UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

École Doctorale : Sciences, Technologies et Ingénierie

UFR SCIENCES ET TECHNOLOGIES

DÉPARTEMENT DE MATHÉMATIQUES

THÈSE

Numéro d'ordre : 02

Domaine :	**Sciences et Technologies**
Mention :	**Mathématiques et Applications**
Spécialité :	**Mathématiques Pures**
Option :	**Géométrie Algébrique**

Présentée par :

Boubacar Sidy BALDE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE ASSANE SECK DE ZIGUINCHOR

Sujet de la thèse :

Points algébriques sur certaines courbes

Soutenue publiquement le 17 Décembre 2022 devant le jury composé de :

Qualité	Prénoms et Nom	Université(Sénégal)
Président	M.Marie Salomon SAMBOU	Assane Seck de Ziguinchor
Rapporteurs	M.Marie Salomon SAMBOU	Assane Seck de Ziguinchor
	M.Mouhamed Ben Faraj MAAOUIA	Gaston Berger de Saint-Louis
	M.Amadou Lamine FALL	Cheikh Anta Diop de Dakar
Examinateur	M.Moussa FALL	Assane Seck de Ziguinchor
Directeur	M.Oumar SALL	Assane Seck de Ziguinchor

Points algébriques sur certaines courbes

Résumé.

Cette thèse est consacrée d'une part sur la détermination explicite des points algébriques de petit degré sur certaines courbes et d'autre part sur la paramétrisation des points algébriques sur certaines courbes algébriques de degré donné. La méthode utilisée s'appuie d'abord sur la connaissance du groupe de Mordell-Weil de la variété jacobienne J de $\mathcal{C}$, ensuite la condition qu'il soit fini. En plus de cela d'utiliser le théorème d'Abel-Jacobi pour plonger la courbe dans sa jacobienne. Le but sera alors de déterminer explicitement tous les points algébriques de degré au plus 3 sur les courbes $\mathcal{C}$ et $\mathcal{C}_3(11)$, puis de donner une paramétrisation de tous les points algébriques de degré l quelconque donné sur les courbes $\mathcal{C}$ et $\mathcal{C}_3(11)$. Notre étude étend les travaux de Daniel M.Gordon et de David Grant qui ont déterminé le groupe de Mordell-Weil de la variété jacobienne J de $\mathcal{C}$ et l'ensemble des points rationnels sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.

Mots-clefs : Extension algébrique, Groupe de Mordell-Weil, Jacobien, Théorème d'Abel-Jacobi.

Algebraic points on some curves.

Abstract.

This thesis is devoted on the one hand to the explicit determination of algebraic points of small degree on certain curves and on the other hand to the parameterization of algebraic points on certain algebraic curves of given degree. The method used relies first on the knowledge of the Mordell-Weil group of the Jacobian variety J of $\mathcal{C}$, then the condition that it is finite. In addition to that use the Abel-Jacobi theorem to plunge the curve into its Jacobian. The goal will then be to determine explicitly all the algebraic points of degree at most 3 on the curves $\mathcal{C}$ and $\mathcal{C}_3(11)$, and then to give a parametrization of all the algebraic points of any degree l given on the curves $\mathcal{C}$ and $\mathcal{C}_3(11)$. Our study extends from the work of Daniel M. Gordon and David Grant who determined the Mordell-Weil group of the Jacobian variety J of $\mathcal{C}$ and the set of rational points on the curve $\mathcal{C}$ of affine equation $y^2 = x(x-3)(x-4)(x-6)(x-7)$.

Keywords : Algebraic extensions. Mordell-Weil Group. Jacobian. The Abel-Jacobi theorem.

Remerciements

Je ne saurais débuter sans remercier tous ceux qui m'ont permis la réalisation de ce travail.
je tiens d'abord à exprimer toute ma gratitude à mon directeur de thèse Oumar SALL pour toute la confiance qu'il a eue en moi, sa disponibilité constante, mais aussi, pour la patience dont il a fait part à mon égard.

Je suis très honoré que le Professeur Marie Salomon SAMBOU ait accepté d'être rapporteur de cette thèse et je le remercie du temps qu'il a consacré pour ce travail.

Je suis très honoré que le Professeur Mouhamed Ben Faraj MAAOUIA et le professeur Amadou Lamine FALL aient accepté de faire partie du jury. Je leur remercie des taches et des suggestions qu'ils ont consacré pour ce travail.

Je remercie l'ensemble des membres du jury, pour avoir accepté de participer à ma soutenance et pour l'intérêt porté à mes travaux de recherche. Je tiens à exprimer ma reconnaissance tout particulièrement au professeur Moussa FALL de l'université Assane Seck de Ziguinchor des conseils, des suggestions et des guides qu'il m'a toujours apporté.

Mes remerciements à tous mes amis et collègues qui m'ont apporté leur support moral et intellectuel.

Dédicaces

Ce travail est dédié à :

mes parents ;
toute ma famille ;
mes frères & sœurs ;
tous mes sympathisants.

Table des matières

Introduction

L'étude des équations diophantiennes d'un point de vue géométrique commence par l'étude des solutions d'équations $P(x,y) = 0$, où P est un polynôme à coefficients rationnels et où l'on cherche les solutions rationnelles $(x,y) \in \mathbb{Q}^2$. En remplaçant $\mathbb{Q}$ par un corps de nombres $\mathbb{K}$, le problème devient plus intéressant. Pour cela la géométrie algébrique est considérée comme l'étude des variétés algébriques, définies comme ensembles des zéros d'un ou plusieurs polynômes.

On se munit d'une courbe algébrique projective lisse $\mathcal{C}$ définie sur un corps de nombres $\mathbb{K}$ et de genre g. On note $\mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq d} \mathcal{C}(\mathbb{K})$ l'ensemble des points de $\mathcal{C}$ définis sur $\mathbb{K}$ de degré $\leq d$. Le degré d'un point algébrique R est le degré de son corps de définition sur $\mathbb{Q}$.

Un célèbre théorème de Faltings (1983) affirme que si $g \geq 2$ alors l'ensemble $\mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$ est fini. En d'autre terme, la courbe ne rencontre qu'en un nombre fini de points le groupe de Mordell-Weil des points rationnels de la jacobienne. En s'inspirant des idées de Vojta, Faltings a généralisé ce résultat aux sous-variétés abéliennes. En effet, Faltings a démontré que les points rationnels sont répartis sur un nombre fini de translatés de sous-variétés abéliennes contenues dans la variété étudiée. Ce deuxième énoncé peut même être utilisé pour démontrer des résultats qualitatifs sur les points de degré $\leq d$ sur une courbe. Tous ces énoncés sont qualitatifs, un théorème plus précis de Debarre et Klassen [De-Kl-94] montre que, pour une courbe plane lisse définie sur $\mathbb{Q}$ de degré d, on a :

1) Si $d \geq 7$ alors $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq d-2} \mathcal{C}(\mathbb{K})$ est fini.

2) Si $d \geq 8$ alors, à un nombre fini d'exceptions près, les points de $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq d-1} \mathcal{C}(\mathbb{K})$ se présentent comme intersection de $\mathcal{C}$ avec une droite définie sur $\mathbb{Q}$ passant par un point rationnel de $\mathcal{C}$.

Néanmoins notre travail va porter sur une détermination explicite des points algébriques de petit degré sur certaines courbes puis une paramétrisation des points algébriques de degré donné. L'approche s'appuie sur la connaissance préalable du groupe de Mordell-Weil de la variété jacobienne J de $\mathcal{C}$ et la condition qu'il soit fini : elle consiste à utiliser le théorème d'Abel-Jacobi pour plonger la courbe dans sa jacobienne et étudier des systèmes

linéaires sur la courbe $\mathcal{C}$; et tous nos résultats sont dans ce cadre. Notre étude porte sur les courbes suivantes :

- La courbe algébrique d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.
- La courbe algébrique d'équation affine $y^{11} = x^3(x-1)^3$.
- La courbe algébrique d'équation affine $y^2 = x^3 - 8x^2 + x$.

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

Le chapitre 1 intitulé "Les Préliminaires" regroupe quelques formules, définitions, propositions et théorèmes (des notions de base) utiles dans les chapitres suivants.

Le chapitre 2 intitulé "Points algébriques de petit degré sur certaines courbes" comporte deux parties :

La première partie est consacrée à la description explicite de l'ensemble des points algébriques de degré au plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$. L'énoncé obtenu étend le résultat donné par Daniel M. Gordon et de David Grant dans ([Go-Gr-93],p.808) par la proposition suivante :

Proposition

L'ensemble des points rationnels sur $\mathbb{Q}$ sur courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$ est donné par

$$\mathcal{C}(\mathbb{Q}) = \{P_1,P_2,P_3,P_4,P_5,\infty\}$$

avec $P_1 = (0,0)$, $P_2 = (3,0)$, $P_3 = (4,0)$, $P_4 = (6,0)$, $P_5 = (7,0)$ en affine et ∞ le point à infini de $\mathcal{C}$.

Note résultat principal est donné par le théorème suivant :

Théorème 1

1-L'ensemble des points quadratiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$ est donné par :

$$\mathcal{A}_1 = \left\{ \left(x, \pm \sqrt{-\frac{a_0}{a_1}(-\frac{a_0}{a_1}-3)(-\frac{a_0}{a_1}-4)(-\frac{a_0}{a_1}-6)(-\frac{a_0}{a_1}-7)} \right) \mid x \in \mathbb{Q}^* \right\}$$

2-L'ensemble des points cubiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$ est vide.

La deuxième partie donne une description de l'ensemble des points algébriques de degré au plus 3 sur $\mathbb{Q}$ sur la courbe $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$.

Notre étude résulte des travaux sur la famille de courbes $y^p = x^r(x-1)^r$ avec $1 \leq r$, $2r \leq p-1$. Une telle famille a intéressé certains géomètres algébristes dont Gross-Rohrlich

qui ont déterminé $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 2} \mathcal{C}_1(11)(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}_1(11)$ de degré au-plus 2 sur $\mathbb{Q}$.

Théorème 2

L'ensemble des points algébriques sur $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$ de degré au-plus 3 sur $\mathbb{Q}$ est donné par :

$\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 3} \mathcal{C}_3(11)(\mathbb{K}) = \{P_0, P_1, P_\infty\} \cup \mathcal{F}$ avec

$$\mathcal{F} = \left\{ \left(x, [\beta x(x-1)]^{\frac{1}{4}} \right) \mid \beta \in \mathbb{Q}^* \ \ et \ \ x \ \ racine \ \ de \ \ l'équation \ \ x(x-1) = \beta^{11} \right\}.$$

Le chapitre 3 intitulé "Points algébriques de degré quelconque sur certaines courbes" comporte aussi trois parties :

La première partie porte sur une étude qualitative de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathbb{Q}$ de degré au plus l donnés sur $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.

Dans cette partie, nous étendons les résultats du chapitre 2 en donnant une description des points de degré quelconque donné sur $\mathbb{Q}$. Cette extension est obtenue par le théorème suivant :

Théorème 3

Considérons la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.

Soit $w \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = l$. Notons $w_1,...,w_l$ les conjugués de Galois de w et $E\left(\frac{l+4}{2}\right)$ la partie entière de $\frac{l+4}{2}$.

Il existe alors une courbe $\mathcal{M}$ définie sur $\mathbb{Q}$ de degré $\alpha \leq E\left(\frac{l+4}{2}\right)$ telle que

$$\mathcal{M}.\mathcal{C} = w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i + (5\alpha - l - \sum_{i=1}^{4} m_i)\infty \text{ avec } m_i \in \{0,1\}.$$

En particulier

1) Les points algébriques sur $\mathcal{C}$ de degré 2 sur $\mathbb{Q}$ sont donnés :

$\mathcal{M}.\mathcal{C} = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (8 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une conique.

$\mathcal{C}_1.\mathcal{C} = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (3 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est droite.

2) Les points algébriques sur $\mathcal{C}$ de degré 3 sur $\mathbb{Q}$ sont donnés :

$\mathcal{M}.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (12 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une cubique.

$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (7 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est une conique.

$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (2 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_2$ est une droite.

3) Les points algébriques sur $\mathcal{C}$ de degré 4 sur $\mathbb{Q}$ sont donnés :

$\mathcal{M}.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (16 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une quartique.

$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (11 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est une cubique.

$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (6 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_2$ est une conique.

$\mathcal{C}_3.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (1 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_3$ est une droite.

La deuxième partie de chapitre 3 porte sur une étude de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathbb{Q}$ de degré au plus l sur $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$. Nous étendons aussi les résultats du chapitre 2 en donnant une description des points de degré quelconque donné sur $\mathbb{Q}$.

Théorème 4

L'ensemble des points algébriques de degré $l \geq 9$ sur $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$ est donné par :

$$\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}_3(11)(\mathbb{K}) = \mathcal{F}_0 \bigcup \left(\bigcup_{k=1}^{10} \mathcal{F}_k \right) \text{ avec}$$

$$\mathcal{F}_0 = \left\{ \left(-\frac{\sum_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}}}{\sum_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}}}, y \right) \middle| a_0 \neq 0, a_{\frac{l}{2}} \neq 0 \text{ **si l est pair**}, \ b_{\frac{l-11}{2}} \neq 0 \text{ **si l est impair** } \right.$$
$$\left. \text{**et y racine de l'équation**} \quad y^{11}\left(\sum_{j\leq \frac{l-11}{2}} b_j y^j \right)^2 = \left(\sum_{i\leq \frac{l}{2}} a_i y^i \right)\left(\sum_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}} + \sum_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}} \right)^3 \right\}$$

$$\mathcal{F}_k = \left\{ \left(-\frac{\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}}}{\sum_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}}}, y \right) \middle| b_0 \neq 0, a_{\frac{l+11-k}{2}} \neq 0 \text{ **si l est pair**}, \ b_{\frac{l-k}{2}} \neq 0 \text{ **si l est impair** } \right.$$
$$\left. \text{**et y racine de l'équation**} \quad y^k\left(\sum_{j\leq \frac{l-k}{2}} b_j y^j \right)^2 = \left(\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{i-(11-k)} \right)\left(\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}} + \sum_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}} \right)^3 \right\}$$

La troisième partie de chapitre 3 porte sur une étude aussi de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathbb{Q}$ de degré au plus l sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$.

