UNIVERSITE ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES
Département de Mathématiques

Domaine : Sciences et Technologies
Mention : Mathématiques et Applications
Spécialité : Mathématiques pures
Option : Géométrie algébrique

THÈSE DE DOCTORAT

Présentée par : El Hadji SOW

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

Sujet : Points algébriques sur certaines courbes planes lisses

Sous la direction de : Professeur Oumar SALL

Devant le jury ci-après :

Nom et Prénom(s)	Grade	Qualité
SAMBOU Marie Salomon	Professeur titulaire (UASZ)	Président de jury
SALL Oumar	Professeur titulaire (UASZ)	Directeur de thèse
BARRY Mamadou	Professeur titulaire (UCAD)	Rapporteur
FALL Amadou Lamine	Professeur assimilé (UCAD)	Rapporteur
GUEDENON Amoussou Thomas	Professeur assimilé (UASZ)	Rapporteur
FALL Moussa	Maitre de conférences assimilé (UASZ)	Examinateur

Soutenue le 02 Juillet 2022 à l'Université Assane SECK de Ziguinchor

Remerciements

Avant tout, je rends grâce à DIEU de m'avoir donné encore une santé jusqu'à pouvoir continuer mes études jusqu'au doctorat.
J'adresse mes premiers et sincères remerciements à mon directeur de thèse le Professeur Oumar SALL. A travers sa très grande patience, sa disponibilité, et surtout ses conseils, il m' a offert sans compter la possibilité de profiter de sa grande expérience en matière de recherche, je lui en suis vivement et cordialement reconnaissant.
Je tiens à exprimer toute ma gratitude et mes remerciements aux professeurs Mamadou BARRY, Amadou Lamine FALL et Amoussou Thomas GUEDENON d'avoir accepté d' être rapporteurs et membres du jury de cette thèse, et de porter de l'intérêt et de la qualité à mon travail. Je suis honoré d'adresser mes remerciements aux professeurs Marie Salomon SAMBOU et Moussa FALL d'avoir accepté de faire parti des membres du jury.
Je remercie le Docteur Moussa FALL qui fut un collègue au Lycée EL Hadji Omar Lamine BADJI et un frère qui m'a beaucoup aidé du début jusqu'à la fin de mes recherches.
Je suis heureux de remercier tous les professeurs du département de mathématiques particulièrement aux professeurs Amoussou Thomas GUEDENON, Mamadou Eramane BODIAN, Daouda Niang DIATTA et Timack NGOM de m'avoir très bien accueilli et installé dans leurs bureaux à l'élevage durant mes deux dernières années de recherche.
Je remercie tous les membres du service pédagogique, en particulier Alioune Badara DIENG pour ses encouragements. Je remercie tous les membres de la scolarité en particulier à Omar DJIBA pour ses conseils et encouragements. Je tiens à remercier les doctorants GASSAMA, DIALLO, BALDE et particulièrement Pape Modou SARR mon binôme durant toutes mes trois années de recherche. Je remercie aussi le docteur Chérif Mamina COLY de m'avoir aidé dans mes recherches. Je tiens aussi à remercier tous les étudiants et tout le personnel de l'Université Assane Seck de Ziguinchor pour m'avoir ouvert toutes les portes.
Je remercie mes parents, mes tuteurs, mes frères et sœurs et mes amis. Je remercie de façon infinie ma femme Seynabou MBAYE avec toute sa famille ; et mes enfants Ousseynou, Allé, Ramatoulaye et Maodo.
Je remercie les Professeurs Cheikh MBacké DIOP, Masseye GAYE et tous leurs collègues de l'Université Cheikh Anta diop de Dakar par leurs soutiens moraux et pédagogiques.
Je remercie tous les inspecteurs d'académie de Ziguinchor et leurs personnels qui m'ont donné des autorisations d'inscription depuis 2012.
Je remercie infiniment le Proviseur Diakone DJIBA du Lyçée de Niaguis qui fut censeur au Lycée Djignabo.
Je remercie infiniment le Proviseur Mamadou BADJI et le Censeur Moussa MANE du Lycée EL hadji Omar Lamine BADJI. Je remercie mes collègues du CEM de Tendouck et de Mangangoulack, mes collègues du CEM T. Amilcar CABRAL, mes collègues du Bloc scientifique de Tété DIADHIOU, mes collègues du Lycée Djignabo BASSENE et ceux du Lycée EL hadji Omar Lamine BADJI.
Je remercie tous mes voisins des quartiers Boudody (hôpital silence), Corentas et Château d'eau de Ziguinchor. Je remercie tous mes élèves.
Enfin, je remercie toute la population de Ziguinchor en leur souhaitant la paix dans notre chère Casamance.

À mes parents
À ma femme Seynabou MBAYE
À mes enfants Ousseynou, Allé, Ramatoulaye, Maodo
À tous mes tuteurs
À tous ceux qui m'ont enseigné
À tous mes élèves

Points algébriques sur certaines courbes planes lisses

Résumé :
Notre thèse porte essentiellement sur la détermination des points algébriques sur certaines courbes planes lisses.
Tous nos travaux sont dans le cadre où la finitude du groupe de Mordell-Weil des points rationnels de la jacobienne est une condition indispensable.
La détermination de l'ensemble des points algébriques de degré donné est un problème qui intéresse certains mathématiciens dont : Booker et al, Siksek, Stoll, Hindry et Silveman.
En s'inspirant des travaux de ces mathématiciens, on a pu compléter et même parfois étendre les résultats qu'ils ont obtenus.
Les méthodes algébriques et géométriques mises en œuvre, ont permis de déterminer de manière explicite :
- l'ensemble des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur les d'équations courbes affines respectives $y^2 = 4x^5 + 1$, $y^2 = x^5 - 243$ et $y^2 = 3x(x^4 + 3)$,
- l'ensemble des points algébriques de petits degrés sur $\mathbb{Q}$ sur les courbes d'équations affines respectives $y^2 = x^5 + 20736$ et $y^2 + y = x^5$,
- l'ensemble des points algébriques de degré quelconque sur Q sur les courbes d'équations affines respectives $y^2 = x(x^2 + 1)(x^2 + 3)$ et $y^2 = 3(x^5 - 1)$.

Mots-clés : Groupe de Mordell-Weil, jacobienne d'une courbe, conjugués de Galois, points algébriques.

Table des matières

Introduction

La géométrie algébrique s'intéresse à l'étude des ensembles définis par l'annulation d'un ou plusieurs polynômes. De tels ensembles sont appelés ensembles algébriques.
Parmi les chefs de file de cette branche des mathématiques, on peut citer d'abord Descartes qui a inauguré l'étude des courbes algébriques par les méthodes de la géométrie analytique. Ensuite après les années 1930, certains mathématiciens comme Weil, Zariski ont participé largement au développement de la géométrie algébrique et d'autres algébristes comme Jean-Pierre Serre, Pierre Samuel l'ont considérablement impulsée.
Dans cette thèse, l'étude portera sur un cas particulier de variétés algébriques : les variétés affines et les variétés projectives.
Étant donnée $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K, on note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Nos principaux résultats concernent la détermination des points algébriques de degrés donnés d sur certaines courbes algébriques.
Le degré d'un point algébrique est le degré de son corps de définition sur $\mathbb{Q}$.
C'est dans ce cadre qu'on a pu compléter ou étendre les travaux de certains mathématiciens dont : Booker, Sijsling, Sutherland, Voight et Yasak dans [1] qui ont déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 4x^5 + 1$, ensuite ceux de Mulholland dans [13] qui a déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^5 - 243$ et aussi ceux de Bruin dans [2] qui a déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 3x(x^4 + 3)$.
On a aussi étendu les travaux de Siksek et Stoll dans [20] qui ont donné l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 = x^5 + 20736$ et des travaux de Siksek dans [18] et dans [19] qui a donné respectivement l'ensemble des points $\mathbb{Q}$-rationnels sur les courbes d'équations affines $y^2 = x(x^2 + 1)(x^2 + 3)$ et $y^2 = 3(x^5 - 1)$, mais aussi des travaux de Hindry et Silverman dans [9] qui ont décrit l'ensemble des points algébriques de degré 1 sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 + y = x^5$.
La thèse comprend quatre chapitres structurés de la manière suivante :
Le chapitre 1 intitulé "notions préliminaires" rassemble quelques formules, définitions et théorèmes utiles, et introduit des notions classiques de géométrie algébrique que nous utiliserons dans la suite.
Au chapitre 2 intitulé "courbes elliptiques, courbes hyperelliptiques" on parlera de quelques définitions et propriétés de base concernant ces deux types de courbes algébriques particulières.
Le chapitre 3 intitulé "points algébriques de degrés au plus 5 sur $\mathbb{Q}$ sur certaines courbes",

comprend trois parties :
- La première partie concerne la courbe d'équation affine $y^2 = 4x^5 + 1$.
Cette partie étend les résultats obtenus par Booker, Sijsling, Sutherland, Voight et Yasak qui avaient décrit dans [1] l'ensemble des points algébriques de degré 1 sur $\mathbb{Q}$ sur la courbe étudiée.
Notre résultat principal est donné par le théorème suivant :

Théorème :
L'ensemble des points algébriques de degré au plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 4x^5 + 1$ est composé de :

1. L'ensemble des points quadratiques sur $\mathcal{C}$ donné par
$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{4\alpha^5 + 1}\right),\ \alpha \in \mathbb{Q}^* \right\}$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ donné par
$$\mathcal{C}' = \left\{ (x, \pm 1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_3(x) = 4x^3 - \alpha^2 x^2 \pm 2\alpha^2 \right\}$$
3. L'ensemble des points quartiques sur $\mathcal{C}$ donné par $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ avec
$$\mathcal{C}_0 = \left\{ \left(x, \pm\sqrt{4x^5 + 1}\right) \mid x \in \overline{\mathbb{Q}},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$
$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x + \beta)) \ \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_1(x) = 4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 - (2\alpha + \alpha^2\beta^2)x - 2\alpha\beta \end{array} \right\}$$
$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, -1 - \alpha x^2\,(x + \beta)) \ \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_2(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 + 2\alpha x + 2\alpha\beta \end{array} \right\}$$
.
$$\mathcal{C}_3 = \left\{ \begin{array}{l} (x, 1 - \alpha x^2\,(x + \beta)) \ \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_3(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 - 2\alpha x - 2\alpha\beta \end{array} \right\}$$
.
$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x + \beta)) \ \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_4(x) = 4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 + (2\alpha + \alpha^2\beta^2)x + 2\alpha\beta \end{array} \right\}$$
.
4. L'ensemble des points quintiques sur $\mathcal{C}$ donné par $\mathcal{D}_0 \cup \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4$ avec
$$\mathcal{D}_0 = \left\{ \begin{array}{l} (x, \alpha + \lambda x(x + \mu) \ \mid \alpha, \mu, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_0(x) = 4x^5 - (\alpha + \lambda x(x + \mu))^2 + 1 \end{array} \right\}$$
$$\mathcal{D}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x^2 + \beta x + \gamma)) \ \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_1(x) = \alpha^2 x\,(x^2 + \beta x + \gamma)^2 - 4x^4 + 2\alpha\,(x^2 + \beta x + \gamma) \end{array} \right\}$$

$$\mathcal{D}_2 = \left\{ \begin{array}{l} \left(x, 1 - \dfrac{\alpha}{x+\beta}x^2\right) \mid \alpha, \beta \in \mathbb{Q} \text{ et } x \text{ racine} \in \overline{\mathbb{Q}} \text{ de} \\ \\ \mathcal{F}_2(x) = 4x^3(x+\beta)^2 - \alpha^2 x^2(x+\gamma)^2 - 2\alpha(x+\gamma)(x+\beta) \end{array} \right\}.$$

$$\mathcal{D}_3 = \left\{ \begin{array}{l} \left(x, 1 - \dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_3(x) = 4x^3(x+\beta)^2 - \alpha^2 x^2(x+\gamma)^2 + 2\alpha(x+\gamma)(x+\beta) \end{array} \right\}$$

$$\mathcal{D}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x^2+\beta x+\gamma)) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_4(x) = \alpha^2 x\left(x^2+\beta x+\gamma\right)^2 - 4x^4 - 2\alpha\left(x^2+\beta x+\gamma\right) \end{array} \right\}$$

Ce résultat est publié dans SCIREA Journal of Mathematics.

- La deuxième partie traite la courbe d'équation affine $y^2 = x^5 - 243$.
Dans cette partie nous étendons les travaux de Mulholland qui avait donné dans [13] une description des points algébriques de degré 1 sur $\mathbb{Q}$ sur la courbe étudiée.
Notre résultat principal est donné par le théorème suivant :

Théorème :
L'ensemble des points algébriques de degré au plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^5 - 243$ est composé de :

1. L'ensemble des points quadratiques sur $\mathcal{C}$ donné par
$$\mathcal{S} = \left\{\left(\alpha, \pm\sqrt{\alpha^5 - 243}\right),\ \alpha \in \mathbb{Q}\right\}$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ qui est vide.
3. L'ensemble des points quartiques sur $\mathcal{C}$ donné par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec
$$\mathcal{C}_1 = \left\{\left(x, \pm\sqrt{\alpha^5 - 243}\right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\right\}$$
$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+3))^2 \end{array} \right\}$$
4. L'ensemble des points quintiques sur $\mathcal{C}$ donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec
$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\}$$
$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)[n_1 + n_2(x+3) + n_3(x^2+3x+9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ C(x) = (x-3)(n_1 + n_2(x+3) + n_3(x^2+3x+9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

Ce résultat est publié Asian Research Journal of Mathematics.

- Dans la troisième partie, nous déterminons de manière explicite l'ensemble algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = 3x(x^4+3)$. Ce travail complète et étend le résultat obtenu par Bruin qui avait décrit dans [2] l'ensemble des points $\mathbb{Q}$-rationnels sur cette même courbe.
Le théorème de notre résultat principal s'énonce suit :

Théorème :
L'ensemble des points algébriques de degré au plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 3x(x^4+3)$ est composé de :

1. L'ensemble des points quadratiques sur $\mathcal{C}$ donné par
$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{3\alpha(\alpha^4+3}\right),\ \alpha \in \mathbb{Q}^* \right\}$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ qui est vide.
3. L'ensemble des points quartiques sur $\mathcal{C}$ donné par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec
$$\mathcal{C}_1 = \left\{ \left(x, \pm\sqrt{3\alpha(\alpha^4+3}\right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x):\mathbb{Q}] = 2 \right\}$$
$$\mathcal{C}_2 = \left\{ (x, x(\lambda_1 + \lambda_2 x)\ \mid \lambda_1, \lambda_2 \in \mathbb{Q}^\star, x \textit{ racine de } \mathcal{F}(x) = 3(x^4+3) - x\left(\lambda_1 + \lambda_2 x\right)^2 \right\}$$
4. L'ensemble des points quintiques sur $\mathcal{C}$ donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec
$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{G}(x) = (\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 - 3x(x^4+3) \end{array} \right\}$$
$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, n_1 x + n_2 x^2 + n_3 x^3) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{H}(x) = x(n_1 + n_2 x + n_3 x^2)^2 - 3(x^4+3) \end{array} \right\}$$

Ce résultat est publié dans International Journal Of Development Research.

Le chapitre 4 intitulé "paramétrisation des points algébriques sur certaines courbes", est divisé en quatre parties parties :
- Dans la première partie consacrée à la courbe d'équation affine $y^2 = x^5 + 20736$, nous donnons une généralisation du résultat obtenu par Siksek et Stoll qui avaient décrit dans [20] l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe étudiée.
Notre résultat principal est donné par le théorème suivant :

Théorème :
L'ensemble des points algébriques de degré au plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^5 + 20736$ est composé de :

1. L'ensemble des points quadratiques sur $\mathcal{C}$ donné par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. L'ensemble des points cubiques sur $\mathcal{C}$ donné par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -144 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_1(x) = x^3 - \alpha^2 x^2 - 288\alpha \right\}$$

$$\mathcal{B} = \left\{ (x, -144 - \alpha x^3) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_2(x) = \alpha^2 x^3 - x^2 + 288\alpha \right\}$$

Ce résultat est publié dans EPH-International Journal of Mathematics and Statistics.

- Dans la deuxième partie aussi, nous étendons le résultat obtenu par Hindry et Silverman qui avaient décrit dans [9] l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 + y = x^5$.
Le théorème de notre résultat principal s'énonce comme suit :

Théorème :
L'ensemble des points algébriques de degré au plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 + y = x^5$ est composé de :

1. L'ensemble des points quadratiques sur $\mathcal{C}$ donné par

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. L'ensemble des points cubiques sur $\mathcal{C}$ donné par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\},$$

$$\mathcal{B} = \left\{ (x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_2(x) = x^3 - \alpha^2 x^2 - \alpha \right\}.$$

Ce résultat est soumis pour publication.

- Dans la troisième partie, nous donnons une généralisation du résultat obtenu par Siksek qui avait donné dans [18] l'ensemble des points algébriques de degré 1 sur $\mathbb{Q}$ sur la courbe d'équations affine d'équation affine $y^2 = x(x^2 + 1)(x^2 + 3)$ par le théorème suivant :

Théorème :
L'ensemble des points algébriques de degré au plus d quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x^2 + 1)(x^2 + 3)$ est donné par :

$$\bigcup_{[K:\mathbb{Q}] \leq d} \mathcal{C}(K) = \mathcal{H}_0 \cup \mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3 \text{ où}$$

$$\mathcal{H}_0 = \left\{ \begin{pmatrix} x, -\dfrac{\sum\limits_{r\leq\frac{k}{2}} a_r x^r}{\sum\limits_{s\leq\frac{k-5}{2}} b_s x^s} \end{pmatrix} \mid a_r, b_s \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\},$$

$$\mathcal{H}_1 = \left\{ \begin{array}{l} \begin{pmatrix} x, -\dfrac{\sum\limits_{r\leq\frac{k+2}{2}} a_r x^r}{\sum\limits_{s\leq\frac{k-3}{2}} b_s x^s} \end{pmatrix} \mid a_r, b_s \in \mathbb{Q} \text{ satisfaisant} \\ \\ \sum_{r\leq\frac{k+2}{2}} a_r (i)^r = 0 \quad , \quad \sum_{r\leq\frac{k+2}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (\mathcal{E}_2) \end{array} \right\},$$

$$\mathcal{H}_2 = \left\{ \begin{array}{l} \begin{pmatrix} x, -\dfrac{\sum\limits_{1\ \leq\ r\ \leq\frac{k+1}{2}} a_r x^r}{\sum\limits_{s\leq\frac{k-4}{2}} b_s x^s} \end{pmatrix} \mid a_r, b_s \in \mathbb{Q} \text{ satisfaisant } a_0 = 0, \\ \\ \text{et } x \text{ racine de l'équation } (E_1) \end{array} \right\},$$

$$\mathcal{H}_3 = \left\{ \begin{array}{l} \begin{pmatrix} x, -\dfrac{\sum\limits_{1\ \leq\ r\ \leq\frac{k+3}{2}} a_r x^r}{\sum\limits_{s\leq\frac{k-2}{2}} b_s x^s} \end{pmatrix} \mid a_r, b_s \in \mathbb{Q} \text{ vérifiant } a_0 = 0, \\ \\ \sum_{1\ \leq\ r\ \leq\frac{k+3}{2}} a_r (i)^r = 0 \quad , \quad \sum_{1\ \leq\ r\ \leq\frac{k+3}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (E_3) \end{array} \right\}.$$

On désigne par $(\mathcal{E}_l)$ et (E_t) les équations respectives suivantes :

$$(\mathcal{E}_l) : \left(\sum_{r\leq\frac{k+l}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s\leq\frac{k-5+l}{2}} b_s x^s \right)^2,$$

$$(E_t) : \left(\sum_{1\ \leq\ r\ \leq\frac{k+t}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s\leq\frac{k-5+t}{2}} b_s x^s \right)^2.$$

- Dans la quatrième partie, nous étendons aussi le résultat obtenu par Siksek qui avait donné dans [19] l'ensemble des points algébriques de degré 1 sur $\mathbb{Q}$ sur la courbe d'équations affine d'équation affine $y^2 = 3(x^5 - 1)$ par le théorème suivant :
Notre résultat principal est donné par le théorème suivant :

Théorème :
L'ensemble des points algébriques de degré au plus d quelconque sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = 3(x^5 - 1)$ est donné par :

$$\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K) = \mathcal{F}_0 \cup \mathcal{F}_1$$

avec

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum_{i\leq \frac{n}{2}} a_i x^i}{\sum_{j\leq \frac{n-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}$$

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i\leq \frac{n+1}{2}} a_i x^i}{\sum_{j\leq \frac{n-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ vérifiant } \sum_{i\leq \frac{n+1}{2}} a_i = 0 \text{ et } x \text{ racine de l'équation } (\mathcal{E}_1) \right\}$$

où :

$$(\mathcal{E}_0) : \left(\sum_{i\leq \frac{l}{2}} a_i x^i \right)^2 = 3 \left(\sum_{j\leq \frac{n-5}{2}} b_j x^j \right)^2 (x^5 - 1) \ ;$$

$$(\mathcal{E}_1) : \left(\sum_{i\leq \frac{n+1}{2}} a_i x^i \right)^2 = 3 \left(\sum_{j\leq \frac{n-4}{2}} b_j x^j \right)^2 (x^5 - 1)$$

Ce résultat est publié dans International Journal of Mathematics and Statistics Invention.

Chapitre 1

Notions préliminaires

Dans ce chapitre nous introduisons les notions basiques jugées nécessaires dans la suite. Des définitions et des résultats supposés classiques constitueront ces notions de bases.

1.1 Notions d'algèbre commutative

1.1.1 Extensions de corps

On rappelle sans démonstrations quelques définitions et résultats de base sur les extensions de corps, qui serviront à de multiples reprises dans la suite.

Définition 1. Soient K et E deux corps.
On dit que E est une extension de K et l'on note $K \subset E$ si K est un sous corps de E.

Soit $\alpha \in E$; on désigne par :
· $K[\alpha]$ le sous-anneau de E engendré par $K \cup \{\alpha\}$, c'est-à-dire

$$K[\alpha] = \{x \in E \mid x = P(\alpha), avec\ P \in K[X]\}.$$

· $K(\alpha)$ le sous-corps de E engendré par $K \cup \{\alpha\}$, c'est-à-dire

$$K(\alpha) = \{x \in E \mid x = \frac{P(\alpha)}{Q(\alpha)}, avec\ P \in K[X], Q \in K[X], Q(\alpha) \neq 0\}.$$

Définition 2. Une extension $K \subset E$ est dite simple s'il existe $\alpha \in E$ tel que $E = K(\alpha)$.

Exemple 1. *(1) $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$.*

(2) $\mathbb{R}$ est une extension de $\mathbb{Q}\left[\sqrt{2}\right]$.

(3) $\mathbb{Q}\left[\sqrt{2}\right]$ est une extension de $\mathbb{Q}$.

(4) Le corps $K(X)$ des fractions rationnelles à une indéterminée sur le corps K est une extension de K.

(5) $\mathbb{C}$ est une extension simple de $\mathbb{R}$ car $\mathbb{C} = \mathbb{R}(i)$.

(6) $K(X)$ est une extension simple de K.

Définition 3. (équation polynômiale)
On appelle équation polynomiale sur K toute équation de la forme $P(x) = 0$, avec $P \in K[X]$. Le degré de cette équation est le degré de P.

