UNIVERSITE ASSANE SECK DE ZIGUINCHOR

École Doctorale : Sciences, Technologies et Ingénierie

U.F.R DES SCIENCES ET TECHNOLOGIES

Département de Mathématiques

THÈSE

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

Présentée par : Pape Modou SARR

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

Sujet de la thèse :

THÉORÈME DE CHEVALLEY-WEIL ET COURBES ALGÉBRIQUES

Sous la direction de : Professeur Oumar SALL

Soutenue publiquement le 02 juillet 2022 devant le jury ci-après :

Nom et Prénom(s)	**Grade**	**Qualité**
SANGHARE Mamadou	Professeur titulaire (UCAD)	Président du jury
SALL Oumar	Professeur titulaire (UASZ)	Directeur de Thèse
SANGHARE Mamadou	Professeur titulaire (UCAD)	Rapporteur
BEN MAAOUIA Mohamed Ben Faraj	Professeur titulaire (UGB)	Rapporteur
SAMBOU Marie Salomon	Professeur titulaire (UASZ)	Rapporteur
DIATTA Daouda Niang	Maître de conférences titulaire (UASZ)	Examinateur

Année universitaire : 2020 – 2021

THÈSE EFFECTUÉE AU SEIN DU LABORATOIRE DE MATHÉMATIQUES ET APPLICATIONS (LMA) DE L'UFR DES SCIENCES ET TECHNOLOGIES DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

BP : 523 - ZIGUINCHOR - SENEGAL

THÉORÈME DE CHEVALLEY-WEIL ET COURBES ALGÉBRIQUES

Pape Modou SARR

02 juillet 2022

Remerciements

À travers ces quelques lignes, je vais tenter de satisfaire au difficile exercice de remerciements. Eh oui, difficile puisque je ne veux oublier personne. C'est pourquoi, je remercie par avance ceux dont le nom n'apparaît pas dans cette page.

C'est avec joie que j'adresse mes premiers et sincères remerciements à mon directeur de thèse, le Professeur Oumar SALL de l'Université Assane SECK de Ziguinchor (UASZ) Sénégal. A travers sa patience systématique, sa disponibilité constante, et surtout ses judicieux et innombrables conseils, il m'a offert sans compter la possibilité de profiter de sa grande expérience en matière de recherche, je lui en suis vivement reconnaissant.

Je tiens aussi à exprimer mes remerciements et ma profonde gratitude au Professeur Mamadou SANGHARE de l'Université Cheikh Anta DIOP de Dakar (UCAD) Sénégal, qui a accepté, et j'en suis très honoré, de présider mon jury.
Je suis également honoré que les Professeurs Mamadou SANGHARE de l'Université Cheikh Anta DIOP de Dakar (UCAD) Sénégal, Mohamed Ben Faraj BEN MAAOUIA de l'Université Gaston BERGER de Saint-Louis (UGB) Sénégal et Marie Salomon SAMBOU de l'Université Assane SECK de Ziguinchor (UASZ) Sénégal aient accepté de rapporter ma thèse. Je les remercie très chaleureusement pour leurs suggestions et l'attention qu'ils ont consacré à cette tâche difficile.

Je remercie très chaleureusement le Professeur Daouda Niang DIATTA de l'Université Assane SECK de Ziguinchor (UASZ) Sénégal d'avoir accepté de faire partie du jury.

Je remercie très sincèrement toute ma famille et plus particulièrement mon oncle Jules SAMBOU dont le soutien constant m'a toujours apporté du courage dans les moments difficiles.

Je ne saurais terminer sans exprimer ma reconnaissance envers le Docteur Moussa FALL pour sa disponibilité et ses conseils qui m'ont guidé pour accomplir ce travail, mes amis Christophe, Alain et Marcel pour leur soutien personnel et tous les enseignants du département de Mathématiques.

Dédicaces

Je dédie cette thèse à :
ma mère Emma SAMBOU
ma tante Colette BASSENE
mes frères et sœurs
mes cousins et cousines.

Résumé

Dans cette thèse, on s'intéresse à la détermination des points algébriques en général sur certaines courbes, et en particulier à la détermination de l'ensemble des points algébriques de degrés donnés sur $\mathbb{Q}$. On remarque que certains résultats obtenus dans ce domaine ne sont explicites que pour de petits degrés, d'où la nécessité de les étendre ou de les compléter. Les méthodes que nous utiliserons pour démontrer nos résultats fondamentaux reposent essentiellement sur l'idée de la finitude du groupe de Mordell-Weil des points rationnels de la jacobienne. Dans certains cas, on contournera cette contrainte de finitude du groupe de Mordell-Weil en utilisant le théorème de Chevalley-Weil.
Les approches algébriques et géométriques mises en œuvre, permettront de déterminer de manière explicite :

- l'ensemble des points algébriques de degrés au plus 4 ou 5 sur $\mathbb{Q}$ sur les courbes affines d'équations respectives $y^2 = x(x^2+1)(x^2+3)$, $y^2 = 3x(x^4+3)$ et $y^2 = x^5 - 243$,
- l'ensemble des points algébriques de degrés quelconques sur $\mathbb{Q}$ sur les courbes affines d'équations respectives $y^2 = x(x^2+1)(x^2+3)$ et $y^2 = 3(x^5-1)$,
- l'ensemble des points algébriques de petits degrés sur $\mathbb{Q}$ sur la courbe affine $y^2 = x^5 - 20736$ et sur la famille de courbes affines $y^{2n} = x^5 + 1$ pour $n \in \mathbb{N}^*$.

Concernant les courbes affines $y^{2n} = x^5+1$ pour $n \in \mathbb{N}^*$, le cas $n = 1$ avait été étudié par Schaefer [12] qui avait déterminé les points algébriques de degrés au plus 2 sur $\mathbb{Q}$. Ensuite, les résultats obtenus par Schaefer ont été étendus aux points algébriques de degrés quelconques sur $\mathbb{Q}$ par SALL, FALL et COLY [9]. Pour $n > 1$, le théorème de Chevalley-Weil nous permettra de déterminer, dans cette thèse, l'ensemble des points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur les courbes affines $y^{2n} = x^5+1$.

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

Table des matières

Introduction

Cette thèse s'intéresse aux domaines des mathématiques que sont la géométrie algébrique et la théorie des nombres.
Historiquement, la géométrie algébrique s'est d'abord intéressé à des objets géométriques (courbes, surfaces, ...) composés des points dont les coordonnées vérifiaient des équations ne faisant intervenir que des sommes et des produits. Aujourd'hui, les besoins théoriques ont contraint les mathématiciens à introduire des objets plus généraux dont l'étude a eu des applications dans plusieurs domaines et en particulier en théorie des nombres.
La genèse de la géométrie algébrique est marquée par plusieurs étapes dont :

- la première étape remonte aux mathématiques arabes avec les travaux d'Omar Khayyam qui proposa des méthodes de résolution géométriques des équations algébriques. Cette branche des mathématiques est maintenant appelée algèbre géométrique.
- la deuxième étape est marquée par la géométrie de Descartes qui inaugura l'étude des courbes algébriques par les méthodes de la géométrie analytique.

Il faut attendre le début du vingtième siècle pour que la géométrie algébrique devienne un domaine à part entière sous l'initiative, d'une part, de David Hilbert, dont les travaux ont permis de s'affranchir des méthodes de l'analyse pour n'utiliser que des méthodes algébriques. D'autre part, l'école italienne (Enriques, Chisini, Castelnuovo, Segre, ...) a donné une interprétation géométrique du théorème de Bézout. C'est vers la fin des années 1930 qu'André Weil a introduit un formalisme qui a permis de démontrer rigoureusement les résultats des travaux de l'école italienne. Après 1930, les écoles américaine (Zariski, Mumford, ...), allemande (Noether, Brauer), russe (Kolmogorov, ...) et française (Weil, Chevalley, ...) développèrent sous une forme plus algébrique l'étude des variétés sur un corps commutatif quelconque en utilisant essentiellement la théorie des anneaux.
Dans les années 1950, il y a eu un grand développement par les travaux de l'école française sous l'impulsion de Pierre Samuel, d'Henri Cartan, de Jean-Pierre Serre et d'Alexandre Grothendieck. En une décennie, la géométrie algébrique se développa,

répondant à des questions classiques sur la géométrie des variétés algébriques. Des applications furent très vite trouvées en théorie des nombres.
Aujourd'hui la géométrie algébrique est l'un des domaines fondamentaux et un outil indispensable dans de nombreuses parties des mathématiques.
Cette thèse traite des questions de géométrie algébrique et de théorie des nombres. L'étude porte essentiellement sur les méthodes permettant de déterminer l'ensemble des points algébriques de degrés donnés, et même dans certains cas de degrés quelconques sur certaines courbes algébriques. Ces questions intéressent beaucoup de mathématiciens, et en particulier, des géomètres algébristes. Pourtant les résultats obtenus sont souvent qualitatifs et non explicites.
Nous donnons dans cette thèse quelques méthodes qui nous ont permis de déterminer de manière explicite l'ensemble des points algébriques de degrés d fixés ou parfois quelconques sur certaines courbes.
L'essentiel des résultats obtenus dans cette thèse complètent et/ou étendent des travaux d'autres mathématiciens dont : Bruin [1], Mulholland [7], Schaefer [12], Siksek [13], Siksek [14] et Siksek et Stoll [15].
Voici la description plus précise du contenu de cette thèse.
Le **chapitre** 1 intitulé " Notions préliminaires " rassemble d'une part quelques formules, définitions et théorèmes utiles, et d'autre part introduit des notions classiques de géométrie algébrique que nous utiliserons dans la suite.
Le **chapitre** 2 intitulé " Points algébriques de degrés au plus 4 ou 5 " est consacré à la détermination de l'ensemble des points algébriques de degrés au plus 4 ou 5 sur $\mathbb{Q}$ sur les courbes affines d'équations respectives

$$y^2 = x(x^2+1)(x^2+3)\ ,\ y^2 = 3x(x^4+3) \text{ et } y^2 = x^5 - 243.$$

– Pour la courbe affine $y^2 = x^5 - 243$:
Le résultat obtenu étend celui donné par Mulholland dans [7] par la proposition suivante :

Proposition (**Mulholland**).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C} : y^2 = x^5 - 243$ sont donnés par :

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

Le résultat principal obtenu sur cette courbe est publié dans Asian Research Journal of Mathematics, Volume 17, Issue 10, (2021) [17]. Il s'énonce comme suit :

Théorème.

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

$$\mathcal{A}_0 = \left\{\left(\alpha, \pm\sqrt{\alpha^5 - 243}\right)\ ,\ \alpha \in \mathbb{Q}\right\}.$$

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

3. *L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec*

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

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}.$$

4. *L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{B}_1 \cup \mathcal{B}_2$ avec*

$$\mathcal{B}_1 = \left\{ \begin{array}{l} \left(x, \alpha_1 + \alpha_2 x + \alpha_3 x^2\right) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_1(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\},$$

$$\mathcal{B}_2 = \left\{ \begin{array}{l} \left(x, (x-3)\left[n_1 + n_2(x+3) + n_3(x^2+3x+9)\right]\right) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_2(x) = (x-3)\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}.$$

– Pour la courbe affine $y^2 = 3x(x^4+3)$:

Le résultat obtenu étend celui donné par Bruin dans [1] par la proposition suivante :

Proposition (Bruin).

Les points $\mathbb{Q}$-rationnels sur la courbe $\mathcal{C}$ sont donnés par :

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

Le résultat principal obtenu sur cette courbe est publié dans International Journal of Development Research, Vol. 11, Issue-12, pp. 52435 - 52439, December, **(2021)** [16]. Il 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*

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

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

4. *L'ensemble des points quintiques sur* $\mathcal{C}$ *est donné par* $\mathcal{A}_1 \cup \mathcal{A}_2$ *avec*

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

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

– Pour la courbe affine $y^2 = x(x^2+1)(x^2+3)$:

Le résultat obtenu étend celui donné par Siksek dans [13] par la proposition suivante :

Proposition (Siksek).

Les points $\mathbb{Q}$*-rationnels sur* $\mathcal{C}$ *sont donnés par* :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{Q_0 \ , \ \infty\}.$$

Notre principal résultat obtenu sur cette courbe s'énonce comme suit :

Théorème. *L'ensemble* $\bigcup_{[K:\mathbb{Q}]\leq 4} \mathcal{C}(K)$ *des points algébriques sur* $\mathcal{C}$ *de degrés au plus 4 sur* $\mathbb{Q}$ *est donné par* :

$$\bigcup_{[K:\mathbb{Q}]\leq 4} \mathcal{C}(K) = \{Q_0 \ , \ \infty\} \cup \mathcal{C}^{(2)}(\mathbb{Q}) \cup \mathcal{C}^{(3)}(\mathbb{Q}) \cup \mathcal{C}^{(4)}(\mathbb{Q}) \text{ avec}$$

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \left\{Q_1 \ , \ \overline{Q}_1 \ , \ Q_2 \ , \ \overline{Q}_2\right\} \cup \left\{ \left(\alpha, \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)}\ \right) \ \mid \alpha \in \mathbb{Q}^* \right\},$$

$$\mathcal{C}^{(3)}(\mathbb{Q}) = \mathcal{F}_1 \cup \mathcal{F}_2,$$

$$\mathcal{C}^{(4)}(\mathbb{Q}) = \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3 \cup \mathcal{G}_4, \text{ où}$$

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \left(x, \lambda(x^2+1)\right) \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ A_1(x) = x^3 - \lambda^2 x^2 + 3x - \lambda^2 \end{array} \right\},$$

$$\mathcal{F}_2 = \left\{ \begin{array}{l} \left(x, \lambda x(x^2+1)\right) \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ A_2(x) = \lambda^2 x^3 - x^2 + \lambda^2 x - 3 \end{array} \right\},$$

$$\mathcal{G}_1 = \left\{ \left(x, \pm\sqrt{x(x^2+1)(x^2+3)}\ \right) \ \mid x \in \overline{\mathbb{Q}} \text{ et } [\mathbb{Q}(x):\mathbb{Q}] = 2 \right\},$$

$$\mathcal{G}_2 = \left\{ \begin{array}{l} \big(x, \lambda(x-\mu)(x^2+1)\big) \ | \ \lambda \ , \ \mu \in \mathbb{Q}^* \ et \ x \ racine \ de \\ A(x) = \lambda^2(x-\mu)^2(x^2+1) - x^3 - 3x \end{array} \right\},$$

$$\mathcal{G}_3 = \left\{ \begin{array}{l} (x, \lambda x(x-\mu)) \ | \ \lambda \ , \ \mu \in \mathbb{Q}^* \ et \ x \ racine \ de \\ B(x) = x^4 - \lambda^2 x^3 + (2\lambda^2\mu + 4)x^2 - \lambda^2\mu^2 x + 3 \end{array} \right\},$$

$$\mathcal{G}_4 = \left\{ \begin{array}{l} \left(x, \dfrac{\lambda}{x-\mu}x(x^2+1)\right) \ | \ \lambda \ , \ \mu \in \mathbb{Q}^* \ et \ x \ racine \ de \\ C(x) = (x-\mu)^2(x^2+3) - \lambda^2 x^3 - \lambda^2 x \end{array} \right\}.$$

Le **chapitre** 3 intitulé " Points algébriques de degrés quelconques " consiste en la détermination de l'ensemble des points algébriques de degrés quelconques sur $\mathbb{Q}$ sur les courbes affines respectives $y^2 = x(x^2+1)(x^2+3)$ et $y^2 = 3(x^5-1)$.

– Pour la courbe affine $y^2 = x(x^2+1)(x^2+3)$:

Nous étendons le résultat du **chapitre** 2 obtenu sur cette courbe en donnant une description des points algébriques de degrés quelconques sur $\mathbb{Q}$.

Le théorème principal obtenu sur cette courbe, à paraître dans [11], s'énonce comme suit :

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

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

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

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

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

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

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

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

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

– Pour la courbe affine $y^2 = 3(x^5 - 1)$:

Le résultat obtenu étend celui donné par Siksek dans [14] par la proposition suivante :

Proposition (Siksek).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

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

Le résultat principal obtenu sur cette courbe est publié dans International Journal of Mathematics and Statistics Invention (IJMSI), E-ISSN : 2321 - 4767, P-ISSN : 2321 - 4759, Vol. 10, Issue 1, January, **(2022)**, PP 01 - 04 [19]. Il s'énonce comme suit :

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

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

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

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

On désigne par $(\mathcal{E}_k)$ l'équation suivante :

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

Au **chapitre** 4 intitulé " Points algébriques de petits degrés " on donne une paramétrisation des points algébriques de petits degrés sur la courbe affine $y^2 = x^5 + 20736$ d'une part et d'autre part, nous nous proposons de contourner la contrainte de la finitude du groupe de Mordell-Weil, en déterminant explicitement les points algébriques sur la famille de courbes affines $y^{2n} = x^5 + 1$ sans se préoccuper de la finitude du groupe de Mordell-Weil.

