UNIVERSITE ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES
Département de Mathématiques

THESE DE DOCTORAT

Spécialité : Mathématiques Pures

Pour l'obtention du grade de docteur de :

UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

Sujet :

Détermination des points algébriques de degré donné quelconque sur certaines courbes

Soutenue le 17 Décembre 2022
par :
MOHAMADOU MOR DIOGOU DIALLO

Sous la direction du
Professeur OUMAR SALL

Soutenue publiquement devant le jury :

Qualité	Nom et prénom	Grade	Établissement
Président	SAMBOU Marie Salomon	Professeur titulaire	Université Assane SECK de Ziguinchor
Rapporteurs	SAMBOU Marie Salomon	Professeur titulaire	Université Assane SECK de Ziguinchor
	MAAOUIA Mohamed Ben Faraj	Professeur titulaire	Université Gaston Berger de Saint-Luis
	DIAGANA Youssouf	Professeur titulaire	Université Nangui Abrogoua (Côte d'Ivoire)
Examinateur	DIATTA Douda Niang	Maître de conférences titulaire	Université Assane SECK de Ziguinchor
Directeur	SALL Oumar	Professeur titulaire	Université Assane SECK de Ziguinchor

année Universitaire : 2021 - 2021

Remerciements

Je souhaite dans un premier temps exprimer mes sincères remerciements envers mon directeur de thèse le professeur Oumar SALL. La thèse est une aventure et monsieur SALL m'a toujours soutenu durant ces années et m'a initié à un monde mathématique riche et très ouvert. J'ai appris beaucoup à ses côtés. Son optimisme m'a permis de voir les mathématiques sous un autre regard. Je suis certain que cette expérience à ses côtés me sera utile pour le reste de ma carrière.

Je voudrais remercier les professeurs Marie Salomon SAMBOU, Mouhamed Ben Faraj MAAOUIA et Yousouf DIAGANA pour avoir accepté d'être les rapporteurs de cette thèse. Leur lecture attentive a permis d'améliorer la qualité de ce manuscrit. Je remercie également au professeur Daouda Niang DIATTA de faire partie de mon jury de thèse.

Mes remerciements vont à ces personnes dont la qualité humaine est des meilleurs, notamment le professeur Édouard DIOUF directeur de l'UFR sciences et technologies (UASZ) ainsi que les professeurs Mansour SANÉ et Moussa FALL du département de mathématiques (UASZ) qui m'a été d'un grand apport sur cette expérience et sans oublier le professeur Mamadou SARR de l'université Sherbrooke (Canada), ainsi que mon chef d'établissement le proviseur Ibou BADJI qui m'a apporté un grand aide lors de la reproduction de ce document et tout le personnel du lycee kénia de Ziguinchor et surtout Madame Ramatoulaye DIALLO secretaire rattachée du recteur de l'UASZ.

La dernière partie des remerciements revient à mes proches et ma famille, notamment à mes parents, ma grande sœur Rabiyatou et petite sœur Jeynab, ainsi que mon frère Youssouph qui m'ont soutenu en toutes circonstances. Je sais que je dois énormément à l'éducation que ma famille m'a transmise et aux encouragements dans toutes les étapes importantes de ma vie.

Enfin, je remercie mes amis qui m'ont encouragé et m'ont permis de ne jamais abandonner tout le long de ce parcours.

Je dédie cette thèse à mon très bien aimé neveu qui est spécial
pour moi et toute notre famille, Mohamadou Adama Eric
Khar DIALLO, pour qui je prie qu'ALLAH lui octroie
une longue vie, pleine de succès, de santé
et enveloppée de bonheur.....

Détermination des points algébriques de degré donné quelconque sur certaines courbes.

Résumé de la thèse

La géométrie algébrique a connu un grand développement dans les années 50 par les travaux de l'école française sous l'impulsion de Pierre Samuel, Henri Cartan, Jean-Pierre Serre et d'Alexandre Grothendieck. En une décennie, elle se développa, répondant à des questions classiques sur la géométrie des variétés algébriques. Des applications furent très vite trouvées en théorie des nombres. De nos jours la géométrie algébrique est l'un des domaines fondamentaux et un outil indispensable dans de nombreuses parties des mathématiques. Cette thèse traite des questions de géométrie algébrique et de la théorie des nombres. L'étude porte essentiellement sur les méthodes permettant de déterminer la famille de points algébriques de degré donné quelconque sur certaines courbes en particulier lisses. Ces questions intéressent beaucoup de mathématiciens, et en particulier, des géomètres algébristes. Pourtant les résultats obtenus sont souvent qualitatifs, non explicites et réduits aux points rationnels. Dans cette thèse, nous déterminons de manière explicite l'ensemble des points algébrique de degrés ℓ quelconques sur certaines courbes. L'essentiel des résultats obtenus dans cette thèse complètent et/ou étendent des travaux d'autres mathématiciens dont : Nil Bruin & E.Victor Flynn [1], Anna ARNTH-JENSEN & E. Victor FLYNN [6], Nil BRUIN [13] et Benedict H. Gross & David E. Rohrlich [3].

Mots-clés : Groupe de Mordell-Weil, jacobienne d'une courbe, conjugués de Galois.
Classification Mathématiques AMS 2020 : 14L40, 14H40, 14C20.

Summary of the thesis

Algebraic geometry underwent a great development in the 1950s through the work of the French school under the impulse of Pierre Samuel, Henri Cartan, Jean-Pierre Serre and Alexandre Grothendieck. Within a decade, it developed, answering classical questions on the geometry of algebraic varieties. Applications were soon found in number theory. Nowadays algebraic geometry is one of the fundamental fields and an indispensable tool in many parts of mathematics. This thesis deals with issues of algebraic geometry and number theory. The study focuses on methods for determining the family of algebraic points of any given degree on certain curves, in particular smooth curves. These questions interest many mathematicians, and in particular, algebraic geometers. However, the results obtained are often qualitative, not explicit and reduced to rational points. In this thesis we explicitly determine the set of algebraic points of any degree ℓ on certain curves. Most of the results obtained in this thesis complement and/or extend the work of other mathematicians including : Nil Bruin & E.Victor Flynn [1], Anna ARNTH-JENSEN & E. Victor FLYNN [6], Nil BRUIN [13] and Benedict H. Gross & David E. Rohrlich [3].

Key words : Mordell-Weil Group, Jacobian, Linear system.
AMS 2020 Mathematics Subject Classification : 14L40, 14H40, 14C20.

Table des matières

Introduction

La géométrie algébrique est l'étude des ensembles algébriques, définis comme des ensembles des zéros d'un ou de plusieurs polynômes. Un cas particulièrement intéressant est celui des variétés algébriques. L'origine de cette fascinante branche des mathématiques remonte à Descartes et à de nombreux autres mathématiciens dont Abel, Riemann, Poincaré, Hilbert.
Après les années 1930, les mathématiciens Weil, Zariski, Chevalley, Brauer se sont illustrés par leur apport remarquable. Il y a eu un grand essor de cette branche sous l'impulsion de Pierre Samuel, d'Henri Cartan, de Jean-Pierre Serre et d'Alexandre Grothendieck. Aujourd'hui, la géométrie algébrique est considérée comme l'une des disciplines fondamentales non seulement pour elle-même mais aussi pour de nombreux domaines des mathématiques.
Soit $\mathcal{C}$ une courbe algébrique lisse définie sur $\mathbb{Q}$. Soit $\mathbb{K}$ un corps de nombres ; on note $\mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[K:\mathbb{Q}]\leq \ell} \mathcal{C}(K)$ l'ensemble des points de $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré sur $\mathbb{Q}$ d'un point algébrique R de $\mathcal{C}$ est défini comme étant le degré de son corps de définition sur $\mathbb{Q}$; c'est-à-dire $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Cette thèse s'inspire largement des travaux de certains géomètres algébristes dont :

- Gross et Rohrlich [3] qui ont déterminé l'ensemble des points rationnels sur $\mathbb{Q}$ sur la courbe d'équation affine $y^{11} = x(x - 1)$.
- E.F. Schaefer qui donne dans [9] la description de l'ensemble des points algébriques de degré au-plus 2 sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = x^5 + 1$.

La thèse comprend trois grands chapitres structurés de la manière suivante :

a) Le chapitre 1 intitulé ˝Notions de base ˝est constitué de définitions et résultats classiques.

b) Au chapitre 2 intitulé ˝Points algébriques de degré donné quelconque sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$ ˝, on donne une description explicite de l'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$.

Le théorème principal de ce travail, publié dans [8], s'énonce comme suit :

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

$$\mathcal{F}_\ell = \mathcal{F}'_\ell \bigcup \mathcal{F}''_\ell$$

avec

$$\mathcal{F}'_\ell = \left\{ \left(x, \ -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls }, \ a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est impair et} \\ x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \end{array} \right\}$$

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

c) Au dernier chapitre intitulé ˝Points algébriques de degré quelconque sur certaines courbes lisses ˝, on explicite les points algébriques de degré quelconque sur quelques courbes planes et lisses dont le groupe de Mordell-Weil des points

rationnels de la jacobienne est fini et est donné dans leurs références.
Nos résultats sont illustrés par les théorèmes suivants :

i) **Théorème 1**

L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ est donné par :

$$\mathcal{S} = \mathcal{S}_1 \bigcup \mathcal{S}_2 \bigcup \mathcal{S}_3 \bigcup \mathcal{S}_4$$

avec :

$$\mathcal{S}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}}}{\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_0 \text{ et } c_0 \text{ non simultanément nuls,} \\ b_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-7}{2}} \neq 0 \text{ si} \\ \ell \text{ est impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}}\right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \end{array} \right\}$$

$$\mathcal{S}_2 = \left\{ \left(x, -\frac{a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \\ \text{est impair et } x \text{ solution de} \\ \text{l'équation :} \\ \left(a\left(\frac{x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}}{x}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(\frac{x^i + (-1)^i}{x}\right)\right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \end{array} \right\}$$

$$\mathcal{S}_3 = \left\{ \begin{array}{l} \left(\begin{array}{c} x,\ -\dfrac{a\left(x^{\frac{5}{2}}+\psi\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\omega^i\right)}{\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \end{array} \right) \left| \begin{array}{l} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \left(a\left(\dfrac{x^{\frac{5}{2}}+\psi}{x}\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(\dfrac{x^i+\omega^i}{x}\right)\right)^2 = 109\left(\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \\ \text{avec} \\ \psi \ = \ -\dfrac{1}{2}\left(\left(-\sqrt{2}\right)^{\frac{5}{2}}+\left(\sqrt{2}\right)^{\frac{5}{2}}\right) \quad \text{et} \quad \omega^i \ = \ -\dfrac{1}{2}\left(\left(-\sqrt{2}\right)^i+\left(\sqrt{2}\right)^i\right) \end{array} \right\}$$

$$\mathcal{S}_4 = \left\{ \begin{array}{l} \left(\begin{array}{c} x,\ -\dfrac{a\left(x^{\frac{5}{2}}+\mu\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\nu^i\right)}{\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \end{array} \right) \left| \begin{array}{l} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \left(a\left(\dfrac{x^{\frac{5}{2}}+\mu}{x}\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(\dfrac{x^i+\nu^i}{x}\right)\right)^2 = 109\left(\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \\ \text{avec} \\ \mu \ = \ -\dfrac{1}{2}\left((\zeta)^{\frac{5}{2}}+(-\zeta)^{\frac{5}{2}}\right) \quad \text{et} \quad \nu^i \ = \ -\dfrac{1}{2}\left((\zeta)^i+(-\zeta)^i\right) \end{array} \right\}$$

ii) **Théorème 2**

L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = (x-74)(x^2-2730)(x^2+5476)$ est donné par :

$$\mathcal{M} \ = \ \mathcal{M}_1 \bigcup \mathcal{M}_2 \bigcup \mathcal{M}_3 \bigcup \mathcal{M}_4$$

avec

$$\mathcal{M}_1 \ = \ \left\{ \begin{array}{l} \left(\begin{array}{c} x,\ -\dfrac{\sum\limits_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum\limits_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \end{array} \right) \left| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair,} \\ b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \left(\sum\limits_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = \left(\sum\limits_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \end{array} \right\}$$

$$\mathcal{M}_2 \;=\; \left\{ \begin{array}{l} \left(x,\; -\dfrac{\displaystyle\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i \;-\; (74)^i)}{\displaystyle\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \;\Bigg|\; \begin{array}{l} a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair, } \; b_{\frac{\ell-4}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \\ \left(\displaystyle\sum_{i=1}^{\frac{\ell+1}{2}} a_i \left(\frac{x^i - (74)^i}{x} \right) \right)^2 = \left(\displaystyle\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \end{array} \right\}$$

$$\mathcal{M}_3 \;=\; \left\{ \begin{array}{l} \left(x,\; -\dfrac{\displaystyle\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i \;+\; \xi^i)}{\displaystyle\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \;\Bigg|\; \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair , } \; b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \\ \left(\displaystyle\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i \;+\; \xi^i}{x} \right) \right)^2 = \left(\displaystyle\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \\ \text{avec} \\ \xi^i = -\dfrac{1}{2}\left((37\sqrt{2})^i \;+\; (-37\sqrt{2})^i \right) \end{array} \right\}$$

$$\mathcal{M}_4 \;=\; \left\{ \begin{array}{l} \left(x,\; -\dfrac{\displaystyle\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i \;+\; \gamma^i)}{\displaystyle\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \;\Bigg|\; \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair , } \; b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \\ \left(\displaystyle\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i \;+\; \gamma^i}{x} \right) \right)^2 = \left(\displaystyle\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \\ \text{avec} \\ \gamma^i \;=\; -\dfrac{1}{2}\left((74\zeta)^i \;+\; (-74\zeta)^i \right) \end{array} \right\}$$

iii) **Théorème 3**

L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 \;=\; 6x(x^4 \;+\; 3)$ est donné par :

$$\mathcal{H} \;=\; \mathcal{H}_1 \bigcup \mathcal{H}_2$$

avec

$$\mathcal{H}_1 \;=\; \left\{ \left(x,\; -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair }, b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair} \\ \text{et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 \;=\; 6x \left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x^4 \;+\; 3) \end{array} \right\}$$

$$\mathcal{H}_2 \;=\; \left\{ \left(x,\; -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} b_0 \;\neq\; 0,\; a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-4}{2}} \neq 0 \\ \text{si } \ell \text{ est impair et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 \;=\; 6 \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_i x^j\right)^2 (x^4 \;+\; 3) \end{array} \right\}$$

iv) **Théorème 4**

L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $-y^2 \;=\; x^6 \;-\; 20x^3 \;-\; 8$ est donné par :

$$\mathcal{R} \;=\; \mathcal{R}_1 \bigcup \mathcal{R}_2$$

avec

$$\mathcal{R}_1 \;=\; \left\{ \left(x,\; \left(\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right)^6 \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \\ \text{est pair }, \; b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair et } x \\ \text{solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^{i-\frac{5\ell}{12}}\right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2-\frac{5\ell}{12}}\right)^{12} \left(x^6 \;-\; 20x^3 \;-\; 8\right) \end{array} \right\}$$

$$\mathcal{R}_2 \;=\; \left\{ \begin{array}{l} \left(x,\; \left(\dfrac{\sum\limits_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i \;+\; \rho^i \right)}{\sum\limits_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+2}} \right)^6 \right) \;\Big|\; a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est impair et } x \text{ solution de l'équation :} \\ \left(\sum\limits_{i=1}^{\frac{\ell+2}{2}} a_i \left(\dfrac{x^i \;+\; \rho^i}{x^{\frac{\ell}{12}+1}} \right) \right)^{12} = - \left(\sum\limits_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+1-\frac{\ell}{12}} \right)^{12} \left(x^6 \;-\; 20x^3 \;-\; 8 \right) \\ \text{avec} \\ \rho^i \;=\; -\dfrac{1}{2} \left(\left(1 \;+\; \sqrt{3} \right)^i \;+\; \left(1 \;-\; \sqrt{3} \right)^i \right) \end{array} \right\}$$

v) **Théorème 5**

L'ensemble des points algébriques de degré au-plus $\ell \;\geq\; 9$ sur la courbe $\mathcal{C}_3(11)$ d'équation affine $y^{11} \;=\; x^3 \left(x \;-\; 1 \right)^3$ est donné par :

$$\mathcal{W} \;=\; \mathcal{W}_0 \bigcup \left(\bigcup_{m=1}^{10} \mathcal{W}_m \right)$$

avec

$$\mathcal{W}_0 \;=\; \left\{ \begin{array}{l} \left(\dfrac{\sum\limits_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}}{\sum\limits_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}},\; y \right) \;\Big|\; a_0 \neq 0,\; a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-11}{2}} \neq 0 \text{ si } \ell \text{ est impair et } y \text{ solution de l'équation :} \\ y^{11} \left(\sum\limits_{j=0}^{\frac{\ell-11}{2}} b_j y^j \right)^6 \;=\; \left(\sum\limits_{i=0}^{\frac{\ell}{2}} a_i y^i \right)^3 \left(\sum\limits_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}} \;+\; \sum\limits_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}} \right)^3 \end{array} \right\}$$

$$\mathcal{W}_m \;=\; \left\{ \begin{array}{l} \left(\dfrac{\sum\limits_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}}}{\sum\limits_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}}, y \right) \;\Big|\; a_{\frac{\ell+11-m}{2}} \neq 0 \;\text{ si } \ell \text{ est pair, } b_{\frac{\ell-m}{2}} \neq 0 \text{ si } \ell \text{ est impair et } y \text{ est solution de l'équation :} \\ y^{11} \left(\sum\limits_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{2j+m-11}{6}} \right)^6 = \left(\sum\limits_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i+m-11}{3}} \right)^3 \left(\sum\limits_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} + \sum\limits_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}} \right)^3 \end{array} \right\}$$

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

Chapitre 1

Notions de base

Dans ce chapitre on introduit les notions de base que nous jugeons utiles dans la suite. Ces notions seront constituées de définitions et résultats supposés classiques.