Théorème 5

L'ensemble des points algébriques de degré au plus l sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par :

$$\bigcup_{[\mathbb{Q}(R):\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K}) = \mathcal{F}_1 \bigcup \mathcal{F}_2$$

$$\text{avec } \mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j} \right) \middle| (a_0 \wedge b_0) \neq 0, a_{\frac{l}{2}} \neq 0 \text{ **si l est pair**}, \ b_{\frac{l-3}{2}} \neq 0 \text{ **si l est impair** } \right.$$
$$\left. \text{**et x solution de l'équation :**} \quad \left(\sum_{i=0}^{\frac{l}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \right\}$$

$$\mathcal{F}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{l+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-2}{2}} b_j x^j} \right) \middle| b_0 \neq 0, a_{\frac{l+1}{2}} \neq 0 \text{ **si l est pair**}, \ b_{\frac{l-2}{2}} \neq 0 \text{ **si l est impair** } \right.$$
$$\left. \text{**et x solution de l'équation :**} \quad \left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j \right)^2 \left(x - (4 - \sqrt{15}) \right) \left(x - (4 - \sqrt{15}) \right) \right\}$$

Chapitre 1

Préliminaires

1.1 Variétés algébriques

1.1.1 Espaces affines

Définitions 1.1.1. Soit k un corps parfait et $\overline{k}$ la clôture algébrique de k. On appelle **espace affine de dimension n sur** k, l'ensemble des n-uplets d'éléments a_i de k noté $\mathbb{A}^n(k)$ ou simplement $\mathbb{A}^n$:

$$\mathbb{A}^n(k) = \{(a_1,...,a_n), a_i \in k\}$$

Un élément $a = (a_1,...,a_n) \in \mathbb{A}^n(k)$ est appelé un point de l'espace affine $\mathbb{A}^n(k)$, les a_i sont les coordonnées de ce point. Les espaces $\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite et plan affine.
Si S une partie quelconque de l'anneau des polynômes $k[X_1,...,X_n]$, On pose alors

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

qui est l'ensemble des zéros communs à tous les polynômes de S.
On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S.

Proposition 1.1.1. La réunion de deux ensembles algébriques affines est un ensembles algébrique affine. L'intersection d'une famille d'ensembles algébriques affines est un ensembles algébrique affine.

1.1.2 Espaces projectifs

Définitions 1.1.2. Considérons la relation $\Re$ définie sur $k^{n+1} - \{0\}$ par : pour tous vecteurs non nuls x et y, on a $x\Re y$ si et seulement s'ils sont colinéaires, i.e,

$$x\Re y \Leftrightarrow \exists \lambda \in k^* : y = \lambda x$$

On appelle **espace projectif de dimension** n **sur** k, et l'on note $\mathbb{P}^n$ (ou $\mathbb{P}^n(k)$), l'ensemble des classes d'équivalence définies par la relation d'équivalence $\Re$. La classe de x notée $\overline{x}$ est donc l'ensemble des éléments de $k^{n+1} - \{0\}$ colinéaires à x :

$$\overline{x} = \{y \in k^{n+1} - \{0\} \mid y = \lambda x, \lambda \in k^*\}$$

Autrement dit, $\mathbb{P}^n = k^{n+1} - \{0\}/\Re$ est donc l'ensemble des droites vectorielles de $k^{n+1} - \{0\}$. Les éléments (droites vectorielles) de $\mathbb{P}^n$ sont appelés points. Si $x = (x_0,...,x_n) \in k^{n+1} - \{0\}$, on note $\overline{x} = (x_0 : ... : x_n)$ qui est un point de $\mathbb{P}^n(k)$. Pour $F \in k[X_0,...,X_n]$ et $P = (x_0 : ... : x_n) \in \mathbb{P}^n$, $F(P) = F(x_0,...,x_n)$.
On dit que $\mathbb{P}^1$ est la droite projective sur k, et que $\mathbb{P}^2$ est le plan projectif sur k.
En particulier, $\mathbb{P}^1$ s'interprète comme l'ensemble des directions de $\mathbb{A}^2$ et le plan projectif peut être vu comme le plan affine auquel on a ajouté l'ensemble des directions donc $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$.
Un élément F de $k[X_0,...,X_n]$ est dit homogène de degré d si, pour tout $\lambda \in k$, on a :

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

Si S **une partie de** $k[X_0,...,X_n]$ **formée de polynômes homogènes, On pose alors :**

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

qui est l'ensemble des zéros communs à tous les polynômes de S**.**
On dit que $\mathcal{V}_p(S)$ **est l'ensemble algébrique projectif défini par** S.

On vérifie qu'un point $P = (x_0 : ... : x_n)$ est un zéro d'un polynôme homogène F si et seulement si $F(\lambda x_0,...,\lambda x_n) = 0$ pour tout $\lambda \in k$.
Une conséquence de la définition précédente est que, si F est homogène, on a : pour tout $\lambda \neq 0$, $F(x_0,...,x_n) = 0$ si seulement si $F(\lambda x_0,...,\lambda x_n) = 0$.

Proposition 1.1.2.

1. Une intersection quelconque d'ensembles algébriques projectifs est un ensemble algébrique projectif :
$$\bigcap_i \mathcal{V}_p(S_i) = \mathcal{V}_p(\bigcup_i S_i)$$
2. Une réunion finie d'ensembles algébriques projectifs est un ensemble algébrique projectif.

Définition 1.1.1. La topologie de Zariski sur un espace (affine ou projectif) est la topologie pour laquelle les ensembles algébriques sont des fermés.

Définition 1.1.2. Un ensemble algébrique est dit irréductible s'il est irréductible pour la topologie de Zariski.

Définition 1.1.3. On appelle variété algébrique affine, tout ensemble algébrique affine irréductible.

Définition 1.1.4. On appelle variété algébrique projective, tout ensemble algébrique projectif irréductible.

Définition 1.1.5. Soient X et Y des variétés algébriques irréductibles.
$\varphi : X \to Y$ une application rationnelle. On dit que φ est dominante si l'image de φ est partout dense dans Y.
Une application rationnelle dominante $\varphi : X \to Y$ est birationnelle s'il existe $\psi : Y \to X$ rationnelle dominante avec $\psi \circ \varphi = id_X$.

Définition 1.1.6. Deux variétés algébriques irréductibles X et Y sont dites birationnellement équivalentes s'il existe $\varphi : X \to Y$ birationnelle.

Définition 1.1.7. Soit X un ensemble. Une chaîne de parties de X est une suite $X_0 \subset ... \subset X_n$ avec les $X_i \subset X$ distincts. Une telle chaîne est dite de longueur n.

Définition 1.1.8. Soit X un espace topologique. La dimension de X est la borne supérieure des longueurs des chaînes de parties irréductibles de X que l'on note $dimX$. C'est un entier positif, ou $+\infty$, ou $-\infty$ si X est vide.
Notons que si X est la réunion de fermés X_1,...,X_n, on a $dimX = maxdimX_i$. Nous constatons que la dimension d'un ensemble algébrique est le maximum des dimensions de ses composantes irréductibles.

Exemple 1. $dim\mathbb{P}^n = n$.

1.2 Courbes algébriques

1.2.1 Courbe affine plane

Définitions 1.2.1. On appelle hypersurface définie par f, et on note $\mathcal{V}(f)$, l'ensemble des zéros de f (pour f non constant et k algébriquement clos)

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

Définition 1.2.1. Une courbe affine plane est une hypersurface du plan affine $\mathbb{A}^2$:

$$\mathcal{V}(f) = \{(x,y) \in \mathbb{A}^2 \mid f(x,y) = 0\}$$

Le degré de $\mathcal{V}(f)$ est le degré de f. Une courbe $\mathcal{V}(f)$ est appelée conique, cubique, quartique, . . . si d = 2, 3, 4, . . .

Définition 1.2.2. Un point $P = (a,b) \in \mathbb{A}^2$ d'une courbe affine plane $\mathcal{C}$ est dit singulier si :

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

Un point $P = (a;b) \in \mathbb{A}^2$ d'une courbe affine plane $\mathcal{C}$ 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 la courbe $\mathcal{C}$ est la droite d'équation :

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

1.2.2 Courbe projective plane

Définition 1.2.3. On appelle hypersurface définie par un polynôme F homogène en $n+1$ variables, et on note $\mathcal{V}_p(F)$, l'ensemble des zéros de F (pour F non constant et k algébriquement clos)

$$\mathcal{V}_p(F) = \{\overline{x} \in \mathbb{P}^n \mid F(\overline{x}) = 0\}$$

Le degré de $\mathcal{V}_p(F)$ est le degré de F.

Définition 1.2.4. Une courbe projective plane est une hypersurface du plan projection $\mathbb{P}^2$ de type

$$\mathcal{V}_p(F) = \{P = (x_0 : x_1 : x_2) \in \mathbb{P}^2 \mid F(P) = 0\}$$

Définition 1.2.5. Un point $P = (a : b : c) \in \mathbb{P}^2$ d'une courbe projective plane $\mathcal{C}$ est dit singulier si :

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

Un point $P = (a : b : c) \in \mathbb{P}^2$ d'une courbe projective plane $\mathcal{C}$ est dit lisse si

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

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

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

Une courbe projective plane est dite non-singulière ou lisse si elle n'a pas de point singulier.

1.3 Diviseurs et l'espace des vecteurs $\mathcal{L}(D)$

Définitions 1.3.1. Un diviseur D sur une courbe algébrique lisse $\mathcal{C}$ est une combinaison formelle finie à coefficients entiers de points de $\mathcal{C}$:

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

où les n_p sont des entiers presque tous nuls. L'ensemble des diviseurs sur $\mathcal{C}$ est un groupe commutatif noté $Div(\mathcal{C})$ où la loi de groupe est l'addition formelle de points.
Si $D = \sum_{P \in \mathcal{C}} n_p P$ et $D' = \sum_{P \in \mathcal{C}} n'_p P$, alors $(D + D') = \sum_{P \in \mathcal{C}} (n_p + n'_p) P$.
Le degré de D est la somme de ses coefficients :

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

Le degré est un homomorphisme de groupe de $Div(\mathcal{C})$ vers $\mathbb{Z}$. Le noyau de cet homomorphisme est l'ensemble des diviseurs de degré 0, noté $Div^0(\mathcal{C})$. C'est un sous-groupe de $Div(\mathcal{C})$.
Un diviseur D est dit effectif et on note $D \geq 0$, si $n_p \geq 0$ pour tout $P \in \mathcal{C}$.

Définitions 1.3.2. Soit $\mathcal{C}$ une courbe projective plane irréductible de sorte que l'anneau des polynômes $k[\mathcal{C}]$ est intègre.
Soient $f \in k(\mathcal{C})$ (le corps des fonctions rationnelles sur $\mathcal{C}$) et $P \in \mathcal{C}$. On dit que f est régulière (ou définie) au point P s'il existe g,$h \in k[\mathcal{C}]$ avec $g(P) \neq 0$ tel que $f = h/g$.
L'ensemble des fonctions régulières en P est noté $\mathcal{O}_P(\mathcal{C})$, et appelé l'anneau local de $\mathcal{C}$ en P :

$$\mathcal{O}_P(\mathcal{C}) = \{f \in k(\mathcal{C}) \mid \exists h,g \in k[\mathcal{C}] \text{ avec } g(P) \neq 0 : f = \frac{h}{g}\}$$

L'ensemble des fonctions régulières en P qui s'annulent en P est noté $\mathcal{M}_{\mathcal{P}}(\mathcal{C})$, et appelé l'idéal maximal de $\mathcal{C}$ en P :

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

Les éléments inversibles de $\mathcal{O}_P(\mathcal{C})$ sont ceux qui n'appartiennent pas à $\mathcal{M}_{\mathcal{P}}(\mathcal{C})$, on les appelle les unités de $\mathcal{O}_P(\mathcal{C})$.
Si f est définie et s'annule en P, on dit que P est un zéro de f.
L'ensemble des points de $\mathcal{C}$ où la fonction rationnelle f est définie et s'annule en P est noté $\mathcal{Z}(f)$, et appelé l'ensemble des zéros de f.
L'ensemble des points de $\mathcal{C}$ où la fonction rationnelle f n'est pas définie est noté $\mathcal{P}(f)$, et appelé l'ensemble des pôles de f.

Définitions 1.3.3. Soit $\mathcal{C}$ une courbe projective plane et lisse, et f une fonction non nulle de $k(\mathcal{C})$.
On associe à f le diviseur noté $div(f)$ et défini par :

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

Un tel diviseur est appelé diviseur principal. On note $Siv(\mathcal{C})$ **l'ensemble des diviseurs principaux sur** $\mathcal{C}$; c'est un sous-groupe de $Div(\mathcal{C})$.
On définit aussi la relation d'équivalence " $\backsimeq$ " sur l'ensemble des diviseurs sur $\mathcal{C}$ par :
$D \backsimeq D'$ si et seulement si $\exists f \in k(\mathcal{C}) : D - D' = div(f)$.

Remarque 1.3.1. Soit f une fonction non nulle de $k(\mathcal{C})$.

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

Si l'on pose

$$div(f)_0 = \sum_{P \in \mathcal{Z}(f)} ord_p(f)P = \sum_{ord_p(f)>0} ord_p(f)P$$

et

$$div(f)_\infty = \sum_{P \in \mathcal{P}(f)} -ord_p(f)P = \sum_{ord_p(f)<0} -ord_p(f)P$$

alors $div(f) = div(f)_0 - div(f)_\infty$.
$div(f)_0$ est appelé diviseur des zéros de f et $div(f)_\infty$ diviseur des pôles de f. Cela signifie géométriquement que $div(f)_0$ correspond à l'intersection de $\mathcal{C}$ avec la courbe $f = 0$ et $div(f)_\infty$ correspond à l'intersection de $\mathcal{C}$ avec la courbe $\frac{1}{f} = 0$. Une fonction rationnelle f a autant de zéros que de pôles donc $deg(div(f)) = 0$. L'ensemble des diviseurs principaux est un sous-groupe de $Div^0(\mathcal{C})$.

Définition 1.3.1. Soit $\mathcal{C}$ une courbe plane projective et soit $D \in Div(\mathcal{C})$. On associe à D l'ensemble des fonctions :

$$\mathcal{L}(D) = \{f \in k(C) \mid div(f) + D \geq 0\} \cup \{0\}$$

$\mathcal{L}(D)$ est un k-espace vectoriel de dimension finie et on note $l(D)$ sa dimension :

$$l(D) = dim_k \mathcal{L}(D).$$

Proposition 1.3.1. Soient D et D' deux diviseurs.
1) Si $D \leq D'$, alors $\mathcal{L}(D) \subset \mathcal{L}(D')$.
2)Si $deg(D) < 0$, alors $\mathcal{L}(D) = 0; \mathcal{L}(0) = k$.
3) $\mathcal{L}(D)$ est de dimension finie pour tout diviseur D. Si $deg(D) \geq 0$ alors
$l(D) \leq deg(D) + 1$.

