui nous permet de définir le degré de cette application ϕ.

Définition 1.2.19. Soit $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ une application de courbes définie sur K. Si ϕ est constante, on définit le degré de ϕ comme étant 0 ; sinon on dit que ϕ est une application finie et on définit son degré comme étant

$$\deg(\phi) = [K(\mathcal{C}_1) : \phi^*(K(\mathcal{C}_2))].$$

Nous explicitons maintenant les liens entre les courbes algébriques affines et les courbes algébriques projectives. Pour ce faire, nous commençons par donner la description classique de $\mathbb{P}^2$ comme union d'un espace affine $\mathbb{A}^2$ et d'un hyperplan à l'infini.

Considérons les ensembles U_2 et L_∞ définis par

$$U_2 = \{(X : Y : Z) \in \mathbb{P}^2 \mid Z \neq 0\} \text{ et } L_\infty = \{(X : Y : Z) \in \mathbb{P}^2 \mid Z = 0\}.$$

On introduit les coordonnées x, y telles que

$$x = \frac{X}{Z} \text{ et } y = \frac{Y}{Z}.$$

L'application définie par

$$\phi_2 : \mathbb{A}^2 \to U_2, \ \ (x, y) \mapsto (x : y : 1)$$

est une bijection dont la réciproque est

$$\phi_2^{-1} : U_2 \to \mathbb{A}^2, \ \ (X : Y : Z) \mapsto \Big(\frac{X}{Z}, \frac{Y}{Z}\Big).$$

On définit aussi une bijection avec l'application

$$\psi : \mathbb{P}^1 \to L_\infty, \ \ (X : Y) \mapsto (X : Y : 0).$$

Puisque $\mathbb{P}^2 = U_2 \cup L_\infty$, on obtient une description de $\mathbb{P}^2$ comme réunion disjointe du plan affine $\mathbb{A}^2$ et de l'hyperplan à l'infini L_∞. Les élément de L_∞ sont appelés points à l'infini.

De la même manière que U_2, on peut définir d'autres sous-ensembles de $\mathbb{P}^2$ tels que

$$U_0 = \{(X : Y : Z) \in \mathbb{P}^2 \,|\, X \neq 0\} \text{ et } U_1 = \{(X : Y : Z) \in \mathbb{P}^2 \,|\, Y \neq 0\}.$$

et des bijections

$$\phi_0^{-1} : U_0 \to \mathbb{A}^2, \ \ (X : Y : Z) \mapsto \Big(\frac{Y}{X}, \frac{Z}{X}\Big) \text{ et } \phi_1^{-1} : U_1 \to \mathbb{A}^2, \ \ (X : Y : Z) \mapsto \Big(\frac{X}{Y}, \frac{Z}{Y}\Big).$$

Les applications ϕ_j^{-1} permettent d'identifier le plan affine $\mathbb{A}^2$ avec un ouvert U_j de $\mathbb{P}^2$. Notons que la réunion des U_j récouvre $\mathbb{P}^2$. Il suit qu'une courbe projective $\mathcal{C}$ d'équation $F(X, Y, Z) = 0$ est la réunion de trois courbes planes $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2$ avec $\mathcal{C}_j = \mathcal{C} \cap U_j$. Lorsque nous identifions U_j avec $\mathbb{A}^2$, alors $\mathcal{C}_0$, $\mathcal{C}_1$ et $\mathcal{C}_2$ s'identfient avec les courbes affines définies respectivement par les polynômes

$$f_0(Y, Z) = F(1, Y, Z), \ f_1(X, Z) = F(X, 1, Z) \ \text{ et } \ f_2(X, Y) = F(X, Y, 1).$$

Le processus de remplacement du polynôme $F(X, Y, Z)$ par le polynôme $f_0(Y, Z)$, $f_1(X, Z)$ ou $f_2(X, Y)$ est appelé déshomogénéisation suivant respectivement X, Y et Z. Ce processus peut être inversé. Pour tout polynôme non nul $f(X, Y) \in \overline{K}[X, Y]$, on définit

$$F(X, Y, Z) = Z^d f\Big(\frac{X}{Z}, \frac{Y}{Z}\Big),$$

avec $\deg(f) = d$. On dit que F est l'homogénéisé de f par rapport à Z.

Le passage d'une courbe affine en une courbe projective peut se faire en homogénéisant le polynôme qui la définit. Inversement, le passage d'une courbe projective en une courbe affine peut se faire en déshomogénéisant le polynôme qui la définit.

1.3 Quelques propriétés des courbes algébriques planes

1.3.1 Multiplicités, courbes lisses et anneaux locaux

Définition 1.3.1 (**Multiplicité d'une courbe affine à l'origine**).
Soit $\mathcal{C} = \mathcal{V}(f)$ une courbe affine et $P = (0, 0)$. On écrit $f = f_m + f_{m+1} + \cdots + f_q$ où les f_i sont des polynômes homogènes de degré i, et $f_m \neq 0$. On appelle multiplicité de $\mathcal{C}$ en P et l'on note $m_P(\mathcal{C})$ l'entier m.

Notons que $P \in \mathcal{C}$ si, et seulement si $m_P(\mathcal{C}) > 0$. On dit que P est un point simple (resp. double, triple, etc.) sur $\mathcal{C}$ si $m_P(\mathcal{C}) = 1$ (resp. 2, 3, etc.).

Remarque 1.3.1. Lorsque $\mathcal{C} = \mathcal{V}(f)$ avec cette fois $f = \prod_i f_i^{n_i}$ où les f_i sont les facteurs irréductibles de f, alors

$$m_P(\mathcal{C}) = \sum_i n_i.m_P(\mathcal{C}_i),$$

avec $\mathcal{C}_i = \mathcal{V}(f_i)$. Pour le cas général, nous faisons un changement de coordonnées affines pour calculer la multiplicité de la courbe affine en un point $P = (a, b) \neq (0, 0)$. Concrètement, soit une courbe affine d'équation $f(x, y) = 0$. Il suffit de ramener le point $P = (a, b)$ à l'origine en construisant une nouvelle fonction h définie comme suit

$$h(x, y) = f(x + a, y + b).$$

Puisque, le changement de coordonnées affines ne change pas la multiplicité et on a $h(0, 0) = f(P) = 0$ alors, chercher la multiplicité de f en $P = (a, b)$ revient à trouver la multiplicité de h à l'origine. Pour le cas d'une courbe projective, on pourra consulter [Ful69, Chapitre 5].

Définitions 1.3.2. Soit $\mathcal{C}$ une courbe algébrique.
Si $\mathcal{C} : f(x, y) = 0$ une courbe plane affine et $P = (a, b) \in \mathcal{C}$. On dit que P est un point singulier si

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0;$$

sinon on dit que P est un point lisse (ou non singulier ou régulier), auquel cas la tangente à $\mathcal{C}$ en P est donnée par

$$\frac{\partial f}{\partial x}(P)(x - a) + \frac{\partial f}{\partial y}(P)(y - b) = 0.$$

Si $\mathcal{C} : F(X, Y, Z) = 0$ une courbe plane projective et $P = (a : b : c) \in \mathcal{C}$. On dit que P est un point singulier si

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0;$$

sinon on dit que P est un point lisse (ou non singulier ou régulier), auquel cas la tangente à $\mathcal{C}$ en P est donnée par

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

Une courbe $\mathcal{C}$ est lisse (ou non singulière ou régulière) si elle l'est en chacun de ses points.

Définition 1.3.3. Une courbe elliptique E définie sur un corps K est une courbe projective lisse de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

avec chaque $a_i \in K$.

Une équation de cette forme est appelée équation de Weierstrass. Il existe un point à l'infini donné par $\mathcal{O} = (0 : 1 : 0) \in E$ et que c'est le seul point qui se trouve sur la courbe avec $Z = 0$. On peut écrire l'équation de Weierstrass affine pour la courbe elliptique E en utilisant les coordonnées $x = X/Z$ et $y = Y/Z$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

en se rappelant toujours qu'il y a un point supplémentaire le point à l'infini $\mathcal{O} = (0 : 1 : 0)$.

Si $\mathrm{car}(K) \neq 2$, la substitution de (x, y) par $\left(x, \dfrac{y - a_1x - a_3}{2}\right)$ donne une équation de la forme

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

avec $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^2 + 4a_6$.
Si de plus car$(K) \neq 2, 3$, la substitution de (x, y) par $\left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ à l'équation ci-dessus donne une équation plus simple de la forme

$$y^2 = x^3 - 27c_4x - 54c_6,$$

avec $c_4 = b_2^2 - 24b_4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

Il en résulte que lorsque la caractéristique de K est différente de 2 et 3, une courbe elliptique E définie sur K est une courbe d'équation affine

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

avec $a, b \in K$ tels que $4a^3 + 27b^2 \neq 0$, à laquelle on rajoute le point $\mathcal{O} = (0 : 1 : 0)$. Cette équation est appelée forme réduite de Weierstrass.
L'ensemble des points $K-$rationnels sur E, noté $E(K)$, est défini par

$$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

Définition 1.3.4. Soit $\mathcal{C}$ une courbe projective définie sur K et irréductible. On appelle corps des fractions de l'anneau $\overline{K}[\mathcal{C}]$ le corps des fonctions rationnelles sur $\mathcal{C}$; il est noté $\overline{K}(\mathcal{C})$. En d'autres termes, on a

$$\overline{K}(\mathcal{C}) = \{f \ : \ \exists\ f_1, f_2 \in \overline{K}[\mathcal{C}] \text{ homogènes de même degré, } f = f_1/f_2\}.$$

Définition 1.3.5. Soient $f \in \overline{K}(\mathcal{C})$ et $P \in \mathcal{C}$. On dit que f est régulière (ou est définie) au point P s'il existe $f_1,\ f_2 \in \overline{K}[\mathcal{C}]$ telles que $f = f_1/f_2$ avec $f_2(P) \neq 0$.

Définition 1.3.6. Soient $\mathcal{C}$ une courbe projective irréductible définie sur K et $P \in \mathcal{C}$. On appelle anneau local de $\mathcal{C}$ en P et l'on note $\mathcal{O}_P(\mathcal{C})$ l'ensemble des fonctions régulières en P, i.e., on a

$$\mathcal{O}_P(\mathcal{C}) = \{f \in \overline{K}(\mathcal{C}) \ : \ f = f_1/f_2,\ \ f_1, f_2 \in \overline{K}[\mathcal{C}] \text{ et } f_2(P) \neq 0\}.$$

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

$$\mathcal{M}_P(\mathcal{C}) = \{f \in \mathcal{O}_P(\mathcal{C}) \ : \ f(P) = 0\}$$

qui est un idéal maximal.

Les éléments inversibles de $\mathcal{O}_P(\mathcal{C})$ sont ceux qui n'appartiennent pas à $\mathcal{M}_P(\mathcal{C})$, on les appelle les unités de $\mathcal{O}_P(\mathcal{C})$ et ils forment un groupe multiplicatif.

Si $\mathcal{C}$ est définie par l'équation affine $f(x, y) = 0$, alors $\mathcal{M}_P(\mathcal{C})$ pour $P = (a, b)$ est engendré par $x - a$ et $y - b$, i.e., $\mathcal{M}_P(\mathcal{C}) =< x - a, y - b >$ (voir [EM07, Chapitre 1]).

Définition 1.3.7. On dit que $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète s'il existe $t \in \mathcal{M}_P(\mathcal{C}),\ t \neq 0$, tel que tout élément non nul $f \in \mathcal{O}_P(\mathcal{C})$ s'écrive de manière unique $f = u.t^m$, u unité de $\mathcal{O}_P(\mathcal{C})$, $m \in \mathbb{N}$. L'entier m est appelé la valuation (ou l'ordre) de f au point P, notée $\text{ord}_P(f)$; il ne dépend pas du choix du paramétre t appelé uniformisante de $\mathcal{O}_P(\mathcal{C})$.

Plus généralement, si $f \in \mathcal{O}_P(\mathcal{C}),\ f \neq 0$ on peut l'écrire sous la forme $u.t^m$, avec cette fois $m \in \mathbb{Z}$ et on pose $\text{ord}_P(f) = m$.

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

$$\mathcal{O}_P(\mathcal{C})/\mathcal{M}_P(\mathcal{C})$$

est appelé corps résiduel.

La connaissance de la fonction $\mathrm{ord}_P : f \longmapsto \mathrm{ord}_P(f)$ détermine l'anneau de valuation discrète $\mathcal{O}_P(\mathcal{C})$:

$$\mathcal{O}_P(\mathcal{C}) = \{f \in \overline{K}(\mathcal{C}) \mid \mathrm{ord}_P(f) \geq 0\}$$

et $\mathcal{M}_P(\mathcal{C})$:

$$\mathcal{M}_P(\mathcal{C}) = \{f \in \overline{K}(\mathcal{C}) \mid \mathrm{ord}_P(f) > 0\}.$$

Propriétés 1.3.1. Soit $\mathcal{C}$ une courbe lisse en P. Soient f_1 et f_2 deux éléments non nuls de $\overline{K}(\mathcal{C})$. On a :

a) $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$

b) $\mathrm{ord}_P\left(\dfrac{f_1}{f_2}\right) = \mathrm{ord}_P(f_1) - \mathrm{ord}_P(f_2)$

c) $\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$

d) Si P est un pôle de f_1, alors $\mathrm{ord}_P(f_1) = -\mathrm{ord}_P\left(\dfrac{1}{f_1}\right)$

Exemple 1.3.1. Considérons une courbe $\mathcal{C}$ irréductible et lisse définie sur $\mathbb{Q}$ d'équation affine

$$y^2 = (x-1)(x-2)(x-3).$$

Soit $P_k = (k, 0)$ où $k \in \{1, 2, 3\}$. On a $\mathcal{M}_{P_k}(\mathcal{C})$ est donné par $< x-k, y >$ et pour tout $j \neq k$, les éléments $x - j$ sont inversibles dans l'anneau local $\mathcal{O}_{P_k}(\mathcal{C})$ avec $j \in \{1, 2, 3\}$. On a pour $j \neq k$, $(x-k) = u.y^2$. Alors, l'uniformisante de $\mathcal{O}_{P_k}(\mathcal{C})$ est y. Ainsi, on a $\mathrm{ord}_{P_k}(y) = 1$ et donc $\mathrm{ord}_{P_k}(x-k) = 2$.

Soit $\mathcal{F}(\overline{K})$ l'ensemble des paires de polynômes $f_1, f_2 \in \overline{K}[X, Y]$ n'ayant pas de facteur commun $h \in \overline{K}[X, Y]$, tel que $h(0, 0) = 0$. Pour $(f_1, f_2) \in \mathcal{F}(\overline{K})$, nous voulons définir le nombre d'intersection des courbes $\mathcal{C} = \mathcal{V}(f_1)$ et $\mathcal{C}' = \mathcal{V}(f_2)$ à l'origine ; il sera noté $I(P, \mathcal{C} \cap \mathcal{C}')$ ou $\mathrm{mult}_P(\mathcal{C} \cap \mathcal{C}')$. On notera souvent, par abus d'écriture, $I(P, \mathcal{C} \cap \mathcal{C}')$ par $I(f_1, f_2)$. La proposition suivante montre qu'il y a exactement une façon raisonnable de le faire.

Propositions 1.3.2. Il existe une unique application $I : \mathcal{F}(\overline{K}) \to \mathbb{N}$ telle que

a) $I(X, Y) = 1$;

b) $I(f_1, f_2) = I(f_2, f_1)$ pour tout $(f_1, f_2) \in \mathcal{F}(\overline{K})$;

c) $I(f_1, f_2 f_3) = I(f_1, f_2) + I(f_1, f_3)$ pour tous $(f_1, f_2), (f_1, f_3) \in \mathcal{F}(\overline{K})$;

d) $I(f_1, f_2 + f_3 f_1) = I(f_1, f_2)$ pour tous $(f_1, f_2) \in \mathcal{F}(\overline{K})$, $f_3 \in \overline{K}[X, Y]$;

e) $I(f_1, f_2) = 0$ si $f_2(0, 0) \neq 0$.

On trouve une démonstration dans [Mil06, Chapitre I] ou [Ful69, Chapitre 3].

Considérons deux courbes $\mathcal{C} = \mathcal{V}(f_1)$ et $\mathcal{C}' = \mathcal{V}(f_2)$ dans $\mathbb{A}^2$ et soit $P = (a, b) \in \mathcal{C} \cap \mathcal{C}'$. On dit que P est un point isolé de $\mathcal{C} \cap \mathcal{C}'$ si $\mathcal{C}$ et $\mathcal{C}'$ n'ont pas de composante irréductible commune passant par P et nous pouvons donc définir le nombre d'intersection de $\mathcal{C}$ et $\mathcal{C}'$ en P comme suit

$$I(P, \mathcal{C} \cap \mathcal{C}') = I(f_1(x + a, y + b), f_2(x + a, y + b)).$$

En particulier, si $P = (0, 0)$, on obtient $I(P, \mathcal{C} \cap \mathcal{C}') = I(f_1, f_2)$.

Théorème 1.3.1. Le nombre d'intersection de $\mathcal{C}$ et $\mathcal{C}'$ en P est donné par la formule suivante

$$I(P, \mathcal{C} \cap \mathcal{C}') = \dim_{\overline{K}} \mathcal{O}_P(\mathbb{A}^2)/ < f_1, f_2 > .$$

Une démonstration de ce théorème est donnée dans [Ful69, Chapitre 3].

Exemple 1.3.2. Soient $\mathcal{C} : y^2 = x^3$ la courbe affine, et $L : y = 0$ la droite tangente en $P = (0, 0)$. Alors

$$I(P, \mathcal{C} \cap L) = I(y^2 - x^3, y) = I(x^3, y) = 3.$$

Remarque 1.3.2. On a $I(P, \mathcal{C} \cap \mathcal{C}') = 1$ si, et seulement si P est lisse à la fois sur $\mathcal{C}$ et $\mathcal{C}'$ et que les droites tangentes à $\mathcal{C}$ et $\mathcal{C}'$ en P sont distinctes. On a aussi $I(P, \mathcal{C} \cap \mathcal{C}') \geq m_P(\mathcal{C}).m_P(\mathcal{C}')$ avec égalité si, et seuement si les deux courbes n'ont aucune droite tangente commune en P.

Théorème 1.3.2 (**Bézout**)**.**
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes projectives planes définies sur un corps algébriquement clos, sans composante irréductible commune, de degré respectif d et d'. Alors le nombre d'intersection (comptés avec multiplicités) de ces deux courbes est égal à dd'. C'est-à-dire

$$\sum_P I(P, \mathcal{C} \cap \mathcal{C}') = dd'.$$

On définit le cycle d'intersection de $\mathcal{C}$ et $\mathcal{C}'$, noté $\mathcal{C}.\mathcal{C}'$ par

$$\mathcal{C}.\mathcal{C}' = \sum_{P \in \mathbb{P}^2} I(P, \mathcal{C} \cap \mathcal{C}')P.$$

1.3.2 Diviseurs

Soit X une variété algébrique.

Définition 1.3.8 (**Diviseur de Weil**)**.**
On appelle diviseur de Weil D sur X une somme formelle finie à coefficients entiers d'hypersurfaces irréductibles de X de codimension 1. Ainsi, un diviseur de Weil D sur X s'écrit

$$D = \sum_i m_i Y_i,$$

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

Définition 1.3.9 (**Diviseur de Cartier**)**.**
Un diviseur de Cartier D sur X est la donnée d'un recouvrement (U_i) de X par des ouverts, et chaque U_i d'une fonction rationnelle f_i, avec la condition de compatibilité : sur chaque intersection $U_i \cap U_j$, la fonction $f_{ij} = f_i/f_j$ est une fonction à valeurs dans $\overline{K}^*$ (i.e., sans zéro ni pôle).

Voici une proposition importante qui nous permet d'identifier les deux diviseurs et ainsi, nous pouvons les écrire de façon simple.

Proposition 1.3.3. Sur une variété lisse les notions de diviseur de Weil et de diviseur de Cartier coïncident.

Nous déduisons de cette proposition qu'un diviseur sur une courbe lisse et irréductible est simplement une somme formelle finie de points affectés par des coefficients entiers. Dans la suite, nous entendons par courbe, une variété algébrique projective de dimension 1.

Définition 1.3.10. Soit $\mathcal{C}$ une courbe lisse. Un diviseur D sur $\mathcal{C}$ est une somme formelle de points appartenant à $\mathcal{C}$:

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

où les n_P sont des entiers presque tous nuls.

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

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

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

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

Manifestement, $\deg(D + D') = \deg(D) + \deg(D')$. Les diviseurs sur $\mathcal{C}$ de degré 0 forment un sous-groupe de $\mathrm{Div}(\mathcal{C})$ que l'on note $\mathrm{Div}^0(\mathcal{C})$. Le support de D est l'ensemble des points $P \in \mathcal{C}$ tels que $n_P \neq 0$. Le diviseur D est effectif (ou positif) et on note $D \geq 0$ si $n_P \geqslant 0$ pour tout $P \in \mathcal{C}$. Ainsi, on peut définir la relation d'ordre partiel "$\geqslant$" sur les diviseurs par :

$$D \geqslant D' \text{ si et seulement si } D - D' \geqslant 0.$$

Soit $\mathcal{C}$ une courbe lisse définie sur K. Le groupe de Galois G_K agit sur $\mathrm{Div}(\mathcal{C})$ et sur $\mathrm{Div}^0(\mathcal{C})$ de la manière suivante :

$$D^\sigma = \sum_{P\in\mathcal{C}} n_P P^\sigma.$$

On dit que D est défini sur K s'il est invariant sous l'action du groupe de Galois : $D^\sigma = D$ pour tout $\sigma \in G_K$. Précisons que D est défini sur K, cela ne signifie pas que tous les P qui composent D sont définis sur K. Le groupe de Galois G_K permute les P d'une manière appropriée. On désigne le groupe des diviseurs sur $\mathcal{C}$ définis sur K par $\mathrm{Div}_K(\mathcal{C})$ et de même pour $\mathrm{Div}^0_K(\mathcal{C})$.

Exemple 1.3.3. Soit $\mathcal{C}$ la courbe lisse définie sur $\mathbb{Q}$ d'équation affine

$$y^2 = x(x^2 + 1)(x^3 + 1).$$

Considérons les diviseurs sur $\mathcal{C}$ suivants

$$D_1 = 2(0,0) + (1,2),\ D_2 = (i,0) - (-i,0) \text{ et } D_3 = (i,0) + (-i,0) - 2(1,2).$$

On a

- $\deg(D_1) = 3$, $\deg(D_2) = 0$ et $\deg(D_3) = 0$.
- On sait que tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ envoie i en lui-même ou envoie i en son conjugué complexe. Ainsi, les diviseurs D_1 et D_3 sont définis sur $\mathbb{Q}$, alors que D_2 ne l'est pas.
- $D_3 \in \mathrm{Div}^0_{\mathbb{Q}}(\mathcal{C})$, mais $D_1,\ D_2 \notin \mathrm{Div}^0_{\mathbb{Q}}(\mathcal{C})$.

Remarque 1.3.3. Tout diviseur D peut s'écrire sous la forme $D = D_1 - D_2$, où les D_i sont effectifs et de supports disjoints. En effet, soit $D = \sum_{P\in\mathcal{C}} n_P P$, en posnat $D_1 = \sum_{n_P\geq 0} n_P P$ et $D_2 = -\sum_{n_P<0} n_P P$; on a $D = D_1 - D_2$.

Définition 1.3.11 (**Diviseur principal**). Soient $\mathcal{C}$ une courbe lisse et f une fonction non nulle de $\overline{K}(\mathcal{C})$. On associe à f le diviseur noté $\mathrm{div}(f)$ défini par

$$\mathrm{div}(f) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f) P.$$

Un tel diviseur est appelé diviseur principal. L'ensemble des diviseurs principaux est noté par $\mathrm{Prin}(\mathcal{C})$.

Le diviseur des zéros de f, noté $\mathrm{div}(f)_0$, et le diviseur des pôles de f, noté $\mathrm{div}(f)_\infty$, sont définis par

$$\mathrm{div}(f)_0 = \sum_{\mathrm{ord}_P(f) \geq 0} \mathrm{ord}_P(f) P \ \text{ et } \ \mathrm{div}(f)_\infty = - \sum_{\mathrm{ord}_P(f) < 0} \mathrm{ord}_P(f) P.$$

Ainsi, le diviseur d'une fonction est la différence de ses zéros et de ses pôles (comptés avec leur ordre de multiplicité). Pour $\sigma \in G_K$, on a

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma.$$

Ainsi, si $f \in K(\mathcal{C})^*$, $\mathrm{div}(f) \in \mathrm{Div}_K(\mathcal{C})$, c'est-à-dire, le diviseur d'une fonction $K-$rationnelle sera aussi $K-$rationnel. L'ensemble des diviseurs principaux $K-$rationnels est noté par $\mathrm{Prin}_K(\mathcal{C})$.

Propriétés 1.3.2. Soit $\mathcal{C}$ une courbe lisse. Soient f_1 et f_2 deux éléments de $\overline{K}(\mathcal{C})^*$. On a

1. $\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + \mathrm{div}(f_2)$
2. $\mathrm{div}\left(\dfrac{1}{f_1}\right) = -\mathrm{div}(f_1)$
3. $\mathrm{div}(f_1) = 0$ si, et seulement si $f_1 \in \overline{K}^*$
4. $\mathrm{div}(f_1) = \mathrm{div}(f_2)$ si, et seulement si $\exists\, \lambda \in \overline{K}^* \ : \ f_1 = \lambda f_2$

Un diviseur principal est un diviseur de degré zéro, c'est-à-dire, une fonction rationnelle non nulle a le même nombre de zéros que de pôles s'ils sont comptés avec leur multiplicité. Les diviseurs principaux forment un sous-groupe de $\mathrm{Div}^0(\mathcal{C})$.

Exemple 1.3.4. Considérons une courbe $\mathcal{C}$ lisse définie sur $\mathbb{Q}$ d'équation affine

$$y^2 = (x-1)(x-2)(x-3).$$

Soit $P_k = (k, 0)$ où $k \in \{1, 2, 3\}$. On sait déjà que $\mathrm{ord}_{P_k}(x-k) = 2$. De plus, on vérifie sans difficulté que $\mathcal{C}$ admet un unique point à l'infini $\mathcal{O}$. Ainsi, on a

- $\mathrm{div}(x-k) = 2P_k - 2\mathcal{O}, \quad \forall\, k \in \{1, 2, 3\}$;
- $\mathrm{div}(y) = P_1 + P_2 + P_3 - 3\mathcal{O}$.

Deux diviseurs sont linéairement équivalents si leur différence est un diviseur principal. On note $\sim$ la relation d'équivalence linéaire entre diviseurs : soient D et D' deux éléments de $\mathrm{Div}(\mathcal{C})$, on a

$$D \sim D' \text{ si et seulement si il existe } f \in \overline{K}(\mathcal{C})^* \ : \ D - D' = \mathrm{div}(f).$$

Nous examinons maintenant la jacobienne d'une courbe $\mathcal{C}$. Nous nous intéressons par la suite aux éléments de la jacobienne qui sont invariants sous G_K. Cette partie est fondamentale pour étudier l'arithmétique des courbes algébriques. Commençons par définir le groupe de Picard.

Définition 1.3.12. On définit le groupe de Picard (aussi appelé le groupe des classes de diviseurs) de $\mathcal{C}$, noté $\mathrm{Pic}(\mathcal{C})$, comme le quotient de $\mathrm{Div}(\mathcal{C})$ par le sous-groupe des diviseurs principaux :

$$\mathrm{Pic}(\mathcal{C}) = \frac{\mathrm{Div}(\mathcal{C})}{\mathrm{Prin}(\mathcal{C})}.$$

Nous pouvons aussi définir, de la même manière, le groupe des classes de diviseurs de degré 0, noté $\mathrm{Pic}^0(\mathcal{C})$ par

$$\mathrm{Pic}^0(\mathcal{C}) = \frac{\mathrm{Div}^0(\mathcal{C})}{\mathrm{Prin}(\mathcal{C})}.$$

Définition 1.3.13. La jacobienne d'une courbe $\mathcal{C}$ que l'on note par $J_{\mathcal{C}}$ est le groupe $\mathrm{Pic}^0(\mathcal{C})$.