1.1 Théorie des corps

1.1.1 Corps de décomposition

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

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

Soit $\alpha \in \mathbb{L}$; on désigne par :

- $\mathbb{K}[\alpha]$ le sous-anneau de $\mathbb{L}$ engendré par $\mathbb{K} \cup \{\alpha\}$, c'est-à -dire :

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

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

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

Définition 1.1.2

Une extension $\mathbb{K} \subset \mathbb{L}$ est dite simple s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} \ = \ \mathbb{K}(\alpha)$.

Exemple 1.1.3

* $\mathbb{Q}(\sqrt{5}) \ = \ \left\{ a \ + \ \sqrt{5}b \mid (a, \ b) \ \in \ \mathbb{Q} \right\}$ *est une extension de* $\mathbb{Q}$.
* $\mathbb{R} \ \subset \ \mathbb{C} \ = \ \mathbb{R}(i) \ := \ \{a \ + \ ib \mid (a, \ b) \ \in \ \mathbb{Q}\}$ *est une extension simple de* $\mathbb{R}$.
* *Le corps* $\mathbb{K}(X)$ *des fractions rationnelles à une indéterminée sur le corps* $\mathbb{K}$ *est une extension de* $\mathbb{K}$.

Définition 1.1.4

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

Définition 1.1.5

Une extension $\mathbb{K} \subset \mathbb{L}$ est un corps de rupture sur $\mathbb{K}$ pour le polynôme $P \in \mathbb{K}[X]$ si, $\mathbb{L}$ contient un zéro de P.

Définition 1.1.6

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

Exemple 1.1.7

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

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

1.1.2 Éléments entiers, éléments algébriques

Définition 1.1.8

Soient $\mathbb{A}$ un anneau et $\mathbb{B}$ une $\mathbb{A}$-algèbre.

- *On dit que $b \in \mathbb{A}$ est algébrique sur $\mathbb{A}$ s'il existe un polynôme non nul $P \in \mathbb{A}[X]$ tel que $P(b) = 0$.*
- *Un élément non algébrique est appelé élément transcendant.*
- *On dit que $b \in \mathbb{B}$ est entier sur $\mathbb{A}$ s'il existe un polynôme unitaire $P \in \mathbb{A}[X]$ tel que $P(b) = 0$.*

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

Définition 1.1.9
Soient $\mathbb{A}$ un anneau et $\mathbb{B}$ une $\mathbb{A}$-algèbre. L'ensemble des éléments de $\mathbb{B}$ qui sont entiers sur $\mathbb{A}$ est une sous-$\mathbb{A}$-algèbre de $\mathbb{B}$. On l'appelle clôture intégrale de $\mathbb{A}$ dans $\mathbb{B}$.

Définition 1.1.10
Soient $\mathbb{K}$ un corps et $\mathbb{B}$ une $\mathbb{K}$-algèbre intègre. L'ensemble des éléments de $\mathbb{B}$ qui sont algébriques sur $\mathbb{K}$ est un corps contenu dans $\mathbb{B}$. On l'appelle clôture algébrique de $\mathbb{K}$ dans $\mathbb{B}$.

Définition 1.1.11
Soient $\mathbb{K}$ un corps et B une $\mathbb{K}$-algèbre intègre. Soit $b \in \mathbb{B}$ un élément algébrique.
L'ensemble $\{P \in \mathbb{K}[X] \mid P(b) = 0\}$ est un idéal premier de $\mathbb{K}[X]$. Le polynôme minimal de b en est l'unique générateur unitaire. On remarquera que le polynôme minimal de b est le polynôme unitaire de P de plus petit degré tel que $P(b) = 0$; c'est aussi un polynôme irréductible.

1.1.3 Extensions entières, extensions algébriques

Définition 1.1.12
On dit qu'une extension d'anneaux $\mathbb{A} \subset \mathbb{B}$ est entière si tout élément de $\mathbb{B}$ est entier sur $\mathbb{A}$. On dit qu'une extension de corps $\mathbb{K} \subset \mathbb{L}$ est algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Définition 1.1.13

- *On dit qu'une extension d'anneaux $\mathbb{A} \subset \mathbb{B}$ est finie si $\mathbb{B}$ est une $\mathbb{A}$-module de type fini. On dit qu'une extension de corps $\mathbb{K} \subset \mathbb{L}$ est finie si $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie.*
- *On appelle degré de $\mathbb{L}$ sur $\mathbb{K}$, et l'on note $[\mathbb{L} : \mathbb{K}]$, la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel.*

Définition 1.1.14
Soient $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps des fractions. On dit que $\mathbb{A}$ est intégralement clos si la clôture intégrale de $\mathbb{A}$ dans $\mathbb{K}$ est à $\mathbb{A}$, autrement dit si les éléments de $\mathbb{A}$ sont les seuls éléments de $\mathbb{K}$ qui sont entiers sur $\mathbb{A}$.

Exemple 1.1.15

a. *l'anneau $\mathbb{Z}$ est intégralement clos.*

b. *Si $\mathbb{A}$ est un anneau intégralement clos, $\mathbb{A}[X]$ est intégralement clos.*

Proposition 1.1.16

Soit $\mathbb{K}$ *un corps.*

1- $\mathbb{K}$ *n'admet pas d'extension algébrique* $\mathbb{K} \subset \mathbb{L}$ *avec* $\mathbb{L} \neq \mathbb{K}$ *;*

2- *Les polynômes irréductibles de* $\mathbb{K}[X]$ *sont les polynômes de degré* 1 *;*

3- *Tout polynôme non constant à coefficients dans* $\mathbb{K}$ *possède une racine dans* $\mathbb{K}$ *;*

4- *Tout polynôme à coefficients dans* $\mathbb{K}$ *est scindé.*

Définition 1.1.17

On dit qu'un corps $\mathbb{K}$ *est algébriquement clos s'il vérifie une des conditions de la proposition ci-dessus.*

Définition 1.1.18

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

1.2 Théorie de Galois

1.2.1 Extensions normales

Soit $\mathbb{K}$ un corps.

Définition 1.2.1

Une extension $\mathbb{K} \subset \mathbb{F}$ *est dite normale si, chaque fois que* $\mathbb{F}$ *est un corps de rupture pour un polynôme irréductible* $P \in \mathbb{K}[X]$ *sur* $\mathbb{K}$*, il est un corps de décomposition pour* P *sur* $\mathbb{K}$*. En d'autres termes : une extension* $\mathbb{K} \subset \mathbb{F}$ *est dite normale si, chaque fois qu'un polynôme irréductible* $P \in \mathbb{K}[X]$ *possède une racine dans* $\mathbb{F}$*, alors il se décompose en produit de polynômes linéaires dans* $\mathbb{F}[X]$*.*

Ou encore une extension $\mathbb{K} \subset \mathbb{F}$ *est dite normale si, chaque fois qu'un polynôme irréductible* $P \in \mathbb{K}[X]$ *possède une racine dans* $\mathbb{F}$*, alors il possède toutes ses racines dans* $\mathbb{F}$*.*

Exemple et Contre-exemple 1.2.2

(a) $\mathbb{C}$ *est une extension normale de* $\mathbb{R}$*.*

(b) *L'extension* $\mathbb{Q}(\sqrt[3]{7})$ *de* $\mathbb{Q}$ *n'est pas normale car, le polynôme* $X^3 - 7 \in \mathbb{Q}[X]$ *possède une racine dans* $\mathbb{Q}(\sqrt[3]{7})$ *sans se décomposer en produit de polynômes linéaires dans* $\mathbb{Q}(\sqrt[3]{7})[X]$*.*

Définition 1.2.3

Soit une extension $\mathbb{K} \subset \mathbb{F}$*.*

Une clôture normale de $\mathbb{F}$ *est une extension normale* $\mathbb{K} \subset \mathbb{N}$ *qui satisfait les conditions suivantes :*

(i) $\mathbb{K} \subset \mathbb{F} \subset \mathbb{N}$.

(ii) *Si* $\mathbb{K} \subset \mathbb{M}$ *est une extension normale vérifiant* $\mathbb{K} \subset \mathbb{F} \subset \mathbb{M} \subset \mathbb{N}$, *alors* $\mathbb{M} = \mathbb{N}$.

Exemple 1.2.4
$\mathbb{C}$ *est une clôture normale de l'extension* $\mathbb{Q} \subset \mathbb{R}$.

1.2.2 Extensions séparables

Définition 1.2.5
Soit $\mathbb{K}$ *un corps,* $\mathbb{K} \subset \mathbb{E}$ *et* $\mathbb{K} \subset \mathbb{F}$ *deux extensions de* $\mathbb{K}$.
On appelle $\mathbb{K}$*-isomorphisme de* $\mathbb{E}$ *dans* $\mathbb{F}$ *tout isomorphisme* $\sigma : \mathbb{E} \to \mathbb{F}$ *laissant fixe tout élément de* $\mathbb{K}$, *c'est à dire* $\sigma(\lambda) = \lambda$ *pour tout* $\lambda \in \mathbb{K}$.

Exemple 1.2.6
L'application $\sigma : \mathbb{C} \to \mathbb{C}$ *définie par* $\sigma(z) = \bar{z}$ *(le conjugué de z) est un* $\mathbb{R}$*-isomorphisme de* $\mathbb{C}$ *dans* $\mathbb{C}$.

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

Définition 1.2.7
On appelle degré galoisien d'une extension $\mathbb{K} \subset \mathbb{F}$, *et l'on note* $\overline{[\mathbb{F} : \mathbb{K}]}$, *le cardinal de l'ensemble des* $\mathbb{K}$*-isomorphismes de* $\mathbb{F}$ *dans une clôture normale de* $\mathbb{F}$.

NB : La définition du degré galoisien ne dépend pas du choix de la clôture normale de $\mathbb{F}$

Théorème 1.2.8
Si $\mathbb{F} = \mathbb{K}(a)$, *alors* $\overline{[\mathbb{F} : \mathbb{K}]}$ *est le nombre de racines distinctes de* $Irr(a, \mathbb{K})$ *polynôme minimal de* $\mathbb{A}$ *sur* $\mathbb{K}$.

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

CQFD

Définition 1.2.9
Une extension $\mathbb{K} \subset \mathbb{L}$ *est dite séparable si,* $\overline{[\mathbb{L} : \mathbb{K}]} = [\mathbb{L} : \mathbb{K}]$.
Un élément $a \in \mathbb{L}$ *est séparable sur* $\mathbb{K}$, *si toutes les racines de* $Irr(a, \mathbb{K})$ *sont simples.*

Exemple 1.2.10
$\mathbb{C}$ *est une extension séparable de* $\mathbb{R}$. *Le nombre complexe i est séparable sur* $\mathbb{R}$. $\sqrt{5}$ *est séparable sur* $\mathbb{Q}$.

Théorème 1.2.11
Une extension $\mathbb{K}(a)$ *est séparable, si et seulement si* a *est séparable sur* $\mathbb{K}$.

Preuve :
Soit $[\mathbb{L} : \mathbb{K}] = n = \deg(Irr(a, K))$. Nous avons les équivalences Suivantes :

$$\begin{aligned} \mathbb{L} \text{ est séparable sur } \mathbb{K} &\iff [\overline{[\mathbb{L} : \mathbb{K}]} = [\mathbb{L} : \mathbb{K}]] \\ &\iff Irr(a, \mathbb{K}) \text{ posséde } n \text{ racines distinctes} \\ &\iff \text{ toute racine de } Irr(a, K) \text{ est simple} \\ &\iff a \text{ est séparable sur } \mathbb{K} \end{aligned}$$

CQFD

$\mathbb{B}$

1.2.3 Extensions galoisiennes

Définition 1.2.12
Soit $\mathbb{L}$ *une extension normale finie d'un corps* $\mathbb{K}$. *L'ensemble des* $\mathbb{K}$*-automorphismes de* $\mathbb{L}$ *forme un groupe pour la composition des applications noté* $G(\mathbb{L}/\mathbb{K})$ *et appelé le groupe de Galois de l'extension* $\mathbb{L}$ *de* $\mathbb{K}$.

Exemple 1.2.13
$\mathbb{C}$ *est une extension normale finie de* $\mathbb{R}$. $G(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \rho\}$ *où* ρ *est le* $\mathbb{R}$*-automorphisme qui associe à chaque nombre complexe* z *son conjugué* $\bar{z}$.

Théorème 1.2.14
Le groupe de Galois $G(\mathbb{L}/\mathbb{K})$ *est fini, et son ordre est le degré galoisien* $\overline{[\mathbb{L} : \mathbb{K}]}$.

Preuve :
Le groupe de Galois $G(\mathbb{L}/\mathbb{K})$ est l'ensemble des $\mathbb{K}$-isomorphismes de $\mathbb{L}$ dans une clôture normale de $\mathbb{L}$.
En effet, $\mathbb{L}$ est sa propre clôture normale car elle est une extension normale de $\mathbb{K}$, donc on a $G(\mathbb{L}/\mathbb{K})$ est fini.Ainsi on voit que l'ordre de $G(\mathbb{L}/\mathbb{K})$ est le degré galoisien $\overline{[\mathbb{L} : \mathbb{K}]}$.

CQFD

Corollaire 1.2.15
Soit $\mathbb{L}$ *une extension normale de* $\mathbb{K}$, *alors on a :* $ord(G(\mathbb{L}/\mathbb{K})) \leq [\mathbb{L} : \mathbb{K}]$.

Définition 1.2.16
Soit $\mathbb{K} \subset \mathbb{L}$ *une extension finie d'un corps* $\mathbb{K}$. *L'extension* $\mathbb{K} \subset \mathbb{L}$ *est dite galoisienne si elle est normale et séparable.*

Exemple 1.2.17
$\mathbb{R} \subset \mathbb{C}$ *est une extension galoisienne.*

Définition 1.2.18
Soient $\mathbb{K} \subset \mathbb{L}$ *et* $x \in \mathbb{L}$ *algébrique sur* $\mathbb{K}$ *de polynôme minimal* $irr(x, \mathbb{K})$ *à coefficients dans* $\mathbb{K}$.

(∗) *Les zéros de* $irr(x, \mathbb{K})$ *dans* $\mathbb{K}$ *sont appelés les conjugués de* x.

(∗) *Les conjugués de* x *qui sont laissés fixes sous l'action de Galois (c'est-à -dire qui sont laissés fixes par les* $\mathbb{K}$*-automorphismes de* $\mathbb{L}$*) sont appelés les conjugués de Galois de* x.

1.3 Variétés algébriques

1.3.1 Variétés affines

Dans tout le paragraphe on considérera $\mathbb{K}$, un corps commutatif .

Définitions 1.3.1

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

Les éléments de $\mathbb{K}^n$ *sont appelés points.*

Un point P *de* $\mathbb{K}^n$ *est dit zéro d'un polynôme* $F \in \mathbb{K}[X_1, \ldots, X_n]$ *si* $F(P) = 0$.

Définitions 1.3.2
On considère $S \subset \mathbb{K}[X_1, \ldots, X_n]$.
On note $\mathcal{V}(S)$ *l'ensemble défini par :*

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

c'est l'ensemble des zéros communs à tous les éléments de S.
L'ensemble $\mathcal{V}(S)$ *est appelé l'ensemble algébrique affine défini par* S.