Définition 4. (corps de rupture)
Une extension $K \subset E$ est appelée corps de rupture pour le polynôme $P \in K[X]$ si E contient un zéro de P.

Exemple 2. *$\mathbb{R}$ est un corps de rupture pour le polynôme $X^3 - 2$ sur $\mathbb{Q}$.*

Définition 5. (corps de décomposition)
Une extension $K \subset E$ est un corps de décomposition sur K pour le polynôme $P \in K[X]$ si, P peut être scindé dans $E[X]$ ie peut être décomposé en produit de polynômes linéaires dans $E[X]$.

Exemple 3. *$\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme $X^2 + 2$.*

1.1.2 Points algébriques

Définition 6. (élément algébrique, élément transcendant)
Soient A un anneau commutatif et B une A-algèbre.
On dit que $b \in B$ est algébrique sur A s'il existe un polynôme non nul $P \in A[X]$ tel que $P(b) = 0$. Un élément non algébrique est appelé élément transcendant.

Exemple 4. *Le corps $\bar{\mathbb{Q}}$ des nombres $z \in \mathbb{C}$ algébriques sur $\mathbb{Q}$ s'appelle corps des nombres algébriques.*

Définition 7. (clôture algébrique)
Soient K un corps et B une K-algèbre intègre.
L'ensemble des éléments de B qui sont algébriques sur K est un corps contenu dans B. On l'appelle clôture algébrique de K dans B.

Définition 8. (extension algébrique)
On dit qu'une extension de corps $K \subset L$ est algébrique si tout élément de L est algébrique sur K.

Définition 9. (extension finie, degré d'une extension finie)
On dit qu'une extension de corps $K \subset L$ est finie si L est un K-espace vectoriel de dimension finie. On appelle degré de L sur K, et l'on note $[L : K]$, la dimension de L en tant que K-espace vectoriel.

Proposition 1. *Soit K un corps. Les assertions suivantes sont équivalentes.*

(1) Tout polynôme non constant de $K[X]$ est scindé dans $K[X]$, c'est-à-dire qu'il se décompose comme produit de polynômes de degré 1 de $K[X]$,

(2) Tout polynôme irréductible de $K[X]$ est de degré 1, ie les éléments irréductibles de $K[X]$ sont les $X - a, a \in K$,

(3) Si une extension $K \subset E$ est algébrique alors $E = K$,

(4) Tout polynôme non constant de $K[X]$ admet au moins une racine dans K.

Définition 10. (corps algébriquement clos)
Un corps K satisfaisant une des conditions équivalentes de la proposition précédente est dit algébriquement clos.

Exemple 5. $\mathbb{Q}$ *et* $\mathbb{R}$ *ne sont pas algébriquement clos car* $X^2 + 2$ *n'a pas de racine dans* $\mathbb{Q}$ *ou* $\mathbb{R}$.

Définition 11. (clôture algébrique)
Soit K un corps. Une clôture algébrique $\bar{K}$ de K est une extension algébrique $K \subset \bar{K}$ telle que $\bar{K}$ est algébriquement clos.

Exemple 6. $\mathbb{C}$ *est la clôture algébrique de* $\mathbb{R}$.

Définition 12. (polynôme minimal)
Soient K un corps et B une K-algèbre intègre. Soit $b \in B$ un élément algébrique.
L'ensemble $\{P \in K[X] \mid P(b) = 0\}$ est un idéal premier de $K[X]$. Le polynôme minimal de b en est l'unique générateur unitaire. On remarquera que le polynôme minimal de b est le polynôme unitaire P de plus petit degré tel que $P(b) = 0$; c'est aussi un polynôme irréductible.

1.1.3 Théorie de Galois des extensions finies

Toutes les extensions considérées dans la suite de ce paragraphe seront supposées finies.

Proposition 2. *Soit* K *un corps. Les assertions suivantes sont équivalentes.*

(1) Chaque fois que E est un corps de rupture pour un polynôme irréductible $P \in K[X]$ sur K, il est un corps de décomposition pour P sur K,

(2) Chaque fois qu'un polynôme irréductible $P \in K[X]$ posssède une racine dans E, alors il posssède toutes ses racines dans E,

(3) Chaque fois qu'un polynôme irréductible $P \in K[X]$ posssède une racine dans E, alors il se décompose en produit de polynômes linéaires dans $E[X]$.

Définition 13. (extension normale)
Une extension algébrique $K \subset E$ satisfaisant une des conditions équivalentes de la proposition précédente est dit normale.

Exemple 7. *(1)* $\mathbb{C}$ *est une extension normale de* $\mathbb{R}$ *car* $\mathbb{C}$ *est un corps de décomposition de* $X^2 + 1$ *sur* $\mathbb{R}$.

(2) L'extension $E = \mathbb{Q}(\sqrt[3]{2})$ *de* $\mathbb{Q}$ *n'est pas normale car le polynôme* $X^3 - 2 \in \mathbb{Q}[X]$ *posssède une racine dans* E *mais pas toutes.*

Définition 14. (clôture normale)
Soit une extension $K \subset E$. Une cl*ôture* normale de E est une extension normale $K \subset N$ qui satisfait les conditions suivantes :
(i) $K \subset E \subset N$
(ii) Si $K \subset M$ est une extension normale vérifiant $K \subset E \subset M \subset N$, alors $M = N$.

Exemple 8. $\mathbb{C}$ *est une clôture normale de l'extension* $\mathbb{Q} \subset \mathbb{R}$.

Définition 15. (K-isomorphisme)
Soit K un corps, $K \subset E$ et $K \subset F$ deux extensions du *même* corps K. On appelle K-isomorphisme de E dans F tout isomorphisme $\sigma : E \to F$ laissant fixe tout élément de K ie $\sigma(k) = k$ pour tout $k \in K$.

Exemple 9. *Soit* $\bar{z}$ *le conjugué de* z *dans* $\mathbb{C}$. *L'application* $\sigma : \mathbb{C} \to \mathbb{C}$ *définie par* $\sigma(z) = \bar{z}$ *est un* $\mathbb{R}$*-isomorphisme de* $\mathbb{C}$ *dans* $\mathbb{C}$.

Toutes les extensions considérées dans la suite de ce paragraphe seront supposées finies.

Définition 16. (degré galoisien)
On appelle degré galoisien d'une extension $K \subset E$, et l'on note $\overline{[E : K]}$, le cardinal de l'ensemble des K-isomorphismes de E dans une cl*ôture* normale de E. La définition du degré galoisien ne dépend pas du choix de la cl*ôture* normale de E.

Théorème 17. *Si* $E = K(a)$, *alors* $\overline{[E : K]}$ *est le nombre de racines distinctes de* $Irr(a, K)$ *polynôme minimal de* a *sur* K.

Preuve : Soient N une cl*ôture* normale de E, H l'ensemble de tous les K-isomorphismes de E dans N et A l'ensemble des racines distinctes de $Irr(a, K)$ dans N. L'application $H \to A$ qui associe σ à $\sigma(a)$ est bijective, d'où $\overline{[E : K]} = card(I) = card(A)$

Exemple 10. $\overline{[\mathbb{C} : \mathbb{R}]} = 2$.

Définition 18. (extension séparable, élément séparable)
Une extension $K \subset E$ est dite séparable si, $\overline{[E : K]} = [E : K]$.
Un élément $a \in E$ est séparable sur K si, toutes les racines de $Irr(a, K)$ sont simples.

Exemple 11. $\mathbb{C}$ *est une extension séparable de* $\mathbb{R}$.
Le nombre complexe i *est séparable sur* $\mathbb{R}$. $\sqrt{3}$ *est séparable sur* $\mathbb{Q}$.

Théorème 19. *Une extension* $E = K(a)$ *est séparable, si et seulement si,* a *est séparable sur* K.

Preuve : Soit $[E : K] = n = deg(Irr(a, K))$. Nous avons les équivalences suivantes :
$[E$ *est séparable sur* $K] \Leftrightarrow [\overline{[E : K]} = [E : K]]$
$\Leftrightarrow [Irr(a, K)$ posssède n racines distinctes$]$
$\Leftrightarrow [$*toute racine de* $Irr(a, K)$ est simple $]$
$\Leftrightarrow [a$ *est séparable sur* $K]$.

Définition 20. (groupe de Galois)
Soit E une extension normale finie d'un corps K. Le groupe de Galois de l'extension E de K noté $G(E/K)$ est l'ensemble des K-automorphismes de E formant un groupe pour la composition des applications.

Exemple 12. $\mathbb{C}$ *est une extension normale finie de* $\mathbb{R}$. $G(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \rho\}$ *où* ρ *est le* $\mathbb{R}$*-automorphisme qui associe à chaque nombre complexe* z *son conjugué* $\bar{z}$.

Théorème 21. *Le groupe de Galois $G(E/K)$ est fini, et son ordre est le degré galoisien $\overline{[E:K]}$.*

Peuve : Le groupe de Galois $G(E/K)$ est l'ensemble H de tous les K-isomorphismes de E dans une cl*ôture* normale de E. En effet, E est sa propre cl*ôture* normale car elle est une extension normale de K, donc on a $G(E/K) = H$, par suite on a l'ordre de $G(E/K)$ est le degré galoisis $\overline{[E:K]}$.

Corollaire 1. $Ord(G(E/K)) \leq [E:K]$.

Définition 22. (conjugués d'un élément, conjugués de Galois)
Soient $K \subset E$ et $x \in E$ algébrique sur K de polyn*ôme* minimal $irr(x, K)$ à coefficients dans K. Les conjugués de x sont zéros de $irr(x, K)$ dans E. Les conjugués de x qui sont laissés fixes sous l'action de Galois (c'est-à-dire qui sont laissés fixes par les K-automorphismes de E) sont appelés les conjugués de Galois de x.

Définition 23. (extension galoisienne)
Soit $K \subset E$ une extension finie d'un corps K. L'extension $K \subset E$ est dite galoisienne si elle est une extension normale et séparable.

Exemple 13. $\mathbb{R} \subset \mathbb{C}$ *est une extension galoisienne.*

1.2 Courbes algébriques

On appelle plan affine sur un corps K l'ensemble $\mathbb{A}^2$ et plan projectif sur K l'ensemble $\mathbb{P}^2$. Nous noterons par (x, y) un élément de $\mathbb{A}^2$ et par (x, y, z) un élément de $\mathbb{P}^2$.

1.2.1 Variété affine

Définition 24. (espace affine)
On appelle espace affine de dimension n sur K, et on note $\mathbb{A}^n(K)$, ou encore $\mathbb{A}^n$ s'il n'y a pas de risque de confusion sur K, l'ensemble K^n produit cartésien itéré n fois du corps K. Les éléments de $\mathbb{A}^n(K)$ sont appelés points.
L'espace affine de dimension 1 est appelé droite affine.
L'espace affine de dimension 2 est appelé plan affine.

Définition 25. (zéro d'un polynôme)
Un point a de $\mathbb{A}^n$ est dit zéro de $f \in K[X_1, ..., X_n]$ si $f(a) = 0$.

Définition 26. (ensemble algébrique affine)
Soit $S \subset K[X_1, ..., X_n]$ un ensemble de polynômes à n variables. L'ensemble

$$\mathcal{V}(S) = \{a \in \mathbb{A}^n(K) \mid \forall\ f \in S,\ f(a) = 0\}. \tag{1.1}$$

est le sous-ensemble de $\mathbb{A}^n$ formé des zéros communs à tous les éléments de S.
On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S. Si $S = \{f\}$ est un singleton, nous noterons $\mathcal{V}(f)$ au lieu de $\mathcal{V}(\{f\})$.

Une partie V de $\mathbb{A}^n(K)$ est un ensemble algébrique affine s'il existe $S \subset K[X_1, ..., X_n]$ tel que $V = \mathcal{V}(S)$.

Exemple 14. *Le vide et l'espace tout entier sont des ensembles algébriques affines.*

En effet :
Etant donné que le polynôme constant 1 ne s'annule jamais , on a $\mathcal{V}(1) = \emptyset$.
De même que, le polynôme constant 0 est identiquement nul, on a $\mathcal{V}(0) = \mathbb{A}^n$.

Définition 27. (hypersurface, hyperplan)
On appelle hypersurface définie par $f \in K[X_1, ..., X_n]$, l'ensemble des zéros de f (pour f non constant et K algébriquement clos) et l'on note $\mathcal{V}(f)$.
Un hyperplan est une hypersurface définie par f de degré 1.
Une droite est un hyperplan de $\mathbb{A}^2$.

Définition 28. (courbe affine plane)
On appelle courbe algébrique plane un ensemble des points de $\mathbb{A}^2$ dont les coordonnées (x, y) satisfont l'équation

$$f(x, y) = 0 \tag{1.2}$$

pour un polynôme $f \in K[X, Y]$. Une telle courbe est appelée courbe affine plane.

Voilà une définition équivalente à la précédente :

Définition 29. (courbe affine plane)
Une courbe affine plane est une hypersurface du plan affine.

Nous noterons $\mathcal{C}_f \subset \mathbb{A}^2$ la courbe affine plane définie par f.
Le degré d'une courbe est le degré d'un polynôme qui la définit (*i.e* $deg(\mathcal{C}_f) = deg(f)$).

Exemple 15. *(de courbes affines planes)*

- Une droite affine L est une courbe affine plane d'équation $ax + by + c = 0$.

- Une conique ou quadrique affine est une courbe affine $\mathcal{C}$ d'équation $f(x, y) = 0$, où f est un polynôme de degré 2 :

$$f(x, y) = \sum_{0 \leq i,\, j,\, i+j \leq 2} a_{i,j} x^i y^j;$$

- Une cubique affine est une courbe affine $\mathcal{C}$ d'équation $f(x, y) = 0$, où f est un polynôme de degré 3 :

$$f(x, y) = \sum_{0 \leq i,\, j,\, i+j \leq 3} a_{i,j} x^i y^j;$$

- Une quartique affine est une courbe affine $\mathcal{C}$ d'équation $f(x, y) = 0$, où f est un polynôme de degré 4 :

$$f(x, y) = \sum_{0 \leq i,\, j,\, i+j \leq 4} a_{i,j} x^i y^j;$$

  où les coefficients $a_{i,j}$ sont dans K.

– Une quintique affine est une courbe affine $\mathcal{C}$ d'équation $f(x,y) = 0$, où f est un polynôme de degré 5 :

$$f(x,y) = \sum_{0 \leq i,\, j,\, i+j \leq 5} a_{i,j} x^i y^j;$$

où les coefficients $a_{i,j}$ sont dans K.

Définition 30. (point singulier, point lisse, courbe lisse)
Un point $P = (a,b)$ d'une courbe $\mathcal{C} : f(x,y) = 0$ est dit singulier si :

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

Un point $P = (a,b)$ d'une courbe $\mathcal{C} : f(x,y) = 0$ est dit lisse si :

$$\left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right) \neq (0,0).$$

La tangente en un point lisse $P = (a,b)$ à $\mathcal{C}$ est la droite d'équation :

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

Une courbe $\mathcal{C}$ dont tous les points sont lisses est dite lisse.

Définition 31. (point ordinaire, point d'inflexion, nœud, point de rebroussement)
Soient C une courbe algébrique et $P = (x,y)$ un point de C.

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

Avec les ensembles algébriques affines, nous introduisons une topologie particulière appelée la topologie de Zariski.

Définition 32. (topologie de Zariski)
On appelle topologie de Zariski sur l'espace affine $\mathbb{A}^n$, la topologie dont les ensembles algébriques sont les fermés.

Cette topologie satisfait les trois axiomes suivants :
– l'intersection quelconque de fermés est un fermé.
– la réunion finie de fermés est un fermé.
– l'ensemble vide et l'espace affine sont les seuls ensembles ouverts et fermés à la fois.

Définition 33. (sous-ensemble irréductible)
Un sous-ensemble E' d'un espace topologique E est irréductible s'il n'est pas la réunion de deux sous-ensembles fermés non vides disjoints de E.

Définition 34. (variété affine)
Une variété affine est un sous-ensemble irréductible fermé de l'espace affine $\mathbb{A}^n$, pour la topologie de Zariski.

1.2.2 Variété projective

Considérons la relation d'équivalence $\sim$ sur $K^{n+1}\setminus\{0\}$ définie par : pour tous vecteurs x et y dans $K^{n+1}\setminus\{0\}$, on a

$$x \sim y \text{ si et seulement s'il existe } \lambda \in K\setminus\{0\} \text{ tel que } x = \lambda y.$$

Définition 35. (espace projectif)
On appelle espace projectif de dimension n sur K et l'on note $\mathbb{P}^n$ (ou $\mathbb{P}^n(K)$ ou encore $\mathbb{P}(K^{n+1})$), l'ensemble-quotient

$$(K^{n+1}\setminus\{0\})/\sim$$

En d'autres termes, $\mathbb{P}^n$ est l'ensemble des droites vectorielles de K^{n+1}.

Si un point $P \in \mathbb{P}^n$ a pour vecteur directeur (représentant) $(x_0, x_1, ..., x_n) \in K^{n+1}\setminus\{0\}$, on écrit $P = (x_0 : x_1 : ... : x_n)$ la classe de $(x_0, x_1, ..., x_n)$; on dit que $(x_0 : x_1 : ... : x_n)$ est un système de coordonnées homogènes de P et ils ne sont définis qu'à multiplication par un scalaire non nul près .
On dit que $\mathbb{P}^1$ est la droite projective sur K, et que $\mathbb{P}^2$ est le plan projectif sur K.

Définition 36. (polynôme homogène)
Un polynôme $F \in K[X_0, ..., X_n]$ est dit homogène de degré d si pour tout $(x_0, ..., x_n) \in K^{n+1}$ on a

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

pour tout $\lambda \in K^\star$.

Définition 37. (ensemble algébrique projectif)
Soit $S \subset K[X_0, ..., X_n]$ un ensemble de polynômes homogènes à $n+1$ variables. L'ensemble

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

est le lieu des zéros de S dans $\mathbb{P}^n$. On dit que $\mathcal{V}_p(S)$ est l'ensemble algébrique projectif défini par S.

Définition 38. (hypersurface, hyperplan, variété algébrique projective)
Une partie V de $\mathbb{P}^n$ est un ensemble algébrique projectif s'il existe $S \subset K[X_0, ..., X_n]$ tel que $V = \mathcal{V}_p(S)$. C'est une hypersurface s'il existe $F \in K[X_0, ..., X_n]$ homogène non constant (et K algébriquement clos) tel que $V = \mathcal{V}_p(F)$.
Un hyperplan est une hypersurface définie par un polynôme homogène de degré 1.
On appelle variété algébrique projective, tout ensemble algébrique projectif et irréductible.

Définition 39. (courbe projective plane, conique, cubique, quartique, ...)
Une courbe projective plane est une hypersurface de $\mathbb{P}^2$.
Une courbe projective plane est dite conique, cubique, quartique, ... si son degré est respectivement 2, 3, 4, ...

Nous notons $\mathcal{C}_F \subset \mathbb{P}^2$ la courbe définie par F. Le degré d'une courbe est le degré d'un polynôme homogène qui la définie ($i.e\ deg(\mathcal{C}_F) = deg(F)$).

Définition 40. (ensemble des points K-rationnels, point K-rationnel)
Soit $\mathcal{C}_F$ une courbe projective plane définie par un polynôme homogène $F \in K[X,Y,Z]$. L'ensemble des points K-rationnels de $\mathcal{C}_F$ est

$$\mathcal{C}_F(K) = \left\{(x,y,z) \in \mathbb{P}^2 : \ F(x,y,z) = 0\right\}.$$

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

Si $K = \mathbb{Q}$ alors on peut définir le degré d'un point algébrique sur $\mathbb{Q}$.

Définition 41. (degré d'un point algébrique)
Le degré d'un point algébrique sur le corps $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$.

Si $P = (x_1, x_2, x_3)$ alors $\mathbb{Q}(P) = \mathbb{Q}\left(\frac{x_i}{x_j}, \frac{x_k}{x_j}\right)$ pour tout j tel que $x_j \neq 0$. Le point P est dit alors de degré d si $[\mathbb{Q}(P) : \mathbb{Q}] = d$, on note $degP = d$.

Définition 42. (point singulier, point lisse, courbe lisse)
Un point P d'une courbe $C : F(X,Y,Z) = 0$ est dit singulier si

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

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

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0,0,0).$$

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

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

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

Selon un invariant appelé le genre de la courbe, l'ensemble des points rationnels sur un corps de nombres K est de différentes natures et en s'intéressant aux courbes planes projectives et lisses, on peut énoncer le résultat suivant qui détermine le lien entre le genre et le degré d'une courbe.

Théorème 43. *Soit $\mathcal{C}$ une courbe lisse projective et plane de degré d. Alors le genre de $\mathcal{C}$ est donné par :*

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

Remarque 1. *La formule exclut l'existence de courbes planes lisses projectives de certains genres, par exemple le genre 2.*

Chapitre 2

Courbes elliptiques, Courbes hyperelliptiques

Dans ce chapitre, nous parlerons de deux cas courbes algébriques particulières : courbes elliptiques, courbes hyperelliptiques. Quelques définitions et propriétés de base y seront données. Commençons par courbes elliptiques.

2.1 Courbes elliptiques

2.1.1 Equations de Weierstrass

Définition 44. (équation de Weierstrass)
Soit K un corps. On appelle équation de Weierstrass (forme projective) sur K une équation plane de la forme

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

avec les $a_i \in K$.

Remarque 2. *Si $Z = 0$, alors le point $O = (0 : 1 : 0)$ est appelé point à l'infini de l'équation* (2.1).
La tangente $Z = 0$ coupe la courbe uniquement en ce point et avec multiplicité 3.

En effet pour $Z = 0$, (2.1) *donne $0 = X^3$ d'où $X = 0$.*
Ainsi $(X : Y : Z) = (0 : Y : 0) = Y(0 : 1 : 0)$. On note $O = (0 : 1 : 0)$ que l'on appelle point à l'infini.
Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$ et l'équation de Weierstrass (2.1) *devient (forme affine)*

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

avec les $a_i \in K$.

Théorème 45. *Soit K un corps de caractéristique $p > 3$.*
Il existe des changements de variables permettant de simplifier (2.2) *en une équation plus simple dite équation courte de Weierstrass ou équation réduite de Weierstrass*

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

avec a, b dans K.

Preuve

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

Si le corps K est de caractéristique différente de 2 alors $(*)$ devient

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

et dans cet égalité en ajoutant à chaque membre $\left(\frac{a_1x}{2}\right)^2 + \left(\frac{a_3}{2}\right)^2 + \frac{a_3}{2}x$, on aura :

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

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

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

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

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

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

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

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

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

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

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

$y_1^2 = x_1^3 + Ax + B$ avec $x_1 = x + \dfrac{a'}{3}$, $A = b' - 3\left(\dfrac{a'}{3}\right)^2$ et $B = c' - \left(\dfrac{a'}{3}\right)^2$.
Comme les variables sont muettes alors $y^2 = x^3 + ax + b$.

Ces équations de Weierstrass nous permettront de définir des courbes elliptiques. Mais dans la suite, nous travaillerons avec l'équation réduite de Weierstrass (2.3).

2.1.2 Quelques définitions

Définition 46. Une courbe elliptique est une paire (E, O) où :
- E est une cubique irréductible non-singulière de genre 1,
- $O \in E$.