4) Si $D \backsimeq D'$, alors $l(D) = l(D')$.

Définition 1.3.2. Le genre géométrique d'une courbe projective plane irréductible $\mathcal{C}$ est l'entier positif ou nul noté $g(\mathcal{C})$ défini par

$$g(\mathcal{C}) = \frac{(d-1)(d-2)}{2} - s \text{ avec } d > 1$$

où d est le degré de la courbe et s le nombre de points singuliers. Ce qui permet de faire un lien entre le genre et le degré d'une courbe.

Théorème 1.3.1 (RIEMANN-ROCH). Soit $\mathcal{C}$ une courbe projective irréductible et lisse. Alors il existe un diviseur $K_{\mathcal{C}}$ appelé diviseur canonique et un entier $g \geq 0$ appelé genre de $\mathcal{C}$ tel que pour tout diviseur $D \in Div(\mathcal{C})$ on a

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

Corollaire 1.
1) $deg(K_{\mathcal{C}}) = 2g - 2$ et $l(K_{\mathcal{C}}) = g$ si $K_{\mathcal{C}}$ est un diviseur canonique.
2) Si $deg(D) \geq 2g - 1$, alors $l(D) = deg(D) - g + 1$.
3) Si $deg(D) \geq 2g$, alors

$$l(D - P) = l(D) - 1$$

pour tout $P \in X$.
4)(Théorème de Clifford) si $l(D) \neq 0$ et $l(K_{\mathcal{C}} - D) \neq 0$, alors on a

$$l(D) \leq \frac{1}{2} deg(D) + 1$$

1.4 Jacobienne d'une courbe

Définitions 1.4.1. On définit le groupe de Picard de $\mathcal{C}$ comme étant l'ensemble des classes de diviseurs sur $\mathcal{C}$ modulo l'équivalence linéaire :

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

De même $Pic^0(\mathcal{C})$ est l'ensemble des classes de diviseurs zéro dans $Pic(\mathcal{C})$.
La jacobienne d'une courbe $\mathcal{C}$ définie sur $\mathbb{K}$ est le sous-groupe des éléments de degré 0 dans le groupe de Picard de $\mathcal{C}$ notée $Jac(\mathcal{C})$. Autrement dit,

$$\begin{aligned} deg : Pic(\mathcal{C}) &\longrightarrow \mathbb{Z} \\ cl(D) &\longmapsto deg(D) \end{aligned}$$

$$Jac(\mathcal{C}) = Ker[deg : Pic(\mathcal{C}) \longrightarrow \mathbb{Z}]$$

1.5 Plongement jacobien

Définition 1.5.1.
Soit P_∞ un point rationnel de $\mathcal{C}$ défini sur $\mathbb{K}$. Pour tout D diviseur, on note $[D]$ sa classe dans $Pic^0(\mathcal{C})$. On définit le plongement jacobien de la manière suivante :

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

Remarque 1.5.1.
j donne un morphisme de $\mathcal{C}(\mathbb{K}) \longrightarrow Jac(\mathcal{C})(\mathbb{K})$ défini par $P \longmapsto [P - P_\infty]$. L'application j s'étend par linéarité aux diviseurs $Div^0(\mathcal{C})$ vers $Jac(\mathcal{C})$.

Théorème 1.5.1. (D'Abel)
Les énoncés suivantes sont équivalentes
1) Pour tout diviseur D dans $Div^0(\mathcal{C})$, il existe une fonction rationnelle f définie sur $\mathcal{C}$ à coefficients dans $\mathbb{K}^*$ telle que $div(f) = D$. Autrement dit : $\forall D \in Div^0(\mathcal{C})$, $\exists f \in \mathbb{K}^*(\mathcal{C})$: $div(f) = D$.
2) $j(D) = 0$.

Théorème 1.5.2. (Abel-Jacobi)
L'application j est surjective et $Ker(j) = Im(div)$. En d'autre terme : $Pic^0(\mathcal{C}) \simeq Jac(\mathcal{C})$

1.6 Groupe de Mordeil-Weil

Théorème 1.6.1. Soit A une variété abélienne définie sur un corps de nombre (K). Alors le groupe $A(\mathbb{K})$ des points $\mathbb{K}-$rationnels de A est fini. En d'autre terme :

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

L'entier naturel r est le rang de la variété et $A(\mathbb{K})_{tor}$ est le groupe de torsion.

Remarque 1.6.1. Si A est la jacobienne d'une courbe algébrique définie sur $\mathbb{Q}$ alors

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

Si le rang de la courbe est nul alors

$$J(\mathbb{Q}) \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_s\mathbb{Z}$$

Il existe s diviseurs D_1,...D_i...,D_s sur $\mathcal{C}$ définis sur $\mathbb{Q}$ tels que $j(D_i)$ soit d'ordre m_i et $j(D_1)$,...,$j(D_s)$ engendrent $J(\mathbb{Q})$.

1.7 Cycle d'intersection

Définition 1.7.1.
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes projectives planes, sans composante irréductible commune, de degré n et m. On définit le **cycle d'intersection** de $\mathcal{C}$ et $\mathcal{C}'$ noté

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

Où $\sum_{P\in\mathbb{P}^2} I(\mathcal{C}.\mathcal{C}',P)$ est le nombre total de points d'intersections d'une courbe projective plane $\mathcal{C}$ et d'une courbe projective plane $\mathcal{C}'$

Remarque 1.7.1.
Le nombre total de points d'intersections d'une courbe projective plane $\mathcal{C}$ et d'une droite D dans le plan projectif noté $\sum_{P\in\mathbb{P}^2} I(\mathcal{C}.D,P)$ et donné par

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

Chapitre 2

Points algébriques de petit degré sur certaines courbes

2.1 Points algébriques de petit degré sur la courbe d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$

2.1.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique définie sur $\mathbb{K}$ et $\mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$. Le degré d'un point algébrique w est le degré de son corps de définition sur $\mathbb{Q}$, i.e, $deg(w) = [\mathbb{Q}(w) : \mathbb{Q}]$.
Nous nous proposons d'étudier en détail $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 3} \mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques de degré au plus trois sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.
La courbe $\mathcal{C}$ est hyper-elliptique de genre $g = 2$ et le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C} : y^2 = x(x-3)(x-4)(x-6)(x-7)$ est fini et donné par $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ (voir [Go-Gr-93], p.822).
Notons par $P_1 = (0,0)$, $P_2 = (3,0)$, $P_3 = (4,0)$, $P_4 = (6,0)$, $P_5 = (7,0)$ en affine et ∞ le point à infini de $\mathcal{C}$.
Daniel M.Gordon et David Grant qui ont déterminé dans ([Go-Gr-93],p.808) l'ensemble des points rationnels sur la courbe $\mathcal{C}$ donné par la proposition suivante :

Proposition 2.1.1.
L'ensemble des points rationnels sur $\mathbb{Q}$ de la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$ est donné par

$$\mathcal{C}(\mathbb{Q}) = \{P_1,P_2,P_3,P_4,P_5,\infty\}$$

Nos outils essentiels sont :

1. Le groupe de Mordell–Weil $J(\mathbb{Q})$ de la jacobienne de $\mathcal{C}$,
2. Le théorème d'Abel–Jacobi(voir [Gri-89] page 156),

Théorème 1
1-L'ensemble des points quadratiques sur la courbe $\mathcal{C}$ d'équation affine
$y^2 = x(x-3)(x-4)(x-6)(x-7)$ est donné par :

$$\mathcal{A}_1 = \left\{ \left(x, \pm \sqrt{-\frac{a_0}{a_1}(-\frac{a_0}{a_1}-3)(-\frac{a_0}{a_1}-4)(-\frac{a_0}{a_1}-6)(-\frac{a_0}{a_1}-7)} \right) \mid x \in \mathbb{Q}^* \right\}$$

2-L'ensemble des points cubiques sur la courbe $\mathcal{C}$ d'équation affine
$y^2 = x(x-3)(x-4)(x-6)(x-7)$ est vide.

2.1.2 Résultats auxiliaires

Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

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

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

L'équation projective de la courbe $\mathcal{C}$ est : $Y^2Z^3 = X(X-3Z)(X-4Z)(X-6Z)(X-7Z)$.

Lemme 2.1.1.
i) $div(x) = 2P_1 - 2\infty$; $div(x-3) = 2P_2 - 2\infty$; $div(x-4) = 2P_3 - 2\infty$; $div(x-6) = 2P_4 - 2\infty$; $div(x-7) = 2P_5 - 2\infty$; $div(y) = P_1 + P_2 + P_3 + P_4 + P_5 - 5\infty$.
ii) $\mathcal{L}(\infty) =< 1 >$
$\mathcal{L}(2\infty) =< 1,x >$
$\mathcal{L}(3\infty) = \mathcal{L}(2\infty) =< 1,x >$
$\mathcal{L}(4\infty) =< 1,x,x^2 >$
$\mathcal{L}(5\infty) =< 1,x,x^2,y >$
$\mathcal{L}(6\infty) =< 1,x,x^2,y,x^3 >$

Preuve 2.1.1.
i) il s'agit d'un calcul de type

$$div(x-i) = ((X-iZ) = 0).\mathcal{C} - (Z = 0).\mathcal{C} \qquad (\star)$$

D'après $(\star)$, on a $div(x) = (X = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
Pour $X = 0$, l'équation projective donne $Y^2Z^3 = 0$; et pour $Z = 1$, on obtient le point $P_1 = [0 : 0 : 1]$ de multiplicité égale à 2. Ainsi $(X = 0).\mathcal{C} = 2P_1 + 3\infty$.
Pour $Z = 0$, l'équation projective donne $X^5 = 0$; et pour $Y = 1$, on obtient le point

$\infty = [0:1:0]$ de multiplicité égale à 5. Ainsi $(Z=0).\mathcal{C} = 5\infty$.
Donc $div(x) = 2P_1 + 3\infty - 5\infty = 2P_1 - 2\infty$. De la même manière on montre que $div(x-3) = 2P_2 - 2\infty$, $div(x-4) = 2P_3 - 2\infty$, $div(x-6) = 2P_4 - 2\infty$, $div(x-7) = 2P_5 - 2\infty$ et $div(y) = P_1 + P_2 + P_3 + P_4 + P_5 - 5\infty$.
ii) On déduit de i) et du fait que d'après le théorème de Riemann-Roch, on a $l(p\infty) = p - g + 1 = p - 1$ dès que $p \geq 2g - 1 = 3$ □

Conséquences 2.1.1.
$2j(P_1) = 2j(P_2) = 2j(P_3) = 2j(P_4) = 2j(P_5) = 0$
$j(P_1) + j(P_2) + j(P_3) + j(P_4) + j(P_5) = 0$

Lemme 2.1.2.
$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \cong < j(P_1), j(P_2), j(P_3), j(P_4) >$

Preuve 2.1.2.
On sait que $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ or $dim_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})^4 = 4$ donc $dim_{\mathbb{Z}/2\mathbb{Z}} J(\mathbb{Q}) = 4$.
$Card\left(\left\{j(P_1), j(P_2), j(P_3), j(P_4)\right\}\right) = 4$, or on sait que le plongement jacobien

$$\begin{array}{ccc} j : \mathcal{C}(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ P & \longmapsto & [P - \infty] \end{array}$$ est surjective, donc $j(P_i) \in J(\mathbb{Q})$ avec $i \in \{1,2,3,4,5\}$. D'après la conséquence (2.1.1) , pour que $\left\{j(P_1), j(P_2), j(P_3), j(P_4)\right\}$ soit une base il suffit que la famille soit génératrice, ce qui est vrai cf [Sc-98] et [Sa-To-Fa-10].

2.1.3 Démonstration du théorème

Détermination des points quadratiques

Soit $w \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = 2$. Notons w_1, w_2 les conjugués de Galois de w et considérons $[w_1 + w_2 - 2\infty]$ qui est un point de $J(\mathbb{Q})$. On remarque que $w \notin \left\{P_1, P_2, P_3, P_4, P_5, \infty\right\}$.
On a
$[w_1 + w_2 - 2\infty] = m_1 j(P_1) + m_2 j(P_2) + m_3 j(P_3) + m_4 j(P_4)$ avec $m_i \in \{0,1\}$. Ce qui donne la relation

$$[w_1 + w_2 + \sum_{i=1}^{4} m_i P_i - (2 + \sum_{i=1}^{4} m_i)\infty] = 0$$

Il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i - (2 + \sum_{i=1}^{4} m_i)\infty \qquad (2.1.1)$$

Premier cas : les m_i sont tous nuls

La relation (2.1.1) donne : $div(f) = w_1 + w_2 - 2\infty$, donc $f \in \mathcal{L}(2\infty)$ et par suite $f = a_0 + a_1x$ ($a_0 \neq 0$ sinon un des w_i serait égal à P_1 ou à ∞ et $a_1 \neq 0$ sinon un des w_i serait égal à ∞). Aux points w_i, on a : $a_0 + a_1x = 0$, d'où $x = -\frac{a_0}{a_1}$. On sait que $y^2 = x(x-3)(x-4)(x-6)(x-7)$ donc $y = \pm\sqrt{-\frac{a_0}{a_1}(-\frac{a_0}{a_1}-3)(-\frac{a_0}{a_1}-4)(-\frac{a_0}{a_1}-6)(-\frac{a_0}{a_1}-7)}$ et on obtient l'ensemble des points quadratiques

$$\mathcal{A}_1 = \left\{ \left(x, \pm\sqrt{-\frac{a_0}{a_1}(-\frac{a_0}{a_1}-3)(-\frac{a_0}{a_1}-4)(-\frac{a_0}{a_1}-6)(-\frac{a_0}{a_1}-7)} \right) \mid x \in \mathbb{Q}^* \right\}$$

Deuxième cas : seul un des m_i n'est pas nul

Supposons $m_1 \neq 0$, la relation (2.1.1) donne $div(f) = w_1 + w_2 + P_1 - 3\infty$, donc $f \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, un des w_i est alors égal à ∞ ; ce qui est absurde. De la même manière, on montre que c'est absurde pour $m_i \neq 0$ avec $i \in \{2,3,4\}$

Troisième cas : seuls deux des m_i ne sont pas nuls

Supposons $m_1 = m_2 = 1$, la relation (2.1.1) donne $div(f) = w_1 + w_2 + P_1 + P_2 - 4\infty$, donc $f \in \mathcal{L}(4\infty)$, par suite $f = a_0 + a_1x + a_2x^2$; et comme $ordf_{P_1} = 1$, on doit avoir $a_0 = a_1 = a_2 = 0$, ce qui est absurde car un des w_i devrait être égal P_1. De la même manière, on montre que c'est absurde pour $m_i = m_j = 1$ avec $i \neq j$ et $i,j \in \{1,2,3,4\}$.