Soient $\mathcal{C}$ une courbe définie sur K et $J_{\mathcal{C}}$ sa jacobienne. Supposons qu'il existe un point $K-$rationnel P_0 de $\mathcal{C}$. Nous nous intéressons particulièrement à l'ensemble des points rationnels de la jacobienne $J_{\mathcal{C}}$, noté $J_{\mathcal{C}}(K)$. Il s'agit des éléments de $J_{\mathcal{C}}$ fixés sous l'action du groupe de Galois G_K. Nous pouvons identifier $J_{\mathcal{C}}(K)$ au groupe des classes de diviseurs $K-$rationnels de degré 0, défini comme

$$\mathrm{Pic}^0_K(\mathcal{C}) = \mathrm{Div}^0_K(\mathcal{C})/\mathrm{Prin}_K(\mathcal{C}).$$

Définition 1.3.14 (**Espace de Riemann-Roch**)**.**
Soient $\mathcal{C}$ une courbe lisse et D un diviseur sur $\mathcal{C}$. L'espace de Riemann-Roch associé à D est l'espace vectoriel

$$\mathcal{L}(D) = \{f \in \overline{K}(\mathcal{C})^* \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

C'est un $\overline{K}-$espace vectoriel de dimension finie et on désignera par $l(D)$ sa dimension.

Proposition 1.3.4. Soient D et D' deux diviseurs sur une courbe lisse $\mathcal{C}$.

1) Si $\deg(D) < 0$, alors $\mathcal{L}(D) = 0$ et $l(D) = 0$.
2) Si $D < D'$, alors $\mathcal{L}(D) \subset \mathcal{L}(D')$.
3) Si $D \sim D'$, alors $\mathcal{L}(D) \simeq \mathcal{L}(D')$ et $l(D) = l(D')$.

Définitions 1.3.15 (**Formes différentielles**)**.** Soit X une variété de dimension n.

1. Une $p-$forme différentielle ω régulière sur X est une forme qui dans un voisinage de chaque point $x \in X$ s'écrit
$$\omega = \sum_{|I|=p} f_I dg_I$$
où $I = (i_1, \ldots, i_p)$ est un multi-indice d'entiers avec $1 \leqslant i_1 < i_2 < \ldots < i_p \leqslant n$, $f_I = f_{i_1 \ldots i_p}$, $g_I = \{g_{i_1}, \ldots, g_{i_p}\}$; f_I et g_I sont des fonctions régulières en x et $dg_I = dg_{i_1} \wedge \ldots \wedge dg_{i_p}$.
Une $n-$forme différentielle ω régulière sur X s'écrit $\omega = f dg_1 \wedge \ldots \wedge dg_n$.
2. Une $p-$forme différentielle rationnelle sur X est la donnée d'une $p-$forme différentielle régulière ω sur un ouvert de X, modulo la relation d'équivalence $\approx$ définie comme suit :
$$(\omega, U) \approx (\omega', U') \text{ si et seulement si } \omega = \omega' \text{ sur } U \cap U'.$$

Définition 1.3.16 (**Diviseur canonique**)**.** Soit X une variété lisse de dimension n. Un diviseur canonique sur X est un diviseur d'une $n-$forme différentielle rationnelle sur X.

Un tel diviseur est noté W_X ou simplement W s'il n'y a pas risque de confusion sur X.

Proposition 1.3.5. Si ω et ω' sont deux n-formes différentielles rationnelles sur X, alors $W \sim W'$. Autrement dit, il existe une fonction rationnelle non nulle f telle que $\omega = f\omega'$.

Cette proposition montre que les diviseurs des $n-$formes différentielles rationnelles non nulles forment une seule classe de diviseurs, appelée classe canonique. Par conséquent, sur X, tous les diviseurs canoniques ont le même degré. Etudions maintenant le cas d'une courbe.

Définition 1.3.17. Soit $\mathcal{C}$ une courbe. L'espace des formes différentielles sur $\mathcal{C}$, noté $\Omega_{\mathcal{C}}$, est le $\overline{K}(\mathcal{C})-$ espace vectoriel engendré par les symboles de la forme dx pour $x \in \overline{K}(\mathcal{C})$, vérifiant les relations usuelles :

(i) $d(x+y) = dx + dy$ pour tous x, $y \in \overline{K}(\mathcal{C})$.

(ii) $d(xy) = xdy + ydx$ pour tous x, $y \in \overline{K}(\mathcal{C})$.

(iii) $d\alpha = 0$ pour tout $\alpha \in \overline{K}$.

Proposition 1.3.6. Soit $\mathcal{C}$ une courbe.

1) L'espace vectoriel $\Omega_{\mathcal{C}}$ est de dimension 1 sur $\overline{K}(\mathcal{C})$.

2) Si t est une uniformisante en un point lisse de $\mathcal{C}$, alors dt est une base de $\Omega_{\mathcal{C}}$.

Propositions 1.3.7. Soit $\mathcal{C}$ une courbe. Soient $P \in \mathcal{C}$ et $t \in \overline{K}(\mathcal{C})$ une uniformisante en P.

(a) Pour tout $\omega \in \Omega_{\mathcal{C}}$, il existe une unique fonction $f \in \overline{K}(\mathcal{C})$ qui ne dépend que de ω et t, telle que $\omega = fdt$.
On note f par ω/dt.

(b) Soit $f \in \overline{K}(\mathcal{C})$ une fonction régulière en P. Alors $\dfrac{df}{dt}$ est aussi une fonction régulière en P.

(c) Soit $\omega \in \Omega_{\mathcal{C}}$ avec $\omega \neq 0$. La quantité $\mathrm{ord}_P(\omega/dt)$ dépend seulement de ω et P, elle est indépendante du choix de l'uniformisante t.
Cette valeur s'appelle l'ordre en P de ω et on la note $\mathrm{ord}_P(\omega)$.

(d) Soient f_1, $f_2 \in \overline{K}(\mathcal{C})$ avec $f_2(P) = 0$ et soit $p = \mathrm{car}(K)$. Alors

$$\mathrm{ord}_P(f_1 df_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2) - 1, \text{ si } p = 0 \text{ ou si } p \nmid \mathrm{ord}_P(f_2).$$

(e) Soit $\omega \in \Omega_{\mathcal{C}}$ avec $\omega \neq 0$. Alors

$$\mathrm{ord}_P(\omega) = 0 \text{ sauf un nombre fini de } P \in \mathcal{C}.$$

Cette proposition nous permet d'énoncer la définition suivante :

Définition 1.3.18. Soit $\omega \in \Omega_{\mathcal{C}}$ avec $\omega \neq 0$. On associe à ω le diviseur noté $\mathrm{div}(\omega)$ défini par

$$\mathrm{div}(\omega) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\omega) P.$$

Un tel diviseur est appelé diviseur canonique. On le note W au lieu de $\mathrm{div}(\omega)$. La différentielle $\omega \in \Omega_{\mathcal{C}}$ est régulière (ou holomorphe) si

$$\mathrm{ord}_P(\omega) \geq 0, \ \ \forall\, P \in \mathcal{C}.$$

Remarque 1.3.4. Soient $\mathcal{C}$ une courbe, $W = \mathrm{div}(\omega)$ un diviseur canonique sur $\mathcal{C}$ et $f \in \mathcal{L}(W)$. On a $\mathrm{div}(f) + \mathrm{div}(\omega) \geq 0$, i.e., $\mathrm{div}(f\omega) \geq 0$, donc $f\omega$ est holomorphe. Reciproquement, si la différentielle $f\omega$ est holomorphe alors $f \in \mathcal{L}(W)$. Puisque, chaque différentielle sur $\mathcal{C}$ a la forme $f\omega$ pour un certain $f \in \overline{K}(\mathcal{C})^*$, nous avons établi un isomorphisme des $\overline{K}-$espaces vectoriels,

$$\mathcal{L}(W) \simeq \{\omega \in \Omega_{\mathcal{C}} \mid \omega \text{ est holomorphe}\}.$$

La dimension $l(W)$ de ces espaces est un invariant important de la courbe $\mathcal{C}$. Cette dimension est le genre de la courbe $\mathcal{C}$.

Exemple 1.3.5. Considérons une courbe $\mathcal{C}$ lisse définie sur $\mathbb{Q}$ d'équation affine

$$y^2 = (x-1)(x-2)(x-3).$$

On garde les mêmes notations que l'exemple 1.3.4 et soit la $1-$forme différentielle

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 - 12x + 11}.$$

On cherche à déterminer $\mathrm{div}(\omega)$. Cherchons d'abord $\mathrm{div}(dx)$, nous avons

$$dx = \frac{2ydy}{3x^2 - 12x + 11}.$$

La différentielle dx a trois zéros $P_1,\ P_2$, et P_3 et un pôle $\mathcal{O}$ et on a $dx = -x^2 d(1/x)$. Alors, on obtient

$$\mathrm{div}(dx) = P_1 + P_2 + P_3 - 3\mathcal{O}.$$

Ainsi, nous voyons donc que

$$\mathrm{div}(dx/y) = 0,\ \text{i.e., } \mathrm{div}(\omega) = 0.$$

Nous en arrivons au théorème de Riemann-Roch qui est un outil de base permettant de calculer dans la plupart des cas la dimension des espaces de Riemann-Roch. Il fournit l'existence de représentants agréables dans chaque classe de la jacobienne d'une courbe.

Théorème 1.3.3 (**Riemann-Roch**)**.**
Soient $\mathcal{C}$ une courbe lisse de genre g et W un diviseur canonique sur $\mathcal{C}$. Alors, pour tout diviseur D sur $\mathcal{C}$

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

Nous renvoyons à [Ful69, Chapitre 8] ou [Sti93, Chapitre 1] pour une démonstration.

Corollaire 1.3.1. Soient $\mathcal{C}$ une courbe lisse de genre g et W un diviseur canonique sur $\mathcal{C}$. On a

a) $l(W) = g$ et $\deg(W) = 2g - 2$;

b) si $\deg(D) \geq 2g - 1$, alors $l(D) = \deg(D) + 1 - g$;

c) (Théorème de Clifford) si $l(D) \neq 0$ et $l(W - D) \neq 0$, alors on a $l(D) \leq \frac{1}{2}\deg(D) + 1$.

Démonstration. Le théorème de Riemann-Roch affirme que

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

a) Pour $D = 0$, on obtient

$$1 = l(0) = l(W) + 1 - g,$$

ce qui prouve que $l(W) = g$. Ensuite pour $D = W$, on trouve

$$g = l(W) = \deg W + 2 - g,$$

donc, $\deg(W) = 2g - 2$.

b) Puisque $\deg(D) \geq 2g - 1$ et $\deg(W) = 2g - 2$ alors $\deg(W - D) < 0$, et donc $l(W - D) = 0$; ainsi la relation se simplifie.

c) Voir [Sti93, Chapitre 1]

❑

Voici quelques formules pour calculer le genre d'une courbe définie sur K de $\mathrm{car}(K) \neq 2$ (voir [Per95] et [Tow96]) :

◇ Soit $\mathcal{C}$ une courbe projective plane lisse définie sur K de degré d. Le genre g de $\mathcal{C}$ est donné par

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

◇ Soit $\mathcal{C}$ une courbe lisse définie sur K d'équation affine $y^2 = f(x)$, avec $\deg(f) = d$. Le genre g de $\mathcal{C}$ est donné par

$$g = \begin{cases} (d-1)/2 & \text{si } d \text{ impair} \\ (d-2)/2 & \text{si } d \text{ pair.} \end{cases}$$

Soient $\mathcal{C}$ une courbe lisse définie sur K de genre $g \geq 1$ et $J_{\mathcal{C}}$ sa jacobienne. Supposons que la courbe $\mathcal{C}$ ait un point base $K-$rationnel P_0. On définit le plongement jacobien comme suit

$$j : \mathcal{C} \longrightarrow J_{\mathcal{C}},\ P \longmapsto [P - P_0],$$

où $[D]$ représente la classe du diviseur D.

L'application j s'étend par additivité, notée encore j, de $\mathrm{Div}^0(C)$ vers $J_{\mathcal{C}}$, donnée par

$$j : \mathrm{Div}^0(C) \longrightarrow J_{\mathcal{C}},\ \ D \longmapsto [D - \deg(D)P_0].$$

et appelée application d'Abel-Jacobi.

Théorème 1.3.4 (**Abel-Jacobi**).
L'application d'Abel-Jacobi j est surjective et son noyau est formé des diviseurs de fonctions rationnelles sur $\mathcal{C}$. En d'autres termes, j induit un isomorphisme de $\mathrm{Pic}^0(\mathcal{C})$ vers $J_{\mathcal{C}}$.

Nous pouvons traduire le théorème d'Abel-Jacobi en trois points dont une preuve se trouve dans [Gri89, Chapitre 5].

- L'application d'Abel-Jacobi j est surjective.
- $\mathrm{Im}(\mathrm{div}(f)) \subset \ker(j)$, i.e., pour tout $f \in \overline{K}(\mathcal{C})^*$ avec $\mathrm{div}(f) = D$, alors $j(D) = 0$.
- $\ker(j) \subset \mathrm{Im}(\mathrm{div}(f))$, i.e., si $j(D) = 0$ avec $D \in \mathrm{Div}^0(C)$, il existe $f \in \overline{K}(\mathcal{C})^*$ telle que $\mathrm{div}(f) = D$.

1.4 Variétés abéliennes et isogénies

Considérons K un corps de nombres (i.e., une extension de dimension finie du corps $\mathbb{Q}$).

1.4.1 Variétés abéliennes

Définition 1.4.1. Une variété de groupe définie sur K est une variété algébrique V définie sur K munie d'un point $e \in V(K)$ et de deux morphismes

$$m : V \times V \longrightarrow V \quad \text{et} \quad \iota : V \longrightarrow V,$$

satisfaisant les axiomes d'une loi de groupe

(i) pour tout $x \in V$, $m(e, x) = m(x, e) = x$;

(ii) pour tout $x \in V$, $m(\iota(x), x) = m(x, \iota(x)) = e$;

(iii) pour tous $x, y, z \in V$, $m(m(x,y),z) = m(x,m(y,z))$.

Exemples 1.4.1.

- Le groupe additif V_a est la variété $\mathbb{A}^1$ dont la loi de groupe est l'addition

$$m : V_a \times V_a \longrightarrow V_a, \ \ (x,y) \longmapsto x+y \quad \text{et} \quad \iota : V_a \longrightarrow V_a, \ \ x \longmapsto -x.$$

- Le groupe multiplicatif V_m est la variété $\mathbb{A}^1 - 0$ dont la loi de groupe est la multiplication

$$m : V_m \times V_m \longrightarrow V_m, \ \ (x,y) \longmapsto xy \quad \text{et} \quad \iota : V_m \longrightarrow V_m, \ \ x \longmapsto \frac{1}{x}.$$

Un morphisme de variétés de groupes $\alpha : V \longrightarrow V'$ est un morphisme de variétés algébriques qui commute avec la structure de groupe

$$\alpha(e) = e' \text{ avec } e' \in V'(K), \quad \alpha(m(x,y)) = m'(\alpha(x),\alpha(y)), \quad \alpha(\iota(x)) = \iota'(\alpha(x)).$$

Définition 1.4.2. Une variété algébrique X est complète si pour toute variété Y, la projection $X \times Y \longrightarrow Y$ est fermée (c'est-à-dire, envoie les fermés sur des fermés).

Définition 1.4.3. Une variété abélienne est une variété de groupe complète.

Notons que toute variété abélienne est projective [Mil08, I.6]. La jacobienne d'une courbe de genre g est une variété abélienne de dimension g.

1.4.2 Isogénies

Soit $\alpha : A \to B$ un homomorphisme de variétés abéliennes. Le noyau de α est une variété algébrique.

Définition 1.4.4. Un homomorphisme $\alpha : A \to B$ de variétés abéliennes est appelé isogénie, s'il est surjectif et a un noyau fini (i.e., le noyau a une dimension nulle).

Proposition 1.4.1. Soit $\alpha : A \to B$ un homomorphisme de variétés abéliennes. Alors, les conditions suivantes sont équivalentes :

a) α est une isogénie ;

b) $\dim(A) = \dim(B)$ et α est surjectif ;

c) $\dim(A) = \dim(B)$ et $\ker(\alpha)$ est fini.

Démonstration. On trouvera une démonstration dans [Mil08, I.7]. ❑

Le degré d'une isogénie $\alpha : A \to B$ est son degré en tant qu'application régulière, c'est-à-dire,

$$\deg(\alpha) = [K(A) : \alpha^*(K(B))].$$

Soient A une variété abélienne définie sur K de dimension g et n un entier naturel non nul. Alors, la multiplication par n, notée $[n]_A$, définie par

$$[n]_A : A \to A, \quad P \mapsto nP = \underbrace{P + P + \cdots + P}_{n \text{ fois}},$$

est une isogénie de A vers A dont le noyau est de cardinal n^{2g} (voir [Lan59]). On définit l'ensemble des points de $n-$torsion comme étant le noyau de la multiplication par n et on le note $A[n] = \ker([n]_A)$. Explicitement, on a

$$A[n] = \{P \in A(\overline{K}) : nP = 0_A\}.$$

Proposition 1.4.2. Soit $\alpha : A \to B$ une isogénie de degré d. Il existe une isogénie duale $\widehat{\alpha} : B \to A$ de même degré que α telle que

$$\alpha\widehat{\alpha} = [d]_B \quad \text{et} \quad \widehat{\alpha}\alpha = [d]_A,$$

où $[d]_A$ et $[d]_B$ désignent respectivement les multiplications par d sur A et B.

Ainsi, la relation $\ll$ il existe une isogénie entre deux variétés abéliennes $\gg$ est symétrique. Elle est transitive car la composée de deux isogénies est une isogénie. Finalement c'est une relation d'équivalence, et l'on dira que deux variétés abéliennes sont isogènes s'il existe une isogénie entre les deux. Si A et B sont deux variétés abéliennes isogènes, on note $A \approxeq B$.

Définition 1.4.5. Une variété abélienne A est dite simple s'il n'existe pas de variété abélienne $B \subset A$ telle que $0 \neq B \neq A$. Autrement dit, les seules sous-variété abéliennes de A sont A et $\{0\}$.

Définition 1.4.6. Toute variétés abéliennes est isogène à un produit de variétés abéliennes simples, unique à permutation et isogénie près.

Il en résulte que pour toute variété abélienne A, on a

$$A \approxeq A_1^{n_1} \times \cdots \times A_r^{n_r},$$

où chaque A_i est une variété abélienne simple et A_i n'est pas isogène à A_j pour $i \neq j$.

Théorème 1.4.1 (**Mordell-Weil**).
Soit A une variété abélienne définie sur K. Alors, le groupe $A(K)$ des points $K-$rationnels sur A est de type fini. En d'autres termes, on a

$$A(K) \cong \mathbb{Z}^r \oplus A(K)_{\text{tors}}, \quad \text{avec } r \in \mathbb{N}.$$

Le groupe $A(K)$ est appelé le groupe de Mordell-Weil, l'entier naturel r le rang de la variété abélienne A, et $A(K)_{\text{tors}}$ est le sous-groupe de torsion.

Du point de vue informatique, le calcul du sous-groupe $A(K)_{\text{tors}}$ est une tâche simple ; par contre la déterminaton du rang r et des générateurs de $\mathbb{Z}^r$ est très délicate.

Ce théorème a été prouvé par Mordell [Mor22] dans le cas où la variété abélienne est une courbe elliptique. Weil [Wei29] dans sa thèse a traité le cas des jacobiennes des courbes de genre supérieur. Une preuve se trouve dans [HS00] ou [Ser90].

Le principe de la méthode utilisée pour étudier les points algébriques de degré donné sur les courbes dont le groupe de Mordell-Weil est fini

Soit $\mathcal{C}$ une courbe projective lisse définie sur $\mathbb{Q}$ de genre $g \geq 2$. Le célèbre théorème de Faltings affirme que, étant donné un corps de nombres K, l'ensemble $\mathcal{C}(K)$ est fini. Nous nous intéressons à décrire cet ensemble. Plus précisement, nous donnons une description de l'ensemble des points algébriques sur $\mathcal{C}$ de degré au plus d donné sur $\mathbb{Q}$. On note cet ensemble par

$$\bigcup_{[K:\mathbb{Q}]\leqslant d} \mathcal{C}(K).$$

Le degré d'un point algébrique R sur $\mathcal{C}$ est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire, la dimension de $\mathbb{Q}(R)$ en tant que $\mathbb{Q}-$espace vectoriel. Le principe sous-jacent de la méthode utilisée pour étudier ces points algébriques est le suivant.

On suppose que l'on connaisse ou détermine la structure du groupe de Mordell-Weil $J_{\mathcal{C}}(\mathbb{Q})$ et que celui-ci soit fini :

$$J_{\mathcal{C}}(\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}.$$

On considère un point base $P_0 \in \mathcal{C}(\mathbb{Q})$; l'application d'Abel-Jacobi associée à P_0 est le plongement jacobien

$$j : \mathcal{C} \longrightarrow J_{\mathcal{C}},\ P \longmapsto [P - P_0],$$

où $[P - P_0]$ est la classe du diviseur $P - P_0$. On détermine ensuite $D_1, \cdots, D_s$ des diviseurs sur $\mathcal{C}$ définis sur $\mathbb{Q}$ tels que $j(D_i)$ soit d'ordre n_i et $j(D_1), \cdots, j(D_s)$ engendrent $J_{\mathcal{C}}(\mathbb{Q})$.
Soit R un point algébrique sur $\mathcal{C}$ de degré d. Notons $R_1, \cdots, R_d$ les conjugués de Galois de R. On a $j(R_1 + \cdots + R_d)$ appartient à $J_{\mathcal{C}}(\mathbb{Q})$ et par conséquent, il existe m_i tels que

$$j(R_1 + \cdots + R_d) = m_1 j(D_1) + \cdots + m_s j(D_s), \quad \text{avec } \ 0 \leq m_i \leq n_i - 1.$$

Le théorème d'Abel-Jacobi entraîne l'existence d'une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\mathrm{div}(f) = R_1 + \cdots + R_d - m_1 D_1 - \cdots - m_s D_s + \Big(\sum_{1 \leq i \leq s} m_i \mathrm{deg}(D_i) - d \Big) P_0.$$

La fonction f a donc des zéros et des pôles prescrits, et si l'on sait analyser les espaces de Riemann-Roch sur la courbe $\mathcal{C}$, on en déduit des restrictions sur les zéros et les pôles de f ; ainsi, dans les bons cas, on donne une description explicite.

Chapitre 2

Points algébriques sur des courbes hyperelliptiques de genre deux

Dans ce chapitre, nous nous intéressons à donner une paramétrisation des points algébriques de degré donné sur des courbes hyperelliptiques de genre 2. L'originalité des résultats obtenus dans ce chapitre porte essentiellement sur : le théorème 2.2.4 qui donne de manière explicite les points algébriques de degré au plus d sur les courbes hyperelliptiques $y^2 = x^5 + n^2$ avec $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$; le théorème 2.3.2 qui décrit explicitement les points algébriques de degré au plus 3 sur les courbes hyperelliptiques $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$ avec $n \in \{1, 2, 3, q$ un nombre premier et $q \equiv 7 \pmod{24}\}$.

2.1 Arithmétique des courbes hyperelliptiques

Dans cette section, nous nous sommes inspirés principalement sur [Sto15a], [Gau00], [CF96], [Fly93], [CF06], [GPN02] et [Sto01].

2.1.1 Courbes hyperelliptiques

Définition 2.1.1. Une courbe hyperelliptique $\mathcal{C}$ définie sur un corps de nombres K de genre g est une courbe projective lisse associée à une courbe plane affine donnée par une équation de la forme

$$y^2 = f(x),$$

où $f \in K[X]$ est un polynôme sans facteur carré avec $\deg(f) = 2g + 1$ ou $\deg(f) = 2g + 2$.

Les courbes hyperelliptiques sont une classe de courbes algébriques et sont une généralisation naturelle des courbes elliptiques. Il existe des courbes hyperelliptiques de tout genre $g \geq 1$. Une courbe hyperelliptique de genre $g = 1$ est une courbe elliptique. Nous voyons que lorsque nous avons un point (x, y) sur cette courbe $\mathcal{C}$, alors nous avons aussi $(x, -y)$ sur $\mathcal{C}$. Cela nous donne une application bijective sur $\mathcal{C}$ appelée l'involution hyperelliptique définie par

$$\varphi : \mathcal{C} \longrightarrow \mathcal{C}, \quad (x, y) \longmapsto (x, -y).$$

Dans ce qui suit, on exige que f ait un degré d'au moins 5. Cela correspond à restreindre le genre $g \geq 2$. Si le degré de f est égal à $2g+1$, la courbe possède un unique point $K-$rationnel à l'infini $P_\infty = (1:0:0)$. On dit que la courbe a un modèle imaginaire. Lorsque le degré de f est égal à $2g+2$, il y a deux points à l'infini $\infty_{\pm s} = (1:\pm s:0)$, où s est une racine carrée du coefficient dominant de f. Ces points sont $K-$rationnels si, et seulement si $s \in K$, c'est-à-dire, le coefficient dominant de f est un carré dans K. On parle de modèle réel. Nous écrivons $\mathcal{C}(K)$ pour l'ensemble des points $K-$rationnels sur $\mathcal{C}$. Il s'agit des points de la courbe $\mathcal{C}$ à coordonnées dans K :

$$\mathcal{C}(K) = \begin{cases} \{(x,y) \in K^2 : y^2 = f(x)\} \cup \{P_\infty\} & \text{si } 2 \nmid \deg(f) \\ \{(x,y) \in K^2 : y^2 = f(x)\} & \text{si } 2 \mid \deg(f) \text{ et } \operatorname{lc}(f) \neq s^2 \text{ avec } s \in K \\ \{(x,y) \in K^2 : y^2 = f(x)\} \cup \{\infty_s, \infty_{-s}\} & \text{si } 2 \mid \deg(f) \text{ et } \operatorname{lc}(f) = s^2 \text{ avec } s \in K \end{cases}$$

(où $\operatorname{lc}(f)$ désigne le coefficient dominant de f).

Les points de $\mathcal{C}(K)$ autres que les points à l'infini sont appelés points finis.

Définition 2.1.2 (**Point opposé, point spécial, point ordinaire**).
Soit P un point fini de $\mathcal{C}$. L'opposé de P, noté $-P$, est donné par $-P = \varphi(P)$. Le point P est spécial si $P = \varphi(P)$; sinon on dit que P est un point ordinaire.

Pour une courbe hyperelliptique $\mathcal{C}$, une uniformisante peut être déterminée explicitement (voir [Sto14]) :

Pour les points finis $P = (u, v)$

$$t_P = \begin{cases} y - v & \text{si } P \text{ est spécial} \\ x - u & \text{si } P \text{ est ordinaire.} \end{cases}$$

Pour les points à l'infini $\infty_{\pm s}$

$$t_{\infty_{\pm s}} = \begin{cases} y/x^{g+1} & \text{si } s = 0 \\ 1/x & \text{si } s \neq 0. \end{cases}$$

Notons $J_\mathcal{C}$ la jacobienne de la courbe $\mathcal{C}$. Le célèbre théorème de Mordell-Weil affirme que le groupe $J_\mathcal{C}(K)$ des points rationnels de la jacobienne $J_\mathcal{C}$ est un groupe abélien de type fini. En d'autres termes, $J_\mathcal{C}(K)$ peut s'écrire

$$J_\mathcal{C}(K) \cong J_\mathcal{C}(K)_{\text{tors}} \oplus \mathbb{Z}^r,$$

où r est un entier naturel et $J_\mathcal{C}(K)_{\text{tors}}$ le sous-groupe de torsion de $J_\mathcal{C}(K)$. L'entier r est appelé le rang de la jacobienne $J_\mathcal{C}$. Dans le cas d'une courbe elliptique E, il est bien connu qu'il existe une bijection entre $E(\overline{K})$ et $J_E(\overline{K})$. Pour être plus précis, le théorème de Riemann-Roch, nous dit que chaque élément de $J_E(\overline{K})$ a un unique représentant de la forme $P - \mathcal{O}$, donc la bijection $E(K) \longrightarrow J_E(K)$ est donnée par $P \longmapsto [P - \mathcal{O}]$ où $[P - \mathcal{O}]$ est la classe du diviseur $P - \mathcal{O}$. Dans ce cas, l'ensemble $E(K)$ forme un groupe abélien de type fini (avec l'élément neutre $\mathcal{O}$) et la loi de groupe a une description géométrique : si P, Q sont deux points sur E à coordonnées rationnelles, alors la droite passant par P et Q (si $P = Q$, on prend la tangente à la courbe) recoupe E en un troisième point R dont les coordonnées sont également rationnelles. On définit $P + Q$ comme étant le troisième point d'intersection de E avec la droite passant par R et $\mathcal{O}$. Pour les courbes hyperelliptiques $\mathcal{C}$ de genre $g \geq 2$, il n'y a pas de loi de groupe sur $\mathcal{C}(K)$; à la place, nous travaillons sur le groupe $J_\mathcal{C}(K)$ des points rationnels de la jacobienne $J_\mathcal{C}$.