Définition 47. Une courbe elliptique est définie sur un corps K si :
- E est une courbe sur K (i.e donnée par l'annulation d'un polynôme de $K[X, Y]$),
- O est un point de la courbe dont les coordonnées sont dans K.

Définition 48. Soit K un corps de caractéristique $p > 3$. Une courbe elliptique définie sur K notée E est une courbe d'équation affine :

$$y^2 = x^3 + ax + b \tag{2.4}$$

avec a et b dans K tels que $4a^3 + 27b^2 \neq 0$, à laquelle on rajoute un point $O = (0 : 1 : 0)$ que l'on appelle le point à l'infini.

Notation
L'ensemble des points de E à coordonnées dans K sera noté $E(K)$. Lorsqu'il n'y a pas d'ambiguïté sur le corps, nous noterons les courbes $E(K)$ ou E. Donc on a :

$$E(K) = \left\{(x, y) \in K^2 | y^2 = x^3 + ax + b\right\} \cup \{O\} \tag{2.5}$$

Remarque 3. *Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$ et* (2.4) *devient (forme projective)*

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{2.6}$$

Définition 49. (invariants d'une courbe elliptique)
Le discriminant d'une courbe elliptique définie sur K par l'équation affine réduite (2.4) est la quantité

$$\Delta(E) = -16(4a^3 + 27b^2) \tag{2.7}$$

Le j-invariant d'une telle courbe est la quantité

$$j = -1728\frac{(4a)^3}{\Delta(E)} = \frac{6912a^3}{4a^3 + 27b^2} \tag{2.8}$$

Remarque 4. *Du point de vue algébrique, le j-invariant est une quantité importante qui permet de caractériser les courbes elliptiques.*

Définition 50. Une courbe elliptique est dite super-singulière lorsque son j-invariant est nul, c'est à dire $j = 0$.

Remarque 5. *Le signe du discriminant $\Delta(E)$ peut nous permettre de dire si la courbe elliptique est composée de deux composantes ou d'une seule composante.*

- Si $\Delta(E) > 0$ alors le graphe de la courbe elliptique possède deux composantes.
  Le polynôme $x^3 + ax + b$ possède trois racines qui correspondent aux abscisses des points d'intersection de la courbe avec l'axe des abscisses.
- Si $\Delta(E) < 0$ alors le graphe de la courbe elliptique possède une seule composante.
  Le polynôme $x^3 + ax + b$ possède une seule racine qui correspond à l'abscisse du point d'intersection de la courbe avec l'axe des abscisses.
- Si $\Delta(E) = 0$ alors nous ne pouvons pas parler de courbe elliptique.
  En effet le polynôme $x^3 + ax + b$ a une racine double, c'est-à-dire que le polynôme $x^3 + ax + b = (x - \alpha)^2(x - \beta)$ avec $2\alpha + \beta = 0$.
  $*$ Si $\alpha = \beta = 0$ ou $a = b = 0$ alors la courbe a un point de rebroussement en 0 (zéro).
  $*$ Si $\alpha > \beta$ alors la courbe a un point singulier en $(\alpha, 0)$.
  $*$ Si $\alpha < \beta$ alors la courbe a un point double $(\beta, 0)$ et les tangentes en ce point sont situées de part et d'autre de l'axe des abscisses.
  Finalement, d'où la nécessité d'avoir $\Delta(E) \neq 0$ et le j-invariant d'une courbe elliptique est toujours défini.

Exemple 16.

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

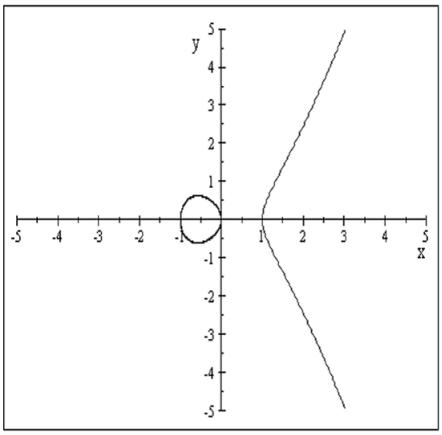

FIGURE 2.1 – $E : y^2 = x^3 - x$

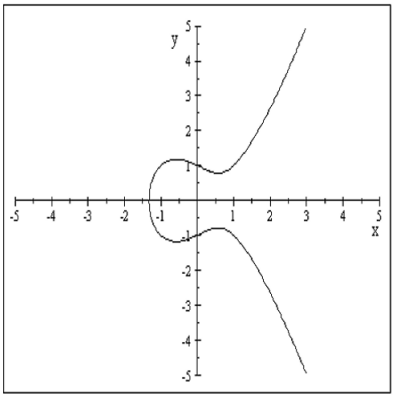

FIGURE 2.2 – $E : y^2 = x^3 - x + 1$

Théorème 51. *Soit E une courbe elliptique définie par l'équation réduite de Weierstrass (2.4). E est non singulière si $\Delta(E) \neq 0$.*

Preuve

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

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

On a :

$$\frac{\partial F}{\partial X} = -3X^2 - aZ^2 \ \ et \ \ \frac{\partial F}{\partial X}(O) = 0$$

$$\frac{\partial F}{\partial Y} = 2YZ \ \ et \ \ \frac{\partial F}{\partial Y}(O) = 0$$

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

Les dérivées partielles en $O = (0, 1, 0)$ ne sont pas simultanément nulles. Par suite, O n'est pas singulier. Pour les autres points, considérons la définition de la courbe E donnée par son équation réduite de Weierstrass $E : f(x, y) = y^2 - x^3 - ax - b = 0$.
La courbe est singulière en un point $P_0 = (x_0, y_0) \in E$ si et seulement si :

$$\frac{\partial f}{\partial x}(x_0, y_0) = -3x_0^2 - a = 0 \ et \ \frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0 \Longleftrightarrow -3x_0^2 = a \ et \ y_0 = \frac{0}{2}$$

$$x_0^2 = \frac{-a}{3} \ et \ y_0 = 0 \ car \ 2 \neq 0 \ et \ 3 \neq 0$$

Comme P_0 est un point de la courbe alors $y_0^2 = 0 = x_0^3 + ax_0 + b$.
On a $(x_0^2)\, x_0 + ax_0 + b = 0 \Longleftrightarrow \frac{-a}{3}x_0 + ax_0 + b = 0$ car $x_0^2 = \frac{-a}{3}$.

Donc on a $\frac{2}{3}ax_0 = -b$.
D'où $x_0 = \frac{-3b}{2a} \Rightarrow x_0^2 = \frac{9b^2}{4a^2} \Rightarrow \frac{9b^2}{4a^2} = \frac{-a}{3}$. Par suite $-(27b^2 + 4a^3) = 0$, soit $\Delta = 0$.
Finalement E est non singulière si et seulement si $\Delta \neq 0$.

2.2 Courbes hyperelliptiques

Dans ce paragraphe, on donnera des notions de base sur des courbes hyperelliptiques. On va aussi introduire la notion de diviseur sur une courbe, qui va nous permettre de définir une arithmétique sur des courbes hyperelliptiques.

2.2.1 Définitions de base

Dans tout ce qui suit K désigne un corps et $\bar{K}$ sa clôture algébrique, $K[x]$: l'ensemble des polynômes à une indéterminée x et $K[x, y]$: l'ensemble des polynômes à deux indéterminées x et y.

Définition 52. (courbe hyperelliptique)
Une courbe hyperelliptique $\mathcal{C}$ de genre $g \geq 1$ sur un corps K est une courbe non singulière donnée par une équation du type

$$\mathcal{C} : y^2 + H(x)y = F(x) \tag{2.9}$$

avec H et $F \in K[x]$, $2g + 1 \leq deg(F) \leq 2g + 2$, $deg(H) \leq g + 1$.
On ne considérera que les courbes hyperelliptiques imaginaires, c'est à dire avec F de degré $2g + 1$ et $deg(H) \leq g$. Dans ce cas, $\mathcal{C}$ a un point à l'infini, noté ∞.

Remarque 6. *Si on travaille sur un corps de caractéristique différente de* 2*, via la transformation* $y \longmapsto y - \frac{H(x)}{2}$*, la courbe* $\mathcal{C}$ *donnée dans* (2.9) *est isomorphe à*

$$y^2 = F'(x) \tag{2.10}$$

avec $deg(F') = 2g + 1$.

Définition 53. (genre d' une courbe hyperelliptique)
Le genre d' une courbe $\mathcal{C}$ hyperelliptique imaginaire de degré d est donné par : $g = \frac{(d-1)}{2}$.

Définition 54. (points rationnels, points à l'infini, points finis)
Soit L une extension du corps K. L'ensemble des points L-rationnels sur $\mathcal{C}$, noté $\mathcal{C}(L)$ est l'ensemble des points $P = (x, y)$ de $L \times L$ satisfaisant l'équation (2.10) et le point à l'infini noté ∞. L'ensemble des points $\mathcal{C}(\bar{K})$ sera noté $\mathcal{C}$. Les points de $\mathcal{C}$ autres que ∞ sont appelés points finis.

Définition 55. (point opposé, point spécial, point ordinaire)
Soit $P = (x, y)$ un point fini sur $\mathcal{C}$. L'opposé de P est le point $\bar{P} = (x, -y - H(x))$, (on remarque que le point $\bar{P}$ est aussi dans $\mathcal{C}$). L'opposé du point ∞ est égal à lui même. Si $P = \bar{P}$ on dit que P est un point spécial, sinon il est appelé point ordinaire.

Exemple 17.

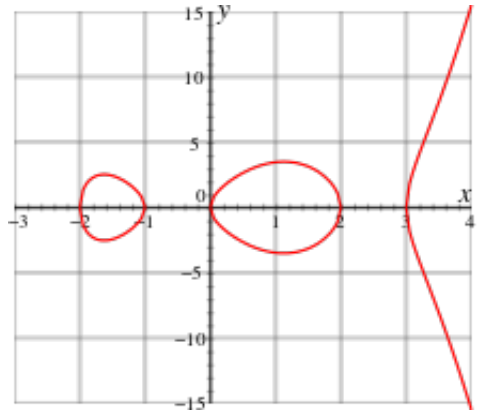

FIGURE 2.3 – Une courbe hyperelliptique $\mathcal{C} : y^2 = x(x-2)(x-3)(x+1)(x+2)$

Exemple 18.

Considérons la courbe hyperelliptique $\mathcal{C} : y^2 = 4x^5 + 1$.
On a $P = (0, 1) \in \mathcal{C}$. Son opposé est $\bar{P} = (0, -1) \in \mathcal{C}$.

À chacune de ces courbes, est associé un groupe abélien : sa jacobienne. On commence par rappeler la notion de diviseur.

2.2.2 Théorie des diviseurs

Définition 56. (diviseur, degré, ordre, support)
Un diviseur D de $\mathcal{C}$ est une somme formelle finie de points appartenant à $\mathcal{C}$:

$$D = \sum_{P \in \mathcal{C}} n_p P$$

où les $n_p \in \mathbb{Z}$ sont presque tous nuls.
Le degré d'un diviseur est la somme de ses coefficients définie par :

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

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

$$D = \sum_{P \in \mathcal{C}} n_p P \; et \; D' = \sum_{P \in \mathcal{C}} n'_p P$$

Alors on a :

$$D + D' = \sum_{P \in \mathcal{C}} (n_p + n'_p) P.$$

Le degré est un homomorphisme de groupe de $Div(\mathcal{C})$ dans $\mathbb{Z}$. Le noyau de cet homomorphisme est l'ensemble des diviseurs de degré 0, noté $Div^0(\mathcal{C})$ qui est un sous-groupe de $Div(\mathcal{C})$.
L'ordre d'un diviseur D au point P est l'entier n_P, on écrit $ord_P(D) = n_P$.
Le support de D est l'ensemble des points $P \in \mathcal{C}$ tels que $n_p \neq 0$.
La définition du support a bien un sens car la somme est finie.

Définition 57. (diviseur effectif)
On dit qu'un diviseur

$$D = \sum_{P \in \mathcal{C}} n_p P$$

est effectif, et on note $D \geq 0$ si : $\forall\, P \in \mathcal{C}$, $n_P \geq 0$.
Si D_1 et D_2 sont deux diviseurs sur $\mathcal{C}$, on notera $D_1 \geq D_2$ lorsque $D_1 - D_2$ est effectif.

Définition 58. (diviseur principal)
Soit $\mathcal{C}$ une courbe plane lisse définie sur un corps de nombre K et f une fonction rationnelle non nulle de $K(\mathcal{C})$. On associe à f le diviseur noté $Div(f)$ et défini par

$$Div(f) = \sum_{P \in \mathcal{C}} ord_p(f) P.$$

Un tel diviseur est appelé diviseur principal et nous notons $PDiv\,(\mathcal{C})$ leur ensemble.

Proposition 3. *Soient f et g deux fonctions rationnelles de $K(\mathcal{C})$, alors :*

$$Div\,(fg) = Div\,(f) + Div\,(g)\,,$$
$$Div\left(\frac{f}{g}\right) = Div\,(f) - Div\,(g)\,.$$

Remarque 7. *Une fonction rationnelle f a autant de zéros que de pôles donc $deg(Div(f)) = 0$. L'ensemble des diviseurs principaux est un sous-groupe de $Div^0(\mathcal{C})$.*

Définition 59. (diviseurs linéairement équivalents)
On dit que deux diviseurs D_1 et D_2 sont linéairement équivalents si le diviseur $D_1 - D_2$ est principal c'est à dire qu'il existe une fonction rationnelle f définie sur $\mathcal{C}$ tel que $D_1 = D_2 + div(f)$. On note $D_1 \sim D_2$.

Définition 60. (groupe de Picard)
Le quotient de $Div(\mathcal{C})$ par $PDiv(\mathcal{C})$ est appelé groupe de Picard de $\mathcal{C}$ et est noté par $Pic(\mathcal{C})$:

$$Pic(\mathcal{C}) = Div(\mathcal{C})/PDiv(\mathcal{C}).$$

On définit $Pic(\mathcal{C})$ comme étant l'ensemble des classes de diviseurs sur $\mathcal{C}$ modulo l'équivalence linéaire.
On définit de même $Pic^0(\mathcal{C})$ par :

$$Pic^0(\mathcal{C}) = Div^0(\mathcal{C})/PDiv(\mathcal{C}).$$

Définition 61. (Jacobienne d'une courbe)
La jacobienne d'une courbe $\mathcal{C}$ définie sur K est le sous-groupe des éléments de degré 0 dans le groupe de Picard de $\mathcal{C}$ noté $Jac(\mathcal{C})$.

Notons par $Pic_K(\mathcal{C})$ le sous-groupe de $Pic(\mathcal{C})$ fixé par $Gal(\overline{K}/K)$. Le groupe quotient $Div_K^0(\mathcal{C})/Pdiv_K(\mathcal{C})$ est la jacobienne de la courbe $\mathcal{C}$ définie sur K, ses éléments sont invariants sous l'action de Galois, on le note $J(K)$.

Théorème 62. *(théorème de Mordell-Weil)*
Soit A une variété abélienne définie sur un corps de nombre K. Alors le groupe des points rationnels $A(K)$ est un groupe de type

$$A(K) \cong \mathbb{Z}^r \oplus A(K)_{tor}$$

avec $A(K)_{tor}$ est le groupe de torsion et l'entier $r \geq 0$ est le rang de la variété.

Remarque 8.

- Si A est la jacobienne d'une courbe algébrique définie sur $\mathbb{Q}$ alors

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus J(\mathbb{Q})_{tor}.$$

- Si le rang de la courbe $r = 0$ alors

$$J(\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

  Il existe t diviseurs $D_1, \ldots, D_i \ldots, D_t$ sur $\mathcal{C}$ définis sur $\mathbb{Q}$ tels que $j(D_i)$ soit d'ordre n_i et $j(D_1), \ldots, j(D_t)$ engendrent $J(\mathbb{Q})$.

2.2.3 Théorème de Riemann-Roch

Cette section est dédiée au résultat le plus important concernant les diviseurs sur une courbe : le théorème de Riemann-Roch qui classe les courbes suivant leur genre. Introduisons les espaces $\mathcal{L}(D)$ qui interviennent dans le théorème de Riemann-Roch.

Définition 63. (les espaces $\mathcal{L}(D)$)
Soit $\mathcal{C}$ une courbe lisse et soit $D \in Div(\mathcal{C})$. On lui associe l'ensemble des fonctions :

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

Proposition 4. *Soit $\mathcal{C}$ une courbe lisse et soit $D \in Div(\mathcal{C})$.*
i) $\mathcal{L}(D)$ est un espace vectoriel sur K de dimension finie notée $l(D)$.
ii) Si $degD < 0$ alors $\mathcal{L}(D) = \{0\}$, $l(D) = 0$.
iii) Si D, $D' \in Div(\mathcal{C})$ sont linéairement équivalents, alors $\mathcal{L}(D)$ et $\mathcal{L}(D')$ sont isomorphes.
iv) Si D, $D' \in Div(\mathcal{C})$ vérifient $D \leq D'$ alors $\mathcal{L}(D) \subset \mathcal{L}(D')$.

Théorème 64. *(Théorème de Riemann-Roch)*
Soit $\mathcal{C}$ une courbe lisse. Alors il existe un diviseur $K_{\mathcal{C}}$ appelé diviseur canonique et un entier $g \geq 0$ appelé genre de $\mathcal{C}$ tel que pour tout diviseur $D \in Div(\mathcal{C})$ on ait :

$$l(D) = deg(D) + 1 - g + l(K_{\mathcal{C}} - D).$$

Un diviseur canonique d'une courbe $\mathcal{C}$ est un diviseur d'une forme différentielle sur $\mathcal{C}$. Si on choisi $D = 0$, le diviseur nul, on obtient : $l(D) = l(0) = 1$ car les seules fonctions régulières sur les variétés projectives sont les constantes. Comme le degré du diviseur est égale à zéro alors le théorème donne l'égalité : $l(K_{\mathcal{C}}) = g$.

Corollaire 2. *: Avec les notations précédentes, on a :*
(1) $deg(K_{\mathcal{C}}) = 2g - 2$.
(2) Si $deg(D) < 0$ alors $\mathcal{L}(D) = \{0\}$ et $l(D) = 0$.
(3) Si $deg(D) > 2g - 1$ alors $l(D) = deg(D) + 1 - g$.
(4) Si $l(D)l(K_{\mathcal{C}} - D) \neq 0$ alors $l(D) \leq 1 + deg(D)/2$.
(5) Si $deg(D) \geq 2g$ alors D est sans point base.

2.2.4 Théorème d'Abel-Jacobi

Définition 65. (point de base)
Un point $\infty \in \mathcal{C}$ est dit point de base du système linéaire s'il apparait dans chacun de ses diviseurs.

Définition 66. (plongement jacobien)
On désigne par $[D]$ la classe dans $Pic^0(\mathcal{C})$ d'un diviseur D. Soit $\infty \in \mathcal{C}$ un point base.
• On appelle plongement jacobien l'application j définie par :
$j : \mathcal{C} \to Jac(\mathcal{C})$
$P \mapsto [P - \infty]$
• L'application j appelée application d'Abel-Jacobi, s'étend par additivité, encore notée j, de $Div^0(\mathcal{C})$ vers $Jac(\mathcal{C})$ définie par :

$$j(\sum_{P_i \in \mathcal{C}} n_i P_i) = \sum_{P_i \in \mathcal{C}} n_i j(P_i)$$

.

D'après le théorème d'Abel-Jacobi, pour tout diviseur $D \in Dic^0(\mathcal{C})$, il existe une fonction $f \in K^*(\mathcal{C})$ tel que $div(f) = D$, si et seulement si $j(D) = 0$. Mais le théorème suivant est plus fort.

Théorème 67. *(théorème d'Abel-Jacobi)*
L'application j est surjective et son noyau est formé des diviseurs de fonctions sur $\mathcal{C}$. En d'autres termes, l'application j induit un isomorphisme de $Pic^0(\mathcal{C})$ vers $Jac(\mathcal{C})$.

Chapitre 3

Points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur certaines courbes

Dans ce chapitre, nous regroupons les courbes algébriques pour lesquelles nous avons déterminé de manière explicite l'ensemble des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$.

3.1 Courbe $\mathcal{C} : y^2 = 4x^5 + 1$

3.1.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K. On note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$, autrement dit $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine :

$$y^2 = 4x^5 + 1 \tag{3.1}$$

La courbe $\mathcal{C}$ est hyperelliptique de genre $g = 2$ et de rang nul d'après [1].
Notons $P = (0, 1),\ \bar{P} = (0, -1)$ *et* ∞ le point à l'infini.
Dans [1] Booker, Sijsling, Sutherland, Voight et Yasak ont donné une description des points rationnels. De même dans [26] Stoll a donné cette même description.
Cette description s'énonce comme suit :

Proposition 5. *Les points* $\mathbb{Q}-$*rationnels sur la courbe* $\mathcal{C}$ *sont donnés par*

$$\mathcal{C}(\mathbb{Q}) = \left\{P,\ \bar{P},\ \infty\right\} \tag{3.2}$$

Nous étendons ce résultat en donnant une description des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$. Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathcal{C}$ sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$, (voir [1]),
- Le théorème d'Abel Jacobi, (voir [8]),
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :

Théorème.

1. L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par
$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{4\alpha^5 + 1} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ est donné par
$$\mathcal{C}' = \left\{ (x, \pm 1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_2(x) = 4x^3 - \alpha^2 x^2 \pm 2\alpha^2 \right\}$$
3. L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ avec
$$\mathcal{C}_0 = \left\{ \left(x, \pm\sqrt{4x^5 + 1} \right) |\ x \in \overline{\mathbb{Q}},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$
$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x + \beta)) \ |\ \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_1(x) = 4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 - (2\alpha + \alpha^2\beta^2)x - 2\alpha\beta \end{array} \right\}$$
$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, -1 - \alpha x^2 (x + \beta)) \ |\ \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_2(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 + 2\alpha x + 2\alpha\beta \end{array} \right\}$$
.
$$\mathcal{C}_3 = \left\{ \begin{array}{l} (x, 1 - \alpha x^2 (x + \beta)) \ |\ \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_3(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 - 2\alpha x - 2\alpha\beta \end{array} \right\}$$
.
$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x + \beta)) \ |\ \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_4(x) = 4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 + (2\alpha + \alpha^2\beta^2)x + 2\alpha\beta \end{array} \right\}$$
.
4. L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{D}_0 \cup \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4$ avec
$$\mathcal{D}_0 = \left\{ \begin{array}{l} (x, \alpha + \lambda x(x + \mu) \ |\ \alpha, \mu, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_0(x) = 4x^5 - (\alpha + \lambda x(x + \mu))^2 + 1 \end{array} \right\}$$
$$\mathcal{D}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x^2 + \beta x + \gamma)) \ |\ \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_1(x) = \alpha^2 x (x^2 + \beta x + \gamma)^2 - 4x^4 + 2\alpha (x^2 + \beta x + \gamma) \end{array} \right\}$$
$$\mathcal{D}_2 = \left\{ \begin{array}{l} \left(x, 1 - \dfrac{\alpha}{x + \beta} x^2 (x + \gamma) \right) \ |\ \alpha, \beta \in \mathbb{Q} \text{ et } x \text{ racine} \in \overline{\mathbb{Q}} \text{ de} \\ \\ \mathcal{F}_2(x) = 4x^3(x + \beta)^2 - \alpha^2 x^2 (x + \gamma)^2 - 2\alpha(x + \gamma)(x + \beta) \end{array} \right\}.$$

$$\mathcal{D}_3 = \left\{ \begin{array}{l} \left(x, 1 - \dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_3(x) = 4x^3(x+\beta)^2 - \alpha^2x^2(x+\gamma)^2 + 2\alpha(x+\gamma)(x+\beta) \end{array} \right\}$$

$$\mathcal{D}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x^2+\beta x+\gamma)) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_4(x) = \alpha^2 x\left(x^2+\beta x+\gamma\right)^2 - 4x^4 - 2\alpha\left(x^2+\beta x+\gamma\right) \end{array} \right\}$$

3.1.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\bar{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles F sur $\mathcal{C}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\bar{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$. On montre dans [4] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

$$x(X,Y,Z) = \frac{X}{Z} \qquad et \qquad y(X,Y,Z) = \frac{Y}{Z}$$

L'équation projective de la courbe $\mathcal{C}$ est :

$$\mathcal{C} : Y^2Z^3 = 4X^5 + Z^5 \tag{3.3}$$

On désigne par J la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P-\infty]$ de $P-\infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.