– Pour la courbe affine $y^2 = x^5 + 20736$:

Nous déterminons une paramétrisation des points algébriques de degrés au plus 3 sur $\mathbb{Q}$ sur cette courbe. Le résultat obtenu étend celui donné par Siksek et Stoll dans [15] par la proposition suivante :

Proposition (**Siksek** & **Stoll**)**.**

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

$$\mathcal{C}(\mathbb{Q}) = \left\{ P \ , \ \overline{P} \ , \ \infty \right\}.$$

Notre principal résultat obtenu sur cette courbe est publié dans EPH - International Journal of Mathematics and Statistics, Volume-7, Issue-12, Jan, **(2021)** [18]. Il 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*

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

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

– Pour la famille de courbes affines $y^{2n} = x^5 + 1$:

Nous étudions en détail les points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur les courbes $\mathcal{C}_n$ d'équations affines $y^{2n} = x^5 + 1$.
Le résultat obtenu étend celui donné par E. F. Schaefer dans [12] par la proposition suivante :

Proposition (Schaefer).

(**i**) *Les points* $\mathbb{Q}$*-rationnels sur* $\mathcal{C}$ *sont donnés par* :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

(**ii**) *Les points sur* $\mathcal{C}$ *de degrés* 2 *sur* $\mathbb{Q}$ *sont donnés par* :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \{Q_1\ ,\ Q_2\ ,\ \overline{Q}_1\ ,\ \overline{Q}_2\} \cup \left\{ \left(a, \pm\sqrt{a^5 + 1}\ \right) \mid a \in \mathbb{Q}^* \setminus \{-1\} \right\}.$$

Notre principal résultat obtenu sur cette famille de courbes s'énonce comme suit :

Théorème. *Soit* n *un entier naturel strictement supérieur à* 1.

(**1**) *L'ensemble des points* $\mathbb{Q}$*-rationnels sur les courbes* $\mathcal{C}_n$ *est donné par* :

$$\bigcup_{n \geq 2} \mathcal{C}_n^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

(**2**) *L'ensemble des points algébriques de degrés* 2 *des courbes* $\mathcal{C}_n$ *sur* $\mathbb{Q}$ *est donné par*:

$$\bigcup_{n \geq 2} \mathcal{C}_n^{(2)}(\mathbb{Q}) = \left\{ \begin{array}{l} (0, y) \mid y \text{ racine de l'équation} \\ \\ (y^2 + 1)(y^2 + y + 1)(y^2 - y + 1) = 0 \end{array} \right\}.$$

Le travail se termine par une conclusion dans laquelle on résume les résultats obtenus qui donnent l'idée des perspectives et aussi on cite certains problèmes ouverts qui pourraient intéresser les mathématiciens, en particulier les géomètres algébristes.

Chapitre 1

Notions préliminaires

Dans ce chapitre on introduit les notions de base que nous jugeons utiles dans la suite. Ces notions seront constituées de définitions et résultats supposés classiques ; ce qui explique la rareté des démonstrations.
Les exemples donnés dans ce chapitre permettront de faciliter la compréhension du lecteur.

1.1 Points algébriques

1.1.1 Corps de décomposition

Tous les corps considérés dans ce paragraphe seront des corps commutatifs (sauf mention expresse du contraire). Soit K un tel corps.

Définition 1.1.1. *On dit qu'un corps L est une extension du corps K et l'on note souvent $K \subset L$ (ou L/K) si K est un sous-corps de L.*

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

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

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

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

Définition 1.1.2. *Une extension $K \subset L$ est dite simple s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Exemples :
• $\mathbb{Q}\left(\sqrt{2}\right)$ est une extension de $\mathbb{Q}$;

• $\mathbb{C}$ est une extension simple de $\mathbb{R}$, car $\mathbb{C} = \mathbb{R}(i)$;

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

Définition 1.1.3. *On appelle équation polynômiale 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 1.1.4. *Une extension $K \subset L$ est un corps de rupture sur K pour le polynôme $P \in K[X]$ si, L contient un zéro de P.*

Définition 1.1.5. *Une extension $K \subset L$ est un corps de décomposition sur K pour le polynôme $P \in K[X]$ si, P peut être scindé dans $L[X]$, c'est-à-dire peut être décomposé en produit de polynômes linéaires dans $L[X]$.*

Exemples :

• $\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme $X^2 + 1$;

• $\mathbb{Q}$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme $X^2 - 1$.

1.1.2 Eléments entiers, éléments algébriques

Définition 1.1.6. *Soient A un anneau 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.
◇ On dit que $b \in B$ est entier sur A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(b) = 0$.

Exemples :

• Les nombres complexes $z = \exp\left(\dfrac{2i\pi}{n}\right)$ avec $n \geq 1$ sont algébriques sur $\mathbb{Z}$ car ils vérifient les relations $z^n = 1$;

• Le corps $\overline{\mathbb{Q}}$ des nombres $z \in \mathbb{C}$ algébriques sur $\mathbb{Q}$ s'appelle corps des nombres algébriques.

Définition 1.1.7. *Soient A un anneau et B une A-algèbre.*
L'ensemble des éléments de B qui sont entiers sur A est une sous-A-algèbre de B. On l'appelle clôture intégrale de A dans B.

Définition 1.1.8. *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 1.1.9. *Soient K un corps et B une K-algèbre intègre. Soit $b \in B$ un élément algébrique.*
L'ensemble $E = \{P \in K[X] \mid P(b) = 0\}$ est un idéal premier de $K[X]$.
On appelle polynôme minimal de b le générateur unitaire de E.
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 Extensions entières, extensions algébriques

Définition 1.1.10. *On dit qu'une extension d'anneaux $A \subset B$ est entière si tout élément de B est entier sur A. On dit qu'une extension de corps $K \subset L$ est algébrique si tout élément de L est algébrique sur K.*

Exemple :
$\mathbb{R} \subset \mathbb{C}$ est une extension algébrique.

Définition 1.1.11. *On dit qu'une extension d'anneaux $A \subset B$ est finie si B est un A-module de type fini.*
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. *Soit $K \subset L$ une extension de corps.*
Soient x et y deux éléments de L algébriques sur K, de degrés respectifs $m > 0$ et $n > 0$. Alors l'extension $K \subset K(x, y)$ est de degré fini majoré par mn.
En particulier, $x + y$ et xy sont algébriques sur K, de degré majoré par mn.

Preuve. *Puisque $Irr(y, K(x))$ polynôme minimal de y sur $K(x)$ divise $Irr(y, K)$ polynôme minimal de y sur K alors y est de degré au plus n sur $K(x)$; d'où le premier point par transitivité des extensions finies et multiplicativité des degrés.*
Le deuxième point se déduit du premier, des inclusions $K(x + y) \subset K(x, y)$ et $K(xy) \subset K(x, y)$ et de la traduction de l'algébricité comme propriété de finitude.

□

Définition 1.1.12. *Soient A un anneau intègre et K son corps des fractions.*
On dit que A est intégralement clos si la clôture intégrale de A dans K est égale à A , autrement dit si les éléments de A sont les seuls éléments de K qui sont entiers sur A.

Exemples :
- L'anneau $\mathbb{Z}$ est intégralement clos ;
- Si A est un anneau intégralement clos , $A[X]$ est intégralement clos.

Définition 1.1.13. *Soit K un corps. On dit que le corps K est algébriquement clos s'il vérifie une des conditions équivalentes suivantes* :
(1) *K n'admet pas d'extension algébrique $K \subset L$ avec $L \neq K$;*
(2) *Les polynômes irréductibles de $K[X]$ sont les polynômes de degré 1 ;*
(3) *Tout polynôme non constant à coefficients dans K possède un zéro dans K ;*
(4) *Tout polynôme à coefficients dans K est scindé.*

Définition 1.1.14. *Soit K un corps. Une clôture algébrique de K est une extension algébrique $K \subset L$ telle que L soit algébriquement clos.*

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

1.2 Groupe de Galois

1.2.1 Extensions normales

Définition 1.2.1. *Soit K un corps. Une extension $K \subset E$ est dite normale si, chaque fois qu'un polynôme irréductible $P \in K[X]$ possède une racine dans E, alors il se décompose en produit de polynômes linéaires dans $E[X]$.*
En d'autres termes une extension $K \subset E$ est dite normale si, chaque fois qu'un polynôme irréductible $P \in K[X]$ possède une racine dans E, alors il possède toutes ses racines dans E.

Exemple et contre exemple :
• $\mathbb{C}$ est une extension normale de $\mathbb{R}$ (car les polynômes irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2).

• L'extension $E = \mathbb{Q}\left(\sqrt[3]{5}\right)$ de $\mathbb{Q}$ n'est pas normale puisque, le polynôme

$X^3 - 5 \in \mathbb{Q}[X]$ possède une racine dans E sans se décomposer en produit de polynômes linéaires dans $E[X]$.

Définition 1.2.2. *Soit une extension $K \subset E$. Une clôture 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 :
$\mathbb{C}$ est une clôture normale de l'extension $\mathbb{Q} \subset \mathbb{R}$.

1.2.2 Degré de Galois d'une extension

Définition 1.2.3. *Soient 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 $\sigma : E \longrightarrow F$ laissant fixe tout élément de K, i.e $\sigma(k) = k$ pour tout $k \in K$.*

Exemple :
L'application $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ définie par $\sigma(z) = \overline{z}$ (le conjugué de 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 1.2.4. *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 clôture normale de E.*
La définition du degré galoisien ne dépend pas du choix de la clôture normale de E.

Théorème. *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 clôture normale de E, I 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 $I \longrightarrow A$ qui associe σ à $\sigma(a)$ est bijective, d'où*

$$\begin{aligned}\overline{[E : K]} &= card(I) \\ &= card(A).\end{aligned}$$

□

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

Définition 1.2.5. *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.

Exemples :
- $\mathbb{C}$ est une extension séparable de $\mathbb{R}$.
- Le nombre complexe i est séparable sur $\mathbb{R}$.
- $\sqrt{2}$ est séparable sur $\mathbb{Q}$.

Théorème. *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:

$$[E \text{ est séparable sur } K] \Leftrightarrow \left[\overline{[E : K]} = [E : K]\right]$$

$$\Leftrightarrow [Irr(a, K) \text{ possède } n \text{ racines distinctes}]$$
$$\Leftrightarrow [\text{toute racine de } Irr(a, K) \text{ est simple}]$$
$$\Leftrightarrow [a \text{ est séparable sur } K]$$

□

1.2.3 Extension galoisienne

Définition 1.2.6. *Soient K un corps et $K \subset E$ une extension du corps K.*
On appelle K-automorphisme de E, tout automorphisme $\sigma : E \longrightarrow E$ laissant fixe tout élément de K, i.e $\sigma(k) = k$ pour tout $k \in K$.

Définition 1.2.7. *Soit E une extension normale finie d'un corps K.*
L'ensemble des K-automorphismes de E forme un groupe pour la composition des applications noté $G(E/K)$ et appelé le groupe de Galois de l'extension E de K.

Exemple :
$\mathbb{C}$ est une extension normale finie de $\mathbb{R}$ et on a :

$$G(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}} \ , \ \rho\}$$

où ρ est le $\mathbb{R}$-automorphisme qui associe à chaque nombre complexe z son conjugué $\overline{z}$.

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

Preuve. *Le groupe de Galois $G(E/K)$ est l'ensemble I de tous les K-isomorphismes de E dans une clôture normale de E. En effet, E est sa propre clôture normale car elle est une extension normale de K, donc on a*

$$G(E/K) = I.$$

Ainsi, on voit que l'ordre de $G(E/K)$ est le degré galoisien $\overline{[E : K]}$.

□

Corollaire. *ord* $(G(E/K)) \leq [E : K]$.

Définition 1.2.8. *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 :
$\mathbb{R} \subset \mathbb{C}$ est une extension galoisienne.

Définition 1.2.9. *Soient $K \subset E$ et $x \in E$ algébrique sur K de polynôme minimal $Irr(x, K)$ à coefficients dans K.*
Les zéros de $Irr(x, K)$ dans E sont appelés les conjugués de x.
Les conjugués de x qui sont laissés fixes sous l'action de Galois, i.e qui sont laissés fixes par les K-automorphismes de E sont appelés les conjugués de Galois de x.

1.3 Variétés affines, variétés projectives

1.3.1 Variétés affines

Dans tout le paragraphe on considérera un corps commutatif K.

Définition 1.3.1. *On appelle espace affine de dimension n, et on note $\mathbb{A}^n(K)$ ou $\mathbb{A}^n$, l'ensemble K^n, produit cartésien itéré n fois du corps K.*
Les éléments de K^n sont appelés points.
$\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite affine et plan affine.
Un point P de $\mathbb{A}^n$ est dit zéro d'un polynôme $F \in K[X_1, ..., X_n]$ si $F(P) = 0$.

Définition 1.3.2. *On considère $S \subset K[X_1, ..., X_n]$; On pose*

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

c'est-à-dire l'ensemble des zéros communs à tous les éléments de S.
$\diamond$ *On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S.*
$\diamond$ *On appelle hypersurface définie par un polynôme $F \in K[X_1, ..., X_n]$, et on note $\mathcal{V}(F)$, l'ensemble des zéros de F (pour F non constant et K algébriquement clos).*
Le degré de $\mathcal{V}(F)$ est le degré de F.
$\diamond$ *On appelle courbe algébrique affine toute hypersurface du plan affine $\mathbb{A}^2$.*

Exemple (d'ensembles algébriques affines) :
Le vide et l'espace tout entier sont des ensembles algébriques affines.
En effet :
$\mathcal{V}(1) = \emptyset$ et $\mathcal{V}(0) = \mathbb{A}^n$ où 1 et 0 désignent respectivement le polynôme constant de constante 1 et le polynôme nul.
Si $n = 1$ et si S n'est pas réduit à 0 , $\mathcal{V}(S)$ est un ensemble fini.

Proposition.

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

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

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

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

Définition 1.3.3. *On appelle topologie de Zariski sur l'espace affine $\mathbb{A}^n$, la topologie dont les ensembles algébriques sont les fermés.*

Exemples (de courbes affines planes) :

• Une droite affine $\mathcal{D}$ est une courbe affine plane d'équation $ax + by + c = 0$.

• Une conique 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 :

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

Définition 1.3.4. *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 1.3.5. *Soit E un espace topologique.*
◇ On dit que E est irréductible s'il n'est pas vide et s'il n'est pas réunion de deux fermés distincts de E , c'est-à-dire

$$\begin{cases} E \neq \emptyset \\ \\ \text{Si } E = E_1 \cup E_2 \text{ avec } E_1, E_2 \text{ fermés de } E \text{ alors } E = E_1 \text{ ou } E = E_2. \end{cases}$$

◇ Un ensemble algébrique affine est dit irréductible s'il est irréductible pour la topologie de Zariski.
◇ On appelle variété affine tout ensemble algébrique affine irréductible.

Théorème et Définition. *Tout ensemble algébrique non vide A se décompose de façon unique (à permutation près) en une réunion finie d'ensembles algébriques irréductibles $A_1, ..., A_p$, non contenus l'un dans l'autre.*
Les $A_1, ..., A_p$ sont appelés les composantes irréductibles de A.

1.3.2 Variétés projectives

Dans la suite R désignera l'anneau $K[X_0, ..., X_n]$; on garde notre espace affine $\mathbb{A}^n$ de dimension n sur K.

Définition 1.3.6. *On considère sur $K^{n+1} - \{0\}$ la relation $\mathcal{R}$ définie par : pour tous $x,\ y \in K^{n+1} - \{0\}$, $x\mathcal{R}y$ si et seulement si ils sont colinéaires.*
En d'autres termes $x\mathcal{R}y \iff \exists\ \lambda \in K^* :\ y = \lambda x$.
On montre aisément que $\mathcal{R}$ est une relation d'équivalence sur $K^{n+1} - \{0\}$.
L'ensemble des classes d'équivalence par $\mathcal{R}$ est appelé l'espace projectif de dimension n sur K, et l'on note $\mathbb{P}(K^{n+1})$ ou $\mathbb{P}^n(K)$ ou simplement $\mathbb{P}^n$.
On dit que $\mathbb{P}^1$ la droite projective sur K, et que $\mathbb{P}^2$ est le plan projectif sur K.

Définition 1.3.7. *Soit $F \in R = K[X_0, ..., X_n]$.*
On dit que F est homogène de degré d si, pour tout $\lambda \in K^*$, on a

$$F(\lambda X_0, ..., \lambda X_n) = \lambda^d F(X_0, ..., X_n).$$

Définition 1.3.8. *Soit S une partie de R formée de polynômes homogènes.*
◇ On appelle ensemble algébrique projectif défini par S, l'ensemble noté $\mathcal{V}(S)$ défini par :

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

On voit donc que $\mathcal{V}(S)$ est l'ensemble des zéros communs à tous les polynômes de S.
◇ Une hypersurface définie par un polynôme homogène F, notée $\mathcal{V}(F)$, est l'ensemble des zéros de F (pour F non constant et K algébriquement clos).

◇ *Une courbe algébrique plane projective est une hypersurface du plan projectif.*
◇ *Un hyperplan est une hypersurface définie par un polynôme homogène de degré* 1.