Exemple 1.3.3
Le vide et l'ensemble tout entier sont des ensembles algébriques affines.
En effet : $\mathcal{V}(1) = \phi$ *et* $\mathcal{V}(0) = \mathbb{A}^n$ *où 1 et 0 désignent respectivement les polynômes constants* $P \longmapsto 1$ *et* $P \longmapsto 0$.
Si $n = 1$ *et si* S *n'est pas réduit à* 0, $\mathcal{V}(S)$ *est un ensemble fini.*

Définitions 1.3.4

◇ *Un ensemble algébrique affine* $\mathcal{E}$ *est irréductible s'il n'est pas vide et s'il n'est pas réunion de deux fermés distincts de* $\mathcal{E}$.

◇ *On appelle variété affine tout ensemble algébrique affine irréductible.*

1.3.2 Variétés projectives

Considérons l'anneau $\mathbb{K}[X_0, \ldots, X_n]$; on garde notre corps $\mathbb{K}$ de l'espace affine $\mathbb{A}^n$ de dimension n sur $\mathbb{K}$.

Définition 1.3.5
On considère sur $\mathbb{K}^{n+1}\backslash\{0\}$ la relation $\mathcal{R}$ définie par : $\forall\ x,\ y\ \in\ \mathbb{K}^{n+1}\backslash\{0\}$, $x\ \mathcal{R}\ y$ si et seulement si ils sont colinéaires ; c'est-à -dire :

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

. On montre aisément que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{K}^{n+1}\backslash\{0\}$.
L'ensemble des classes d'équivalence par $\mathcal{R}$ est appelé l'espace projectif de dimension n sur $\mathbb{K}$, et l'on note $\mathbb{P}(\mathbb{K}^{n+1})$ ou $\mathbb{P}^n(\mathbb{K})$ ou simplement $\mathbb{P}^n$.

Définition 1.3.6
Soit $F\ \in\ \mathbb{K}[X_0,\ \ldots\ , X_n]$. On dit que F est homogène de degré d si pour tout $\lambda\ \in\ \mathbb{K}$, on a :

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

Définitions 1.3.7
Soit S une partie de $\mathbb{K}[X_0,\ \ldots\ , X_n]$ formée de polynômes homogènes.
On appelle ensemble algébrique projectif défini par S, l'ensemble noté $\mathcal{V}(S)$ défini par :

$$\mathcal{V}(S)\ =\ \{[X_0 : \ldots : X_n] \in \mathbb{P}^n \mid \forall\ F \in S, F(P) = 0\}$$

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

1.3.3 Courbes planes.

1.3.3.1 Courbes planes affines.

Une courbe algébrique plane sur un corps $\mathbb{K}$ est formée par les points

$$\mathcal{C}\ :\ \{(x,\ y) \in \mathbb{K} \mid f(x,\ y) = 0\}$$

pour un polynôme non constant $f(x,\ y)$ dans $\mathbb{K}[X,\ Y]$. On a : $f\ =\ f_1 \cdot \ldots\ldots \cdot f_r$, où f_i sont irréductibles non proportionnels. Ceci implique que

$$\mathcal{C}\ =\ \bigcup_{i=1}^{r} \mathcal{C}_i$$

où $\mathcal{C}_i\ :\ f_i = 0$ est une courbe irréductible.

1.3.3.2 Courbes planes projectives.

Rappelons qu'un point P du plan projectif $\mathbb{P}^2$ est donné comme la classe d'équivalence, notée $[X : Y : Z]$, d'un triplet non-nul $(X,\ Y,\ Z)\ \in\ \mathbb{K}^3\backslash\{(0,0,0)\}$, de telle façon que : $[X : Y : Z] \sim [X' : Y' : Z']$ si et seulement si $\exists\ \lambda \in \mathbb{K}^*\quad (X',\ Y',\ Z')\ =\ (\lambda X,\ \lambda Y,\ \lambda Z)$
On a l'inclusion

$$\mathbb{A}^2\ \hookrightarrow\ \mathbb{P}^2, \qquad (x,\ y)\ \longmapsto\ [x :\ y :\ 1],$$

qui donne tous les points de $\mathbb{P}^2$ avec $Z\ \neq\ 0$. On a les relations suivantes entre les coordonnées affines (x, y) est les coordonnées projectives $[X\ :\ \ Y\ :Z]$:

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

1.3.3.3 Points singuliers

Rappelons qu'une courbe projective plane $\mathcal{C}$ sur $\mathbb{K}$ est définie par une équation de type $F = 0$, où $F\ \in\ \mathbb{K}[X, Y, Z]$ est une forme homogène des variables projectives $X,\ Y,\ Z$. L'équation de la tangente dans les coordonnées affines a la forme :

$$f'_x(P)(x - \alpha) + f'_y(P)(y - \beta) = 0.$$

Par la construction,

$$f(x, y) = F([x : y : 1])\ \text{, où}\ F([X\ :\ \ Y\ :Z]) = 0$$

l'équation homogène de la courbe.
Ceci implique :$f'_x = F'_x,\ f'_y = F'_y$ et selon le théorème connu de Euler (sur les fonctions homogènes) on a :

$$XF'_X + YF'_Y + ZF'_Z = nF \text{ où } n \text{ est le degré de } F$$

Lorsque $P = [\alpha\ :\ \beta\ :\ 1]$ se trouve sur la courbe alors

$$\alpha F'_X(P) + \beta F'_Y(P) + F'_Z(P) = nF,$$

donc l'équation de la tangente se transforme comme suit :

$$xF'_X(P) + yF'_Y(P) + F'_Z(P) = 0 \Longleftrightarrow XF'_X + YF'_Y + ZF'_Z = 0.$$

(c'est la forme projective de la droite tangente).

Définition 1.3.8

a) Un point singulier sur une courbe projective plane $\mathcal{C}$ sur $\mathbb{K}$ est toute solution du système

$$F = F'_X = F'_Y = F'_Z = 0$$

dans une extension de $\mathbb{K}$.

b) On dit qu'une courbe projective plane $\mathcal{C}$ sur $\mathbb{K}$ est lisse si le système

$$F = F'_X = F'_Y = F'_Z = 0$$

n'a pas de solutions non triviales dans toute extension de $\mathbb{K}$.

Définition 1.3.9
Un ensemble G est appelé un groupe algébrique sur un corps (algébriquement clos) $\mathbb{K}$ s'il est muni d'une structure de variétés (sur $\mathbb{K}$) et d'une structure de groupe telles les applications :

$$m \ : \ \begin{array}{c} G \times G \to G \\ (x,y) \mapsto xy \end{array} \quad \textit{et} \quad n \ : \ \begin{array}{c} G \to G \\ x \mapsto x^{-1} \end{array} \quad \textit{soient des morphismes.}$$

Exemple 1.3.10
Le groupe des automorphismes linéaires d'un espace vectoriel V de dimension n sur $\mathbb{K}$ est un groupe algébrique.

Définition 1.3.11
Une variété Abélienne est variété projective vérifiant une structure de groupe algébrique.

1.4 Diviseurs sur une courbe

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

1.4.1 Notions de base

Définition 1.4.1

— ***Diviseur*** *: Un diviseur D est une somme formelle de la forme :*

$$D \ = \ \sum_{P \in \mathcal{C}} n_p P \textit{ avec } n_P \ = \ 0 \textit{ pour presque tout } P \ \in \ \mathcal{C}$$

Un diviseur de la forme $D \ = \ P$ avec $P \ \in \ \mathcal{C}$ est appelé ***diviseur premier****.*

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

- ***Addition sur les diviseurs*** *:*
  Soient deux diviseurs $D = \sum_{P\in\mathcal{C}} n_p P$ *et* $D' = \sum_{P\in\mathcal{C}} n'_p P$ *alors on a :*

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

- ***Élément neutre*** *: L'élément nul du groupe diviseur est le diviseur :*

$$0 := \sum_{P\in\mathcal{C}} n_p P \text{ avec } n_p = 0 \text{ pour tout } P \in \mathcal{C}$$

— ***Support d'un diviseur*** *: Le support de* $D = \sum_{P\in\mathcal{C}} n_p P$ *est défini par :*

$$supp\ D := \{P \in \mathcal{C} \mid n_p \neq 0\}$$

— ***Diviseur effectif*** *: On dit que le diviseur* $D = \sum_{P\in\mathcal{C}} n_P P$ *est effectif si :*

$$n_P \geq 0, \qquad \forall\ P \in \mathcal{C}.$$

On notera $D \geq 0$ *pour exprimer que* D *est effectif.*
La relation dans $Div(\mathcal{C})$ *définie par*

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

est une relation d'ordre partielle.

— ***Degré d'un diviseur*** *: Le degré d'un diviseur* $D = \sum_{P\in\mathcal{C}} n_P P$ *noté* $\deg(D)$ *est la somme de ses coefficients :*

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

— ***L'ensemble*** Div^0 *: Considérons l'homomorphisme de groupes* $Div(\mathcal{C})$ *dans* $\mathbb{Z}$ *défini par :* $\deg : Div(\mathcal{C}) \longrightarrow \mathbb{Z}, \qquad D \longmapsto \deg(D)$.
Le noyau de ce morphisme est l'ensemble des diviseurs sur $\mathcal{C}$ *de degré nul, que l'on note* $Div^0(\mathcal{C})$*. On a alors* $\ker(\deg) = Div^0(\mathcal{C})$ *est un sous-groupe de* $Div(\mathcal{C})$*.*

Définitions 1.4.2
Soit D *un diviseur d'une courbe* $\mathcal{C}$*.*
On appelle système linéaire complet et on note $|D|$ *l'ensemble des diviseurs effectifs linéairement équivalents à* D *c'est à dire :* $|D| = \{D' \geq 0 \mid D \sim D'\}$.
Un point de $|D|$ *est appelé point base.*

1.4.2 Diviseurs principaux

Considérons $\mathcal{C}$ une courbe algébrique affine et irréductible et $\mathbb{K}[\mathcal{C}]$ un anneau intègre pour cette section.

Définition 1.4.3
Le corps des fractions de $\mathbb{K}[\mathcal{C}]$ *est appelé le corps des fonctions rationnelles sur* $\mathcal{C}$ *et est noté* $\mathbb{K}(\mathcal{C})$.

Définition 1.4.4
Soient $f \in \mathbb{K}(\mathcal{C})$ *et* $P \in \mathcal{C}$. *On dit que* f *est régulière en un point* P *s'il existe* $g,\ h \in \mathbb{K}(\mathcal{C})$ *avec* $h(P) \neq 0$ *tel que* $f = \dfrac{g}{h}$.

NB : Si f est régulière au point $P \in \mathcal{C}$ et $f(P) = 0$, on dit que P est un zéro de f.

On définit l'homomorphisme surjectif $ord_P : \mathcal{O}_P(\mathcal{C}) \to \mathbb{Z} \cup \{\infty\}$ défini par :

$$\divideontimes ord_P(a.x^n) = n,\ \divideontimes ord_P(x) = 1,\ \divideontimes ord_P(a) = 0,\ \divideontimes ord_P(0) = \infty$$

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

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

Propriété 1.4.5
1) $ord_P(x) = \infty$ *si et seulement si* $x = 0$,
2) $ord_P(xy) = ord_P(x) + ord_P(y)$,
3) $ord_P(x/y) = ord_P(x) - ord_P(y)$,
4) $ord_P(x + y) \geq min(ord_P(x),\ ord_P(y))$.

Remarque 1.4.6
Soit $\mathcal{C}$ *une courbe plane lisse et irréductible en* P , *et* $f \in \mathbb{K}(\mathcal{C})$ *une fonction non nulle.*
i) Si f *est régulière en* P *et* $f(P) \neq 0$, *alors* $ord_P(f) = 0$.
iii) Si f *est régulière en* P *et* $f(P) = 0$, *alors* $ord_P(f) > 0$.
vi) Si $\mathcal{C}$ *est lisse en* P *alors* $\mathcal{O}_P(\mathcal{C})$ *est un anneau de valuation discrète.*

Définition 1.4.7
Soit $\mathcal{C}$ *une courbe plane projective lisse et irréductible, et soit un polynôme non nul* $f \in K(\mathcal{C})$. *On associe à* f *le diviseur noté* $div(f)$ *défini par :*

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

Un tel diviseur est appelé diviseur principal.

NB : L'ensemble des diviseurs principaux, noté $Princ(\mathcal{C})$ est un sous-groupe de $Div(\mathcal{C})$.

Consequance 1.4.8

On pose Z (resp. N) l'ensemble des zéros (resp. des pôles) de f. On définit :

- ***Le diviseur des zéros*** *par :* $div(f)_0 := \sum_{P\in Z} ord_P(f).P$
- ***Le diviseur des pôles*** *par :* $div(f)_\infty := \sum_{P\in N} (-ord_P(f)).P$

Alors le diviseur principal de f est : $div(f) := div(f)_0 + div(f)_\infty$

Remarque 1.4.9

⊗ *Si f a un pôle en P, alors* $ord_P(f) = -ord_P(1/f)$.

⊗ *Deux diviseurs D et D' sont linéairement équivalents (noté $D \sim D'$) si leur différence est un diviseur principal.*

Remarque 1.4.10

Pour f et g deux fonctions non nulles de $\mathbb{K}[X]$, on a :

⊛ $div(fg) := div(f) + div(g)$.

⊛ $div\left(\frac{f}{g}\right) := div(f) - div(g)$

Exemple 1.4.11

Considérons une fonction rationnelle $h(x) = a.\frac{f(x)}{g(x)}$ *avec* $a \in \mathbb{K}^*$, $f(x),\ g(x) \in \mathbb{K}[x]$ *et premiers entre eux. Notons* $f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}$ *et* $g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$ *avec $p_i(x)$ et $q_j(x) \in \mathbb{K}[x]$ des polynômes irréductibles.*

Alors le diviseur principal de h dans $Div(\mathbb{C})$ est :

$$div(h) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\deg g - \deg f)P_\infty$$

où P_i respectivement Q_j sont les zéros correspondants aux $p_i(x)$ et $q_j(x)$.

Définition 1.4.12

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

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

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

$$\dot{D} = \{D' \in Div(\mathcal{C}) \mid \exists\ f \in \mathbb{K}(\mathcal{C}) : D - D' = div(f)\}.$$

On note $Pic^0(\mathcal{C})$ l'ensemble des classes de $Pic(\mathcal{C})$ des diviseurs de degré 0.
On montre que $Pic^0(\mathcal{C})$ est un sous-groupe de $Pic(\mathcal{C})$ et on a : $Pic^0(\mathcal{C}) \cong J(K)(\mathcal{C})$ où $J(K)(\mathcal{C})$ désigne la jacobienne de $\mathcal{C}$ sur $\mathbb{K}$.

1.5 Étude de $\mathcal{L}(D)$ et de sa dimension

La définition suivante joue un rôle fondamental dans nos travaux.

1.5.1 Définition

Définition 1.5.1
Pour un diviseur $D \in Div(\mathcal{C})$, on note $\mathcal{L}(D)$ l'ensemble défini par :

$$\mathcal{L}(D) := \{f \in \mathbb{K}(\mathcal{C})\backslash\{0\} \mid div(f) \geq -D\} \cup \{0\}.$$

On note que $\mathcal{L}(D)$ est un $\mathbb{K}$-espace vectoriel de dimension fini noté $\dim_{\mathbb{K}} \mathcal{L}(D)$ ou $\dim \mathcal{L}(D)$ ou plus simplement $l(D)$.

Conséquence de la définition :

Si $D = \sum_{i=1}^{r} n_i.P_i - \sum_{j=1}^{s} m_j.Q_j$ avec $n_i > 0,\ m_j > 0$ pour tout $i = 1 \dots r$ et $j = 1 \dots s$ où $\{P_1, \dots, P_r\} \bigcap \{Q_1, \dots, Q_s\} = \emptyset$ alors $\forall f \in \mathbb{K}[\mathcal{C}]$

$$f \in \mathcal{L}(D) \iff div_0(f) - div_\infty(f) \geq \sum_{j=1}^{s} m_j.Q_j - \sum_{i=1}^{r} n_i.P_i$$

car $div_\infty(f) \leq \sum_{i=1}^{r} n_i.P_i$ et $div_0(f) \geq \sum_{j=1}^{s} m_j.Q_j$

Autrement dit, $\mathcal{L}(D)$ contient tous les éléments $f \in \mathbb{K}(\mathcal{C})$ tels que :

- $div(f)$ a un zéro d'ordre $\geq m_j$ en Q_j pour $j = 1, \dots, s$.
- $div(f)$ peut seulement avoir des pôles en les points $P_1, \dots, P_s$ avec l'ordre du pôle de P_i majoré par n_i pour $i = 1, \dots, r$.