Soit $\eta = e^{i\frac{\Pi}{5}}$ dans $\mathbb{C}$. Posons $B_k = (\sqrt[5]{\frac{1}{4}}\,\eta^{2k+1}, 0)$ pour $k \in \{0,1,2,3,4\}$.

Désignons par $\mathcal{C}'.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{C}'$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 1.

- $div(x) = P + \bar{P} - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(y-1) = 5P - 5\infty$
- $div(y+1) = 5\bar{P} - 5\infty$

Preuve. Calculons seulement $div(x)$ et en procédant de la même manière, on trouve les autres.
On a $div(x) = div(\frac{X}{Z}) = (X=0).\mathcal{C} - (Z=0).\mathcal{C}$.
Pour $X = 0$, on a $Y^2Z^3 = Z^5$ d'après (3.3), ce qui donne $Z^3 = 0$ ou $Y^2 = Z^2$.
D'une part pour $X = 0$, on a $Z^3 = 0$; avec $Y = 1$ on obtient donc le point $\infty = (0,1,0)$ avec multiplicité 3.
D'autre part pour $X = 0$, on a $Y = Z$ ou $Y = -Z$; avec $Z = 1$ on obtient donc les points $P = (0, 144, 1)$ avec multiplicité 1 et $\bar{P} = (0, -144, 1)$ avec multiplicité 1.
D'où $(X=0).\mathcal{C} = P + \bar{P} + 3\infty$. (i)
De même pour $Z = 0$, alors on a $X^5 = 0$ d'après (3.3) ; et pour $Y = 1$, on a le point

$\infty = (0, 1, 0)$ avec multiplicité 5. D'où $(Z = 0).\mathcal{C} = 5\infty$. (ii)
Les relations (i) et (ii) entraînent que $div(x) = P + \bar{P} - 2\infty$.

Conséquences du lemme 1
$5j(P_0) = 5j(P_1) = 0$ et $j(P_0) + j(P_1) = 0$

Lemme 2. .
- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1, x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1, x, x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1, x, x^2, y \rangle$
- $\mathcal{L}(6\infty) = \langle 1, x, x^2, y, x^3 \rangle$
- $\mathcal{L}(7\infty) = \langle 1, x, x^2, y, x^3, xy \rangle$

Preuve. C'est une conséquence du lemme 1 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 3. $J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} = \langle [P - \infty] \rangle = \{a[P - \infty], a \in \{0, 1, 2, 3, 4\}\}$.

Preuve.(voir [4])

3.1.3 Démonstration du théorème

a) **Points quadratiques sur $\mathcal{C}$**
L'ensemble des points quadratiques sur $\mathcal{C}$ est

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{4\alpha^5 + 1} \right),\ \alpha \in \mathbb{Q}^* \right\}$$

Preuve :
Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Notons R_1, R_2 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, d'où

$$t = [R_1 + R_2 - 2\infty] = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4 \quad (*)$$

On remarque que $R \notin \left\{ \infty, P, \bar{P} \right\}$.
Cas $a = 0$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty \tag{3.4}$$

donc $F \in \mathcal{L}(2\infty)$, d'où $F(x, y) = a_1 + a_2 x$, $(a_2 \neq 0)$.
Aux points R_i, on a $a_1 + a_2 x = 0$ donc $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}^*$.
En remplaçant x par α dans (3.1), on a :

$$y^2 = 4\alpha^5 + 1 \tag{3.5}$$

et par suite on a :

$$y = \pm\sqrt{4\alpha^5 + 1} \tag{3.6}$$

On a ainsi une famille de points quadratiques

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{4\alpha^5 + 1}\right),\ \alpha \in \mathbb{Q}^* \right\}$$

Cas $a = 1$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = j(P) = -j(\bar{P})$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \bar{P} - 3\infty \tag{3.7}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, $\bar{P}$ devrait être égal à ∞ ; ce qui est absurde.
Cas $a = 2$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 2j(P) = -2j(\bar{P})$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2\bar{P} - 4\infty \tag{3.8}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2$, $(a_3 \neq 0)$ et comme $ord_{\bar{P}}(F) = 2$, on doit avoir $a_1 = a_2 = 0$, donc $F(x, y) = a_3x^2$ et on devrait avoir $R_1 = R_2 = P$, ce qui est absurde.
Cas $a = 3$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 3j(P) = -2j(P)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2P - 4\infty \tag{3.9}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2$, $(a_2 \neq 0)$ et comme $ord_P(F) = 2$, on doit avoir $a_1 = a_2 = 0$,donc $F(x, y) = a_3x^2$ et on devrait avoir $R_1 = R_2 = \bar{P}$, ce qui est absurde.
Cas $a = 4$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 4j(P) = -j(P)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty \tag{3.10}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P devrait être égal à ∞ ; ce qui est absurde.
Conclusion : L'ensemble des points quadratiques sur $\mathcal{C}$ est :

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{4\alpha^5 + 1}\right),\ \alpha \in \mathbb{Q}^* \right\}$$

b) **Points cubiques sur $\mathcal{C}$**
L'ensemble des points cubiques sur $\mathcal{C}$ est

$$\mathcal{C}' = \left\{ (x, \pm 1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_3(x) = 4x^3 - \alpha^2x^2 \pm 2\alpha^2 \right\}$$

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R et travaillons avec $t = [R_1 + R_2 + R_3 - 3\infty]$ qui est un point de $J(\mathbb{Q}) = \{aj(P),\ 0 \leq a \leq 4\}$, donc $t = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4$.
On remarque que $R \notin \left\{\infty, P, \bar{P}\right\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 0$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 - 3\infty$, donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, alors un des R_i devrait être égal à ∞, ce qui est absurde.
Cas $a = 1$ **et** $a = 4$
Donc pour $a = 1$, on a $[R_1 + R_2 + R_3 - 3\infty] = j(P) = -j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + \bar{P} - 4\infty$, donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2$.
Au point $\bar{P}$, on a $F(\bar{P}) = 0$ donc $a_1 = 0$ d'où $F(x, y) = x(a_2 + a_3x)$.
Aux points R_i, on a $x(a_2 + a_3x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.
Pour $a = 4$, par un raisonnement similaire au cas $a = 1$, on aboutit à la même contradiction.
Cas $a = 2$ **et** $a = 3$
Donc pour $a = 2$, on a $[R_1 + R_2 + R_3 - 3\infty] = 2j(P) = -2j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 2\bar{P} - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y$, $(a_4 \neq 0)$.
La fonction F est d' ordre 2 en $\bar{P}$ donc $a_1 - a_4 = 0$ et $a_2 = 0$, d'où $F(x, y) = a_4(y+1) + a_3x^2$.
Aux points R_i, on doit avoir $a_4(y+1) + a_3x^2 = 0$, d'où $y = -1 - \frac{a_3}{a_4}x^2$. On voit que y est de la forme $y = -1 - \alpha x^2$ avec $\alpha \in \mathbb{Q}^*$, et par suite on a $y^2 = 4x^5 + 1 \Leftrightarrow (-1 - \alpha x^2)^2 = 4x^5 + 1$
$\Leftrightarrow 4x^5 - \alpha^2x^4 - 2\alpha^2x^2 = 0 \Leftrightarrow x^2(4x^3 - \alpha^2x^2 - \alpha^2) = 0$.
On doit avoir $x^2 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques

$$\mathcal{A} = \left\{(x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^*\ et\ x\ racine\ de\ C_1(x) = 4x^3 - \alpha^2x^2 - 2\alpha^2\right\} \tag{3.11}$$

Pour $a = 4$, par un raisonnement similaire au cas $a = 2$, on obtient ainsi une famille de points cubiques

$$\mathcal{B} = \left\{(x, 1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^*\ et\ x\ racine\ de\ C_2(x) = 4x^3 - \alpha^2x^2 + 2\alpha^2\right\} \tag{3.12}$$

En combinant ces deux familles de points cubiques, on obtient alors

$$\mathcal{C}' = \left\{(x, \pm 1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^*\ et\ x\ racine\ de\ C_3(x) = 4x^3 - \alpha^2x^2 \pm 2\alpha^2\right\} \tag{3.13}$$

c) **Points quartiques sur** $\mathcal{C}$
L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ avec

$$\mathcal{C}_0 = \left\{\left(x, \pm\sqrt{4x^5 + 1}\right) \mid x \in \overline{\mathbb{Q}},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\right\}$$

$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x + \beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_1(x) = 4x^4 - \alpha^2x^3 - 2\alpha^2\beta x^2 - (2\alpha + \alpha^2\beta^2)x - 2\alpha\beta \end{array} \right\}$$

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, -1-\alpha x^2\,(x+\beta)) \mid \alpha,\beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_2(x) = \alpha^2x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2x^2 + 2\alpha x + 2\alpha\beta \end{array} \right\}$$

.

$$\mathcal{C}_3 = \left\{ \begin{array}{l} (x, 1-\alpha x^2\,(x+\beta)) \mid \alpha,\beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_3(x) = \alpha^2x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2x^2 - 2\alpha x - 2\alpha\beta \end{array} \right\}$$

.

$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, 1-\alpha x(x+\beta)) \mid \alpha,\beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_4(x) = 4x^4 - \alpha^2x^3 - 2\alpha^2\beta x^2 + (2\alpha - \alpha^2\beta^2)x + 2\alpha\beta \end{array} \right\}$$

.

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}\,(R) : \mathbb{Q}] = 4$. Notons R_1, R_2, R_3, R_4 les conjugués de Galois de R et travaillons avec $t = [R_1 + R_2 + R_3 + R_4 - 4\infty]$ qui est un point de $J(\mathbb{Q}) = \{aj(P),\ 0 \leq a \leq 4\}$, donc $t = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4$.
On remarque que $R \notin \left\{\infty, P, \bar{P}\right\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1+R_2+R_3+R_4-4\infty$, donc $F \in \mathcal{L}\,(4\infty)$ et par suite $F = a_1+a_2x+a_3x^2$.
Aux points R_i, on a $a_1 + a_2x + a_3x^2 = 0$. La relation $y^2 = 4x^5 + 1$ donne $y = \pm\sqrt{4x^5+1}$.
On trouve ainsi une famille de points quartiques

$$\mathcal{C}_0 = \left\{ \left(x, \pm\sqrt{4x^5+1}\right) \mid x \in \overline{\mathbb{Q}},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\} \tag{3.14}$$

Cas $a = 1$
Donc on a $[R_1 + R_2 + R_3 + R_4 - 4\infty] = j(P) = -j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + \bar{P} - 5\infty$, donc $F \in \mathcal{L}\,(5\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y,\ (a_4 \neq 0)$.
Au point $\bar{P}$, on a $F(\bar{P}) = 0$ donc $a_1 - a_4 = 0$ d'où $F(x, y) = a_4(y + 1) + a_2x + a_3x^2$.
Aux points R_i, on a $a_4(y+1)+a_2x+a_3x^2 = 0$, d'où $y = -1-\dfrac{a_2}{a_4}x-\dfrac{a_3}{a_4}x^2 = -1-\dfrac{a_3}{a_4}x(x+\dfrac{a_2}{a_3})$.
On voit que y est de la forme $y = -1 - \alpha x(x + \beta)$ avec $\alpha, \beta \in \mathbb{Q}^\star$; et par suite on a $y^2 = 4x^5+1 \Leftrightarrow (-1 - \alpha x(x + \beta))^2 = 4x^5+1 \Leftrightarrow 4x^5-\alpha^2x^4-2\alpha^2\beta x^3-(2\alpha+\alpha^2\beta^2)x^2-2\alpha\beta x = 0$
$\Leftrightarrow x(4x^4 - \alpha^2x^3 - 2\alpha^2\beta x^2 - (2\alpha + \alpha^2\beta^2)x - 2\alpha\beta) = 0$.
On doit avoir $x \neq 0$ et $\alpha, \beta \in \mathbb{Q}^\star$, on obtient une famille de points quartiques

$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1-\alpha x(x+\beta)) \mid \alpha,\beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_1(x) = 4x^4 - \alpha^2x^3 - 2\alpha^2\beta x^2 - (2\alpha + \alpha^2\beta^2)x - 2\alpha\beta \end{array} \right\}$$

.

Cas $a = 2$
Donc on a $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 2j(P) = -2j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + 2\bar{P} - 6\infty$, donc $F \in \mathcal{L}\,(6\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3,\ (a_5 \neq 0)$.
La fonction F est d' ordre 2 en $\bar{P}$ donc $a_1-a_4 = 0$ et $a_2 = 0$, d'où $F(x, y) = a_4(y+1)+a_3x^2+a_5x^3$. Aux points R_i, on doit avoir $a_4(y+1)+a_3x^2+a_5x^3 = 0$, d'où $y = -1-\frac{a_5}{a_4}x^2\left(\frac{a_3}{a_5}x + \beta\right)$.
On voit que y est de la forme $y = -1 - \alpha x^2\,(x + \beta)$ avec $\alpha, \beta \in \mathbb{Q}^*$, et par suite on a

$y^2 = 4x^5 + 1 \Leftrightarrow (-1 - \alpha x^2 (x + \beta))^2 = 4x^5 + 1 \Leftrightarrow$
$x^2 (\alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 + 2\alpha x + 2\alpha\beta) = 0.$
On doit avoir $x^2 \neq 0$ et $\alpha, \beta \in \mathbb{Q}^*$, on obtient une famille de points quartiques

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, -1 - \alpha x^2 (x + \beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_2(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 + 2\alpha x + 2\alpha\beta \end{array} \right\}$$

.

Cas $a = 3$

Donc on a $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 3j(P) = -2j(P)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + 2P - 6\infty$, donc $F \in \mathcal{L}(6\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y + a_5 x^3$, $(a_5 \neq 0)$.
La fonction F est d' ordre 2 en P donc $a_1 + a_4 = 0$ et $a_2 = 0$, d'où $F(x, y) = a_4(y-1) + a_3 x^2 + a_5 x^3$. Aux points R_i, on doit avoir $a_4(y-1) + a_3 x^2 + a_5 x^3 = 0$, d'où $y = 1 - \frac{a_5}{a_4} x^2 \left(x + \frac{a_3}{a_5}\right)$. On voit que y est de la forme $y = 1 - \alpha x^2 (x + \beta)$ avec $\alpha, \beta \in \mathbb{Q}^*$, et par suite on a $y^2 = 4x^5 + 1$
$\Leftrightarrow (1 - \alpha x^2 (x + \beta))^2 = 4x^5 + 1 \Leftrightarrow x^2 (\alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 - 2\alpha x - 2\alpha\beta) = 0.$
On doit avoir $x^2 \neq 0$ et $\alpha, \beta \in \mathbb{Q}^*$, on obtient une famille de points quartiques

$$\mathcal{C}_3 = \left\{ \begin{array}{l} (x, 1 - \alpha x^2 (x + \beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_3(x) = \alpha^2 x^4 + (2\alpha^2\beta - 4)x^3 + \alpha^2\beta^2 x^2 - 2\alpha x - 2\alpha\beta \end{array} \right\}$$

.

Cas $a = 4$

Donc on a $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 4j(P) = -j(P)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + P - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$, $(a_4 \neq 0)$.
Au point P, on a $F(P) = 0$ donc $a_1 + a_4 = 0$ d'où $F(x, y) = a_4(y - 1) + a_2 x + a_3 x^2$.
Aux points R_i, on doit avoir $a_4(y - 1) + a_2 x + a_3 x^2 = 0$, d'où $y = 1 - \dfrac{a_2}{a_4} x - \dfrac{a_3}{a_4} x^2 = 1 - \dfrac{a_3}{a_4} x(x + \dfrac{a_2}{a_3})$. On voit que y est de la forme $y = 1 - \alpha x(x + \beta)$ avec $\alpha, \beta \in \mathbb{Q}^\star$; et par suite on a $y^2 = 4x^5 + 1 \Leftrightarrow (1 - \alpha x(x + \beta))^2 = 4x^5 + 1 \Leftrightarrow x(4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 + (2\alpha + \alpha^2\beta^2)x + 2\alpha\beta) = 0.$
On doit avoir $x \neq 0$ et $\alpha, \beta \in \mathbb{Q}^*$, on obtient une famille de points quartiques

$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x + \beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B_4(x) = 4x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 + (2\alpha + \alpha^2\beta^2)x + 2\alpha\beta \end{array} \right\}$$

.

Conclusion : L'ensemble des points quartiques sur $\mathcal{C}$ est couvert par $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$.

d) **Points quintiques sur $\mathcal{C}$**

L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{D}_0 \cup \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4$ avec

$$\mathcal{D}_0 = \left\{ \begin{array}{l} (x, \alpha + \lambda x(x + \mu) \mid \alpha, \mu, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_0(x) = 4x^5 - (\alpha + \lambda x(x + \mu))^2 + 1 \end{array} \right\}$$

$$\mathcal{D}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x^2 + \beta x + \gamma)) \ \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_1(x) = \alpha^2 x \left(x^2 + \beta x + \gamma\right)^2 - 4x^4 + 2\alpha \left(x^2 + \beta x + \gamma\right) \end{array} \right\}$$

$$\mathcal{D}_2 = \left\{ \begin{array}{l} \left(x, -1 - \dfrac{\alpha}{x+\beta} x^2(x+\gamma)\right) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_2(x) = 4x^3(x+\beta)^2 - \alpha^2 x^2 (x+\gamma)^2 - 2\alpha(x+\gamma)(x+\beta) \end{array} \right\}$$

$$\mathcal{D}_3 = \left\{ \begin{array}{l} \left(x, 1 - \dfrac{\alpha}{x+\beta} x^2(x+\gamma)\right) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_3(x) = 4x^3(x+\beta)^2 - \alpha^2 x^2 (x+\gamma)^2 + 2\alpha(x+\gamma)(x+\beta) \end{array} \right\}$$

$$\mathcal{D}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x^2 + \beta x + \gamma)) \ \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_4(x) = \alpha^2 x \left(x^2 + \beta x + \gamma\right)^2 - 4x^4 - 2\alpha \left(x^2 + \beta x + \gamma\right) \end{array} \right\}$$

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 5$. Notons R_1, R_2, R_3, R_4, R_5 les conjugués de Galois de R et travaillons avec $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty]$ qui est un point de $J(\mathbb{Q}) = \{aj(P),\ 0 \leq a \leq 4\}$, donc $t = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4$.
On remarque que $R \notin \left\{\infty, P, \bar{P}\right\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 0$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$, $(a_4 \neq 0)$.
Aux points R_i, on doit avoir $a_1 + a_2 x + a_3 x^2 + a_4 y = 0$, d'où $y = -\dfrac{a_1}{a_4} - \dfrac{a_3}{a_4} x(x + \dfrac{a_2}{a_3})$ avec $\alpha = -\dfrac{a_1}{a_4}$, $\lambda = -\dfrac{a_3}{a_4}$, $\mu = \dfrac{a_2}{a_3}$ donc y est de la forme $y = \alpha + \lambda x(x+\mu)$ avec $\alpha, \mu \in \mathbb{Q},\ \lambda \in \mathbb{Q}^*$ et par suite la relation $y^2 = 4x^5 + 1$ donne $\left(\alpha + \lambda x(x+\mu)\right)^2 = 4x^5 + 1 \Longleftrightarrow$

$$4x^5 - \left(\alpha + \lambda x(x+\mu)\right)^2 + 1 = 0.$$

On trouve ainsi une famille de points quintiques

$$\mathcal{D}_0 = \left\{ \begin{array}{l} (x, \alpha + \lambda x(x+\mu) \ \mid \alpha, \mu, \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_0(x) = x^5 - \left(\alpha + \lambda x(x+\mu)\right)^2 + 1 \end{array} \right\}$$

Cas $a = 1$
Donc on a $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = j(P) = -j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + \bar{P} - 6\infty$, donc $F \in \mathcal{L}(6\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y + a_5 x^3$, $(a_5 \neq 0)$.
Au point $\bar{P}$, on a $F(\bar{P}) = 0$ donc $a_1 - a_4 = 0$ d'où $F(x, y) = a_4(y+1) + a_2 x + a_3 x^2 + a_5 x^3$.