Quatrième cas : seul un des m_i est nul

Supposons $m_4 = 0$, la relation (2.1.1) donne $div(f) = w_1 + w_2 + P_1 + P_2 + P_3 - 5\infty$, donc $f \in \mathcal{L}(5\infty)$, par suite $f = a_0 + a_1x + a_2x^2 + a_3y$; et comme $ordf_{P_1} = 1$, on doit avoir $a_0 = a_1 = a_2 = 0$ (sinon un des w_i devrait être égal P_1) donc $f = a_3y$ et un des w_i devrait être égal P_4, ce qui est absurde. De la même manière, on montre que c'est absurde pour $m_i = 0$ avec $i \in \{1,2,3\}$

Cinquième cas : aucun des m_i n'est nul

la relation (2.1.1) donne $div(f) = w_1 + w_2 + P_1 + P_2 + P_3 + P_4 - 6\infty$, donc $f \in \mathcal{L}(6\infty)$, par suite $f = a_0 + a_1x + a_2x^2 + a_3y + a_4x^3$; et comme $ordf_{P_1} = 1$, on doit avoir $a_0 = a_1 = a_2 = a_4 = 0$ (sinon un des w_i devrait être égal P_1) donc $f = a_3y$ et un des w_i devrait être égal P_∞, ce qui est absurde. □

Détermination des points cubiques

Soit $w \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = 3$. Notons w_1,w_2,w_3 les conjugués de Galois de w alors $[w_1 + w_2 + w_3 - 3\infty]$ est un point de $J(\mathbb{Q})$. On remarque que $w \notin \left\{P_1,P_2,P_3,P_4,P_5,\infty\right\}$. On a $[w_1 + w_2 + w_3 - 3\infty] = m_1j(P_1) + m_2j(P_2) + m_3j(P_3) + m_4j(P_4)$ avec $m_i \in \{0,1\}$. Ce qui donne la relation

$$[w_1 + w_2 + w_3 + \sum_{i=1}^{4} m_iP_i - (3 + \sum_{i=1}^{4} m_i)\infty] = 0$$

Il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = w_1 + w_2 + w_3 + \sum_{i=1}^{4} m_iP_i - (3 + \sum_{i=1}^{4} m_i)\infty \tag{2.1.2}$$

Premier cas : les m_i sont tous nuls

La relation (2.1.2) donne : $div(f) = w_1 + w_2 + w_3 - 3\infty$, donc $f \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, un des w_i est alors égal à ∞ ; ce qui est absurde.

Deuxième cas : seul un des m_i n'est pas nul

Supposons $m_1 \neq 0$, la relation (2.1.2) donne $div(f) = w_1 + w_2 + w_3 + P_1 - 4\infty$, donc $f \in \mathcal{L}(4\infty)$, par suite $f = a_0 + a_1x + a_2x^2$; et comme $ordf_{P_1} = 1$, on doit avoir $a_0 = a_1 = a_2 = 0$ (sinon un des w_i devrait être égal P_1), ce qui est absurde. De la même manière, on montre que c'est absurde pour $m_i \neq 0$ avec $i \in \{2,3,4\}$.

Troisième cas : seuls deux des m_i ne sont pas nuls

Supposons $m_1 = m_2 = 1$, la relation (2.1.2) donne $div(f) = w_1 + w_2 + w_3 + P_1 + P_2 - 5\infty$, donc $f \in \mathcal{L}(5\infty)$, par suite $f = a_0 + a_1x + a_2x^2 + a_3y$; et comme $ordf_{P_1} = 1$, on doit

avoir $a_0 = a_1 = a_2 = 0$ (sinon un des w_i devrait être égal P_1) donc $f = a_3y$ et un des w_i devrait être égal P_4, ce qui est absurde. De la même manière on montre que c'est absurde pour $m_i = m_j = 1$ avec $i \neq j$ et $i,j \in \{1,2,3,4\}$.

Quatrième cas : seul un des m_i est nul

Supposons $m_4 = 0$, de la relation (2.1.2), on a $div(f) = w_1 + w_2 + w_3 + P_1 + P_2 + P_3 - 6\infty$, donc $f \in \mathcal{L}(6\infty)$, par suite $f = a_0 + a_1x + a_2x^2 + a_3y + a_4x^3$; et comme $ordf_{P_1} = 1$, on doit avoir $a_0 = a_1 = a_2 = a_4 = 0$ (sinon un des w_i devrait être égal P_1) donc $f = a_3y$ et un des w_i devrait être égal P_4, ce qui est absurde. De la même manière on montre que c'est absurde pour $m_i = 0$ avec $i \in \{1,2,3\}$

Cinquième cas : aucun des m_i n'est nul

la relation (2.1.2) donne $div(f) = w_1 + w_2 + w_3 + P_1 + P_2 + P_3 + P_4 - 7\infty$, donc $f \in \mathcal{L}(7\infty)$, par suite $f = a_0 + a_1x + a_2x^2 + a_3y + a_4x^3 + a_5xy$ avec $(a_3 \neq 0)$ (sinon devrait avoir $P_5 = \infty$). On a $f(P_1) = 0$, $f(P_2) = 0$, $f(P_3) = 0$ et $f(P_4) = 0$, c'est à dire $\begin{cases} a_0 = 0 \\ 3a_1 + 9a_2 + 27a_4 = 0 \\ 4a_1 + 16a_2 + 64a_4 = 0 \\ 6a_1 + 36a_2 + 216a_4 = 0 \end{cases}$; ce qui donne $a_1 = a_2 = a_4 = 0$, d'où $f = a_3y + a_5xy$.
Aux points w_i, on a $a_3y + a_5xy = 0$ d'où $x = -\frac{a_3}{a_5}$. On obtient une famille de points quadratiques, ce qui est absurde. Donc l'ensemble des points cubiques est vide.

2.2 Points algébriques de petit degré sur la courbe d'équation affine $y^{11} = x^3(x-1)^3$

2.2.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique lisse définie sur un corps de nombres $\mathbb{K}$. On note $\mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus l sur $\mathbb{Q}$.
Notre étude résulte des travaux sur la famille de courbes $y^p = x^r(x-1)^r$ avec $1 \leq r$, $2r \leq p-1$. Une telle famille a intéressé certains géomètres algébristes dont Gross-Rohrlich

qui ont déterminé $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 2} \mathcal{C}_1(11)(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}_1(11)$ de degré au-plus 2 sur $\mathbb{Q}$ dans [Gr-Ro-78]. Le groupe de Mordell-Weil $J(\mathbb{Q})$ des points rationnels de la jacobienne J est fini. On note $P_0 = (0:0:0)$, $P_1 = (1:0:1)$, $P_\infty = (1:0:0)$ en projectif et considérons le plongement jacobien $\begin{array}{ccc} j : \mathcal{C}_3(11)(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ P & \longmapsto & [P - P_\infty] \end{array}$.

Nous donnons une description explicite des points algébriques sur $\mathcal{C}_3(11)$ de degré au-plus 3 sur $\mathbb{Q}$. Notre résultat principal s'énonce comme suit :

Théorème 2

L'ensemble des points algébriques sur $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$ de degré au-plus 3 sur $\mathbb{Q}$ est donné par :

$$\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 3} \mathcal{C}_3(11)(\mathbb{K}) = \{P_0,P_1,P_\infty\} \cup \mathcal{F}$$

avec

$$\mathcal{F} = \left\{ \left(x,[\beta x(x-1)]^{\frac{1}{4}} \right) \mid \beta \in \mathbb{Q}^* \quad \textbf{et x racine de l'équation} \;\; x(x-1) = \beta^{11} \right\}$$

2.2.2 Résultats auxiliaires

Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par : $x(X,Y,Z) = \frac{X}{Z}$ et $y(X,Y,Z) = \frac{Y}{Z}$.

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

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

Lemme 2.2.1.

$J(\mathbb{Q}) \cong \mathbb{Z}/11\mathbb{Z}$.

Preuve 2.2.1.

D'après Gross et Rohrlich ([Gr-Ro-78], p.219), on a $J(\mathbb{Q})_{torsion} \cong \mathbb{Z}/11\mathbb{Z}$, et d'après Faddeev [Fa-61], on a $J(\mathbb{Q})_{torsion} \cong J(\mathbb{Q})$.

Lemme 2.2.2. $\mathcal{C}_3(11) : y^{11} = x^3(x-1)^3$

i) $div(x) = 11P_0 - 11P_\infty$; $div(y) = 3P_0 + 3P_1 - 6P_\infty$

$div(x-1) = 11P_1 - 11P_\infty$

ii) $\mathcal{L}(P_\infty) =< 1 >$

$\mathcal{L}(2P_\infty) =< 1, \frac{x^2(x-1)^2}{y^7} >$

$\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$

$\mathcal{L}(4P_\infty) =< 1, \frac{x^2(x-1)^2}{y^7}, \frac{x(x-1)}{y^3} >$

$\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$
$\mathcal{L}(6P_\infty) =< 1, \frac{x^2(x-1)^2}{y^7}, \frac{x(x-1)}{y^3}, y >$
$\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$
$\mathcal{L}(8P_\infty) =< 1, \frac{x^2(x-1)^2}{y^7}, \frac{x(x-1)}{y^3}, y, \frac{x^2(x-1)^2}{y^6} >$
$\mathcal{L}(9P_\infty) = \mathcal{L}(8P_\infty)$
$\mathcal{L}(10P_\infty) =< 1, \frac{x^2(x-1)^2}{y^7}, \frac{x(x-1)}{y^3}, y, \frac{x^2(x-1)^2}{y^6}, \frac{x(x-1)}{y^2} >$

Preuve 2.2.2.
i) Il s'agit d'un calcul de type $div(x-i) = ((X-iZ)=0).\mathcal{C} - (Z=0).\mathcal{C}$. $(\star)$
$Y^{11} = Z^5X^3(X-Z)^3$ est l'équation projective de la courbe $\mathcal{C}_3(11)$.
D'après $(\star)$, $div(x) = (X=0).\mathcal{C} - (Z=0).\mathcal{C}$
Pour $X=0$, l'équation projective donne $Y^{11}=0$; et pour $Z=1$, on obtient le point $P_0 = (0:0:1)$ de multiplicité 11.
Pour $Z=0$, l'équation projective donne $Y^{11}=0$; et pour $X=1$, on obtient le point $P_\infty = (1:0:0)$ de multiplicité 11,donc $div(x) = 11P_0 - 11P_\infty$.
De la même manière on montre que $div(x-1) = 11P_1 - 11P_\infty$ et $div(y) = 3P_0 + 3P_1 - 6P_\infty$. Voir [Sa-03].
ii) On déduit de i) et du fait que d'après le théorème de Riemann-Roch, on a $l(kP_\infty) = k-g+1$ dès que $k \geq 2g-1$ avec $g = \frac{11-1}{2}$. Ainsi on a $l(kP_\infty) = k-4$ dès que $k \geq 9$. □

Conséquences 2.2.1.
$11j(P_0) = 11j(P_1) = 0$;
$3j(P_0) + 3j(P_1) = 0$.
Donc $j(P_0)$ et $j(P_1)$ engendrent le même sous-groupe $J(\mathbb{Q})$ isomorphe à $\mathbb{Z}/11\mathbb{Z}$. Par conséquent $J(\mathbb{Q}) \cong \mathbb{Z}/11\mathbb{Z} = \left\{ mj(P_0), 0 \leq m \leq 10 \right\}$

2.2.3 Démonstration du théorème

Détermination des points $\mathbb{Q}-$rationnels

Soit $w \in \mathcal{C}_3(11)(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w):\mathbb{Q}] = 1$, posons $t = [w-\infty]$ qui est un point de $J(\mathbb{Q})$. Par conséquent $t = mj(P_0)$, $0 \leq m \leq 10$. Ce qui donne la relation $[w-\infty] = mj(P_0)$ avec $0 \leq m \leq 10$.
Discutons suivant les valeurs m.
cas m=0
$[w - P_\infty] = 0$, ce qui donne $w = P_\infty$.
cas m=1
$[w - P_\infty] = j(P_0) = 3j(P_0) - 2j(P_0) = -3j(P_1) - 2j(P_0)$

$[w - P_\infty] = -3[P_1 - P_\infty] - 2[P_0 - P_\infty]$ d'où $[w + 3P_1 + 2P_0 - 6P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 3P_1 + 2P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + \frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3 y$. $ord_{P_1}(f) = 3$ d'où $a_0 = a_1 = a_2 = 0$, donc $f = a_3 y$; et par conséquent $w = P_0$.

cas m=2

$[w - P_\infty] = 2j(P_0) = 3j(P_0) - j(P_0) = -3j(P_1) - j(P_0)$

$[w - P_\infty] = -3[P_1 - P_\infty] - [P_0 - P_\infty]$ d'où $[w + 3P_1 + P_0 - 5P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 3P_1 + P_0 - 5P_\infty$, donc $f \in \mathcal{L}(5\infty)$; or $\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$, d'où $w = P_\infty$.

cas m=3

$[w - P_\infty] = 3j(P_0) = -3j(P_1)$

$[w - P_\infty] = -3[P_1 - P_\infty]$ d'où $[w + 3P_1 - 4P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 3P_1 - 4P_\infty$, donc $f \in \mathcal{L}(4P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3}$. $ord_{P_1}(f) = 3$ d'où $a_0 = a_1 = a_2 = 0$, ce qui est absurde.

m=4

on a : $[w - P_\infty] = 4j(P_0) = -7j(P_0)$

$[w - P_\infty] = -7[P_0 - P_\infty]$ d'où $[w + 7P_0 - 8P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 7P_0 - 8P_\infty$, donc $f \in \mathcal{L}(8\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3 y + a_4\frac{x^2(x-1)^2}{y^6}$.