2.1.2 Jacobienne d'une courbe hyperelliptique

Nous décrivons d'abord une façon canonique de représenter les éléments de la jacobienne qui est analogue à la représentation que nous avons pour les courbes elliptiques.

Proposition 2.1.1. Soient $\mathcal{C}$ une courbe projective lisse définie sur K de genre g ayant un point $K-$rationnel P_0 fixé et $D \in \mathrm{Div}_K^0(\mathcal{C})$.
Il existe un unique diviseur effectif D_1 de degré minimal $m \leq g$, ne contenant pas P_0, tel que

$$D \sim D_1 - mP_0.$$

Un diviseur sous cette forme est dit réduit. L'entier m s'appelle le poids du diviseur. Si l'on relâche la condition $m = \deg(D_1) \leq g$, on n'a plus l'unicité et on dit que le diviseur est semi-réduit.

Démonstration.
L'existence. Considérons le diviseur $D_2 = D + gP_0$ de degré g. Soit W un diviseur canonique sur $\mathcal{C}$. D'après le théorème de Riemann-Roch

$$l(D_2) - l(W - D_2) = \deg(D_2) + 1 - g = 1.$$

Ainsi, $l(D_2) \geq 1$, ce qui assure l'existence d'une fonction rationnelle f telle que $\mathrm{div}(f) + D_2 \geq 0$. Notons D_3 le diviseur effectif $\mathrm{div}(f) + D_2$. On a $D + \mathrm{div}(f) = D_3 - gP_0$, donc

$$D \sim D_3 - gP_0.$$

Si l'on prend en compte le fait qu'il faut éliminer les éventuels P_0 intervenant dans D_3, on obtient l'existence de D_1.

L'unicité. Si D est principal, on prend $m = 0$ et $D_1 = 0$. Si D n'est pas principal, on pose $D_4 = D_1 - mP_0$ une représentation de D avec m minimal.
Vérifions que $l(D_1) = 1$. Supposons que $l(D_4 + (m-1)P_0)$ soit non nul. Alors, il existe une fonction f telle que $\mathrm{div}(f) + D_4 + (m-1)P_0 \geq 0$. Notons D_5 le diviseur effectif $\mathrm{div}(f) + D_4 + (m-1)P_0$. On a $D_4 + \mathrm{div}(f) = D_5 - (m-1)P_0$, et donc $D_5 - (m-1)P_0$ est aussi une représentation de poids $m-1$ de D, ce qui contredit la minimalité de m. Ainsi, $l(D_4 + (m-1)P_0) = 0$. Puisque, le fait de rajouter un point à un diviseur fait augmenter la dimension de l'espace vectoriel associé d'au plus une unité, donc $l(D_4 + mP_0) \leq 1$. Or le diviseur $D_4 + mP_0 = D_1$ est effectif, les fonctions constantes forment un sous-espace vectoriel de $\mathcal{L}(D_4 + mP_0)$. Il s'ensuit que

$$l(D_1) = 1.$$

Supposons maintenant qu'il existe D_1' effectif de degré m tel que $D_1' - mP_0 \sim D_1 - mP_0$. Alors il existe une fonction f telle que $\mathrm{div}(f) + D_1 = D_1' \geq 0$, d'où f appartient à $\mathcal{L}(D_1)$, donc f est une constante. Ainsi, $\mathrm{div}(f) = 0$ et $D_1 = D_1'$. ❑

Considérons $\mathcal{C} : y^2 = f(x)$ une courbe hyperelliptique imaginaire définie sur K de genre 2. La proposition précédente montre que pour chaque élément $[D]$ de $J_{\mathcal{C}}(\overline{K})$ autre que l'élément neutre a un unique représentant réduit de la forme

$$D \sim P_1 + P_2 - 2P_\infty,$$

avec $P_1 \neq -P_2$. Nous utiliserons $\{P_1,\, P_2\}$ comme notation abrégée pour la classe de diviseurs contenant $P_1 + P_2 - 2P_\infty$. Il existe alors une correspondance bijective entre les éléments de $J_{\mathcal{C}}(\overline{K})$ autre que l'élément neutre et l'ensemble des paires de points non ordonnés

$$\Big\{\{P_1,\, P_2\} : P_1,\, P_2 \in \mathcal{C}(\overline{K}),\ \ P_1 \neq -P_2\Big\}.$$

L'élément neutre de $J_{\mathcal{C}}(\overline{K})$ est $\mathcal{O} = \{P_\infty, P_\infty\}$ et les diviseurs de la forme $\{P_1, -P_1\}$ sont identifiés à $\mathcal{O}$. Ainsi,

$$J_{\mathcal{C}}(\overline{K}) = \Big\{\{P_1, P_2\} : P_1, P_2 \in \mathcal{C}(\overline{K}),\ \ P_1 \neq -P_2\Big\} \cup \{\mathcal{O}\}.$$

La loi de groupe sur $J_{\mathcal{C}}(\overline{K})$ peut être décrite géométriquement de la même manière que pour les courbes elliptiques. L'inverse d'un diviseur $\{P_1, P_2\}$ est

$$-\{P_1, P_2\} = \{-P_1, -P_2\}.$$

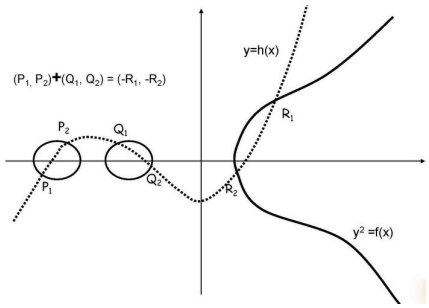
Soient $D_1 = \{P_1, P_2\}$ et $D_2 = \{Q_1, Q_2\}$ deux éléments de $J_{\mathcal{C}}(\overline{K})$. Il existe un unique polynôme $h \in \overline{K}[X]$ de degré 3 (voir [CF96]) tel que $y = h(x)$ passant par les quatre points P_1, P_2, Q_1, Q_2. Cette courbe coupe $\mathcal{C}$ en deux autres points R_1 et R_2 et donc

$$D_1 + D_2 + \{R_1, R_2\} = \mathcal{O}.$$

Ce qui s'écrit aussi,

$$\{P_1, P_2\} + \{Q_1, Q_2\} = \{-R_1, -R_2\}.$$

La construction géométrique qui donne $D_1 + D_2$ est illustrée dans la figure suivante.



Un élément $\{P_1, P_2\}$ de $J_{\mathcal{C}}(\overline{K})$ est d'ordre 2 si $\{P_1, P_2\} \neq \mathcal{O}$ et $\{P_1, P_2\} = -\{P_1, P_2\}$. Il s'ensuit que les éléments de la forme $\{(x_1, 0), (x_2, 0)\}$ où x_1, x_2 sont des racines distinctes de $f(x)$ sont d'ordre 2. De même que les éléments de la forme $\{(x_1, 0), P_\infty\}$ où x_1 est une racine de $f(x)$ sont d'ordre 2. Ce sont précisément tous les points d'ordre 2 sur $J_{\mathcal{C}}(\overline{K})$. Ainsi, le sous-groupe de $J_{\mathcal{C}}(\overline{K})$ des points de $2-$torsion, que l'on note $J_{\mathcal{C}}(\overline{K})[2]$ a 16 éléments : il y a les 15 éléments d'ordre 2 dans $J_{\mathcal{C}}(\overline{K})$ et l'élément neutre $\mathcal{O}$.

Le groupe de Galois G_K agit sur $J_{\mathcal{C}}(\overline{K})$ comme suit

$$\{P_1, P_2\}^\sigma = \{P_1^\sigma, P_2^\sigma\}.$$

Ainsi, l'ensemble $J_{\mathcal{C}}(K)$ des points rationnels de la jacobienne $J_{\mathcal{C}}(\overline{K})$ est donné par

$$J_{\mathcal{C}}(K) = \Big\{\{P_1, P_2\} \in J_{\mathcal{C}}(\overline{K}) : \{P_1, P_2\}^\sigma = \{P_1, P_2\} \text{ pour tout } \sigma \in G_K\Big\}.$$

Il en résulte qu'un élément $\{P_1, P_2\} \in J_{\mathcal{C}}(\overline{K})$ est $K-$rationnel si :

(i) soit $P_1, P_2 \in \mathcal{C}(K)$ ou

(ii) soit P_1 et P_2 sont définis sur une extension quadratique de K et conjugués sur K, c'est-à-dire, il existe une extension quadratique $K(\sqrt{\alpha})$ de K telle que

$$P_1 = (a + b\sqrt{\alpha},\ c + d\sqrt{\alpha}) \text{ et } P_2 = (a - b\sqrt{\alpha},\ c - d\sqrt{\alpha}).$$

Nous allons décrire une représentation polynômiale pour les diviseurs semi-réduits de la jacobienne. Une façon pratique de le faire est d'utiliser la représentation de Mumford [Mum84]. Nous présentons ensuite l'algorithme de Cantor [Can87] pour l'addition des diviseurs représentés en forme de Mumford.

Définition 2.1.3. Soit $\mathcal{C} : y^2 = f(x)$ une courbe hyperelliptique imaginaire définie sur K de genre 2. Tout élément $D = \{P_1 = (x_1, y_1), P_2 = (x_2, y_2)\} \in J_{\mathcal{C}}(\overline{K})$ peut être représenté par une paire unique de polynômes $u(x)$ et $v(x)$, $u, v \in K[x]$, où

- $u(x) = (x - x_1)(x - x_2)$,
- $\deg(v) < \deg(u) \leq 2$,
- $v(x_i) = y_i$ pour $1 \leq i \leq 2$,
- u divise $v^2 - f$.

On dit que $u(x)$ et $v(x)$ sont les coordonnées de Mumford du diviseur D. $(u(x), v(x))$ est la représentation de Mumford du diviseur D.

Le polynôme u code les abscisses des points du support de D tandis que v code leurs ordonnées. La dernière condition permet de prendre en compte les multiplicités des points.

Explicitement, étant donné $D = \{P_1 = (x_1, y_1), P_2 = (x_2, y_2)\}$ un élément de $J_{\mathcal{C}}(\overline{K})$. Alors D est représenté par

- si $P_1 \neq -P_2$, $u(x) = (x - x_1)(x - x_2)$ et $y = v(x)$ est l'unique droite passant par P_1 et P_2 ;
- si $P_1 = P_2$, $u(x) = (x - x_1)^2$ et $y = v(x)$ est la droite tangente à $\mathcal{C}$;
- lorsque nous avons $\{P_1, P_\infty\}$, alors $u(x) = x - x_1$ et $v(x) = y_1$;
- l'élément neutre $\mathcal{O} = \{P_\infty, P_\infty\}$ est représenté par $(1, 0)$.

L'algorithme de Cantor (voir [Kob89] pour une généralisation sur un corps arbitraire) permet de trouver le diviseur réduit (en coordonnées de Mumford) représentant la somme de deux diviseurs réduits D_1 et D_2 de $J_{\mathcal{C}}(\overline{K})$ représentés en forme de Mumford. Il se décompose en deux étapes : la première étape (points 1 à 4) consiste à calculer les coordonnées du diviseur semi-réduit $D_1 + D_2$ et la deuxième étape (points 5 à 8) consiste à le réduire jusqu'à obtenir un diviseur de poids inférieur ou égal à 2.

Algorithm 1 Algorithme de Cantor

Entrée : les coordonnées de Mumford (u_1, v_1) et (u_2, v_2) de deux diviseurs D_1 et D_2 de $J_{\mathcal{C}}$ où $\mathcal{C}$ est la courbe d'équation $y^2 = f(x)$.
Sortie : les coordonnées de Mumford (u, v) de $D_1 + D_2$

1. $d_1 \leftarrow \text{pgcd}(u_1, u_2) = e_1u_1 + e_2u_2$
2. $d_2 \leftarrow \text{pgcd}(d_1, u_1 + u_2) = c_1d_1 + c_2(u_1 + u_2)$
3. $s_1 \leftarrow c_1e_1$, $s_2 \leftarrow c_1e_2$ et $s_3 \leftarrow c_2$
4. $u \leftarrow \dfrac{u_1u_2}{d_2^2}$ et $v \leftarrow \dfrac{s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)}{d_2} \pmod{u}$
5. **tant que** $\deg(u) > 2$ **faire :**
6. $u' \leftarrow \dfrac{f - v^2}{u}$ et $v' \leftarrow -v \pmod{u'}$
7. $u \leftarrow u'$ et $v \leftarrow v'$
8. **fin tant que**
9. rendre u unitaire
10. **retourner** (u, v).

Des formules explicites ont été données par Lange [Lan05] et un compte rendu complet des différents algorithmes d'addition peut être trouvé dans [CF06]. Pour le modèle réel, on peut se référer à [GHM08].

2.1.3 Cohomologie galoisienne

Dans cette section, nous discutons des propriétés de base de la cohomologie des groupes. Comme nous n'avons besoin que de H^0 et H^1, nous avons limité notre attention à ces deux groupes. Nous passons ensuite en revue les complétions des corps, le groupe de $2-$Selmer et le groupe de Tate-Shafarevich. Pour une discussion plus détaillée de ces notions, on pourra se référer à [Mor96], [Mil22], [Wei08], [HS00], [Hei98], [BG06], [Ser02], [Sto01], [Sch95], [Mül15].

Définition 2.1.4. Soit G un groupe. On dit que G est un groupe topologique si G a une topologie dans laquelle les applications $G \times G \longrightarrow G,\ (x, y) \mapsto xy$ et $G \longrightarrow G,\ x \mapsto x^{-1}$ sont continues.

Soit L/K une extension galoisienne de corps. Notons

$$\mathcal{N} = \Big\{F \ :\ K \subseteq F \subseteq L,\ [F : K] < +\infty \text{ et } F/K \text{ est galoisienne}\Big\}.$$

On définit une base $\mathcal{B}$ d'une topologie sur $\text{Gal}(L/K)$ par

$$\mathcal{B} = \Big\{\sigma\text{Gal}(L/F) \ :\ \sigma \in \text{Gal}(L/K) \text{ et } F \in \mathcal{N}\Big\}.$$

Ainsi, tout sous-ensemble de $\text{Gal}(L/K)$ est un ouvert si, et seulement si c'est l'union d'éléments de $\mathcal{B}$. On peut vérifier que cela définit une topologie. Cette topologie sur $\text{Gal}(L/K)$ est appelée topologie de Krull. Dans cette topologie, la composition $(\sigma, \tau) \mapsto \sigma\tau$ et l'inversion $\sigma \mapsto \sigma^{-1}$ sont continues. Cela fait de $\text{Gal}(L/K)$ un groupe topologique. En particulier, en prenant $L = \overline{K}$, on obtient une topologie sur $G_K = \text{Gal}(\overline{K}/K)$.

Définition 2.1.5. On dit qu'un ensemble M est un G_K-module à gauche si M est un groupe abélien et s'il existe une application $G_K \times M \to M$ définie par $(\sigma, m) \mapsto {}^{\sigma}m$ telle que

(i) ${}^{\sigma}(m+m') = {}^{\sigma}m + {}^{\sigma}m'$, pour tous $m,\ m' \in M$;

(ii) ${}^{\sigma\tau}m = {}^{\sigma}({}^{\tau}m)$, pout tous $\sigma,\ \tau \in G_K$ et $m \in M$;

(iii) ${}^{1}m = m$, pour tout $m \in M$ et 1 désigne l'élément neutre de G_K.

Pour un G_K-module M donné, nous sommes intéressés par le plus grand sous-module de M sur lequel G_K agit trivialement.

Définition 2.1.6. On définit le $0^{\text{ième}}$ groupe de cohomologie d'un G_K-module M que l'on note $\mathrm{H}^0(G_K,\, M)$ ou M^{G_K} comme étant le groupe

$$\mathrm{H}^0(G_K,\, M) = \Big\{ m \in M \ :\ {}^{\sigma}m = m,\ \forall\, \sigma \in G_K \Big\}.$$

Soit M un G_K-module. Une application $\xi : G_K \to M$ est continue si elle est continue pour la topologie de Krull sur G_K et la topologie discrète sur M. De manière équivalente, pour chaque $m \in M$, l'ensemble $\xi^{-1}(\{m\})$ est l'union des éléments de la base $\mathcal{B}$.

Le groupe des $1-$cochaînes de G_K dans M, noté $\mathcal{C}^1(G_K,\, M)$, est défini par

$$\mathcal{C}^1(G_K,\, M) = \Big\{ \text{applications continues } \xi : G_K \to M \Big\}.$$

Le groupe des $1-$cocycles continues de G_K dans M, noté $Z^1(G_K,\, M)$, est défini par

$$Z^1(G_K,\, M) = \Big\{ \xi \in \mathcal{C}^1(G_K,\, M)\ : \xi(\sigma\tau) = {}^{\sigma}\xi(\tau) + \xi(\sigma),\ \forall\, \sigma,\ \tau \in G_K \Big\}.$$

Le groupe des $1-$cobords continues de G_K dans M, noté $B^1(G_K,\, M)$, est défini par

$$B^1(G_K,\, M) = \Big\{ \xi \in \mathcal{C}^1(G_K,\, M)\ : \exists\, m \in M,\ \xi(\sigma) = {}^{\sigma}m - m,\ \forall\, \sigma \in G_K \Big\}.$$

On observe que $B^1(G_K,\, M)$ est un sous-groupe de $Z^1(G_K,\, M)$. Cela se voit de la manière suivante : soit $\xi \in B^1(G_K,\, M)$, on a

$$\xi(\sigma\tau) = {}^{\sigma\tau}m - m = {}^{\sigma\tau}m - {}^{\sigma}m + {}^{\sigma}m - m = {}^{\sigma}\xi(\tau) + \xi(\sigma).$$

Définition 2.1.7. On définit le 1^{er} groupe de cohomologie d'un G_K-module M comme étant le groupe quotient

$$\mathrm{H}^1(G_K,\, M) = \frac{Z^1(G_K,\, M)}{B^1(G_K,\, M)}.$$

Un élément de $\mathrm{H}^1(G_K,\, M)$ est appelé classe de cohomologie et est écrite $[\xi]$ pour un $1-$cocycle ξ.

Définition 2.1.8. Soient M, N des G_K-modules. Un homomorphisme de G_K-modules est un homomorphisme $\psi : M \longrightarrow N$ qui commute avec l'action de G_K, c'est-à-dire,

$$\psi({}^{\sigma}m) = {}^{\sigma}\psi(m),\ \forall\, m \in M \text{ et } \sigma \in G_K.$$

On définit une suite exacte de G_K-modules P, M, N comme étant une suite

$$0 \longrightarrow P \xrightarrow{\ \phi\ } M \xrightarrow{\ \psi\ } N \longrightarrow 0$$

où ϕ et ψ des homomorphismes de G_K-modules, ϕ injectif, ψ surjectif et $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$.

Proposition 2.1.2. Soit $0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$ une suite exacte de G_K-modules. Alors, il existe une suite exacte longue de groupes de cohomologie

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0(G_K,\, P) &\xrightarrow{\phi} \mathrm{H}^0(G_K,\, M) \xrightarrow{\psi} \mathrm{H}^0(G_K,\, N) \\ &\xrightarrow{\delta} \mathrm{H}^1(G_K,\, P) \xrightarrow{\phi_1} \mathrm{H}^1(G_K,\, M) \xrightarrow{\psi_1} \mathrm{H}^1(G_K,\, N), \end{aligned}$$

où l'application δ est définie de la manière suivante : soit $n \in \mathrm{H}^0(G_K,\, N)$, il existe $m \in M$ tel que $\psi(m) = n$. Comme n est invariant sous G_K, pour tout $\sigma \in G_K$, $\psi({}^{\sigma}m - m) = 0$, et donc ${}^{\sigma}m - m \in \mathrm{Im}(\phi) \cong P$. On définit une $1-$cochaîne $\xi \in \mathcal{C}^1(G_K,\, P)$ par $\xi(\sigma) = {}^{\sigma}m - m$. Alors $\xi \in Z^1(G_K,\, P)$ et $\delta(n)$ est la classe de cohomologie dans $\mathrm{H}^1(G_K,\, P)$ du $1-$cocycle ξ

$$\delta(n) : G_K \longrightarrow P, \qquad \sigma \longmapsto \delta(n)(\sigma) = {}^{\sigma}m - m.$$

Considérons un autre élément m' de M tel que $\psi(m') = n$. Alors, la différence $m - m'$ est dans P et donc ${}^{\sigma}(m - m') - (m - m')$ est dans $\mathrm{B}^1(G_K,\, P)$. Ainsi, l'application $\delta(n)$ est bien définie.

Définition 2.1.9. Soit K un corps. Une valuation sur K est une fonction $v : K \to \mathbb{R} \cup \{\infty\}$ vérifiant

- $v(x + y) \geq \min\{v(x),\, v(y)\}$;
- $v(xy) = v(x) + v(y)$;
- $v(x) = \infty$ si, et seulement si $x = 0$.

On dit que deux valuations v_1 et v_2 sont équivalentes s'il existe $\lambda \in \mathbb{R}_+^*$ tel que $v_1 = \lambda v_2$. Une valuation v est dite discrète si $v(K^*) \subset \mathbb{Z}$.

Définition 2.1.10. Soit K un corps. Une valeur absolue sur K est une fonction $|.| : K \to \mathbb{R}$ satisfaisant les trois propriétés suivantes :

(a) $|x| \geq 0$ pour tout $x \in K$ et $|x| = 0$ si, et seulement si $x = 0$;

(b) $|xy| = |x||y|$ pour tous $x,\, y \in K$;

(c) $|x + y| \leq |x| + |y|$ pour tous $x,\, y \in K$ (inégalité triangulaire).

Si au lieu de (c), la valeur absolue satisfait la condition plus forte

$$(c)' \qquad |x + y| \leq \max\{|x|,\, |y|\}, \quad \text{(inégalité ultramétrique)}$$

alors, elle est dite non-archimédienne. Si $(c)'$ ne tient pas pour un certain $x,\, y \in K$, la valeur absolue est dite archimédienne.
La valeur absolue triviale est égale

$$|x| = \begin{cases} 1 & \text{si } x \neq 0 \\ 0 & \text{si } x = 0. \end{cases}$$

Les définitions 2.1.9 et 2.1.10 sont liées dans le sens où toute valuation peut-être transformée en une valeur absolue non-archimédienne et vice versa. En effet, soit v une valuation sur K et soit $a > 1$ un nombre réel fixé. On définit une valeur absolue non-archimédienne sur K comme suit :

$$|x| = \begin{cases} a^{-v(x)} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0. \end{cases}$$

Si on considère une valeur absolue $|.|$ non-archimédienne sur K, on définit une valuation v comme suit :

$$v(x) = \begin{cases} -\log(|x|) & \text{si } x \neq 0 \\ \infty & \text{si } x = 0. \end{cases}$$

Ces applications sont chacune inverse l'une de l'autre. C'est pourquoi lorsqu'on parle d'une valuation sur un corps K, on peut utiliser la valeur absolue associée à la valuation également et vice versa.

Soit K un corps de nombres et v une valuation discrète sur K dont on associe une valeur absolue $|.|$ non-archimédienne. Alors on peut définir une métrique d sur K par $d(x, y) = |x - y|$ pour tous $x, y \in K$. Cette métrique induit une topologie sur K. Deux valeurs absolues non-triviales sont dites équivalentes si elles définissent la même topologie. Autrement dit, deux valeurs alsolues $|.|_1$ et $|.|_2$ sont équivalentes s'il existe un nombre réel positif λ tel que

$$|x|_1 = |x|_2^{\lambda}, \qquad \text{pour tout } x \in K.$$

Une place v est une classe d'équivalence de valeurs absolues non-triviale.
Soient L/K une extension de corps, v une place sur K et w une place sur L. On dit que w divise v (ou w se trouve sur v) et on écrit $w|v$ si la restriction à K de tout représentant de w est un représentant de v.

La complétion de K par rapport à la place v est une extension de corps K_v avec une place w telle que

i) $w|v$;

ii) la topologie de K_v induit par w est complète ;

iii) K est un sous-ensemble dense de K_v dans la topologie ci-dessus.

Par abus de notation, nous désignerons w par v.

Soit A une variété abélienne définie sur un corps de nombres K. On sait que l'application de multiplication par 2

$$[2] : A(\overline{K}) \longrightarrow A(\overline{K}), \qquad P \longmapsto 2P$$

est surjective et notons $A(\overline{K})[2]$ le noyau de cette application. Alors la suite exacte suivante

$$0 \longrightarrow A(\overline{K})[2] \xrightarrow{i} A(\overline{K}) \xrightarrow{[2]} A(\overline{K}) \longrightarrow 0$$

induit une suite exacte longue de groupes de cohomologie

$$\begin{aligned} 0 \longrightarrow A(K)[2] \longrightarrow A(K) \xrightarrow{[2]} A(K) \xrightarrow{\delta} \mathrm{H}^1(G_K, A(\overline{K})[2]) \\ \longrightarrow \mathrm{H}^1(G_K, A(\overline{K})) \xrightarrow{[2]} \mathrm{H}^1(G_K, A(\overline{K})). \end{aligned}$$

L'homomorphisme de connexion δ induit une application injective

$$A(K)/2A(K) \hookrightarrow \mathrm{H}^1(G_K, A(\overline{K})[2]),$$

car $\mathrm{Ker}(\delta) = \mathrm{Im}([2]) = 2A(K)$. Notons $\mathrm{H}^1(G_K, A(\overline{K}))[2]$ le noyau de l'application

$$[2] : \mathrm{H}^1(G_K, A(\overline{K})) \longrightarrow \mathrm{H}^1(G_K, A(\overline{K})).$$

Nous obtenons ainsi la suite exacte fondamentale suivante

$$0 \longrightarrow A(K)/2A(K) \xrightarrow{\delta} \mathrm{H}^1(G_K, A(\overline{K})[2]) \longrightarrow \mathrm{H}^1(G_K, A(\overline{K}))[2] \longrightarrow 0.$$

Soit v une place sur K. Soient K_v la complétion de K en v et $G_v = \mathrm{Gal}(\overline{K_v}/K_v)$ le groupe de Galois sur K_v. Comme précédemment, nous obtenons une suite exacte fondamentale suivante

$$0 \longrightarrow A(K_v)/2A(K_v) \xrightarrow{\delta_v} \mathrm{H}^1(G_v, A(\overline{K_v})[2]) \longrightarrow \mathrm{H}^1(G_v, A(\overline{K_v}))[2] \longrightarrow 0.$$

L'inclusion $G_v \hookrightarrow G_K$ nous donne des applications de restriction $\mathrm{H}^1(G_K, -) \longrightarrow \mathrm{H}^1(G_v, -)$. Nous obtenons ainsi le diagramme commutatif suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/2A(K) & \xrightarrow{\delta} & \mathrm{H}^1(G_K,\, A(\overline{K})[2]) & \longrightarrow & \mathrm{H}^1(G_K,\, A(\overline{K}))[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(K_v)/2A(K_v) & \xrightarrow{\delta_v} & \mathrm{H}^1(G_v,\, A(\overline{K_v})[2]) & \longrightarrow & \mathrm{H}^1(G_v,\, A(\overline{K_v}))[2] & \longrightarrow & 0. \end{array}$$

Le groupe de 2−Selmer est défini comme suit

$$\mathrm{Sel}^2(A/K) = \bigcap_v \ker\Big\{\mathrm{H}^1(G_K,\, A(\overline{K})[2]) \longrightarrow \mathrm{H}^1(G_v,\, A(\overline{K_v}))[2]\Big\},$$

et le groupe de Tate-Shafarevich de A/K est

$$Ш(A/K) = \bigcap_v \ker\Big\{\mathrm{H}^1(G_K,\, A(\overline{K})) \longrightarrow \mathrm{H}^1(G_v,\, A(\overline{K_v}))\Big\}.$$

Proposition 2.1.3. On a la suite exacte suivante

$$0 \longrightarrow A(K)/2A(K) \longrightarrow \mathrm{Sel}^2(A/K) \longrightarrow Ш(A/K)[2] \longrightarrow 0.$$

Intéressons-nous au cas où A est la jacobienne $J_{\mathcal{C}}$ d'une courbe hyperelliptique imaginaire $\mathcal{C} : y^2 = f(x)$ définie sur $\mathbb{Q}$ de genre 2. D'après la proposition précédente, on a

$$0 \longrightarrow J_{\mathcal{C}}(\mathbb{Q})/2J_{\mathcal{C}}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^2(J_{\mathcal{C}}/\mathbb{Q}) \longrightarrow Ш(J_{\mathcal{C}}/\mathbb{Q})[2] \longrightarrow 0.$$

Le groupe de 2−Selmer $\mathrm{Sel}^2(J_{\mathcal{C}}/\mathbb{Q})$ est fini, ce qui entraîne la finitude de $J_{\mathcal{C}}(\mathbb{Q})/2J_{\mathcal{C}}(\mathbb{Q})$. Il a été conjecturé que le sous-groupe de 2−torsion $Ш(J_{\mathcal{C}}/\mathbb{Q})[2]$ est aussi fini. Ces groupes ont une structure de $\mathbb{F}_2$-espace vectoriel. Ainsi, on obtient la formule

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}}/\mathbb{Q}) = \dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})/2J_{\mathcal{C}}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(J_{\mathcal{C}}/\mathbb{Q})[2].$$

Puisque $\dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})/2J_{\mathcal{C}}(\mathbb{Q}) = \mathrm{rang}(J_{\mathcal{C}}(\mathbb{Q})) + \dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})[2]$, il en résulte que

$$\mathrm{rang}(J_{\mathcal{C}}(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}}/\mathbb{Q}) - \dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})[2].$$

La dimension de $\dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})[2]$ peut être calculer à partir de la factorisation du polynôme $f(x)$ dans $\mathbb{Q}[X]$:

$$\dim_{\mathbb{F}_2} J_{\mathcal{C}}(\mathbb{Q})[2] = -1 + \#\{\text{facteurs irréductibles de } f(x) \text{ dans } \mathbb{Q}[X]\}.$$

Ainsi, si on sait ou détermine $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}}/\mathbb{Q})$, on obtient une borne supérieure de r.