Remarques :
- Par abus d'écriture un point $P = (x_0 : ... : x_n)$ de l'espace projectif $\mathbb{P}^n$ sera noté simplement $P = (x_0, ..., x_n)$.
- Comme dans le cas affine, on peut définir une topologie sur $\mathbb{P}^n$, appelée topologie de Zariski, en prenant comme ouvert les complémentaires des ensembles projectifs.

Définition 1.3.9. *On appelle variété algébrique projective tout ensemble algébrique projectif irréductible pour la topologie de Zariski.*

Définition 1.3.10. *Un point $P = (a, b, c)$ d'une courbe $\mathcal{C} : F(X, Y, Z) = 0$ est dit singulier si:*

$$\frac{\partial F}{\partial X}(a, b, c) = \frac{\partial F}{\partial Y}(a, b, c) = \frac{\partial F}{\partial Z}(a, b, c) = 0.$$

Un point $P = (a, b, c)$ d'une courbe $\mathcal{C} : (X, Y, Z) = 0$ est dit lisse si:

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

L'équation de la tangente en un point lisse $P = (a, b, c)$ à $\mathcal{C}$ est donnée par la formule suivante:

$$X\ \frac{\partial F}{\partial X}(a, b, c) + Y\ \frac{\partial F}{\partial Y}(a, b, c) + Z\ \frac{\partial F}{\partial Z}(a, b, c) = 0.$$

La courbe $\mathcal{C}$ est lisse si tous ses points sont lisses.

Définition 1.3.11 (**Morphisme de variétés projectives**). *Soient V_1 , $V_2 \in \mathbb{P}^n$ deux variétés projectives définies sur K.*
On dit qu'une application $f : V_1 \longrightarrow V_2$ est un morphisme de V_1 dans V_2 s'il existe des polynômes $F_0, ..., F_n \in K[X_0, ..., X_n]$ tels que $\forall\ X = (x_0, ..., x_n) \in V_1$, $f(X) = (F_0(X), ..., F_n(X))$. On note $f = (F_0, ..., F_n)$.

1.4 Groupe de Picard

Dans ce paragraphe, $\mathcal{C}$ désignera une courbe algébrique plane et lisse définie sur un corps de nombres K.

1.4.1 Diviseurs sur une courbe

Définition 1.4.1. *Un diviseur D sur $\mathcal{C}$ est une somme formelle de points appartenant à $\mathcal{C}$:*

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

où les $n_P \in \mathbb{Z}$ sont presque tous nuls.
L'ensemble des diviseurs sur $\mathcal{C}$ est un groupe commutatif , où la loi de groupe est l'addition formelle de points de $\mathcal{C}$. Ce groupe est noté $Div(\mathcal{C})$.
Soient deux diviseurs D et D' de $Div(\mathcal{C})$:

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

On appelle support d'un diviseur $D = \sum_{P \in \mathcal{C}} n_P P$, l'ensemble des points $P \in \mathcal{C}$ tels que $n_P \neq 0$.
Le degré de $D = \sum_{P \in \mathcal{C}} n_P P$ est la somme de ses coefficients :

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

On remarque que le degré est un homomorphisme de groupes de $Div(\mathcal{C})$ vers $\mathbb{Z}$:

$$\deg : Div(\mathcal{C}) \longrightarrow \mathbb{Z}$$

$$D \longmapsto \deg(D)$$

Le noyau de cet homomorphisme est l'ensemble des diviseurs sur $\mathcal{C}$ de degré nul , et on le note $Div^0(\mathcal{C})$. On a alors $\ker(\deg) = Div^0(\mathcal{C})$ qui est un sous-groupe de $Div(\mathcal{C})$.

Définition 1.4.2. *On dit qu'un diviseur $D = \sum_{P \in \mathcal{C}} n_P P$ est effectif si $n_P \geq 0$, $\forall$ $P \in \mathcal{C}$. On notera $D \geq 0$ pour exprimer que D est effectif.*
La relation dans $Div(\mathcal{C})$ définie par

$$D_1 \leq D_2 \text{ si et seulement si } D_2 - D_1 \geq 0$$

est une relation d'ordre partiel.

1.4.2 Diviseurs principaux

Dans cette section, on suppose que la courbe $\mathcal{C}$ est affine et irréductible de manière à avoir un anneau $K[\mathcal{C}]$ intègre.

Définition 1.4.3. *Le corps des fractions de l'anneau $K[\mathcal{C}]$ est appelé corps des fonctions rationnelles sur $\mathcal{C}$; il est noté $K(\mathcal{C})$.*

Définition 1.4.4. *Soient $f \in K(C)$ et $P \in \mathcal{C}$.*
On dit que f est régulière (ou est définie) au point P s'il existe $g,\ h \in K[\mathcal{C}]$ avec $h(P) \neq 0$ telles que $f = \frac{g}{h}$.
L'ensemble des fonctions régulières en P est noté $\mathcal{O}_P(\mathcal{C})$, et appelé l'anneau local de $\mathcal{C}$ en P.
L'ensemble des points de $\mathcal{C}$ pour lesquels f n'est pas régulière est appelé l'ensemble des pôles de f.
Si f est régulière au point $P \in \mathcal{C}$ et $f(P) = 0$, on dit que P est un zéro de f.
L'ensemble des fonctions régulières en P et qui s'annulent en P est appelé l'idéal maximal de $\mathcal{C}$ en P et noté $\mu_P(\mathcal{C})$.
Si $P = (a, b)$, alors $\mu_P(\mathcal{C}) = \{f \in \mathcal{O}_P(\mathcal{C}) \mid f(P) = 0\}$ est de la forme $\langle x - a\ ,\ y - b\rangle$: c'est l'idéal engendré par $x - a$ et $y - b$.
Les éléments inversibles de $\mathcal{O}_P(\mathcal{C})$ sont ceux n'appartenant pas à $\mu_P(\mathcal{C})$; on les appelle les unités de $\mathcal{O}_P(\mathcal{C})$ et ils forment un groupe multiplicatif.

Définition 1.4.5. *On dit que $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète s'il existe $t \in \mathcal{O}_P(\mathcal{C})$, $t \neq 0$, $t \in \mu_P(\mathcal{C})$, tel que tout élément non nul $f \in \mathcal{O}_P(\mathcal{C})$ s'écrit de manière unique $f = u.t^n$, u unité de $\mathcal{O}_P(\mathcal{C})$, $n \in \mathbb{N}$.*
L'entier n est appelé la valuation ou l'ordre de f noté $ord_P(f)$. Il ne dépend pas du choix de t qu'on appelle uniformisante.

Remarques :

· Si $x \in \mathcal{O}_P(\mathcal{C})$, $x \neq 0$, on peut écrire x sous la forme $u.t^n$ avec $n \in \mathbb{Z}$ et poser $n = ord_P(x)$.

· Si $\mathcal{C}$ est lisse en P alors $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète, et le corps $\mathcal{O}_P(\mathcal{C})/\mu_P(\mathcal{C})$ est appelé corps résiduel.

Propriétés :

∘ L'application $ord_P : \mathcal{O}_P(\mathcal{C}) \longrightarrow \mathbb{Z} \cup \{\infty\}$ est un homomorphisme surjectif défini par : $ord_P(u.t^n) = n\ ,\ ord_P(t) = 1\ ,\ ord_P(u) = 0\ ,\ ord_P(0) = \infty$.

∘ $ord_P(x) = \infty \Longleftrightarrow x = 0$.

∘ $ord_P(xy) = ord_P(x) + ord_P(y)$.

∘ $ord_P\left(\frac{x}{y}\right) = ord_P(x) - ord_P(y)$.

∘ $ord_P(x + y) \geq \min(ord_P(x)\ ,\ ord_P(y))$.

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

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

$$\mu_P(\mathcal{C}) = \{f \in K(\mathcal{C}) \mid ord_P(f) > 0\}$$

Remarques : Soit $\mathcal{C}$ une courbe plane lisse en P et irréductible , et $f \in K(\mathcal{C})$ une fonction non nulle.

· Si f est régulière en P et $f(P) \neq 0$ alors $ord_P(f) = 0$.

· Si f est régulière en P et $f(P) = 0$ alors $ord_P(f) > 0$.

· Si f a un pôle en P alors $ord_P(f) = -ord_P\left(\frac{1}{f}\right)$.

Définition 1.4.6. *Soit $\mathcal{C}$ une courbe plane projective lisse et irréductible , et f une fonction non nulle de $K(\mathcal{C})$. On associe à f le diviseur noté $div(f)$ défini par :*

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

Un tel diviseur est appelé diviseur principal.

Définition 1.4.7. *Deux diviseurs D_1 et D_2 sur $\mathcal{C}$ sont linéairement équivalents si le diviseur $D_1 - D_2$ est principal ; c'est à dire qu'il existe une fonction rationnelle non nulle f définie sur $\mathcal{C}$ telle que $D_1 = D_2 + div(f)$. On note $D_1 \sim D_2$.*
L'ensemble des diviseurs principaux , noté $Princ(\mathcal{C})$ est un sous-groupe de $Div(\mathcal{C})$.

Proposition. *Soient f et g deux fonctions rationnelles de $K(C)^*$, alors :*

$$div(fg) = div(f) + div(g)$$
$$div\left(\frac{f}{g}\right) = div(f) - div(g)$$

En désignant par $div_0(f)$ le diviseur des zéros de f et par $div_\infty(f)$ le diviseur des pôles de f , on a : $div(f) = div_0(f) - div_\infty(f)$. Géométriquement cela signifie que $div_0(f)$ correspond à l'intersection de $\mathcal{C}$ avec la courbe d'équation $f = 0$ et $div_\infty(f)$ correspond à l'intersection de $\mathcal{C}$ avec la courbe d'équation $\frac{1}{f} = 0$.
Une fonction rationnelle f a autant de zéros que de pôles ; donc $\deg(div(f)) = 0$.

Définition 1.4.8. *On appelle groupe de Picard de $\mathcal{C}$, noté $Pic(\mathcal{C})$ le quotient de $Div(\mathcal{C})$ par $Princ(\mathcal{C})$:*

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

$x \in Pic(\mathcal{C})$ signifie qu'il existe $D \in Div(\mathcal{C})$ tel que $x = \dot{D}$; avec

$$\begin{aligned}\dot{D} &= \{D' \in Div(\mathcal{C}) \mid D \sim D'\} \\ &= \{D' \in Div(\mathcal{C}) \mid \exists\ f \in K(\mathcal{C})^* \ :\ D - D' = div(f)\}.\end{aligned}$$

On note $Pic^0(\mathcal{C})$ l'ensemble des classes de diviseurs de degré 0 dans $Pic(\mathcal{C})$.
On montre que $Pic^0(\mathcal{C})$ est un sous-groupe de $Pic(\mathcal{C})$ et on a :

$$Pic^0(\mathcal{C}) \cong J$$

où J désigne la jacobienne de la courbe $\mathcal{C}$.

1.5 Groupe de Mordell-Weil

En théorie des nombres , le théorème de Mordell - Weil affirme que pour toute variété abélienne A définie sur un corps de nombres K , le groupe $A(K)$ des points K-rationnels de A est un groupe abélien de type fini, appelé le groupe de Mordell-Weil. Nous donnons dans ce paragraphe une formulation du théorème de Mordell-Weil pour une variété abélienne définie sur un corps de nombres K.

Définition 1.5.1. *Soient G un groupe d'élément neutre e et $x \in G$.*
$\diamond$ On dit que x est un point de torsion (ou que x est d'ordre fini) s'il existe un entier non nul n tel que $x^n = e$.
$\diamond$ Le plus petit entier $n > 0$ vérifiant $x^n = e$ est appelé ordre de x.
$\diamond$ L'ensemble des points de torsion de G est un sous-groupe de G noté G_{tors}.
$\diamond$ On dit que G est un groupe de torsion si $G = G_{tors}$.

Théorème. *Soit A une variété abélienne définie sur un corps de nombres K. Alors le groupe des points rationnels $A(K)$ est un groupe de type*

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

L'entier naturel r est le rang du groupe $A(K)$ et $A(K)_{tors}$ est le groupe de torsion. Si A est la jacobienne J d'une courbe algébrique $\mathcal{C}$ définie sur $\mathbb{Q}$ alors

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

Si le rang du groupe $J(\mathbb{Q})$ est nul $(r = 0)$ alors $J(\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$.

1.6 Théorème de Riemann-Roch

1.6.1 Systèmes linéaires

Définition 1.6.1. *Soient $\mathcal{C}$ une courbe lisse et $D \in Div(\mathcal{C})$.*
On associe à D l'ensemble des fonctions :

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

La proposition suivante résume les propriétés de $\mathcal{L}(D)$:

Proposition. *Soient $\mathcal{C}$ une courbe lisse et $D \in Div(\mathcal{C})$.*
(i) $\mathcal{L}(D)$ est un K-espace vectoriel de dimension finie notée $l(D)$.
(ii) Si $D, D' \in Div(C)$ sont linéairement équivalents alors $\mathcal{L}(D)$ et $\mathcal{L}(D')$ sont isomorphes.
(iii) Si $D, D' \in Div(C)$ satisfont $D \leq D'$ alors $\mathcal{L}(D) \subset \mathcal{L}(D')$.

Définition 1.6.2. *Soit D un diviseur d'une courbe $\mathcal{C}$. On appelle système linéaire complet et on note $|D|$ l'ensemble des diviseurs effectifs linéairement équivalents à D ; c'est à dire* : $|D| = \{D' \geq 0 \mid D \sim D'\}$.
Le degré du système linéaire complet est le degré de chacun de ses diviseurs.
Un point P de $\mathcal{C}$ est dit point base du système linéaire s'il apparait dans chacun de ses diviseurs.

1.6.2 Théorème (Riemann-Roch)

Définition 1.6.3. *Soit $\mathcal{C}$ une courbe projective lisse de degré d.*

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

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

Remarque : Soit $\mathcal{C}$ une courbe algébrique plane et lisse définie sur un corps de nombres K. Le diviseur noté $K_{\mathcal{C}}$ et vérifiant la relation $l(K_{\mathcal{C}}) = g$ où g désigne le genre de $\mathcal{C}$ est appelé le diviseur canonique de $\mathcal{C}$.

Théorème. *Soit $\mathcal{C}$ une courbe projective lisse de genre g.*
Pour tout diviseur D de $\mathcal{C}$, on a :

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

Si $D = 0$ (le diviseur nul) alors $l(D) = l(0) = 1$ car les seules fonctions régulières sur les variétés projectives sont les constantes. Comme le degré du diviseur est égal à 0 , alors le théorème donne l'égalité $l(K_{\mathcal{C}}) = g$.

Corollaire (***cf*** [6])**.** *Avec les notations précédentes, on a* :
(i) $\deg(K_{\mathcal{C}}) = 2g - 2$.
(ii) *Si* $\deg D < 0$ *alors* $\mathcal{L}(D) = \{0\}$, $l(D) = 0$.
(iii) *Si* $\deg D > 2g - 1$ *alors* $l(D) = \deg(D) + 1 - g$.

(iv) *Si* $l(D)l(K_{\mathcal{C}} - D) \neq 0$ *alors* $l(D) \leq 1 + \dfrac{1}{2}\deg(D)$.

(v) *Si* $\deg D \geq 2g$ *alors D est sans point base.*

Définition 1.6.4. *Une courbe $\mathcal{C}$ définie sur un corps K est dite hyperelliptique si elle admet un modèle affine lisse d'équation* :

$$y^2 + h(x)y = f(x) \ , \ \text{où.}$$

$\diamond$ $h \in K[X]$ *est un polynôme de degré au-plus g,*
$\diamond$ $f \in K[X]$ *est un polynôme unitaire de degré* $2g + 1$.

1.7 Théorème d'Abel-Jacobi

Définition 1.7.1. *On désigne par $[D]$ la classe dans $Pic^0(\mathcal{C})$ d'un diviseur D sur $\mathcal{C}$.*

$\diamond$ *On appelle plongement jacobien l'application j définie par :*

$$j : \mathcal{C} \longrightarrow J$$

$$P \longmapsto [P - P_\infty]$$

où P_∞ est un point K-rationnel de $\mathcal{C}$ défini par $(x, y, 0)$.

$\diamond$ *L'application j s'étend par additivité, encore notée j, de $Div^0(\mathcal{C})$ vers J définie par :*

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

Théorème (**Abel-Jacobi** , ***cf*** [5]). *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 J.

Chapitre 2

Points algébriques de degrés au plus 4 ou 5

Introduction

Dans ce chapitre on détermine l'ensemble des points algébriques de degrés au plus 4 ou 5 sur $\mathbb{Q}$ sur les courbes affines d'équations respectives :

$$y^2 = x(x^2+1)(x^2+3)\ ,\ y^2 = 3x(x^4+3) \text{ et } y^2 = x^5 - 243.$$

Soit $\mathcal{C}$ une courbe algébrique 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 l'ensemble des points algébriques sur $\mathcal{C}$ à coordonnées dans K de degrés au plus d sur $\mathbb{Q}$ est noté $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$.
Un théorème de Faltings dans [4] affirme que, si $g \geq 2$ alors l'ensemble $\mathcal{C}(K)$ est fini. Une généralisation aux sous-variétés d'une variété abélienne permet une étude qualitative de l'ensemble $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$.
Ces résultats sont en général ineffectifs. La situation est plus favorable dans le cas où le rang du groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ est nul. Les résultats de ce chapitre se situent dans ce cadre.