$ord_{P_0}(f) = 7$ d'où $a_0 = a_1 = a_2 = a_3 = a_4 = 0$, ce qui est absurde.

cas m=5

$[w - P_\infty] = 5j(P_0) = -6j(P_0)$

$[w - P_\infty] = -6[P_0 - P_\infty]$ d'où $[w + 6P_0 - 7P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 6P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$; or $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ d'où $w = P_\infty$.

m=6

$[w - P_\infty] = 6j(P_0) = -5j(P_0)$

$[w - P_\infty] = [-5P_0 + 5P_\infty]$ d'où $[w + 5P_0 - 6P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 5P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3 y$. $ord_{P_0}(f) = 5$ d'où $a_0 = a_1 = a_2 = a_3 = 0$, ce qui est absurde.

cas m=7

$[w - P_\infty] = 7j(P_0) = -4j(P_0)$

$[w - P_\infty] = [-4P_0 + 4P_\infty]$ d'où $[w + 4P_0 - 5P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 4P_0 - 5P_\infty$, donc $f \in \mathcal{L}(5P_\infty)$; or $\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$, d'où $w = P_\infty$.

cas m=8

$[w - P_\infty] = 8j(P_0) = -3j(P_0)$

$[w - P_\infty] = [-3P_0 + 3P_\infty]$ d'où $[w + 3P_0 - 4P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 3P_0 - 4P_\infty$, donc $f \in \mathcal{L}(4P_\infty)$; par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3}$. $ord_{P_0}(f) = 3$ d'où $a_0 = a_1 = a_2 = 0$, ce qui est absurde.

cas m=9

$[w - P_\infty] = 9j(P_0) = -2j(P_0)$

$[w - P_\infty] = [-2P_0 + 2P_\infty]$ d'où $[w + 2P_0 - 3P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + 2P_0 - 3P_\infty$, donc $f \in \mathcal{L}(3P_\infty)$; or $\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$, d'où $w = P_\infty$.

cas m=10

$[w - P_\infty] = 10j(P_0) = -j(P_0)$

$[w - P_\infty] = [-P_0 + P_\infty]$ d'où $[w + P_0 - 2P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w + P_0 - 2P_\infty$, donc $f \in \mathcal{L}(2P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7}$, et comme $ord_{P_0}(f) = 1$ d'où $a_0 = 0$; donc $f = a_1\frac{x^2(x-1)^2}{y^7}$ et par conséquent $w = P_1$.

Détermination des points quadratiques

Soit $w \in \mathcal{C}_3(11)(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = 2$. Notons w_1,w_2 les conjugués de Galois de w et posons $t = [w_1 + w_2 - 2P_\infty]$ qui est un élément de $J(\mathbb{Q})$. On remarque que $w \notin \{P_0,P_1,P_\infty\}$. On a la relation $[w_1 + w_2 - 2P_\infty] = mj(P_0)$ avec $0 \leq m \leq 10$.

Discutons suivant les valeurs de m

cas m=0

$[w_1 + w_2 - 2P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 - 2P_\infty$, donc $f \in \mathcal{L}(2P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7}$.

Aux points w_i, on a $a_0 + a_1\frac{x^2(x-1)^2}{y^7} = 0$ d'où $y = \left[\frac{-a_1}{a_0}x^2(x-1)^2\right]^{\frac{1}{7}}$.

$y^{11} = x^3(x-1)^3 \Leftrightarrow [\frac{-a_1}{a_0}x^2(x-1)^2]^{\frac{11}{7}} = x^3(x-1)^3 \Leftrightarrow [\frac{-a_1}{a_0}]^{\frac{11}{7}}[x(x-1)]^{\frac{22}{7}} = x^3(x-1)^3$
$\Leftrightarrow [\frac{-a_1}{a_0}]^{\frac{11}{7}}[x(x-1)]^3[x(x-1)]^{\frac{1}{7}} = x^3(x-1)^3 \Leftrightarrow [\frac{-a_1}{a_0}]^{\frac{11}{7}}[x(x-1)]^{\frac{1}{7}} = 1$
$\Leftrightarrow [\frac{-a_1}{a_0}]^{11}x(x-1) = 1 \Leftrightarrow x(x-1) = [\frac{-a_1}{a_0}]^{-11}$, ce qui est absurde.

cas m=1

$[w_1 + w_2 - 2P_\infty] = j(P_0) = 3j(P_0) - 2j(P_0) = -3j(P_1) - 2j(P_0)$
$[w_1 + w_2 - 2P_\infty] = -3[P_1 - P_\infty] - 2[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 3P_1 + 2P_0 - 7P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients telle que $div(f) = w_1 + w_2 + 3P_1 + 2P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$; et comme $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=2

$[w_1 + w_2 - 2P_\infty] = 2j(P_0) = 3j(P_0) - j(P_0) = -3j(P_1) - j(P_0)$
$[w_1 + w_2 - 2P_\infty] = -3[P_1 - P_\infty] - [P_0 - P_\infty]$ d'où $[w_1 + w_2 + 3P_1 + P_0 - 6P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 3P_1 + P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y$.
$ord_{P_1}(f) = 3$, on doit avoir $a_0 = a_1 = a_2 = 0$ donc $f = a_3y$, d'où un des w_i doit être égale à P_0, ce qui absurde.

cas m=3

$[w_1 + w_2 - 2P_\infty] = 3j(P_0) = -3j(P_1)$
$[w_1 + w_2 - 2P_\infty] = -3[P_1 - P_\infty]$ d'où $[w_1 + w_2 + 3P_1 - 5P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients telle que $div(f) = w_1 + w_2 + 3P_1 - 5P_\infty$, donc $f \in \mathcal{L}(5P_\infty)$; et comme $\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$, donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=4

$[w_1 + w_2 - 2P_\infty] = 4j(P_0) = -7j(P_0)$
$[w_1 + w_2 - 2P_\infty] = -7[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 7P_0 - 9P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 7P_0 - 9P_\infty$, donc $f \in \mathcal{L}(9P_\infty)$; et comme $\mathcal{L}(9P_\infty) = \mathcal{L}(8P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=5

$[w_1 + w_2 - 2P_\infty] = 5j(P_0) = -6j(P_0)$
$[w_1 + w_2 - 2P_\infty] = -6[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 6P_0 - 8P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 6P_0 - 8P_\infty$, donc $f \in \mathcal{L}(8P_\infty)$; et par suite $f = a_0 + a_1a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y + a_4\frac{x^2(x-1)^2}{y^6}$. $ord_{P_0}(f) = 6$,

on doit avoir $a_0 = a_1 = a_2 = a_3 = a_4 = 0$, ce qui absurde.

cas m=6

$[w_1 + w_2 - 2P_\infty] = 6j(P_0) = -5j(P_0)$

$[w_1 + w_2 - 2P_\infty] = -5[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 5P_0 - 7P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 5P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$; et comme $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=7

$[w_1 + w_2 - 2P_\infty] = 7j(P_0) = -4j(P_0)$

$[w_1 + w_2 - 2P_\infty] = -4[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 4P_0 - 6P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 4P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + a_1 a_1 \frac{x^2(x-1)^2}{y^7} + a_2 \frac{x(x-1)}{y^3} + a_3 y$.

$ord_{P_0}(f) = 4$, on doit avoir $a_0 = a_1 = a_2 = a_3 = 0$, ce qui est absurde.

cas m=8

$[w_1 + w_2 - 2P_\infty] = 8j(P_0) = -3j(P_0)$

$[w_1 + w_2 - 2P_\infty] = -3[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 3P_0 - 5P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + 3P_0 - 5P_\infty$, donc $f \in \mathcal{L}(5P_\infty)$; et comme $\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=9

$[w_1 + w_2 - 2P_\infty] = 9j(P_0) = -2j(P_0)$

$[w_1 + w_2 - 2P_\infty] = -2[P_0 - P_\infty]$ d'où $[w_1 + w_2 + 2P_0 - 4P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que

$div(f) = w_1 + w_2 + 2P_0 - 4P_\infty$, donc $f \in \mathcal{L}(4P_\infty)$; et par suite $f = a_0 + a_1 \frac{x^2(x-1)^2}{y^7} + a_2 \frac{x(x-1)}{y^3}$.

$ord_{P_0}(f) = 2$, on doit avoir $a_0 = a_1 = a_2 = 0$ donc $f = a_2 \frac{x(x-1)}{y^3}$. Ce qui donne $div(f) = 2P_1 + 2P_0 - 4P_\infty$ donc un des w_i doit être égale à P_1, ce qui est absurde.

cas m=10

$[w_1 + w_2 - 2P_\infty] = 10j(P_0) = -j(P_0)$

$[w_1 + w_2 - 2P_\infty] = -[P_0 - P_\infty]$ d'où $[w_1 + w_2 + P_0 - 3P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + P_0 - 3P_\infty$, donc $f \in \mathcal{L}(3P_\infty)$; et comme $\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

Détermination des points cubiques

Soit $w \in \mathcal{C}_3(11)(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = 3$. Notons w_1,w_2 et w_3 les conjugués de Galois de w et posons $t = [w_1 + w_2 + w_3 - 3P_\infty]$ qui est un élément de $J(\mathbb{Q})$. On remarque que $w \notin \{P_0,P_1,P_\infty\}$. On a la relation $[w_1 + w_2 + w_3 - 3P_\infty] = mj(P_0)$ avec $0 \leq m \leq 10$.
Discutons suivant les valeurs de m

cas m=0
$[w_1 + w_2 + w_3 - 3P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 - 3P_\infty$, donc $f \in \mathcal{L}(3P_\infty)$; et comme $\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$, donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=1
$[w_1 + w_2 + w_3 - 3P_\infty] = j(P_0) = 3j(P_0) - 2j(P_0) = -3j(P_1) - 2j(P_0)$
$[w_1 + w_2 + w_3 - 3P_\infty] = -3[P_1 - P_\infty] - 2[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 3P_1 + 2P_0 - 8P_\infty] = 0$.
Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 3P_1 + 2P_0 - 8P_\infty$, donc $f \in \mathcal{L}(8P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y + a_4\frac{x^2(x-1)^2}{y^6}$.
$ord_{P_1}(f) = 3$, on doit avoir $a_0 = a_1 = a_2 = 0$ donc $f = a_3y + a_4\frac{x^2(x-1)^2}{y^6}$, ce qui implique $f = y(a_3 + a_4\frac{x^2(x-1)^2}{y^7})$; d'où un des w_i doit être égale à P_0, ce qui est absurde.

cas m=2
on a : $[w_1 + w_2 + w_3 - 3P_\infty] = 2j(P_0) = 3j(P_0) - j(P_0) = -3j(P_1) - j(P_0)$
$[w_1 + w_2 + w_3 - 3P_\infty] = -3[P_1 - P_\infty] - [P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 3P_1 + P_0 - 7P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 3P_1 + P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$; et comme $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=3
$[w_1 + w_2 + w_3 - 3P_\infty] = 3j(P_0) = -3j(P_1)$
$[w_1 + w_2 + w_3 - 3P_\infty] = -3[P_1 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 3P_1 - 6P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 3P_1 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y$.
$ord_{P_1}(f)$, on doit avoir $a_0 = a_1 = a_2 = 0$ donc $f = a_3y$ d'où un des w_i doit être égale à

P_0, ce qui est absurde.

cas m=4

$[w_1 + w_2 + w_3 - 3P_\infty] = 4j(P_0) = -7j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -7[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 7P_0 - 10P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 7P_0 - 10P_\infty$, donc $f \in \mathcal{L}(10P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y + a_4\frac{x^2(x-1)^2}{y^6} + a_5\frac{x(x-1)}{y^2}$.

$ord_{P_0}(f) = 7$, on doit avoir tous les coefficients nuls, ce qui est absurde.

cas m=5

$[w_1 + w_2 + w_3 - 3P_\infty] = 5j(P_0) = -6j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -6[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 6P_0 - 9P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 6P_0 - 9P_\infty$, donc $f \in \mathcal{L}(9P_\infty)$; et comme $\mathcal{L}(9P_\infty) = \mathcal{L}(8P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=6

on a : $[w_1 + w_2 + w_3 - 3P_\infty] = 6j(P_0) = -5j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -5[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 5P_0 - 8P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 5P_0 - 8P_\infty$, donc $f \in \mathcal{L}(8P_\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} + a_3y + a_4\frac{x^2(x-1)^2}{y^6}$.

$ord_{P_0}(f) = 5$, on doit avoir $a_0 = a_1 = a_2 = a_3 = a_4 = 0$, ce qui est absurde.

cas m=7

$[w_1 + w_2 + w_3 - 3P_\infty] = 7j(P_0) = -4j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -4[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 4P_0 - 7P_\infty] = 0$. Il existe une fonction f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 4P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$; et comme $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=8

$[w_1 + w_2 + w_3 - 3P_\infty] = 8j(P_0) = -3j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -3[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 3P_0 - 6P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 3P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$; et par suite $f = a_0 + a_1\frac{y^4}{x(x-1)} + a_2\frac{x(x-1)}{y^3} + a_3y$.

$ord_{P_0}(f) = 3$, on doit avoir $a_0 = a_1 = a_2 = 0$ donc $f = a_3y$ d'où un des w_i doit être égale à P_1, ce qui est absurde.

cas m=9

$[w_1 + w_2 + w_3 - 3P_\infty] = 9j(P_0) = -2j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -2[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + 2P_0 - 5P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + 2P_0 - 5P_\infty$, donc $f \in \mathcal{L}(5P_\infty)$; et comme $\mathcal{L}(5P_\infty) = \mathcal{L}(4P_\infty)$ donc un des w_i doit être égale à P_∞, ce qui est absurde.

cas m=10

$[w_1 + w_2 + w_3 - 3P_\infty] = 10j(P_0) = -j(P_0)$

$[w_1 + w_2 + w_3 - 3P_\infty] = -[P_0 - P_\infty]$ d'où $[w_1 + w_2 + w_3 + P_0 - 4P_\infty] = 0$. Il existe une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = w_1 + w_2 + w_3 + P_0 - 4P_\infty$, donc $f \in \mathcal{L}(4P\infty)$; et par suite $f = a_0 + a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3}$.

$ord_{P_0}(f) = 1$,on doit avoir $a_0 = 0$ donc $f = a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3}$.