2.2 Points algébriques de degré donné sur les courbes hyperelliptiques $y^2 = x^5 + n^2$

Soit A un entier naturel non nul. Soit $\mathcal{C}_A$ la courbe hyperelliptique définie sur $\mathbb{Q}$ de genre 2 d'équation affine

$$\mathcal{C}_A : y^2 = x^5 + A.$$

Stoll [Sto98, Sto02] a étudié l'arithmétique des courbes $\mathcal{C}_A$ et de leurs jacobiennes $J_{\mathcal{C}_A}$. Sous des conditions appropriées sur A, il donne des bornes pour les rangs du groupe de Mordell-Weil $J_{\mathcal{C}_A}(\mathbb{Q})$. En utilisant ces résultats, Mulholland [Mul06, p. 177 − 178] a étudié les points $\mathbb{Q}$−rationnels sur $\mathcal{C}_A$ pour $A = \pm 2^\alpha 3^\beta$ avec $0 \leq \alpha,\, \beta \leq 9$. Il a établi le théorème suivant :

Théorème 2.2.1. Soient α et β des entiers tels que $0 \leq \alpha,\ \beta \leq 9$ et $\varepsilon \in \{\pm 1\}$. Supposons que $(\alpha,\ \beta,\ \varepsilon) \neq (3,\ 9,\ -1)$. Soit la courbe

$$\mathcal{C}_A : y^2 = x^5 + A, \quad \text{avec} \quad A = \varepsilon 2^\alpha 3^\beta.$$

Alors, les points rationnels finis sur $\mathcal{C}_A$ sont donnés dans la table 2.1.

$\mathcal{C}_A$			$\mathcal{C}_A(\mathbb{Q})\backslash\{P_\infty\}$
α	β	ε	
0	0	1	$(-1, \pm 0)$, $(0, \pm 1)$
0	0	1	$(1, \pm 2)$
0	2	1	$(0, \pm 3)$
0	4	1	$(0, \pm 9)$, $(-2, \pm 7)$, $(3, \pm 18)$
0	5	1	$(3, \pm 0)$
0	6	1	$(0, \pm 27)$
0	8	1	$(0, \pm 81)$, $(18, \pm 1377)$
1	0	1	$(-1, \pm 1)$
1	5	1	$(3, \pm 27)$
1	8	1	$(7, \pm 173)$
2	0	1	$(0, \pm 2)$, $(2, \pm 6)$
2	2	1	$(0, \pm 6)$, $(-2, \pm 2)$
2	4	1	$(0, \pm 18)$, $(-3, \pm 9)$, $(6, \pm 90)$
2	5	1	$(-3, \pm 27)$
2	6	1	$(0, \pm 54)$
2	8	1	$(0, \pm 162)$
3	0	1	$(1, \pm 3)$
3	1	1	$(1, \pm 5)$
4	0	1	$(0, \pm 4)$
4	1	1	$(1, \pm 7)$, $(-2, \pm 4)$
4	2	1	$(0, \pm 12)$
4	3	1	$(-2, \pm 20)$
4	4	1	$(0, \pm 36)$
4	5	1	$(6, \pm 108)$, $(-2, \pm 4)$
4	6	1	$(0, \pm 108)$
4	8	1	$(1, \pm 324)$, $(9, \pm 405)$
5	0	1	$(-2, \pm 0)$, $(2, \pm 8)$
5	1	1	$(-2, \pm 8)$

$\mathcal{C}_A$			$\mathcal{C}_A(\mathbb{Q})\backslash\{P_\infty\}$
α	β	ε	
5	2	1	$(1, \pm 17)$, $(-2, \pm 16)$
5	5	1	$(-6, \pm 0)$, $(-2, \pm 88)$
6	0	1	$(0, \pm 8)$
6	2	1	$(0, \pm 24)$, $(4, \pm 40)$
6	4	1	$(0, \pm 72)$, $(12, \pm 504)$
6	6	1	$(0, \pm 216)$
6	8	1	$(0, \pm 648)$
8	0	1	$(0, \pm 16)$
8	2	1	$(0, \pm 48)$
8	4	1	$(0, \pm 144)$
8	6	1	$(0, \pm 432)$
8	8	1	$(0, \pm 1296)$
0	0	-1	$(1, \pm 0)$
0	5	-1	$(3, \pm 0)$
1	2	-1	$(3, \pm 15)$
1	4	-1	$(3, \pm 9)$
3	8	-1	$(9, \pm 81)$
4	0	-1	$(2, \pm 4)$
4	2	-1	$(10, \pm 316)$
5	0	-1	$(2, \pm 0)$, $(6, \pm 88)$
5	4	-1	$(6, \pm 72)$
5	5	-1	$(6, \pm 0)$
5	6	-1	$(9, \pm 189)$
5	8	-1	$(18, \pm 1296)$
7	4	-1	$(33, \pm 6255)$
8	1	-1	$(4, \pm 16)$
8	5	-1	$(12, \pm 432)$

TABLE 2.1 – Tous les points $\mathbb{Q}-$rationnels sur $y^2 = x^5 \pm 2^\alpha 3^\beta$.

Ensuite, Bruni [Bru15, p. 142] a étudié les points $\mathbb{Q}-$rationnels sur $\mathcal{C}_A$ pour $A = \pm 2^\alpha 5^\beta$ avec $0 \leq \alpha, \beta \leq 9$. Il a énoncé le résultat suivant

Théorème 2.2.2. Soit $(\alpha, \beta) \in \{(0, 0), (0, 2), (0, 5), (0, 8), (2, 2), (2, 8), (4, 0), (4, 2), (4, 2), (6, 0), (6, 8), (8, 0), (8, 4), (8, 5)\}$. Soit la courbe

$$\mathcal{C}_A : y^2 = x^5 + A, \quad \text{avec} \quad A = 2^\alpha 5^\beta.$$

Alors, les points rationnels finis sur $\mathcal{C}_A$ sont donnés dans la table 2.2.

$\mathcal{C}_A$		
α	β	$\mathcal{C}_A(\mathbb{Q})\backslash\{P_\infty\}$
0	0	$(-1, \pm 0), (0, \pm 1)$
0	2	$(0, \pm 5)$
0	5	$(-5, \pm 0)$
0	8	$(0, \pm 625)$
2	2	$(0, \pm 10)$
2	8	$(0, \pm 1250)$
4	0	$(0, \pm 4)$
4	2	$(0, \pm 20)$
6	0	$(0, \pm 8)$
6	8	$(0, \pm 5000)$
8	0	$(0, \pm 16)$
8	4	$(0, \pm 400)$
8	5	$(20, \pm 2000)$

TABLE 2.2 – Tous les points $\mathbb{Q}-$rationnels sur $y^2 = x^5 \pm 2^\alpha 5^\beta$ pour des courbes de rang 0.

Dans cette section, nous nous intéréssons principalement à la détermination explicite de l'ensemble des points algébriques sur $\mathcal{C}_A$ de degré au plus d pour un certain entier A. Soulignons que le cas $A = 1$ remontre à Schaefer [Sch98], Fall [Fal21] et Sall, et al [SFC16]. L'objectif est d'étudier le cas $A = n^2$ avec

$$n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}.$$

Posons $P_n = (0, n)$, $\overline{P_n} = (0, -n)$ et P_∞ le point à l'infini sur $\mathcal{C}_{n^2}$. En combinant les travaux de Mulholland et Bruni, nous obtenons le théorème suivant :

Théorème 2.2.3. Soit $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Soit la courbe

$$\mathcal{C}_{n^2} : y^2 = x^5 + n^2.$$

Alors, les points $\mathbb{Q}-$rationnels sur $\mathcal{C}_{n^2}$ sont donnés par

$$\mathcal{C}_{n^2}(\mathbb{Q}) = \{P_n, \overline{P_n}, P_\infty\}.$$

Nous étendons ces résultats en donnant une description algébrique de l'ensemble des points algébriques sur $\mathcal{C}_{n^2}$ de degré au plus d sur $\mathbb{Q}$. On note cet ensemble par $\mathcal{C}_{n^2}^d(\mathbb{Q})$, ce qui s'écrit aussi $\mathcal{C}_{n^2}^d(\mathbb{Q}) = \bigcup_{[K:\mathbb{Q}]\leqslant d} \mathcal{C}_{n^2}(K)$. Notons également $\mathcal{C}_{n^2}^{(d)}(\mathbb{Q})$ l'ensemble des points algébriques sur $\mathcal{C}_{n^2}$ de degré exactement d sur $\mathbb{Q}$. Notre première contribution dans ce chapitre s'énonce comme suit :

Théorème 2.2.4. Soit $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Soit la courbe

$$\mathcal{C}_{n^2} : y^2 = x^5 + n^2.$$

Alors

1. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 2 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(2)}(\mathbb{Q}) = \left\{ \left(x, \pm\sqrt{x^5 + n^2} \right) : x \in \mathbb{Q}^* \right\}.$$
2. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 3 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(3)}(\mathbb{Q}) = \left\{ (x, \pm n - \lambda x^2) : \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } x^3 - \lambda^2 x^2 \pm 2\lambda n = 0 \right\}.$$
3. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 4 sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{(4)}(\mathbb{Q}) = \mathcal{A}_0^n \cup \mathcal{A}_1^n \cup \mathcal{A}_2^n$$
avec
$$\mathcal{A}_0^n = \left\{ \left(x, \pm\sqrt{x^5 + n^2} \right) : [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\};$$
$$\mathcal{A}_1^n = \left\{ \begin{array}{l} \left(x, \pm n - \lambda x - \mu x^2 \right) : \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ et } x \text{ racine de} \\ x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 \pm 2\mu n)x \pm 2\lambda n = 0 \end{array} \right\};$$
$$\mathcal{A}_2^n = \left\{ \begin{array}{l} \left(x, \pm n - \lambda x^2 - \mu x^3 \right) : \lambda,\ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \mu^2 x^4 + (2\lambda\mu - 1)x^3 + \lambda^2 x^2 \mp 2\mu n x \mp 2\lambda n = 0 \end{array} \right\}.$$
4. Les points algébriques sur $\mathcal{C}_{n^2}$ de degré au plus d avec $d \geq 5$ sur $\mathbb{Q}$ sont donnés par
$$\mathcal{C}_{n^2}^{d}(\mathbb{Q}) = \mathcal{D}_0^n \cup \mathcal{D}_1^n \cup \mathcal{D}_2^n \cup \mathcal{D}_3^n$$
avec
$$\mathcal{D}_0^n = \left\{ \left(x, \pm\sqrt{x^5 + n^2} \right) : [\mathbb{Q}(x) : \mathbb{Q}] \leq \frac{d}{2} \text{ si } d \text{ est pair} \right\};$$
$$\mathcal{D}_1^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0 \leq i \leq \frac{d}{2}} a_i x^i}{\sum\limits_{0 \leq j \leq \frac{d-5}{2}} b_j x^j} \right) : a_{\frac{d}{2}} \neq 0 \text{ et } \exists\, b_j \neq 0 \text{ si } d \text{ est pair, } b_{\frac{d-5}{2}} \neq 0 \text{ si } d \\ \text{est impair et } x \text{ racine de } \left(\sum\limits_{i=0}^{\frac{d}{2}} a_i x^i \right)^2 - \left(\sum\limits_{j=0}^{\frac{d-5}{2}} b_j x^j \right)^2 (x^5 + n^2) = 0 \end{array} \right\};$$
$$\mathcal{D}_2^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0 \leq i \leq \frac{d+1}{2}} a_i x^i}{\sum\limits_{0 \leq j \leq \frac{d-4}{2}} b_j x^j} \right) : a_0 = \pm n b_0, a_{\frac{d+1}{2}} \neq 0 \text{ si } d \text{ est impair, } b_{\frac{d-4}{2}} \neq 0 \text{ si } d \\ \text{est pair et } x \text{ racine de } \left(\sum\limits_{i=0}^{\frac{d+1}{2}} a_i x^i \right)^2 - \left(\sum\limits_{j=0}^{\frac{d-4}{2}} b_j x^j \right)^2 (x^5 + n^2) = 0 \end{array} \right\};$$
$$\mathcal{D}_3^n = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0 \leq i \leq \frac{d+2}{2}} a_i x^i}{\sum\limits_{0 \leq j \leq \frac{d-3}{2}} b_j x^j} \right) : a_0 = \pm n b_0, a_1 = \pm n b_1, a_{\frac{d+2}{2}} \neq 0 \text{ si } d \text{ est pair, } b_{\frac{d-3}{2}} \neq 0 \\ \text{si } d \text{ est impair et } x \text{ racine de } \left(\sum\limits_{i=0}^{\frac{d+2}{2}} a_i x^i \right)^2 - \left(\sum\limits_{j=0}^{\frac{d-3}{2}} b_j x^j \right)^2 (x^5 + n^2) = 0 \end{array} \right\}.$$

2.2.1 Lemmes fondamentaux

Le lemme suivant donne la structure de $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ des points rationnels de la jacobienne $J_{\mathcal{C}_{n^2}}$. Pour toutes les courbes $\mathcal{C}_{n^2}$, nous utiliserons MAGMA [Mag10] pour calculer le sous-groupe de torsion $J_{\mathcal{C}_{n^2}}(\mathbb{Q})_{\text{tors}}$ et le rang de la jacobienne $J_{\mathcal{C}_{n^2}}$.

Lemme 2.2.1. *$J_{\mathcal{C}_{n^2}}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.*

Démonstration. A titre d'exemple, nous traitons la courbe $\mathcal{C}_{4^2} : y^2 = x^5 + 4^2$ définie sur $\mathbb{Q}$. Pour commencer, nous définissons l'anneau $\mathbb{Q}[X]$ des polynômes en une indéterminée et à coefficients dans $\mathbb{Q}$, la courbe hyperelliptique $\mathcal{C}_{4^2}$ et sa jacobienne $J_{\mathcal{C}_{4^2}}$. Ensuite, nous calculons le sous-groupe de torsion $J_{\mathcal{C}_{4^2}}(\mathbb{Q})_{\text{tors}}$.

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^5+4^2);
> J:=Jacobian(C);
> Jtors, map :=TorsionSubgroup(J);
> Jtors;
```

Abelian Group isomorphic to $\mathbb{Z}/5$
Defined on 1 generator
Relations :
$5 * P[1] = 0$

Ceci montre que $J_{\mathcal{C}_{4^2}}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$.

Il ne nous reste plus qu'à déterminer le rang de la jacobienne $J_{\mathcal{C}_{4^2}}$. Pour cela, nous pouvons utiliser la commande **RankBounds**.

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^5+4^2);
> J:=Jacobian(C);
> RankBounds(J);
```

0 0.

La sortie de **RankBounds** est une borne inférieure sur le rang suivie d'une borne supérieure sur le rang, qui sont toutes deux égales à 0. Par conséquent, le rang de $J_{\mathcal{C}_{4^2}}$ est 0. Par suite, $J_{\mathcal{C}_{4^2}}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Les autres cas se traitent de la même manière. ❑

Soient x et y les fonctions sur $\mathcal{C}_{n^2}$ définies par

$$x(X, Y, Z) = \frac{X}{Z} \text{ et } y(X, Y, Z) = \frac{Y}{Z^3}.$$

L'équation projective de la courbe $\mathcal{C}_{n^2}$ lisse est donnée par

$$\mathcal{C}_{n^2} : Y^2 = X^5 Z + n^2 Z^6.$$

Lemme 2.2.2.

(i) $\mathrm{div}(y-n) = 5P_n - 5P_\infty$, $\mathrm{div}(y+n) = 5\overline{P_n} - 5P_\infty$;

(ii) $\mathrm{div}(x) = P_n + \overline{P_n} - 2P_\infty$, $\mathrm{div}(y) = A_0^n + \cdots + A_4^n - 5P_\infty$.

Démonstration. Nous appliquons la formule suivante :

$$\mathrm{div}(x-\alpha) = (X - \alpha Z = 0).\mathcal{C}_{n^2} - (Z=0).\mathcal{C}_{n^2},$$

avec $\alpha \in \mathbb{Z}$ où $\Gamma.\mathcal{C}_{n^2}$ est le cycle d'intersection d'une courbe algébrique Γ définie sur $\mathbb{Q}$ et la courbe $\mathcal{C}_{n^2}$. En effet,

- On a $\mathrm{div}(y-n) = (Y - nZ^3 = 0).\mathcal{C}_{n^2} - 3(Z=0).\mathcal{C}_{n^2}$.
  - Si $Y - nZ^3 = 0$, alors $X^5 Z = 0$ ce qui implique $X^5 = 0$ ou $Z = 0$, on obtient P_n avec la multiplicité 5 ou P_∞ avec la multiplicité 1 ; ainsi $(Y - nZ^3 = 0).\mathcal{C}_{n^2} = 5P_n + P_\infty$.
  - Si $Z = 0$, $Y^2 = 0$, on obtient P_∞ avec la multiplicité 2 ; par suite $(Z=0).\mathcal{C}_{n^2} = 2P_\infty$.

  En définitive, on a $\mathrm{div}(y-n) = 5P_n - 5P_\infty$.

  De même, on vérifie que $\mathrm{div}(y+n) = 5\overline{P_n} - 5P_\infty$ et $\mathrm{div}(x) = P_n + \overline{P_n} - 2P_\infty$.
- On a $\mathrm{div}(y) = (Y=0).\mathcal{C}_{n^2} - 3(Z=0).\mathcal{C}_{n^2}$.
  - Si $Y = 0$, $X^5 Z + n^2 Z^6 = 0$ ce qui implique $Z = 0$ ou $X^5 + n^2 Z^5 = 0$. Soit η une racine primitive $10^{\text{ième}}$ de l'unité dans $\overline{\mathbb{Q}}$, posons $A_k^n = (\sqrt[5]{n^2}\eta^{2k+1}, 0)$ avec $0 \le k \le 4$. On obtient P_∞ avec la multiplicité 1 ou les A_k^n avec la multiplicité 1 en chacun de ces points ; donc $(Y=0).\mathcal{C}_{n^2} = A_0^n + \cdots + A_4^n + P_\infty$.
  - Si $Z = 0$, $Y^2 = 0$, on obtient P_∞ avec la multiplicité 2 ; par suite $(Z=0).\mathcal{C}_{n^2} = 2P_\infty$.

  En définitive, on a $\mathrm{div}(y) = A_0^n + \cdots + A_4^n - 5P_\infty$.

❑

Posons $D_n = j(P_n) = [P_n - P_\infty]$.
Vérifions par exemple à l'aide de l'algorithme de Cantor que $5D_4 = \mathcal{O}$. On a

$$\begin{aligned} D_4 &\longleftrightarrow (x,\, 4),\\ 2D_4 = D_4 + D_4 &\longleftrightarrow (x^2,\, 4),\\ 3D_4 = 2D_4 + D_4 &\longleftrightarrow (x^2,\, -4),\\ 4D_4 = 3D_4 + D_4 &\longleftrightarrow (x,\, -4),\\ 5D_4 = 4D_4 + D_4 &\longleftrightarrow (1,\, 0). \end{aligned}$$

Nous voyons que D_4 est d'ordre 5 dans $J_{\mathcal{C}_{4^2}}(\mathbb{Q})$. De même, on montre que $5j(\overline{P_4}) = \mathcal{O}$ et $j(P_4) + j(\overline{P_4}) = \mathcal{O}$. Ainsi, $j(P_4)$ et $j(\overline{P_4})$ engendrent le même groupe $J_{\mathcal{C}_{4^2}}(\mathbb{Q})$ qui est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

Plus généralement, on a $5j(P_n) = \mathcal{O}$, $5j(\overline{P_n}) = \mathcal{O}$ et $j(P_n) + j(\overline{P_n}) = \mathcal{O}$. Par suite, $j(P_n)$ et $j(\overline{P_n})$ engendrent le même groupe $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ qui est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

Lemme 2.2.3. On a

$$\mathcal{L}(P_\infty) =< 1 >,\quad \mathcal{L}(2P_\infty) = \mathcal{L}(3P_\infty) =< 1,\, x >,\quad \mathcal{L}(4P_\infty) =< 1,\, x,\, x^2 >,$$
$$\mathcal{L}(5P_\infty) =< 1,\, x,\, x^2,\, y >,\quad \mathcal{L}(6P_\infty) =< 1,\, x,\, x^2,\, y,\, x^3 > .$$

Plus généralement, pour $p \geq 5$, une $\overline{\mathbb{Q}}-$ base pour $\mathcal{L}(pP_\infty)$ est donnée par

$$\mathcal{B}_p = \Big\{x^i \,:\, i \in \mathbb{N} \text{ et } 0 \leq i \leq \frac{p}{2}\Big\} \cup \Big\{yx^j \,:\, j \in \mathbb{N} \text{ et } 0 \leq j \leq \frac{p-5}{2}\Big\}.$$

Démonstration.

- Il est clair que $l(P_\infty) = 1$. L'espace $\mathcal{L}(P_\infty)$ contient certainement les fonctions constantes, ainsi $\mathcal{L}(P_\infty) =< 1 >$.
- Comme le genre de $\mathcal{C}_{n^2}$ est égal à 2, $2P_\infty$ est un diviseur canonique sur $\mathcal{C}_{n^2}$, donc $l(2P_\infty) = 2$. Ainsi, $\{1,\, x\}$ constitue une base pour $\mathcal{L}(2P_\infty)$.
- Pour $p \geq 3$, on peut voir que les éléments de $\mathcal{B}_p$ sont linéairement indépendants et appartiennent à $\mathcal{L}(pP_\infty)$. Ainsi, il reste à montrer que la cardinalité de $\mathcal{B}_p$ est égale à $l(pP_\infty)$. D'après le théorème de Riemann-Roch, on a $l(pP_\infty) = p-1$. Deux cas se présentent :

  Cas 1 : si p est pair, alors en posant $p = 2h$, on a

  $$i \leq \frac{p}{2} = h;\;\; j \leq \frac{p-5}{2} = \frac{2h-5}{2} \Longleftrightarrow j \leq h-3.$$

  Par suite, on a $\mathcal{B}_p = \{1,\, x,\, \ldots,\, x^h\} \cup \{y,\, yx,\, \ldots,\, yx^{h-3}\}$ et donc

  $$\#\mathcal{B}_p = (h+1) + (h-3+1) = 2h-1 = p-1.$$

  Cas 2 : si p est impair, alors en posant $p = 2h+1$, on a

  $$i \leq \frac{p}{2} = \frac{2h+1}{2} \Longleftrightarrow i \leq h;\;\; j \leq \frac{p-5}{2} = \frac{2h-4}{2} = h-2.$$

  Ainsi, on a $\mathcal{B}_p = \{1,\, x,\, \ldots,\, x^h\} \cup \{y,\, yx,\, \ldots,\, yx^{h-2}\}$ et donc

  $$\#\mathcal{B}_p = (h+1) + (h-2+1) = 2h = p-1.$$

❑

2.2.2 Preuve du Théorème 2.2.4

Soit R un point algébrique sur $\mathcal{C}_{n^2}$ de degré d sur $\mathbb{Q}$ avec $d \geq 2$. Notons $R_1, \cdots, R_d$ les conjugués de Galois de R. Il est clair que $R_i \notin \{P_n,\, \overline{P_n},\, P_\infty\}$. On a $[R_1 + \cdots + R_d - dP_\infty] \in J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ et comme

$$J_{\mathcal{C}_{n^2}}(\mathbb{Q}) = \Big\{mj(P_n) \text{ avec } 0 \leq m \leq 4\Big\},$$

alors

$$[R_1 + \cdots + R_d - dP_\infty] = mj(P_n) \text{ avec } 0 \leq m \leq 4. \qquad (1)$$

2.2.2.1 Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 2 sur $\mathbb{Q}$

Cas $m = 0$:
La formule (1) devient $[R_1 + R_2 - 2P_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\mathrm{div}(f) = R_1 + R_2 - 2P_\infty.$$

Donc $f \in \mathcal{L}(2P_\infty)$ et s'écrit $f = a_0 + a_1 x$ avec $a_i \neq 0$, sinon un des R_i serait égal à P_n, $\overline{P_n}$ ou P_∞, ce qui est absurde. Aux points R_i, on a $a_0 + a_1 x = 0$, d'où $x \in \mathbb{Q}^*$. La relation $y^2 = x^5 + n^2$ donne $y = \pm\sqrt{x^5 + n^2}$, ainsi on obtient une famille de points de degré 2,

$$\{(x,\, \pm\sqrt{x^5 + n^2}) \,:\, x \in \mathbb{Q}^*\}.$$

Cas $m = 1$ et $m = 4$:

- pour $m = 1$: (1) devient $[R_1 + R_2 + \overline{P_n} - 3P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + \overline{P_n} - 3P_\infty.$$

Donc $f \in \mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$, un des R_i est alors égal à P_∞, ce qui est absurde.

- pour $m = 4$: par un raisonnement analogue au cas $m = 1$, on obtient une absurdité.

Cas $m = 2$ et $m = 3$:

- pour $m = 2$: (1) devient $[R_1 + R_2 + 2\overline{P_n} - 4P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + 2\overline{P_n} - 4P_\infty.$$

Donc $f \in \mathcal{L}(4P_\infty)$ et s'écrit $f = a_0 + a_1x + a_2x^2$ avec $a_2 \neq 0$. La fonction f est d'ordre 2 en $\overline{P_n}$, d'où $a_0 = a_1 = 0$ donc $f = a_2x^2$ et par suite $R_1 = R_2 = P_n$, ce qui est absurde.

- pour $m = 3$: par un raisonnement analogue au cas $m = 2$, on obtient une absurdité.

Ainsi, on obtient une famille de points de degré 2

$$\mathcal{C}^{(2)}_{n^2}(\mathbb{Q}) = \{(x, \pm\sqrt{x^5 + n^2}) \,:\, x \in \mathbb{Q}^*\}.$$

2.2.2.2 Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 3 sur $\mathbb{Q}$

Cas $m = 0$:

La formule (1) devient $[R_1 + R_2 + R_3 - 3P_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 - 3P_\infty.$$

Donc $f \in \mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$, un des R_i est alors égal à P_∞, ce qui est absurde.