Remarque 1.5.2
Soit $D \in Div(\mathcal{C})$. Alors les deux assertions suivantes sont équivalentes :
a. *On a pour tout $f \in \mathbb{K}(\mathcal{C})$:*

$$f \in \mathcal{L}(D) \iff div(f) \geq -D$$

b. $\mathcal{L}(D) \neq 0$ *si et seulement si il y a un diviseur $D' \sim D$ avec $D' \geq 0$.*

1.5.2 Propriétés de $\mathcal{L}(D)$

Lemme 1.5.3
Soit $D \in Div(\mathcal{C})$, alors on a :

a. *$\mathcal{L}(D)$ est un $\mathbb{K}$-espace vectoriel.*

b. *Si D' est un diviseur équivalent à D alors $\mathcal{L}(D) \simeq \mathcal{L}(D')$ (isomorphisme d'espaces vectoriels sur $\mathbb{K}$).*

Lemme 1.5.4
Soient D et D' des diviseurs de $Div(\mathcal{C})$ avec $D \leq D'$. Alors on a : $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ et $\dim\left(\dfrac{\mathcal{L}(D')}{\mathcal{L}(D)}\right) \leq \deg(D) - \deg(D')$

Remarque 1.5.5
On peut maintenant reformuler le Lemme précédent, en écrivant :

$$D' \geq D \implies 0 \leq \dim \mathcal{L}(D') - \dim \mathcal{L}(D) \leq \deg(D) - \deg(D')$$

1.5.3 Propriétés de $\dim_{\mathbb{K}} \mathcal{L}(D)$

Proposition 1.5.6
Pour tout diviseur $D \in Div(\mathcal{C})$, l'espace $\mathcal{L}(D)$ est un espace vectoriel de dimension finie sur $\mathbb{K}$. Plus précisément : si $D = D_+ - D_-$ avec les diviseurs positifs D_+ et D_- alors :

$$\dim \mathcal{L}(D) \leq \deg D_+ + 1$$

Théorème 1.5.7
Soit $D \in \mathbb{K}(\mathcal{C})$ et soient D_0 et D_∞ respectivement les diviseurs des zéros et les diviseurs des pôles de D. Alors : $\deg(D_0) = \deg(D_\infty) = [\mathbb{L} : \mathbb{K}]$

Corollaire 1.5.8

a. *Soit D et D' des diviseurs tels que $D \sim D'$. Alors on a :* $\dim \mathcal{L}(D) = \dim \mathcal{L}(D')$.

b. *Si* $\deg D < 0$ *alors* $\dim \mathcal{L}(D) = 0$

c. *Pour un diviseur D de degré 0 les assertions suivantes sont équivalentes :*

- **(a)** *D est principal*
- **(b)** $\dim \mathcal{L}(D) \geq 1$
- **(c)** $\dim \mathcal{L}(D) = 1$

1.6 Théorème de Riemman-Roch

1.6.1 Énoncé du théorème

Soit $\mathcal{C}$ une courbe algébrique plane et lisse sur un corps de nombres $\mathbb{K}$.

Définition 1.6.1
Considérons $\mathcal{C}$ une courbe lisse projective de degré d. Le genre de la courbe $\mathcal{C}$ est l'entier g défini par : $g = \dfrac{(d-1)(d-2)}{2}$.

Définition 1.6.2
On peut définir un diviseur noté $W_{\mathcal{C}}$, appelé diviseur canonique de $\mathcal{C}$ tel que $\dim \mathcal{L}(W_{\mathcal{C}}) = g$ où g désigne le genre de la courbe $\mathcal{C}$.

Théorème 1.6.3 *(Théorème de Riemman-Roch) :*
Considérons une courbe $\mathcal{C}$ lisse et projective de genre g.
Pour tout diviseur $D \in Div(D)$, on a :

$$\dim \mathcal{L}(D) = \deg(D) + 1 - g + \dim \mathcal{L}(W_{\mathcal{C}} - D)$$

où g est le genre de $\mathcal{C}$ et $W_{\mathcal{C}}$ est un diviseur canonique.

1.6.2 Conséquences du théorème de Riemann-Roch

Un conséquence immédiate du théorème de Riemann-Roch est le corollaire suivant :

Corollaire 1.6.4
Si D est un un diviseur canonique, alors :

$$\deg D = 2g - 2 \qquad et \qquad \dim \mathcal{L}(D) = g.$$

Corollaire 1.6.5
Pour un diviseur $D \in Div(\mathcal{C})$, on l'assertion suivante :

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

Théorème 1.6.6
Si D est un diviseur tel que $\deg D \geq 2g - 1$ alors :

$$\dim \mathcal{L}(D) = \deg D + 1 - g$$

Théorème 1.6.7 *(Théorème de Clifford)*
Soit $D \in Div(\mathcal{C})$ tel que $0 \leq \deg D \leq 2g - 2$ alors :

$$\dim \mathcal{L}(D) \leq 1 + \frac{1}{2}\deg D$$

1.7 Groupe de Mordell-Weil

En théorie des nombres, le théorème de Mordell-Weil affirme que pour toute variété abélienne $\mathcal{A}$ sur un corps de nombres $\mathbb{K}$, le groupe $\mathcal{A}(\mathbb{K})$ des points $\mathbb{K}$-rationnels de $\mathcal{A}$ est un groupe abélien de type fini, appelé le groupe de Mordell-Weil. Le théorème de Mordell-Weil généralise le théorème de Mordell qui correspond au cas particulier où $\mathcal{A}$ est une courbe elliptique et $\mathbb{K}$ le corps de nombres $\mathbb{Q}$.

Définition 1.7.1
Soient G un groupe et $x \in G$. S'il existe un entier non nul n tel que $x^n = e_G$, on dit que x est un point de torsion (ou que x est d'ordre fini).

- *Le plus petit entier n vérifiant $x^n = e_G$ est appelé ordre de x.*
- *L'ensemble des points de torsion de G est un sous-groupe de G noté G_{tors}.*
- *On dit que G est un groupe de torsion si $G = G_{tors}$.*

Définition 1.7.2
Soit $\mathbb{K}$ un corps, on appelle équation de Weierstrass sur $\mathbb{K}$ une équation du type :

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

avec $a_i \in \mathbb{K}$. Une courbe donnée par une telle équation est dite lisse si le système suivant n'admet pas de solution

$$\begin{cases} 3x^2 \ + \ 2a_2x \ + \ a_4 \ = \ a_1y \\ 2y \ + \ a_1x \ + \ a_3 \ = \ 0 \end{cases}$$

autrement dit si les dérivées partielles en x et en y de

$$f(x,y) = y^2 \ + \ a_1xy \ + \ a_3y \ - \ x^3 \ - \ a_2x^2 \ - \ a_4x \ - \ a_6$$

ne s'annulent pas en même temps.

Définition 1.7.3
Une courbe elliptique $\mathbb{E}$ définie sur $\mathbb{K}$ est une courbe lisse donnée par une équation de Weierstrass définie sur $\mathbb{K}$ à laquelle, on a rajouté un point "à l'infini", noté O.

Autrement dit c'est une courbe lisse de la forme

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

Si la caractéristique de $\mathbb{K}$ (char($\mathbb{K}$)) n'est pas 2 ni 3, alors en faisant les deux changements de variables successifs $y \to \frac{1}{2}(y \ - \ a_1x \ - \ a_3)$ et ensuite $(x, \ y) \to (\frac{1}{36}(x - 3b_2), \frac{1}{216}y)$

dans $\mathbb{K}$ où $b_2 = a_1^2 + 4a_2$, nous obtenons :

$$\mathcal{E} : y^2 = x^3 - 27c_4x - 54c_6,$$

avec $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^3 + 4a_6$, $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.
Si $char(K) \neq 2, 3$, nous pouvons toujours travailler avec des courbes elliptiques de la forme :

$$\mathcal{E} : y^2 = x^3 + Ax + B.$$

Théorème 1.7.4 *(Mordell-Weil)*
Le groupe $\mathcal{E}(\mathbb{Q})$ est un groupe de type fini.

Remarque 1.7.5
On remarque que $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathcal{J}_{tor}(\mathbb{Q})$ avec r le rang de la courbe et $\mathcal{J}_{tor}(\mathbb{Q}) = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \ldots \times \mathbb{Z}/n_p\mathbb{Z}$.

Théorème 1.7.6
En considérant les notations de la Remarque 1.7.5 si $r = 0$, alors on a :

$$\mathcal{J}(\mathbb{Q}) = \mathcal{J}_{tor}(\mathbb{Q}) = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \ldots \times \mathbb{Z}/n_p\mathbb{Z}$$

1.8 Théorème d'Abel-Jacobi

Définitions 1.8.1
Désignons par $[D]$ la classe dans $Pic^0(\mathcal{C})$ d'un diviseur D. Soit $P_\infty \in \mathcal{C}$ un point base.

- *On appelle plongement jacobien l'application j définie par :*

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

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

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

et est appelée application d'Abel-Jacobi.

Théorème 1.8.2 *(Abel-Jacobi)*
L'application j est surjective et son noyau est formé des diviseurs de fonctions sur $\mathcal{C}$. En d'autres termes, l'application j induit un isomorphisme de $Pic^0(\mathcal{C})$ vers $\mathcal{J}(\mathcal{C})$.

Chapitre 2

Points algébriques de degré donné quelconque sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$

2.1 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 sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leqslant\ell} \mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à -dire qu'on a $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera par $\mathcal{J}$ la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

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

où $\mathcal{J}(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (voir [1, 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

$$\mathcal{C} : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

étudiées dans [15, page 107].
Notre courbe $\mathcal{C} : y^2 = x^3 - 8x^2 + x$ est d'équation projective

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 - 8\left(\frac{X}{Z}\right)^2 + \frac{X}{Z} \qquad (*)$$

qui peut s'écrire

$$ZY^2 = X\left(X - (4 - \sqrt{15})Z\right)\left(X - (4 + \sqrt{15})Z\right) \qquad (**)$$

ce qui correspond aussi à l'équation affine

$$y^2 = x\left(x - (4 - \sqrt{15})\right)\left(x - (4 + \sqrt{15})\right)$$

On note P_0, P_1, P_2 et P_∞ les points sur $\mathcal{C}$, définis par :$P_0 = [0 : 0 : 1]$, $P_1 = [4 - \sqrt{15} : 0 : 1]$, $P_2 = [4 + \sqrt{15} : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$.
Dans cette note, on détermine l'ensemble :

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

Notre résultat principal est donné par :

Théorème :
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 :

$$\mathcal{F}'_\ell = \left\{ \left(x, \ -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls }, \ a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est impair et} \\ x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right) \end{array} \right\}$$

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

2.2 Résultats auxiliaires

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

Lemme 2.2.1
On a : $\mathcal{J}(\mathbb{Q}) \;\cong\; \mathbb{Z}/2\mathbb{Z}$

Démonstration : (voir [1, page 272])

Lemme 2.2.2
Pour la courbe $\mathcal{C} \;:\; y^2 \;=\; x^3 \;-\; 8x^2 \;+\; x$ *qui est aussi donnée par :*

$$\mathcal{C} \;:\; y^2 \;=\; x\Big(x \;-\; \Big(4-\sqrt{15}\Big)\Big)\Big(x \;-\; \Big(4+\sqrt{15}\Big)\Big).$$

On a :

$(i)\; div(x) \;=\; 2P_0 \;-\; 2P_\infty,$
$(ii)\; div(x \;-\; (4-\sqrt{15})) \;=\; 2P_1 \;-\; 2P_\infty,$
$(iii)\; div(x \;-\; (4+\sqrt{15})) \;=\; 2P_2 \;-\; 2P_\infty,$
$(viii)\; div(y) \;=\; P_0 \;+\; P_1 \;+\; P_2 \;-\; 3P_\infty.$

Démonstration :
Notons x, y les coordonnées affines et X, Y et Z les coordonnées projectives.
Posons : $x \;=\; \dfrac{X}{Z}$ et $y \;=\; \dfrac{Y}{Z}$.
L'équation projective de la courbe $\mathcal{C}$ est définie par : $\left(\dfrac{Y}{Z}\right)^2 \;=\; \left(\dfrac{X}{Z}\right)^3 - 8\left(\dfrac{X}{Z}\right)^2 + \left(\dfrac{X}{Z}\right)$.
Cette équation devient : $ZY^2 \;=\; X(X \;-\; (4-\sqrt{15})Z)(X \;-\; (4+\sqrt{15})Z)$.

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

- Pour $X = 0$, on déduit de $(**)$ que $Y^2 = 0$ ou $Z = 0$.
  On obtient donc les points $P_0 = [0 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 1 respectivement. D'où

$$(X = 0)\cdot\mathcal{C} = 2P_0 + P_\infty. \tag{2.2.1}$$

- De même pour $Z = 0$, on déduit que $X^3 = 0$.
  On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 3. D'où

$$(Z = 0)\cdot\mathcal{C} = 3P_\infty. \tag{2.2.2}$$

  Des relations (2.2.1) et (2.2.2), on déduit que :

$$div(x) = 2P_0 - 2P_\infty.$$

(ii) Calculons : $div(x - (4-\sqrt{15}))$.
Notons tout d'abord que : $div(x-\gamma) = div(X-\gamma Z) - div(Z) = (X = \gamma Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.
$div(x - (4-\sqrt{15})) = (X = (4-\sqrt{15})Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = (4-\sqrt{15})Z$, on déduit que : $Y^2 = 0$ ou $Z = 0$.
  On obtient donc les points $P_1 = [4-\sqrt{15} : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 1 respectivement. D'où

$$\Big(X = (4-\sqrt{15})Z\Big)\cdot\mathcal{C} = 2P_1 + P_\infty. \tag{2.2.3}$$

- De même pour $Z = 0$, cela implique : $X^3 = 0$.
  On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 3. D'où

$$(Z = 0)\cdot\mathcal{C} = 3P_\infty. \tag{2.2.4}$$

  Des relations (2.2.3) et (2.2.4), induisent que :

$$div(x - (4-\sqrt{15})) = 2P_1 - 2P_\infty.$$

NB : On procède de la même manière pour (iii).

(vi) $div(y) = div\left(\dfrac{Y}{Z}\right) = (Y = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $Y = 0$, on a : $X(X - (4-\sqrt{15})Z)(X - (4+\sqrt{15})Z) = 0$.
  On obtient donc les points : $P_0 = [0 : 0 : 1]$, $P_1 = [4-\sqrt{15} : 0 : 1]$,

$P_2 = [4+\sqrt{15} : 0 : 1]$ avec un ordre multiplicité égal à 1 pour chacun des points. D'où

$$(Y = 0)\cdot\mathcal{C} = P_0 + P_1 + P_2 \tag{2.2.5}$$

- Pour $Y = 0$, on retrouve la relation (2.2.2).
  Ainsi des relations (2.2.2) et (2.2.5), entraînent donc que :

$$div(y) = P_0 + P_1 + P_2 - 3P_\infty.$$

CQFD

Corollaire 2.2.3
Les résultats suivants sont des conséquences du Lemme 2.2.2 :

- $j(P_0) = -(j(P_1) + j(P_2))$,
- $2j(P_0) = 2j(P_1) = 2j(P_2) = 0$

Donc les $j(P_i)$ engendrent le même sous-groupe de $\mathcal{J}(\mathbb{Q})$.

Lemme 2.2.4
On a :

$$\mathcal{J}(\mathbb{Q}) = \langle j(P_0)\rangle = \{nj(P_0), \quad avec \quad n \in \{0\,,1\}\}$$

Lemme 2.2.5

- *On a les espaces linéaires suivants :*
  $\mathcal{L}(P_\infty) = \langle\ 1\ \rangle$,
  $\mathcal{L}(2P_\infty) = \langle\ 1,\ x\ \rangle$,
  $\mathcal{L}(3P_\infty) = \langle\ 1,\ x,\ y\rangle$,
  $\mathcal{L}(4P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2\ \right\rangle$,
  $\mathcal{L}(5P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ \right\rangle$,
  $\mathcal{L}(6P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ \right\rangle$,
  $\mathcal{L}(7P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ ,\ yx^2\ \right\rangle$,
  $\mathcal{L}(8P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ ,\ yx^2\ ,\ x^4\ \right\rangle$.
  $\mathcal{L}(9P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ ,\ yx^2\ ,\ x^4\ ,\ yx^3\ \right\rangle$,
  $\mathcal{L}(10P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ ,\ yx^2\ ,\ x^4\ ,\ yx^3\ ,\ x^5\ \right\rangle$,
  $\mathcal{L}(11P_\infty) = \left\langle\ 1,\ x,\ y,\ x^2,\ xy\ ,\ x^3\ ,\ yx^2\ ,\ x^4\ ,\ yx^3\ ,\ x^5\ ,\ yx^4\right\rangle$.
- *Une $\mathbb{Q}$-base de $\mathcal{L}(mP_\infty)$ est donnée par :*

$$\mathcal{B}_m = \left\{\ x^i\ \middle|\ i\in\mathbb{N},\ i \le \frac{m}{2}\right\} \bigcup \left\{\ yx^j\ \middle|\ j\in\mathbb{N},\ j \le \frac{m-3}{2}\right\}$$

Démonstration :
le premier point est une conséquence du théorème de Riemann-Roch. Le second point, on

montre aisément que $\mathcal{B}_m$ est une famille libre, il reste alors à montrer que card $\mathcal{B}_m = \dim \mathcal{L}(mP_\infty)$. Puisque $\mathcal{C}$ est une courbe elliptique donc son genre g est égal à 1. La courbe étant de genre 1, d'après le théorème de Riemann-Roch, on a $\dim \mathcal{L}(mP_\infty) = m-g+1 = m$ si $m \geq 1$. Deux cas sont possibles :

1^{er} **cas :** supposons que m est pair, on pose alors $m = 2h$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h}{2} = h$ de même $j \leq \frac{m-3}{2} \Leftrightarrow j \leq \frac{2h-3}{2} \Leftrightarrow j < h-1 \Longrightarrow j \leq h-2$.