2.1 Points algébriques de degrés au plus 5 sur la courbe affine $\mathcal{C} : y^2 = x^5 - 243$

Cette section complète et étend les travaux de Mulholland [7].
Nous nous proposons d'étudier en détail les points algébriques de degrés au plus 5 sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = x^5 - 243$.
La courbe est hyperelliptique de genre 2 d'après J. TH. Mulholland.

Notons $P = (3, 0)$ et ∞ le point à l'infini de coordonnées projectives $(0, 1, 0)$.
Dans [7] J. TH. Mulholland a donné une description des points de degrés 1 sur $\mathbb{Q}$.
Cette description s'énonce comme suit :

Proposition (Mulholland).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

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

Nous étendons ce résultat en donnant une description des points algébriques sur $\mathcal{C}$ de degrés au plus 5 sur $\mathbb{Q}$.

Nos outils essentiels sont :

∘ Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ (voir [7]),

∘ Le Théorème d'Abel Jacobi (voir [5]),

∘ Des systèmes linéaires sur $\mathcal{C}$.

Notre principal résultat s'énonce comme suit :

Théorème.

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

$$\mathcal{A}_0 = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right),\ \alpha \in \mathbb{Q} \right\}.$$

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

3. *L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{A}_1 \cup \mathcal{A}_2$ avec*

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

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}.$$

4. *L'ensemble des points quintiques sur $\mathcal{C}$ est donné par $\mathcal{B}_1 \cup \mathcal{B}_2$ avec*

$$\mathcal{B}_1 = \left\{ \begin{array}{l} \left(x, \alpha_1 + \alpha_2 x + \alpha_3 x^2\right) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_1(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\},$$

$$\mathcal{B}_2 = \left\{ \begin{array}{l} \left(x, (x-3)\left[n_1 + n_2(x+3) + n_3(x^2+3x+9)\right]\right) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_2(x) = (x-3)\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}.$$

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 [7] que le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L'équation projective de la courbe $\mathcal{C}$ est : $Y^2Z^3 = X^5 - 243Z^5 \quad (*)$.
On désigne par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Soit $\eta_1 = e^{\frac{i\Pi}{2}}$ dans $\mathbb{C}$. Posons $A_k = (0, 9\sqrt{3}\ \eta_1^{2k+1})$ pour $k \in \{0,1\}$.
Soit $\eta_2 = e^{\frac{2i\Pi}{5}}$ 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 $\mathcal{D}$ et $\mathcal{C}$.

Lemme 2.1.1. .
• $div(x-3) = 2P - 2\infty$,
• $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$,
• $div(x) = A_0 + A_1 - 2\infty$.

Preuve. 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 $\mathcal{C} : Y^2Z^3 = X^5 - (3Z)^5$ (équation projective).
Il résulte de $(**)$ que :
• $div(x-3) = (X = 3Z).\mathcal{C} - (Z = 0).\mathcal{C}$ pour $w = x$ et $\alpha = 3$ dans $(**)$.
Pour $X = 3Z$, on a $Y^2Z^3 = 0$ d'après $(*)$, 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 $(X = 3Z).\mathcal{C} = 2P + 3\infty$. (i)
De même pour $Z = 0$, alors on a $X^5 = 0$ d'après $(*)$; 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 $div(x-3) = 2P - 2\infty$.
• De la même manière que $div(x-3)$, on montre que $div(x) = A_0 + A_1 - 2\infty$ et $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$. □

Conséquence du Lemme 2.1.1 : $2j\,(P) = 0$.

Lemme 2.1.2.

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

Preuve. Il résulte du Lemme 2.1.1 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 2.1.3. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P - \infty]\rangle = \{a\,[P - \infty]\,, a \in \{0, 1\}\}$.

Preuve. Voir [7]. □

Démonstration du théorème

2.1.1 Points quadratiques

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

$$\mathcal{A}_0 = \left\{\left(\alpha, \pm\sqrt{\alpha^5 - 243}\right),\ \alpha \in \mathbb{Q}\right\}.$$

Preuve : Soit $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}\,(R) : \mathbb{Q}] = 2$.
Notons R_1 et R_2 les conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

d'où

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

On a les deux cas suivants :
Premier cas : $a = 0$.
La relation (1) devient $[R_1 + R_2 - 2\infty] = 0$.
Le théorème d'Abel-Jacobi entraine l'existence d'une fonction rationnelle F définie sur $\mathbb{Q}$ telle que

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

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 la formule $y^2 = x^5 - 243$, on obtient :

$$y^2 = \alpha^5 - 243;$$

et par suite on a :

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

On trouve ainsi une famille de points quadratiques donnée par :

$$\mathcal{A}_0 = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right),\ \alpha \in \mathbb{Q} \right\}.$$

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

$$div(F) = R_1 + R_2 + P - 3\infty;$$

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 $\mathcal{A}_0$.

2.1.2 Points cubiques

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 et R_3 les conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

d'où

$$t = [R_1 + R_2 + R_3 - 3\infty] = a[P - \infty],\ a \in \{0, 1\}. \quad (2)$$

On a les deux cas suivants :
Premier cas : $a = 0$.
La relation (2) devient $[R_1 + R_2 + R_3 - 3\infty] = 0$.
Le théorème d'Abel-Jacobi entraine l'existence d'une fonction rationnelle F définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 - 3\infty;$$

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

Deuxième cas : $a = 1$.
La relation (2) devient $[R_1 + R_2 + R_3 + P - 4\infty] = 0$.
Le théorème d'Abel-Jacobi entraine l'existence d'une fonction rationnelle F définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + P - 4\infty;$$

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 sa valeur dans l'expression de $F(x,y)$ on a :

$$\begin{aligned} F(x,y) &= -3a_2 - 9a_3 + a_2x + a_3x^2 \\ F(x,y) &= a_2(x-3) + a_3\left(x^2 - 9\right) \\ F(x,y) &= (x-3)\left[a_2 + a_3(x+3)\right] \end{aligned}$$

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.

2.1.3 Points quartiques

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

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

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}.$$

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 et R_4 les conjugués de Galois de R et 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

$$t = [R_1 + R_2 + R_3 + R_4 - 4\infty] = a[P - \infty], \ a \in \{0, 1\}. \quad (3)$$

On a les deux cas suivants :
Premier cas : $a = 0$.
La relation (3) 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty;$$

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 être ∞. Aux points R_i, on a : $a_1 + a_2x + a_3x^2 = 0$; la relation $y^2 = x^5 - 243$ donne

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

On trouve ainsi une famille de points quartiques donnée par :

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

Deuxième cas : $a = 1$.
La relation (3) 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = [R_1 + R_2 + R_3 + R_4 + P - 5\infty];$$

donc $F \in \mathcal{L}(5\infty)$, d'où $F(x,y) = a_1 + a_2x + a_3x^2 + a_4y, \quad (a_4 \neq 0)$.
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 obtient :

$$\begin{aligned} F(x,y) &= -3a_2 - 9a_3 + a_2x + a_3x^2 + a_4y \\ F(x,y) &= a_2(x-3) + a_3\left(x^2 - 9\right) + a_4y \\ F(x,y) &= (x-3)\left(a_2 + a_3(x+3)\right) + a_4y. \end{aligned}$$

Aux points R_i on a $(x-3)(a_2 + a_3(x+3)) + a_4y = 0$, 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

$$\begin{aligned} y^2 = x^5 - 243 &\Leftrightarrow (x-3)^2\left(\lambda_1 + \lambda_2(x+3)\right)^2 = x^5 - 243. \\ &\Leftrightarrow (x-3)^2\left(\lambda_1 + \lambda_2(x+3)\right)^2 = (x-3)(x^4 + 3x^3 + 9x^2 + 27x + 81). \end{aligned}$$

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

$$(x-3)\left(\lambda_1 + \lambda_2(x+1)\right)^2 = x^4 + 3x^3 + 9x^2 + 27x + 81;$$

d'où

$$x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)\left(\lambda_1 + \lambda_2(x+1)\right)^2 = 0.$$

On trouve ainsi une famille de points quartiques donnée par :

$$\mathcal{A}_2 = \left\{ \begin{array}{l} \left(x, (x-3)(\lambda_1 + \lambda_2(x+3))\right) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ et } x \text{ racine de} \\ \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)\left(\lambda_1 + \lambda_2(x+1)\right)^2 \end{array} \right\}.$$

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

2.1.4 Points quintiques

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

$$\mathcal{B}_1 = \left\{ \begin{array}{l} \left(x, \alpha_1 + \alpha_2 x + \alpha_3 x^2\right) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_1(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\},$$

$$\mathcal{B}_2 = \left\{ \begin{array}{l} \left(x, (x-3)\left[n_1 + n_2(x+3) + n_3(x^2+3x+9)\right]\right) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_2(x) = (x-3)\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}.$$

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 et R_5 les conjugués de Galois de R et 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

$$t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = a\,[P - \infty]\,,\ a \in \{0, 1\}\,. \quad (4)$$

On a les deux cas suivants :
Premier cas : $a = 0$.
La relation (4) 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty;$$

donc $F \in \mathcal{L}(5\infty)$, 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

$$\alpha_1 = \frac{-a_1}{a_4}\ ,\ \alpha_2 = \frac{-a_2}{a_4} \text{ et } \alpha_3 = \frac{-a_3}{a_4}.$$

En remplaçant y par son expression dans la relation $y^2 = x^5 - 243$, on obtient :

$$x^5 - 243 = \alpha_1^2 + \alpha_2^2 x^2 + \alpha_3^2 x^4 + 2\alpha_1\alpha_2 x + 2\alpha_1\alpha_3 x^2 + 2\alpha_2\alpha_3 x^3;$$

d'où

$$x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_3)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) = 0.$$

On trouve ainsi une famille de points quintiques

$$\mathcal{B}_1 = \left\{ \begin{array}{l} \left(x, \alpha_1 + \alpha_2 x + \alpha_3 x^2\right) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_1(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2\alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\}.$$

Deuxième cas : $a = 1$.
La relation (4) 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty;$$

donc $F \in \mathcal{L}(6\infty)$, 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 obtient :

$$\begin{aligned} F(x,y) &= -3a_2 - 9a_3 - 37a_5 + a_2x + a_3x^2 + a_4y + a_5x^3, \\ &= a_2(x-3) + a_3(x^2-9) + a_5(x^3-27) + a_4y. \end{aligned}$$

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 $n_1, n_2, n_3 \in \mathbb{Q}^*$.
Finalement on a :

$$y = (x-3)\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right).$$

En remplaçant y par son expression dans la relation

$$y^2 = x^5 - 243,$$

on a :

$$(x-3)^2\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 = x^5 - 243,$$
$$(x-3)^2\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 = (x-3)(x^4+3x^3+9x^2+27x+81).$$

En simplifiant par $x-3$, on obtient :

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

On trouve ainsi une famille de points quintiques

$$\mathcal{B}_2 = \left\{ \begin{array}{l} \left(x, (x-3)\left[n_1 + n_2(x+3) + n_3(x^2+3x+9)\right]\right) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B_2(x) = (x-3)\left(n_1 + n_2(x+3) + n_3(x^2+3x+9)\right)^2 - (x^4+3x^3+9x^2+27x+81) \end{array} \right\}.$$

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

CQFD $\square$

2.2 Points algébriques de degrés au plus 5 sur la courbe affine $\mathcal{C} : y^2 = 3x(x^4 + 3)$

Cette section complète et étend les travaux de Bruin [1].
Nous nous proposons d'étudier en détail les points algébriques de degrés au plus 5 sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = 3x(x^4+3)$. La courbe est hyperelliptique de genre $g = 2$ d'après N. Bruin.
Notons $P = (0, 0)$ et ∞ le point à l'infini de coordonnées projectives $(0, 1, 0)$.
Dans [1] N. Bruin a donné une description des points de degrés 1 sur $\mathbb{Q}$.
Cette description s'énonce comme suit :

Proposition (Bruin).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

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

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 [1]),
- Le théorème d'Abel-Jacobi (voir [5]),
- 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*

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

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, x(\lambda_1 + \lambda_2 x)\ \mid \lambda_1, \lambda_2 \in \mathbb{Q}^*\ \textit{et } x\ \textit{racine de} \\ \\ F(x) = 3(x^4 + 3) - x\left((\lambda_1 + \lambda_2 x)\right)^2 \end{array} \right\}.$$

4. *L'ensemble des points quintiques sur* $\mathcal{C}$ *est donné par* $\mathcal{A}_1 \cup \mathcal{A}_2$ *avec*

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

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

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 $\overline{\mathbb{Q}}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\overline{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$. On montre dans [1] que le groupe de Mordell-Weil $J(\mathbb{Q})$ de la jacobienne J de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

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

$$\mathcal{C} : Y^2Z^3 = 3X(X^4 + 3Z^4).$$

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

Lemme 2.2.1.

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

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

$$div(x-a) = (X - aZ = 0).\mathcal{C} - (Z = 0).\mathcal{C}.$$

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 2.2.2.

- $\mathcal{L}(\infty) = \langle 1 \rangle$,

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

Preuve. Résulte du Lemme 2.2.1.

Lemme 2.2.3. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle 0, [(0,0) - \infty]\rangle = \{b\,[P - \infty]\,, b \in \{0,1\}\}$.

Preuve. (voir [1])

Démonstration du théorème

2.2.1 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. On a $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

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

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty,$$

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 la relation $y^2 = 3x(x^4+3)$, on obtient : $y^2 = 3\alpha(\alpha^4+3)$; et par suite on a :

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

On a ainsi une famille de points quadratiques donnée par

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

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty,$$

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 $\mathcal{S}$.

2.2.2 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. On a

$$t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 - 3\infty,$$

donc $F \in \mathcal{L}(3\infty)$ et comme$\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + P - 4\infty,$$

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

$$F(x, y) = x(a_2 + a_3x).$$

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 degrés ≤ 2.

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

2.2.3 Points quartiques sur $\mathcal{C}$

L'ensemble des points quartiques sur $\mathcal{C}$ est donné par $\mathcal{C}_1 \cup \mathcal{C}_2$ avec

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

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

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. On a

$$t = [R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty,$$

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

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

On trouve ainsi une famille de points quartiques donnée par

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

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = [R_1 + R_2 + R_3 + R_4 + P - 5\infty],$$

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

$$F(x,y) = x(a_2 + a_3 x) + a_4 y.$$

Aux points R_i, on a $y = x(\lambda_1 + \lambda_2 x)$ avec $\lambda_1 = \dfrac{-a_2}{a_4}$, $\lambda_2 = \dfrac{-a_3}{a_4}$ avec $\lambda_1, \lambda_2 \in \mathbb{Q}^*$.
En remplaçant y par son expression dans la relation $y^2 = 3x(x^4+3)$, on a :

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

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

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

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

2.2.4 Points quintiques sur $\mathcal{C}$

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

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

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

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. On a $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty,$$

donc $F \in \mathcal{L}(5\infty)$, 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 $\alpha_1 = \dfrac{-a_1}{a_4}$, $\alpha_2 = \dfrac{-a_2}{a_4}$, $\alpha_3 = \dfrac{-a_3}{a_4}$ et $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^*$.
En remplaçant y par son expression dans la relation $y^2 = 3x(x^4+3)$, on a :

$$(\alpha_1 + \alpha_2 x + \alpha_3 x^2)^2 = 3x(x^4+3)$$

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

On trouve ainsi une famille de points quintiques donnée par

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

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty,$$

donc $F \in \mathcal{L}(6\infty)$, 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 obtient :

$$F(x,y) = a_2 x + a_3 x^2 + a_4 y + a_5 x^3.$$

Aux points R_i, on a : $a_2 x + a_3 x^2 + a_4 y + a_5 x^3 = 0$, donc $y = n_1 x + n_2 x^2 + n_3 x^3$ avec $n_1 = \dfrac{-a_2}{a_4}$, $n_2 = \dfrac{-a_3}{a_4}$, $n_3 = \dfrac{-a_5}{a_4}$ et $n_1, n_2, n_3 \in \mathbb{Q}^*$.

En remplaçant y par son expression dans la relation $y^2 = 3x(x^4+3)$, on a :

$$(n_1 x + n_2 x^2 + n_3 x^3)^2 = 3x(x^4+3)$$

$$(n_1 x + n_2 x^2 + n_3 x^3)^2 - 3x(x^4+3) = 0$$

$$x\left(x(n_1 + n_2 x + n_3 x^2)^2 - 3(x^4+3)\right) = 0$$

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

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

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

CQFD □

2.3 Points algébriques de degrés au plus 4 sur la courbe affine $\mathcal{C} : y^2 = x(x^2+1)(x^2+3)$

Cette section complète et étend les travaux de Siksek [13].