Cas $m = 1$ et $m = 4$:

- pour $m = 1$: (1) devient $[R_1 + R_2 + R_3 + \overline{P_n} - 4P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + \overline{P_n} - 4P_\infty.$$

Donc $f \in \mathcal{L}(4P_\infty)$ et s'écrit $f = a_0 + a_1x + a_2x^2$ avec $a_2 \neq 0$. La fonction f est d'ordre 1 en $\overline{P_n}$, donc $a_0 = 0$, d'où $f = a_1x + a_2x^2$. Aux points R_i, on a $x(a_1 + a_2x) = 0$, donc $x \in \mathbb{Q}$, ainsi les R_i devraient être de degré ≤ 2, ce qui est absurde.

- pour $m = 4$: par un raisonnement similaire au cas $m = 1$, on aboutit à la même conclusion.

Cas $m = 2$ et $m = 3$:

- pour $m = 2$: (1) devient $[R_1 + R_2 + R_3 + 2\overline{P_n} - 5P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + 2\overline{P_n} - 5P_\infty.$$

Donc $f \in \mathcal{L}(5P_\infty)$ et s'écrit $f = a_0 + a_1x + a_2x^2 + b_0y$ avec $b_0 \neq 0$. La fonction f est d'ordre 2 en $\overline{P_n}$, donc $a_0 - nb_0 = 0$ et $a_1 = 0$. Ainsi, $f = b_0(y + n) + a_2x^2$. Aux points R_i, on a $b_0(y + n) + a_2x^2 = 0$. En posant $\lambda = \dfrac{a_2}{b_0}$, on obtient

$$y = -n - \lambda x^2.$$

En remplaçant l'expression de y dans $y^2 - x^5 - n^2 = 0$, on a

$$-x^2(x^3 - \lambda^2 x^2 - 2\lambda n) = 0.$$

On doit avoir $x^2 \neq 0$, $\lambda \neq 0$ et $x^3 - \lambda^2 x^2 - 2\lambda n$ un polynôme irréductible ; ainsi on obtient une famille de points de degré 3,

$$\{(x, -n - \lambda x^2) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } x^3 - \lambda^2 x^2 - 2\lambda n = 0\}. \tag{2.1}$$

- pour $m = 3$: par un raisonnement analogue au cas $m = 2$, on obtient une famille de points de degré 3,

$$\{(x, n - \lambda x^2) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } x^3 - \lambda^2 x^2 + 2\lambda n = 0\}. \tag{2.2}$$

Ainsi, en combinant (2.1) et (2.2), on obtient

$$\mathcal{C}^{(3)}_{n^2}(\mathbb{Q}) = \left\{(x, \pm n - \lambda x^2) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } x^3 - \lambda^2 x^2 \pm 2\lambda n = 0\right\}.$$

2.2.2.3 Les points algébriques sur $\mathcal{C}_{n^2}$ de degré 4 sur $\mathbb{Q}$

Cas $m = 0$:
La formule (1) devient $[R_1 + R_2 + R_3 + R_4 - 4P_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + R_4 - 4P_\infty.$$

Donc $f \in \mathcal{L}(4P_\infty)$ et s'écrit $f = a_0 + a_1 x + a_2 x^2$ avec $a_2 \neq 0$. Aux points R_i, on a $a_0 + a_1 x + a_2 x^2 = 0$. La relation $y^2 = x^5 + n^2$ donne $y = \pm\sqrt{x^5 + n^2}$, d'où on obtient une famille de points de degré 4,

$$\mathcal{A}^n_0 = \{(x, \pm\sqrt{x^5 + n^2}) \,:\, [\mathbb{Q}(x) : \mathbb{Q}] = 2\}.$$

Cas $m = 1$ et $m = 4$:

- pour $m = 1$: (1) devient $[R_1 + R_2 + R_3 + R_4 + \overline{P_n} - 5P_\infty]$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + R_4 + \overline{P_n} - 5P_\infty.$$

Donc $f \in \mathcal{L}(5P_\infty)$ et s'écrit $f = a_0 + a_1 x + a_2 x^2 + b_0 y$ avec $b_0 \neq 0$. La fonction f est d'ordre 1 en $\overline{P_n}$, donc $a_0 - n b_0 = 0$, d'où $f = b_0(y + n) + a_1 x + a_2 x^2$. Aux points R_i, on a $b_0(y + n) + a_1 x + a_2 x^2 = 0$. En posant $\lambda = \dfrac{a_1}{b_0}$ et $\mu = \dfrac{a_2}{b_0}$, on obtient

$$y = -n - \lambda x - \mu x^2.$$

La substitution y dans $y^2 - x^5 - n^2 = 0$ donne

$$x(x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n) = 0.$$

On doit avoir $x \neq 0$, $\lambda \neq 0$ et $x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n$ un polynôme irréductible. On obtient une famille de points de degré 4,

$$\mathcal{A}^n_{1,1} = \left\{ \begin{array}{l} \left(x, -n - \lambda x - \mu x^2\right) \,:\, \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ et } x \text{ racine de} \\ x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n = 0 \end{array} \right\}.$$

- pour $m = 4$: par un raisonnement analogue au cas $m = 1$, on obtient une famille de points de degré 4,

$$\mathcal{A}^n_{1,4} = \left\{ \begin{array}{l} \left(x, n - \lambda x - \mu x^2\right) \,:\, \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ et } x \text{ racine de} \\ x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 + 2\mu n)x + 2\lambda n = 0 \end{array} \right\}.$$

Cas $m = 2$ et $m = 3$:

- pour $m = 2$: (1) devient $[R_1 + R_2 + R_3 + R_4 + 2\overline{P_n} - 6P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + R_4 + 2\overline{P_n} - 6P_\infty.$$

Donc $f \in \mathcal{L}(6P_\infty)$ et s'écrit $f = a_0 + a_1x + a_2x^2 + b_0y + a_3x^3$ avec $a_3 \neq 0$. La fonction f est d'ordre 2 en $\overline{P_n}$, donc $a_0 - nb_0 = 0$ et $a_1 = 0$, d'où $f = b_0(y+n) + a_2x^2 + a_3x^3$. Aux points R_i, on a $b_0(y+n) + a_2x^2 + a_3x^3 = 0$. En remarquant que $b_0 \neq 0$ puis en posant $\lambda = \dfrac{a_2}{b_0}$ et $\mu = \dfrac{a_3}{b_0}$, on a

$$y = -n - \lambda x^2 - \mu x^3.$$

En remplaçant l'expression de y dans $y^2 - x^5 - n^2 = 0$, on obtient

$$x^2(\mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 + 2\mu nx + 2\lambda n) = 0.$$

On doit avoir $x^2 \neq 0$, $\lambda \neq 0$ et $\mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 + 2\mu nx + 2\lambda n$ un polynôme irréductible. On obtient une famille de points de degré 4,

$$\mathcal{A}^n_{2,2} = \left\{ \begin{array}{l} \left(x, -n - \lambda x^2 - \mu x^3\right) : \lambda,\ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 + 2\mu nx + 2\lambda n = 0 \end{array} \right\}.$$

- pour $m = 3$: par un raisonnement analogue au cas $m = 2$, on obtient une famille de points de degré 4,

$$\mathcal{A}^n_{2,3} = \left\{ \begin{array}{l} \left(x, n - \lambda x^2 - \mu x^3\right) : \lambda,\ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 - 2\mu nx - 2\lambda n = 0 \end{array} \right\}.$$

2.2.2.4 Les points algébriques sur $\mathcal{C}_{n^2}$ de degré au plus d avec $d \geq 5$ sur $\mathbb{Q}$

Cas $m = 0$:

La formule (1) devient $[R_1 + \cdots + R_d - dP_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\mathrm{div}(f) = R_1 + \cdots + R_d - dP_\infty.$$

Donc $f \in \mathcal{L}(dP_\infty)$, d'où $f = \displaystyle\sum_{0 \leq i \leq \frac{d}{2}} a_ix^i + y \sum_{0 \leq j \leq \frac{d-5}{2}} b_jx^j$ avec

(i) $a_{\frac{d}{2}} \neq 0$ si d est pair

- si pour $0 \leq j \leq \dfrac{d-5}{2}$, $b_j = 0$, alors aux points R_i, on a $\displaystyle\sum_{0 \leq i \leq \frac{d}{2}} a_ix^i = 0$. La relation $y^2 = x^5 + n^2$ donne $y = \pm\sqrt{x^5 + n^2}$, d'où on obtient une famille de points de degré au plus d,

$$\mathcal{D}^n_0 = \left\{ \left(x, \pm\sqrt{x^5 + n^2}\right) : [\mathbb{Q}(x) : \mathbb{Q}] \leq \frac{d}{2} \text{ si } d \text{ est pair} \right\}.$$

- sinon il existe j avec $0 \leq j \leq \dfrac{d-5}{2}$ tel que $b_j \neq 0$, alors $y = -\dfrac{\displaystyle\sum_{0 \leq i \leq \frac{d}{2}} a_ix^i}{\displaystyle\sum_{0 \leq j \leq \frac{d-5}{2}} b_jx^j}$. En remplaçant l'expression de y dans $y^2 - x^5 - n^2 = 0$, on obtient

$$\Big(\sum_{0 \leq i \leq \frac{d}{2}} a_ix^i\Big)^2 - \Big(\sum_{0 \leq j \leq \frac{d-5}{2}} b_jx^j\Big)^2 (x^5 + n^2) = 0.$$

Ainsi, on obtient une famille de points de degré au plus d,

$$\mathcal{D}^n_{1,0} = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\le i\le \frac{d}{2}} a_i x^i}{\sum\limits_{0\le j\le \frac{d-5}{2}} b_j x^j} \right) \ : \ a_{\frac{d}{2}} \neq 0 \text{ et } \exists\, b_j \neq 0 \text{ si } d \text{ est pair} \\ \text{et } x \text{ racine de } \Big(\sum\limits_{i=0}^{\frac{d}{2}} a_i x^i\Big)^2 - \Big(\sum\limits_{j=0}^{\frac{d-5}{2}} b_j x^j\Big)^2 (x^5+n^2) = 0 \end{array} \right\}.$$

(ii) $b_{\frac{d-5}{2}} \neq 0$ si d est impair. Aux points R_i, on a $\sum\limits_{0\le i\le \frac{d}{2}} a_i x^i + y \sum\limits_{0\le j\le \frac{d-5}{2}} b_j x^j = 0$, d'où $y = -\dfrac{\sum\limits_{0\le i\le \frac{d}{2}} a_i x^i}{\sum\limits_{0\le j\le \frac{d-5}{2}} b_j x^j}$. En remplaçant l'expression de y dans $y^2 - x^5 - n^2 = 0$, on obtient

$$\Big(\sum_{0\le i\le \frac{d}{2}} a_i x^i\Big)^2 - \Big(\sum_{0\le j\le \frac{d-5}{2}} b_j x^j\Big)^2 (x^5+n^2) = 0.$$

Ainsi, on obtient une famille de points de degré au plus d,

$$\mathcal{D}^n_{1,1} = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\le i\le \frac{d}{2}} a_i x^i}{\sum\limits_{0\le j\le \frac{d-5}{2}} b_j x^j} \right) \ : \ b_{\frac{d-5}{2}} \neq 0 \text{ si } d \text{ est impair et } x \\ \text{racine de } \Big(\sum\limits_{i=0}^{\frac{d}{2}} a_i x^i\Big)^2 - \Big(\sum\limits_{j=0}^{\frac{d-5}{2}} b_j x^j\Big)^2 (x^5+n^2) = 0 \end{array} \right\}.$$

Cas $m = 1$ et $m = 4$:

- pour $m = 1$: la formule (1) devient $[R_1 + \cdots + R_d + \overline{P_n} - (d+1)P_\infty] = 0$. Il existe une fonction f telle que

$$\mathrm{div}(f) = R_1 + \cdots + R_d + \overline{P_n} - (d+1)P_\infty.$$

Par conséquent $f \in \mathcal{L}((d+1)P_\infty)$, d'où $f = \sum\limits_{0\le i\le \frac{d+1}{2}} a_i x^i + y \sum\limits_{0\le j\le \frac{d-4}{2}} b_j x^j$ avec $a_{\frac{d+1}{2}} \neq 0$ si d est impair ou $b_{\frac{d-4}{2}} \neq 0$ si d est pair. La fonction f est d'ordre 1 en $\overline{P_n}$, d'où $a_0 = nb_0$. Aux points R_i, on a $\sum\limits_{0\le i\le \frac{d+1}{2}} a_i x^i + y \sum\limits_{0\le j\le \frac{d-4}{2}} b_j x^j = 0$, ce qui implique que $y = -\dfrac{\sum\limits_{0\le i\le \frac{d+1}{2}} a_i x^i}{\sum\limits_{0\le j\le \frac{d-4}{2}} b_j x^j}$. La substitution y dans $y^2 - x^5 - n^2 = 0$ donne

$$\Big(\sum_{0\le i\le \frac{d+1}{2}} a_i x^i\Big)^2 - \Big(\sum_{0\le j\le \frac{d-4}{2}} b_j x^j\Big)^2 (x^5+n^2) = 0.$$

Ainsi, on obtient une famille de points de degré au plus d,

$$\mathcal{D}^n_{2,1} = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{0\le i\le \frac{d+1}{2}} a_i x^i}{\sum\limits_{0\le j\le \frac{d-4}{2}} b_j x^j} \right) \ : \ a_0 = nb_0, \ \text{ et } x \text{ racine de} \\ \Big(\sum\limits_{0\le i\le \frac{d+1}{2}} a_i x^i\Big)^2 - \Big(\sum\limits_{0\le j\le \frac{d-4}{2}} b_j x^j\Big)^2 (x^5+n^2) = 0 \end{array} \right\}.$$

- pour $m=4$: par un raisonnement similaire au cas $m=1$, on obtient une famille de points de degré au plus d,

$$\mathcal{D}_{2,4}^n=\left\{\begin{array}{l}\left(x,-\dfrac{\sum\limits_{0\leq i\leq\frac{d+1}{2}}a_ix^i}{\sum\limits_{0\leq j\leq\frac{d-4}{2}}b_jx^j}\right)\ :\ a_0=-nb_0,\ \text{ et } x \text{ racine de}\\ \Big(\sum\limits_{0\leq i\leq\frac{d+1}{2}}a_ix^i\Big)^2-\Big(\sum\limits_{0\leq j\leq\frac{d-4}{2}}b_jx^j\Big)^2(x^5+n^2)=0\end{array}\right\}.$$

Cas $m=2$ et $m=3$:

- pour $m=2$: la formule (1) devient $[R_1+\cdots+R_d+2\overline{P_n}-(d+2)P_\infty]=0$. Il y a une fonction f telle que

$$\operatorname{div}(f)=R_1+\cdots+R_d+2\overline{P_n}-(d+2)P_\infty.$$

Donc $f\in\mathcal{L}((d+2)P_\infty)$, d'où $f=\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i+y\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j$ avec $a_{\frac{d+2}{2}}\neq0$ si d est pair ou $b_{\frac{d-3}{2}}\neq0$ si d est impair. La fonction f est d'ordre 2 en $\overline{P_n}$, donc $a_0=nb_0$ et $a_1=nb_1$. Aux points R_i, on a $\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i+y\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j=0$, ce qui entraîne que $y=-\dfrac{\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i}{\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j}$. La substitution de y dans $y^2-x^5-n^2=0$ donne

$$\Big(\sum_{0\leq i\leq\frac{d+2}{2}}a_ix^i\Big)^2-\Big(\sum_{0\leq j\leq\frac{d-3}{2}}b_jx^j\Big)^2(x^5+n^2)=0.$$

Ainsi, on trouve une famille de points de degré au plus d,

$$\mathcal{D}_{3,2}^n=\left\{\begin{array}{l}\left(x,-\dfrac{\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i}{\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j}\right)\ :\ a_0=nb_0,a_1=nb_1,\ \text{et } x \text{ racine de}\\ \Big(\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i\Big)^2-\Big(\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j\Big)^2(x^5+n^2)=0\end{array}\right\}.$$

- pour $m=3$: par un raisonnement similaire au cas $m=2$, on trouve une famille de points de degré au plus d,

$$\mathcal{D}_{3,3}^n=\left\{\begin{array}{l}\left(x,-\dfrac{\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i}{\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j}\right)\ :\ a_0=-nb_0,a_1=-nb_1,\ \text{et } x \text{ racine de}\\ \Big(\sum\limits_{0\leq i\leq\frac{d+2}{2}}a_ix^i\Big)^2-\Big(\sum\limits_{0\leq j\leq\frac{d-3}{2}}b_jx^j\Big)^2(x^5+n^2)=0\end{array}\right\}.$$

Remarque 2.2.1. Le résultat obtenu reste vrai pour tout entier n pour lequel $J_{\mathcal{C}_{n^2}}(\mathbb{Q})\cong\mathbb{Z}/5\mathbb{Z}$ et que l'ensemble des points $\mathbb{Q}-$rationnels sur $\mathcal{C}_{n^2}$ est donné par $\{P_n,\ \overline{P_n},\ P_\infty\}$.

2.3 Points algébriques de petit degré sur les courbes hyperelliptiques $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$

Dans cette section, nous étudions les points algébriques de degré au plus 3 sur les courbes hyperelliptiques $\mathcal{C}_n$ définies sur $\mathbb{Q}$ de genre 2 d'équations affines

$$\mathcal{C}_n : y^2 = x(x^2 - n^2)(x^2 - 4n^2),$$

avec $n \in \{1,\ 2,\ 3,\ q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. L'étude de ces courbes a été motivée par les travaux de Heiden [Hei98], Evink [Evi20] et Evink, et al. [EHT21] qui ont déterminé l'ensemble des points $\mathbb{Q}-$rationnels sur les mêmes courbes.

Posons $P_0 = (0,\ 0)$, $P_n = (n,\ 0)$, $\overline{P_n} = (-n,\ 0)$, $P_{2n} = (2n,\ 0)$, $\overline{P_{2n}} = (-2n,\ 0)$ et P_∞ le point à l'infini sur $\mathcal{C}_n$. Il résulte des travaux de Heiden, Evink et de Evink et al., le théorème suivant :

Théorème 2.3.1. Soit $n \in \{1,\ 2,\ 3,\ q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Soit la courbe

$$\mathcal{C}_n : y^2 = x(x^2 - n^2)(x^2 - 4n^2).$$

Alors, les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}_n$ sont donnés par

$$\mathcal{C}_n(\mathbb{Q}) = \{P_0,\ P_n,\ \overline{P_n},\ P_{2n},\ \overline{P_{2n}},\ P_\infty\}.$$

Notre seconde contribution qui étend les travaux de Heiden, Evink et Top est donnée par le théorème suivant :

Théorème 2.3.2. Soit $n \in \{1, 2, 3, q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Soit la courbe

$$\mathcal{C}_n : y^2 = x(x^2 - n^2)(x^2 - 4n^2).$$

Alors, les points algébriques sur $\mathcal{C}_n$ de degré au plus 3 sur $\mathbb{Q}$ sont donnés par

$$\bigcup_{[K:\mathbb{Q}]\leqslant 3} \mathcal{C}_n(K) = \mathcal{C}_n(\mathbb{Q}) \cup \mathcal{B}^n \cup \mathcal{A}_0^n \cup \mathcal{A}_1^n \cup \mathcal{A}_2^n \cup \mathcal{A}_3^n \cup \mathcal{A}_4^n \cup \mathcal{A}_5^n$$

avec

$$\begin{aligned}
\mathcal{C}_n(\mathbb{Q}) &= \left\{P_0, P_n, \overline{P_n}, P_{2n}, \overline{P_{2n}}, P_\infty\right\};\\
\mathcal{B}^n &= \left\{\left(x, \pm\sqrt{x(x^2 - n^2)(x^2 - 4n^2)}\right) :\ x \in \mathbb{Q}\backslash\{0,\ \pm n,\ \pm 2n\}\right\};\\
\mathcal{A}_0^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ x^3 + (-\lambda^2 \mp n)x^2 + (\mp\lambda^2 n - 4n^2)x \pm 4n^3 = 0\end{array}\right\};\\
\mathcal{A}_1^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm 2n)) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ x^3 + (-\lambda^2 \mp 2n)x^2 + (\mp 2\lambda^2 n - n^2)x \pm 2n^3 = 0\end{array}\right\};\\
\mathcal{A}_2^n &= \left\{\begin{array}{l}\left(x, \lambda x(x^2 - n^2)\right) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ \lambda^2 x^3 - x^2 - \lambda^2 n^2 x + 4n^2 = 0\end{array}\right\};\\
\mathcal{A}_3^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)(x \pm 2n)) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ \lambda^2 x^3 + (\pm 3\lambda^2 n - 1)x^2 + (2\lambda^2 n^2 \pm 3n)x - 2n^2 = 0\end{array}\right\};\\
\mathcal{A}_4^n &= \left\{\begin{array}{l}(x, \lambda x(x \pm n)(x \mp 2n)) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ \lambda^2 x^3 + (\mp\lambda^2 n - 1)x^2 + (-2\lambda^2 n^2 \mp n)x + 2n^2 = 0\end{array}\right\};\\
\mathcal{A}_5^n &= \left\{\begin{array}{l}\left(x, \lambda x(x^2 - 4n^2)\right) :\ \lambda \in \mathbb{Q}^*\ \text{ et } x \text{ racine de}\\ \lambda^2 x^3 - x^2 - 4\lambda^2 n^2 x + n^2 = 0\end{array}\right\}.
\end{aligned}$$

2.3.1 Lemmes fondamentaux

Lemme 2.3.1. $J_{\mathcal{C}_n}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$.

Démonstration. On sait que la suite

$$0 \longrightarrow J_{\mathcal{C}_n}(\mathbb{Q})/2J_{\mathcal{C}_n}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^2(J_{\mathcal{C}_n}/\mathbb{Q}) \longrightarrow Ш(J_{\mathcal{C}_n}/\mathbb{Q})[2] \longrightarrow 0,$$

est exacte. Ainsi, on a la formule

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}_n}/\mathbb{Q}) = \dim_{\mathbb{F}_2} J_{\mathcal{C}_n}(\mathbb{Q})/2J_{\mathcal{C}_n}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(J_{\mathcal{C}_n}/\mathbb{Q})[2].$$

Puisque $\dim_{\mathbb{F}_2} J_{\mathcal{C}_n}(\mathbb{Q})/2J_{\mathcal{C}_n}(\mathbb{Q}) = \mathrm{rang}(J_{\mathcal{C}_n}(\mathbb{Q})) + \dim_{\mathbb{F}_2} J_{\mathcal{C}_n}(\mathbb{Q})[2]$, il en résulte que

$$\mathrm{rang}(J_{\mathcal{C}_n}(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}_n}/\mathbb{Q}) - \dim_{\mathbb{F}_2} J_{\mathcal{C}_n}(\mathbb{Q})[2].$$

D'après [Evi20] et [EHT21], on a $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(J_{\mathcal{C}_n}/\mathbb{Q}) = 4$ et comme $\dim_{\mathbb{F}_2} J_{\mathcal{C}_n}(\mathbb{Q})[2] = 4$, alors

$$\mathrm{rang}(J_{\mathcal{C}_n}(\mathbb{Q})) = 0.$$

Cherchons le sous-groupe de torsion $J_{\mathcal{C}_n}(\mathbb{Q})_{\mathrm{tors}}$.
Soit p un nombre premier ; considérons l'application de réduction suivante

$$J_{\mathcal{C}_n}(\mathbb{Q}) \longrightarrow J_{\mathcal{C}_n}(\mathbb{F}_p).$$

Posons $f_n(x) = x(x^2 - n^2)(x^2 - 4n^2)$. Le discriminant de f_n, noté $\mathrm{disc}(f_n)$, est

$$\mathrm{disc}(f_n) = 2^{10}3^4n^{20}.$$

Soit p un nombre premier ne divisant pas $2\mathrm{disc}(f_n)$. Alors, l'application de réduction est injective sur le sous-groupe de torsion $J_{\mathcal{C}_n}(\mathbb{Q})_{\mathrm{tors}}$ (voir [CF96] ou [Sto14]). En prenant $p = 5$, on trouve $J_{\mathcal{C}_n}(\mathbb{F}_5) = 16$ qui ne dépend pas de n, donc $\#J_{\mathcal{C}_n}(\mathbb{Q})_{\mathrm{tors}} \leq 16$. Puisque $\#J_{\mathcal{C}_n}(\mathbb{Q})[2] = 16$, il en résulte que $J_{\mathcal{C}_n}(\mathbb{Q})_{\mathrm{tors}} = J_{\mathcal{C}_n}(\mathbb{Q})[2]$. D'après le lemme 2.1. dans [Mül15], $J_{\mathcal{C}_n}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$; par suite

$$J_{\mathcal{C}_n}(\mathbb{Q})_{\mathrm{tors}} = J_{\mathcal{C}_n}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

❑

Soient x et y les fonctions rationnelles sur $\mathcal{C}_n$ définies par

$$x(X, Y, Z) = \frac{X}{Z} \text{ et } y(X, Y, Z) = \frac{Y}{Z^3}.$$

L'équation projective de la courbe $\mathcal{C}_n$ lisse est donnée par

$$\mathcal{C}_n : Y^2 = XZ(X^2 - n^2Z^2)(X^2 - 4n^2Z^2).$$

Lemme 2.3.2. Soit $P = (u, v) \in \mathcal{C}_n$ avec $P \neq P_\infty$ et $f \in \overline{K}(\mathcal{C}_n)$ telle que $f = x - u$. Alors on a

$$\mathrm{div}(f) = P + \varphi(P) - 2P_\infty.$$

Démonstration.

- Supposons que P soit ordinaire. Soit $Q \in \mathcal{C}_n$. Il est clair que $f(Q) = 0$ si, et seulement si $Q \in \{P, \varphi(P)\}$ et $x - u$ est une uniformisante en P, d'où $\mathrm{ord}_P(f) = 1$. Il en va de même pour $\varphi(P)$ donc $\mathrm{ord}_{\varphi(P)}(f) = 1$. Lorsque $f(Q) \neq 0$, on a $\mathrm{ord}_Q(f) = 0$. Pour calculer l'ordre de f en P_∞, on utilise une uniformisante $t = y/x^3$ et on trouve $\mathrm{ord}_{P_\infty}(f) = -2$. Par conséquent, $\mathrm{div}(f) = P + \varphi(P) - 2P_\infty$.

– Supposons que P soit spécial. Le seul zéro de f est P. La fonction $y - v$ est une uniformisante en P, et donc $\mathrm{ord}_P(f) = 2$. D'où $\mathrm{div}(f) = 2P - 2P_\infty$, c'est-à-dire, $\mathrm{div}(f) = P + \varphi(P) - 2P_\infty$.

❑

Comme conséquence, on a

- $\mathrm{div}(x) = 2P_0 - 2P_\infty$;
- $\mathrm{div}(x - n) = 2P_n - 2P_\infty$, $\mathrm{div}(x + n) = 2\overline{P_n} - 2P_\infty$;
- $\mathrm{div}(x - 2n) = 2P_{2n} - 2P_\infty$, $\mathrm{div}(x + 2n) = 2\overline{P_{2n}} - 2P_\infty$.

Ce qui entraîne que

$$\mathrm{div}(y) = P_0 + P_n + \overline{P_n} + P_{2n} + \overline{P_{2n}} - 5P_\infty.$$

Ainsi, on voit que

(i) $2j(P_0) = 0$, $2j(P_n) = 0$, $2j(\overline{P_n}) = 0$, $2j(P_{2n}) = 0$ et $2j(\overline{P_{2n}}) = 0$;
(ii) $j(P_0) + j(P_n) + j(\overline{P_n}) + j(P_{2n}) + j(\overline{P_{2n}}) = 0$.

En combinant (i) et le fait que les classes de diviseurs $j(P_n)$, $j(\overline{P_n})$, $j(P_{2n})$ et $j(\overline{P_{2n}})$ sont lineairement indépendantes, alors $j(P_n)$, $j(\overline{P_n})$, $j(P_{2n})$ et $j(\overline{P_{2n}})$ forment une base du groupe $J_{\mathcal{C}_n}(\mathbb{Q})$.