Aux points R_i, on a $a_4(y+1)+a_2x+a_3x^2+a_5x^3=0$, d'où $y=-1-\dfrac{a_2}{a_4}x-\dfrac{a_3}{a_4}x^2-\dfrac{a_5}{a_4}x^3=-1-\dfrac{a_5}{a_4}x(x^2+\dfrac{a_3}{a_5}x+\dfrac{a_2}{a_5})$. On voit que y est de la forme $y=-1-\alpha x(x^2+\beta x+\gamma)$ avec $\alpha,\beta,\gamma\in\mathbb{Q}^\star$. Par suite on a $y^2=4x^5+1\Leftrightarrow(-1-\alpha x(x^2+\beta x+\gamma))^2=4x^5+1\Leftrightarrow x\left(\alpha^2x\left(x^2+\beta x+\gamma\right)^2-4x^4+2\alpha\left(x^2+\beta x+\gamma\right)\right)=0$.
On doit avoir $x\neq 0$ et $\alpha,\beta,\gamma\in\mathbb{Q}^\star$, obtient une famille de points quintiques

$$\mathcal{D}_1=\left\{\begin{array}{l}(x,-1-\alpha x(x^2+\beta x+\gamma))\ \mid \alpha,\beta,\gamma\in\mathbb{Q}^*\text{ et }x\text{ racine de}\\ \\ \mathcal{F}_1(x)=\alpha^2x\left(x^2+\beta x+\gamma\right)^2-4x^4+2\alpha\left(x^2+\beta x+\gamma\right)\end{array}\right\}$$

Cas $a=2$
Donc on a $[R_1+R_2+R_3+R_4+R_5-5\infty]=2j(P)=-2j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F)=R_1+R_2+R_3+R_4+R_5+2\bar{P}-7\infty$, donc $F\in\mathcal{L}(7\infty)$ et par suite $F(x,y)=a_1+a_2x+a_3x^2+a_4y+a_5x^3+a_6xy$, $(a_6\neq 0)$.
La fonction F est d' ordre 2 en $\bar{P}$ donc $a_1-a_4=0$ et $a_2-a_6=0$, et par suite on a $F(x,y)=a_4(y+1)+a_6x(y+1)+a_3x^2+a_5x^3$.
Aux points R_i , on doit avoir $a_4(y+1)+a_6x(y+1)+a_3x^2+a_5x^3=0$, d'où
$y=-1-\dfrac{a_5}{a_4+a_6x}x^2(x+\frac{a_3}{a_5})$; donc y est de la forme $y=-1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)$ avec $\alpha,\beta,\gamma\in\mathbb{Q}^*$ et par suite on a $y^2=4x^5+1\Leftrightarrow\left(-1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right)^2=4x^5+1\Leftrightarrow$ $x^2\left(4x^3(x+\beta)^2-\alpha^2x^2(x+\gamma)^2-2\alpha(x+\gamma)(x+\beta)\right)=0$.
On doit avoir $x^2\neq 0$ et $\alpha,\beta,\gamma\in\mathbb{Q}^\star$, obtient une famille de points quintiques

$$\mathcal{D}_2=\left\{\begin{array}{l}\left(x,-1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right)\mid \alpha,\beta,\gamma\in\mathbb{Q}^*\text{ et }x\text{ racine de}\\ \\ \mathcal{F}_2(x)=4x^3(x+\beta)^2-\alpha^2x^2(x+\gamma)^2-2\alpha(x+\gamma)(x+\beta)\end{array}\right\}$$

Cas $a=3$
Donc on a $[R_1+R_2+R_3+R_4+R_5-5\infty]=3j(P)=-2j(P)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F)=R_1+R_2+R_3+R_4+R_5+2P-7\infty$, donc $F\in\mathcal{L}(7\infty)$ et par suite $F(x,y)=a_1+a_2x+a_3x^2+a_4y+a_5x^3+a_6xy$, $(a_6\neq 0)$.
La fonction F est d' ordre 2 en P donc $a_1+a_4=0$ et $a_2+a_6=0$, et par suite on a $F(x,y)=a_4(y+1)+a_6x(y+1)+a_3x^2+a_5x^3$.
Aux points R_i , on doit avoir $a_4(y-1)+a_6x(y-1)+a_3x^2+a_5x^3=0$, d'où
$y=1-\dfrac{a_5}{a_4+a_6x}x^2(x+\frac{a_3}{a_5})$; donc y est de la forme $y=1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)$ avec $\alpha,\beta,\gamma\in\mathbb{Q}^*$ et par suite on a $y^2=4x^5+1\Leftrightarrow\left(1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right)^2=4x^5+1\Leftrightarrow$ $x^2\left(4x^3(x+\beta)^2-\alpha^2x^2(x+\gamma)^2+2\alpha(x+\gamma)(x+\beta)\right)=0$.
On doit avoir $x^2\neq 0$ et $\alpha,\beta,\gamma\in\mathbb{Q}^\star$, obtient une famille de points quintiques

$$\mathcal{D}_3=\left\{\begin{array}{l}\left(x,1-\dfrac{\alpha}{x+\beta}x^2(x+\gamma)\right)\mid \alpha,\beta,\gamma\in\mathbb{Q}^*\text{ et }x\text{ racine de}\\ \\ \mathcal{F}_3(x)=4x^3(x+\beta)^2-\alpha^2x^2(x+\gamma)^2+2\alpha(x+\gamma)(x+\beta)\end{array}\right\}$$

Cas $a = 4$
Donc on a $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 4j(P) = -j(P)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1+R_2+R_3+R_4+R_5+P-6\infty$, donc $F \in \mathcal{L}(6\infty)$ et par suite $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3$, $(a_5 \neq 0)$.
Au point P, on a $F(P) = 0$ donc $a_1 + a_4 = 0$ d'où $F(x, y) = a_4(y11) + a_2x + a_3x^2 + a_5x^3$.
Aux points R_i, on a $a_4(y + 1) + a_2x + a_3x^2 + a_5x^3 = 0$, d'où $y = 1 - \dfrac{a_2}{a_4}x - \dfrac{a_3}{a_4}x^2 - \dfrac{a_5}{a_4}x^3 = 1 - \dfrac{a_5}{a_4}x(x^2 + \dfrac{a_3}{a_5}x + \dfrac{a_2}{a_5})$. On voit que y est de la forme $y = 1 - \alpha x(x^2 + \beta x + \gamma)$ avec $\alpha, \beta, \gamma \in \mathbb{Q}^\star$. Par suite on a $y^2 = 4x^5 + 1 \Leftrightarrow (1 - \alpha x(x^2 + \beta x + \gamma))^2 = 4x^5 + 1 \Leftrightarrow x\left(\alpha^2 x\left(x^2 + \beta x + \gamma\right)^2 - 4x^4 - 2\alpha\left(x^2 + \beta x + \gamma\right)\right) = 0$.
On doit avoir $x \neq 0$ et $\alpha, \beta, \gamma \in \mathbb{Q}^\star$, obtient une famille de points quintiques

$$\mathcal{D}_4 = \left\{ \begin{array}{l} (x, 1 - \alpha x(x^2 + \beta x + \gamma)) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ \mathcal{F}_4(x) = \alpha^2 x\left(x^2 + \beta x + \gamma\right)^2 - 4x^4 - 2\alpha\left(x^2 + \beta x + \gamma\right) \end{array} \right\}$$

Conclusion : L'ensemble des points quintiques sur $\mathcal{C}$ est $\mathcal{D}_0 \cup \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4$.

3.2 Courbe $\mathcal{C} : y^2 = x^5 - 243$

3.2.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K. On note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$, autrement dit $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine :

$$y^2 = x^5 - 243 \tag{3.15}$$

La courbe $\mathcal{C}$ est hyperelliptique de genre 2 et de rang nul d'après [13].
Notons $P = (3, 0)$ et $\infty = (0, 1, 0)$ le point à l'infini.
Dans [13] Mulholland a donné une description des points rationnels.
Cette description s'énonce comme suit :

Proposition 6. *Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par*

$$\mathcal{C}(\mathbb{Q}) = \{P, \infty, \} \tag{3.16}$$

Nous étendons ce résultat en donnant une description des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.
Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$, (voir [13]),

- Le théorème d'Abel Jacobi, (voir [8])
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :

Théorème.

1. L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par
$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right),\ \alpha \in \mathbb{Q} \right\}$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ est vide.
3. L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec
$$\mathcal{C}_1 = \left\{ \left(x, \pm\sqrt{\alpha^5 - 243} \right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$
$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+3))^2 \end{array} \right\}$$
4. L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec
$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\}$$
$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)[n_1 + n_2(x+3) + n_3(x^2+3x+9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ C(x) = (x-3)(n_1 + n_2(x+3) + n_3(x^2+3x+9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

3.2.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\bar{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles f sur $\mathcal{C}$ telles que $f = 0$ ou $div(f) \geq -D$; $l(D)$ désigne la $\bar{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$. On montre dans [13] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L'équation projective de la courbe $\mathcal{C}$:

$$\mathcal{C} : Y^2Z^3 = X^5 - 243Z^5 \tag{3.17}$$

On désigne par J la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Soit $\eta_1 = e^{i\frac{\Pi}{2}}$ dans $\mathbb{C}$. Posons $A_k = (0, 9\sqrt{3}\,\eta_1^{2k+1})$ pour $k \in \{0, 1\}$.
Soit $\eta_2 = e^{i\frac{2\Pi}{5}}$ dans $\mathbb{C}$. Posons $B_k = (3\eta_2^k, 0)$ pour $k \in \{0, 1, 2, 3, 4\}$.
Désignons par $\mathcal{D}.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{D}$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 4.

- $div(x-3) = 2P - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(x) = A_0 + A_1 - 2\infty$

Preuve.
Calculons seulement $div(x-3)$ et en procédant de la même manière, on trouve les autres.
On a $div(x-3) = div\left(\frac{X}{Z} - 3\right) = div\left(\frac{X-3Z}{Z}\right) = (X = 3Z).\mathcal{C} - (Z = 0).\mathcal{C}$.
Pour $X = 3Z$, on a $Y^2Z^3 = 0$ d'après (3.17), ce qui donne $Y^2 = 0$ ou $Z^3 = 0$.
D'une part pour $X = 3Z$, on a $Y^2 = 0$; pour $Z = 1$, on obtient donc le point $P = (3, 0, 1)$ avec multiplicité 2.
D'autre part pour $X = 3Z$, on a $Z^3 = 0$; pour $Y = 1$, on obtient donc le point $\infty = (0, 1, 0)$ avec multiplicité 3. D'où $(X = Z).\mathcal{C} = 2P + 3\infty$. (i)
De même pour $Z = 0$, alors on a $X^5 = 0$ d'après (3.17) ; et pour $Y = 1$, on a le point $\infty = (0, 1, 0)$ avec multiplicité 5 d'où $(Z = 0).\mathcal{C} = 5\infty$. (ii)
Les relations (i) et (ii) entraînent que $div(x-3) = 2P - 2\infty$.

Conséquence du lemme 4 : $2j(P) = 0$.

Lemme 5. .

- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\ x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\ x,\ x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1,\ x,\ x^2,\ y \rangle$
- $\mathcal{L}(6\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3 \rangle$

Preuve. C'est une conséquence du lemme 5 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 6. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P - \infty] \rangle = \{a\,[P - \infty], a \in \{0, 1\}\}$.

Preuve.(voir [13])

3.2.3 Démonstration du théorème

a) **Points quadratiques sur $\mathcal{C}$**
L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{\left(\alpha, \pm\sqrt{\alpha^5 - 243}\right),\ \alpha \in \mathbb{Q}\right\}$$

Preuve :
Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Notons R_1, R_2 les conjugués de Galois de R.Travaillons avec $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 - 2\infty] = a\,[P - \infty],\ a \in \{0, 1\} \quad (*)$$

On remarque que $R \notin \{\infty, P\}$.
On a les deux cas suivants :
Premier cas : $a = 0$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty \tag{3.18}$$

donc $F \in \mathcal{L}(2\infty)$, d'où $F(x, y) = a_1 + a_2 x$ avec $a_2 \neq 0$ sinon un des R_i devrait être à ∞. En effet si $a_2 = 0$ alors $F \in \mathcal{L}(\infty)$, ce qui est absurde.
Aux points R_i, on a $a_1 + a_2 x = 0$ donc $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}$.
En remplaçant x par α dans (3.15), on a :

$$y^2 = \alpha^5 - 243 \tag{3.19}$$

et par suite on a :

$$y = \pm\sqrt{\alpha^5 - 243} \tag{3.20}$$

On a ainsi une famille de points quadratiques

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right),\ \alpha \in \mathbb{Q} \right\}$$

Deuxième cas : $a = 1$
La relation $(*)$ donne $[R_1 + R_2 + P - 3\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty \tag{3.21}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ alors un des R_i devrait être égal à ∞, ce qui est absurde.

Conclusion : L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par $\mathcal{S}$.

b) **Points cubiques sur $\mathcal{C}$**
Il n'existe pas de points cubiques sur $\mathcal{C}$.

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 - 3\infty] = a\,[P - \infty],\ a \in \{0, 1\} \quad (**)$$

On remarque que $R \notin \{\infty, P\}$.
On a les deux cas suivants :
Premier cas : $a = 0$
La relation $(**)$ devient $[R_1 + R_2 + R_3 - 3\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 - 3\infty \tag{3.22}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ alors un des R_i devrait être égal à ∞, ce qui est absurde.
Deuxième cas : $a = 1$
La relation $(**)$ devient $[R_1 + R_2 + R_3 + P - 4\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + P - 4\infty \tag{3.23}$$

donc $F \in \mathcal{L}(4\infty)$, d'où $F(x,y) = a_1 + a_2x + a_3x^2, \quad (a_3 \neq 0)$.
Au point P, on a : $a_1 + 3a_2 + 9a_3 = 0$, donc $a_1 = -3a_2 - 9a_3$ et en remplaçant a_1 par son expression dans $F(x,y)$ on a :

$$F(x,y) = -3a_2 - 9a_3 + a_2x + a_3x^2 \tag{3.24}$$

$$F(x,y) = a_2(x-3) + a_3\left(x^2 - 9\right) \tag{3.25}$$

$$F(x,y) = (x-3)\left[a_2 + a_3(x+3)\right] \tag{3.26}$$

Aux points R_i , on a $(x-3)\left[a_2 + a_3(x+3)\right] = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.

Conclusion : L'ensemble des points cubiques sur $\mathcal{C}$ est vide.

c) **Points quartiques sur $\mathcal{C}$**
L'ensemble des points quartiques sur $\mathcal{C}$ est couvert par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec

$$\mathcal{C}_1 = \left\{\left(x, \pm\sqrt{x^5 - 243}\right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\right\}$$

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+3))^2 \end{array} \right\}$$

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 4$. Notons R_1, R_2, R_3, R_4 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 + R_4 - 4\infty] = a[P - \infty],\ a \in \{0,1\} \quad (***)$$

On remarque que $R \notin \{\infty, P\}$.
On a les deux cas suivants :
Premier cas : $a = 0$
La relation $(***)$ devient $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty \tag{3.27}$$

donc $F \in \mathcal{L}(4\infty)$, d'où $F(x,y) = a_1 + a_2x + a_3x^2$ avec $a_3 \neq 0$ sinon un des R_i devrait etre ∞. Aux points R_i, on a : $a_1 + a_2x + a_3x^2 = 0$; la relation $y^2 = x^5 - 243$ donne

$$y = \pm\sqrt{x^5 - 243}. \tag{3.28}$$

On trouve ainsi une famille de points quartiques

$$\mathcal{C}_1 = \left\{ \left(x, \pm\sqrt{x^5 - 243} \right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

Deuxième cas : $a = 1$
La relation $(***)$ donne $[R_1 + R_2 + R_3 + R_4 + P - 5\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = [R_1 + R_2 + R_3 + R_4 + P - 5\infty] \tag{3.29}$$

donc $F \in \mathcal{L}(5\infty)$, d'où $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y, \quad (a_4 \neq 0)$.
Au point P, on a : $a_1 + 3a_2 + 9a_3 = 0$, donc $a_1 = -3a_2 - 9a_3$ et en remplaçant a_1 par son expression dans $F(x, y)$ on a :

$$F(x, y) = -3a_2 - 9a_3 + a_2 x + a_3 x^2 + a_4 y \tag{3.30}$$

$$F(x, y) = a_2 (x - 3) + a_3 \left(x^2 - 9 \right) + a_4 y \tag{3.31}$$

$$F(x, y) = (x - 3)(a_2 + a_3(x + 3)) + a_4 y \tag{3.32}$$

Aux points R_i on a $(x - 3)(a_2 + a_3(x + 3)) + a_4 y = 0$, donc y est de la forme $y = (x - 3)(\lambda_1 + \lambda_2(x + 3))$ avec $\lambda_1, \lambda_2 \in \mathbb{Q}$.
La relation $y^2 = x^5 - 243 \Leftrightarrow (x - 3)^2 (\lambda_1 + \lambda_2(x + 3))^2 = x^5 - 243$

$$(x - 3)^2 (\lambda_1 + \lambda_2(x + 3))^2 = (x - 3)(x^4 + 3x^3 + 9x^2 + 27x + 81) \tag{3.33}$$

En simplifiant par $x - 3$ et en développant on obtient

$$(x - 3)(\lambda_1 + \lambda_2(x + 3))^2 = x^4 + 3x^3 + 9x^2 + 27x + 81 \tag{3.34}$$

$$x^4 + 3x^3 + 9x^2 + 27x + 81 - (x - 3)(\lambda_1 + \lambda_2(x + 3))^2 = 0 \tag{3.35}$$

On trouve ainsi une famille de points quartiques

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x - 3)(\lambda_1 + \lambda_2(x + 3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x - 3)(\lambda_1 + \lambda_2(x + 3))^2 \end{array} \right\}$$

Conclusion : L'ensemble des points quartiques sur $\mathcal{C}$ est couvert par $\mathcal{C}_1 \cup \mathcal{C}_2$.

d) **Points quintiques sur $\mathcal{C}$**
L'ensemble des points quintiques sur $\mathcal{C}$ est couvert par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\}$$

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x - 3)[n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ C(x) = (x - 3)(n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 5$. Notons R_1, R_2, R_3, R_4, R_5 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = a\,[P - \infty]\,,\ a \in \{0, 1\} \quad (***)$$

On remarque que $R \notin \{\infty, P\}$.
On a les deux cas suivants :
Premier cas : $a = 0$
La relation $(***)$ devient $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty \tag{3.36}$$

donc $F \in \mathcal{L}(5\infty)$, d'où $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y, \quad (a_4 \neq 0)$.
Aux points R_i, on a : $a_1 + a_2x + a_3x^2 + a_4y = 0$, donc $y = \alpha_1 + \alpha_2x + \alpha_3x^2$ avec $\alpha_1 = \frac{-a_1}{a_4}$, $\alpha_2 = \frac{-a_2}{a_4}$ et $\alpha_3 = \frac{-a_3}{a_4}$.
En remplaçant y par son expression dans (3.15), on a :

$$x^5 - 243 = \alpha_1^2 + \alpha_2^2x + \alpha_3^2x^4 + 2\alpha_1\alpha_2x + 2\alpha_1\alpha_3x^2 + 2\alpha_2\alpha_3x^3 \tag{3.37}$$

$$3x^5 - \alpha_3^2x^4 - 2\alpha_2\alpha_3x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2x - (\alpha_1^2 + 243) = 0 \tag{3.38}$$

On trouve ainsi une famille de points quintiques

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2x + \alpha_3x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ B(x) = x^5 - \alpha_3^2x^4 - 2\alpha_2\alpha_3x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2x - (\alpha_1^2 + 243) \end{array} \right\}$$

Deuxième cas : $a = 1$
La relation $(***)$ donne $[R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty \tag{3.39}$$

donc $F \in \mathcal{L}(6\infty)$, d'où $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3, \quad (a_5 \neq 0)$.
Au point P, on a : $a_1 + 3a_2 + 9a_3 + 27a_5 = 0$, donc $a_1 = -3a_2 - 9a_3 - 27a_5$ et en remplaçant a_1 par son expression dans $F(x, y)$ on a :

$$F(x, y) = -3a_2 - 9a_3 - 27a_5 + a_2x + a_3x^2 + a_4y + a_5x^3 \tag{3.40}$$

$$F(x, y) = a_2(x - 3) + a_3(x^2 - 9) + a_5(x^3 - 27) + a_4y \tag{3.41}$$

Aux points R_i, on a : $a_2(x-3) + a_3(x^2-9) + a_5(x^3-27) + a_4y = 0$, donc y est de la forme $y = n_1(x - 3) + n_2(x^2 - 9) + n_3(x^3 - 27)$ avec $n_1, n_2, n_3 \in \mathbb{Q}^\star$.
Finalement on a :

$$y = (x - 3)\left(n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9)\right) \tag{3.42}$$

En remplaçant y par son expression dans (1), on a :

$$(x - 3)^2\left(n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9)\right)^2 = x^5 - 243 \tag{3.43}$$

$$(x-3)^2\left(n_1+n_2(x+3)+n_3(x^2+3x+9)\right)^2=(x-3)(x^4+3x^3+9x^2+27x+81) \quad (3.44)$$

En simplifiant par $x-3$, on obtient

$$(x-3)\left(n_1+n_2(x+3)+n_3(x^2+3x+9)\right)^2-(x^4+3x^3+9x^2+27x+81)=0 \quad (3.45)$$

On trouve ainsi une famille de points quintiques

$$\mathcal{A}_2=\left\{\begin{array}{l}(x,(x-3)\left[n_1+n_2(x+3)+n_3(x^2+3x+9)\right])\mid n_1,n_2,n_3\in\mathbb{Q}^\star \text{ et } x \text{ racine de}\\ \\ C(x)=(x-3)\left(n_1+n_2(x+3)+n_3(x^2+3x+9)\right)^2-(x^4+3x^3+9x^2+27x+81)\end{array}\right\}$$

Conclusion : L'ensemble des points quintiques de $\mathcal{C}$ est couvert par $\mathcal{A}_1\cup\mathcal{A}_2$.

3.3 Courbe $\mathcal{C}: y^2=3x(x^4+3)$

3.3.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique définie sur un corps de nombres K. On note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup\limits_{[K:\mathbb{Q}]\leq d}\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$, autrement dit $deg(R)=[\mathbb{Q}(R):\mathbb{Q}]$.
Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine :

$$\mathcal{C}: y^2=3x(x^4+3) \quad (3.46)$$

La courbe est hyperelliptique de genre $g=2$ et de rang nul d'après Bruin (voir [2]).
Notons : $P=(0,0)$ et $\infty=(0,1,0)$ le point à l'infini.
Dans [2] Bruin a donné une description des points rationnels.
Cette description s'énonce comme suit :

Proposition 7. *Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par*

$$\mathcal{C}(\mathbb{Q})=\{P,\infty\} \quad (3.47)$$

Nous étendons ce résultat en donnant une description des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.
Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ (voir [2]),
- Le théorème d'Abel Jacobi, (voir [8]),
- L'étude des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :
Théorème.

1. L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par
$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{3\alpha(\alpha^4+3}\right),\ \alpha \in \mathbb{Q}^* \right\}$$
2. L'ensemble des points cubiques sur $\mathcal{C}$ est vide.
3. L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec
$$\mathcal{C}_1 = \left\{ \left(x, \pm\sqrt{3\alpha(\alpha^4+3}\right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x):\mathbb{Q}] = 2 \right\}$$
$$\mathcal{C}_2 = \left\{ (x, x(\lambda_1 + \lambda_2 x)\ \mid \lambda_1, \lambda_2 \in \mathbb{Q}^\star, x \textit{ racine de } \mathcal{F}(x) = 3(x^4+3) - x\left(\lambda_1 + \lambda_2 x\right)^2 \right\}$$
4. L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec
$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{G}(x) = (\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 - 3x(x^4+3) \end{array} \right\}$$
$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, n_1 x + n_2 x^2 + n_3 x^3) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{H}(x) = x(n_1 + n_2 x + n_3 x^2)^2 - 3(x^4+3) \end{array} \right\}$$

3.3.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\bar{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles F sur $\overline{\mathbb{Q}}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\bar{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$. On montre dans [2] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :
$$x(X,Y,Z) = \frac{X}{Z} \qquad et \qquad y(X,Y,Z) = \frac{Y}{Z}.$$
L'équation projective de la courbe $\mathcal{C}$ est :
$$\mathcal{C} : Y^2Z^3 = 3X(X^4 + 3Z^4) \tag{3.48}$$
On désigne par J la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P-\infty]$ de $P-\infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Soit $\eta = e^{i\frac{\Pi}{4}}$ dans $\mathbb{C}$. Posons $C_k = ({}^4\sqrt{3}\,\eta^{2k+1}, 0)$ pour $k \in \{0,1,2,3\}$.
Désignons par $\mathcal{D}.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{D}$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 7.

- $div(x) = 2P - 2\infty$
- $div(y) = P + C_0 + C_1 + C_2 + C_3 - 5\infty$

Preuve. Il s'agit d'un simple calcul du type
$$div(x-a) = (X - aZ = 0).\mathcal{C} - (Z = 0).\mathcal{C} \tag{3.49}$$
Par exemple $div(x) = (X=0).\mathcal{C} - (Z=0).\mathcal{C}$.
On a $(X=0).\mathcal{C} = 2P + 3\infty$ et $(Z=0).\mathcal{C} = 5\infty$, d'où $div(x) = 2P - 2\infty$

Lemme 8. .
- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\ x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\ x,\ x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1,\ x,\ x^2,\ y \rangle$
- $\mathcal{L}(6\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3 \rangle$

Preuve. C'est une conséquence du lemme 7 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 9. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle 0, [(0,0) - \infty] \rangle = \{b\,[P - \infty]\,, b \in \{0,1\}\}$.