Aux points w_i, $a_1\frac{x^2(x-1)^2}{y^7} + a_2\frac{x(x-1)}{y^3} = 0 \Rightarrow a_1\frac{x(x-1)}{y^4} + a_2 = 0 \Rightarrow y^4 = -\frac{a_1}{a_2}x(x-1)$ d'où $y = [-\frac{a_1}{a_2}x(x-1)]^{\frac{1}{4}}$.

$$\begin{aligned} y^{11} = x^3(x-1)^3 &\Leftrightarrow [\tfrac{-a_1}{a_2}x(x-1)]^{\frac{11}{4}} = x^3(x-1)^3 \\ &\Leftrightarrow (\tfrac{-a_1}{a_2})^{\frac{11}{4}}[x(x-1)]^{\frac{11}{4}} = x^3(x-1)^3 \\ &\Leftrightarrow (\tfrac{-a_1}{a_2})^{\frac{11}{4}}x^3(x-1))^3[x(x-1)]^{-\frac{1}{4}} = x^3(x-1)^3 \\ &\Leftrightarrow (\tfrac{-a_1}{a_2})^{\frac{11}{4}}[x(x-1)]^{-\frac{1}{4}} = 1 \\ &\Leftrightarrow x(x-1) = (\tfrac{-a_1}{a_2})^{11} \end{aligned}$$

Ainsi on trouve une famille de points :

$$\mathcal{F} = \left\{ \left(x, [\beta x(x-1)]^{\frac{1}{4}} \right) \mid x \textit{ racine de l'équation } x(x-1) = \beta^{11} \right\} \text{ avec } \beta = (\tfrac{-a_1}{a_2}) \in \mathbb{Q}^*$$

Chapitre 3

Points algébriques de degrés quelconques sur certaines courbes

3.1 Points algébriques de degrés quelconques sur la courbe d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$

3.1.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique définie sur $\mathbb{K}$. Nous nous proposons d'étudier en détail les points algébriques de degré quelconque donnée sur le corps $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.
Dans le **chapitre 2**, on a donné une description explicite des points algébriques de degré au plus trois sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.
Par la suite, on va étendre ce résultat en déterminant qualitativement de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathbb{Q}$ de degré au plus l donnés sur $\mathcal{C}$ d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$.
Le résultat principal s'énonce comme suit :

Théorème 3
Considérons la courbe d'équation affine $y^2 = x(x-3)(x-4)(x-6)(x-7)$. Soit $w \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(w) : \mathbb{Q}] = l$. Notons w_1,...,w_l les conjugués de Galois de w et $E\left(\frac{l+4}{2}\right)$ la partie entière de $\frac{l+4}{2}$.
Alors il existe une courbe $\mathcal{M}$ définie sur $\mathbb{Q}$ de degré $\alpha \leq E\left(\frac{l+4}{2}\right)$ telle que

$\mathcal{M}.\mathcal{C} = w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i + (5\alpha - l - \sum_{i=1}^{4} m_i)\infty$ avec $m_i \in \{0,1\}$.

En particulier

1) Les points algébriques sur $\mathcal{C}$ de degré 2 sur $\mathbb{Q}$ sont donnés :

$\mathcal{M}.\mathcal{C} = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (8 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une conique.

$\mathcal{C}_1.\mathcal{C} = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (3 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est droite.

2) Les points algébriques sur $\mathcal{C}$ de degré 3 sur $\mathbb{Q}$ sont donnés :

$\mathcal{M}.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (12 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une cubique.

$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (7 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est une conique.

$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (2 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_2$ est une droite.

3) Les points algébriques sur $\mathcal{C}$ de degré 4 sur $\mathbb{Q}$:

$\mathcal{M}.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (16 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{M}$ est une quartique.

$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (11 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_1$ est une cubique.

$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (6 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_2$ est une conique.

$\mathcal{C}_3.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (1 - \sum_{i=1}^{4} m_i)\infty$ où $\mathcal{C}_3$ est une droite.

3.1.2 Résultats auxiliaires

Lemme 3.1.1. $\mathcal{C} : y^2 = x(x-3)(x-4)(x-6)(x-7)$

i) $div(x) = 2P_1 - 2\infty$; $div(x-3) = 2P_2 - 2\infty$; $div(x-4) = 2P_3 - 2\infty$;
$div(x-6) = 2P_4 - 2\infty$; $div(x-7) = 2P_5 - 2\infty$; $div(y) = P_1 + P_2 + P_3 + P_4 + P_5 - 5\infty$.

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

$$\mathcal{B}_p = \left\{ x^i \mid i \in \mathbb{N}, i \leq \frac{p}{2} \right\} \bigcup \left\{ yx^j \mid j \in \mathbb{N}, j \leq \frac{p-5}{2} \right\}$$

Preuve 3.1.1.

voir (2.1.1)

ii) Il est clair $\mathcal{B}_p$ est libre. Il reste à montrer que $dim(\mathcal{B}_p) = dim(\mathcal{L}(p\infty))$.

D'après le théorème de Riemann-Roch, on a $dim(\mathcal{L}(p\infty)) = p - g + 1$ dès que $p \geq 2g - 1$ avec $g = \frac{(5-1)(2-1)}{2} = 2$

Considérons les cas suivants :

cas 1 : supposons que p est pair, et posons $p = 2h$. On a alors

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

Donc on obtient $\mathcal{B}_p = \left\{1,x,...,x^h\right\} \cup \left\{y,yx,...,yx^{h-g-1}\right\}$, et par conséquent
$dim(\mathcal{B}_p) = (h+1) + (h-g) = 2h-g+1 = p-g+1 = dim(\mathcal{L}(p\infty)$
cas 2 : supposons que p est impair, et posons $p = 2h+1$. On a alors
$i \leq \frac{p}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h$ et $j \leq \frac{p-5}{2} \Leftrightarrow j \leq \frac{2h-4}{2} = h-g$
Donc on obtient $\mathcal{B}_p = \left\{1,x,...,x^h\right\} \cup \left\{y,yx,...,yx^{h-g}\right\}$, et par conséquent
$dim(\mathcal{B}_p) = (h+1) + (h-g+1) = 2h+1-g+1 = p-g+1 = dim(\mathcal{L}(p\infty))$
□

Conséquences 3.1.1.
i) $2j(P_1) = 2j(P_2) = 2j(P_3) = 2j(P_4) = 2j(P_5) = 0$;
$j(P_1) + j(P_2) + j(P_3) + j(P_4) + j(P_5) = 0$
ii) Les $f \in \mathcal{L}(p\infty)$ sont des polynômes de la forme :

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

Lemme 3.1.2.

$$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \cong < j(P_1),j(P_2),j(P_3),j(P_4) >$$

Preuve 3.1.2.
Voir (2.1.2) .

Lemme 3.1.3.
Soient L_{m_i} avec $i \in \{1,...,4\}$ et L_∞ les droites tangentes à $\mathcal{C}$ en m_i et ∞ respectivement. Alors ces droites ont un point de contact d'ordre 5 avec $\mathcal{C}$ en m_i et ∞ respectivement. Aussi, si une courbe M de degré ≤ 4 a un point de contact d'ordre $> degM$ avec $\mathcal{C}$ en m_i ou ∞, alors M contient L_{m_i} ou L_∞ respectivement.

Preuve 3.1.3.
$(\mathcal{C}.L_{m_i})$ est l'intersection de la courbe $\mathcal{C}$ avec la droite L_{m_i} aux points m_i.
$(\mathcal{C}.L_{m_i})_{m_i} = mult_{m_i}(\mathcal{C}.L_{m_i})_{m_i} = [(deg\mathcal{C}).(degL_{m_i})]_{m_i} = [5 \times 1]_{m_i} = 5m_i$ et $(\mathcal{C}.L_\infty)_\infty = 5\infty$.
$\mathcal{M}$ une quintique et $\begin{cases} m_i \in \mathcal{M}.\mathcal{C} \\ ord_{m_i}\mathcal{M}.\mathcal{C} \geq 6 \end{cases} \Rightarrow \begin{cases} \mathcal{M}\text{est redutible} \\ L_{m_i} \subset \mathcal{C} \end{cases}$
On déduit que $\mathcal{M} = \mathcal{C}_1 \cup L_{m_i}$.
Voir [Tz-98].

3.1.3 Démonstration du théorème

Soit $w \in \mathcal{C}(\overline{\mathbb{Q}})$ un point de la courbe tel que $[\mathbb{Q}(w) : \mathbb{Q}] = l$. Notons $w_1,...,w_l$ les conjugués de Galois de w et $[w_1 + ... + w_l - l\infty]$ qui est un point de $J(\mathbb{Q})$. On remarque que

$w \notin \left\{P_1,P_2,P_3,P_4,P_5,\infty\right\}$ et on a :

$$\begin{aligned}[w_1 + ... + w_l - l\infty] &= m_1 j(P_1) + m_2 j(P_2) + m_3 j(P_3) + m_4 j(P_4) \\ &= -m_1 j(P_1) - m_2 j(P_2) - m_3 j(P_3) - m_4 j(P_4)\end{aligned}$$

avec $m_i \in \{0,1\}$. Ce qui donne la relation

$$[w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i - (l + \sum_{i=1}^{4} m_i)\infty] = 0$$

Il existe alors une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que

$$div(f) = w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i - (l + \sum_{i=1}^{4} m_i)\infty \tag{3.1.1}$$

donc $f \in \mathcal{L}(l + \sum_{i=1}^{4} m_i)\infty$, et (3.1.1) montre que $f = P(x,y)$. Par la suite $\alpha = degP \leq E\left(\frac{l+4}{2}\right)$; et comme la droite $Z = 0$ coupe $\mathcal{C}$ en 5∞, on déduit qu'il existe alors une courbe $\mathcal{M}$ de degré α définie sur $\mathbb{Q}$. $\overline{f}(X,Y,Z) = Z^\alpha f(\frac{X}{Z},\frac{Y}{Z})$ donc $div(\overline{f}) = \alpha div(Z) + div(f)$
$div(\overline{f}) = w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i + (5\alpha - l - \sum_{i=1}^{4} m_i)\infty$. Par conséquent
$\mathcal{M}.\mathcal{C} = w_1 + ... + w_l + \sum_{i=1}^{4} m_i P_i + (5\alpha - l - \sum_{i=1}^{4} m_i)\infty$.

Les points algébriques sur $\mathcal{C}$ de degré 2 sur $\mathbb{Q}$:

La relation (3.1.1) donne $div(f) = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i - (2 + \sum_{i=1}^{4} m_i)\infty$ et $f = P(x,y)$ avec $degP = 2$ alors f définie une conique $\mathcal{M}$ sur $\mathbb{Q}$.
$\overline{f}(X,Y,Z) = Z^2 f(\frac{X}{Z},\frac{Y}{Z})$ donc $div(\overline{f}) = 2div(Z) + div(f)$ or $div(Z) = 5\infty$ d'où
$div(\overline{f}) = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (10 - 2 - \sum_{i=1}^{4} m_i)\infty$. Par conséquent

$$\mathcal{M}.\mathcal{C} = w_1 + w_2 + \sum_{i=1}^{4} m_i P_i + (8 - \sum_{i=1}^{4} m_i)\infty$$

$8 - m_1 - m_2 - m_3 - m_4 \leq 2$ avec $m_i \in \{0,1\}$ est impossible car $8 - m_1 - m_2 - m_3 - m_4 \geq 4$.

Supposons $8 - m_1 - m_2 - m_3 - m_4 \geq 3$, d'après le Lemme (3.1.3) $\mathcal{M}$ est alors réductible donc il existe une droite $\mathcal{C}_1$ tel que

$$\mathcal{C}_1.\mathcal{C} = w_1 + w_2 + m_1 P_1 + m_2 P_2 + m_3 P_3 + m_4 P_4 + (3 - m_1 - m_2 - m_3 - m_4)\infty$$

Les points algébriques sur $\mathcal{C}$ de degré 3 sur $\mathbb{Q}$:

La relation (3.1.1) donne $div(f) = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i - (3 + \sum_{i=1}^{4} m_i)\infty$ et $f = P(x,y)$ avec $degP = 3$ alors f définie une cubique $\mathcal{M}$ sur $\mathbb{Q}$.
$\overline{f}(X,Y,Z) = Z^3 f(\frac{X}{Z},\frac{Y}{Z})$ donc $div(\overline{f}) = 3div(Z) + div(f)$ or $div(Z) = 5\infty$ d'où
$div(\overline{f}) = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (15 - 3 - \sum_{i=1}^{4} m_i)\infty$. Par conséquent

$$\mathcal{M}.\mathcal{C} = w_1 + ... + w_3 + \sum_{i=1}^{4} m_i P_i + (12 - \sum_{i=1}^{4} m_i)\infty$$

$12 - m_1 - m_2 - m_3 - m_4 \leq 3$ avec $m_i \in \{0,1\}$ est impossible car $12 - m_1 - m_2 - m_3 - m_4 \geq 8$.

Supposons $12 - m_1 - m_2 - m_3 - m_4 \geq 4$, d'après le Lemme (3.1.3) $\mathcal{M}$ est alors réductible donc il existe une conique $\mathcal{C}_1$ tel que

$$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_3 + m_1P_1 + m_2P_2 + m_3P_3 + m_4P_4 + (7 - m_1 - m_2 - m_3 - m_4)\infty$$

$7 - m_1 - m_2 - m_3 - m_4 \leq 2$ avec $m_i \in \{0,1\}$ est impossible car $7 - m_1 - m_2 - m_3 - m_4 \geq 3$

Supposons $7 - m_1 - m_2 - m_3 - m_4 \geq 3$, d'après le Lemme (3.1.3) $\mathcal{C}_1$ est alors réductible donc il existe une droite $\mathcal{C}_2$ tel que

$$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_3 + m_1P_1 + m_2P_2 + m_3P_3 + m_4P_4 + (2 - m_1 - m_2 - m_3 - m_4)\infty$$

Les points algébriques sur $\mathcal{C}$ de degré 4 sur $\mathbb{Q}$:
La relation (3.1.1) donne $div(f) = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i - (4 + \sum_{i=1}^{4} m_i)\infty$ et $f = P(x,y)$ avec $degP = 4$ alors f définie une quartique $\mathcal{M}$ sur $\mathbb{Q}$.
$\overline{f}(X,Y,Z) = Z^4 f(\frac{X}{Z},\frac{Y}{Z})$ donc $div(\overline{f}) = 4div(Z) + div(f)$ or $div(Z) = 5\infty$ d'où
$div(\overline{f}) = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (20 - 4 - \sum_{i=1}^{4} m_i)\infty$ Par conséquent

$$\mathcal{M}.\mathcal{C} = w_1 + ... + w_4 + \sum_{i=1}^{4} m_i P_i + (16 - \sum_{i=1}^{4} m_i)\infty$$

$16 - m_1 - m_2 - m_3 - m_4 \leq 4$ avec $m_i \in \{0,1\}$ est impossible car $16 - m_1 - m_2 - m_3 - m_4 \geq 12$

Supposons $16 - m_1 - m_2 - m_3 - m_4 \geq 5$, d'après Lemme (3.1.3) $\mathcal{M}$ est alors réductible

donc il existe une cubique $\mathcal{C}_1$ tel que

$$\mathcal{C}_1.\mathcal{C} = w_1 + ... + w_4 + m_1P_1 + m_2P + m_3P_3 + m_4P_4 + (11 - m_1 - m_2 - m_3 - m_4)\infty$$

$11 - m_1 - m_2 - m_3 - m_4 \leq 3$ avec $m_i \in \{0,1\}$ est impossible car $11 - m_1 - m_2 - m_3 - m_4 \geq 7$

Supposons $11 - m_1 - m_2 - m_3 - m_4 \geq 4$, d'après Lemme (3.1.3) $\mathcal{C}_1$ est alors réductible donc il existe une conique $\mathcal{C}_2$ tel que

$$\mathcal{C}_2.\mathcal{C} = w_1 + ... + w_4 + m_1P_1 + m_2P + m_3P_3 + m_4P_4 + (6 - m_1 - m_2 - m_3 - m_4)\infty$$

Supposons $6 - m_1 - m_2 - m_3 - m_4 \leq 2$, on a $-m_1 - m_2 - m_3 - m_4 \geq -4$ donc $6 - m_1 - m_2 - m_3 - m_4 \geq$ alors $2 \leq 6 - m_1 - m_2 - m_3 - m_4 \leq 2$, ce qui est absurde.