Lemme 2.3.3. On a

$$\mathcal{L}(P_\infty) =< 1 >,\ \ \mathcal{L}(2P_\infty) = \mathcal{L}(3P_\infty) =< 1, x >,\ \ \mathcal{L}(4P_\infty) =< 1, x, x^2 >,$$
$$\mathcal{L}(5P_\infty) =< 1, x, x^2, y >,\ \ \mathcal{L}(6P_\infty) =< 1, x, x^2, y, x^3 > .$$

Plus généralement, pour $m \geq 5$, une $\overline{\mathbb{Q}}-$ base pour $\mathcal{L}(mP_\infty)$ est donnée par

$$\mathcal{B}_m = \Big\{x^i \ : \ i \in \mathbb{N} \text{ et } 0 \leq i \leq \frac{m}{2}\Big\} \cup \Big\{yx^j \ : \ j \in \mathbb{N} \text{ et } 0 \leq j \leq \frac{m-5}{2}\Big\}.$$

Démonstration.

– Il est clair que $l(P_\infty) = 1$. L'espace $\mathcal{L}(P_\infty)$ contient certainement les fonctions constantes, ainsi $\mathcal{L}(P_\infty) =< 1 >$.
– Comme le genre de $\mathcal{C}_n$ est égal à 2, $2P_\infty$ est un diviseur canonique sur $\mathcal{C}_n$, donc $l(2P_\infty) = 2$. Ainsi, $\{1, x\}$ constitue une base pour $\mathcal{L}(2P_\infty)$.
– Pour $m \geq 3$, on peut voir que les éléments de $\mathcal{B}_m$ sont linéairement indépendants et appartiennent à $\mathcal{L}(mP_\infty)$. Ainsi, il reste à montrer que la cardinalité de $\mathcal{B}_m$ est égale à $l(mP_\infty)$. D'après le théorème de Riemann-Roch, on a $l(mP_\infty) = m - 1$. Deux cas se présentent :

Cas 1 : si m est pair, alors en posant $m = 2h$, on a

$$i \leq \frac{m}{2} = h;\ \ j \leq \frac{m-5}{2} = \frac{2h-5}{2} \Longleftrightarrow j \leq h - 3.$$

Par suite, on a $\mathcal{B}_m = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-3}\}$ et donc

$$\#\mathcal{B}_m = (h + 1) + (h - 3 + 1) = 2h - 1 = m - 1.$$

Cas 2 : si m est impair, alors en posant $m = 2h + 1$, on a

$$i \leq \frac{m}{2} = \frac{2h+1}{2} \Longleftrightarrow i \leq h;\ \ j \leq \frac{m-5}{2} = \frac{2h-4}{2} = h - 2.$$

Ainsi, on a $\mathcal{B}_m = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-2}\}$ et donc

$$\#\mathcal{B}_m = (h + 1) + (h - 2 + 1) = 2h = m - 1.$$

❑

2.3.2 Preuve du Théorème 2.3.2

Soit R un point algébrique sur $\mathcal{C}_n$ de degré d sur $\mathbb{Q}$ avec $2 \leq d \leq 3$. Soit $R_1, \cdots, R_d$ les conjugués de Galois de R. On a $[R_1 + \cdots + R_d - dP_\infty] \in J_{\mathcal{C}_n}(\mathbb{Q})$ et comme

$$J_{\mathcal{C}_n}(\mathbb{Q}) = \Big\{ m_0 j(P_n) + m_1 j(\overline{P_n}) + m_2 j(P_{2n}) + m_3 j(\overline{P_{2n}}),\ \text{avec } 0 \leq m_i \leq 1 \}$$

alors

$$[R_1 + \cdots + R_d - dP_\infty] = m_0 j(P_n) + m_1 j(\overline{P_n}) + m_2 j(P_{2n}) + m_3 j(\overline{P_{2n}}). \quad (1)$$

Les combinaisons possibles pour les m_i sont :

m_0	m_1	m_2	m_3
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	0
0	0	1	1
0	1	0	1
1	0	1	0

m_0	m_1	m_2	m_3
0	1	1	0
1	0	0	1
1	1	0	0
0	0	0	1
0	0	1	0
0	1	0	0
1	0	0	0
1	1	1	1

2.3.2.1 Les points algébriques sur $\mathcal{C}_n$ de degré 2 sur $\mathbb{Q}$

Si tous les m_i sont nuls

La formule (1) devient $[R_1 + R_2 - 2P_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\text{div}(f) = R_1 + R_2 - 2P_\infty.$$

Par conséquent, $f \in \mathcal{L}(2P_\infty)$, d'où par le Lemme 2, $f = a_0 + a_1 x$ avec $a_i \neq 0$ sinon un des R_i serait égal à P_0 ou P_∞, ce qui est absurde. Aux points R_i, on a $a_0 + a_1 x = 0$, d'où $x \in \mathbb{Q}\backslash\{0, \pm n, \pm 2n\}$. La relation $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$ donne

$$y = \pm\sqrt{x(x^2 - n^2)(x^2 - 4n^2)},$$

ainsi on obtient une famille de points de degré 2,

$$\Big\{ (x, \pm\sqrt{x(x^2 - n^2)(x^2 - 4n^2)}) \ :\ x \in \mathbb{Q}\backslash\{0, \pm n, \pm 2n\} \Big\}.$$

Pour les autres cas, on obtient une absurdité.

Ainsi, on obtient une famille de points de degré 2,

$$\mathcal{B}^n = \Big\{ (x, \pm\sqrt{x(x^2 - n^2)(x^2 - 4n^2)}) \ :\ x \in \mathbb{Q}\backslash\{0, \pm n, \pm 2n\} \Big\}.$$

2.3.2.2 Les points algébriques sur $\mathcal{C}_n$ de degré 3 sur $\mathbb{Q}$

Si un des m_i est nul

– Pour $(0, 1, 1, 1)$, la formule (1) devient $[R_1 + R_2 + R_3 + P_0 + P_n - 5P_\infty] = 0$. Il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$\text{div}(f) = R_1 + R_2 + R_3 + P_0 + P_n - 5P_\infty.$$

Par conséquent, $f \in \mathcal{L}(5P_\infty)$, d'où $f = a_0 + a_1x + a_2x^2 + b_0y$ avec $b_0 \neq 0$. La fonction f est d'ordre 1 en P_0 et P_n, donc $f = a_2x(x-n) + b_0y$. Aux points R_i, on a $a_2x(x-n) + b_0y = 0$. En posant $\lambda = -\dfrac{a_2}{b_0}$, on obtient

$$y = \lambda x(x-n).$$

En remplaçant l'expression de y dans $y^2 = x(x^2-n^2)(x^2-4n^2)$, on obtient

$$-x(-x+n)(x^3 + (-\lambda^2+n)x^2 + (\lambda^2 n - 4n^2)x - 4n^3) = 0.$$

On doit avoir $x(-x+n) \neq 0$ et $x^3+(-\lambda^2+n)x^2+(\lambda^2n-4n^2)x-4n^3$ un polynôme irréductible ; donc on obtient une famille de points de degré 3,

$$\mathcal{A}^n_{0,0} = \left\{ \begin{array}{l} (x, \lambda x(x-n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ x^3 + (-\lambda^2+n)x^2 + (\lambda^2 n - 4n^2)x - 4n^3 = 0 \end{array} \right\}.$$

– Pour les cases $(1,0,1,1)$, $(1,1,0,1)$ et $(1,1,1,0)$, par un raisonnement analogue au case $(0,1,1,1)$, on obtient respectivement les familles de points de degré 3,

$$\mathcal{A}^n_{0,1} = \left\{ \begin{array}{l} (x, \lambda x(x+n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ x^3 + (-\lambda^2-n)x^2 + (-\lambda^2 n - 4n^2)x + 4n^3 = 0 \end{array} \right\};$$

$$\mathcal{A}^n_{1,0} = \left\{ \begin{array}{l} (x, \lambda x(x-2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ x^3 + (-\lambda^2+2n)x^2 + (2\lambda^2 n - n^2)x - 2n^3 = 0 \end{array} \right\};$$

$$\mathcal{A}^n_{1,1} = \left\{ \begin{array}{l} (x, \lambda x(x+2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ x^3 + (-\lambda^2-2n)x^2 + (-2\lambda^2 n - n^2)x + 2n^3 = 0 \end{array} \right\}.$$

Si deux des m_i sont nuls

– Pour $(0,0,1,1)$, la formule (1) devient $[R_1 + R_2 + R_3 + P_0 + P_n + \overline{P_n} - 6P_\infty] = 0$. Il y a une fonction f telle que

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + P_0 + P_n + \overline{P_n} - 6P_\infty.$$

Par conséquent, $f \in \mathcal{L}(6P_\infty)$, d'où $f = a_0 + a_1x + a_2x^2 + b_0y + a_3x^3$ avec $a_3 \neq 0$. La fonction f est d'ordre 1 en P_0, P_n et $\overline{P_n}$, donc $f = a_3x(x^2-n^2) + b_0y$. Aux points R_i, $a_3x(x^2-n^2) + b_0y = 0$. Notons que $b_0 \neq 0$ et en posant $\lambda = -\dfrac{a_3}{b_0}$, on a

$$y = \lambda x(x^2 - n^2).$$

La substitution de y dans $y^2 = x(x^2-n^2)(x^2-4n^2)$ donne

$$x(-x+n)(x+n)(\lambda^2x^3 - x^2 - \lambda^2n^2x + 4n^2) = 0.$$

On doit avoir $x(-x+n)(x+n) \neq 0$ et $\lambda^2x^3 - x^2 - \lambda^2n^2x + 4n^2$ un polynôme irréducible. On obtient une famille de points de degré 3,

$$\mathcal{A}^n_2 = \left\{ \begin{array}{l} \left(x, \lambda x(x^2-n^2)\right) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \lambda^2x^3 - x^2 - \lambda^2n^2x + 4n^2 = 0 \end{array} \right\}.$$

– Pour les cases $(0,1,0,1)$, $(1,0,1,0)$, $(0,1,1,0)$, $(1,0,0,1)$ et $(1,1,0,0)$, par un raisonnement similaire au case $(0,0,1,1)$, on obtient respectivement les familles de points de degré 3,

$$\mathcal{A}^n_{3,0} = \left\{ \begin{array}{l} (x, \lambda x(x-n)(x-2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \lambda^2x^3 + (-3\lambda^2n - 1)x^2 + (2\lambda^2n^2 - 3n)x - 2n^2 = 0 \end{array} \right\};$$

$$\mathcal{A}_{3,1}^n = \left\{ \begin{array}{l} (x, \lambda x(x+n)(x+2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \lambda^2 x^3 + (3\lambda^2 n - 1)x^2 + (2\lambda^2 n^2 + 3n)x - 2n^2 = 0 \end{array} \right\};$$

$$\mathcal{A}_{4,0}^n = \left\{ \begin{array}{l} (x, \lambda x(x-n)(x+2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \lambda^2 x^3 + (\lambda^2 n - 1)x^2 + (-2\lambda^2 n^2 + n)x + 2n^2 = 0 \end{array} \right\};$$

$$\mathcal{A}_{4,1}^n = \left\{ \begin{array}{l} (x, \lambda x(x+n)(x-2n)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \lambda^2 x^3 + (-\lambda^2 n - 1)x^2 + (-2\lambda^2 n^2 - n)x + 2n^2 = 0 \end{array} \right\};$$

$$\mathcal{A}_5^n = \Big\{ (x,\, \lambda x(x^2 - 4n^2)) \,:\, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de } \lambda^2 x^3 - x^2 - 4\lambda^2 n^2 x + n^2 = 0 \Big\}.$$

Pour les autres cas, on obtient une absurdité.

Chapitre 3

Septique de Fermat et courbes d'équations affines $x^p + y^{pq} = 1$

3.1 Points algébriques de degré au plus 14 sur la septique de Fermat

Dans cette section, nous étudions des points algébriques sur la septique de Fermat, c'est-à-dire, sur la courbe plane lisse de degré 7 d'équation projective

$$F_7 = \{(X, Y, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}.$$

Tzermias a déterminé l'ensemble des points algébriques sur F_7 de degré au plus 5 sur $\mathbb{Q}$ et Sall a étendu ces résultats en donnant une description géométrique des points algébriques sur F_7 de degré au plus 10 sur $\mathbb{Q}$. Nous donnons une extension de cette description géométrique des points algébriques sur la même courbe de degré au plus 14 sur $\mathbb{Q}$.

3.1.1 Introduction

Soit $\mathcal{C}$ une courbe plane lisse de degré d définie sur $\mathbb{Q}$. Le degré d'un point algébrique R sur $\mathcal{C}$ est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire, la dimension de $\mathbb{Q}(R)$ en tant que $\mathbb{Q}-$espace vectoriel. Un théorème de Debarre et Klassen [DK94] affirme que

(1) si $d \geq 7$ alors, l'ensemble des points algébriques sur $\mathcal{C}$ de degré au plus $d-2$ sur $\mathbb{Q}$ est fini.

(2) si $d \geq 8$ alors, à un nombre fini d'exceptions près, l'ensemble des points algébriques sur $\mathcal{C}$ de degré au plus $d-1$ sur $\mathbb{Q}$ se présente comme l'intersection de $\mathcal{C}$ avec une droite définie sur $\mathbb{Q}$ passant par un point rationnel de $\mathcal{C}$.

Soit p un nombre premier impair. Nous notons F_p la courbe de Fermat de degré p, c'est-à-dire, la courbe plane lisse d'équation projective

$$F_p = \{(X, Y, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^p + Y^p + Z^p = 0\}.$$

On désigne par J_p sa jacobienne. Faddeev [Fad61a, Fad61b] a prouvé que pour $p \leq 7$, le groupe $J_p(\mathbb{Q})$ des points rationnels de la jacobienne J_p de F_p est fini. Soulignons que, par un résultat de Gross et Rohrlich [GR78] pour $p \geq 11$, $J_p(\mathbb{Q})$ est infini.

Le premier cas du théorème de Debarre et Klassen montre que l'ensemble des points algébriques sur F_7 de degré au plus 5 sur $\mathbb{Q}$ est fini. Tzermias [Tze98] a décrit cet ensemble. Il existe exactement cinq points algébriques sur F_7 de degré au plus 5 sur $\mathbb{Q}$, à savoir

$$a = (0, -1, 1), \quad b = (-1, 0, 1), \quad \infty = (-1, 1, 0),$$

$$P = (-\eta, -\overline{\eta}, 1), \quad \overline{P} = (-\overline{\eta}, -\eta, 1),$$

où η est une racine primitive $6^{\text{ième}}$ de l'unité dans $\overline{\mathbb{Q}}$ et $\overline{\eta}$ est le complexe conjugué de η. Notons [Tze98] que les cinq points ci-dessus sont les seuls points d'intersection de F_7 avec la droite $X + Y + Z = 0$.

Sall [Sal00a, Sal03] a amélioré ces résultats en donnant une description géométrique des points algébriques sur F_7 de degré au plus 10 sur $\mathbb{Q}$, et il a établi le théorème suivant :

Théorème 3.1.1. Considérons la septique de Fermat

$$F_7 = \{(X, Y, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}.$$

1) Les points algébriques sur F_7 de degré 6 sur $\mathbb{Q}$ sont obtenus en coupant F_7 par une droite définie sur $\mathbb{Q}$ passant par a, b ou ∞.
2) Les points algébriques sur F_7 de degré 7 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une droite définie sur $\mathbb{Q}$.
3) Il n'existe pas sur F_7 de points algébriques de degré 8 ou 9 sur $\mathbb{Q}$.
4) Les points algébriques sur F_7 de degré 10 sur $\mathbb{Q}$ sont obtenus comme intersection résiduelle de F_7 avec une conique $\mathcal{C}$ définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 2 en $\{a, b\}$ ou $\{a, \infty\}$ ou $\{b, \infty\}$.

Notre résultat principal s'énonce comme suit :

Théorème 3.1.2. Considérons la septique de Fermat

$$F_7 = \{(X, Y, Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}.$$

1. Les points algébriques sur F_7 de degré 11 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞ et tangente en un des deux autres.
2. Les points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$
      (i) passant par deux des points a, b, ∞ ou par P et $\overline{P}$,
      (ii) tangente à F_7 en un des points a, b, ∞,
   (b) une cubique définie sur $\mathbb{Q}$ ayant a, b et ∞ comme points de contact d'ordre 3 en chacun de ces points,
   (c) une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme points de contact d'ordre 8 en chacun de ces points.
3. Les points algébriques sur F_7 de degré 13 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞,
   (b) une cubique définie sur $\mathbb{Q}$ tangente à F_7 en un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres.

4. Les points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus soit comme intersection de F_7 avec
   (a) une conique définie sur $\mathbb{Q}$,
   (b) une cubique définie sur $\mathbb{Q}$
      (i) passant par l'un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres,
      (ii) tangente à F_7 en deux des points a, b, ∞ et ayant un point de contact d'ordre 3 avec l'autre,
   (c) une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme point de contact d'ordre 7 en chacun de ces points,
   (d) une quintique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 5 en un des points a, b, ∞ et d'ordre 8 en chacun des points P et $\overline{P}$,
   (e) une sextique définie sur $\mathbb{Q}$ ayant deux points de contact d'ordre 6 parmi les points a, b, ∞ et d'ordre 8 en chacun des points P et $\overline{P}$.

3.1.2 Notions auxiliaires

3.1.2.1 L'espace de Riemann-Roch

Pour un diviseur D sur F_7, notons par $l(D)$ la $\overline{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$, où $\mathcal{L}(D)$ est le $\overline{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles f défini par

$$\mathcal{L}(D) = \{f \in \overline{\mathbb{Q}}(F_7)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Considérons x et y les fonctions rationnelles sur F_7 données par

$$x(X, Y, Z) = \frac{X}{Z} \quad \text{et} \quad y(X, Y, Z) = \frac{Y}{Z}.$$

Soit ε une racine primitive $14^{\text{ième}}$ de l'unité dans $\overline{\mathbb{Q}}$. Considérons a_j, b_j et c_j les points sur F_7 définis par

$$a_j = (0, \varepsilon^{2j+1}, 1), \quad b_j = (\varepsilon^{2j+1}, 0, 1), \quad c_j = (\varepsilon^{2j+1}, 1, 0),$$

pour $0 \leq j \leq 6$. Observons que $a = a_3$, $b = b_3$ et $\infty = c_3$.

Lemme 3.1.1 (**Rohrlich**, [Roh77])**.** On a
(1) $\mathrm{div}(x) = (a_0 + \cdots + a_6) - (c_0 + \cdots + c_6)$
(2) $\mathrm{div}(x + y) = 7\infty - (c_0 + \cdots + c_6)$.

Lemme 3.1.2. Si $k \in \{4, 6\}$, les fonctions rationnelles f_{rs} définies par

$$f_{rs}(x, y) = \frac{x^r}{(x + y)^s}, \quad \text{avec} \quad 0 \leq r \leq s \leq k,$$

forment une base pour l'espace vectoriel $\mathcal{L}(7k\infty)$.

Démonstration. D'après le Lemme 3.1.1, on a

$$\begin{aligned}\mathrm{div}(f_{rs}(x, y)) &= r\mathrm{div}(x) - s\mathrm{div}(x + y) \\ &= r(a_0 + \cdots + a_6) + (s - r)(c_0 + c_1 + c_2 + c_4 + c_5 + c_6) - (6s + r)\infty.\end{aligned}$$

Comme $0 \leq r \leq s \leq k$, $6s + r \leq 7k$, on a $f_{rs}(x, y) \in \mathcal{L}(7k\infty)$. Pour chaque k fixé, la fonction f_{rs} a un unique pôle en ∞ d'ordre $6s + r$ et que tous ces pôles sont différents. En effet,

- Pour $k = 4$:

f_{rs}	f_{00}	f_{01}	f_{02}	f_{03}	f_{04}	f_{11}	f_{12}	f_{13}	f_{14}	f_{22}
ordre du pôle de f_{rs}	0	6	12	18	24	7	13	19	25	14

f_{23}	f_{24}	f_{33}	f_{34}	f_{44}
20	26	21	27	28

Par conséquent, les fonctions f_{rs} avec $0 \leq r \leq s \leq 4$ sont linéairement indépendantes. Comme le genre de F_7 est égal à 15, 28∞ est un diviseur canonique sur F_7, d'où $l(28\infty) = 15 = \#\{f_{rs},\ 0 \leq r \leq s \leq 4\}$.

- Pour $k = 6$:
Si $6s + r = 6s' + r'$ avec $0 \leq r \leq s \leq 6$ et $0 \leq r' \leq s' \leq 6$ alors $r \equiv r' \pmod 6$. Comme $0 \leq r, r' \leq 6$, $r = r'$ ou $r, r' \in \{0, 6\}$ avec $r \neq r'$. Supposons qu'on ait $r, r' \in \{0, 6\}$ avec $r \neq r'$. Si par exemple $r = 0$, $r' = 6$ donc $s' = 6$. De $6s + r = 6s' + r'$, on obtient $s = 7$, ce qui contredit $s \leq 6$. On conclut que $r = r'$, ce qui entraîne $s = s'$. Par suite, les fonctions f_{rs} avec $0 \leq r \leq s \leq 6$ sont linéairement indépendantes. D'après le théorème de Riemann-Roch, on a $l(42\infty) = 28 = \#\{f_{rs},\ 0 \leq r \leq s \leq 6\}$.

❑

3.1.2.2 Lemmes géométriques

Lemme 3.1.3. Soient L_a, L_b et L_∞ les droites tangentes à F_7 en a, b et ∞ respectivement.

(i) Les droites L_a, L_b, L_∞ ont un point de contact d'ordre 7 avec F_7 en a, b, ∞ respectivement.

(ii) Si une courbe algébrique plane Γ de degré ≤ 6 a un point de contact d'ordre $> \deg(\Gamma)$ avec F_7 en a, b ou ∞, alors Γ est réductible et contient L_a, L_b ou L_∞ respectivement.

Démonstration.

(i) En affine, on a $F_7 : x^7 + y^7 + 1 = 0$. La droite tangente à F_7 en a est $L_a : y + 1 = 0$. Il est clair que a est le seul point d'intersection de la droite L_a et la courbe F_7. Ainsi, par le théoème de Bézout, on a

$$L_a.F_7 = (\deg L_a \times \deg F_7)a = 7a = \mathrm{mult}_a(L_a \cap F_7)a.$$

On montre de même pour L_b et L_∞.

(ii) Soient H, G et F des courbes planes. Supposons que H est irréductible et sans composante commune ni avec G ni avec F. Soit $\mathcal{A}$ un point lisse de H. Alors, d'après le Lemme 2.3.2 dans [Nam79], on a

$$\min\{\mathrm{mult}_{\mathcal{A}}(H \cap F), \mathrm{mult}_{\mathcal{A}}(H \cap G)\} \leq \mathrm{mult}_{\mathcal{A}}(F \cap G).$$

Ainsi, pour obtenir le résultat souhaité, il suffit de prendre $\mathcal{A} \in \{a, b, \infty\}$, $H = L_{\mathcal{A}}$, $G = \Gamma$ et $F = F_7$ en tenant compte de (i).

❑

Lemme 3.1.4. Soit L la droite d'équation $X + Y + Z = 0$. Alors $L.F_7 = a + b + \infty + 2P + 2\overline{P}$.

Démonstration. En affine, on a $L : x + y + 1 = 0$ et $F_7 : x^7 + y^7 + 1 = 0$. On sait que $L \cap F_7 = \{a, b, \infty, P, \overline{P}\}$, il existe alors des entiers strictement positifs n_1, n_2, n_3, n_4, n_5 tels que $L.F_7 = n_1 a + n_2 b + n_3 \infty + n_4 P + n_5 \overline{P}$ avec $n_1 + n_2 + n_3 + n_4 + n_5 = 7$. Comme P et $\overline{P}$ sont des conjugués, $n_4 = n_5$. La tangente à F_7 au point P est $T_P : x + y + 1 = 0$, par conséquent $n_4 \geq 2$; d'où $n_1 = n_2 = n_3 = 1$ et $n_4 = n_5 = 2$. ❑

3.1.2.3 Groupe de Mordell-Weil

Pour un entier s avec $1 \leq s \leq 5$, C_s désigne la courbe d'équation affine $v^7 = u(1-u)^s$ et J_s sa jacobienne. Considérons l'application rationnelle définie par

$$f_s : F_7 \longrightarrow C_s, \quad (x, y) \longmapsto (-x^7, (-1)^{s+1} x y^s).$$

Cette application induit un morphisme (noté aussi par f_s)

$$f_s : J_7 \longrightarrow J_s$$

et son dual

$$f_s^* : J_s \longrightarrow J_7.$$

Il est bien connu (voir [Lan82, Chapitre 2] ou [Mur93, Chapitre 8]) que ces applications induisent une isogénie définie sur $\mathbb{Q}$

$$f = \prod_{s=1}^{5} f_s : J_7 \longrightarrow \prod_{s=1}^{5} J_s$$

et son dual

$$f^* = \sum_{s=1}^{5} f_s^* : \prod_{s=1}^{5} J_s \longrightarrow J_7$$

telles que $f^* \circ f = 7$ sur J_7.

Lemme 3.1.5. $J_7(\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/7\mathbb{Z})^2$.

Démonstration. D'après Faddeev [Fad61a, Fad61b], $J_7(\mathbb{Q})$ est fini. Dans [Tze98], Tzermias conclut les deux faits suivants :

(i) pour un nombre premier $l \neq 2, 7$, le groupe $J_7[l^\infty](\mathbb{Q})$ est trivial.

(ii) le groupe $J_7[7^\infty](\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/7\mathbb{Z})^2$ et est engendré par $[a - \infty]$ et $[b - \infty]$.

Il ne nous reste qu'à calculer la partie 2−torsion de $J_7(\mathbb{Q})$. Comme il existe une isogénie

$$f : J_7 \longrightarrow \prod_{s=1}^{5} J_s,$$

alors cela revient à calculer la partie 2−torsion de chaque $J_s(\mathbb{Q})$. Or un résultat de Gross et Rohrlich dans [GR78] affirme que

$$J_s(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } 1 \equiv s^3 \equiv (6-s)^3 \pmod 7 \\ \mathbb{Z}/7\mathbb{Z} & \text{sinon} \end{cases}$$

mais les seuls $s \leq 5$ tels que $1 \equiv s^3 \equiv (6-s)^3 \pmod 7$ sont $s = 2$ ou $s = 4$, en effet, on a le tableau suivant

s	s^3	$(6-s)^3$
1	1	125
2	8	64
3	27	27
4	64	8
5	125	1

Ce qui donne deux copies de $\mathbb{Z}/2\mathbb{Z}$ et ainsi

$$J_7[2^\infty](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

❑

Soient A et B les automorphismes de F_7 donnés par

$$A(X,Y,Z) = (\zeta X, Y, Z) \quad \text{et} \quad B(X,Y,Z) = (X, \zeta Y, Z),$$

où ζ est une racine primitive $7^{\text{ième}}$ de l'unité telle que $\varepsilon^2 = \zeta$.

Puisque $f_s : F_7 \longrightarrow C_s$ est un revêtement galoisien dont le groupe de Galois est engendré par $A^{-s}B$, alors pour un diviseur D de degré zéro sur F_7, on a

$$(f_s^* \circ f_s)(D) = \sum_{j=0}^{6} (A^{-s}B)^j(D)$$

sur J_7 (voir [GR78]).

Posons maintenant $x_0 = -P - \overline{P} + 2\infty$, $x_1 = (f_4^* \circ f_4)(x_0)$ et $x_2 = (f_2^* \circ f_2)(x_0)$. Nous avons la proposition suivante :

Proposition 3.1.1.

(P1) Le diviseur x_0 est d'ordre 14. On montre que $-2x_1$ est le diviseur de $y^3 + x + x^3y$. Ainsi, x_1 est un point d'ordre 2 sur $J_7(\mathbb{Q})$.

(P2) $(f_4^* \circ f_4)(x_1) = 7x_1$ et $(f_2^* \circ f_2)(x_2) = 7x_2$.

(P3) $(\mathbb{Z}/2\mathbb{Z})^2 =< x_1, x_2 >$.

(P4) $f_s(a - \infty)$ et $f_s(b - \infty)$ sont d'ordre 7.