Nous nous proposons d'étudier en détail les points algébriques de degrés au plus 4

sur $\mathbb{Q}$ sur la courbe affine $y^2 = x(x^2+1)(x^2+3)$. La courbe est de genre $g = 2$. Notons $Q_0 = (0,0)$, ∞ le point à l'infini de coordonnées projectives $(0,1,0)$ et $\mathcal{C}^{(d)}(\mathbb{Q})$ l'ensemble des points algébriques sur $\mathcal{C}$ de degrés d sur $\mathbb{Q}$.
Posons

$$\begin{aligned} &Q_1 = (i,0)\ ,\ \overline{Q}_1 = (-i,0)\ , \\ &Q_2 = \left(\sqrt{-3},0\right)\ ,\ \overline{Q}_2 = \left(-\sqrt{-3},0\right)\ , \\ &D_0 = Q_1 + \overline{Q}_1\ . \end{aligned}$$

Dans [13] Siksek a donné une description des points rationnels. Cette description s'énonce comme suit :

Proposition (Siksek).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{Q_0\ ,\ \infty\}.$$

Nous étendons ce résultat en donnant une paramétrisation des points algébriques sur $\mathcal{C}$ de degrés ≤ 4 sur $\mathbb{Q}$.

Nos outils fondamentaux sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ (voir [13]),
- Le Théorème d'Abel-Jacobi (voir [5]),
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre principal résultat s'énonce comme suit :

Théorème. *L'ensemble des points algébriques sur $\mathcal{C}$ de degrés au plus 4 sur $\mathbb{Q}$ est donné par* :

$$\bigcup_{[K:\mathbb{Q}]\leq 4} \mathcal{C}(K) = \{Q_0\ ,\ \infty\} \cup \mathcal{C}^{(2)}(\mathbb{Q}) \cup \mathcal{C}^{(3)}(\mathbb{Q}) \cup \mathcal{C}^{(4)}(\mathbb{Q}) \text{ avec}$$

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \left\{Q_1\ ,\ \overline{Q}_1\ ,\ Q_2\ ,\ \overline{Q}_2\right\} \cup \left\{\left(\alpha, \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)}\ \right)\ \mid\ \alpha \in \mathbb{Q}^*\right\},$$

$$\mathcal{C}^{(3)}(\mathbb{Q}) = \mathcal{F}_1 \cup \mathcal{F}_2,$$

$$\mathcal{C}^{(4)}(\mathbb{Q}) = \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3 \cup \mathcal{G}_4, \text{ où}$$

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \left(x, \lambda(x^2+1)\right)\ \mid\ \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_1(x) = x^3 - \lambda^2 x^2 + 3x - \lambda^2 \end{array} \right\},$$

$$\mathcal{F}_2 = \left\{ \begin{array}{l} \left(x, \lambda x(x^2+1)\right)\ \mid\ \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_2(x) = \lambda^2 x^3 - x^2 + \lambda^2 x - 3 \end{array} \right\},$$

$$\mathcal{G}_1 = \left\{ \left(x, \pm\sqrt{x(x^2+1)(x^2+3)} \right) \mid x \in \overline{\mathbb{Q}} \text{ et } [\mathbb{Q}(x):\mathbb{Q}] = 2 \right\},$$

$$\mathcal{G}_2 = \left\{ \begin{array}{l} \big(x, \lambda(x-\mu)(x^2+1)\big) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ A(x) = \lambda^2(x-\mu)^2(x^2+1) - x^3 - 3x \end{array} \right\},$$

$$\mathcal{G}_3 = \left\{ \begin{array}{l} (x, \lambda x(x-\mu)) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ B(x) = x^4 - \lambda^2 x^3 + (2\lambda^2\mu + 4)x^2 - \lambda^2\mu^2 x + 3 \end{array} \right\},$$

$$\mathcal{G}_4 = \left\{ \begin{array}{l} \left(x, \dfrac{\lambda}{x-\mu} x(x^2+1) \right) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ C(x) = (x-\mu)^2(x^2+3) - \lambda^2 x^3 - \lambda^2 x \end{array} \right\}.$$

Résultats auxiliaires

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

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

$l(D)$ désigne la $\overline{\mathbb{Q}}$-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 :

$$\left\{ \begin{array}{l} x(X,Y,Z) = \dfrac{X}{Z} \\ \\ y(X,Y,Z) = \dfrac{Y}{Z} \end{array} \right.$$

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

$$Y^2Z^3 = X(X^2+Z^2)(X^2+3Z^2).$$

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

On a $\mathcal{C} : y^2 = x(x^2+1)(x^2+3)$.

Lemme 2.3.1.

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

(*ii*) $div(x^2+1) = 2Q_1 + 2\overline{Q}_1 - 4\infty$.

(iii) $div(x^2+3) = 2Q_2 + 2\overline{Q}_2 - 4\infty$.

(iv) $div(y) = Q_0 + Q_1 + \overline{Q}_1 + Q_2 + \overline{Q}_2 - 5\infty$.

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

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

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

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

pour $w = x$ et $a = 0$ 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 :

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

On a :

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

$$\begin{cases} div(x-\sqrt{-3}) = 2Q_2 - 2\infty \\ div(x+\sqrt{-3}) = 2\overline{Q}_2 - 2\infty \end{cases}$$

D'où

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

□

Conséquences du Lemme 2.3.1

* $2j\,(Q_0) = 0$
* $2j\,(D_0) = 2j\left(Q_2 + \overline{Q}_2\right) = 0.$

Lemme 2.3.2.

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

Preuve. C'est une conséquence du Lemme 2.3.1 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

□

Lemme 2.3.3.

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

Preuve. Voir [13].

□

Démonstration du théorème

2.3.1 Points quadratiques

L'ensemble des points algébriques sur $\mathcal{C}$ de degrés 2 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \{Q_1 \ , \ \overline{Q}_1 \ , \ Q_2 \ , \ \overline{Q}_2\} \cup \left\{ \left(\alpha, \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)} \right) \ | \ \alpha \in \mathbb{Q}^* \right\}$$

Preuve. Soit un point $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$.
Notons R_1, R_2 les points conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 - 2\infty].$$

On remarque qu'aucun des R_i , $i = 1, 2$ n'est égal à Q_0 ou ∞ car $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. On a $t \in J(\mathbb{Q})$ et le Lemme 2.3.3 donne

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

Ainsi, on obtient :

$$[R_1 + R_2 - 2\infty] = mj(Q_0) + nj(D_0) \ , \ 0 \leq m \ , \ n \leq 1 \tag{2.1}$$

Notre démonstration se scinde en quatre cas suivants :

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

La relation (2.1) devient

$$[R_1 + R_2 - 2\infty] = 0.$$

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

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

Donc $\mathrm{f} \in \mathcal{L}(2\infty)$; d'où $\mathrm{f}(x, y) = a_0 + a_1 x$ avec $a_1 \neq 0$ sinon $\mathcal{L}(2\infty) = \mathcal{L}(\infty)$.
Aux points R_i, on a $a_0 + a_1 x = 0$; d'où $x = -\dfrac{a_0}{a_1}$; on doit avoir $a_0 \neq 0$ sinon un des R_i devrait être égal à Q_0. On voit que x est de la forme $x = \alpha$ avec $\alpha = -\dfrac{a_0}{a_1} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\Longleftrightarrow y^2 = \alpha(\alpha^2+1)(\alpha^2+3) \\ &\Longleftrightarrow y = \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)} \ . \end{aligned}$$

Ainsi on trouve une famille de points quadratiques donnée par :

$$\mathcal{S}_{00} = \left\{ \left(\alpha, \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)} \right) \mid \alpha \in \mathbb{Q}^* \right\}.$$

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

La relation (2.1) devient

$$[R_1 + R_2 - 2\infty] = j(D_0) = -j(D_0) \ ;$$

d'où

$$[R_1 + R_2 + Q_1 + \overline{Q}_1 - 4\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + Q_1 + \overline{Q}_1 - 4\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(4\infty)$; d'où $\mathrm{f}(x,y) = a_0 + a_1 x + a_2 x^2$ avec $a_2 \neq 0$ sinon $\mathcal{L}(4\infty) = \mathcal{L}(3\infty)$.
La fonction f est d'ordre 1 au point Q_1 ; donc on doit avoir

$$\begin{cases} a_1 = 0 \\ \\ a_0 = a_2 \end{cases}$$

Ainsi, on obtient :

$$\begin{aligned} \mathrm{f}(x,y) &= a_2 + a_2 x^2 \\ &= a_2(x^2+1). \end{aligned}$$

Aux points R_i , on a $x^2 + 1 = 0$ c'est-à-dire $x = \pm i$.
On trouve ainsi une famille de points quadratiques donnée par :

$$\mathcal{S}_{01} = \left\{ Q_1 \ , \ \overline{Q}_1 \right\}.$$

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

La relation (2.1) devient

$$[R_1 + R_2 - 2\infty] = j(Q_0) = -j(Q_0);$$

d'où

$$[R_1 + R_2 + Q_0 - 3\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + Q_0 - 3\infty.$$

Donc f $\in \mathcal{L}(3\infty)$. Puisque $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$ alors f $\in \mathcal{L}(2\infty)$ et par suite $div(\mathrm{f}) = R_1 + R_2 - 2\infty$. Par ailleurs, on a $div(\mathrm{f}) = R_1 + R_2 + Q_0 - 3\infty$; donc on doit avoir

$$R_1 + R_2 + Q_0 - 3\infty = R_1 + R_2 - 2\infty.$$

On voit que Q_0 devrait être égal à ∞, ce qui est absurde.

$$\underline{\textbf{Cas}} : m = 1 \text{ et } n = 1.$$

La relation (2.1) devient

$$[R_1 + R_2 - 2\infty] = j(Q_0) + j(D_0) = -j(Q_0) - j(D_0);$$

d'où

$$[R_1 + R_2 + Q_0 + Q_1 + \overline{Q}_1 - 5\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + Q_0 + Q_1 + \overline{Q}_1 - 5\infty.$$

Donc f $\in \mathcal{L}(5\infty)$; d'où $\mathrm{f}(x, y) = a_0 + a_1x + a_2x^2 + a_3y$ avec $a_3 \neq 0$ sinon $\mathcal{L}(5\infty) = \mathcal{L}(4\infty)$. La fonction f est d'ordre 1 aux points Q_0 , Q_1 ; donc on doit avoir

$$\begin{cases} a_0 = 0 \\ a_1 = 0 \\ a_2 = 0 \end{cases}$$

Ainsi, on obtient :

$$\mathrm{f}(x, y) = \ a_3y.$$

Aux points R_i , on a $y = 0$; d'où $x = 0$ ou $x = \pm i$ ou $x = \pm\sqrt{-3}$. Or $R_i \neq Q_0$; donc $x = \pm i$ ou $x = \pm\sqrt{-3}$.
On trouve ainsi une famille de points quadratiques donnée par :

$$\mathcal{S}_{11} = \left\{Q_1 \ , \ \overline{Q}_1 \ , \ Q_2 \ , \ \overline{Q}_2\right\}.$$

En conclusion, l'ensemble des points algébriques sur $\mathcal{C}$ de degrés 2 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \mathcal{S}_{00} \cup \mathcal{S}_{01} \cup \mathcal{S}_{11}$$

$$= \left\{Q_1 \ , \ \overline{Q}_1 \ , \ Q_2 \ , \ \overline{Q}_2\right\} \cup \left\{\left(\alpha, \pm\sqrt{\alpha(\alpha^2+1)(\alpha^2+3)}\right) \ | \ \alpha \in \mathbb{Q}^*\right\}$$

2.3.2 Points cubiques

L'ensemble des points algébriques sur $\mathcal{C}$ de degrés 3 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(3)}(\mathbb{Q}) = \mathcal{F}_1 \cup \mathcal{F}_2 \text{ avec}$$

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \big(x, \lambda(x^2+1)\big) \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_1(x) = x^3 - \lambda^2 x^2 + 3x - \lambda^2 \end{array} \right\}$$

$$\mathcal{F}_2 = \left\{ \begin{array}{l} \big(x, \lambda x(x^2+1)\big) \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_2(x) = \lambda^2 x^3 - x^2 + \lambda^2 x - 3 \end{array} \right\}$$

Preuve. Soit un point $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$.
Notons $R_1,\ R_2,\ R_3$ les points conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 + R_3 - 3\infty].$$

On remarque qu'aucun des R_i , $i = 1, 2, 3$ n'est égal à Q_0 , ∞ , Q_1 , $\overline{Q}_1$, Q_2 ou $\overline{Q}_2$. On a $t \in J(\mathbb{Q})$ et le Lemme 2.3.3 donne

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

Ainsi, on obtient :

$$[R_1 + R_2 + R_3 - 3\infty] = mj(Q_0) + nj(D_0) \text{ , } 0 \leq m \text{ , } n \leq 1 \tag{2.2}$$

Notre démonstration se scinde en quatre cas ci-après :

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

La relation (2.2) devient

$$[R_1 + R_2 + R_3 - 3\infty] = 0.$$

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

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

Donc $\mathrm{f} \in \mathcal{L}(3\infty)$. Comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$ alors $\mathrm{f} \in \mathcal{L}(2\infty)$ et par conséquent

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

On a déjà $div(\mathrm{f}) = R_1 + R_2 + R_3 - 3\infty$; donc on doit avoir

$$R_1 + R_2 + R_3 - 3\infty = R_1 + R_2 - 2\infty.$$

On voit que un des R_i devrait être égal à ∞, ce qui est absurde.

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

La relation (2.2) devient

$$[R_1 + R_2 + R_3 - 3\infty] = j(D_0) = -j(D_0);$$

d'où

$$[R_1 + R_2 + R_3 + Q_1 + \overline{Q}_1 - 5\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + R_3 + Q_1 + \overline{Q}_1 - 5\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(5\infty)$; d'où $\mathrm{f}(x, y) = a_0 + a_1 x + a_2 x^2 + a_3 y$ avec $a_3 \neq 0$ sinon $\mathcal{L}(5\infty) = \mathcal{L}(4\infty)$. La fonction f est d'ordre 1 au point Q_1 ; donc on doit avoir

$$\begin{cases} a_0 = a_2 \\ \\ a_1 = 0 \end{cases}$$

Ainsi, on obtient : $\mathrm{f}(x, y) = a_2(x^2 + 1) + a_3 y$.
Aux points R_i , on a $a_2(x^2 + 1) + a_3 y = 0$; d'où

$$y = -\frac{a_2}{a_3}(x^2 + 1);$$

on doit avoir $a_2 \neq 0$ sinon un des R_i devrait vérifier $R_i \in \{Q_0\ ,\ Q_1\ ,\ \overline{Q}_1\ ,\ Q_2\ ,\ \overline{Q}_2\}$.

On voit que y est de la forme $y = \lambda(x^2 + 1)$ avec $\lambda = -\dfrac{a_2}{a_3} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\Longleftrightarrow \lambda^2(x^2+1)^2 = x(x^2+1)(x^2+3) \\ &\Longleftrightarrow \lambda^2(x^2+1) = x(x^2+3) \\ &\Longleftrightarrow x^3 - \lambda^2 x^2 + 3x - \lambda^2 = 0. \end{aligned}$$

Ainsi on trouve une famille de points cubiques donnée par :

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \big(x, \lambda(x^2+1)\big) \ \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_1(x) = x^3 - \lambda^2 x^2 + 3x - \lambda^2 \end{array} \right\}$$

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

La relation (2.2) devient

$$[R_1 + R_2 + R_3 - 3\infty] = j(Q_0) = -j(Q_0);$$

d'où

$$[R_1 + R_2 + R_3 + Q_0 - 4\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + R_3 + Q_0 - 4\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(4\infty)$; d'où $\mathrm{f}(x, y) = a_0 + a_1 x + a_2 x^2$ avec $a_2 \neq 0$ sinon $\mathcal{L}(4\infty) = \mathcal{L}(3\infty)$.
La fonction f est d'ordre 1 au point Q_0 ; donc on doit avoir $a_0 = 0$.
Ainsi, on obtient :

$$\mathrm{f}(x, y) = x(a_2 x + a_1).$$

Aux points R_i , on a $x(a_2 x + a_1) = 0$, donc $x \in \mathbb{Q}$ et par suite les R_i devraient être de degrés ≤ 2 , ce qui est absurde.