Donc on a :

$$\mathcal{B}_m = \left\{1,\ x,\ \ldots\ldots,\ x^h\right\} \bigcup \left\{y,\ yx,\ \ldots\ldots,\ yx^{h-2}\right\}.$$

On en déduit que : card $\mathcal{B}_m = h + 1 + h - 2 + 1 = 2h = m = \dim \mathcal{L}(mP_\infty)$.

$2^{éme}$ **cas :** supposons que m est impair, on pose alors $m = 2h+1$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Longrightarrow i < h+1 \Longrightarrow i \leqslant h$ de même $j \leq \frac{m-3}{2} \Leftrightarrow j \leq \frac{2h-2}{2} = h - 1$. Donc on a :

$$\mathcal{B}_m = \left\{1,\ x,\ \ldots\ldots,\ x^h\right\} \bigcup \left\{y,\ yx,\ \ldots\ldots,\ yx^{h-1}\right\}.$$

On en déduit que : card $\mathcal{B}_m = h + 1 + h - 1 + 1 = 2h+1 = m = \dim \mathcal{L}(mP_\infty)$.

CQFD

2.3 Démonstration du théorème

2.3.1 Détermination des points rationnels

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 1$. Considérons R_1 le conjugué de Galois de R et notons $t = [R_1 - P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\ ;1\}$ et par suite

$$[R_1 - P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

ainsi, on obtient la formule suivante :

$$[R_1 + nP_0 - (1+n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

D'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + nP_0 - (1+n)P_\infty \qquad \text{avec} \qquad n \in \{0\ ,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

Dans ce cas, on a : $[R_1 - P_\infty] = 0$, impliquant ainsi que R_1 est égal à P_∞.

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + P_0 - 2P_\infty$, donc $f \in \mathcal{L}(2P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1 x$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant $f = a_1 x$ induisant ainsi que $div(f) = 2P_0 - 2P_\infty$, d'ou R_1 s'identifie a P_0.

Conclusion : l'ensemble des points rationnels de la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\mathcal{F}_1 = \{P_0,\ P_\infty\}.$$

CQFD

2.3.2 Détermination des points quadratiques

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Considérons R_1, R_2 les conjugués de Galois de R et notons $t = [R_1 + R_2 - 2P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\ ;1\}$ et par suite

$$[R_1 + R_2 - 2P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + R_2 + nP_0 - (2 + n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

D'après le théorème d'Abel Jacobi , il existe une fonction rationnelle f sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + R_2 + nP_0 - (2 + n)P_\infty \qquad \text{avec} \qquad n \in \{0\ ,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 - 2P_\infty$, donc $f \in \mathcal{L}(2P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1 x$ avec $a_0 \neq 0$ (sinon un des R_i serait égal à P_0, ce qui serait absurde) et $a_1 \neq 0$ (sinon $div(f) = 0$, ce qui serait absurde) . Aux points R_i, on a : $a_0 + a_1 x = 0$, qui donne : $x = -\dfrac{a_0}{a_1}$.

En remplaçant l'expression de x dans $y^2 = x^3 - 8x^2 + x$, on en déduit que :

$$y = \pm\sqrt{\alpha^3 - 8\alpha^2 + \alpha} \qquad \text{avec} \qquad \alpha = -\frac{a_0}{a_1} \in \mathbb{Q}^*$$

On obtient ainsi un ensemble de points quadratiques :

$$\mathcal{F}_2' = \left\{ \left(\alpha, \pm\sqrt{n\alpha^3 - 8\alpha^2 + \alpha} \right) | \alpha \in \mathbb{Q}^* \right\}$$

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + P_0 - 3P_\infty$, donc $f \in \mathcal{L}(3P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1 x + a_3 y$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = a_1 x + a_2 y$ avec $a_1 \neq 0$ et $a_2 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $a_1 x + a_3 y = 0$ ce qui implique que $y = -\left(\frac{a_1}{a_2} x\right)$. En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$x^2 - \left(8 + \psi^2\right) x - 1 = 0 \qquad \text{avec} \qquad \psi = \frac{a_1}{a_2} \in \mathbb{Q}^*$$

On obtient ainsi une famille de points quadratiques :

$$\mathcal{F}_2'' = \left\{ \begin{array}{c} (x, -\psi x) \mid \psi \in \mathbb{Q}^* \text{ et } x \text{ solution de l'équation :} \\ x^2 - \left(8 + \psi^2\right) x - 1 = 0 \end{array} \right\}$$

<u>Conclusion</u> : L'ensemble des points quadratiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\mathcal{F}_2 = \mathcal{F}_2' \bigcup \mathcal{F}_2''$$

CQFD

2.3.3 Détermination des points cubiques

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Considérons R_1, R_2, R_3 les conjugués de Galois de R et notons $t = [R_1 + R_2 + R_3 - 3P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\ ;1\}$ et par suite

$$[R_1 + R_2 + R_3 - 3P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + R_2 + R_3 + nP_0 - (3+n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\,,1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + R_2 + R_3 + nP_0 - (3+n)P_\infty \qquad \text{avec} \qquad n \in \{0\,,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 - 3P_\infty$, donc $f \in \mathcal{L}(3P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1x + a_2y$, avec $a_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_2 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $a_0 + a_1x + a_2y = 0$ ce qui implique que $y = -\left(\frac{a_0}{a_2} + \frac{a_1}{a_2}x\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient :

$$\left(-\left(\frac{a_0}{a_2} + \frac{a_1}{a_2}x\right)\right)^2 = \left(x^3 - 8x^2 + x\right)$$

cette équation peut s'ecrire :

$$(\eta_0 + \eta_1 x)^2 = x^3 - 8x^2 + x \quad \text{avec} \quad \eta_0 = \frac{a_0}{a_2} \in \mathbb{Q}^* \text{ et } \eta_1 = \frac{a_1}{a_2} \in \mathbb{Q}$$

On obtient ainsi une famille de points quartiques :

$$\mathcal{F}_3' = \left\{ (x,\ -(\eta_0 + \eta_1 x)) \;\middle|\; \begin{array}{c} \eta_0 \in \mathbb{Q}^* \text{ et } \eta_1 \in \mathbb{Q} \text{ et } x \text{ solution} \\ \text{de l'équation :} \\ (\eta_0 + \eta_1 x)^2 = x^3 - 8x^2 + x \end{array} \right\}$$

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 + P_0 - 4P_\infty$, donc $f \in \mathcal{L}(4P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1x + a_2x^2 + a_3y$, et puisque $ord_{P_0}f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = a_1x + a_3y + a_2x^2$ avec $a_2 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $a_3 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) . Aux points R_i, on a : $a_1x + a_2x^2 + a_3y = 0$ ce qui implique que $y = -\left(\frac{a_1}{a_3}x + \frac{a_2}{a_3}x^2\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\Big(-\Big(\frac{a_1}{a_3}x \ + \ \frac{a_2}{a_3}x^2\Big)\Big)^2 \ = \ \Big(x^3 \ - \ 8x^2 \ + \ x\Big)$$

cette équation peut s'ecrire :

$$\Big(\frac{a_1}{a_3}x^{\frac{1}{2}} \ + \ \frac{a_2}{a_3}x^{\frac{3}{2}}\Big)^2 \ = \ \Big(x^2 \ - \ 8x \ + \ 1\Big)$$

ce qui correspond aussi à l'équation

$$\Big(\gamma_1 x^{\frac{1}{2}} \ + \ \gamma_2 x^{\frac{3}{2}}\Big)^2 \ = \ x^2 \ - \ 8x \ + \ 1 \quad \text{avec} \quad \gamma_1 \ = \ \frac{a_1}{a_3} \in \mathbb{Q} \text{ et } \gamma_2 = \frac{a_2}{a_3} \in \mathbb{Q}^*$$

On obtient ainsi une famille de points quartiques :

$$\mathcal{F}_3'' \ = \ \left\{ \begin{array}{l|l} \Big(x, \ -\Big(\gamma_1 x \ + \ \gamma_2 x^2\Big)\Big) & \gamma_1 \in \mathbb{Q}, \ \gamma_2 \in \mathbb{Q}^* \text{ et } x \text{ solution} \\ & \text{de l'équation :} \\ & \Big(\gamma_1 x^{\frac{1}{2}} \ + \ \gamma_2 x^{\frac{3}{2}}\Big)^2 \ = \ x^2 \ - \ 8x \ + \ 1 \end{array} \right\}$$

<u>Conclusion</u> : L'ensemble des points cubiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 \ = \ x^3 \ - \ 8x^2 \ + \ x$ est donné par :

$$\mathcal{F}_3 \ = \ \mathcal{F}_3' \bigcup \mathcal{F}_3''$$

CQFD

2.3.4 Détermination des points quartiques

Soit $R \ \in \ \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] \ = \ 4$. Considérons R_1, R_2, R_3, R_4 les conjugués de Galois de R et notons $t \ = \ [R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ - \ 4P_\infty] \ \in \ \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t \ = \ -nj(P_0)$, avec $n \ \in \ \{0 \ ; 1\}$ et par suite

$$[R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ - \ 4P_\infty] \ = \ [nP_\infty \ - \ nP_0] \qquad \text{avec} \qquad n \ \in \ \{0 \ , 1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ + \ nP_0 \ - \ (4 \ + \ n)P_\infty] \ = \ 0 \qquad \text{avec} \qquad n \ \in \ \{0 \ , 1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle

que :

$$div(f) \;=\; R_1 \,+\, R_2 \,+\, R_3 \,+\, R_4 \,+\, nP_0 \,-\, (4 \,+\, n)P_\infty \qquad \text{avec} \qquad n \;\in\; \{0\ ,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n \;=\; 0$ **.**

La formule $(\star)$ devient : $div(f) \;=\; R_1 + R_2 + R_3 + R_4 - 4P_\infty$, donc $f \;\in\; \mathcal{L}(4P_\infty)$, d'après le Lemme 2.2.5, on a : $f \;=\; a_0 \,+\, a_1x \,+\, a_2x^2 \,+\, a_3y$, avec $a_0 \;\neq\; 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_3 \;\neq\; 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $a_0 \,+\, a_1x \,+\, a_2x^2 \,+\, a_3y \;=\; 0$ ce qui équivaux à $y \;=\; -\Big(\dfrac{a_0}{a_3} \,+\, \dfrac{a_1}{a_3}x \,+\, \dfrac{a_2}{a_3}x^2\Big)$.
En remplaçant la valeur de y dans l'expression l'équation de la courbe, on obtient :

$$\Big(-\Big(\frac{a_0}{a_3} \,+\, \frac{a_1}{a_3}x \,+\, \frac{a_2}{a_3}x^2\Big)\Big)^2 \;=\; \Big(x^3 \,-8x^2 \,+\, x\Big)$$

cette équation peut s'ecrire :

$$\Big(\beta_0 \,+\, \beta_1x \,+\, \beta_2x^2\Big)^2 \;=\; x^3 \,-8x^2 \,+\, x \text{ avec } \begin{cases} \beta_0 \;=\; -\dfrac{a_0}{a_3} \;\in\; \mathbb{Q}^* \\ \text{et} \\ \beta_{i\{i\in\{1,\,2\}\}} \;=\; -\dfrac{a_i}{a_3} \;\in\; \mathbb{Q} \end{cases}$$

Ainsi, on obtient une famille de points quartiques :

$$\mathcal{F}_4' \;=\; \left\{ \Big(x,\, -\Big(\beta_0 \,+\, \beta_1x \,+\, \beta_2x^2\Big)\Big) \;\middle|\; \begin{array}{c} \beta_0 \;\in\; \mathbb{Q}^*,\;\; \beta_{i\{i\in\{1,\,2\}\}} \;\in\; \mathbb{Q} \text{ et} \\ \\ x \text{ est solution de l'equation :} \\ \\ \Big(\beta_0 \,+\, \beta_1x \,+\, \beta_2x^2\Big)^2 \;=\; x^3 \,-8x^2 \,+\, x \end{array} \right\}$$

$2^{\acute{e}me}$ **cas :** $n \;=\; 1$**.**

La formule $(\star)$ devient : $div(f) \;=\; R_1 \,+\, R_2 \,+\, R_3 \,+\, R_4 \,+\, P_0 \,-\, 5P_\infty$, donc $f \;\in\; \mathcal{L}(5P_\infty)$, d'après le Lemme 2.2.5, on a : $f \;=\; a_0 \,+\, a_1x \,+\, a_2x^2 \,+\, a_3y \,+\, a_4xy$, et puisque $ord_{P_0}f \;=\; 1$, donc $f(P_0) \;=\; 0$ entraîne donc que $a_0 \;=\; 0$, impliquant ainsi que $f \;=\; a_1x \,+\, a_2x^2 \,+\, a_3y \,+\, a_4xy$ avec $a_4 \;\neq\; 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) . Aux points R_i, on a : $a_1x \,+\, a_2x^2 \,+\, a_3y \,+\, a_4xy \;=\; 0$ ce qui implique que $y \;=\; -\left(\dfrac{a_1x \,+\, a_2x^2}{a_3 \,+\, a_4x}\right)$.
En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient

l'équation suivante :

$$\left(-\frac{a_1x \ + \ a_2x^2}{a_3 \ + \ a_4x}\right)^2 \ = \ x^3 \ - \ 8x^2 \ + \ x$$

cette équation peut s'ecrire :

$$\left(a_1x^{\frac{1}{2}} \ + \ a_2x^{\frac{3}{2}}\right)^2 \ = \ (a_3 \ + \ a_4x)^2\left(x^2 \ - \ 8x \ + \ 1\right)$$

On obtient ainsi une famille de points quartiques :

$$\mathcal{F}_4'' \ = \ \left\{ \begin{array}{l|l} \left(x, \ -\left(\dfrac{a_1x \ + \ a_2x^2}{a_3 \ + \ a_4x}\right)\right) & a_4 \ \neq \ 0 \text{ et } x \text{ solution} \\ & \text{de l'équation :} \\ \left(a_1x^{\frac{1}{2}} \ + \ a_2x^{\frac{3}{2}}\right)^2 \ = \ (a_3 \ + \ a_4x)^2\left(x^2 \ - \ 8x \ + \ 1\right) & \end{array} \right\}$$

Conclusion : L'ensemble des points quartiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 \ = \ x^3 \ - \ 8x^2 \ + \ x$ est donné par :

$$\mathcal{F}_4 \ = \ \mathcal{F}_4' \bigcup \mathcal{F}_4''$$

CQFD

2.3.5 Détermination des points quintiques

Soit $R \ \in \ \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] \ = \ 5$. Considérons R_1, R_2, R_3, R_4, R_5 les conjugués de Galois de R et notons $t \ = \ [R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ + \ R_5 \ - \ 5P_\infty] \ \in \ \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t \ = \ -nj(P_0),$ avec $n \ \in \ \{0 \ ; 1\}$ et par suite

$$[R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ + \ R_5 \ - \ 5P_\infty] \ = \ [nP_\infty \ - \ nP_0] \qquad \text{avec} \qquad n \ \in \ \{0 \ , 1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + R_2 + R_3 + R_4 + R_5 + nP_0 - (5 + n)P_\infty] \ = \ 0 \qquad \text{avec} \qquad n \ \in \ \{0 \ , 1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) \ = \ R_1 \ + \ R_2 \ + \ R_3 \ + \ R_4 \ + \ R_5 \ + \ nP_0 \ - \ (5 \ + \ n)P_\infty \ \text{ avec } \ n \ \in \ \{0 \ , 1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 + R_4 + R_5 - 5P_\infty$, donc $f \in \mathcal{L}(5P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1x + a_2x^2 + a_3y + a_4xy$, avec $a_0 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) $a_4 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde). Aux points R_i, on a : $a_0 + a_1x + a_2x^2 + a_3y + a_4xy = 0$ ce qui implique que $y = -\left(\dfrac{a_0 + a_1x + a_2x^2}{a_3 + a_4x}\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\frac{a_0 + a_1x + a_2x^2}{a_3 + a_4x}\right)^2 = x^3 - 8x^2 + x$$

cette équation peut s'ecrire :

$$\left(a_0 + a_1x + a_2x^2\right)^2 = (a_3 + a_4x)^2\left(x^2 - 8x + 1\right)$$

On obtient ainsi une famille de points quintiques :

$$\mathcal{F}_5'' = \left\{ \begin{array}{l|l} \left(x,\ -\left(\dfrac{a_1x + a_2x^2}{a_3 + a_4x}\right)\right) & a_0 \neq 0,\ a_4 \neq 0 \text{ et } x \text{ solution} \\ & \text{de l'équation :} \\ \left(a_0 + a_1x + a_2x^2\right)^2 = (a_3 + a_4x)^2\left(x^2 - 8x + 1\right) & \end{array} \right\}$$