(P5) $J_s(\mathbb{Q})_{\text{tors}} \subseteq \ker(f_s^*)$.

(P6) $\ker(f_s^* \circ f_s) \subseteq J_7[7]$.

Démonstration.

(P1) : on a

$$-x_1 = (f_4^* \circ f_4)(-x_0) = \sum_{j=0}^{6} (A^3B)^j(-x_0) = \sum_{j=0}^{6} (A^3B)^j(P + \overline{P}) - 2\sum_{j=0}^{6} (A^3B)^j(\infty).$$

On a aussi

$$(A^3B)^j(X,Y,Z) = (\zeta^{3j}X, \zeta^j Y, Z) \text{ et donc } (A^3B)^j(\infty) = (-\zeta^{3j}, \zeta^j, 0) = (\varepsilon^{4j+7}, 1, 0).$$

Il en résulte que $(A^3B)^0(\infty) = c_3$, $(A^3B)^1(\infty) = c_5$, $(A^3B)^2(\infty) = c_0$, $(A^3B)^3(\infty) = c_2$, $(A^3B)^4(\infty) = c_4$, $(A^3B)^5(\infty) = c_6$ et $(A^3B)^6(\infty) = c_1$. Ainsi,

$$-x_1 = \sum_{j=0}^{6} (A^3B)^j(P + \overline{P}) - 2\sum_{j=0}^{6} c_j.$$

Cherchons $\text{div}(y^3 + x + x^3y)$. On a

$$\begin{aligned} \text{div}(y^3 + x + x^3y) &= \text{div}\Big(\frac{Y^3Z + XZ^3 + X^3Y}{Z^4}\Big) \\ &= \text{div}(Y^3Z + XZ^3 + X^3Y) - 4\text{div}(Z) \\ &= (Y^3Z + XZ^3 + X^3Y = 0).F_7 - 4(Z = 0).F_7 \end{aligned}$$

Considérons la courbe suivante $\mathcal{K} : Y^3Z + XZ^3 + X^3Y = 0$. Une vérification directe montre que

$$(X, Y, Z) \in \mathcal{K} \cap F_7 \quad \text{si, et seulemnt si} \quad (A^3B)^j(X, Y, Z) \in \mathcal{K} \cap F_7.$$

Les points P et $\overline{P}$ appartiennent à $\mathcal{K} \cap F_7$, il en est de même des points $(A^3B)^j(P)$ et $(A^3B)^j(\overline{P})$ avec $0 \leq j \leq 6$ soient 14 points avec la même multiplicité. La tangente à $\mathcal{K}$ au point P est $T_P : X + Y + Z = 0$ qui est aussi la tangente à F_7 au point P ; donc $\text{mult}_P(\mathcal{K} \cap F_7) \geq 2$. Le point P apparaît avec une multiplicité ≥ 2, ce qui veut dire que chacun des points $(A^3B)^j(P)$ apparaît avec une multiplicité ≥ 2. Puisque les 14 points $(A^3B)^j(P)$ et $(A^3B)^j(\overline{P})$ apparaîssent avec la même multiplicité, et que $\mathcal{K} \cap F_7$ comportent 28 points comptés avec leur multiplicité, alors cette multiplicité commune ne peut être que 2. On peut donc écrire

$$\text{div}(y^3 + x + x^3y) = 2\sum_{j=0}^{6}(A^3B)^j(P + \overline{P}) - 4\sum_{j=0}^{6} c_j.$$

Ainsi, $\text{div}(y^3 + x + x^3y) = -2x_1$, ce qui prouve que x_1 est d'ordre 2.

Puisque $x_1 = (f_4^* \circ f_4)(x_0)$ et que le noyau de $f_4^* \circ f_4$ est annulé par 7, alors $14x_0 = 0$; par suite, x_0 est d'ordre 14.

Pour (P2), (P3), (P4), (P5) et (P6), on pourra consulter [GR78] et [Sal00b].

❑

Corollaire 3.1.1.

$$J_7(\mathbb{Q}) = \Big\{m[\infty - a] + n[\infty - b] + kx_0 + lx_2, \text{ avec } 0 \leq m, n \leq 6 \text{ et } 0 \leq k, l \leq 1\Big\}$$

ou bien

$$J_7(\mathbb{Q}) = \Big\{m[\infty - a] + n[\infty - b] + kx_0 + lx_1, \text{ avec } 0 \leq m, n \leq 6 \text{ et } 0 \leq k, l \leq 1\Big\}.$$

Démonstration. En combinant le Lemme 3.1.5 et (P3), on a

$$J_7(\mathbb{Q}) = \Big\{m_1[\infty - a] + n_1[\infty - b] + kx_1 + lx_2, \text{ avec } 0 \leq m_1, n_1 \leq 6 \text{ et } 0 \leq k, l \leq 1\Big\}.$$

Ensuite (P1) et (P2) donnent $(f_4^* \circ f_4)(x_1) = x_1 = (f_4^* \circ f_4)(x_0)$. D'après (P6), on a $x_1 - x_0 \in \ker(f_4^* \circ f_4) \subseteq J_7[7]$, donc

$$x_1 - x_0 = m_2[\infty - a] + n_2[\infty - b] \text{ avec } 0 \leq m_2, n_2 \leq 6.$$

Par suite

$$J_7(\mathbb{Q}) = \Big\{m[\infty - a] + n[\infty - b] + kx_0 + lx_2, \text{ avec } 0 \leq m, n \leq 6 \text{ et } 0 \leq k, l \leq 1\Big\}.$$

De même, en utilisant $f_2^* \circ f_2$, on trouve l'autre expression de $J_7(\mathbb{Q})$. ❑

3.1.3 Preuve du Théorème 3.1.2

Soit R un point algébrique sur F_7 de degré d sur $\mathbb{Q}$ avec $11 \leq d \leq 14$. Soient $R_1, \cdots, R_d$ les conjugués de Galois de R. On pose $t = [R_1 + \cdots + R_d - d\infty] \in J_7(\mathbb{Q})$. D'après le corollaire 3.1.1, on peut considérer les quatre cas suivants :

Cas 1. $t = m[\infty - a] + n[\infty - b]$ avec $0 \leq m, n \leq 6$.

Alors, on a $[R_1 + \cdots + R_d - d\infty] = m[\infty - a] + n[\infty - b]$, c'est-à-dire,

$$[R_1 + \cdots + R_d + ma + nb - (d + m + n)\infty] = 0.$$

Puisque $d + m + n \leq 28$, le Lemme 3.1.2 entraîne l'existence d'un polynôme quartique $f(x, y)$ tel que

$$\operatorname{div}(f(x, y)/(x + y)^4) = R_1 + \cdots + R_d + ma + nb - (d + m + n)\infty.$$

Ainsi, d'après le Lemme 3.1.1, on a

$$\operatorname{div}(f(x, y)) = R_1 + \cdots + R_d + ma + nb + (28 - d - m - n)\infty - 4(c_0 + \cdots + c_6).$$

En utilisant l'homogénéisé f^* de f, on a

$$f^*(X, Y, Z) = Z^4 f(\frac{X}{Z}, \frac{Y}{Z}),$$

où $f^*(X, Y, Z)$ définit une courbe Γ_4 de degré 4 ; ce qui montre l'existence d'une quartique Γ_4 définie sur $\mathbb{Q}$. Comme la courbe F_7 est lisse, $\operatorname{div}(f(x, y)) = \Gamma_4.F_7 - 4(c_0 + \cdots + c_6)$. Par conséquent,

$$\Gamma_4.F_7 = R_1 + \cdots + R_d + ma + nb + (28 - d - m - n)\infty.$$

Si $m \geq 5$ alors, d'après le Lemme 3.1.3, Γ_4 est réductible et contient L_a. De plus, puisque $m \leq 6$, un des R_i est égal à a, ce qui est absurde. En effet, on a :

$$\left.\begin{array}{c} \Gamma_4 = L_a + \Gamma_3 \\ L_a.F_7 = 7a \end{array}\right\} \Longrightarrow \Gamma_4.F_7 = L_a.F_7 + \Gamma_3.F_7 = 7a + \Gamma_3.F_7.$$

On voit que $\Gamma_4.F_7$ contient a avec une multiplicité ≥ 7. Comme $m \leq 6$ et a est différent de b et de ∞, un des R_i est égal à a ; ce qui contredit le fait que R_i et a ne sont pas de même degré. D'où $m \leq 4$, de même, $n \leq 4$. Par conséquent, $6 \leq 28 - d - m - n \leq 17$. Le Lemme 3.1.3 montre aussi que Γ_4 contient L_∞, il existe une cubique Γ_3 telle que

$$\Gamma_3.F_7 = R_1 + \cdots + R_d + ma + nb + (21 - d - m - n)\infty. \qquad (*)$$

On doit avoir $0 \leq m, n \leq 3$ et donc $1 \leq 21 - d - m - n \leq 10$. La somme des coefficients de a, b et ∞ est égale à $21 - d$.

1.1. Supposons que $1 \leq 21 - d - m - n \leq 3$. Alors, la somme des coefficients de a, b et ∞ est ≤ 9, i.e., $21 - d \leq 9$, d'où $d \geq 12$. Notons m_1, m_2 et m_3 les coefficients de a, b et ∞ respectivement. On a $0 \leq m_1, m_2 \leq 3$, $1 \leq m_3 \leq 3$ et $m_1 + m_2 + m_3 = 21 - d$.
Ainsi, on obtient :

1.1.a. pour $d = 12$, la relation $(*)$ devient

$$\Gamma_3.F_7 = R_1 + \cdots + R_{12} + 3a + 3b + 3\infty,$$

ce qui montre que des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une cubique définie sur $\mathbb{Q}$ ayant a, b et ∞ comme points de contact d'ordre 3 en chacun de ces points.

1.1.b. pour $d = 13$, la relation $(*)$ devient

$$\Gamma_3.F_7 = R_1 + \cdots + R_{13} + m_1a + m_2b + m_3\infty \text{ avec } m_i \in \{2, 3\} \text{ et } m_1 + m_2 + m_3 = 8,$$

ce qui montre que des points algébriques sur F_7 de degré 13 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une cubique définie sur $\mathbb{Q}$ tangente à F_7 en un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres.

1.1.c. pour $d = 14$, la relation $(*)$ devient

$$\Gamma_3.F_7 = R_1 + \cdots + R_{14} + m_1a + m_2b + m_3\infty \text{ avec } m_i \in \{1, 2, 3\} \text{ et } m_1 + m_2 + m_3 = 7,$$

ce qui montre que des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une cubique définie sur $\mathbb{Q}$
- passant par l'un des points a, b, ∞ et ayant un point de contact d'ordre 3 avec les deux autres,
- tangente à F_7 en deux des points a, b, ∞ et ayant un point de contact d'ordre 3 avec l'autre.

1.2. Supposons que $21 - d - m - n \geq 4$. Alors, d'après le Lemme 3.1.3, Γ_3 contient L_∞, il existe une conique Γ_2 telle que

$$\Gamma_2.F_7 = R_1 + \cdots + R_d + ma + nb + (14 - d - m - n)\infty. \qquad (**)$$

On doit avoir $0 \leq m, n \leq 2$ et $0 \leq 14 - d - m - n \leq 2$. La somme des coefficients de a, b et ∞ est égale à $14 - d$. Notons m_1, m_2 et m_3 les coefficients de a, b et ∞ respectivement. On a $0 \leq m_i \leq 2$ et $m_1 + m_2 + m_3 = 14 - d$. Si les $m_i \neq 0$ alors, d'après le Lemme 3.1.4, Γ_2 contient L, ce qui est absurde sinon un des R_i serait égal à P ou $\overline{P}$. D'où, un au moins des m_i est nul.
Ainsi, on obtient :

1.2.a. pour $d = 11$, la relation $(**)$ devient

$$\Gamma_2.F_7 = R_1 + \cdots + R_{11} + m_1a + m_2b + m_3\infty \text{ avec } m_i \neq m_j \in \{0, 1, 2\} \text{ et } m_1 + m_2 + m_3 = 3,$$

ainsi, des points algébriques sur F_7 de degré 11 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞ et tangente en un des deux autres.

1.2.b. pour $d = 12$, la relation $(**)$ devient

$$\Gamma_2.F_7 = R_1 + \cdots + R_{12} + m_1a + m_2b + m_3\infty \text{ avec } m_i \in \{0, 1, 2\} \text{ et } m_1 + m_2 + m_3 = 2,$$

ainsi, des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$
- passant par deux des points a, b, ∞,
- tangente à F_7 en un des points a, b, ∞.

1.2.c. pour $d = 13$, la relation $(**)$ devient

$$\Gamma_2.F_7 = R_1 + \cdots + R_{13} + m_1a + m_2b + m_3\infty \text{ avec } m_i \in \{0, 1\} \text{ et } m_1 + m_2 + m_3 = 1,$$

ainsi, des points algébriques sur F_7 de degré 13 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞.

1.2.d. pour $d = 14$, la relation $(**)$ devient

$$\Gamma_2.F_7 = R_1 + \cdots + R_{14},$$

ainsi, des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$.

Cas 2. $t = m[\infty - a] + n[\infty - b] + x_0$ avec $0 \leq m, n \leq 6$.

Alors, on a $[R_1 + \cdots + R_d + ma + nb + P + \overline{P} - (d+m+n+2)\infty] = 0$. Comme $d+m+n+2 \leq 28$, les Lemmes 3.1.2 et 3.1.1 assurent l'existence d'un polynôme quartique $f(x, y)$ tel que

$$\mathrm{div}(f(x,y)) = R_1 + \cdots + R_d + ma + nb + P + \overline{P} + (26 - d - m - n)\infty - 4(c_0 + \cdots + c_6).$$

La courbe plane F_7 étant lisse, il existe alors une quartique Γ_4 telle que $\mathrm{div}(f(x,y)) = \Gamma_4.F_7 - 4(c_0 + \cdots + c_6)$. Par suite,

$$\Gamma_4.F_7 = R_1 + \cdots + R_d + ma + nb + P + \overline{P} + (26 - d - m - n)\infty.$$

On doit avoir $0 \leq m, n \leq 4$ et donc $4 \leq 26 - d - m - n \leq 15$.

2.1. Si $26 - d - m - n = 4$, i.e., $d = 14$, $m = n = 4$, alors

$$\Gamma_4.F_7 = R_1 + \cdots + R_{14} + 4a + 4b + P + \overline{P} + 4\infty.$$

Ainsi, d'après le Lemme 3.1.4, Γ_4 contient L, ce qui est absurde sinon un des R_i serait égal à P ou $\overline{P}$.

2.2. Si $26 - d - m - n \geq 5$, alors Γ_4 contient L_∞, il existe une cubique Γ_3 telle que

$$\Gamma_3.F_7 = R_1 + \cdots + R_d + ma + nb + P + \overline{P} + (19 - d - m - n)\infty.$$

On doit avoir $0 \leq m, n \leq 3$ et $19 - d - m - n \geq 0$.

2.2.a. Si $m = n = 0$, alors

$$\Gamma_3.F_7 = R_1 + \cdots + R_d + P + \overline{P} + (19 - d)\infty.$$

On a $19 - d \geq 5$, donc Γ_3 contient L_∞, il existe une conique Γ_2 telle que

$$\Gamma_2.F_7 = R_1 + \cdots + R_d + P + \overline{P} + (12 - d)\infty,$$

ce qui donne $d = 12$, d'où

$$\Gamma_2.F_7 = R_1 + \cdots + R_{12} + P + \overline{P},$$

ainsi, des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par P et $\overline{P}$.

2.2.b. Si $m \neq 0$ ou $n \neq 0$, alors deux au moins des coefficients de a, b et ∞ sont non nuls, donc, d'après le Lemme 3.1.4, Γ_3 contient L, ce qui est absurde sinon un des R_i serait égal P ou $\overline{P}$.

Cas 3. $t = m[\infty - a] + n[\infty - b] + kx_0 + x_1$ avec $0 \leq m, n \leq 6$ et $0 \leq k \leq 1$.

Alors, on a $[R_1 + \cdots + R_d - d\infty] = [m(\infty - a) + n(\infty - b) + kx_0 + x_1]$. En composant par $f_4^* \circ f_4$ puis en utilisant (P4) et (P5), on a $(f_4^* \circ f_4)([R_1 + \cdots + R_d - d\infty]) = (f_4^* \circ f_4)(kx_0) + (f_4^* \circ f_4)(x_1)$. Ensuite, en combinant (P2) et la définition de x_1, on a

$$(f_4^* \circ f_4)([R_1 + \cdots + R_d - d\infty]) = (f_4^* \circ f_4)(kx_0) + (f_4^* \circ f_4)(7x_0).$$

Ainsi, on a

$$(f_4^* \circ f_4)([R_1 + \cdots + R_d - (7+k)x_0 - d\infty]) = 0.$$

De (P6), on obtient

$$[R_1 + \cdots + R_d - (7+k)x_0 - d\infty] = m[\infty - a] + n[\infty - b],$$

ce qui s'écrit aussi

$$[R_1 + \cdots + R_d + ma + nb + (7+k)P + (7+k)\overline{P} - (14 + d + m + n + 2k)\infty] = 0.$$

Puisque $14 + d + m + n + 2k \leq 42$, les Lemmes 3.1.2 et 3.1.1 assurent l'existence d'un polynôme sextique $f(x, y)$ tel que

$$\mathrm{div}(f(x,y)) = R_1+\cdots+R_d+ma+nb+(7+k)P+(7+k)\overline{P}+(28-d-m-n-2k)\infty-6(c_0+\cdots+c_6).$$

La courbe F_7 étant lisse, il existe une sextique Γ_6 telle que $\mathrm{div}(f(x,y)) = \Gamma_6.F_7 - 6(c_0 + \cdots + c_6)$. Par suite,

$$\Gamma_6.F_7 = R_1 + \cdots + R_d + ma + nb + (7+k)P + (7+k)\overline{P} + (28 - d - m - n - 2k)\infty.$$

3.1. $m = 0$ ou $n = 0$

3.1.a. Si $m = n = 0$, alors $\Gamma_6.F_7 = R_1 + \cdots + R_d + (7+k)P + (7+k)\overline{P} + (28-d-2k)\infty$ avec $12 \leq 28 - d - 2k \leq 17$. La courbe Γ_6 contient L_∞, il existe une quintique Γ_5 telle que $\Gamma_5.F_7 = R_1+\cdots+R_d+(7+k)P+(7+k)\overline{P}+(21-d-2k)\infty$ avec $5 \leq 21-d-2k \leq 10$.

3.1.a.i. Si $21 - d - 2k = 5$, i.e., $d = 14$ et $k = 1$, alors

$$\Gamma_5.F_7 = R_1 + \cdots + R_{14} + 8P + 8\overline{P} + 5\infty,$$

c'est-à-dire, des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une quintique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 5 en ∞ et d'ordre 8 en chacun des points P et $\overline{P}$.

3.1.a.ii. Si $21 - d - 2k \geq 6$, alors Γ_5 contient L_∞, il existe une quartique Γ_4 telle que $\Gamma_4.F_7 = R_1 + \cdots + R_d + (7+k)P + (7+k)\overline{P} + (14 - d - 2k)\infty$. On voit que le coefficient de ∞ doit être nul sinon un des R_i devrait être égal à a ou b. Donc, $14 - d - 2k = 0$, i.e., on a ($d = 14$ et $k = 0$) ou ($d = 12$ et $k = 1$). Par conséquent,

$$\Gamma_4.F_7 = R_1 + \cdots + R_{14} + 7P + 7\overline{P},$$

en d'autres termes, des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme point de contact d'ordre 7 en chacun de ces points ; ou

$$\Gamma_4.F_7 = R_1 + \cdots + R_{12} + 8P + 8\overline{P},$$

en d'autres termes, des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une quartique définie sur $\mathbb{Q}$ ayant P et $\overline{P}$ comme point de contact d'ordre 8 en chacun de ces points.

3.1.b. Si $m = 0$ et $n \geq 1$ (resp. $m \geq 1$ et $n = 0$), alors

$$\Gamma_6.F_7 = R_1 + \cdots + R_d + nb + (7+k)P + (7+k)\overline{P} + (28 - d - n - 2k)\infty,$$

avec $6 \leq 28 - d - n - 2k \leq 16$.

3.1.b.i. Si $28 - d - n - 2k = 6$, i.e., $d = 14$, $n = 6$ et $k = 1$, alors

$$\Gamma_6.F_7 = R_1 + \cdots + R_{14} + 6b + 8P + 8\overline{P} + 6\infty,$$

ce qui prouve que des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une sextique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 6 en b et ∞ et d'ordre 8 en P et $\overline{P}$.

3.1.b.ii. Si $28 - d - n - 2k \geq 7$, alors Γ_6 contient L_∞, il existe une quintique Γ_5 telle que $\Gamma_5.F_7 = R_1 + \cdots + R_d + nb + (7+k)P + (7+k)\overline{P} + (21 - d - n - 2k)\infty$ avec $0 \leq 21 - d - n - 2k \leq 9$. Puisque $n \neq 0$, le coefficient de ∞ doit être nul, i.e., $21 - d - n - 2k = 0$, dans ce cas, on a ($d = 13$, $n = 6$ et $k = 1$) ou ($d = 14$, $n = 5$ et $k = 1$). Par consequent, $\Gamma_5.F_7 = R_1 + \cdots + R_{13} + 6b + 8P + 8\overline{P}$, ce cas est absurde sinon un des R_i devrait être égal à b ou

$$\Gamma_5.F_7 = R_1 + \cdots + R_{14} + 5b + 8P + 8\overline{P},$$

c'est-a-dire, des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une quintique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 5 en b et d'ordre 8 en chacun des points P et $\overline{P}$.

3.2. $m = 1$ ou $n = 1$

3.2.a. Si $m = n = 1$, alors $\Gamma_6.F_7 = R_1 + \cdots + R_d + a + b + (7+k)P + (7+k)\overline{P} + (26 - d - 2k)\infty$. La courbe Γ_6 contient L, il existe une quintique Γ_5 telle que $\Gamma_5.F_7 = R_1 + \cdots + R_d + (5+k)P + (5+k)\overline{P} + (25 - d - 2k)\infty$ avec $9 \leq 25 - d - 2k \leq 14$. La courbe Γ_5 contient L_∞, il existe une quartique Γ_4 telle que $\Gamma_4.F_7 = R_1 + \cdots + R_d + (5+k)P + (5+k)\overline{P} + (18 - d - 2k)\infty$ avec $2 \leq 18 - d - 2k \leq 7$. Comme le coefficient de ∞ est non nul, Γ_4 contient L ce qui est absurde sinon un des R_i devrait être égal à a ou b.

3.2.b. Si $m = 1$ et $n \geq 2$ (resp. $m \geq 2$ et $n = 1$), alors $\Gamma_6.F_7 = R_1 + \cdots + R_d + a + nb + (7+k)P + (7+k)\overline{P} + (27 - d - n - 2k)\infty$. On voit que Γ_6 contient L, il existe une quintique Γ_5 telle que $\Gamma_5.F_7 = R_1 + \cdots + R_d + (n-1)b + (7+k)P + (7+k)\overline{P} + (26 - d - n - 2k)\infty$. Comme le coefficient de ∞ est non nul, Γ_5 contient L ce qui est absurde sinon un des R_i devrait être égal à a.

3.3. $2 \leq m, n \leq 6$

3.3.a. Si $28 - d - m - n - 2k = 0$, i.e., $d = 14$, $m = n = 6$ et $k = 1$, alors

$$\Gamma_6.F_7 = R_1 + \cdots + R_{14} + 6a + 6b + 8P + 8\overline{P},$$

ce qui prouve que des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une sextique définie sur $\mathbb{Q}$ ayant un point de contact d'ordre 6 en a et b et d'ordre 8 en P et $\overline{P}$.

3.3.b. Si $28 - d - m - n - 2k \geq 1$, alors Γ_6 contient L, il existe une quintique Γ_5 telle que

$$\Gamma_5.F_7 = R_1 + \cdots + R_d + (m-1)a + (n-1)b + (5+k)P + (5+k)\overline{P} + (27 - d - m - n - 2k)\infty.$$

On voit que Γ_5 contient L, il existe une quartique Γ_4 telle que

$$\Gamma_4.F_7 = R_1 + \cdots + R_d + (m-2)a + (n-2)b + (3+k)P + (3+k)\overline{P} + (26 - d - m - n - 2k)\infty.$$

Puisque, les coefficients de a, b et ∞ ne sont pas simultanément nuls, alors Γ_4 contient L, il existe une cubique Γ_3 telle que

$$\Gamma_3.F_7 = R_1 + \cdots + R_d + (m-3)a + (n-3)b + (1+k)P + (1+k)\overline{P} + (25 - d - m - n - 2k)\infty.$$

On doit avoir $3 \leq m, n \leq 6$ et $25 - d - m - n - 2k \geq 0$.

3.3.b.i. Si $m = n = 3$, alors

$$\Gamma_3.F_7 = R_1 + \cdots + R_d + (1+k)P + (1+k)\overline{P} + (19 - d - 2k)\infty,$$

avec $3 \leq 19 - d - 2k \leq 8$.

- Si $19 - d - 2k = 3$, i.e., $d = 14$ et $k = 1$, alors

$$\Gamma_3.F_7 = R_1 + \cdots + R_{14} + 2P + 2\overline{P} + 3\infty.$$

On voit que Γ_3 contient L, ce qui est absurde.
- Si $19 - d - 2k \geq 4$, alors Γ_3 contient L_∞, il existe une conique Γ_2 telle que $\Gamma_2.F_7 = R_1 + \cdots + R_d + (1+k)P + (1+k)\overline{P} + (12 - d - 2k)\infty$. On doit avoir $12 - d - 2k = 0$, i.e., $d = 12$ et $k = 0$ donc

$$\Gamma_2.F_7 = R_1 + \cdots + R_{12} + P + \overline{P},$$

ainsi, des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par P et $\overline{P}$.

3.3.b.ii. Si $m \neq 3$ ou $n \neq 3$, on voit que Γ_3 contient L, il existe une conique Γ_2 telle que

$$\Gamma_2.F_7 = R_1+\cdots+R_d+(m-4)a+(n-4)b+(k-1)P+(k-1)\overline{P}+(24-d-m-n-2k)\infty.$$

On doit avoir $4 \leq m, n \leq 6$, $k = 1$ et $0 \leq 24 - d - n - 2k \leq 2$. La somme des coefficients de a, b et ∞ est égale à $14 - d$. On a

- $\Gamma_2.F_7 = R_1 + \cdots + R_{11} + m_1a + m_2b + m_3\infty$ avec $m_i \neq m_j \in \{0, 1, 2\}$ et $m_1 + m_2 + m_3 = 3$, ainsi, des points algébriques sur F_7 de degré 11 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞ et tangente en un des deux autres.
- $\Gamma_2.F_7 = R_1 + \cdots + R_{12} + m_1a + m_2b + m_3\infty$ avec $m_i \in \{0, 1, 2\}$ et $m_1 + m_2 + m_3 = 2$, ainsi, des points algébriques sur F_7 de degré 12 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$
  * passant par deux des points a, b, ∞,
  * tangente à F_7 en un des points a, b, ∞.
- $\Gamma_2.F_7 = R_1+\cdots+R_{13}+m_1a+m_2b+m_3\infty$ avec $m_i \in \{0, 1\}$ et $m_1+m_2+m_3 = 1$, ainsi, des points algébriques sur F_7 de degré 13 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$ passant par l'un des points a, b, ∞.
- $\Gamma_2.F_7 = R_1 + \cdots + R_{14}$, ainsi, des points algébriques sur F_7 de degré 14 sur $\mathbb{Q}$ sont obtenus comme intersection de F_7 avec une conique définie sur $\mathbb{Q}$.

Cas 4. $t = m[\infty - a] + n[\infty - b] + kx_0 + x_2$ avec $0 \leq m, n \leq 6$ et $0 \leq k \leq 1$.