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

La relation (2.2) devient

$$[R_1 + R_2 + R_3 - 3\infty] = j(Q_0) + j(D_0) = -j(Q_0) - j(D_0);$$

d'où

$$[R_1 + R_2 + R_3 + Q_0 + Q_1 + \overline{Q}_1 - 6\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + R_3 + Q_0 + Q_1 + \overline{Q}_1 - 6\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(6\infty)$ et par suite $\mathrm{f}(x, y) = a_0 + a_1 x + a_2 x^2 + a_3 y + a_4 x^3$ avec $a_4 \neq 0$ sinon $\mathcal{L}(6\infty) = \mathcal{L}(5\infty)$.
La fonction f est d'ordre 1 aux points Q_0 , Q_1; donc on doit avoir $a_0 = a_2 = 0$ et $a_1 = a_4$.
Ainsi, on obtient :

$$\mathrm{f}(x, y) = a_4 x(x^2 + 1) + a_3 y.$$

Aux points R_i, on a $a_4 x(x^2 + 1) + a_3 y = 0$; donc

$$y = -\frac{a_4}{a_3} x(x^2 + 1) \quad (a_3 \neq 0).$$

On voit que y est de la forme

$$y = \lambda x(x^2 + 1)$$

avec $\lambda = -\dfrac{a_4}{a_3} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\Longleftrightarrow \lambda^2 x^2(x^2+1)^2 = x(x^2+1)(x^2+3) \\ &\Longleftrightarrow \lambda^2 x(x^2+1) = (x^2+3) \\ &\Longleftrightarrow \lambda^2 x^3 + \lambda^2 x = x^2 + 3 \\ &\Longleftrightarrow \lambda^2 x^3 - x^2 + \lambda^2 x - 3 = 0. \end{aligned}$$

On trouve ainsi une famille de points cubiques donnée par :

$$\mathcal{F}_2 = \left\{ \begin{array}{l} \big(x, \lambda x(x^2+1)\big) \mid \lambda \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A_2(x) = \lambda^2 x^3 - x^2 + \lambda^2 x - 3 \end{array} \right\}$$

En conclusion, l'ensemble des points algébriques sur $\mathcal{C}$ de degrés 3 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(3)}(\mathbb{Q}) = \mathcal{F}_1 \cup \mathcal{F}_2.$$

2.3.3 Points quartiques

L'ensemble des points algébriques sur $\mathcal{C}$ de degrés 4 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(4)}(\mathbb{Q}) = \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3 \cup \mathcal{G}_4 \text{ avec}$$

$$\mathcal{G}_1 = \left\{ \left(x, \pm\sqrt{x(x^2+1)(x^2+3)} \right) \mid x \in \overline{\mathbb{Q}} \text{ et } [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

$$\mathcal{G}_2 = \left\{ \begin{array}{l} \big(x, \lambda(x-\mu)(x^2+1)\big) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A(x) = \lambda^2(x-\mu)^2(x^2+1) - x^3 - 3x \end{array} \right\}$$

$$\mathcal{G}_3 = \left\{ \begin{array}{l} (x, \lambda x(x-\mu)) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B(x) = x^4 - \lambda^2 x^3 + (2\lambda^2\mu + 4)x^2 - \lambda^2\mu^2 x + 3 \end{array} \right\}$$

$$\mathcal{G}_4 = \left\{ \begin{array}{l} \left(x, \dfrac{\lambda}{x-\mu} x(x^2+1) \right) \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ C(x) = (x-\mu)^2(x^2+3) - \lambda^2 x^3 - \lambda^2 x \end{array} \right\}$$

Preuve. Soit un point $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 4$.
Notons $R_1,\ R_2,\ R_3,\ R_4$ les points conjugués de Galois de R et travaillons avec

$$t = [R_1 + R_2 + R_3 + R_4 - 4\infty].$$

On remarque qu'aucun des R_i , $i = 1, 2, 3, 4$ n'est égal à Q_0 , ∞ , Q_1 , $\overline{Q}_1$, Q_2 ou $\overline{Q}_2$. On a $t \in J(\mathbb{Q})$ et le Lemme 2.3.3 donne

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

Ainsi, on obtient :

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = mj(Q_0) + nj(D_0) \ , \ 0 \leq m \ , \ n \leq 1 \tag{2.3}$$

Notre démonstration se scinde en quatre cas suivants :

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

La relation (2.3) 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 définie sur $\mathbb{Q}$ telle que

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

Donc $\mathrm{f} \in \mathcal{L}(4\infty)$ et par suite $\mathrm{f}(x, y) = a_0 + a_1x + a_2x^2$ avec $a_2 \neq 0$ sinon $\mathcal{L}(4\infty) = \mathcal{L}(3\infty)$. Aux points R_i , on a $a_0 + a_1x + a_2x^2 = 0$.
La relation $y^2 = x(x^2 + 1)(x^2 + 3)$ donne

$$y = \pm\sqrt{x(x^2 + 1)(x^2 + 3)} \ .$$

On trouve ainsi une famille de points quartiques

$$\mathcal{G}_1 = \left\{ \left(x, \pm\sqrt{x(x^2 + 1)(x^2 + 3)} \right) \ | \ x \in \overline{\mathbb{Q}} \text{ et } [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

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

La relation (2.3) devient

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = j(D_0) = -j(D_0);$$

d'où

$$[R_1 + R_2 + R_3 + R_4 + Q_1 + \overline{Q}_1 - 6\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + R_3 + R_4 + Q_1 + \overline{Q}_1 - 6\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(6\infty)$ et par suite $\mathrm{f}(x, y) = a_0 + a_1x + a_2x^2 + a_3y + a_4x^3$ avec $a_4 \neq 0$ sinon $\mathcal{L}(6\infty) = \mathcal{L}(5\infty)$. La fonction f est d'ordre 1 au point Q_1 ; donc on doit avoir

$a_0 = a_2$ et $a_1 = a_4$.
Ainsi, on obtient :

$$\begin{aligned} \mathrm{f}(x,y) &= a_2 + a_4x + a_2x^2 + a_3y + a_4x^3 \\ &= a_2(x^2+1) + a_4x(x^2+1) + a_3y. \end{aligned}$$

Aux points R_i , on a $a_2(x^2+1) + a_4x(x^2+1) + a_3y = 0$; donc

$$y = -\frac{a_4}{a_3}\left(x + \frac{a_2}{a_4}\right)(x^2+1) \ ;$$

on doit avoir $a_2 \neq 0$ et $a_3 \neq 0$ sinon un des R_i devrait vérifier $R_i \in \{Q_0 \ , \ Q_1 \ , \ \overline{Q}_1\}$. On voit que y est de la forme

$$y = \lambda(x-\mu)(x^2+1)$$

avec $\lambda = -\dfrac{a_4}{a_3} \in \mathbb{Q}^*$ et $\mu = -\dfrac{a_2}{a_4} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\Longleftrightarrow \lambda^2(x-\mu)^2(x^2+1)^2 = x(x^2+1)(x^2+3) \\ &\Longleftrightarrow \lambda^2(x-\mu)^2(x^2+1) = x(x^2+3) \\ &\Longleftrightarrow \lambda^2(x-\mu)^2(x^2+1) - x^3 - 3x = 0. \end{aligned}$$

On trouve ainsi une famille de points quartiques donnée par :

$$\mathcal{G}_2 = \left\{ \begin{array}{l} \big(x, \lambda(x-\mu)(x^2+1)\big) \ \mid \lambda \ , \ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ A(x) = \lambda^2(x-\mu)^2(x^2+1) - x^3 - 3x \end{array} \right\}$$

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

La relation (2.3) devient

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = j(Q_0) = -j(Q_0);$$

d'où

$$[R_1 + R_2 + R_3 + R_4 + Q_0 - 5\infty] = 0.$$

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

$$div(\mathrm{f}) = R_1 + R_2 + R_3 + R_4 + Q_0 - 5\infty.$$

Donc $\mathrm{f} \in \mathcal{L}(5\infty)$ et par suite $\mathrm{f}(x,y) = a_0 + a_1x + a_2x^2 + a_3y$ avec $a_3 \neq 0$ sinon $\mathcal{L}(5\infty) = \mathcal{L}(4\infty)$. La fonction f est d'ordre 1 au point Q_0 ; donc on doit avoir $a_0 = 0$.
Ainsi, on obtient :

$$\mathrm{f}(x,y) = a_1x + a_2x^2 + a_3y.$$

Aux points R_i , on a $a_1x + a_2x^2 + a_3y = 0$; donc

$$y = -\frac{a_2}{a_3}x\left(x + \frac{a_1}{a_2}\right) \ ;$$

on doit avoir $a_1 \neq 0$ et $a_2 \neq 0$ sinon un des R_i devrait vérifier
$R_i \in \{Q_0\ ,\ Q_1\ ,\ \overline{Q}_1\ ,\ Q_2\ ,\ \overline{Q}_2\}$. On voit que y est de la forme $y = \lambda x(x-\mu)$ avec $\lambda = -\frac{a_2}{a_3} \in \mathbb{Q}^*$ et $\mu = -\frac{a_1}{a_2} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\iff \lambda^2x^2(x-\mu)^2 = x(x^2+1)(x^2+3) \\ &\iff \lambda^2x(x-\mu)^2 = (x^2+1)(x^2+3) \\ &\iff \lambda^2x(x^2-2\mu x+\mu^2) = x^4+4x^2+3 \\ &\iff \lambda^2x^3 - 2\lambda^2\mu x^2 + \lambda^2\mu^2x = x^4+4x^2+3 \\ &\iff x^4 - \lambda^2x^3 + (2\lambda^2\mu+4)x^2 - \lambda^2\mu^2x + 3 = 0. \end{aligned}$$

On trouve ainsi une famille de points quartiques donnée par :

$$\mathcal{G}_3 = \left\{ \begin{array}{l} (x, \lambda x(x-\mu)) \ \mid \lambda\ ,\ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ B(x) = x^4 - \lambda^2x^3 + (2\lambda^2\mu+4)x^2 - \lambda^2\mu^2x + 3 \end{array} \right\}$$

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

La relation (2.3) devient $[R_1+R_2+R_3+R_4-4\infty] = j(Q_0)+j(D_0) = -j(Q_0)-j(D_0)$; d'où $[R_1+R_2+R_3+R_4+Q_0+Q_1+\overline{Q}_1-7\infty] = 0$.
Le théorème d'Abel-Jacobi entraine l'existence d'une fonction rationnelle f définie sur $\mathbb{Q}$ telle que $div(\mathrm{f}) = R_1+R_2+R_3+R_4+Q_0+Q_1+\overline{Q}_1-7\infty$.
D'où $\mathrm{f} \in \mathcal{L}(7\infty)$ et par suite $\mathrm{f}(x,y) = a_0 + a_1x + a_2x^2 + a_3y + a_4x^3 + a_5xy$ avec $a_5 \neq 0$ sinon $\mathcal{L}(7\infty) = \mathcal{L}(6\infty)$.
La fonction f est d'ordre 1 aux points Q_0 , Q_1 ; donc on doit avoir $a_0 = a_2 = 0$ et $a_1 = a_4$.
Ainsi, on obtient :

$$\mathrm{f}(x,y) = a_4x(x^2+1) + a_5y\left(x + \frac{a_3}{a_5}\right).$$

Aux points R_i , on a $a_4x(x^2+1) + a_5y\left(x + \frac{a_3}{a_5}\right) = 0$; donc

$$y = -\frac{a_4}{a_5}\frac{x}{\left(x+\frac{a_3}{a_5}\right)}(x^2+1) \ ;$$

on doit avoir $a_4 \neq 0$ et $a_3 \neq 0$ sinon un des R_i devrait vérifier
$R_i \in \{Q_0\ ,\ Q_1\ ,\ \overline{Q}_1\ ,\ Q_2\ ,\ \overline{Q}_2\}$. On voit que y est de la forme

$$y = \frac{\lambda}{x-\mu}x(x^2+1)$$

avec $\lambda = -\dfrac{a_4}{a_5} \in \mathbb{Q}^*$ et $\mu = -\dfrac{a_3}{a_5} \in \mathbb{Q}^*$ et par suite on a

$$\begin{aligned} y^2 = x(x^2+1)(x^2+3) &\iff \frac{\lambda^2}{(x-\mu)^2}x^2(x^2+1)^2 = x(x^2+1)(x^2+3) \\ &\iff \frac{\lambda^2}{(x-\mu)^2}x(x^2+1) = (x^2+3) \\ &\iff \lambda^2 x(x^2+1) = (x-\mu)^2(x^2+3) \\ &\iff \lambda^2 x^3 + \lambda^2 x = (x-\mu)^2(x^2+3) \\ &\iff (x-\mu)^2(x^2+3) - \lambda^2 x^3 - \lambda^2 x = 0. \end{aligned}$$

On trouve ainsi une famille de points quartiques donnée par :

$$\mathcal{G}_4 = \left\{ \begin{array}{l} \left(x, \dfrac{\lambda}{x-\mu}x(x^2+1)\right) \mid \lambda\ ,\ \mu \in \mathbb{Q}^* \text{ et } x \text{ racine de} \\ \\ C(x) = (x-\mu)^2(x^2+3) - \lambda^2 x^3 - \lambda^2 x \end{array} \right\}$$

En conclusion, l'ensemble des points algébriques sur $\mathcal{C}$ de degrés 4 sur $\mathbb{Q}$ est donné par :

$$\mathcal{C}^{(4)}(\mathbb{Q}) = \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_3 \cup \mathcal{G}_4.$$

CQFD $\square$

Chapitre 3

Points algébriques de degrés quelconques

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 $\mathcal{C}$ rationnels sur K et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ définis sur K de degrés $\leq$ d.

3.1 Points algébriques de degrés quelconques sur la courbe affine $\mathcal{C} : y^2 = x(x^2+1)(x^2+3)$

Dans cette section, notre travail va consister en l'étude de quelques cas particuliers où l'on peut déterminer explicitement les points algébriques de degrés quelconques sur la courbe d'équation affine

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

Dans [13], il a été montré que le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de la courbe à étudier est fini.
La courbe $\mathcal{C}$ est de genre $g = 2$.

Notons $Q_0 = (0,0), \infty$ le point à l'infini de coordonnées projectives $(0,1,0)$ et

$$\begin{aligned} &Q_1 = (i,0)\ ,\ \overline{Q}_1 = (-i,0)\ , \\ &Q_2 = \left(\sqrt{-3},0\right)\ ,\ \overline{Q}_2 = \left(-\sqrt{-3},0\right)\ , \\ &D_0 = Q_1 + \overline{Q}_1\ . \end{aligned}$$

Dans [13] Siksek a donné une description des points rationnels de $\mathcal{C}$.
Cette description s'énonce comme suit :

Proposition (**Siksek**).

Les points $\mathbb{Q}$-rationnels de la courbe $\mathcal{C}$ sont donnés par :

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

Nous étendons ce résultat, en donnant une description explicite des points algébriques de degrés quelconques sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.

Nos outils fondamentaux sont :

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

◦ Le Théorème d'Abel-Jacobi (voir [5]),

◦ Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre principal résultat s'énonce comme suit :

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

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

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

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

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

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

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

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

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

Résultats auxiliaires

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

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

$l(D)$ désigne la $\overline{\mathbb{Q}}$-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 :

$$\left\{ \begin{array}{l} x(X,Y,Z) = \dfrac{X}{Z} \\ \\ y(X,Y,Z) = \dfrac{Y}{Z} \end{array} \right.$$

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

$$Y^2 Z^3 = X(X^2 + Z^2)(X^2 + 3Z^2).$$

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

On a $\mathcal{C} : y^2 = x(x^2+1)(x^2+3)$.

Lemme 3.1.1.

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

(ii) $div(x^2+1) = 2Q_1 + 2\overline{Q}_1 - 4\infty$.

(iii) $div(x^2+3) = 2Q_2 + 2\overline{Q}_2 - 4\infty$.

(iv) $div(y) = Q_0 + Q_1 + \overline{Q}_1 + Q_2 + \overline{Q}_2 - 5\infty$.

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

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

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

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

pour $w = x$ et $a = 0$ 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 :

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

On a :

$$\begin{cases} div(x - i) = 2Q_1 - 2\infty \\ \\ div(x + i) = 2\overline{Q}_1 - 2\infty \end{cases} \quad ; \quad \begin{cases} div(x - \sqrt{-3}) = 2Q_2 - 2\infty \\ \\ div(x + \sqrt{-3}) = 2\overline{Q}_2 - 2\infty \end{cases}$$

D'où

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

□

Conséquences du Lemme 3.1.1

* $2j\,(Q_0) = 0$
* $2j\,(D_0) = 2j\left(Q_2 + \overline{Q}_2\right) = 0.$

Lemme 3.1.2.

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

Preuve. C'est une conséquence du Lemme 3.1.1 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

□

Lemme 3.1.3.

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

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

Preuve. Voir [3].

□

Lemme 3.1.4.

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

Preuve. Voir [13].

□

Démonstration du théorème

Soit un point $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = k$.
Les travaux de Siksek dans [13] 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 3.1.4 donne

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

Ainsi, on obtient :

$$[R_1 + R_2 + \cdots + R_k - k\infty] = mj(Q_0) + nj(D_0) \ , \ 0 \leq m \ , \ n \leq 1 \tag{3.1}$$

Notre démonstration se scinde en quatre cas suivants :

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

La formule (3.1) 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 3.1.3 , 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 (3.1) 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 3.1.3 , 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

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

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 :

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

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

La formule (3.1) 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 3.1.3 , 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 :

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

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

La formule (3.1) 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 f $\in \mathcal{L}((k+3)\infty)$ et d'après le Lemme 3.1.3 , 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 :

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

En conclusion, l'ensemble des points algébriques de degrés au plus d quelconques sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par :

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

CQFD □

3.2 Points algébriques de degrés quelconques sur la courbe affine $\mathcal{C} : y^2 = 3(x^5 - 1)$

Dans cette section, notre travail va consister en l'étude de quelques cas particuliers, où l'on peut déterminer explicitement les points algébriques de degrés quelconques sur la courbe d'équation affine $y^2 = 3(x^5 - 1)$.
Notons $P = (1, 0)$ et ∞ le point à l'infini de coordonnées projectives $(0, 1, 0)$.
Dans [14], Siksek a donné une description des points de degrés 1 sur $\mathbb{Q}$ sur cette courbe. Cette description s'énonce comme suit :

Proposition (Siksek).

Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

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

Nous étendons ce résultat, en donnant une description explicite des points algébriques de degrés quelconques sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.

Nos outils essentiels sont :

∘ Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ (voir [14]),

∘ Le théorème d'Abel Jacobi (voir [5]),

∘ Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :

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

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

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

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

On désigne par $(\mathcal{E}_k)$ l'équation suivante :

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

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 [14] que le groupe de Mordell-Weil $J(\mathbb{Q})$ de la jacobienne J 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 :

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

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

$$\mathcal{C} : Y^2 Z^3 = 3(X^5 - Z^5).$$

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 3.2.1.

- $div(x - 1) = 2P - 2\infty$,
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$,
- $div(x) = A_0 + A_1 - 2\infty$.

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

$$div(x - a) = (X - aZ = 0).\mathcal{C} - (Z = 0).\mathcal{C}.$$

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 $(Z = 0).\mathcal{C} = 5\infty$, donc

$$div(x-1) = 2P - 2\infty.$$

Lemme 3.2.2.

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

Preuve. Résulte du Lemme 3.2.1 et du fait que d'après le théorème de Riemann-Roch on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 3.2.3. .

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 [9]).

Lemme 3.2.4. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P - \infty] \rangle = \{ a\,[P - \infty],\ a \in \{0, 1\} \}$.

Preuve. (Voir [14]).

Démonstration du théorème

Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$, avec $[\mathbb{Q}[R] : \mathbb{Q}] = n$.
Les travaux de Siksek dans [14] 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 3.2.4 on a :

$$[R_1 + R_2 + \cdots + R_n - n\infty] = a\,[P - \infty],\ 0 \leq a \leq 1 \quad (*).$$

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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \cdots + R_n - n\infty,$$

donc $F \in \mathcal{L}(n\infty)$, et d'après le Lemme 3.2.3 on a

$$F(x,y) = \left(\sum_{i\leq \frac{n}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-5}{2}} b_j x^j\right).$$

Aux points R_i on doit avoir

$$\left(\sum_{i\leq \frac{n}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-5}{2}} b_j x^j\right) = 0,$$

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 donnée par

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

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 rationnelle F définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \cdots + R_n + P - (n+1)\infty,$$

donc $F \in \mathcal{L}((n+1)\infty)$, et d'après le Lemme 3.2.3, on a

$$F(x,y) = \left(\sum_{i\leq \frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq \frac{n-4}{2}} b_j x^j\right).$$

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

$$\left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq\frac{n-4}{2}} b_j x^j\right) = 0,$$

d'où

$$y = -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j};$$

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 donnée par

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

CQFD □

Chapitre 4

Points algébriques de petits degrés

Introduction

Soit $\mathcal{C}$ une courbe algébrique de genre g définie sur un corps de nombres K. Un théorème de Faltings dans [4] affirme que, si $g \geq 2$ alors l'ensemble $\mathcal{C}(K)$ des points rationnels sur K est fini. Une généralisation aux sous-variétés d'une variété abélienne permet une étude qualitative de l'ensemble des points de degrés bornés $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$.

4.1 Paramétrisation des points algébriques de petits degrés sur la courbe affine $\mathcal{C} : y^2 = x^5+20736$

Dans ce travail, nous déterminons une paramétrisation des points algébriques de degrés au plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$. La courbe $\mathcal{C}$ est hyperelliptique de genre 2 d'après Siksek et Stoll.
Notons $P = (0, 144)$, $\overline{P} = (0, -144)$ et ∞ le point à l'infini de coordonnées projectives $(0, 1, 0)$.
Dans [15] Siksek et Stoll ont donné une description des points de degrés 1 sur $\mathbb{Q}$. Cette description s'énonce comme suit :

Proposition (**Siksek** & **Stoll**)**.**

Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par :

$$\mathcal{C}(\mathbb{Q}) = \left\{P\ ,\ \overline{P}\ ,\ \infty\right\}.$$

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

Nos outils fondamentaux sont :

◦ Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne J de $\mathcal{C}$ (voir [15]),

◦ Le théorème d'Abel Jacobi (voir [5])

◦ 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*

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

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

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 [15] que le groupe de Mordell-Weil $J(\mathbb{Q})$ de la jacobienne J de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.
Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

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

$$\mathcal{C} : Y^2 Z^3 = X^5 + 20736 Z^5 \quad (a).$$

On désigne par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est-à-dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
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 4.1.1.

- $div(x) = P + \overline{P} - 2\infty$,
- $div(y - 144) = 5P - 5\infty$,

- $div(y+144) = 5\overline{P} - 5\infty$,
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$.

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 (a), 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 $(X=0).\mathcal{C} = P + \overline{P} + 3\infty$. (i)

De même pour $Z=0$, alors on a $X^5=0$ d'après (a) ; 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 4.1.1

* $5j(P) = 5j\left(\overline{P}\right) = 0$,
* $j(P) + j\left(\overline{P}\right) = 0$.

Lemme 4.1.2.

- $\mathcal{L}(\infty) = \langle 1\rangle$,
- $\mathcal{L}(2\infty) = \langle 1,\, x\rangle = \mathcal{L}(3\infty)$,
- $\mathcal{L}(4\infty) = \langle 1,\, x,\, x^2\rangle$,
- $\mathcal{L}(5\infty) = \langle 1,\, x,\, x^2,\, y\rangle$,
- $\mathcal{L}(6\infty) = \langle 1,\, x,\, x^2,\, y,\, x^3\rangle$,
- $\mathcal{L}(7\infty) = \langle 1,\, x,\, x^2,\, y,\, x^3,\, xy\rangle$,
- *De façon générale, pour $m \geq 3$, 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. 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 $m \geq 2g-1 = 3$.

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

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

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

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

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

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

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

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

Lemme 4.1.3.

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

Démonstration du théorème

4.1.1 Points quadratiques

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

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

On remarque que $R \notin \left\{\infty, P, \overline{P}\right\}$.
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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 - 2\infty,$$

donc $F \in \mathcal{L}\left(2\infty\right)$, 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 la relation $y^2 = \alpha^5 + 20736$, on a :

$$y^2 = \alpha^5 + 20736;$$

et par suite on a :

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

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

$$[R_1 + R_2 - 2\infty] = j(P) = -j(\overline{P}).$$

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

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

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

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

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 $\overline{P}$ donc on doit avoir $a_1 = a_2 = 0$, donc $F(x, y) = a_3 x^2$ et on devrait avoir $R_1 = R_2 = P$, 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + 2P - 4\infty,$$

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 P donc $a_1 = a_2 = 0$, donc $F(x, y) = a_3 x^2$ 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 définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + P - 3\infty,$$

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

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

4.1.2 Points cubiques

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

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

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

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 $t = aj(P) = -aj(\overline{P}),\ 0 \leq a \leq 4$. On remarque que $R \notin \left\{\infty, P, \overline{P}\right\}$.
Cas $a = 0$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 0$. Il existe alors une fonction rationnelle F définie 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 $[R_1 + R_2 + R_3 - 3\infty] = j(P) = -j(\overline{P})$. Il existe alors une fonction rationnelle F définie sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + \overline{P} - 4\infty$, 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 ∞.
Au point $\overline{P}$ on a $F(\bar{P}) = 0$ 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 degrés ≤ 2.
Cas $a = 2$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 2j(P) = -2j(\overline{P})$. Il existe alors une fonction rationnelle F définie sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 2\overline{P} - 5\infty$, donc $F \in \mathcal{L}(5\infty)$ et par suite $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$ avec $a_4 \neq 0$ sinon un des R_i devrait être égal à ∞.

La fonction F est d'ordre 2 au point $\overline{P}$ 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 $y = -144 - \dfrac{a_3}{a_4}x^2$. 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

$$\begin{aligned} y^2 = x^5 + 20736 &\Leftrightarrow \left(-144 - \alpha x^2\right)^2 = x^5 + 20736 \\ &\Leftrightarrow x^5 - \alpha^2 x^4 - 288\alpha x^2 = 0 \\ &\Leftrightarrow x^2(x^3 - \alpha^2 x^2 - 288\alpha) = 0. \end{aligned}$$

On doit avoir $x^2 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques donnée par

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

Cas $a = 3$
Donc on a $[R_1 + R_2 + R_3 - 3\infty] = 3j(P) = -3j(\overline{P})$. Il existe alors une fonction rationnelle F définie sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 3\overline{P} - 6\infty$, 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 $\overline{P}$ 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 $y = -144 - \dfrac{a_5}{a_4}x^3$. 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 $\overline{P}$, et par suite on a

$$\begin{aligned} y^2 = x^5 + 20736 &\Leftrightarrow \left(-144 - \alpha x^3\right)^2 = x^5 + 20736 \\ &\Leftrightarrow \alpha^2 x^6 - x^5 + 288\alpha x^3 = 0 \\ &\Leftrightarrow x^3(\alpha^2 x^3 - x^2 + 288\alpha) = 0. \end{aligned}$$

On doit avoir $x^3 \neq 0$ et $\alpha \in \mathbb{Q}^*$, on obtient une famille de points cubiques donnée par

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

Cas $a = 4$
Donc on a

$$[R_1 + R_2 + R_3 - 3\infty] = 4j(P) = -4j(\overline{P}).$$

Il existe alors une fonction rationnelle F définie sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 + 4\overline{P} - 7\infty$, 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 $\overline{P}$, ce qui est absurde.
Conclusion : L'ensemble des points cubiques sur $\mathcal{C}$ est donné par $\mathcal{A} \cup \mathcal{B}$.

CQFD □

4.2 Points algébriques de petits degrés sur les courbes affines $\mathcal{C}_n : y^{2n} = x^5 + 1$

Dans cette section, nous nous proposons d'étudier en détail les points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur les courbes $\mathcal{C}_n$ d'équations affines $y^{2n} = x^5 + 1$, sans se préoccuper de la finitude du groupe de Mordell-Weil.

Dans [12] Schaefer a donné une description des points de degrés 1 et des points de degrés 2 sur $\mathbb{Q}$ sur la courbe affine $y^2 = x^5 + 1$.

Notons $P_0 = (-1, 0)$, $P_1 = (0, 1)$, $\overline{P}_1 = (0, -1)$, ∞ le point à l'infini et $\mathcal{C}^{(d)}(\mathbb{Q})$ l'ensemble des points algébriques sur $\mathcal{C}$ de degrés d sur $\mathbb{Q}$.

Posons

$$\begin{aligned} &Q_1 = (1 + i, 1 - 2i)\ ,\ Q_2 = (1 - i, 1 + 2i)\ , \\ &\overline{Q}_1 = (1 + i, -1 + 2i)\ ,\ \overline{Q}_2 = (1 - i, -1 - 2i)\ , \\ &R_0 = P_0 + P_1\ . \end{aligned}$$

La proposition donnée dans [12] s'énonce comme suit :

Proposition (**Schaefer**)**.**

(**i**) *Les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par* :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

(**ii**) *Les points sur $\mathcal{C}$ de degrés 2 sur $\mathbb{Q}$ sont donnés par* :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \{Q_1\ ,\ Q_2\ ,\ \overline{Q}_1\ ,\ \overline{Q}_2\} \cup \left\{ \left(a, \pm\sqrt{a^5 + 1}\ \right)\ \mid a \in \mathbb{Q}^* \setminus \{-1\} \right\}.$$

Preuve. Voir [12].

□

Nous déduisons de ces résultats les points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur les courbes $\mathcal{C}_n$ d'équations affines $y^{2n} = x^5 + 1$.
Nos outils essentiels sont :

$*$ Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}$ (voir [12]) ,

$*$ Le Théorème de Chevalley-Weil.

Notre principal résultat s'énonce comme suit :

Théorème. *Soit n un entier naturel strictement supérieur à 1.*

(**1**) *L'ensemble des points $\mathbb{Q}$-rationnels sur $\mathcal{C}_n$ est donné par :*

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

(**2**) *L'ensemble des points algébriques de degrés 2 sur $\mathcal{C}_n$ est donné par :*

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(2)}(\mathbb{Q}) = \left\{ \begin{array}{l} (0,y) \mid y \text{ racine de l'équation} \\ \\ (y^2+1)(y^2+y+1)(y^2-y+1)=0 \end{array} \right\}.$$

Résultats auxiliaires

On a le lemme classique suivant :

Lemme 4.2.1 (***cf*** **[2]).** *Soient $K(x)$ et $K(y)$ deux extensions algébriques du corps K , telles que $[K(x):K]=m>0$ et $[K(y):K]=n>0$.*
Alors l'extension $K\subset K(x,y)$ est de degré fini sur K. En particulier, ce degré est un multiple de m et de n tel que

$$1\leq [K(x,y):K]\leq mn.$$

De plus, si m et n sont premiers entre eux (c'est-à-dire $m\wedge n=1$) , alors

$$[K(x,y):K]=mn.$$

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

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

$l(D)$ désigne la $\overline{\mathbb{Q}}$-dimension de $\mathcal{L}(D)$.

La classe $[P-\infty]$ de $P-\infty$ est notée $j(P)$; j étant le plongement jacobien $\mathcal{C}\to J(\mathbb{Q})$.

Lemme 4.2.2.

$$J(\mathbb{Q})\cong(\mathbb{Z}\ /\ 10\mathbb{Z})\cong\langle\ j(R_0)\ \rangle\,.$$

Preuve. Voir [12].

□

Polynômes cyclotomiques

Définition 4.2.1. *Soient n un entier strictement positif et ξ_n le nombre complexe $e^{\frac{2i\pi}{n}}$.*
Le $n^{ième}$ polynôme cyclotomique par définition est

$$\Phi_n(x) = \prod_{0\leq k<n\ ,\ k\wedge n=1} \left(x - \xi_n^k\right)$$

Clairement le degré de Φ_n est $\varphi(n)$, où φ est la fonction d'Euler.

Lemme 4.2.3. *Pour tout n entier naturel strictement positif, le polynôme $P_n(x) = x^n - 1$ est factorisable sous la forme :*

$$P_n(x) = x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Le polynôme $\Phi_d(x)$ est à coefficients entiers. $\Phi_d(x)$ est irréductible sur le corps $\mathbb{Q}$ des nombres rationnels.

Preuve. Voir [8].

□

Les seuls polynômes cyclotomiques de degré au plus 2 sont les suivants :
$\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$, $\Phi_4(x) = x^2+1$ et $\Phi_6(x) = x^2-x+1$.

Lemme 4.2.4. *Soient n un entier positif et ξ_n le nombre complexe $e^{\frac{2i\pi}{n}}$:*

$$[\mathbb{Q}(e^{\frac{2i\pi}{n}}) : \mathbb{Q}] = \varphi(n) \qquad , \qquad [\mathbb{Q}(e^{\frac{2i\pi}{n}})^m : \mathbb{Q}] = \varphi\left(\frac{n}{pgcd(n,m)}\right).$$

Preuve. Voir ([6], p. 9) et, combinée avec $Q(\xi_n^m) = Q(\xi_n^{pgcd(n,m)})$, on prouve la seconde assertion.

□

Théorème de Chevalley-Weil

On a le théorème de Chevalley-Weil suivant :

Théorème. *Soit $\phi : X \longrightarrow Y$ un revêtement non ramifié de variétés projectives normales définies sur un corps de nombres K. Alors il existe une extension finie L/K de K telle que*

$$\phi^{-1}(Y(K)) \subset X(L).$$

Preuve. Voir [6].

□

Démonstration du théorème

Considérons le morphisme

$$\begin{array}{rccc} f: & \mathcal{C}_n & \longrightarrow & \mathcal{C} \\ & (x,y) & \longmapsto & (x,y^n) \end{array}$$

où n est un entier ≥ 1.

Ainsi on a $\mathcal{C}_n^{(d)}(\mathbb{Q}) \subset f^{-1}\left(\bigcup_{1\leq k\leq d} \mathcal{C}^{(k)}(\mathbb{Q})\right)$ et $J_{\mathcal{C}_n}(\mathbb{Q}) \twoheadrightarrow J(\mathbb{Q})$ (voir [10])

avec $J_{\mathcal{C}_n}$ la jacobienne de $\mathcal{C}_n$.

Nous savons que $J(\mathbb{Q})$ est fini et la courbe $\mathcal{C}: y^2 = x^5 + 1$ a été étudiée dans [9]. Le Théorème de Chevalley-Weil nous permettra de déterminer certains points algébriques sur $\mathcal{C}_n$ à partir de ceux sur $\mathcal{C}$.