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 + R_4 + R_5 + P_0 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$, d'après le Lemme 2.2.5, on a : $f = a_0 + a_1x + a_2x^2 + a_3y + a_4xy + a_5x^3$, et puisque $ord_{P_0}f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = a_1x + a_2x^2 + a_3y + a_4xy + a_5x^3$ avec $a_5 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a :

$$y = -\left(\frac{a_1x + a_2x^2 + a_5x^3}{a_3 + a_4x}\right).$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(\frac{a_1x + a_2x^2 + a_5x^3}{a_3 + a_4x}\right)^2 = x^3 - 8x^2 + x$$

cette équation peut s'ecrire :

$$\left(a_1x^{\frac{1}{2}} + a_2x^{\frac{3}{2}} + a_5x^{\frac{5}{2}}\right)^2 = (a_3 + a_4x)^2\left(x^2 - 8x + 1\right)$$

Ainsi, on obtient une famille de points quintiques :

$$\mathcal{F}_5'' = \left\{ \left(x, -\left(\frac{a_1x + a_2x^2 + a_5x^3}{a_3 + a_4x}\right)\right) \middle| \begin{array}{c} a_5 \neq 0 \text{ et } x \text{ solution} \\ \\ \text{de l'équation :} \end{array} \right\}$$

$$\left(a_1x^{\frac{1}{2}} + a_2x^{\frac{3}{2}} + a_5x^{\frac{5}{2}}\right)^2 = (a_3 + a_4x)^2\left(x^2 - 8x + 1\right)$$

Conclusion : L'ensemble des points quintiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\mathcal{F}_5 = \mathcal{F}_5' \bigcup \mathcal{F}_5''$$

CQFD

2.3.6 Détermination des points six-tiques

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 6$. Considérons $R_1,\ R_2,\ R_3,\ R_4,\ R_5,\ R_6$ les conjugués de Galois de R et notons $t = [R_1 + R_2 + R_3 + R_4 + R_5 + R_6 - 6P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\ ;1\}$ et par suite

$$[R_1 + R_2 + R_3 + R_4 + R_5 + R_6 - 6P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + R_2 + R_3 + R_4 + R_5 + R_6 + nP_0 - (6+n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\ ,1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + R_2 + R_3 + R_4 + R_5 + R_6 + nP_0 - (5+n)P_\infty \quad \text{avec} \quad n \in \{0\ ,1\} \quad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 + R_4 + R_5 + R_6 - 6P_\infty$, donc $f \in \mathcal{L}(6P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{3} a_ix^i + b_0y + b_1xy$,

avec a_0 et b_0 non simultanément nul (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_3 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{3} a_i x^i + b_0 y + b_1 xy = 0$ ce qui implique que

$$y = -\left(\frac{\sum_{i=0}^{3} a_i x^i}{b_0 + b_1 x} \right).$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\frac{\sum_{i=0}^{3} a_i x^i}{b_0 + b_1 x} \right)^2 = \left(x^3 - 8x^2 + x \right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{3} a_i x^i \right)^2 = (b_0 + b_1 x)^2 \left(x^3 - 8x^2 + x \right)$$

On obtient ainsi une famille de points six-tiques :

$$\mathcal{F}'_6 = \left\{ \left(x, -\left(\frac{\sum_{i=0}^{3} a_i x^i}{b_0 + b_1 x} \right) \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non sumultanemant nul ,} \\ a_3 \neq 0 \text{ et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum_{i=0}^{3} a_i x^i \right)^2 = (b_0 + b_1 x)^2 \left(x^3 - 8x^2 + x \right) \end{array} \right\}$$

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + R_2 + R_3 + R_4 + R_5 + R_6 + P_0 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{2} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = \sum_{i=1}^{3} a_i x^i + \sum_{j=0}^{2} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $b_2 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) . Aux points R_i, on a : $\sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{2} b_j y x^j = 0$ ce qui implique

que $y \ = \ - \left(\dfrac{\sum\limits_{i=1}^{3} a_i x^i}{\sum\limits_{j=0}^{2} b_j x^j} \right)$.
En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\dfrac{\sum\limits_{i=1}^{3} a_i x^i}{\sum\limits_{j=0}^{2} b_j x^j} \right)^2 \ = \ \left(x^3 \ - \ 8x \ + \ x \right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{3} a_i x^i \right)^2 \ = \ \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^3 \ - \ 8x \ + \ x \right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{3} a_i x^{i-\frac{1}{2}} \right)^2 \ = \ \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^2 \ - \ 8x \ + \ 1 \right)$$

On obtient ainsi une autre famille de points six-tiques :

$$\mathcal{F}_6'' \ = \ \left\{ \left(x, \ - \left(\dfrac{\sum\limits_{i=1}^{3} a_i x^i}{\sum\limits_{j=0}^{2} b_j x^j} \right) \right) \ \middle| \ \begin{array}{c} b_0 \ \neq \ 0, \ b_2 \ \neq \ 0 \text{ et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum\limits_{i=1}^{3} a_i x^{i-\frac{1}{2}} \right)^2 \ = \ \left(\sum\limits_{j=0}^{2} b_j x^j \right)^2 \left(x^2 \ - \ 8x \ + \ 1 \right) \end{array} \right\}$$

<u>Conclusion</u> : L'ensemble des points six-tiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 \ = \ x^3 \ - \ 8x^2 \ + \ x$ est donné par :

$$\mathcal{F}_6 \ = \ \mathcal{F}_6' \bigcup \mathcal{F}_6''$$

CQFD

2.3.7 Détermination des points septiques

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 7$. Considérons $R_1, R_2, R_3, R_4, R_5, R_6, R_7$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots + R_7 - 7P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\,;1\}$ et par suite

$$[R_1 + \ldots\ldots + R_7 - 7P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\,,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots\ldots + R_7 + nP_0 - (7 + n)P_\infty] = 0 \quad \text{avec} \quad n \in \{0\,,1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots + R_7 + nP_0 - (7 + n)P_\infty \quad \text{avec} \quad n \in \{0\,,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_7 - 7P_\infty$, donc $f \in \mathcal{L}(7P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{2} b_j y x^j$, avec a_0 et b_0 non simultanément nul (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $b_2 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{2} b_j y x^j = 0$ ce qui implique que $y = -\left(\dfrac{\sum_{i=0}^{3} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\frac{\sum_{i=0}^{3} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)^2 = \left(x^3 - 8x^2 + x\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{3} a_i x^i\right)^2 = \left(\sum_{j=0}^{2} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$$

On obtient ainsi une famille de points six-tiques :

$$\mathcal{F}_7' = \left\{ \left(x, -\left(\frac{\sum_{i=0}^{3} a_i x^i}{\sum_{j=0}^{2} b_j x^j} \right) \right) \middle| \begin{array}{l} a_0 \text{ et } b_0 \text{ non sumultanemant nul ,} \\ \\ b_2 \neq 0 \text{ et } x \text{ solution de l'équation :} \end{array} \right.$$

$$\left. \left(\sum_{i=0}^{3} a_i x^i \right)^2 = \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \right\}$$

$2^{éme}$ cas : $n = 1$.

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_7 + P_0 - 8P_\infty$, donc $f \in \mathcal{L}(8P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{4} a_i x^i + \sum_{j=0}^{2} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = \sum_{i=1}^{4} a_i x^i + \sum_{j=0}^{2} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_4 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) . Aux points R_i, on a : $\sum_{i=0}^{4} a_i x^i + \sum_{j=0}^{2} b_j y x^j = 0$ ce qui implique que $y = -\left(\frac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j} \right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\frac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j} \right)^2 = \left(x^3 - 8x + x \right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=1}^{4} a_i x^i \right)^2 = \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^3 - 8x + x \right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{4} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^2 - 8x + 1 \right)$$

On obtient ainsi une autre famille de points six-tiques :

$$\mathcal{F}_7'' \;=\; \left\{ \left(x,\; -\left(\frac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j} \right) \right) \;\middle|\; b_0 \;=\; 0,\; a_4 \;=\; 0 \text{ et } x \text{ solution de l'équation : } \left(\sum_{i=1}^{4} a_i x^{i-\frac{1}{2}} \right)^2 \;=\; \left(\sum_{j=0}^{2} b_j x^j \right)^2 \left(x^2 \;-\; 8x \;+\; 1 \right) \right\}$$

Conclusion : L'ensemble des points septiques sur la courbe $\mathcal{C}$ d'équation affine $y^2 \;=\; x^3 \;-\; 8x^2 \;+\; x$ est donné par :

$$\mathcal{F}_7 \;=\; \mathcal{F}_7' \bigcup \mathcal{F}_7''$$

CQFD

2.3.8 Points algébriques de degré au-plus 8

Soit $R \;\in\; \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] \;=\; 8$. Considérons $R_1, \ldots\ldots, R_8$ les conjugués de Galois de R et notons $t \;=\; [R_1 \;+\; \ldots\ldots \;+\; R_8 \;-\; 8P_\infty] \;\in\; \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t \;=\; -nj(P_0)$, avec $n \;\in\; \{0\,;1\}$ et par suite

$$[R_1 \;+\; \ldots\ldots \;+\; R_8 \;-\; 8P_\infty] \;=\; [nP_\infty \;-\; nP_0] \qquad \text{avec} \qquad n \;\in\; \{0\,,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 \;+\; \ldots\ldots \;+\; R_8 \;+\; nP_0 \;-\; (8 \;+\; n)P_\infty] \;=\; 0 \quad \text{avec} \quad n \;\in\; \{0\,,1\}$$

D'après le théorème d'Abel Jacobi , il existe une fonction rationnelle f sur $\mathbb{Q}$ telle que :

$$div(f) \;=\; R_1 \;+\; \ldots \;+\; R_8 \;+\; nP_0 \;-\; (8 \;+\; n)P_\infty \quad \text{avec} \quad n \;\in\; \{0\,,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n \;=\; 0$ **.**

La formule $(\star)$ devient : $div(f) \;=\; R_1 \;+\; \ldots\ldots \;+\; R_8 \;-\; 8P_\infty$, donc $f \;\in\; \mathcal{L}(8P_\infty)$, d'après le Lemme 2.2.5, on a : $f \;=\; \sum_{i=0}^{4} a_i x^i \;+\; \sum_{j=0}^{2} b_j y x^j$, avec a_0 et b_0 non simultanément nul (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_4 \;\neq\; 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points

R_i, on a : $\sum_{i=0}^{4} a_i x^i \ + \ \sum_{j=0}^{2} b_j y x^j \ = \ 0$ ce qui implique que $y \ = \ -\left(\dfrac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient l'équation suivante :

$$\left(-\frac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)^2 \ = \ \left(\sum_{j=0}^{2} b_j x^j\right)^2 \left(x^3 \ - \ 8x^2 \ + \ x\right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=0}^{4} a_i x^i\right)^2 \ = \ \left(\sum_{j=0}^{2} b_j x^j\right)^2 \left(x^3 \ - \ 8x^2 \ + \ x\right)$$

On obtient ainsi une famille de points de degré au-plus 8 :

$$\mathcal{F}'_8 \ = \ \left\{ \left(x, \ -\left(\frac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)\right) \ \middle| \ \begin{array}{l} a_0 \text{ et } b_0 \text{ non sumultanemant nul ,} \\ \\ a_4 \neq 0 \text{ et } x \text{ solution de l'équation :} \\ \\ \left(\sum_{i=0}^{4} a_i x^i\right)^2 \ = \ \left(\sum_{j=0}^{2} b_j x^j\right)^2 \left(x^3 \ - \ 8x^2 \ + \ x\right) \end{array} \right\}$$

$2^{éme}$ **cas :** $n \ = \ 1$**.**

La formule $(\star)$ devient : $div(f) \ = \ R_1 \ + \ \ldots\ldots \ + \ R_8 \ + \ P_0 \ - \ 9P_\infty$, donc $f \ \in \ \mathcal{L}(9P_\infty)$, d'après le Lemme 2.2.5, on a : $f \ = \ \sum_{i=0}^{4} a_i x^i \ + \ \sum_{j=0}^{3} b_j y x^j$, et puisque $ord_{P_0} f \ = \ 1$, donc $f(P_0) \ = \ 0$ entraîne donc que $a_0 \ = \ 0$, impliquant ainsi que $f \ = \ \sum_{i=1}^{4} a_i x^i \ + \ \sum_{j=0}^{3} b_j y x^j$ avec $b_0 \ \neq \ 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $b_3 \ \neq \ 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) . Aux points R_i, on a : $\sum_{i=0}^{4} a_i x^i \ + \ \sum_{j=0}^{3} b_j y x^j \ = \ 0$ ce qui implique que $y \ = \ -\left(\dfrac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j}\right)$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe ; on obtient

l'équation suivante :

$$\left(-\frac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right)^2 \;=\; \left(x^3 \;-\; 8x \;+\; x\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{4} a_i x^i\right)^2 \;=\; \left(\sum_{j=0}^{3} b_j x^j\right)^2 \left(x^3 \;-\; 8x \;+\; x\right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{4} a_i x^{i-\frac{1}{2}}\right)^2 \;=\; \left(\sum_{j=0}^{3} b_j x^j\right)^2 \left(x^2 \;-\; 8x \;+\; 1\right)$$

On obtient ainsi une autre famille de points de degré au-plus 8 :

$$\mathcal{F}_8'' \;=\; \left\{ \left(x,\; -\left(\frac{\sum_{i=1}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right) \right) \;\middle|\; \begin{array}{c} b_0 \;\neq\; 0,\; b_3 \;\neq\; 0 \text{ et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum_{i=1}^{4} a_i x^{i-\frac{1}{2}}\right)^2 \;=\; \left(\sum_{j=0}^{3} b_j x^j\right)^2 \left(x^2 \;-\; 8x \;+\; 1\right) \end{array} \right\}$$

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

$$\mathcal{F}_8 \;=\; \mathcal{F}_8' \bigcup \mathcal{F}_8''$$

CQFD

2.3.9 Points algébriques de degré au-plus 9

Soit $R \;\in\; \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] \;=\; 9$. Considérons $R_1, \ldots\ldots, R_8$ les conjugués de Galois de R et notons $t \;=\; [R_1 \;+\; \ldots\ldots \;+\; R_9 \;-\; 9P_\infty] \;\in\; \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t \;=\; -nj(P_0)$, avec $n \;\in\; \{0\,;1\}$ et par suite

$$[R_1 \;+\; \ldots\ldots \;+\; R_9 \;-\; 9P_\infty] \;=\; [nP_\infty \;-\; nP_0] \qquad \text{avec} \qquad n \;\in\; \{0\,,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 \ + \ ..... \ + \ R_9 \ + \ nP_0 \ - \ (9 \ + \ n)P_\infty] \ = \ 0 \qquad \text{avec} \qquad n \ \in \ \{0 \ , 1\}$$

D'après le théorème d'Abel Jacobi , il existe une fonction rationnelle f sur $\mathbb{Q}$ telle que :

$$div(f) \ = \ R_1 \ + \ ..... \ + \ R_9 \ + \ nP_0 \ - \ (9 \ + \ n)P_\infty \quad \text{avec} \quad n \ \in \ \{0 \ , 1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n \ = \ 0$ **.**