Preuve.(voir [2])

3.3.3 Démonstration du théorème

a) **Points quadratiques sur $\mathcal{C}$**

L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{3\alpha(\alpha^4+3}\right),\ \alpha \in \mathbb{Q}^* \right\}.$$

Preuve :

Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Notons R_1, R_2 les conjugués de Galois de R. $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 - 2\infty] = b\,[P - \infty]\,,\ \ 0 \leq b \leq 1 \quad (*)$$

On remarque que $R \notin \{P, \infty\}$.

Premier cas : $b = 0$

La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 0$.

Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty \tag{3.50}$$

donc $F \in \mathcal{L}(2\infty)$, d'où $F(x,y) = a_1 + a_2 x,\ \ (a_2 \neq 0)$.

Aux points R_i, on doit avoir $a_1 + a_2 x = 0$ donc $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}^*$.

En remplaçant x par son expression dans (3.46), on a :

$$y^2 = 3\alpha(\alpha^4 + 3) \tag{3.51}$$

et par suite on a :

$$y = \pm\sqrt{3\alpha(\alpha^4+3)} \tag{3.52}$$

On a ainsi une famille de points quadratiques

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{3\alpha(\alpha^4+3}\right),\ \alpha \in \mathbb{Q}^* \right\} \tag{3.53}$$

Deuxième cas : $b = 1$
La relation $(*)$ donne $[R_1 + R_2 + P - 3\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty \tag{3.54}$$

donc $F \in \mathcal{L}(3\infty)$ et comme$\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, un des R_i est devrait être égal à ∞ ; ce qui est absurde.

Conclusion : L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par $\mathcal{S}$.

b) **Points cubiques sur $\mathcal{C}$**
L'ensemble des points cubiques sur $\mathcal{C}$ est vide.

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R. $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 - 3\infty] = b[P - \infty], \ \ 0 \leq b \leq 1 \qquad (**)$$

On remarque que $R \notin \{P, \infty\}$.
Premier cas : $b = 0$
La relation $(**)$ devient $[R_1 + R_2 + R_3 - 3\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 - 3\infty \tag{3.55}$$

donc $F \in \mathcal{L}(3\infty)$ et comme$\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, un des R_i devrait être égal à ∞ ; ce qui est absurde.
Deuxième cas : $b = 1$
La relation $(**)$ donne $[R_1 + R_2 + R_3 + P - 4\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + P - 4\infty \tag{3.56}$$

donc $F \in \mathcal{L}(4\infty)$, d'où $F(x, y) = a_1 + a_2x + a_3x^2 \quad (a_3 \neq 0)$.
Au point P on a $a_1 = 0$ et par suite on a

$$F(x, y) = x(a_2 + a_3x) \tag{3.57}$$

Aux points R_i , on a $x(a_2 + a_3x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.

Conclusion : L'ensemble des points cubiques sur $\mathcal{C}$ est vide.

c) **Points quartiques sur $\mathcal{C}$**
L'ensemble des points quartiques sur $\mathcal{C}$ est $\mathcal{C}_1 \cup \mathcal{C}_2$ avec

$$\mathcal{C}_1 = \left\{ \left(x, \pm\sqrt{3x(x^4 + 3)} \right) \mid x \in \mathbb{Q}, \ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

$$\mathcal{C}_2 = \left\{(x, x(\lambda_1 + \lambda_2 x) \mid \lambda_1, \lambda_2 \in \mathbb{Q}^\star, x \text{ racine de } \mathcal{F}(x) = 3(x^4+3) - x\left(\lambda_1 + \lambda_2 x\right)^2\right\}$$

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 4$. Notons R_1, R_2, R_3, R_4 les conjugués de Galois de R. $t = [R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 + R_4 - 4\infty] = b\,[P - \infty]\,, \;\; 0 \leq b \leq 1 \qquad (***)$$

On remarque que $R \notin \{P, \infty\}$.
Premier cas : $b = 0$
La relation $(***)$ devient $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty \tag{3.58}$$

donc $F \in \mathcal{L}(4\infty)$, d'où $F(x,y) = a_1 + a_2 x + a_3 x^2, \quad (a_3 \neq 0)$.
Aux points R_i, on a : $a_1 + a_2 x + a_3 x^2 = 0$; la relation $y^2 = 3x(x^4+3)$ donne

$$y = \pm\sqrt{3x(x^4+3)}. \tag{3.59}$$

On trouve ainsi une famille de points quartiques

$$\mathcal{C}_1 = \left\{\left(x, \pm\sqrt{3x(x^4+3)}\right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\right\} \tag{3.60}$$

Deuxième cas : $b = 1$
La relation $(***)$ donne $[R_1 + R_2 + R_3 + R_4 + P - 5\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = [R_1 + R_2 + R_3 + R_4 + P - 5\infty] \tag{3.61}$$

donc $F \in \mathcal{L}(5\infty)$, d'où $F(x,y) = a_1 + a_2 x + a_3 x^2 + a_4 y, \quad (a_4 \neq 0)$ et comme $\mathrm{ord}_{P_1}(F) = 1$, on doit avoir $a_1 = 0$ et on a par suite on a

$$F(x,y) = x(a_2 + a_3 x) + a_4 y \tag{3.62}$$

Aux points R_i, on a $y = x(\lambda_1 + \lambda_2 x)$ avec $\lambda_1 = \frac{-a_2}{a_4}$ et $\lambda_2 = \frac{-a_3}{a_4}$ avec $\lambda_1, \lambda_2 \in \mathbb{Q}^\star$.
En remplaçant y par son expression dans (3.46), on a :

$$3x(x^4+3) - \left(x(\lambda_1 + \lambda_2 x)\right)^2 = 0 \tag{3.63}$$

$$x\left(3(x^4+3) - x\left(\lambda_1 + \lambda_2 x\right)^2\right) = 0 \tag{3.64}$$

On doit avoir $x \neq 0$ et $\lambda_1, \lambda_2 \in \mathbb{Q}^\star$, on obtient une famille de points quartiques donnée par

$$\mathcal{C}_2 = \left\{(x, x(\lambda_1 + \lambda_2 x) \mid \lambda_1, \lambda_2 \in \mathbb{Q}^\star, x \text{ racine de } \mathcal{F}(x) = 3(x^4+3) - x\left(\lambda_1 + \lambda_2 x\right)^2\right\}$$

Conclusion : L'ensemble des points quartiques de $\mathcal{C}$ est couvert par $\mathcal{C}_1 \cup \mathcal{C}_2$.

d) **Points quintiques sur $\mathcal{C}$**

L'ensemble des points quintiques sur $\mathcal{C}$ est $\mathcal{A}_1 \cup \mathcal{A}_2$ avec

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{G}(x) = (\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 - 3x(x^4+3) \end{array} \right\}$$

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, n_1 x + n_2 x^2 + n_3 x^3) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{H}(x) = x(n_1 + n_2 x + n_3 x^2)^2 - 3(x^4+3) \end{array} \right\}$$

Preuve :

Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 5$. Notons R_1, R_2, R_3, R_4, R_5 les conjugués de Galois de R. $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$$t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = b\,[P - \infty]\,, \;\; 0 \leq b \leq 1 \qquad (***)$$

On remarque que $R \notin \{P, \infty\}$. On a les deux cas suivants :

Premier cas : $b = 0$

La relation $(***)$ devient $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 0$.

Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty \tag{3.65}$$

donc $F \in \mathcal{L}(5\infty)$, d'où $F(x,y) = a_1 + a_2 x + a_3 x^2 + a_4 y, \quad (a_4 \neq 0)$.

Aux points R_i, on a : $a_1 + a_2 x + a_3 x^2 + a_4 y = 0$, donc $y = \alpha_1 + \alpha_2 x + \alpha_3 x^2$ avec $\alpha_1 = \frac{-a_1}{a_4}$, $\alpha_2 = \frac{-a_2}{a_4}$ et $\alpha_3 = \frac{-a_3}{a_4}$ avec $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star$.

En remplaçant y par son expression dans (3.46), on a :

$$(\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 = 3x(x^4+3) \tag{3.66}$$

$$(\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 - 3x(x^4+3) = 0 \tag{3.67}$$

On trouve ainsi une famille de points quintiques donnée par

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{G}(x) = (\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 - 3x(x^4+3) \end{array} \right\}$$

Deuxième cas : $b = 1$

La relation $(*)$ donne $[R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty] = 0$.

Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty \tag{3.68}$$

donc $F \in \mathcal{L}(6\infty)$, d'où $F(x,y) = a_1 + a_2 x + a_3 x^2 + a_4 y + a_5 x^3, \quad (a_5 \neq 0)$.

Au point P, on a : $a_1 = 0$ et par suite on a

$$F(x,y) = a_2 x + a_3 x^2 + a_4 y + a_5 x^3 \tag{3.69}$$

Aux points R_i, on a : $a_2x + a_3x^2 + a_4y + a_5x^3 = 0$, donc $y = n_1x + n_2x^2 + n_3x^3$ avec $n_1 = \frac{-a_2}{a_4}$, $n_2 = \frac{-a_3}{a_4}$ et $n_3 = \frac{-a_5}{a_4}$ avec $n_1, n_2, n_3 \in \mathbb{Q}^\star$.
En remplaçant y par son expression dans (3.46), on a :

$$(n_1x + n_2x^2 + n_3x^3)^2 = 3x(x^4 + 3) \tag{3.70}$$

$$(n_1x + n_2x^2 + n_3x^3)^2 - 3x(x^4 + 3) = 0 \tag{3.71}$$

$$x\left(x(n_1 + n_2x + n_3x^2)^2 - 3(x^4 + 3)\right) = 0 \tag{3.72}$$

On doit avoir $x \neq 0$ et $n_1, n_2, n_3 \in \mathbb{Q}^\star$, on obtient une famille de points quintiques donnée par

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, n_1x + n_2x^2 + n_3x^3) \mid n_1, n_2, n_3 \in \mathbb{Q}^\star \text{ et } x \text{ racine de} \\ \\ \mathcal{H}(x) = x(n_1 + n_2x + n_3x^2)^2 - 3(x^4 + 3) \end{array} \right\}$$

Conclusion : L'ensemble des points quintiques de $\mathcal{C}$ est couvert par $\mathcal{A}_1 \cup \mathcal{A}_2$

Chapitre 4

Paramétrisation des points algébriques sur certaines courbes

Dans ce chapitre, nous donnons une paramétrisation des points algébriques de petits degrés sur chacune des courbes d'équation affines $y^2 = x^5 + 20736$ et $y^2 + y = x^5$. Nous déterminons aussi les points algébriques de degré quelconque sur chacune des courbes d'équations affines
$y^2 = x(x^2 + 1)(x^2 + 3)$ et $y^2 = 3(x^5 - 1)$.

4.1 Courbe $\mathcal{C} : y^2 = x^5 + 20736$

4.1.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K. On note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$, autrement dit $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine :

$$y^2 = x^5 + 20736 \tag{4.1}$$

La courbe $\mathcal{C}$ est hyperelliptique de genre 2 d'après Siksek et Stoll dans [20].
Notons $P = (0, 144),\ \bar{P} = (0, -144)$ *et* ∞ le point à l'infini.
Dans [20] Siksek et Stoll ont donné une description des points rationnels.
Cette description s'énonce comme suit :

Proposition 8. *Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par*

$$\mathcal{C}(\mathbb{Q}) = \left\{P,\ \bar{P},\ \infty\right\} \tag{4.2}$$

Nous étendons ce résultat en donnant une description des points algébriques de degrés au-plus 3 sur $\mathbb{Q}$.
Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$, (voir dans [20]),
- Le théorème d'Abel Jacobi, (voir dans [8]),
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :
Théorème.

1. L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. L'ensemble des points cubiques sur $\mathcal{C}$ est donné par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -144 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \ et\ x\ racine\ de\ E_1(x) = x^3 - \alpha^2 x^2 - 288\alpha \right\}$$

$$\mathcal{B} = \left\{ (x, -144 - \alpha x^3) |\ \alpha \in \mathbb{Q}^* \ et\ x\ racine\ de\ E_2(x) = \alpha^2 x^3 - x^2 + 288\alpha \right\}$$

4.1.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\overline{\mathbb{Q}}-$ espace vectoriel des fonctions rationnelles F sur $\mathcal{C}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\overline{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$. On montre dans [20] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.
Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L'équation projective de la courbe $\mathcal{C}$ est :

$$\mathcal{C} : Y^2 Z^3 = X^5 + 20736 Z^5 \tag{4.3}$$

On désigne par J la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Soit $\eta = e^{i\frac{\Pi}{5}}$ dans $\mathbb{C}$. Posons $B_k = (\sqrt[5]{20736}\ \eta^{2k+1}, 0)$ pour $k \in \{0, 1, 2, 3, 4\}$.
Désignons par $\mathcal{C}'.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{C}'$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 10.

- $div(x) = P + \bar{P} - 2\infty$
- $div(y - 144) = 5P - 5\infty$
- $div(y + 144) = 5\bar{P} - 5\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$

Preuve.
Calculons seulement $div(x)$ et en procédant de la même manière, on trouve les autres.
On a $div(x) = div(\frac{X}{Z}) = (X = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
Pour $X = 0$, on a $Y^2Z^3 = 20736Z^5$ d'après (4.3), ce qui donne $Z^3 = 0$ ou $Y^2 = (144Z)^2$.
D'une part pour $X = 0$, on a $Z^3 = 0$ avec $Y = 1$. On obtient donc le point $\infty = (0, 1, 0)$ avec multiplicité 3.
D'autre part pour $X = 0$, on a $Y = 144Z$ ou $Y = -144Z$ avec $Z = 1$. On obtient donc les points $P = (0, 144, 1)$ avec multiplicité 1 et $\bar{P} = (0, -144, 1)$ avec multiplicité 1. D'où $(X = 0).\mathcal{C} = P + \bar{P} + 3\infty$. (i)
De même pour $Z = 0$, alors on a $X^5 = 0$ d'après (4.3) ; et pour $Y = 1$, on a le point $\infty = (0, 1, 0)$ avec multiplicité 5 d'où $(Z = 0).\mathcal{C} = 5\infty$. (ii)
Les relations (i) et (ii) entraînent que $div(x) = P + \bar{P} - 2\infty$.

Conséquences du lemme 10 : $5j(P) = 5j\left(\bar{P}\right) = 0$ et $j(P) + j\left(\bar{P}\right) = 0$.

Lemme 11. .
- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\ x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\ x,\ x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1,\ x,\ x^2,\ y \rangle$
- $\mathcal{L}(6\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3 \rangle$
- $\mathcal{L}(7\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3,\ xy \rangle$
- *De façon générale, pour $m \geq 3$, une $\mathbb{Q}$-base de $\mathcal{L}(m\infty)$ est donné par :*

$$\mathcal{B}_m = \{x^i \mid i \in \mathbb{N} \text{ et } i \leq \frac{m}{2}\} \cup \{x^j y \mid j \in \mathbb{N} \text{ et } j \leq \frac{m-5}{2}\} \tag{4.4}$$

Preuve.
Si $m \leq 2g - 2 = 2$, la réponse est évidente.
Il est clair que $\mathcal{B}_m$ est libre et il reste à montrer que $card(\mathcal{B}_m) = dim(\mathcal{L}(m\infty))$.
D'après le théorème de Riemann-Roch, on a $dim(\mathcal{L}(m\infty)) = m - g + 1$ si $m \geq 2g - 1$.
Selon la parité de m, on a les deux cas suivants :
Cas 1 : supposons que m est pair et posons $m = 2h$. Ainsi on a

$$i \leq \frac{m}{2} = h \ \text{ et } \ j \leq \frac{2h-5}{2} \Leftrightarrow j \leq \frac{2h-5-1}{2} = h - 3 = h - g - 1.$$

On obtient alors $\mathcal{B}_m = \{1,\ x,\ ...,\ x^h\} \cup \left\{y,\ yx\ ...,\ yx^{h-g-1}\right\}$ d'où on a

$$card(\mathcal{B}_m) = h + 1 + (h - g - 1 + 1) = 2h + 1 - g = m + 1 - g = dim(\mathcal{L}(m\infty))$$

Cas 2 : supposons que m est impair et posons $m = 2h + 1$. Ainsi on a

$$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h \ \text{ et } \ j \leq \frac{m-5}{2} \Leftrightarrow j \leq \frac{2h+1-5}{2} = h - g.$$

On obtient alors $\mathcal{B}_m = \{1,\ x,\ ...,\ x^h\} \cup \left\{y,\ yx\ ...,\ yx^{h-g}\right\}$ d'où on a

$$card(\mathcal{B}_m) = h + 1 + (h - g + 1) = m + 1 - g = dim(\mathcal{L}(m\infty))$$

Lemme 12. $J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} = \langle [P - \infty] \rangle = \{a[P - \infty], a \in \{0, 1, 2, 3, 4\}\}$.

Preuve.(voir [20])

4.1.3 Démonstration du théorème

a) **Points quadratiques sur $\mathcal{C}$**

L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

Preuve :

Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Notons R_1, R_2 les conjugués de Galois de R.
$t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, d'où

$$t = [R_1 + R_2 - 2\infty] = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4 \quad (*)$$

On remarque que $R \notin \left\{ \infty, P, \bar{P} \right\}$.

Cas $a = 0$

La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty \tag{4.5}$$

donc $F \in \mathcal{L}(2\infty)$, d'où $F(x, y) = a_1 + a_2 x$ avec $(a_2 \neq 0)$ sinon un des R_i devrait être égal à ∞.
Aux points R_i, on a $a_1 + a_2 x = 0$ donc $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}^*$.
En remplaçant x par son expression dans (4.1), on a :

$$y^2 = \alpha^5 + 20736 \tag{4.6}$$

et par suite on a :

$$y = \pm\sqrt{\alpha^5 + 20736} \tag{4.7}$$

On a ainsi une famille de points quadratiques donnée par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}$$

Cas $a = 1$

La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = j(P) = -j(\bar{P})$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \bar{P} - 3\infty \tag{4.8}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, $\bar{P}$ devrait être égal à ∞ ; ce qui est absurde.

Cas $a = 2$

La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 2j(P) = -2j(\bar{P})$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2\bar{P} - 4\infty \tag{4.9}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2$ avec $a_3 \neq 0$ sinon un des R_i devrait être égal à ∞. La fonction F est d'ordre 2 au point $\bar{P}$ donc on doit avoir $a_1 = a_2 = 0$,

donc $F(x,y) = a_3x^2$ et on devrait avoir $R_1 = R_2 = P$, ce qui est absurde.
Cas $a = 3$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 3j(P) = -2j(P)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2P - 4\infty \tag{4.10}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x,y) = a_1 + a_2x + a_3x^2$ avec $a_3 \neq 0$ sinon un des R_i devrait être égal à ∞. La fonction F est d'ordre 2 au point P donc $a_1 = a_2 = 0$, donc $F(x,y) = a_3x^2$ et on devrait avoir $R_1 = R_2 = \bar{P}$, ce qui est absurde.
Cas $a = 4$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 4j(P) = -j(P)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty \tag{4.11}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P devrait être égal à ∞ ; ce qui est absurde.
Conclusion : L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

b) **Points cubiques sur $\mathcal{C}$**
L'ensemble des points cubiques sur $\mathcal{C}$ est donné par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -144 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_1(x) = x^3 - \alpha^2x^2 - 288\alpha \right\}$$

$$\mathcal{B} = \left\{ (x, -144 - \alpha x^3) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_2(x) = \alpha^2x^3 - x^2 + 288\alpha \right\}$$

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R et travaillons avec $t = [R_1 + R_2 + R_3 - 3\infty]$ qui est un point de $J(\mathbb{Q}) = \{aj(P),\ 0 \leq a \leq 4\}$, donc $t = aj(P) = -aj(\bar{P}),\ 0 \leq a \leq 4$.
On remarque que $R \notin \left\{ \infty, P, \bar{P} \right\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 0$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 - 3\infty$, donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, alors un des R_i devrait être égal à ∞, ce qui est absurde.
Cas $a = 1$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = j(P) = -j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + \bar{P} - 4\infty$, donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x,y) = a_1 + a_2x + a_3x^2$ avec $a_3 \neq 0$ sinon un des R_i devrait être égal à ∞.
Au point $\bar{P}$ on a $F(\bar{P}) = 0$ donc $a_1 = 0$ d'où $F(x,y) = x(a_2 + a_3x)$. Aux points R_i on a $x(a_2 + a_3x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.
Cas $a = 2$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 2j(P) = -2j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 2\bar{P} - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x,y) = a_1 + a_2x + a_3x^2 + a_4y$ avec $a_4 \neq 0$ sinon un des R_i devrait être égal à ∞.

La fonction F est d'ordre 2 au point $\bar{P}$ donc $a_1 - 144a_4 = 0$ et $a_2 = 0$ d'où $F(x,y) = a_4(y+144) + a_3x^2$.
Aux points R_i on doit avoir $a_4(y+144) + a_3x^2 = 0$, d'où $y = -144 - \frac{a_3}{a_4}x^2$. On voit que y est de la forme $y = -144 - \alpha x^2$ avec $\alpha \in \mathbb{Q}^*$ sinon un des R_i devrait être égal à $\bar{P}$, et par suite on a $y^2 = x^5 + 20736 \Leftrightarrow (-144 - \alpha x^2)^2 = x^5 + 20736 \Leftrightarrow x^5 - \alpha^2x^4 - 288\alpha x^2 = 0 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - 288\alpha) = 0$.
On doit avoir $x^2 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques donnée par

$$\mathcal{A} = \left\{(x, -144 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_1(x) = x^3 - \alpha^2x^2 - 288\alpha\right\}$$

Cas $a = 3$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 3j(P) = -3j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 3\bar{P} - 6\infty$, donc $F \in \mathcal{L}(6\infty)$ et par suite $F(x,y) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3$ avec $a_5 \neq 0$ sinon un des R_i devrait être égal à ∞.
La fonction F est d'ordre 3 au point $\bar{P}$ donc $a_1 - 144a_4 = 0$ et $a_2 = a_3 = 0$ d'où $F(x,y) = a_4(y+144) + a_5x^3$.
Aux points R_i on doit avoir $a_4(y+144) + a_5x^3 = 0$, d'où $y = -144 - \frac{a_5}{a_4}x^3$. On voit que y est de la forme $y = -144 - \alpha x^3$ avec $\alpha \in \mathbb{Q}^*$ sinon un des R_i devrait être égal à $\bar{P}$, et par suite on a $y^2 = x^5 + 20736 \Leftrightarrow (-144 - \alpha x^3)^2 = x^5 + 20736 \Leftrightarrow \alpha^2x^6 - x^5 + 288\alpha x^3 = 0 \Leftrightarrow x^3(\alpha^2x^3 - x^2 + 288\alpha) = 0$.
On doit avoir $x^3 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques donnée par

$$\mathcal{B} = \left\{(x, -144 - \alpha x^3) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } E_2(x) = \alpha^2x^3 - x^2 + 288\alpha\right\}$$

Cas $a = 4$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 4j(P) = -4j(\bar{P})$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 4\bar{P} - 7\infty$, donc $F \in \mathcal{L}(7\infty)$ et par suite $F = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3 + a_6xy$ avec $a_6 \neq 0$ sinon un des R_i devrait être égal à ∞.
La fonction F est d'ordre 4 au point $\bar{P}$ donc $a_1 - 144a_4 = 0$, $a_2 - 144a_6 = 0$ et $a_3 = a_5 = 0$ d'où $F(x,y) = a_4(y+144) + a_6x(y+144)$ et par suite un des R_i devrait être égal à $\bar{P}$, ce qui est absurde.