4.2.1 Points $\mathbb{Q}$-rationnels sur $\mathcal{C}_n$

Nous savons dans [12] que les points $\mathbb{Q}$-rationnels sur $\mathcal{C}$ sont donnés par :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

On a alors

$$\mathcal{C}_n^{(1)}(\mathbb{Q}) \subset f^{-1}\left(\{P_0,\ P_1,\ \overline{P}_1,\ \infty\}\right) = f^{-1}\left(\{P_0\}\right) \cup f^{-1}\left(\{P_1\}\right) \cup f^{-1}\left(\left\{\overline{P_1}\right\}\right) \cup f^{-1}\left(\{\infty\}\right).$$

On remarque que si $n = 1$, le problème est résolu car $\mathcal{C}_1 = \mathcal{C}$.

Supposons $n \geq 2$ et déterminons les points rationnels sur les courbes $\mathcal{C}_n$:

a) Le point $(x,y) \in f^{-1}\left(\{P_0\}\right) \Leftrightarrow f(x,y) = (0,0) \Leftrightarrow (x,y^n) = (0,0) \Leftrightarrow (x,y) = (0,0)$. Donc $f^{-1}\left(\{P_0\}\right) = \{P_0\}$.

b) Le point $(x,y) \in f^{-1}\left(\{P_1\}\right) \Leftrightarrow f(x,y) = (0,1) \Leftrightarrow (x,y^n) = (0,1) \Leftrightarrow x = 0$ et $y^n - 1 = 0$. D'après le Lemme 4.2.3, $y^n - 1$ est divisible par les polynômes cyclotomiques de degré 1 qui sont :
- $\Phi_1(y) = y - 1$ et $\Phi_2(y) = y + 1$ si n est pair,
- $\Phi_1(y) = y - 1$ si n est impair.
Donc $f^{-1}\left(\{P_1\}\right) = \left\{P_1,\ \overline{P_1}\right\}$.

c) Le point $(x,y) \in f^{-1}\left(\left\{\overline{P_1}\right\}\right) \Leftrightarrow f(x,y) = (0,-1) \Leftrightarrow (x,y^n) = (0,-1) \Leftrightarrow x = 0$ et $y^n + 1 = 0$. D'après le Lemme 4.2.3, $y^n + 1$ est divisible par le polynôme cyclotomique de degré 1 qui est $\Phi_2(y) = y + 1$ si n est impair.
Donc $f^{-1}\left(\left\{\overline{P_1}\right\}\right) = \left\{\overline{P_1}\right\}$.

d) Le point $(x,y) \in f^{-1}\left(\{\infty\}\right) \Leftrightarrow f(x,y) = (0,1) = \infty$ et on retrouve le cas b).

e) Le point à l'infini de $\mathcal{C}_n$ noté encore ∞ est soit $(1,0)$ si $n \geq 3$ ou $(0,1)$ si $n \leq 2$ qui est un point rationnel.

On obtient alors

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

4.2.2 Points quadratiques sur $\mathcal{C}_n$

Nous savons dans [12] que les points quadratiques sur $\mathcal{C}$ sont donnés par :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \left\{Q_1\ ,\ Q_2\ ,\ \overline{Q}_1\ ,\ \overline{Q}_2\right\} \cup \left\{\left(a, \pm\sqrt{a^5+1}\ \right)\ \mid\ a \in \mathbb{Q}^* \setminus \{-1\}\right\}.$$

On a alors

$$\mathcal{C}_n^{(2)}(\mathbb{Q}) \subset f^{-1}\left(\mathcal{C}^{(1)}(\mathbb{Q}) \cup \mathcal{C}^{(2)}(\mathbb{Q})\right).$$

On remarque que si $n = 1$, le problème est résolu car $\mathcal{C}_1 = \mathcal{C}$.

Supposons $n \geq 2$.

Cas 1 : Déterminons les points quadratiques contenus dans $f^{-1}\left(\mathcal{C}^{(2)}(\mathbb{Q})\right)$.

Le point $(x,y) \in f^{-1}(\{Q_1\}) \Leftrightarrow f(x,y) = Q_1 = (1+i, 1-2i) \Leftrightarrow x = 1+i$ et $y^n = 1-2i$. L'équation $y^n = 1-2i$ admet exactement n racines n-ièmes

$$y_k = \sqrt[n]{1-2i}\,\xi_n^k \ \text{ avec } \ 0 \leq k \leq n-1.$$

Posons $R_k = \left(1+i,\ \sqrt[n]{1-2i}\,\xi_n^k\ \right)$ et étudions le degré du point R_k. On a :

$$[\mathbb{Q}(R_k) : \mathbb{Q}] = \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\,\xi_n^k\ \right) : \mathbb{Q}\right] \text{ et } 1+i \notin \mathbb{Q}.$$

$$n \geq 2 \Longrightarrow \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\,\xi_n^k\ \right) : \mathbb{Q}\right] > \left[\mathbb{Q}\left(\sqrt{1-2i}\ \right) : \mathbb{Q}\right] = 4$$

$$\Longrightarrow \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\,\xi_n^k\ \right) : \mathbb{Q}\right] > 4.$$

Le point $R_k = \left(1+i,\ \sqrt[n]{1-2i}\,\xi_n^k\ \right)$ est donc de degré > 2, et on montre de la même manière que les images réciproques des points $\overline{Q_1}$, Q_2 et $\overline{Q_2}$ sont aussi de degrés > 2.

Le point

$$(x,y) \in f^{-1}\left(\left\{\left(a, \pm\sqrt{a^5+1}\ \right)\right\}\right) \Leftrightarrow f(x,y) = \left(a, \pm\sqrt{a^5+1}\right)$$

$$\Leftrightarrow x = a \text{ et } y^n = \pm\sqrt{a^5+1}.$$

L'équation $y^n = \pm\sqrt{a^5+1}$ admet exactement n racines n-ièmes

$$y_k = \sqrt[n]{\pm\sqrt{a^5+1}}\,\xi_n^k \text{ avec } 0 \leq k \leq n-1.$$

Étudions le degré de $R_{a,k} = \left(a, \sqrt[n]{\pm\sqrt{a^5+1}}\xi_n^k\right)$.

On a :

$$[\mathbb{Q}(R_{a,k}) : \mathbb{Q}] \geq [\mathbb{Q}(R_{a,0}) : \mathbb{Q}] = \left[\mathbb{Q}\left(a, \sqrt[n]{\pm\sqrt{a^5+1}}\right) : \mathbb{Q}\right].$$

De plus, $\mathbb{Q}(R_{a,0})$ contient $\mathbb{Q}(a)$ et $\mathbb{Q}\left(\sqrt[n]{\pm\sqrt{a^5+1}}\right)$ qui sont des corps de degrés 1 et $2n$ respectivement, avec $n \geq 2$.

Puisque $n \geq 2$, on a $1 \wedge 2n = 1$ et d'après le Lemme 4.2.1 on a :

$$\left[\mathbb{Q}\left(a, \sqrt[n]{\pm\sqrt{a^5+1}}\right) : \mathbb{Q}\right] = [\mathbb{Q}(a) : \mathbb{Q}] \times \left[\mathbb{Q}\left(\sqrt[n]{\pm\sqrt{a^5+1}}\right) : \mathbb{Q}\right] = 2n.$$

Le point $R_{a,0} = \left(a, \sqrt[n]{\pm\sqrt{a^5+1}}\right)$ est alors de degré $2n > 2$ car $n \geq 2$.

Donc l'ensemble des points quadratiques de $\mathcal{C}_n$ pour $n \geq 2$ sur le corps $\mathbb{Q}$ dans $f^{-1}\left(\mathcal{C}^{(2)}(\mathbb{Q})\right)$ est vide.

Cas 2 : Déterminons les points quadratiques sur les courbes $\mathcal{C}_n$ contenus dans $f^{-1}\left(\mathcal{C}^{(1)}(\mathbb{Q})\right)$.

a) Le point $(x,y) \in f^{-1}(\{P_0\}) \Leftrightarrow f(x,y) = (0,0) \Leftrightarrow (x,y^n) = (0,0) \Leftrightarrow x = 0$ et $y = 0$. On constate que P_0 est rationnel donc n'est pas de degré 2.

b) Le point $(x,y) \in f^{-1}(\{P_1\}) \Leftrightarrow f(x,y) = (0,1) \Leftrightarrow (x,y^n) = (0,1) \Leftrightarrow x = 0$ et $y^n - 1 = 0$. D'après le Lemme 4.2.3, $y^n - 1$ est divisible par les polynômes cyclotomiques de degré 2 qui sont :

- $\Phi_3(y) = y^2 + y + 1$ si n est un multiple de 3 ;
- $\Phi_4(y) = y^2 + 1$ si n est un multiple de 4 ;
- $\Phi_6(y) = y^2 - y + 1$ si n est un multiple de 6.

Donc $f^{-1}(\{P_1\}) = \{(0,y) \mid y \text{ racine de l'équation } (y^2+1)(y^2+y+1)(y^2-y+1) = 0\}$.

c) Le point $(x,y) \in f^{-1}\left(\{\overline{P_1}\}\right) \Leftrightarrow f(x,y) = (0,-1) \Leftrightarrow (x,y^n) = (0,-1) \Leftrightarrow x = 0$ et $y^n + 1 = 0$. D'après le Lemme 4.2.3, $y^n + 1$ est divisible par le polynôme cyclotomique de degré 2 qui est $\Phi_4(y) = y^2 + 1$ si n est pair.

Donc $f^{-1}\left(\{\overline{P_1}\}\right) = \{(0,y) \mid y \text{ racine de l'équation } y^2 + 1 = 0\}$.

d) Le point $(x,y) \in f^{-1}(\{\infty\}) \Longleftrightarrow f(x,y) = (-1,0) = \infty$.

On constate que ∞ est rationnel donc n'est pas de degré 2.

En conclusion l'ensemble des points algébriques de degrés 2 des courbes $\mathcal{C}_n$ sur $\mathbb{Q}$ est donné par :

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(2)}(\mathbb{Q}) = \left\{ \begin{array}{l} (0,y) \mid y \text{ racine de l'équation} \\ \\ (y^2+1)(y^2+y+1)(y^2-y+1) = 0 \end{array} \right\}.$$

CQFD □

Conclusion et Perspectives

Cette thèse a consisté en l'étude de quelques cas particuliers de courbes algébriques, où l'on peut déterminer explicitement les points algébriques de degrés fixés et même parfois de degrés quelconques.
Les méthodes utilisées pour démontrer les théorèmes fondamentaux obtenus dans cette thèse s'appuient sur deux approches :

- la première suppose que l'on connaisse ou détermine la structure du groupe de Mordell-Weil des points rationnels de la jacobienne et que celui-ci soit fini, et consiste en une détermination explicite de bases de certains systèmes linéaires sur la courbe étudiée à l'aide du théorème de Riemann-Roch, puis en l'utilisation de la géométrie de cette courbe, en particulier l'ordre de contact des tangentes en les points rationnels de la courbe,
- la deuxième consiste à contourner la contrainte de la finitude du groupe de Mordell-Weil en utilisant le théorème de Chevalley-Weil.

Les principaux résultats de recherches contenus dans cette thèse, concernent essentiellement :

1. Les courbes d'équations affines suivantes :

   a) $y^2 = x^5 + 20736$ pour laquelle on a déterminé l'ensemble des points algébriques de degrés au plus 3 sur $\mathbb{Q}$.

   b) $y^2 = x(x^2+1)(x^2+3)$ pour laquelle on a déterminé l'ensemble des points algébriques de degrés au plus 4 sur $\mathbb{Q}$.

   c) $y^2 = x^5 - 243$ et $y^2 = 3x(x^4+3)$ pour lesquelles on a déterminé l'ensemble des points algébriques de degré au plus 5 sur $\mathbb{Q}$.

   d) $y^2 = 3(x^5-1)$ et $y^2 = x(x^2+1)(x^2+3)$ pour lesquelles on a déterminé l'ensemble des points algébriques de degrés quelconques sur $\mathbb{Q}$. Ce dernier résultat généralise celui obtenu en *b*).

   Les résultats obtenus dans cette partie complètent et étendent les travaux de Bruin, Mulholland, Siksek et Siksek & Stoll qui ont décrit, dans [1], [7], [13], [14] et [15] l'ensemble des points algébriques de degrés 1 sur $\mathbb{Q}$ sur ces courbes.

2. La famille de courbes d'équations affines $\mathcal{C}_n : y^{2n} = x^5 + 1$.
   Cette famille de courbes a intéressé un grand nombre de géomètres algébristes dont Schaefer [12] qui a déterminé l'ensemble des points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}_1 : y^2 = x^5 + 1$ qui correspond au cas particulier $n = 1$. Les résultats obtenus par Schaefer ont été étendus aux points algébriques de degrés au plus 3 par Fall et Sall [3], puis généralisés aux points algébriques de degrés quelconques par Sall, Fall et Coly [9].
   Notre contribution a consisté à déterminer l'ensemble des points algébriques de degrés au plus 2 sur $\mathbb{Q}$ sur les courbes d'équations affines $\mathcal{C}_n : y^{2n} = x^5 + 1$ pour $n > 1$.
   Parmi les perspectives de recherches ouvertes par les résultats obtenus dans cette thèse, on peut citer :
   - la détermination de l'ensemble les points algébriques en utilisant des approches permettant de contourner la contrainte de finitude du groupe de Mordell-Weil. Le théorème de Chevalley-Weil répond à cette préoccupation, mais il nous semble qu'on peut utiliser d'autres approches géométriques ou arithmétiques plus efficaces ;
   - la détermination de l'ensemble des points algébriques de degrés exactement d ($d \geq 4$).
   - la détermination de l'ensemble des points algébriques de degrés sur un corps de nombres K.

Bibliographie

[1] Bruin, N., On powers as sums of two cubes, International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, **(2000)**.

[2] Calais, J., Field extensions, Galois theory, Level M1 - M2 (Extensions de corps, Théorie de Galois, Niveau M1 - M2)(French), Mathématiques à l'Université, Paris : Ellipses (ISBN 2 - 7298 - 2780 - 3 / pbk), xii, 218 p. **(2006)**.

[3] Fall, M., Sall, O., Points algébriques de petits degrés sur la courbe d'équation affine $y^2 = x^5 + 1$, Afrika Matematika **(2018)** 29 : 1151 - 1157.

[4] Faltings, G., Finiteness theorems for abelian varieties over number fields (Endlichkeitssätze für abelscheVarietäten über Zahlkörpern.)(German), Invent. Math. 73 **(1983)** no.3, 349 – 366.

[5] Griffiths, P. A., Introduction to Algebraic Curves, In : Translations of Mathematical monographs, vol. 76. American Mathematical Society, Providence, RI **(1989)**.

[6] Hindry, M., Silverman, J., Diophantine geometry, an introduction, Springer-Verlag, New York, **(2000)**, Graduate Texts Mathematics, 201.

[7] Mulholland, J. TH., Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC. Ann Arbor, MI **(2006)**.

[8] Perrin Daniel **(1996)**. Cours d'algèbre. Ellipses, p. 79.

[9] Sall, O., Fall, M., Coly, C. M., 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)**.

[10] Sall, O., Fall, M., Top, T., Points algébriques de petits degrés sur les courbes $\mathcal{C}_n$ d'équation affine $y^{3n} = x(x-1)(x-2)(x-3)$, Annales Mathématiques Africaines, Volume 5 **(2015)** pp. 25 - 28.

[11] Sarr, P. M., Sow, EL. H., Fall, M., Sall, O., Points algébriques de degrés quelconques sur la courbe d'équation affine $y^2 = x(x^2+1)(x^2+3)$, Nonlinear Analysis, Geometry and Appications, Proceedings of the second NLAGA-BIRS Symposium, Cap Skirring, Senegal, January 25-30, **(2022)**.

[12] Schaefer, E. F., Computing a Selmer group of Jacobian using functions on the curve, Math. Ann. 310 **(1998)** 447 - 471.

[13] Siksek, S., 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)**.

[14] Siksek, S., Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, **(2013)**, No. 4, page 765.

[15] Siksek, S., Stoll, M., Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$, Bull. London. Math. Soc. 44 **(2012)**, 151 - 166.

[16] Sow, EL. H., Sarr, P. M., Sall, O., Points algébriques de degrés au plus 5 sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 3x(x^4 + 3)$, International Journal of Development Research Vol. 11, Issue 12, pp. 52435 - 52439, December, **(2021)**.

[17] Sow, EL. H., Sarr, P. M., Sall, O., Algebraic points of degree at most 5 on the affine curve $y^2 = x^5 - 243$, Asian Research Journal of Mathematics, Volume 17, Issue 10, **(2021)**.

[18] Sow, EL. H., Sarr, P. M., Sall, O., Parametrization of algebraic points of low degrees on the affine curve $y^2 = x^5 + 144^2$, EPH - International Journal of Mathematics and Statistics, Volume-7, Issue-12, Jan, **(2021)**.

[19] Sow, EL. H., Sarr, P. M., Fall, M., Sall, O., Points algébriques de degré quelconque sur la courbe d'équation affine $\mathcal{C} : y^2 = 3(x^5 - 1)$, International Journal of Mathematics and Statistics Invention (IJMSI), E-ISSN : 2321 - 4767, P-ISSN : 2321 - 4759, Vol. 10, Issue 1, January, **(2022)**, PP 01 - 04.