Supposons $6 - m_1 - m_2 - m_3 - m_4 \geq 3$; d'après Lemme (3.1.3) $\mathcal{C}_2$ est alors réductible donc il existe une droite $\mathcal{C}_3$ tel que

$$\mathcal{C}_3.\mathcal{C} = w_1 + ... + w_4 + m_1P_1 + m_2P + m_3P_3 + m_4P_4 + (1 - m_1 - m_2 - m_3 - m_4)\infty$$

3.2 Points algébriques de degrés quelconques sur la courbe d'équation affine $y^{11} = x^3(x-1)^3$

3.2.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique définie sur un corps de nombres $\mathbb{K}$. On étudie en détail les points algébriques de degré quelconque donnée sur $\mathbb{Q}$ sur la courbe $\mathcal{C}_3(11)$ d'équation affine
$y^{11} = x^3(x-1)^3$. $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 3} \mathcal{C}_3(11)(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}_3(11)$ de degré au-plus 3 sur $\mathbb{Q}$ est étudié dans le **chapitre 2**. Nous allons étendre ce travail en déterminant l'ensemble de ces points algébriques sur $\mathcal{C}_3(11)$ de degré quelconque l donné sur $\mathbb{Q}$.
Le résultat s'énonce comme suit :

Théorème 4
L'ensemble des points algébriques de degré $l \geq 9$ sur $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$ est donné par :

$$\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}_3(11)(\mathbb{K}) = \mathcal{F}_0 \bigcup \left(\bigcup_{k=1}^{10} \mathcal{F}_k \right) \text{ avec}$$

$$\mathcal{F}_0 = \left\{ \begin{array}{c} \left(- \dfrac{\sum\limits_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}}}{\sum\limits_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}}}, y \right) \Bigg| a_0 \neq 0, a_{\frac{l}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-11}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et y racine de l'équation} \\ y^{11} \Big(\sum\limits_{j\leq \frac{l-11}{2}} b_j y^j \Big)^2 = \Big(\sum\limits_{i\leq \frac{l}{2}} a_i y^i \Big) \Big(\sum\limits_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}} + \sum\limits_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}} \Big)^3 \end{array} \right\}$$

$$\mathcal{F}_k = \left\{ \begin{array}{c} \left(- \dfrac{\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}}}{\sum\limits_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}}}, y \right) \Bigg| b_0 \neq 0, a_{\frac{l+11-k}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-k}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et y racine de l'équation} \\ y^k \Big(\sum\limits_{j\leq \frac{l-k}{2}} b_j y^j \Big)^2 = \Big(\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{i-(11-k)} \Big) \Big(\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}} + \sum\limits_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}} \Big)^3 \end{array} \right\}$$

3.2.2 Résultats auxiliaires

Lemme 3.2.1.
Une $\mathbb{Q}-$base de $\mathcal{L}(lP_\infty)$ est donnée par :

$$\mathcal{B} = \left\{ \left(\frac{x^2(x-1)^2}{y^7} \right)^i \mid i \in \mathbb{N}, i \leq \frac{l}{2} \right\} \bigcup \left\{ x \left(\frac{x^2(x-1)^2}{y^7} \right)^j \mid j \in \mathbb{N}, j \leq \frac{l-11}{2} \right\}$$

Preuve 3.2.1.
Il est clair $\mathcal{B}$ est libre. Il reste à montrer que $dim(\mathcal{B}) = dim(\mathcal{L}(lP_\infty))$.
D'après le théorème de Riemann-Roch, on a $dim(\mathcal{L}(lP_\infty)) = l - g + 1$ dès que $l \geq 2g - 1$ avec $g = \frac{11-1}{2}$
Considérons les cas suivants :
cas 1 : supposons que l est pair, et posons $l = 2h$. On a alors $i \leq \frac{l}{2} = h$ et $j \leq \frac{l-11}{2} \Leftrightarrow j \leq \frac{2h-11}{2} \Leftrightarrow j \leq \frac{2h-11-1}{2} = h - 6 = h - g - 1$.
Donc on obtient $\mathcal{B} = \left\{ 1, \frac{x^2(x-1)^2}{y^7}, ..., \left(\frac{x^2(x-1)^2}{y^7} \right)^h \right\} \cup \left\{ x, x\frac{x^2(x-1)^2}{y^7}, ..., x\left(\frac{x^2(x-1)^2}{y^7} \right)^{h-g-1} \right\}$,
et par conséquent $dim(\mathcal{B}) = (h+1) + (h-g) = 2h - g + 1 = l - g + 1 = dim(\mathcal{L}(lP_\infty))$
cas 2 : supposons que l est impair, et posons $l = 2h + 1$. On a alors $i \leq \frac{l}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h$ et $j \leq \frac{l-11}{2} \Leftrightarrow j \leq \frac{2h-10}{2} = h - g$

Donc on obtient $\mathcal{B} = \left\{1,\frac{x^2(x-1)^2}{y^7},...,\left(\frac{x^2(x-1)^2}{y^7}\right)^h\right\} \cup \left\{x,x\frac{x^2(x-1)^2}{y^7},...,x\left(\frac{x^2(x-1)^2}{y^7}\right)^{h-g}\right\}$, et par conséquent $dim(\mathcal{B}) = (h+1)+(h-g+1) = 2h+1-g+1 = l-g+1 = dim(\mathcal{L}(lP_\infty))$

3.2.3 Démonstration du théorème

Soit $R \in \mathcal{C}_3(11)(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R):\mathbb{Q}] = l$. Notons R_1,...,R_l les conjugués de Galois de R, et posons $t = [R_1 + ... + R_l - lP_\infty]$ qui est un point de $J(\mathbb{Q}) = \left\{mj(P_0), 0 \leq m \leq 10\right\}$; donc $t = mj(P_0)$ avec $0 \leq m \leq 10$. Ce qui donne la relation

$$[R_1 + ... + R_l - lP_\infty] = mj(P_0). \tag{3.2.1}$$

On remarque que $R \notin \left\{P_0,P_1,P_\infty\right\}$.

Cas $m = 0$

Il existe alors une fonction rationnelle f à coefficients dans $\mathbb{Q}$ telle que $div(f) = R_1 + ... + R_l - lP_\infty$, donc $f \in \mathcal{L}(lP_\infty)$. D'après le Lemme (3.2.1) , on a
$f = \sum_{i\leq\frac{l}{2}} a_i\left(\frac{x^2(x-1)^2}{y^7}\right)^i + x\sum_{j\leq\frac{l-11}{2}} b_j\left(\frac{x^2(x-1)^2}{y^7}\right)^j$ avec $a_{\frac{l}{2}} \neq 0$ si l est pair (sinon les R_i seraient égaux à P_∞) et $b_{\frac{l-11}{2}} \neq 0$ si l est impair (sinon les R_i seraient égaux à P_∞). Aux points R_i on a $\sum_{i\leq\frac{l}{2}} a_i\left(\frac{x^2(x-1)^2}{y^7}\right)^i + x\sum_{j\leq\frac{l-11}{2}} b_j\left(\frac{x^2(x-1)^2}{y^7}\right)^j = 0$ d'où
$x = -\dfrac{\sum_{i\leq\frac{l}{2}} a_i\left(\frac{x^2(x-1)^2}{y^7}\right)^i}{\sum_{j\leq\frac{l-11}{2}} b_j\left(\frac{x^2(x-1)^2}{y^7}\right)^j}$ et par suite $y^{11} = x^3(x-1)^3 \Leftrightarrow y^{\frac{1}{3}} = \frac{x^2(x-1)^2}{y^7}$, ainsi
$x = -\dfrac{\sum_{i\leq\frac{l}{2}} a_i y^{\frac{i}{3}}}{\sum_{j\leq\frac{l-11}{2}} b_j y^{\frac{j}{3}}}$.
Donc l'équation $y^{11} = x^3(x-1)^3$ devient
$y^{11}\left(\sum_{j\leq\frac{l-11}{2}} b_j y^j\right)^2 = \left(\sum_{i\leq\frac{l}{2}} a_i y^i\right)\left(\sum_{i\leq\frac{l}{2}} a_i y^{\frac{i}{3}} + \sum_{j\leq\frac{l-11}{2}} b_j y^{\frac{j}{3}}\right)^3$ qui est une équation de degré l en y.

On trouve ainsi une famille de points de degré l

$$\mathcal{F}_0 = \left\{ \left(-\frac{\sum_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}}}{\sum_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}}}, y \right) \middle| a_0 \neq 0, a_{\frac{l}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-11}{2}} \neq 0 \ \textbf{si l est impair} \right.$$
$$\left. \textbf{et y racine de l'équation} \quad y^{11}\left(\sum_{j\leq \frac{l-11}{2}} b_j y^j\right)^2 = \left(\sum_{i\leq \frac{l}{2}} a_i y^i\right)\left(\sum_{i\leq \frac{l}{2}} a_i y^{\frac{i}{3}} + \sum_{j\leq \frac{l-11}{2}} b_j y^{\frac{j}{3}}\right)^3 \right\}$$

Cas $m = k$ avec $k \in \{1,...,10\}$, la relation (3.2.1) donne $[R_1 + ... + R_l - lP_\infty] = kj(P_0) = (k-11)j(P_0)$. Il existe alors une fonction rationnelle f telle que $div(f) = R_1 + ... + R_l + (11-k)P_0 - (l+11-k)P_\infty$, donc $f \in \mathcal{L}[(l+11-k)P_\infty]$. D'après le Lemme (3.2.1) , on a

$f = \sum_{i\leq \frac{l+11-k}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j\leq \frac{l-k}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j$; et comme $ordf_{P_0} = 11-k$, donc

$f = \sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j\leq \frac{l-k}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j$ avec $a_{\frac{l+11-k}{2}} \neq 0$ si l est pair (sinon les R_i seraient égaux à P_∞) et $b_{\frac{l-k}{2}} \neq 0$ si l est impair (sinon les R_i seraient égaux à P_∞).

Aux points R_i on a $\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j\leq \frac{l-k}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j = 0$

d'où $x = -\frac{\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i}{\sum_{j\leq \frac{l-k}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j}$ et par suite $x = -\frac{\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}}}{\sum_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}}}$.

Donc l'équation $y^{11} = x^3(x-1)^3$ devient

$y^k\left(\sum_{j\leq \frac{l-k}{2}} b_j y^j\right)^2 = \left(\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{i-(11-k)}\right)\left(\sum_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}} + \sum_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}}\right)^3$ qui est une équation de degré l en y.

On trouve ainsi une famille de points de degré l

$$\mathcal{F}_k = \left\{ \begin{array}{c} \left(-\dfrac{\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}}}{\sum\limits_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}}}, y \right) \Bigg| b_0 \neq 0, a_{\frac{l+11-k}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-k}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et y racine de l'équation} \\ y^k \Big(\sum\limits_{j\leq \frac{l-k}{2}} b_j y^j \Big)^2 = \Big(\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{i-(11-k)} \Big) \Big(\sum\limits_{11-k\leq i\leq \frac{l+11-k}{2}} a_i y^{\frac{i}{3}} + \sum\limits_{j\leq \frac{l-k}{2}} b_j y^{\frac{j}{3}} \Big)^3 \end{array} \right\}$$

3.3 Points algébriques de degrés quelconques sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$

3.3.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique projective définie sur $\mathbb{Q}$. Pour tout corps de nombres $\mathbb{K}$, On note $\mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$ et $\bigcup\limits_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ de degré au plus l donnée sur $\mathbb{Q}$. Le degré d'un point algébrique R est le degré de son corps de définition sur $\mathbb{Q}$, i.e, $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera J la jacobienne de $\mathcal{C}$ et $j(P)$ la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

$$\begin{array}{ccc} j : \mathcal{C}(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ P & \longmapsto & [P - P_\infty] \end{array}$$

où $J(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (voir [Br-Fl-06],page 287).

Notre courbe $\mathcal{C}$ qui est lisse d'équation affine $y^2 = x^3 - 8x^2 + x$ est un cas spécial de famille de courbes $\mathcal{C}_i : y^2 = (x - e_1)(x - e_2)(x - e_3)$ étudiées dans (voir [Ku-98],page 107). Elle a pour équation projective $ZY^2 = X\Big(X - (4 - \sqrt{15})Z\Big)\Big(X - (4 + \sqrt{15})Z\Big)$, on note P_0, P_1,P_2 et P_∞ les points de $\mathcal{C}$ définis par : $P_0 = (0 : 0 : 1)$, $P_1 = (4 - \sqrt{15} : 0 : 1)$, $P_2 = (4 + \sqrt{15} : 0 : 1)$ et $P_\infty = (0 : 1 : 0)$.