Conclusion : L'ensemble des points cubiques sur $\mathcal{C}$ est donné par $\mathcal{A} \cup \mathcal{B}$.

4.2 Courbe $\mathcal{C} : y^2 + y = x^5$

4.2.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique lisse de genre g définie sur un corps de nombres K. L'ensemble des points algébriques sur $\mathcal{C}$ définis sur K est noté $\mathcal{C}(K)$ et $\bigcup_{[K:\mathbb{Q}]\leq d}\mathcal{C}(K)$ est l'ensemble des points algébriques sur $\mathcal{C}$ à coordonnées dans K de degrés au-plus d sur $\mathbb{Q}$. Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine :

$$y^2 + y = x^5 \tag{4.12}$$

La courbe $\mathcal{C}$ est hyperelliptique de genre $g = 2$ et de rang nul d'après [9].
Notons $P_0 = (0,0),\ P_1 = (0,-1)$ *et* ∞ le point à l'infini.

Dans [9] Hindry et Silverman ont donné une description des points rationnels.
Cette description s'énonce comme suit :
Proposition. Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par

$$\mathcal{C}(\mathbb{Q}) = \{P_0,\ P_1,\ \infty\} \tag{4.13}$$

Nous étendons ce résultat en donnant une paramétrisation des points algébriques de degrés au-plus 3 sur $\mathbb{Q}$. Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathcal{C}$ sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$, (voir [9]),
- Le théorème d'Abel Jacobi, (voir [8])
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :
Théorème.

1. L'ensemble des points quadratiques sur $\mathcal{C}$ est couvert par $\mathcal{S}$ avec

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. L'ensemble des points cubiques sur $\mathcal{C}$ est couvert par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\},$$

$$\mathcal{B} = \left\{ (x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_2(x) = x^3 - \alpha^2 x^2 - \alpha \right\}.$$

4.2.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\overline{\mathbb{Q}}-$ espace vectoriel des fonctions rationnelles F sur $\mathcal{C}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\overline{Q}-$dimension de $\mathcal{L}(D)$. On montre dans [4] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L'équation projective de la courbe $\mathcal{C}$ est :

$$\mathcal{C} : Y^2Z^3 + YZ^4 = X^5 \tag{4.14}$$

On désigne par J la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Désignons par $\mathcal{C}'.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{C}'$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 13. .
• $div(x) = P_0 + P_1 - 2\infty$
• $div(y) = 5P_0 - 5\infty$
• $div(y+1) = 5P_1 - 5\infty$

Preuve. Calculons seulement $div(y)$ et en procédant de la même manière, on trouve les autres. On a $div(y) = div\left(\frac{Y}{Z}\right) = (Y=0).\mathcal{C} - (Z=0).\mathcal{C}$.
Pour $Y = 0$, on a $X^5 = 0$ d'après (4.14) ; et avec $Z = 1$, on obtient donc le point $P_0 = (0, 0, 1)$ avec multiplicité 5. D'où $(Y = 0).\mathcal{C} = 5P_0$. (i)
De même pour $Z = 0$, alors on a $X^5 = 0$ d'après (4.14) ; et avec $Y = 1$, on a le point $\infty = (0, 1, 0)$ avec multiplicité 5 d'où $(Z = 0).\mathcal{C} = 5\infty$. (ii)
Les relations (i) et (ii) entraînent que $div(y) = 5P_0 - 5\infty$.

Conséquences du lemme 1
$5j(P_0) = 5j(P_1) = 0$ et $j(P_0) + j(P_1) = 0$

Lemme 14. .
- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\ x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\ x,\ x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1,\ x,\ x^2,\ y \rangle$
- $\mathcal{L}(6\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3 \rangle$
- $\mathcal{L}(7\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3,\ xy \rangle$

Preuve. Résulte du lemme 1

Lemme 15. $J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} = \langle [P_0 - \infty] \rangle = \{a\,[P_0 - \infty], a \in \{0, 1, 2, 3, 4\}\}$.

4.2.3 Démonstration du théorème

a) **Points quadratiques sur $\mathcal{C}$**
L'ensemble des points quadratiques sur $\mathcal{C}$ est donné par

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}$$

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Notons R_1, R_2 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, d'où

$$t = [R_1 + R_2 - 2\infty] = aj(P_0) = -aj(P_1),\ 0 \leq a \leq 4 \quad (*)$$

On remarque que $R \notin \{\infty, P_0, P_1\}$.
Cas $a = 0$
La relation $(*)$ devient $[R_1 + R_2 - 2\infty] = 0$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty \tag{4.15}$$

donc $F \in \mathcal{L}(2\infty)$, d'où $F(x, y) = a_1 + a_2 x$, $(a_2 \neq 0)$.
Aux points R_i, on a $a_1 + a_2 x = 0$ donc $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}^*$.

En remplaçant x par son expression dans (4.12), on a :

$$y^2 + y = \alpha^5 \Leftrightarrow \left(y + \frac{1}{2}\right)^2 - \frac{1}{4} = \alpha^5 \tag{4.16}$$

et par suite on a :

$$y = -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \tag{4.17}$$

On a ainsi une famille de points quadratiques

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}$$

Cas $a = 1$
La relation $(*)$ donne $[R_1 + R_2 - 2\infty] = j(P_0) = -j(P_1)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P_1 - 3\infty \tag{4.18}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P_1 devrait être égal à ∞ ; ce qui est absurde.

Cas $a = 2$
La relation $(*)$ donne $[R_1 + R_2 - 2\infty] = 2j(P_0) = -2j(P_1)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2P_1 - 4\infty \tag{4.19}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2$, $(a_3 \neq 0)$ et comme $ord_{P_1}(F) = 2$, on doit avoir $a_1 = a_2 = 0$, donc $F(x, y) = a_3 x^2$ et on devrait avoir $R_1 = R_2 = P_0$, ce qui est absurde.

Cas $a = 3$
La relation $(*)$ donne $[R_1 + R_2 - 2\infty] = 3j(P_0) = -2j(P_0)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2P_0 - 4\infty \tag{4.20}$$

donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2$, $(a_2 \neq 0)$ et comme $ord_{P_0}(F) = 2$, on doit avoir $a_1 = a_2 = 0$,donc $F(x, y) = a_3 x^2$ et on devrait avoir $R_1 = R_2 = P_1$, ce qui est absurde.

Cas $a = 4$
La relation $(*)$ donne $[R_1 + R_2 - 2\infty] = 4j(P_0) = -j(P_0)$.
Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P_0 - 3\infty \tag{4.21}$$

donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P_0 devrait être égal à ∞ ; ce qui est absurde.

Conclusion : L'ensemble des points quadratiques sur $\mathcal{C}$ est :

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

b) **Points cubiques sur $\mathcal{C}$**
L'ensemble des points cubiques sur $\mathcal{C}$ est couvert par $\mathcal{A} \cup \mathcal{B}$ avec

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\},$$

$$\mathcal{B} = \left\{ (x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_2(x) = x^3 - \alpha^2 x^2 - \alpha \right\}.$$

Preuve : Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R et travaillons avec $t = [R_1 + R_2 + R_3 - 3\infty]$ qui est un point de $J(\mathbb{Q}) = \{aj(P_0),\ 0 \leq a \leq 4\}$, donc $t = aj(P_0) = -aj(P_1),\ 0 \leq a \leq 4$.
On remarque que $R \notin \{\infty, P_0, P_1\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 0$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 - 3\infty$, donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, alors un des R_i devrait être égal à ∞, ce qui est absurde.

Cas $a = 1$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = j(P_0) = -j(P_1)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + P_1 - 4\infty$, donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2$, $(a_3 \neq 0)$.
Au point P_1, on a $F(P_1) = 0$ donc $a_1 = 0$ d'où $F(x, y) = x(a_2 + a_3 x)$.
Aux points R_i, on a $x(a_2 + a_3 x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.

Cas $a = 2$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 2j(P_0) = -2j(P_1)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 2P_1 - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$, $(a_4 \neq 0)$.
La fonction F est d' ordre 2 en P_1 donc $a_1 - a_4 = 0$ et $a_2 = 0$, d'où $F(x, y) = a_4(y+1) + a_3 x^2$.
Aux points R_i, on doit avoir $a_4(y+1) + a_3 x^2 = 0$, d'où $y = -1 - \frac{a_3}{a_4} x^2$. On voit que y est de la forme $y = -1 - \alpha x^2$ avec $\alpha \in \mathbb{Q}^*$, et par suite on a $y(y+1) = x^5 \Leftrightarrow (-1 - \alpha x^2)(-\alpha x^2) = x^5$
$\Leftrightarrow x^2(x^3 - \alpha^2 x^2 - \alpha) = 0$.
On doit avoir $x^2 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\}$$

Cas $a = 3$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 3j(P_0) = -2j(P_0)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 2P_0 - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite

$F(x,y) = a_1 + a_2x + a_3x^2 + a_4y$, $(a_4 \neq 0)$.
La fonction F est d' ordre 2 en P_0 donc $a_1 = 0$ et $a_2 = 0$, d'où $F(x,y) = a_3x^2 + a_4y$. Aux points R_i, on doit avoir $a_3x^2 + a_4y = 0$, d'où $y = -\frac{a_3}{a_4}x^2$. On voit que y est de la forme $y = \alpha x^2$ avec $\alpha \in \mathbb{Q}^*$, et par suite on a $y^2 + y = x^5 \Leftrightarrow (\alpha x^2)^2 + \alpha x^2 = x^5 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - \alpha) = 0$.
On doit avoir $x^2 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient ainsi une famille de points cubiques

$$\mathcal{B} = \left\{(x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ et } x \textit{ racine de } C_2(x) = x^3 - \alpha^2x^2 - \alpha\right\}$$

Cas $a = 4$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 4j(P_0) = -j(P_0)$. Il existe alors une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + P_0 - 4\infty$, donc $F \in \mathcal{L}(4\infty)$ et par suite $F(x,y) = a_1 + a_2x + a_3x^2$, $a_3 \neq 0$.
Au point P_0, on a $F(P_0) = 0$ donc $a_1 = 0$ d'où $F(x,y) = x(a_2 + a_3x)$.
Aux points R_i, on a $x(a_2 + a_3x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.

Conclusion : L'ensemble des points cubiques sur $\mathcal{C}$ est donné par $\mathcal{A} \cup \mathcal{B}$.

4.3 Courbe $\mathcal{C} : y^2 = x(x^2+1)(x^2+3)$

4.3.1 Introduction

Étant donnée $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K, on note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans K de degré au-plus d sur $\mathbb{Q}$.
Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$, autrement dit $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Notre travail va consister en la détermination de manière explicite les points algébriques de degré quelconque sur la courbe $\mathcal{C}$ d'équation affine :

$$y^2 = x(x^2+1)(x^2+3) \tag{4.22}$$

Il semble qu'une condition indispensable est le fait que le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$ soit fini.
La courbe $\mathcal{C}$ est de genre g = 2 d'après [18]). Notons $Q_0 = (0,0)$ et ∞ le point à l'infini.
Posons $Q_1 = (i,0)$, $\bar{Q}_1 = (-i,0)$, $Q_2 = \left(\sqrt{-3},0\right)$, $\bar{Q}_2 = \left(-\sqrt{-3},0\right)$, $D_0 = Q_1 + \bar{Q}_1$.
Dans [18] Siksek a donné une description des points rationnels de $\mathcal{C}$. Cette description s'énonce comme suit :

Proposition 9. *(Siksek) Les points $\mathbb{Q}$-rationnels de la courbe $\mathcal{C}$ sont donnés par :*

$$\mathcal{C}(\mathbb{Q}) = \{Q_0, \infty\} \tag{4.23}$$

Nous étendons ce résultat en donnant une description explicite des points algébriques de degré quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.
Nos outils fondamentaux sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathcal{C}$ sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$, (voir [18]),
- Le théorème d'Abel Jacobi, (voir [8]),
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre principal résultat s'énonce comme suit :

Théorème 68. *L'ensemble des points algébriques de degré au plus d quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par*

$$\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K) = \mathcal{H}_0 \cup \mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3 \text{ où}$$

$$\mathcal{H}_0 = \left\{ \left(x, -\frac{\sum\limits_{r\leq \frac{k}{2}} a_r x^r}{\sum\limits_{s\leq \frac{k-5}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\},$$

$$\mathcal{H}_1 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{r\leq \frac{k+2}{2}} a_r x^r}{\sum\limits_{s\leq \frac{k-3}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ satisfaisant} \\ \\ \sum_{r\leq \frac{k+2}{2}} a_r (i)^r = 0 \quad , \quad \sum_{r\leq \frac{k+2}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (\mathcal{E}_2) \end{array} \right\},$$

$$\mathcal{H}_2 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{1\ \leq\ r\ \leq \frac{k+1}{2}} a_r x^r}{\sum\limits_{s\leq \frac{k-4}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ satisfaisant } a_0 = 0, \\ \\ \text{et } x \text{ racine de l'équation } (E_1) \end{array} \right\},$$

$$\mathcal{H}_3 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{1\ \leq\ r\ \leq \frac{k+3}{2}} a_r x^r}{\sum\limits_{s\leq \frac{k-2}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ vérifiant } a_0 = 0, \\ \\ \sum_{1\ \leq\ r\ \leq \frac{k+3}{2}} a_r (i)^r = 0 \quad , \quad \sum_{1\ \leq\ r\ \leq \frac{k+3}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (E_3) \end{array} \right\}.$$

On désigne par $(\mathcal{E}_l)$ et (E_t) les équations respectives suivantes :

$$(\mathcal{E}_l) : \left(\sum_{r \leq \frac{k+l}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-5+l}{2}} b_s x^s \right)^2 ,$$

$$(E_t) : \left(\sum_{1 \ \leq \ r \ \leq \frac{k+t}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-5+t}{2}} b_s x^s \right)^2 .$$

4.3.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\bar{\mathbb{Q}}$-espace vectoriel des fonctions rationnelles définies par

$$\mathcal{L}(D) = \left\{ f \in \bar{\mathbb{Q}}(\mathcal{C})^* \mid div\,(f) \geq -D \right\} \cup \{0\} \tag{4.24}$$

$l(D)$ désigne la $\bar{\mathbb{Q}}$-dimension de $\mathcal{L}(D)$.
La classe $[Q-\infty]$ de $Q-\infty$ est notée $j(Q)$; j étant le plongement jacobien $\mathcal{C} \to J(\mathbb{Q})$.
Soient x et y les fonctions rationnelles sur $\mathcal{C}$ données par :

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

L'équation projective de la courbe $\mathcal{C}$ est :

$$Y^2Z^3 = X(X^2+Z^2)(X^2+3Z^2) \tag{4.25}$$

Nous désignerons par $\mathcal{M} \cdot \mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{M}$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 16.

- $div(x) = 2Q_0 - 2\infty$
- $div(x^2+1) = 2Q_1 + 2\bar{Q}_1 - 4\infty$
- $div(x^2+3) = 2Q_2 + 2\bar{Q}_2 - 4\infty$
- $div(y) = Q_0 + Q_1 + \bar{Q}_1 + Q_2 + \bar{Q}_2 - 5\infty$

Preuve. Il s'agit d'un calcul du type :

$$div(w-\alpha) = (W - \alpha Z = 0) \cdot \mathcal{C} - (Z=0) \cdot \mathcal{C} \quad (*) ,$$

où w est une variable (en affine) qui correspond à W (en projectif) et α une constante. On a :

$$\begin{aligned} \mathcal{C} : y^2 &= x(x^2+1)(x^2+3) \\ &= x(x-i)(x+i)(x-\sqrt{-3})(x+\sqrt{-3}). \end{aligned}$$

Il résulte de $(*)$ que :

$$div(x) = (X = 0) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C} \ ,$$

pour $w = x$ et $\alpha = 0$ dans $(*)$.
Pour $(X = 0) \cdot \mathcal{C}$, on a :

$$\begin{cases} X = 0 \\ \\ Y^2Z^3 = X(X^2 + Z^2)(X^2 + 3Z^2) \end{cases} \Rightarrow \begin{cases} X = 0 \\ \\ Y^2Z^3 = 0 \end{cases}$$

$$\Rightarrow \begin{cases} X = 0, \\ \\ Y^2 = 0 \ \text{ ou } \ Z^3 = 0. \end{cases}$$

D'où $Y = 0$ avec ordre de multiplicité 2 ou $Z = 0$ avec ordre de multiplicité 3. Ainsi, les points d'intersection de la courbe d'équation $X = 0$ et $\mathcal{C}$ sont de la forme $(0, 0, Z) = Z(0, 0, 1)$ ou $(0, Y, 0) = Y(0, 1, 0)$.
On trouve ainsi les points $Q_0 = (0, 0, 1)$ avec ordre de multiplicité 2 pour $Z = 1$ et $\infty = (0, 1, 0)$ avec ordre de multiplicité 3 pour $Y = 1$.
Pour $(Z = 0) \cdot \mathcal{C}$, on a :

$$\begin{cases} Z = 0 \\ \\ Y^2Z^3 = X(X^2 + Z^2)(X^2 + 3Z^2) \end{cases} \Rightarrow \begin{cases} Z = 0, \\ \\ X^5 = 0. \end{cases}$$

D'où $X = 0$ avec ordre de multiplicité 5 et les points d'intersection de la courbe d'équation $Z = 0$ et $\mathcal{C}$ sont de la forme $(0, Y, 0) = Y(0, 1, 0)$.
On trouve ainsi le point $\infty = (0, 1, 0)$ avec ordre de multiplicité 5 pour $Y = 1$. Ainsi, $div(x) = 2Q_0 + 3\infty - 5\infty$.
On conclut que

$$div(x) = 2Q_0 - 2\infty.$$

De la même manière que (i) on détermine les diviseurs suivants :

$$div(x - i) \ , \ div(x + i) \ , \ div(x - \sqrt{-3}) \ , \ div(x + \sqrt{-3}) \ , \ div(y).$$

$$\begin{cases} div(x - i) = 2Q_1 - 2\infty, \\ \\ div(x + i) = 2\bar{Q}_1 - 2\infty. \end{cases}$$

D'où

$$\begin{aligned} div(x^2 + 1) &= div(x - i) + div(x + i) \\ &= 2Q_1 + 2\bar{Q}_1 - 4\infty. \\ div(x^2 + 3) &= div(x - \sqrt{-3}) + div(x + \sqrt{-3}) \\ &= 2Q_2 - 2\infty + 2\bar{Q}_2 - 2\infty \\ &= 2Q_2 + 2\bar{Q}_2 - 4\infty. \\ div(y) &= Q_0 + Q_1 + \bar{Q}_1 + Q_2 + \bar{Q}_2 - 5\infty. \end{aligned}$$

Conséquence du lemme 13 : $2j\,(Q_0) = 0$ et $2j\,(D_0) = 2j\left(Q_2 + \bar{Q}_2\right) = 0$.

Lemme 17.

- $\mathcal{L}(\infty) = \langle\ 1\ \rangle$,
- $\mathcal{L}(2\infty) = \langle\ 1,\ x\ \rangle = \mathcal{L}(3\infty)$,
- $\mathcal{L}(4\infty) = \langle\ 1,\ x,\ x^2\ \rangle$,
- $\mathcal{L}(5\infty) = \langle\ 1,\ x,\ x^2,\ y\rangle$,
- $\mathcal{L}(6\infty) = \langle\ 1,\ x,\ x^2,\ y,\ x^3\rangle$,
- $\mathcal{L}(7\infty) = \langle\ 1,\ x,\ x^2,\ y,\ x^3,\ xy\rangle$.

Preuve. C'est une conséquence du lemme 16 et du fait que d'après le théorème de Riemann-Rock on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 18.

Une $\mathbb{Q}$-base de $\mathcal{L}(m\infty)$ est donnée par :

$$\mathcal{B}_m = \left\{x^r\ :\ r \in \mathbb{N}\ et\ r \leq \frac{m}{2}\right\} \cup \left\{x^s y\ :\ s \in \mathbb{N}\ et\ s \leq \frac{m-5}{2}\right\}.$$

Preuve. (voir [16])

Lemme 19.

$$J(\mathbb{Q}) \cong (\mathbb{Z}\ /\ 2\mathbb{Z}) \times (\mathbb{Z}\ /\ 2\mathbb{Z}) \cong \langle\ j(Q_0)\ \rangle \oplus \langle\ j(D_0)\ \rangle\,.$$

Preuve. (voir [18]).

4.3.3 Démonstration du théorème

Soit un point $R \in \mathcal{C}\left(\bar{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = k$.
Les travaux de Siksek dans [18] nous permettent de supposer $k \geq 2$. Notons $R_1,\ R_2, ..., R_k$ les points conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 + \cdots + R_k - k\infty].$$

On a $t \in J(\mathbb{Q})$ et le lemme 16 donne

$$t = mj(Q_0) + nj(D_0)\ ,\ \text{avec}\ 0 \leq m\ ,\ n \leq 1.$$

Ainsi, on obtient :

$$[R_1 + R_2 + \cdots + R_k - k\infty] = mj(Q_0) + nj(D_0)\ ,\ 0 \leq m\ ,\ n \leq 1. \tag{4.26}$$

Notre démonstration se scinde en quatre cas suivants :

$$\underline{\textbf{Cas}} : m = 0 \text{ et } n = 0.$$

La formule (4.26) devient

$$[R_1 + R_2 + \cdots + R_k - k\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + \cdots + R_k - k\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(k\infty)$ et d'après le lemme 18, on a

$$\mathrm{f}(x, y) = \left(\sum_{r \leq \frac{k}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-5}{2}} b_s x^s \right).$$

Aux points R_i , on a

$$\left(\sum_{r \leq \frac{k}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-5}{2}} b_s x^s \right) = 0 \ ; \ \text{donc}$$

$$y = -\frac{\left(\sum_{r \leq \frac{k}{2}} a_r x^r \right)}{\left(\sum_{s \leq \frac{k-5}{2}} b_s x^s \right)} \ ; \ \text{et par suite,}$$

la relation $y^2 = x(x^2+1)(x^2+3)$ donne l'équation

$$(\mathcal{E}_0) : \left(\sum_{r \leq \frac{k}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-5}{2}} b_s x^s \right)^2.$$

On trouve ainsi une famille de points donnée par :

$$\mathcal{H}_0 = \left\{ \left(x, -\frac{\sum_{r \leq \frac{k}{2}} a_r x^r}{\sum_{s \leq \frac{k-5}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}.$$

Cas : $m = 0$ et $n = 1$.