La formule $(\star)$ devient : $div(f) \ = \ R_1 \ + \ ..... \ + \ R_9 \ - \ 9P_\infty$, donc $f \ \in \ \mathcal{L}(9P_\infty)$, d'après le Lemme 2.2.5, on a : $f \ = \ \sum_{i=0}^{4} a_i x^i \ + \ \sum_{j=0}^{3} b_j y x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $b_3 \ \neq \ 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{4} a_i x^i \ + \ \sum_{j=0}^{3} b_j y x^j \ = \ 0$, qui donne : $y \ = \ -\dfrac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j}$. En remplaçant l'expression de y dans l'expression de l'équation de la courbe, on obtient l'équation suivante :

$$\left(-\frac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right)^2 \ = \ \left(x^3 \ - \ 8x^2 \ + \ x \right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{4} a_i x^i \right)^2 = \left(\sum_{j=0}^{3} b_j x^j \right)^2 \left(x^3 \ - \ 8x^2 \ + \ x \right)$$

On obtient ainsi une famille de points de degré au-plus 9 :

$$\mathcal{F}'_9 \ = \ \left\{ \left(x, \ -\frac{\sum_{i=0}^{4} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right) \ \middle| \ \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } b_3 \neq 0 \text{ et} \\ \\ x \text{ solution de l'équation :} \\ \\ \left(\sum_{i=0}^{4} a_i x^i \right)^2 = \left(\sum_{j=0}^{3} b_j x^j \right)^2 \left(x^3 \ - \ 8x^2 \ + \ x \right) \end{array} \right\}$$

$2^{éme}$ **cas :** $n \ = \ 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_9 + P_0 - 10P_\infty$, donc $f \in \mathcal{L}(10P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{5} a_i x^i + \sum_{j=0}^{3} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = \sum_{i=1}^{5} a_i x^i + \sum_{j=0}^{3} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_5 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{5} a_i x^i + \sum_{j=0}^{3} b_j y x^j = 0$, ce qui implique

$$y = -\frac{\sum_{i=1}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j}.$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=1}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right)^2 = \left(x^3 - 8x^2 + x \right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{5} a_i x^i \right)^2 = \left(\sum_{j=0}^{3} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right)$$

ce qui correspond à l'équation :

$$\left(\sum_{i=1}^{5} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum_{j=0}^{3} b_j x^j \right)^2 \left(x - (4-\sqrt{15}) \right) \left(x - (4+\sqrt{15}) \right)$$

On obtient ainsi une famille de points de degré 9 :

$$\mathcal{F}_9'' = \left\{ \begin{array}{l|c} \left(x, \ -\dfrac{\sum_{i=1}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right) & b_0 \neq 0, \ a_5 \neq 0 \text{ et } x \text{ solution} \\ & \text{de l'équation :} \\ \left(\sum_{i=1}^{5} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum_{j=0}^{3} b_j x^j \right)^2 \left(x - (4-\sqrt{15}) \right) \left(x - (4+\sqrt{15}) \right) & \end{array} \right\}$$

Conclusion : L'ensemble des points algébriques de degré au-plus 9 sur la courbe $\mathcal{C}$

d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\mathcal{F}_9 = \mathcal{F}'_9 \bigcup \mathcal{F}''_9$$

CQFD

2.3.10 Points algébriques de degré au-plus 10

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 10$. Considérons $R_1, \ldots\ldots, R_{10}$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots + R_{10} - 10P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\,;1\}$ et par suite

$$[R_1 + \ldots\ldots + R_{10} - 10P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\,,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots\ldots + R_{10} + nP_0 - (10 + n)P_\infty] = 0 \quad \text{avec} \quad n \in \{0\,,1\}$$

D'après le théorème d'Abel Jacobi , il existe une fonction rationnelle f sur $\mathbb{Q}$ telle que :

$$[R_1 + \ldots\ldots + R_{10} + nP_0 - (10 + n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\,,1\}$$

D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots\ldots + R_{10} + nP_0 - (10 + n)P_\infty \quad \text{avec} \quad n \in \{0\,,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_{10} - 10P_\infty$, donc $f \in \mathcal{L}(10P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{5} a_i x^i + \sum_{j=0}^{2} b_j y x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $a_5 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{5} a_i x^i + \sum_{j=0}^{2} b_j y x^j = 0$, qui donne : $y = -\dfrac{\sum_{i=0}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j}$.

En remplaçant la valeurs de y dans l'expression de l'équation de la courbe, on ob-

tient :

$$\left(-\frac{\sum_{i=0}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j}\right)^2 = \left(x^3 - 8x^2 + x\right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=0}^{5} a_i x^i\right)^2 = \left(\sum_{j=0}^{3} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$$

On obtient ainsi une famille de points de degré 10 :

$$\mathcal{F}'_{10} = \left\{ \left(x, -\frac{\sum_{i=0}^{5} a_i x^i}{\sum_{j=0}^{3} b_j x^j} \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_5 \neq 0 \text{ et} \\ x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{5} a_i x^i\right)^2 = \left(\sum_{j=0}^{3} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right) \end{array} \right\}$$

$2^{éme}$ **cas :** $n = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_{10} + P_0 - 11P_\infty$, donc $f \in \mathcal{L}(11P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{5} a_i x^i + \sum_{j=0}^{4} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = \sum_{i=1}^{5} a_i x^i + \sum_{j=0}^{4} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) et $b_3 \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{5} a_i x^i + \sum_{j=0}^{4} b_j y x^j = 0$, ce qui implique $y = -\frac{\sum_{i=1}^{5} a_i x^i}{\sum_{j=0}^{2} b_j x^j}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=1}^{5} a_i x^i}{\sum_{j=0}^{2} b_j x^j}\right)^2 = \left(\sum_{j=0}^{4} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=1}^{5} a_i x^i\right)^2 = \left(\sum_{j=0}^{4} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$$

ce qui correspond à l'équation :

$$\left(\sum_{i=1}^{5} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{4} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4+\sqrt{15})\right) \qquad (2.3.1)$$

On obtient ainsi une famille de points de degré au-plus 10 :

$$\mathcal{F}''_{10} = \left\{ \begin{array}{l|l} \left(x,\ -\dfrac{\sum_{i=0}^{5} a_i x^i}{\sum_{j=0}^{4} b_j x^j} \right) & b_0 \neq 0,\ b_4 \neq 0 \text{ et } x \text{ solution} \\ & \text{de l'équation :} \\ \left(\sum_{i=1}^{5} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{4} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4+\sqrt{15})\right) & \end{array} \right\}$$

Conclusion : L'ensemble des points algébrique de degré au-plus 10 sur la courbe $\mathcal{C}$ d'équation affine $y^2 = x^3 - 8x^2 + x$ est donné par :

$$\mathcal{F}_{10} = \mathcal{F}'_{10} \bigcup \mathcal{F}''_{10}$$

CQFD

2.3.11 Points algébriques de degré au-plus ℓ

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = \ell$. Considérons $R_1, \ldots\ldots, R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots + R_\ell - \ell P_\infty] \in \mathcal{J}(\mathbb{Q})$, d'après le Lemme 2.2.4, on a $t = -nj(P_0)$, avec $n \in \{0\,;1\}$ et par suite

$$[R_1 + \ldots\ldots + R_\ell - \ell P_\infty] = [nP_\infty - nP_0] \qquad \text{avec} \qquad n \in \{0\,,1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots\ldots + R_\ell + nP_0 - (\ell + n)P_\infty] = 0 \qquad \text{avec} \qquad n \in \{0\,,1\}$$

D'après le théorème d'Abel Jacobi , il existe une fonction rationnelle sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots\ldots + R_\ell + nP_0 - (\ell + n)P_\infty \qquad \text{avec} \qquad n \in \{0\,,1\} \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$ **.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_\ell - \ell P_\infty$, donc $f \in \mathcal{L}(\ell P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde), $a_{\frac{\ell}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-3}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j = 0$, qui donne : $y = -\dfrac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \tag{2.3.2}$$

L'équation (2.3.2) est une équation de degré ℓ en x.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation est de degré égal à $2\left(\dfrac{\ell}{2}\right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\dfrac{\ell-3}{2}\right) + 3 = \ell$.

On obtient ainsi une famille de points de degré au-plus ℓ :

$$\mathcal{F}'_\ell = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls , } a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est impair et} \\ x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j \right)^2 \left(x^3 - 8x^2 + x \right) \end{array} \right\}$$

$2^{éme}$ cas : $n = 1$.

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_\ell + P_0 - (\ell+1)P_\infty$, donc $f \in \mathcal{L}((\ell+1)P_\infty)$, d'après le Lemme 2.2.5, on a : $f = \sum_{i=0}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-2}{2}} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc $f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi que $f = \sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-2}{2}} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde), $a_{\frac{\ell+1}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-2}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-2}{2}} b_j y x^j = 0$, ce qui implique $y = -\dfrac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-2}{2}} b_j x^j}$. En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-2}{2}} b_j x^j}\right)^2 = \left(x^3 - 8x^2 + x\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{\ell-2}{2}} b_j x^j\right)^2 \left(x^3 - 8x^2 + x\right)$$

ce qui correspond à l'équation :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{\frac{\ell-2}{2}} b_j x^j\right)^2 \left(x - (4-\sqrt{15})\right)\left(x - (4+\sqrt{15})\right) \qquad (2.3.3)$$

L'expression (2.3.3) est une équation de degré ℓ en x.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation est de degré égal à $2\left(\dfrac{\ell+1}{2} - \dfrac{1}{2}\right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\dfrac{\ell-2}{2}\right) + 2 = \ell$.

On obtient ainsi une famille de points de degré ℓ :

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

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

$$\mathcal{F}_\ell \;=\; \mathcal{F}'_\ell \bigcup \mathcal{F}''_\ell$$

CQFD

Chapitre 3

Points algébriques de degré quelconque sur certaines courbes lisses

3.1 Points algébriques de degré donné quelconque sur la courbe d'équation affine : $y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$

3.1.1 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 sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leqslant\ell} \mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire qu'on a $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera par $\mathcal{J}$ la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe

notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

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

où $\mathcal{J}(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (cf [6]).
Notre courbe $\mathcal{C}$ qui est lisse d'équation affine $y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ est un cas spécial de la famille de courbes

$$\mathcal{C} : y^2 = q(x^2 - 2)(x^2 + x)(x^2 + 1), \qquad \text{avec} \qquad q \equiv 13[24]$$

où q est un nombre premier, étudiées dans [6].
Notre courbe $\mathcal{C} : y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ est d'équation projective :

$$\left(\frac{Y}{Z}\right)^2 = 109\left(\left(\frac{X}{Z}\right)^2 - 2\right)\left(\left(\frac{X}{Z}\right)^2 + \left(\frac{X}{Z}\right)\right)\left(\left(\frac{X}{Z}\right)^2 + 1\right) \qquad (*)$$

qui peut s'ecrire

$$Z^4Y^2 = 109X(X + Z)(X - \sqrt{2}Z)(X + \sqrt{2}Z)(X - \zeta Z)(X + \zeta Z) \qquad (**)$$

ce qui correspond aussi à l'équation affine

$$y^2 = 109x(x + 1)(x - \sqrt{2})(X + \sqrt{2})(X - \zeta)(X + \zeta) \quad \text{avec} \quad \zeta^2 = -1 \quad (**)$$

On note $P_0,\ P_1,\ P_2,\ P_3,\ P_4,\ P_5$ et P_∞ les points de $\mathcal{C}$, définis par : $P_0 = [0 : 0 : 1]$, $P_1 = [-1 : 0 : 1]$, $P_2 = [\sqrt{2} : 0 : 1]$, $P_3 = [-\sqrt{2} : 0 : 1]$, $P_4 = [\zeta : 0 : 1]$, $P_5 = [-\zeta : 0 : 1]$ et $P_\infty = [1 : 0 : 0]$.
Dans cette note, on détermine l'ensemble :

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

Notre résultat principal est s'énonce comme suit :

Théorème 1
L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ est donné par :

$$\mathcal{S} = \mathcal{S}_1 \bigcup \mathcal{S}_2 \bigcup \mathcal{S}_3 \bigcup \mathcal{S}_4$$

avec :

$$\mathcal{S}_1 = \left\{ \left(x,\ -\frac{\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}}}{\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_0 \text{ et } c_0 \text{ non simultanemants nuls,} \\ b_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-7}{2}} \neq 0 \text{ si} \\ \ell \text{ est impair et } x \text{ solution de l'équation :} \end{array} \right\}$$

$$\left(\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}} \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1) \Bigg\}$$

$$\mathcal{S}_2 = \left\{ \left(x,\ -\frac{a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \\ \text{est impair et } x \text{ solution de} \\ \text{l'équation :} \end{array} \right\}$$

$$\left(a\left(\frac{x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}}{x}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(\frac{x^i + (-1)^i}{x}\right) \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1) \Bigg\}$$

$$\mathcal{S}_3 = \left\{ \left(x,\ -\frac{a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i \left(x^i + \omega^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right\}$$

$$\left(a\left(\frac{x^{\frac{5}{2}} + \psi}{x}\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i \left(\frac{x^i + \omega^i}{x}\right) \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1)$$

avec

$$\psi = -\frac{1}{2}\left(\left(-\sqrt{2}\right)^{\frac{5}{2}} + \left(\sqrt{2}\right)^{\frac{5}{2}}\right) \quad et \quad \omega^i = -\frac{1}{2}\left(\left(-\sqrt{2}\right)^i + \left(\sqrt{2}\right)^i\right) \Bigg\}$$

$$\mathcal{S}_4 = \left\{ \begin{array}{l} \left(x,\ -\dfrac{a\left(x^{\frac{5}{2}}+\mu\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\nu^i\right)}{\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \Bigg| \begin{array}{l} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \\ \left(a\left(\dfrac{x^{\frac{5}{2}}+\mu}{x}\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(\dfrac{x^i+\nu^i}{x}\right)\right)^2 = 109\left(\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \\ \text{avec} \\ \mu = -\dfrac{1}{2}\left((\zeta)^{\frac{5}{2}}+(-\zeta)^{\frac{5}{2}}\right) \quad \text{et} \quad \nu^i = -\dfrac{1}{2}\left((\zeta)^i+(-\zeta)^i\right) \end{array} \right\}$$

3.1.2 Résultats auxiliaires

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

Lemme 3.1.1
On a : $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Démonstration : (voir [6, page 8])

Lemme 3.1.2
Pour la courbe $\mathcal{C} : y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ *qui est donnée aussi par :*

$$\mathcal{C} : y^2 = 109x(x + 1)(x - \sqrt{2})(x + \sqrt{2})(x + \zeta)(x - \zeta).$$

On a :

(i) $div(x) = 2P_0 - 2P_\infty$,

(ii) $div(x + 1) = 2P_1 - 2P_\infty$,

(iii) $div(x + \sqrt{2}) = 2P_2 - 2P_\infty$,

(iv) $div(x - \sqrt{2}) = 2P_3 - 2P_\infty$,

(v) $div(x + \zeta) = 2P_4 - 2P_\infty$,

(vi) $div(x - \zeta) = 2P_5 - 2P_\infty$,

(vii) $div(y) = P_0 + P_1 + P_2 + P_3 + P_4 + P_5 - 6P_\infty$.

Démonstration :
Notons x, y les coordonnées affines et X, Y et Z les coordonnées projectives. Posons : $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$.

(i) $div(x) = div\left(\dfrac{X}{Z}\right) = (X = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = 0$, on déduit de $(**)$ que : $Y^2 = 0$ ou $Z^4 = 0$.
  On obtient donc les points : $P_0 = [0 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 4 respectivement. D'où

$$(X = 0)\cdot\mathcal{C} = 2P_0 + 4P_\infty \tag{3.1.1}$$

- De même pour $Z = 0$, cela implique que : $X^6 = 0$.
  On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 6. D'où

$$(Z = 0)\cdot\mathcal{C} = 6P_\infty. \tag{3.1.2}$$

  Des relations (3.1.1) et (3.1.2), on déduit que :

$$div(x) = 2P_0 - 2P_\infty.$$

(ii) calculons : $div(x + 1)$.
Notons tout d'abord que : $div(x - \gamma) = div(X - \gamma Z) - div(Z) = (X = \gamma Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.
$div(x + 1) = (X = -Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = -Z$, on déduit que : $Y^2 = 0$ ou $Z^4 = 0$.
  On obtient donc les points $P_1 = [-1 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 4 respectivement. D'où

$$(X = Z)\cdot\mathcal{C} = 2P_1 + 4P_\infty. \tag{3.1.3}$$

- Pour $Z = 0$, on retrouve la relation (3.1.2).
  Ainsi des relations (3.1.2) et (3.1.3), entraînent donc que :

$$div(x + 1) = 2P_1 - 2P_\infty.$$

NB : On procède de la même manière pour les cas (iii), (ii), (iv) et (v).