Théorème 5 L'ensemble des points algébriques de degré au plus l sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\bigcup_{[\mathbb{Q}(R):\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K}) = \mathcal{F}_1 \bigcup \mathcal{F}_2$$

avec

$$\mathcal{F}_1 = \left\{ \begin{array}{c} \left(x, -\dfrac{\sum\limits_{i=0}^{\frac{l}{2}} a_i x^i}{\sum\limits_{j=0}^{\frac{l-3}{2}} b_j x^j} \right) \Bigg| (a_0 \wedge b_0) \neq 0, a_{\frac{l}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-3}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et x solution de l'équation :} \\ \left(\sum\limits_{i=0}^{\frac{l}{2}} a_i x^i \right)^2 = \left(\sum\limits_{j=0}^{\frac{l-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \end{array} \right\}$$

$$\mathcal{F}_2 = \left\{ \begin{array}{c} \left(x, -\dfrac{\sum\limits_{i=1}^{\frac{l+1}{2}} a_i x^i}{\sum\limits_{j=0}^{\frac{l-2}{2}} b_j x^j} \right) \Bigg| b_0 \neq 0, a_{\frac{l+1}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-2}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et x solution de l'équation :} \\ \left(\sum\limits_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum\limits_{j=0}^{\frac{l-2}{2}} b_j x^j \right)^2 \left(x - (4-\sqrt{15}) \right) \left(x - (4-\sqrt{15}) \right) \end{array} \right\}$$

3.3.2 Résultats auxiliaires

Pour tout diviseur D sur $\mathcal{C}$, on note $\mathcal{L}(D)$ le $\overline{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles f définies sur $\mathbb{Q}$ telles que $f = 0$ ou $dif(f) \geq -D$ et $l(D)$ désigne la $\overline{\mathbb{Q}}$-dimension de $\mathcal{L}(D)$.

Lemme 3.3.1. $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})$

Preuve 3.3.1. (voir [Br-Fl-06],page 272)

Lemme 3.3.2. $\mathcal{C} : y^2 = x^3 - 8x^2 + x$
$div(x) = 2P_0 - 2P_\infty$; $div(x - (4-\sqrt{15})) = 2P_1 - 2P_\infty$; $div(x - (4+\sqrt{15})) = 2P_2 - 2P_\infty$; $div(y) = P_0 + P_1 + P_2 - 3P_\infty$.

Preuve 3.3.2. Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par : $x(X,Y,Z) = \frac{X}{Z}$ et $y(X,Y,Z) = \frac{Y}{Z}$.
$ZY^2 = X(X - (4-\sqrt{15}Z)(X - (4+\sqrt{15})Z)$ est l'équation projective de la courbe $\mathcal{C}$. on a $div(x) = (X = 0).\mathcal{C} - (Z = 0).\mathcal{C}$:
Pour $X = 0$, l'équation projective donne $Y^2Z = 0$; et pour $Z = 1$, on obtient le point $P_0 = (0 : 0 : 1)$ de multiplicité égale à 2. Ainsi $(X = 0).\mathcal{C} = 2P_0 + \infty$.
Pour $Z = 0$, l'équation projective donne donne $X^3 = 0$; et pour $Y = 1$, on obtient le point $P_\infty = (0 : 1 : 0)$ de multiplicité égale à 3. Ainsi $(Z = 0).\mathcal{C} = 3\infty$.
Donc $div(x) = 2P_0 + \infty - 3\infty$ d'où $div(x) = 2P_0 - 2P_\infty$.
Pour $X = 4 - \sqrt{15}$, l'équation projective donne $Y^2Z = 0$; et pour $Z = 1$, on obtient le

point $P_1 = (4-\sqrt{15} : 0 : 1)$ de multiplicité égale à 2. Ainsi $(X = 0).\mathcal{C} = 2P_1 + \infty$.
Pour $Z = 0$, l'équation projective donne donne $X^3 = 0$; et pour $Y = 1$, on obtient le point $P_\infty = (0 : 1 : 0)$ de multiplicité égale à 3. Ainsi $(Z = 0).\mathcal{C} = 3\infty$. Donc $div(x-(4-\sqrt{15})) = 2P_1 + \infty - 3\infty$ d'où $div(x-(4-\sqrt{15})) = 2P_1 - 2P_\infty$.
De la même manière, on montre que $div(x-(4+\sqrt{15})) = 2P_2 - 2P_\infty$ et $div(y) = P_0 + P_1 + P_2 - 3P_\infty$

Conséquences 3.3.1.
i) $2j(P_0) = 2j(P_1) = 2j(P_2) = 0$;
$j(P_0) + j(P_1) + j(P_2) = 0$

Lemme 3.3.3.
$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \cong \{j(P_0)\}$

Lemme 3.3.4.
Une $\mathbb{Q}-$base de $\mathcal{L}(mP_\infty)$ est donnée par :

$$\mathcal{B}_m = \left\{x^i \mid 0 \leq i \leq \frac{m}{2}\right\} \bigcup \left\{yx^j \mid 0 \leq j \leq \frac{m-3}{2}\right\}$$

Preuve 3.3.3. $\mathcal{B}_m$ est libre. Il reste à montrer que $dim(\mathcal{B}_m) = dim(\mathcal{L}(mP_\infty))$.
D'après le théorème de Riemann-Roch, on a $dim(\mathcal{L}(mP_\infty)) = m - g + 1$ dès que $m \geq 2g-1$ avec $g = 1$
Considérons les cas suivants :
cas 1 : supposons que m est pair, et posons $m = 2h$. On a alors
$i \leq \frac{m}{2} = h$ et $j \leq \frac{m-3}{2} \Leftrightarrow j \leq \frac{2h-3}{2}$.
Or : $\frac{2h-3-1}{2} = h-2$ et $\frac{2h-3+1}{2} = h-1$ donc $j \leq h-1 \Leftrightarrow j \leq h-2 = h-g-1$.
Donc on obtient $\mathcal{B}_m = \left\{1,x,...,x^h\right\} \cup \left\{y,yx,...,yx^{h-2}\right\}$, et par conséquent
$dim(\mathcal{B}_m) = (h+1) + (h-2+1) = 2h = m - g + 1 = dim(\mathcal{L}(mP_\infty)$
cas 2 : supposons que m est impair, et posons $m = 2h+1$. On a alors
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h$ et $j \leq \frac{m-3}{2} \Leftrightarrow j \leq \frac{2h-4}{2} = h-g$
Donc on obtient $\mathcal{B}_m = \left\{1,x,...,x^h\right\} \cup \left\{y,yx,...,yx^{h-g}\right\}$, et par conséquent
$dim(\mathcal{B}_m) = (h+1) + (h-g+1) = 2h+1-g+1 = m-g+1 = dim(\mathcal{L}(p\infty))$
□

3.3.3 Démonstration du théorème

Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = l$. Notons $R_1,...,R_l$ les conjugués de Galois de R, et posons $t = [R_1 + ... + R_l - lP_\infty]$ qui est un point de $J(\mathbb{Q}) = \left\{\alpha j(P_0), 0 \leq \alpha \leq 1\right\}$; donc $t = \alpha j(P_0)$ avec $0 \leq \alpha \leq 1$. Ce qui donne la relation

$$[R_1 + ... + R_l - lP_\infty] = \alpha j(P_0). \tag{3.3.1}$$

On remarque que $R \notin \left\{P_0,P_1,P_2,P_\infty\right\}$.

Cas $\alpha = 0$

Il existe alors une fonction rationnelle f telle que $div(f) = R_1 + ... + R_l - lP_\infty$, donc $f \in \mathcal{L}(lP_\infty)$. D'après le Lemme (3.3.4), on a

$f = \sum_{i=0}^{\frac{l}{2}} a_i x^i + y \sum_{j=0}^{\frac{l-3}{2}} b_j x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde), $a_{\frac{l}{2}} \neq 0$ si l est pair (sinon les R_i seraient égaux à P_∞) et $b_{\frac{l-3}{2}} \neq 0$ si l est impair (sinon les R_i seraient égaux à P_∞).

Aux points R_i, on a $\sum_{i=0}^{\frac{l}{2}} a_i x^i + y \sum_{j=0}^{\frac{l-3}{2}} b_j x^j = 0$ d'où $y = -\dfrac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j}$ et par suite $y^2 = x^3 - 8x^2 + x$, ainsi l'équation devient $\left(\sum_{i=0}^{\frac{l}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$ qui est une équation de degré l en x.

On obtient ainsi une famille de points de degré l

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j} \right) \middle| (a_0 \wedge b_0) \neq 0, a_{\frac{l}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-3}{2}} \neq 0 \ \textbf{si l est impair} \right.$$
$$\left. \textbf{et x solution de l'équation :} \quad \left(\sum_{i=0}^{\frac{l}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right) \right\}$$

Cas $\alpha = 1$

la relation (3.3.1) donne

$[R_1 + ... + R_l - lP_\infty] = j(P_0) = (2-1)j(P_0) = 2j(P_0) - j(P_0) = -j(P_0)$

Il existe alors une fonction rationnelle f telle que $div(f) = R_1 + ... + R_l + P_0 - (l+1)P_\infty$, donc $f \in \mathcal{L}(l+1)P_\infty$. D'après le Lemme (3.3.4), on a

$f = \sum_{i=0}^{\frac{l+1}{2}} a_i x^i + y \sum_{j=0}^{\frac{l-2}{2}} b_j x^j$; et comme $ordf_{P_0} = 1$, on doit avoir $a_0 = 0$ et $f = \sum_{i=1}^{\frac{l+1}{2}} a_i x^i + y \sum_{j=0}^{\frac{l-2}{2}} b_j x^j$ avec b_0 non nuls (sinon un des R_i devrait être égal à P_0), $a_{\frac{l+1}{2}} \neq 0$ si l est pair (sinon les R_i seraient égaux à P_∞) et $b_{\frac{l-2}{2}} \neq 0$ si l est impair (sinon les R_i seraient égaux à P_∞).

Aux points R_i, on a $\sum_{i=1}^{\frac{l+1}{2}} a_i x^i + y \sum_{j=0}^{\frac{l-2}{2}} b_j x^j = 0$ d'où $y = -\dfrac{\sum_{i=1}^{\frac{l+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-2}{2}} b_j x^j}$ et par suite $y^2 = x^3 - 8x^2 + x$, ainsi l'équation devient $\left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^i\right)^2 = x\left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4-\sqrt{15})\right)$

$\left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4-\sqrt{15})\right)$ qui est une équation de degré l en x.

On obtient ainsi une famille de points de degré l

$$\mathcal{F}_2 = \left\{ \begin{array}{c} \left(x, -\dfrac{\sum_{i=1}^{\frac{l+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-2}{2}} b_j x^j} \right) \Bigg| b_0 \neq 0, a_{\frac{l+1}{2}} \neq 0 \ \textbf{si l est pair}, \ b_{\frac{l-2}{2}} \neq 0 \ \textbf{si l est impair} \\ \textbf{et x solution de l'équation :} \\ \left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4-\sqrt{15})\right) \end{array} \right\}$$

Conclusion et persperctives

Dans ce mémoire de Thèse, nous avons donné une détermination explicite des points algébriques de petit degré sur $\mathbb{Q}$ et une paramétrisation de points algébriques de degré donné sur $\mathbb{Q}$ sur les courbes d'équations affines $y^2 = x(x-3)(x-4)(x-6)(x-7)$ et $y^{11} = x^3(x-1)^3$.
Notre étude résulte des travaux de Gross-Rohrlich dans [Gr-Ro-78] et de Daniel M.Gordon-David Grant dans ([Go-Gr-93],p.822) qui ont déterminé le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ qui est fini.
La connaissance préalable du groupe de Mordell-Weil de la variété jacobienne J de $\mathcal{C}$ et la condition qu'il soit fini est indispensable pour la méthode utilisée dans ces travaux car elle nous permet d'utiliser le théorème d'Abel-Jacobi pour plonger la courbe dans sa jacobienne et étudier des systèmes linéaires sur les courbes.
La description de ces points est "très explicite" en petit degré ($l \leq 3$),"moins explicite" pour l grand mais reste intéressante en degré quelconque. Cette finitude de $J(\mathbb{Q})$ nous a permis de déterminer explicitement dans le chapitre 2 tous les points algébriques de degré au plus 3 sur certaines courbes, puis dans le chapitre 3 de donner une paramétrisation de tous les points algébriques de degré l quelconque donné sur certaines courbes. On peut citer comme perspectives :
• La détermination des points algébriques de degré exactement l donné sur une courbe. En effet à part les points algébriques de petits degrés ($l \leq 3$), beaucoup de travaux portent sur la détermination de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathbb{Q}$ de degré au plus l.
• La détermination des points algébriques avec le groupe de Mordell-Weil de la jacobienne J de la courbe qui n'est pas fini.

Bibliographie

[Ba-Di-Sa-22] B.S.Balde,M.D.Diallo,O.Sall,Algebraic Points of Any Degree l with $(l \geq 9)$over $\mathbb{Q}$ on the Affine Equation Curve $C_3(11) : y^{11} = x^3(x-1)^3$, Advances in Pure Mathematics,(2022),12, 519-525.

[Br-Fl-06] Bruin N and Flynn E.V : Exhibiting SHA[2] on hyperelliptic Jacobians, Journal of Number Theory 118(2006)266-291.

[De-Kl-94] O.Debarre, M.Klassen, Points of low degree on smooth plane curves, J. Reine Angew. Math. 446 (1994) 81-87.

[Di-Ba-Sa-22] M.D.Diallo, B.Balde, O.Sall, Points algébriques de degrés quelconques sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$. International Journal of Development Research Vol. 12, Issue, 01, pp. 53106-53110, January, 2022.

[Fa-61] D.Faddeev, on the divisor class groups of some algebraic curves, Dokl. Akad. Nauk SSSR 136 (1961) 296-298.

[Go-Gr-93] D. M.Gordon and D.Grant, computing the Mordell-Weil rank of Jacobians of curves of genus two. transactions of the american mathematical society. Volume 337, Number 2, June 1993.

[Gri-89] Griffiths, P. A.Introduction to algebraic curves. In : Translations of mathematical monographs, vol. 76.American Mathematical Society, Providence, RI (1989).

[Gr-Ro-78] B.Gross and D.Rohrlich, some results on the Mordell-Weil of the Jacobian of the Fermat curve, Invent. Math. 44 (1978) 201-224.

[Ku-98] Kulesz L : Courbes algébriques de genre ≥ 2 possédant de nombreux points rationnels, Acta Arithmetica LXXXVII.2(1998)103-120.

[Sa-03] O.Sall, Points algébriques sur certains quotients de courbes de Fermat,C.R. Acad. Sci. Paris Ser. I 336 (2003) 117-120.

[Sa-To-Fa-10] O.Sall, T.Top, M.Fall, Paramétrisation des points algébriques de degré donné sur la courbe d'équation affine $y^3 = x(x-1)(x-2)(x-3)$ .C. R. Acad. Sci.Paris Sér I 348 (2010) 1147-1150.

[Sc-98] E.F.Schaefer, computing a Selmer group of Jacobian usin functions on the curve. Math. Ann.310, 447–471.(1998).

[Tz-98] P.Tzermias : Algebraic points of low degree on the Fermat curve of degree seven, Manuscripta Mathematica. Vol. 97, Fasc. 4(1998), 483-488.