La formule (4.26) devient

$$[R_1 + R_2 + \cdots + R_k - k\infty] = j(D_0) = -j(D_0);$$

d'où

$$[R_1 + R_2 + \cdots + R_k + Q_1 + \overline{Q}_1 - (k+2)\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + \cdots + R_k + Q_1 + \overline{Q}_1 - (k+2)\infty.$$

Donc $\mathrm{f} \in \mathcal{L}((k+2)\infty)$ et d'après le lemme 18, on a

$$\mathrm{f}(x,y) = \left(\sum_{r \leq \frac{k+2}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-3}{2}} b_s x^s \right).$$

La fonction f est d'ordre 1 aux points $Q_1,\ \overline{Q}_1$; donc on doit avoir

$$\sum_{r \leq \frac{k+2}{2}} a_r (i)^r = 0 \ \text{ et } \sum_{r \leq \frac{k+2}{2}} a_r (-i)^r = 0.$$

Aux points R_i , on a

$$\left(\sum_{r \leq \frac{k+2}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-3}{2}} b_s x^s \right) = 0 \ ; \ \text{d'où}$$

$$y = - \frac{\left(\sum_{r \leq \frac{k+2}{2}} a_r x^r \right)}{\left(\sum_{s \leq \frac{k-3}{2}} b_s x^s \right)} \ ; \ \text{et par suite,}$$

la relation $y^2 = x(x^2+1)(x^2+3)$ donne l'équation

$$(\mathcal{E}_2) : \left(\sum_{r \leq \frac{k+2}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-3}{2}} b_s x^s \right)^2.$$

On trouve ainsi une famille de points donnée par :

$$\mathcal{H}_1 = \left\{ \begin{array}{l} \left(x, - \dfrac{\sum\limits_{r \leq \frac{k+2}{2}} a_r x^r}{\sum\limits_{s \leq \frac{k-3}{2}} b_s x^s} \right) \ \mid a_r, b_s \in \mathbb{Q} \text{ satisfaisant} \\ \\ \sum_{r \leq \frac{k+2}{2}} a_r (i)^r = 0 \ \ , \ \ \sum_{r \leq \frac{k+2}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (\mathcal{E}_2) \end{array} \right\}.$$

Cas : $m = 1$ et $n = 0$.

La formule (4.26) devient

$$[R_1 + R_2 + \cdots + R_k - k\infty] = j(Q_0) = -j(Q_0);$$

d'où

$$[R_1 + R_2 + \cdots + R_k + Q_0 - (k+1)\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + \cdots + R_k + Q_0 - (k+1)\infty.$$

Donc $\mathrm{f} \in \mathcal{L}((k+1)\infty)$ et d'après le lemme 15, on a

$$\mathrm{f}(x,y) = \left(\sum_{r \leq \frac{k+1}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-4}{2}} b_s x^s \right).$$

La fonction f est d'ordre 1 au point Q_0 ; donc on doit avoir $a_0 = 0$.
Ainsi, on obtient :

$$\mathrm{f}(x,y) = \left(\sum_{1 \leq r \leq \frac{k+1}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-4}{2}} b_s x^s \right).$$

Aux points R_i , on a

$$\left(\sum_{1 \leq r \leq \frac{k+1}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-4}{2}} b_s x^s \right) = 0 \ ; \ \text{donc}$$

$$y = - \frac{\left(\sum_{1 \leq r \leq \frac{k+1}{2}} a_r x^r \right)}{\left(\sum_{s \leq \frac{k-4}{2}} b_s x^s \right)} \ ; \ \text{et par suite,}$$

la relation $y^2 = x(x^2+1)(x^2+3)$ donne l'équation

$$(E_1) : \left(\sum_{1 \leq r \leq \frac{k+1}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-4}{2}} b_s x^s \right)^2.$$

On trouve ainsi une famille de points donnée par :

$$\mathcal{H}_2 = \left\{ \begin{array}{l} \left(x, - \dfrac{\sum\limits_{1 \leq r \leq \frac{k+1}{2}} a_r x^r}{\sum\limits_{s \leq \frac{k-4}{2}} b_s x^s} \right) \ | \ a_r, b_s \in \mathbb{Q} \text{ satisfaisant } a_0 = 0, \\ \\ \text{et } x \text{ racine de l'équation } (E_1) \end{array} \right\}.$$

Cas : $m = 1$ et $n = 1$.

La formule (4.26) devient

$$[R_1 + R_2 + \cdots + R_k - k\infty] = j(Q_0) + j(D_0) = -j(Q_0) - j(D_0);$$

d'où

$$[R_1 + R_2 + \cdots + R_k + Q_0 + Q_1 + \overline{Q}_1 - (k+3)\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + \cdots + R_k + Q_0 + Q_1 + \overline{Q}_1 - (k+3)\infty.$$

D'où $\mathrm{f} \in \mathcal{L}((k+3)\infty)$ et d'après le lemme 18, on a

$$\mathrm{f}(x,y) = \left(\sum_{r \leq \frac{k+3}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-2}{2}} b_s x^s \right).$$

La fonction f est d'ordre 1 aux points Q_0 , Q_1 et $\overline{Q}_1$; donc on doit avoir

$$a_0 = 0 \ , \quad \sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r (i)^r = 0 \quad \text{et} \quad \sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r (-i)^r = 0.$$

Ainsi, on obtient :

$$\mathrm{f}(x,y) = \left(\sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-2}{2}} b_s x^s \right).$$

Aux points R_i , on a

$$\left(\sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r x^r \right) + y \left(\sum_{s \leq \frac{k-2}{2}} b_s x^s \right) = 0 \ ; \ \text{donc}$$

$$y = - \frac{\left(\sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r x^r \right)}{\left(\sum_{s \leq \frac{k-2}{2}} b_s x^s \right)} \ ; \ \text{et par suite,}$$

la relation $y^2 = x(x^2+1)(x^2+3)$ donne l'équation

$$(E_3) : \left(\sum_{1 \ \leq \ r \ \leq \frac{k+3}{2}} a_r x^r \right)^2 = x(x^2+1)(x^2+3) \left(\sum_{s \leq \frac{k-2}{2}} b_s x^s \right)^2 .$$

On trouve ainsi une famille de points donnée par :

$$\mathcal{H}_3 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{1 \leq r \leq \frac{k+3}{2}} a_r x^r}{\sum\limits_{s \leq \frac{k-2}{2}} b_s x^s} \right) \mid a_r, b_s \in \mathbb{Q} \text{ vérifiant } a_0 = 0, \\ \\ \sum_{1 \leq r \leq \frac{k+3}{2}} a_r (i)^r = 0 \quad , \quad \sum_{1 \leq r \leq \frac{k+3}{2}} a_r (-i)^r = 0 \\ \\ \text{et } x \text{ racine de l'équation } (E_3) \end{array} \right\}.$$

Conclusion : L'ensemble des points algébriques de degré au-plus d quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par :

$$\bigcup_{[K:\mathbb{Q}] \leq d} \mathcal{C}(K) = \mathcal{H}_0 \cup \mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3.$$

4.4 Courbe $\mathcal{C} : y^2 = 3(x^5 - 1)$

4.4.1 Introduction

Etant donnée une courbe algébrique $\mathcal{C}$ définie sur un corps de nombres K, on note $\mathcal{C}$(K) l'ensemble des points sur $\mathcal{C}$ rationnels sur K, et $\bigcup\limits_{[K:\mathbb{Q}] \leq d} \mathcal{C}(K)$ l'ensemble des points algébriques de degré au-plus d sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$. Le degré d'un point algébrique R est le degré de son corps de définition sur $\mathbb{Q}$; en d'autres termes $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Notre travail va consister en l'étude de quelques cas particuliers, où l'on peut déterminer explicitement les points algébriques de degré quelconque sur la courbe $\mathcal{C}$ d'équation affine

$$y^2 = 3(x^5 - 1) \tag{4.27}$$

Il semble qu'une condition indispensable est le fait que le groupe de Mordell-Weil que nous notons $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne J de $\mathcal{C}$ soit fini. Notons $P = (1, 0)$ et ∞ le point à l'infini. Dans [19] Siksek a donné une description des points rationnels sur $\mathbb{Q}$ sur cette courbe. Cette description s'énnonce comme suit :
Proposition. Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par

$$\mathcal{C}(\mathbb{Q}) = \{\infty, P\} \tag{4.28}$$

Nous étendons ce résultat, en donnant une description explicite des points algébriques de degré quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.
Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne de $\mathcal{C}$ (voir [19]),
- Le théorème d'Abel Jacobi (voir [8]),

- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :

Théorème. L'ensemble des points algébriques de degré au-plus d sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par :

$$\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K) = \mathcal{F}_0 \cup \mathcal{F}_1$$

avec

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum\limits_{i\leq \frac{n}{2}} a_i x^i}{\sum\limits_{j\leq \frac{n-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}$$

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum\limits_{i\leq \frac{n+1}{2}} a_i x^i}{\sum\limits_{j\leq \frac{n-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ vérifiant } \sum_{i\leq \frac{n+1}{2}} a_i = 0 \text{ et } x \text{ racine de l'équation } (\mathcal{E}_1) \right\}$$

où :

$$(\mathcal{E}_0) : \left(\sum_{i\leq \frac{l}{2}} a_i x^i \right)^2 = 3 \left(\sum_{j\leq \frac{n-5}{2}} b_j x^j \right)^2 (x^5 - 1) \ ;$$

$$(\mathcal{E}_1) : \left(\sum_{i\leq \frac{n+1}{2}} a_i x^i \right)^2 = 3 \left(\sum_{j\leq \frac{n-4}{2}} b_j x^j \right)^2 (x^5 - 1)$$

4.4.2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\bar{\mathbb{Q}}-$ espace vectoriel des fonctions rationnelles F sur $\mathcal{C}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\bar{Q}-$dimension de $\mathcal{L}(D)$. On montre dans [19] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et $\mathcal{C}$ est une courbe hyperelliptique de genre $g = 2$.
Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L' équation projective de la courbe $\mathcal{C}$ est :

$$\mathcal{C} : Y^2 Z^3 = 3(X^5 - Z^5) \tag{4.29}$$

On désigne par $j(P)$ la classe notée $[P - \infty]$ de $P-\infty$, c'est- à- dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Notons $\eta_1 = e^{i\frac{\Pi}{2}}$ et posons $A_k = (0, \sqrt{3}\eta_1^{2k+1})$ pour $k \in \{0, 1\}$.
Notons $\eta_2 = e^{i\frac{\Pi}{5}}$ et posons $B_k = (\eta_2^{2k}, 0)$ pour $k \in \{0, 1, 2, 3, 4\}$.
Désignons par $\mathcal{D}.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{D}$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 20.

- $div(x-1) = 2P - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(x) = A_0 + A_1 - 2\infty$

Preuve. Il s'agit d'un simple calcul du type

$$div(x-a) = (X - aZ = 0).\mathcal{C} - (Z = 0).\mathcal{C}. \tag{4.30}$$

Par exemple $div(x-1) = (X - Z = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
On a $(X - Z = 0).\mathcal{C} = 2P + 3\infty$ et $(Z = 0).\mathcal{C} = 5\infty$, d'où $div(x-1) = 2P - 2\infty$

Lemme 21.

- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\, x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\, x,\, x^2 \rangle$
- $\mathcal{L}(5\infty) = \langle 1,\, x,\, x^2,\, y \rangle$
- $\mathcal{L}(6\infty) = \langle 1,\, x,\, x^2,\, y,\, x^3 \rangle$

Preuve. Résulte du lemme 20 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 22. .
Une $\mathbb{Q}$-base de $\mathcal{L}(m\infty)$ est donné par :

$$\mathcal{B}_m = \left\{ x^i \mid i \in \mathbb{N} \text{ et } i \leq \frac{m}{2} \right\} \cup \left\{ x^j y \mid j \in \mathbb{N} \text{ et } j \leq \frac{m-5}{2} \right\}$$

Preuve. (Voir [16]).

Lemme 23. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P - \infty] \rangle = \{ a\,[P - \infty], a \in \{0, 1\} \}$.

Preuve. (Voir [19]).

4.4.3 Démonstration du théorème

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$, avec $[\mathbb{Q}[R] : \mathbb{Q}] = n$. Les travaux de Siksek dans [19] nous permettent de supposer que $n \geq 2$. Notons $R_1, R_2, \ldots, R_n$ les conjugués de Galois de R.
On sait que $[R_1 + R_2 + \cdots + R_n - n\infty] \in J(\mathbb{Q})$, d'où d'après le lemme 23,
$[R_1 + R_2 + \cdots + R_n - n\infty] = a\,[P - \infty],\ 0 \leq a \leq 1 \quad (*)$
Selon les valeurs de $a \in \{0, 1\}$, on a les deux cas suivants :
Premier cas : a = 0
La relation $(*)$ devient

$$[R_1 + R_2 + \cdots + R_n - n\infty] = 0$$

Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \cdots + R_n - n\infty \tag{4.31}$$

donc F $\in \mathcal{L}(n\infty)$, et d'après le lemme 22 on a

$$F(x,y) = \left(\sum_{i\leq \frac{n}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-5}{2}} b_j x^j\right) \tag{4.32}$$

Aux points R_i on doit avoir

$$\left(\sum_{i\leq \frac{n}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-5}{2}} b_j x^j\right) = 0 \tag{4.33}$$

d'où $y = -\dfrac{\sum\limits_{i\leq \frac{n}{2}} a_i x^i}{\sum\limits_{j\leq \frac{n-5}{2}} b_j x^j}$ et par suite la relation $y^2 = 3(x^5-1)$ donne l'équation

$$(\mathcal{E}_0) : \left(\sum_{i\leq \frac{n}{2}} a_i x^i\right)^2 = 3\left(\sum_{j\leq \frac{n-5}{2}} b_j x^j\right)^2 (x^5-1)$$

On trouve ainsi une famille de points

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum\limits_{i\leq \frac{n}{2}} a_i x^i}{\sum\limits_{j\leq \frac{n-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}$$

Deuxième cas : a = 1
La relation $(*)$ s'écrit $[R_1 + R_2 + \cdots + R_n - n\infty] = [P - \infty] = -[P - \infty]$.
Il existe alors une fonction F telle que

$$div(F) = R_1 + R_2 + \cdots + R_n + P - (n+1)\infty \tag{4.34}$$

donc F $\in \mathcal{L}((n+1)\infty)$, et d'après le lemme 22, on a

$$F(x,y) = \left(\sum_{i\leq \frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-4}{2}} b_j x^j\right) \tag{4.35}$$

On a $F(P) = 0$ donne la relation

$$\sum_{i\leq \frac{n+1}{2}} a_i = 0$$

.
Aux points R_i on doit avoir

$$\left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq\frac{n-4}{2}} b_j x^j\right) = 0 \tag{4.36}$$

d'où

$$y = -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j} \tag{4.37}$$

et par suite la relation $y^2 = 3(x^5 - 1)$ donne l'équation

$$(\mathcal{E}_1) : \left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right)^2 = 3\left(\sum_{j\leq\frac{n-4}{2}} b_j x^j\right)^2 (x^5 - 1)$$

On trouve ainsi une famille de points

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \; v\acute{e}rifiant \sum_{i\leq\frac{n+1}{2}} a_i = 0 \; et \; x \; racine \; de \; l'\acute{e}quation \; (\mathcal{E}_1) \right\}$$

Conclusion

Dans cette thèse, les résultats obtenus portent particulièrement sur la détermination explicite des points algébriques de petits degrés sur $\mathbb{Q}$ sur chacune des courbes d'équations affines $y^2 = x^5 + 20736$ et $y^2 + y = x^5$, et des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur les courbes d'équations affines : $y^2 = 4x^5 + 1$; $y^2 = x^5 - 243$ et $y^2 = 3x(x^4 + 3)$.
On a aussi donné une paramétrisation des points algébriques de degré quelconque sur $\mathbb{Q}$ sur les courbes d'équations affines $y^2 = x(x^2 + 1)(x^2 + 3)$ et $y^2 = 3(x^5 - 1)$.
En s'inspirant d'abord des travaux de Booker, Sijsling, Sutherland, Voight et Yasak dans [1] qui ont déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 = 4x^5 + 1$, et des travaux de Mulholland dans [13] qui a déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 = x^5 - 243$, mais aussi des travaux de Bruin dans [2] qui a déterminé l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 = 3x(x^4 + 3)$, on a déterminé de manière explicite les points algébriques de degré au-plus 5 sur $\mathbb{Q}$ sur les courbes étudiées au chapitre 3.
Les travaux de Siksek et Stoll dans [20] qui ont décrit l'ensemble des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 = x^5 + 20736$, et ceux de Hindry et Silverman dans [9] qui ont donné une description des points $\mathbb{Q}$-rationnels sur la courbe d'équation affine $y^2 + y = x^5$, mais aussi ceux de Siksek dans [18] et dans [19] qui a donné respectivement l'ensemble des points $\mathbb{Q}$-rationnels sur les courbes d'équations affines $y^2 = x(x^2+1)(x^2+3)$ et $y^2 = 3(x^5 - 1)$ ont été étendus et généralisées dans cette thèse.
En effet, au chapitre 4 on a donné une paramétrisation des points algébriques sur certaines courbes algébriques. Concernant chacune des courbes $y^2 = x^5 + 20736$ et $y^2 + y = x^5$ on a déterminé l'ensemble des points algébriques de degrés au-plus 3. On a aussi déterminé l'ensemble des points algébriques de degré quelconque sur chacune des courbes $y^2 = x(x^2 + 1)(x^2 + 3)$ et $y^2 = 3(x^5 - 1)$.
Notre contribution donnée dans cette thèse consiste en la détermination de manière explicite de l'ensemble des points algébriques de petits degrés, ensuite de degrés au-plus 5 et enfin de degré quelconque sur $\mathbb{Q}$ sur certaines courbes algébriques. Malgré les résultats obtenus dans cette thèse, le champ de recherche reste encore très vaste. En effet :
- Toutes les courbes étudiées sont des courbes dont le Groupe de Mordell-Weil est fini. Cependant le problème reste ouvert pour les courbes dont le Groupe de Mordell-Weil n'est pas fini.
- Tous les résultats obtenus dans le cadre de la détermination des points algébriques de degré au-plus d sur les courbes étudiées, ne concernent que des degrés sur $\mathbb{Q}$.
Le problème reste ouvert pour des points de degrés sur un corps de nombre K ($K \neq \mathbb{Q}$).
- La détermination de l'ensemble des points algébriques de degré fixés est donnés de ma-

nière explicite pour de petits degrés. Dans cette thèse, pour de degrés ≥ 3, les courbes obtenues concernent les points de degrés au-plus d.
Le problème reste ouvert pour les ensembles des points algébriques de degrés exactement d.

Bibliographie

[1] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight and D. Yasak, A database of genus-2 curves over the rational numbers. LMS Journal of Computation and Mathematics, 19(A), 235-254, 2016.

[2] N. Bruin, On powers as sums of two cubes, International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 2000.

[3] A. Chenciner, Courbes algébriques planes. Springer, 2008.

[4] The LMFDB Collaboration, The L-functions and Modular Forms Database. Available at : http ://www.lmfdb.org. [Online ; accessed 8 November 2021].

[5] D. Faddeev, on the divisor class groups of some algebraic curves, Dokl. Akad. Nauk SSSR, Tom 136, 296-298, 1961.

[6] M. Fall, O. Sall, Points algébriques de petits degrés sur la courbe d'équation affine $y^2 = x^5 + 1$, Afrika Matematika 29, 1151 - 1157, 2018.

[7] B. Gross, D. Rohrlich, some results on the Mordell-Weil group of the jacobian of the Fermat curve, Invent. Math. 44, 201-224, 1978.

[8] P. A. Griffiths, Introduction to algebraic curves, Translations of mathematical monographs, volume 76. American Mathematical Society, Providence, 1989.

[9] M. Hindry, J. H. Silverman, Diophantine geometry, an introduction, Springer-Verlag, 2000.

[10] M. Hindry, Les courbes elliptiques racontées à mes enfants-IREM de Paris, 28 Mai 2008.
$www.irem.univ{-}paris{-}diderot.fr/.../les\_courbes\_elliptiques\_racontees\_a\_mes\_enfants/$

[11] M. JOYE, Introduction élémentaire à la théorie des courbes elliptiques, UCL Crypto Group Technical Report Series, 1995.
$https : //sciences.ows.ch/mathematiques/CourbesElliptiques.pdf$

[12] A. J. Menezes, Y.H Wu, R. J. Zuccherato A. J. Menezes, An elementary introduction to hyperelliptic curves. Faculty of Mathematics, University of Waterloo, 1996.

[13] J. TH. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC. Ann Arbor, MI, 2006.

[14] A. NITAJ, Introduction aux courbes elliptiques.
https : //nitaj.users.lmno.cnrs.fr/Introdelliptic.pdf

[15] O. Sall, algebraic points on some Fermat curves and some quotients of Fermat curves : Progress, African Journal Of Mathematical Physics, Volume 8, 79-83, 2010.

[16] O. Sall, M. Fall, C. M. Coly, points algébriques de degré donné sur la courbe d'équation affine $y^2 = x^5 + 1$, International Journal Of Development Research Vol. 06, Issue, 11, pp. 10295-10300, November, 2016.

[17] E.F. Schaefer, Rational points on algebraic curves, lecture II, February 1999.

[18] S. Siksek, Chabauty and the Mordell-Weil Sieve, Beshaj, Lubjana (ed.) et al., Advances on superelliptic curves and their applications. Based on the NATO Advanced Study Institute (ASI), 41, 194-224, 2015.

[19] S. Siksek, Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, No. 4, $765 - 793$, 2013.

[20] S. Siksek, M. Stoll, Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$, Bull. London Math. Soc. 44, 151-166, 2012.

[21] E. H. Sow, M. Fall, O. Sall, Points algébriques de degrés au-plus 5 sur la courbe d'équation affine $y^2 = 4x^5 + 1$, SCIREA Journal of Mathematics, Volume 6, Issue 6, 2021.

[22] E. H. Sow, P. M. Sarr, O. Sall, Points algébriques de degrés au-plus 5 sur la courbe d' équation affine $y^2 = 3x(x^4 + 3)$, International Journal Of Development Research Vol. 11, Issue, 12, 52435-52439, 2021.

[23] E. H. Sow, P. M. Sarr, O. Sall, Algebraic Points of Degree at Most 5 on the Affine Curve $y^2 = x^5 - 243$. Asian Research Journal of Mathematics, 17(10), 51-58. https ://doi.org/10.9734/arjom/2021/v17i1030336, 2021.

[24] E. H. Sow, P. M. Sarr, O. Sall, Parametrization of algebraic points of low degrees on the affine curve $y^2 = x^5 + 144^2$, EPH-International Journal of Mathematics and Statistics, 7.12, 1-5, 2021.

[25] E. H. Sow, P. M. Sarr, M. Fall, O. Sall, Points algébriques de degré quelconque sur la courbe d' équation affine $y^2 = 3(x^5 - 1)$, International Journal of Mathematics and Statistics Invention (IJMSI), Volume 10, Issue 1, PP 01-04, January 2022.

[26] M. Stoll, Chabauty without the Mordell-Weil group. Algorithmic and experimental methods in algebra, geometry, and number theory. Springer, Cham, 623-663, 2017.

[27] P. Tzermias, Torsion parts of Mordell-Weil groups of Fermat jacobians, Internat. Math Res. Notices 7, 359-369, 1998.

[28] O. Zariski, P. Samuel, Commutative Algebra, 2 Vols, Springer-Verlag, Berlin Heidelberg New York, 1975.