Alors, on a $[R_1 + \cdots + R_d - d\infty] = [m(\infty - a) + n(\infty - b) + kx_0 + x_2]$. En composant par $f_2^* \circ f_2$ puis en utilisant (P4) et (P5), on a $(f_2^* \circ f_2)([R_1 + \cdots + R_d - d\infty]) = (f_2^* \circ f_2)(kx_0) + (f_2^* \circ f_2)(x_2)$. Ensuite, en combinant (P2) et la définition de x_2, on a

$$(f_2^* \circ f_2)([R_1 + \cdots + R_d - d\infty]) = (f_2^* \circ f_2)(kx_0) + (f_2^* \circ f_2)(7x_0).$$

Ainsi, on a

$$(f_2^* \circ f_2)([R_1 + \cdots + R_d - (7+k)x_0 - d\infty]) = 0.$$

De (P6), on obtient

$$[R_1 + \cdots + R_d - (7+k)x_0 - d\infty] = m[\infty - a] + n[\infty - b].$$

On trouve exactement la même l'expression que le **Cas 3.** et donc on aboutit aux mêmes résultats.

3.2 Points algébriques de degré au plus 2 sur les courbes affines $x^p + y^{pq} = 1$

Soient p et q deux nombres premiers tels que $p \in \{5, 7, 11\}$ et $q \geq 5$. Notons $\mathcal{C}_{p,q}$ la courbe d'équation affine

$$x^p + y^{pq} = 1.$$

Dans cette section, nous déterminons explicitement l'ensemble des points algébriques sur $\mathcal{C}_{p,q}$ de degré au plus 2 sur $\mathbb{Q}$.

3.2.1 Introduction

Étant donné une courbe algébrique projective lisse $\mathcal{C}$ de genre g définie sur un corps de nombres K, on note $\mathcal{C}(K)$ l'ensemble des points $K-$rationnels sur $\mathcal{C}$. On désigne par $J_{\mathcal{C}}$ la jacobienne de $\mathcal{C}$. On sait que, lorsque $g \geq 2$, l'ensemble $\mathcal{C}(K)$ est fini. On s'intéresse ici à la détermination explicite de l'ensemble $\bigcup_{[K:\mathbb{Q}]\leqslant 2} \mathcal{C}(K)$ des points sur $\mathcal{C}$ de degré ≤ 2. Le degré d'un point algébrique R sur $\mathcal{C}$ est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire, $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. Notons $\mathcal{C}^{(d)}(\mathbb{Q})$ l'ensemble des points algébriques sur $\mathcal{C}$ de degré exactement d sur $\mathbb{Q}$.

Soient p et q deux nombres premiers tels que $p \in \{5, 7, 11\}$ et $q \geq 5$. Considérons $\mathcal{C}_{p,q}$ la courbe d'équation affine

$$\mathcal{C}_{p,q} : x^p + y^{pq} = 1.$$

Notre travail va consister à étudier l'ensemble des points algébriques sur $\mathcal{C}_{p,q}$ de degré au plus 2 sur $\mathbb{Q}$ sans se préoccuper de la finitude du groupe de Mordell-Weil. L'étude de ces courbes a été motivée par le théorème de Chevalley-Weil et par les travaux de Gross et Rohrlich qui ont déterminé l'ensemble des points algébriques sur la courbe $F_p : x^p + y^p = 1$ de degré au plus 2 sur $\mathbb{Q}$.

Posons

$$a = (0, 1, 1), \quad b = (1, 0, 1), \quad \infty \text{ le point à l'infini,}$$
$$P = (\eta, \overline{\eta}, 1), \quad \overline{P} = (\overline{\eta}, \eta, 1), \quad Q = (\eta, \eta, 1), \quad \overline{Q} = (\overline{\eta}, \overline{\eta}, 1),$$

où $\eta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{6}}$ une racine primitive $6^{\text{ième}}$ de l'unité dans $\overline{\mathbb{Q}}$ et $\overline{\eta}$ le complexe conjugué de η.

Le théorème suivant résulte des travaux de Gross et Rohrlich :

Théorème 3.2.1. [GR78, Théorème 5.1] Soit $p \in \{5, 7, 11\}$. Si $[K : \mathbb{Q}] \leq (p-1)/2$, alors

$$F_p(K) \subseteq \{a, b, \infty, P, \overline{P}\}.$$

Notre résultat principal s'énonce comme suit :

Théorème 3.2.2. Soient p et q deux nombres premiers tels que $p \in \{5, 7, 11\}$ et $q \geq 5$. Considérons $\mathcal{C}_{p,q}$ la courbe d'équation affine

$$\mathcal{C}_{p,q} : x^p + y^{pq} = 1.$$

Alors

1. Les points $\mathbb{Q}-$rationnels sur $\mathcal{C}_{p,q}$ sont donnés par

$$\mathcal{C}_{p,q}(\mathbb{Q}) = \{a, b, \infty\}.$$

2. Les points algébriques sur $\mathcal{C}_{p,q}$ de degré 2 sur $\mathbb{Q}$ sont donnés par

$$\mathcal{C}^{(2)}_{p,q}(\mathbb{Q}) = \begin{cases} \{P, \overline{P}\} & \text{si} \quad q \equiv 1 \pmod 6 \\ \{Q, \overline{Q}\} & \text{si} \quad q \equiv 5 \pmod 6. \end{cases}$$

3.2.2 Notions auxiliaires

Définition 3.2.1 (**Fonction d'Euler**). On appelle fonction d'Euler la fonction φ définie pour tout $n \in \mathbb{N}^*$ par :

- $\varphi(1) = 1$,
- $\varphi(n) = n(1 - \frac{1}{n_1})(1 - \frac{1}{n_2}) \cdots (1 - \frac{1}{n_r})$ pour $n = n_1^{m_1} n_2^{m_2} \dots n_r^{m_r}$,

où les n_i, $1 \leqslant i \leqslant r$, sont des nombres premiers deux-à-deux distincts et les m_i sont non nuls dans $\mathbb{N}$.

En particulier, pour n un nombre premier, on a $\varphi(n) = n - 1$.

Lemme 3.2.1. Soient $n,\ m \in \mathbb{N}^*$ et $\zeta_n = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$ une racine primitive $n^{\text{ième}}$ de l'unité. On a

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \quad \text{et} \quad [\mathbb{Q}(\zeta_n^m) : \mathbb{Q}] = \varphi\Big(\frac{n}{\operatorname{pgcd}(n,\, m)}\Big).$$

Démonstration. La première assertion voir [Mil20, Chapitre 6] et, combinée avec $\mathbb{Q}(\zeta_n^m) = \mathbb{Q}(\zeta_n^{\operatorname{pgcd}(n,\, m)})$, on prouve la seconde assertion. ❑

Lemme 3.2.2. Soit q un nombre premier ≥ 5. Alors

$$q \equiv 1 \pmod 6 \quad \text{ou} \quad q \equiv 5 \pmod 6.$$

Démonstration. Considérons l'anneau $\mathbb{Z}/6\mathbb{Z} = \{\overline{0},\, \overline{1},\, \overline{2},\, \overline{3},\, \overline{4},\, \overline{5}\}$ où $\overline{a}$ avec $a \in \{0, 1, 2, 3, 4, 5\}$ représente la classe de a. Soit q un nombre premier ≥ 5. Alors, soit $q \in \overline{1}$ ou soit $q \in \overline{5}$. ❑

Théorème 3.2.3 (**Chevalley-Weil**). Soit $f : X \to Y$ un revêtement non ramifié de variétés projectives normales définies sur un corps de nombres K. Alors, il existe une extension finie L/K telle que

$$f^{-1}(Y(K)) \subset X(L).$$

Démonstration. On pourra consulter le livre [HS00, p. 292]. ❑

3.2.3 Preuve du Théorème 3.2.2

Considérons le morphisme suivant

$$f_q : \mathcal{C}_{p,\,q} \to F_p,\ \ (x,\, y) \mapsto (x,\, y^q)$$

où q un nombre premier ≥ 5 et $p \in \{5,\, 7,\, 11\}$. Alors, on a

$$\mathcal{C}_{p,\,q}^{(d)}(\mathbb{Q}) \subset \bigcup_{i|d} f_q^{-1}(F_p^{(i)}(\mathbb{Q})) \quad \text{et} \quad J_{\mathcal{C}_{p,\,q}}(\mathbb{Q}) \to J_{F_p}(\mathbb{Q}).$$

1. **Les points $\mathbb{Q}-$rationnels sur $\mathcal{C}_{p,\,q}$**

   Comme les points $\mathbb{Q}-$rationnels sur F_p sont donnés par

   $$F_p(\mathbb{Q}) = \{a, b, \infty\},$$

   alors, on a

   $$\mathcal{C}_{p,\,q}(\mathbb{Q}) \subset f_q^{-1}(F_p(\mathbb{Q})) = \{a, b, \infty\}.$$

   Il est clair que $\{a,\, b,\, \infty\} \subset \mathcal{C}_{p,\,q}(\mathbb{Q})$, par suite, pour tout $q \geq 5$, on a

   $$\mathcal{C}_{p,\,q}(\mathbb{Q}) = \{a,\, b,\, \infty\}.$$

2. Les points quadratiques sur $\mathcal{C}_{p,q}$

On sait que les points sur F_p de degré 2 sont donnés par

$$F_p^{(2)}(\mathbb{Q}) = \{P, \overline{P}\}.$$

On a alors la relation

$$f_q^{-1}(F_p^{(2)}(\mathbb{Q})) = \Big\{(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}}),\ (\mathrm{e}^{\frac{-2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k+2)\pi\mathrm{i}}{6q}}),\qquad 0 \leq k \leq q-1\Big\}$$

et donc

$$\mathcal{C}_{p,q}^{(2)}(\mathbb{Q}) \subset f_q^{-1}(F_p^{(2)}(\mathbb{Q})) = \Big\{(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}}),\ (\mathrm{e}^{\frac{-2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k+2)\pi\mathrm{i}}{6q}}),\qquad 0 \leq k \leq q-1\Big\}.$$

a. Le point $(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}})$ est un point de degré 2 si, et seulement si, les deux conditions suivantes sont vérifiées $6k-1 = \alpha q$ avec $\alpha \in \{1,5\}$ et $1 \leq k \leq q-1$. En effet, supposons que $6k-1 = \alpha q$ avec $\alpha \in \{1,5\}$ et $1 \leq k \leq q-1$, alors

$$\mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}} = (\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}})^{\alpha} \in \mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}})$$

or $[\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}}) : \mathbb{Q}] = \varphi(6) = 2$, et donc $[\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{6}}, \mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}}) : \mathbb{Q}] = 2$.
Réciproquement, on raisonne par la contraposition en supposant qu'on ait $6k-1 \neq \alpha q$ avec $\alpha \in \{1,5\}$ ou $k = 0$. Si $6k-1 \neq \alpha q$ avec $\alpha \in \{1,5\}$ alors $6k-1$ et $6q$ sont premiers entre eux ; ainsi, on a

$$\begin{aligned}[\mathbb{Q}(\mathrm{e}^{\frac{(12k-2)\pi\mathrm{i}}{6q}}) : \mathbb{Q}] =& [\mathbb{Q}(\mathrm{e}^{\frac{2(6k-1)\pi\mathrm{i}}{6q}}) : \mathbb{Q}] \\ =& \varphi(6q) = 2(q-1) > 2 \qquad \text{car } q \geq 5;\end{aligned}$$

ou si $k = 0$ alors

$$[\mathbb{Q}(\mathrm{e}^{\frac{-2\pi\mathrm{i}}{6q}}) : \mathbb{Q}] = \varphi(6q) = 2(q-1) > 2.$$

Vérifions que si une solution existe alors elle est unique. Supposons qu'on ait deux entiers k_1 et k_2 tels que $6k_1 - 1 = \alpha q$ et $6k_2 - 1 = \beta q$ avec $\alpha, \beta \in \{1,5\}$ et $1 \leq k_1 \leq k_2 \leq q-1$. On a

$$\begin{cases} 6k_1 - 1 &= \alpha q \\ 6k_2 - 1 &= \beta q \end{cases}$$

ce qui donne $6(k_2 - k_1) = (\beta - \alpha)q$, donc $q | 6(k_2 - k_1)$ et comme q est premier avec 6, alors par le théorème de Gauss $q | (k_2 - k_1)$, ceci impose que $k_1 = k_2$. Ainsi,

- si $q \equiv 1 \pmod 6$, on choisit $k = \dfrac{5q+1}{6}$, on trouve le point P,
- si $q \equiv 5 \pmod 6$, on choisit $k = \dfrac{q+1}{6}$, on trouve le point Q.

b. Le point $(\mathrm{e}^{\frac{-2\pi\mathrm{i}}{6}},\ \mathrm{e}^{\frac{(12k+2)\pi\mathrm{i}}{6q}})$ est un point de degré 2 si, et seulement si les deux conditions suivantes sont vérifiées $6k+1 = \alpha q$ avec $\alpha \in \{1,5\}$ et $1 \leq k \leq q-1$. Il suffit de reprendre le raisonnement proposé en **a.**. On obtient alors

- si $q \equiv 1 \pmod 6$, on choisit $k = \dfrac{q-1}{6}$ et on trouve le point $\overline{P}$,
- si $q \equiv 5 \pmod 6$, on choisit $k = \dfrac{5q-1}{6}$ et on trouve le point $\overline{Q}$.

Conclusion et perspectives

Dans cette thèse, nous nous sommes intéressés principalement à la détermination explicite des points algébriques de degré donné sur des courbes planes lisses. Les principes utilisés pour prouver les résultats principaux dans ce mémoire de thèse reposent sur deux approches :

- La première approche s'appuie sur la connaissance ou la détermination de la structure du groupe de Mordell-Weil et que ce dernier soit fini. C'est dans ce cadre que nous avons pu apporter trois contributions :
  - La première contribution porte sur la détermination des points algébriques de degré au plus d sur les courbes hyperelliptiques $y^2 = x^5 + n^2$, avec $n \in \{4,\ 5,\ 8, 10,\ 12, 16,\ 20,\ 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Cette contribution constitue une extension des travaux de Mulholland [Mul06] et Bruni [Bru15] qui décrivaient les points $\mathbb{Q}-$rationnels.
  - La deuxième contribution concerne la détermination des points algébriques de degré au plus 3 sur les courbes hyperelliptiques $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$, avec $n \in \{1,\ 2,\ 3,\ q$ un nombre premier et $q \equiv 7 \pmod{24}\}$. Ce résultat étend les travaux de Heiden [Hei98], Evink [Evi20] et Evink et al. [EHT21] qui ont donné les points $\mathbb{Q}-$rationnels.
  - Pour la troixième contribution, on étudie les points algébriques de degré au plus 14 sur la septique de Fermat $F_7 = \{(X,\ Y,\ Z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) : X^7 + Y^7 + Z^7 = 0\}$. Cette contribution étend le travail de Tzermias [Tze98] (resp. Sall [Sal00a, Sal03]) qui a décrit les points de degré au plus 5 (resp. au plus 10).
- On constante que le problème de la détermination des points algébriques de degré donné est souvent résolu pour certaines courbes dont le groupe de Mordell-Weil est fini. Pour contourner cette contrainte, on peut dans certains cas utiliser le théorème de Chevalley-Weil. C'est ainsi que la seconde approche représente une application du théorème de Chevalley-Weil pour la détermination explicite de l'ensemble des points algébriques de degré au plus 2 sur les courbes d'équations affines

$$x^p + y^{pq} = 1,$$

  avec p et q deux nombres premiers tels que $p \in \{5,\ 7,\ 11\}$ et $q \geq 5$.

Les résultats obtenus dans cette thèse ouvrent plusieurs perspectives. Et voici quelques pistes :

- La détermination des points algébriques sur $\mathbb{Q}$ de degré ≤ 2 est souvent déterminé de manière explicite. Cependent, pour les points de degré $d \geq 3$, déterminer l'ensemble des points algébriques de degré exactement d reste un problème ouvert.

- La détermination de l'ensemble des points algébriques de degré donné porte essentiellement sur les courbes définies sur $\mathbb{Q}$. Par contre, le cas des courbes définies sur un corps de nombres autre que $\mathbb{Q}$ reste un problème ouvert.
- Soit $\mathcal{C}$ une courbe hyperelliptique définie sur $\mathbb{Q}$ de genre $g \geq 3$. Stoll [Sto15b] a montré que si le rang de $J_{\mathcal{C}}(\mathbb{Q})$ satisfait $r \leq g-3$, alors

$$\#\mathcal{C}(\mathbb{Q}) \leq 33(g-1)+1 \text{ si } r=0 \text{ et } \#\mathcal{C}(\mathbb{Q}) \leq 8rg+33(g-1)-1 \text{ si } r \geq 1.$$

  Un des problèmes reste à déterminer de manière explicite $\mathcal{C}(\mathbb{Q})$.
- Soit $\mathcal{C}$ une courbe projective, lisse irréductible définie sur $\mathbb{Q}$ de genre $g \geq 2$ et r le rang de $J_{\mathcal{C}}(\mathbb{Q})$.
  Chabauty a montré que $\mathcal{C}(\mathbb{Q})$ est fini lorsque $r < g$. Plus tard, Coleman a réinterprété ce résultat de Chabauty en prouvant que si $r < g$ et $p > 2g$ est un nombre premier de bonne réduction pour $\mathcal{C}$, alors

$$\#\mathcal{C}(\mathbb{Q}) \leq \#\mathcal{C}(\mathbb{F}_p)+2g-2.$$

  Un des problèmes reste à déterminer de manière explicite $\mathcal{C}(\mathbb{Q})$.

Bibliographie

[Aud04] M. Audin Topologie : Revêtements et groupe fondamental, ULP, Strasbourg, (2004). http://www-irma.u-strasbg.fr/~maudin.

[BG06] E. Bombieri and W. Gubler, Heights in Diophantine Geometry, Cambridge University Press (2006).

[Bru15] C. A. Bruni, Twisted Extensions of Fermat's Last Theorem. ProQuest LLC, Ann Arbor, MI, (2015). Thesis (Ph.D.)-The University of British Columbia (Canada).

[Can87] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve. Mathematics of Computation, 48, 95 − 101, (1987).

[CFS23a] M. Camara, M. Fall and O. Sall, Algebraic points on the hyperelliptic curves $y^2 = x^5 + n^2$, Annales Universitatis Paedagogicae Cracoviensis. Studia Mathematica, 22, 21 − 31, (2023).

[CFS23b] M. Camara, M. Fall and O. Sall, Algebraic points of degree at most 2 on the affine curves $x^p + y^{pq} = 1$, JP Journal of Algebra, Number Theory and Applications, 61, 109 − 115, (2023).

[CFS23c] M. Camara, M. Fall and O. Sall, Parametrization of algebraic points of low degree on the hyperelliptic curves $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$. In Nonlinear analysis, geometry and applications. Proceedings of the third biennial international research symposium, NLAGA-BIRS, Saly-Mbour, Senegal, August 21 − 25, 2023, to appear. Cham : Birkhäuser, (2023).

[CF96] J. W. S. Cassels and E. V. Flynn, Prolegomena to a middlebrow arithmetic of curves of genus 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, (1996).

[CF06] H. Cohen and G. Frey, éditeurs. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall / CRC, (2006).

[Cha41] C. Chabauty, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. C. R. Acad. Sci. Paris 212, 882 − 885, (1941).

[CLO15] D. Cox, J. Little, and D. O'shea, Ideals, Varieties, and Algorithms : An introduction to Computational Algebraic Geometry and Commutative Algebra. Undergraduate Texts in Mathematics. Springer Verlag, New York, third edition, (2015).

[Col85] R. F. Coleman, Effective Chabauty. Duke Math. J. 52, 765 − 770, (1985).

[DK94] O. Debarre and M. Klassen, Points of low degree on smooth plane curves. J. Reine Angew. Math. 446, 81 − 87, (1994).

[EHT21] T. Evink, G.-J. van der Heiden and J. Top, Two-descent on some genus two curves, Indagationes Mathematicae (2021).
https://doi.org/10.1016/j.indag.2021.06.004.

[EM07] M. Elkadi and B. Mourrain, Introduction à la résolution des systèmes polynomiaux, volume 59 of Springer. Mathématiques & Applications, (2007).

[Evi20] T. Evink, Two-descent on hyperelliptic curves of genus two, (2020).
http://fse.studenttheses.ub.rug.nl/21636

[Fad61a] D. K. Faddeev, On the divisor class groups of some algebraic curves, Dokl. 136, 296 − 298, Sov. Math., 2, 67 − 69, (1961).

[Fad61b] D. K. Faddeev, Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in $l-$adic cyclotomic fields, Trudy Math. Inst. Steklov 64, 284 − 293, (1961).

[Fal21] M. Fall, Parametrization of Algebraic Points of Low Degrees on the Schaeffer Curve, Journal of Mathematical Sciences and Modelling, 4, 51 − 55, (2021).

[Fal83] G. Faltings, Endlichkeitsätze für abelsch Varietäten über Zahlkörpen, Invent. Math. 73, 349 − 366, (1983).

[FCS23] M. Fall, M. Camara and O. Sall, Algebraic points of degree at most 14 on the Fermat septic, Journal of the Nigerian Mathematical Society, 42, 95 − 109, (2023).

[Fly93] E. V. Flynn, The group law on the Jacobian of a curve of genus 2. J. Reine Angew. Math., 439, 45 − 69, (1993).

[Ful69] W. Fulton, Algebraic Curves, Benjamin, (1969).

[Gau00] P. Gaudry, Algorithmique des courbes hyperelliptiques et applications à la cryptologie. Thèse de doctorat, Ecole Polytechnique, Décembre (2000).

[GHM08] S. D. Galbraith, M. Harrison, and D. J Mireles Morales, Efficient hyperelliptic arithmetic using balanced representation for divisors, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, 342 − 356, (2008).

[GPN02] S. Galbraith, S.M. Paulus, and N. Smart. Arithmetic on superelliptic curves. Math. Comp., 71, 393 − 405, (2002).

[Gri89] P. A. Griffiths, Introduction to algebraic curves. In : Translations of mathematical monographs, vol. 76. American Mathematical Society, Providence, RI (1989).

[GR78] B. Gross and D. Rohrlich, Some results on the Mordell-Weil group of the jacobian of the Fermat curve, Invent. Math. 44, 201 − 224, (1978).

[Har77] R. Harshorne, Algebraic Geometry, Graduate texts in Mathematics 52, Springer-Verlag (1977).

[Hei98] G.-J. van der Heiden, Computing the 2−descent over $\mathbb{Q}$ for curves of genus 2, (1998).
http://fse.studenttheses.ub.rug.nl/8657

[HH90] D. Hilbert and A. Hurwitz, Über die diophantischen Gleichungen vom Geschlecht Null. Acta Math., 14(1) : 217 − 224, (1890).

[HS00] M. Hindry and J. H. Silverman, Diophantine geometry, an introduction, springer verlage, (2000). Graduade Texts in Mathematics 201.

[Kob89] N. Koblitz, Hyperelliptic cryptosystems, J. of Cryptology 1, 139 − 150, (1989).

[Lan59] S. Lang, Abelian varieties, Interscience Tracts in Pure and Applied Mathematics, no. 7, Interscience Publishers, (1959).

[Lan82] S. Lang, Introduction to algebraic and abelian functions, volume 89 of Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, second edition, (1982).

[Lan05] T. Lange, Formulae for arithmetic on genus 2 hyperelliptic curves. Applicable Algebra in Engineering, Communication and Computing, 15, 295 − 328, (2005).

[Mag10] MAGMA Computational Algebra System. MAGMA v., 16 – 5, (2010). http://magma.maths.usyd.edu.au/magma.

[Mil06] J.S. Milne, Elliptic Curves, BookSurge Publishers, (2006).

[Mil08] J.S. Milne, Abelian varieties, v. 2.0, 2008, www.jmilne.org.

[Mil20] J.S. Milne, Algebraic Number Theory, v. 3.08, 2020, www.jmilne.org.

[Mil22] J.S. Milne, Fields and Galois Theory, v. 5.10, 2022, www.jmilne.org.

[Mor22] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Camb. Phil. Soc. 21, 179 – 192, (1922).

[Mor96] P. Morandi, Field and Galois Theory, (1996).

[Mum84] D. Mumford, Tata lectures on Theta II. Birkhäuser, progress in mathematics, 43, (1984).

[Mul06] J. T. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC, Ann Arbor, MI, (2006). Thesis (Ph.D.)-The University of British Columbia (Canada).

[Mur93] V. Kumar Murty. Introduction to abelian varieties, volume 3 of CRM Monograph Series. American Mathematical Society, Providence, RI, (1993).

[Mül15] J. S. Müller, Rational points on Jacobians of hyperelliptic curves. Advances on Superelliptic Curves and their Applications, 41, 225 – 259, (2015).

[Nam79] M. Namba, Families of meromorphic functions on compact Riemann surfaces. Lecture Notes in Math. 767, Berlin : Springer-Verlag, (1979).

[Per95] D. Perrin, Geométrie algébrique, Une introduction, Savoirs actuels, InterEditions et CNRS Editions (1995).

[Poi01] H. Poincaré, Sur les propriétés arithmétiques des courbes algébriques, J. de Liouville 7, 161 – 233, (1901).

[Roh77] D. Rohrlich, Points at infinity on the Fermat curves. Invent. Math. 39, 95 – 127, (1977).

[Sal00a] O. Sall, Points algébriques de petits degré sur les courbes de Fermat, C. R. Acad. Sci. Paris, t.330, série I, 67 – 70, (2000).

[Sal00b] O. Sall, Points algébriques sur les courbes de Fermat. Thèse - l'Université Paris 7– Denis Diderot (Paris), (2000).

[Sal03] O. Sall, Points algébriques de degré au plus 10 sur la septique de Fermat, Afrika mathematika, 15, 49 – 55, (2003).

[Sch95] E. F. Schaefer, 2–descent on the Jacobians of hyperelliptic curves. J. Number Theory, 51, 219 – 232, (1995).

[Sch98] E. F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann. 310, 447 – 471, (1998).

[Ser90] J. P. Serre, Lectures on the Mordell- Weil Theorem. Vieweg, Braunschweig/Wiesbaden, (1990).

[Ser02] J. P. Serre, Galois cohomology, Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, (2002).

[SFC16] O. Sall, M. Fall and C. M. Coly, Points algbriques de degré donné sur la courbe d'équation affine $y^2 = x^5 + 1$, International Journal of Development Research. 06, 10295 – 10300, (2016).

[Sha94] I. R. Shafarevich, Basic algebraic geometry 1. Springer-Verlag, Berlin, second edition, (1994). Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[Sil86] J. H. Silverman, The arithmetic of elliptic curves, vol. 106 de Graduate Texts in Mathematics. Springer-Verlag, (1986).

[Sti93] H. Stichtenoth, Algebraic function fields and codes. Springer Universitext, Springer (1993).

[Sto98] M. Stoll, On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians. J. Reine Angew. Math. 501, 171 − 189, (1998).

[Sto01] M. Stoll, Implementing 2−descent for Jacobians of hyperelliptic curves, Acta Arith. 98, 245 − 277, (2001).

[Sto02] M. Stoll, On the arithmetic of the curves $y^2 = x^l + A$, II, J. Number Theory 93, 183 − 206, (2002).

[Sto14] M. Stoll, Arithmetic of hyperelliptic curves. Lecture notes, (2014). `http://www.mathe2.unibayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf`

[Sto15a] M. Stoll, Descent and covering collections. In Advances on superelliptic curves and their applications, volume 41 of NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., pages 176 − 193. IOS, Amsterdam, (2015).

[Sto15b] M. Stoll, Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank, J. Eur. Math. Soc., to appear. `arXiv:1307.1773v5`.

[Tow96] C. Towse, Weierstrass points on cyclic covers of the projective line. To appear in Trans. Amer. Math. Soc. (1996).

[Tze98] P. Tzermias, Algebraic points of low degree on the Fermat curve of degree seven, Manusc. Math. 97, 483 − 488, (1998).

[Vel71] J. Velu, Isogenies entre courbes elliptiques. Comptes de Rendus De Academie Des Sciences Paris, Serie I-Mathematique, Serie A., 273, 238 − 241, (1971).

[Voi02] C. Voisin, Théorie de Hodge et géométrie algébrique complexe, volume 10 de cours Spécialisés. Société Mathématique de France, Paris, (2002).

[Voj91] P. Vojta, Siegel's theorem in the compact case. Ann. of Math. 2, 133 , no. 3, 509 − 548, (1991).

[Wei29] A. Weil, L'arithmétique sur les courbes algébriques. Acta Math., 52, 281 − 315, (1929).

[Wei08] S. H. Weintraub, Galois Theory, Second Edition, (2008).

[ZS60] O. Zariski, P. Samuel, Commutative Algebra, Van Nostrand, Princeton, New Jersey, (1960).