(vi) $div(y) = div\left(\dfrac{Y}{Z}\right) = (Y = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $Y = 0$, on a :

$$109X(X + Z)(X - \sqrt{2}Z)(X + \sqrt{2}Z)(X - \zeta Z)(X + \zeta Z) = 0.$$

On obtient donc les points : $P_0 = [0 : 0 : 1]$, $P_1 = [-1 : 0 : 1]$, $P_2 = [\sqrt{2} : 0 : 1]$, $P_3 = [-\sqrt{2} : 0 : 1]$, $P_4 = [\zeta : 0 : 1]$ et $P_5 = [-\zeta : 0 : 1]$ avec un ordre multiplicité égal à 1 pour chaque points. D'où

$$(Y = 0) \cdot \mathcal{C} = P_0 + P_1 + P_2 + P_3 + P_4 + P_5 \tag{3.1.4}$$

- Pour $Z = 0$, on retrouve la relation (3.1.2).
Ainsi les relations (3.1.2) et (3.1.4), on déduit que :

$$div(y) = P_0 + P_1 + P_2 + P_3 + P_4 + P_5 - 6P_\infty.$$

CQFD

Corollaire 3.1.3
Les résultats suivants sont les conséquences du Lemme 3.1.2 :

- $j(P_0) + j(P_1) + j(P_2) + j(P_3) + j(P_4) + j(P_5) = 0$,
- $2j(P_0) = 2j(P_1) = 2j(P_3) = 2j(P_4) = 2j(P_5) = 0$

Donc les $j(P_i)$ engendrent le même sous-groupe $\mathcal{J}(\mathbb{Q})$.

Lemme 3.1.4
On a :

$$\begin{aligned}\mathcal{J}(\mathbb{Q}) &= \langle [P_0 + P_1 - 2P_\infty],\ [P_1 + P_2 - 2P_\infty] \rangle \\ &= \{-\alpha\,(j(P_0) + j(P_1)) - \beta\,(j(P_2) + j(P_3)),\ où\ \alpha,\ \beta \in \{0\ ,\ 1\}\}\end{aligned}$$

Lemme 3.1.5
Une $\mathbb{Q}$-base de $\mathcal{L}(mP_\infty)$ est donnée par :

$$\mathcal{B}_m = \left\{ x^i \;\middle|\; i \in \mathbb{N},\ i \leq \frac{m}{2} \right\} \bigcup \left\{ yx^{\frac{2j+1}{2}} \;\middle|\; j \in \mathbb{N},\ j \leq \frac{m-7}{2} \right\} \bigcup \left\{ x^{\frac{5}{2}} \right\}$$

Démonstration :
On montre aisément que $\mathcal{B}_m$ est une famille libre, il reste alors à montrer que card $\mathcal{B}_m = \dim \mathcal{L}(mP_\infty)$. La courbe étant de genre 2 (voir [6]), d'après le théorème de Riemann-Roch, on a $\dim \mathcal{L}(mP_\infty) = m - g + 1 = m - 1$ dès que $m \geq 2g - 1 = 3$.
Deux cas sont possibles :

1^{er} **cas :** supposons que m est pair, on pose alors $m = 2h$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h}{2} = h$ de même $j \leq \frac{m-7}{2} \Leftrightarrow j \leq \frac{2h-7}{2} \Leftrightarrow j \leq h - \frac{7}{2}$
$\Longrightarrow j < h - \frac{6}{2} = h - 3 \Longrightarrow j \leqslant h - 4$. Donc on a :

$$\mathcal{B}_m = \left\{x^{\frac{5}{2}}\right\} \bigcup \left\{1,\ x,\ \ldots, x^h\right\} \bigcup \left\{yx,\ \ldots, yx^{h-4}\right\}.$$

On en déduit que :

$$\text{card}\ \mathcal{B}_m = 1 + h + 1 + h - 4 + 1 = 2h - 1 = m - 1 = \dim \mathcal{L}(mP_\infty).$$

$2^{éme}$ **cas :** supposons que m est impair, on pose alors $m = 2h + 1$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Longrightarrow i < h + 1 \Longrightarrow i \leqslant h$ de même $j \leq \frac{m-7}{2} \Leftrightarrow j \leq \frac{2h-6}{2} = h - 3$. Donc on a :

$$\mathcal{B}_m = \left\{x^{\frac{5}{2}}\right\} \bigcup \left\{1,\ x,\ \ldots, x^h\right\} \bigcup \left\{yx,\ \ldots, yx^{h-3}\right\}.$$

On en déduit que :

$$\text{card}\ \mathcal{B}_m = 1 + h + 1 + h - 3 + 1 = 2h = m - 1 = \dim \mathcal{L}(mP_\infty).$$

CQFD

3.1.3 Démonstration du Théorème 1

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = \ell$. Considérons $R_1, \ldots\ldots, R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots + R_\ell - \ell P_\infty] \in \mathcal{J}(\mathbb{Q})$. D'après le Lemme 3.1.4, on a $t = -\alpha\,(j(P_0) + j(P_1)) - \beta\,(j(P_2) + j(P_3))$, $\alpha,\ \beta \in \{0,\ 1\}$ et par suite

$$[R_1 + \ldots + R_\ell - \ell P_\infty] = [(2\alpha + 2\beta)P_\infty - \alpha\,(P_0 + P_1) - \beta\,(P_2 + P_3)]$$

où
$\mathcal{J}(\mathbb{Q}) = \{\alpha P_0 + \alpha P_1 + \beta P_2 + \beta P_3 - (2\alpha + 2\beta)P_\infty$, où $\alpha,\ \beta \in \{0\ ,\ 1\}\}$;
donc $t = \alpha P_0 + \alpha P_1 + \beta P_2 + \beta P_3 - (2\alpha + 2\beta)P_\infty$, avec $\alpha,\ \beta \in \{0,\ 1\}$, ce qui donne :

$$[R_1 + \ldots + R_\ell - \ell P_\infty] = [\alpha P_0 + \alpha P_1 + \beta P_2 + \beta P_3 - (2\alpha + 2\beta)P_\infty], \text{avec}\ \alpha,\ \beta \in \{0,\ 1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots + R_\ell + \alpha(P_0 + P_1) + \beta(P_2 + P_3) - (\ell + 2\alpha + 2\beta)P_\infty] = 0$$

D'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots + R_\ell + \alpha(P_0 + P_1) + \beta(P_2 + P_3) - (\ell + 2\alpha + 2\beta)P_\infty \qquad (\star)$$

Quatre cas sont possibles :

1^{er} **cas :** $\alpha = \beta = 0$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell - \ell P_\infty$, donc $f \in \mathcal{L}(\ell P_\infty)$. D'après le Lemme 3.1.5, on a : $f = ax^{\frac{5}{2}} + \sum_{i=0}^{\frac{\ell}{2}} b_i x^i + \sum_{j=0}^{\frac{\ell-7}{2}} c_j y x^{\frac{2j+1}{2}}$ avec b_0 et c_0 non simultanément tous nul (sinon un des R_i devrait être égal à P_0, ce qui serais absurde), $b_{\frac{\ell}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serais absurde) et $c_{\frac{\ell-7}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serais absurde). Aux points R_1, on a : $ax^{\frac{5}{2}} + \sum_{i=0}^{\frac{\ell}{2}} b_i x^i + \sum_{j=0}^{\frac{\ell-7}{2}} c_j y x^{\frac{2j+1}{2}} = 0$, impliquant ainsi, $y = -\dfrac{\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + ax^{\frac{5}{2}}}{\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + ax^{\frac{5}{2}}}{\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}}\right)^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + ax^{\frac{5}{2}}\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \qquad (3.1.5)$$

L'expression (3.1.5) est une équation de degré ℓ en x :
En effet, quelque soit la parité de ℓ, le premier membre de l'équation (3.1.5) est de degré $2 \times \left(\frac{\ell}{2}\right) = \ell$ et le second membre est de degré

$$2 \times \left(\frac{2 \times (\frac{\ell-7}{2}) + 1}{2} \right) + 6 = \ell.$$

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{S}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}}}{\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_0 \text{ et } c_0 \text{ non simultanemants nuls,} \\ b_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-7}{2}} \neq 0 \text{ si} \\ \ell \text{ est impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} b_i x^i + a x^{\frac{5}{2}} \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-7}{2}} c_j x^{\frac{2j+1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1) \end{array} \right\}$$

$2^{éme}$ **cas :** $\alpha = 1$ **et** $\beta = 0$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_0 + P_1 - (\ell + 2)P_\infty$, donc $f \in \mathcal{L}((\ell+2)P_\infty)$, d'après le Lemme 3.1.5, on a : $f = a x^{\frac{5}{2}} + \sum_{i=0}^{\frac{\ell+2}{2}} b_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$, et puisque $ord_{P_0} f = ord_{P_1} f = 1$, entraine donc que $b_0 = 0$ et $b_1 = a(-1)^{\frac{5}{2}} + \sum_{i=2}^{\frac{\ell+2}{2}} b_i (-1)^i$ implique ainsi que

$$f = a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right) + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$$

avec $b_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $c_{\frac{\ell-5}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde).

Aux points R_i, on a :

$$a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right) + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}} = 0,$$

ce implique que $y = -\dfrac{a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on

obtient :

$$\left(-\frac{a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right)^2 = 109(x^2-2)(x^2+x)(x^2+1)$$

cette équation peut s'ecrire :

$$\left(a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right) \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1)$$

ce qui correspond aussi à l'équation :

$$\left(a\left(\frac{x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}}{x}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(\frac{x^i + (-1)^i}{x}\right) \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1) \quad (3.1.6)$$

L'expression (3.1.6) est une équation de degré ℓ.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation (3.1.6) est de degré $2 \times \left(\frac{\ell+2}{2} - 1\right) = \ell$ et le second membre est de degré $2\left(\frac{2 \times (\frac{\ell-5}{2}) - 1}{2}\right) + 6 = \ell$.

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{S}_2 = \left\{ \left(x,\ -\frac{a\left(x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(x^i + (-1)^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{c} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \\ \text{est impair et } x \text{ solution de} \\ \text{l'équation :} \end{array} \right\}$$

$$\left(a\left(\frac{x^{\frac{5}{2}} + (-1)^{\frac{5}{2}}}{x}\right) + \sum_{i=2}^{\frac{\ell+2}{2}} b_i \left(\frac{x^i + (-1)^i}{x}\right) \right)^2 = 109 \left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}} \right)^2 (x^2-2)(x^2+x)(x^2+1) \Bigg\}$$

$3^{éme}$ **cas :** $\alpha = 0$ **et** $\beta = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_2 + P_3 - (\ell+2)P_\infty$, donc $f \in \mathcal{L}((\ell+2)P_\infty)$, d'après le Lemme 3.1.5, on a :

$f = ax^{\frac{5}{2}} + \sum_{i=0}^{\frac{\ell+2}{2}} b_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$ et puisque $ord_{P_2} f = ord_{P_3} f = 1$, entraine donc que :

$$b_0 = -\frac{1}{2}\left(a\left(\left(-\sqrt{2}\right)^{\frac{5}{2}} + \left(\sqrt{2}\right)^{\frac{5}{2}}\right)\right) - \frac{1}{2}\left(\sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(\left(-\sqrt{2}\right)^{i} + \left(\sqrt{2}\right)^{i}\right)\right).$$

En posant : $\psi = -\frac{1}{2}\left(\left(-\sqrt{2}\right)^{\frac{5}{2}} + \left(\sqrt{2}\right)^{\frac{5}{2}}\right)$ et $\omega^i = -\frac{1}{2}\left(\left(-\sqrt{2}\right)^{i} + \left(\sqrt{2}\right)^{i}\right)$,
on déduit que $b_0 = a\psi + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\omega^i$ implique que

$$f = a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \omega^i\right) + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$$

avec $b_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $c_{\frac{\ell-5}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde).

Aux points R_i, on a : $a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \omega^i\right) + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}} = 0,$

ce qui impliquant que $y = -\dfrac{a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \omega^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \omega^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}}\right)^2 = 109(x^2-2)(x^2+x)(x^2+1)$$

cette équation peut s'ecrire :

$$\left(a\left(x^{\frac{5}{2}} + \psi\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \omega^i\right)\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1)$$

Ce qui correspond aussi à l'équation :

$$\left(a\left(\frac{x^{\frac{5}{2}} + \psi}{x}\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(\frac{x^i + \omega^i}{x}\right)\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \quad (3.1.7)$$

L'expression (3.1.7) est une équation de degré ℓ.

En effet : quelque soit la parité de ℓ, le premier membre de l'équation (3.1.7) est de degré $2\left(\frac{\ell+2}{2}-1\right) = \ell$ et le second membre est de degré $2\left(\frac{2\times(\frac{\ell-5}{2})-1}{2}\right)+6 = \ell$. On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{S}_3 = \left\{ \begin{array}{l} \left(x,\ -\dfrac{a\left(x^{\frac{5}{2}}+\psi\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\omega^i\right)}{\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \left| \begin{array}{l} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \left(a\left(\dfrac{x^{\frac{5}{2}}+\psi}{x}\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(\dfrac{x^i+\omega^i}{x}\right)\right)^2 = 109\left(\sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \\ \text{avec} \\ \psi = -\dfrac{1}{2}\left(\left(-\sqrt{2}\right)^{\frac{5}{2}}+\left(\sqrt{2}\right)^{\frac{5}{2}}\right) \quad \text{et} \quad \omega^i = -\dfrac{1}{2}\left(\left(-\sqrt{2}\right)^i+\left(\sqrt{2}\right)^i\right) \end{array} \right\}$$

$4^{éme}$ **cas : $\alpha = 1$ et $\beta = 1$.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_0 + P_1 + P_2 + P_3 - (\ell+4)P_\infty$. Par le Corollaire 3.1.3, on en déduit que : $div(f) = R_1 + \ldots + R_\ell + P_4 + P_5 - (\ell+2)P_\infty$, donc $f \in \mathcal{L}((\ell+2)P_\infty)$, d'après le Lemme 3.1.5, on a : $f = ax^{\frac{5}{2}} + \sum\limits_{i}^{\frac{\ell+2}{2}} b_i x^i + \sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$, et puisque $ord_{P_4} f = ord_{P_5} f = 1$, entraîne donc que : $b_0 = -\dfrac{1}{2}\left(a\left((\zeta)^{\frac{5}{2}}+(-\zeta)^{\frac{5}{2}}\right)\right) - \dfrac{1}{2}\left(\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left((\zeta)^i+(-\zeta)^i\right)\right)$.

En posant $\mu = -\dfrac{1}{2}\left((\zeta)^{\frac{5}{2}}+(-\zeta)^{\frac{5}{2}}\right)$ et $\nu^i = -\dfrac{1}{2}\left((\zeta)^i+(-\zeta)^i\right)$, on déduit que : $b_0 = a\left(x^{\frac{5}{2}}+\mu\right)+\sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\nu^i\right)$, implique que

$$f = a\left(x^{\frac{5}{2}}+\mu\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\nu^i\right) + \sum_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}}$$

avec $b_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $c_{\frac{\ell-5}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde).

Aux points R_i, on a : $a\left(x^{\frac{5}{2}}+\mu\right) + \sum\limits_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i+\nu^i\right) + \sum\limits_{j=0}^{\frac{\ell-5}{2}} c_i y x^{\frac{2j+1}{2}} = 0$,

impliquant ainsi, $y = -\dfrac{a\left(x^{\frac{5}{2}} + \mu\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \nu^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{a\left(x^{\frac{5}{2}} + \mu\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \nu^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}}\right)^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$$

cette équation peut s'ecrire :

$$\left(a\left(x^{\frac{5}{2}} + \mu\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \nu^i\right)\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}\right)^2 (x^2 - 2)(x^2 + x)(x^2 + 1)$$

ce qui correspond aussi à l'équation :

$$\left(a\left(\frac{x^{\frac{5}{2}} + \mu}{x}\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(\frac{x^i + \nu^i}{x}\right)\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2-2)(x^2+x)(x^2+1) \quad (3.1.8)$$

L'expression (3.1.8) est une équation de degré ℓ.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation (3.1.8) est de degré $2\left(\dfrac{\ell+2}{2} - 1\right) = \ell$ et le second membre est de degré $2\left(\dfrac{2 \times (\frac{\ell-5}{2}) - 1}{2}\right) + 6 = \ell$.

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{S}_4 = \left\{ \left(x,\ -\frac{a\left(x^{\frac{5}{2}} + \mu\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(x^i + \nu^i\right)}{\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j+1}{2}}} \right) \middle| \begin{array}{l} b_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } c_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right.$$

$$\left(a\left(\frac{x^{\frac{5}{2}} + \mu}{x}\right) + \sum_{i=1}^{\frac{\ell+2}{2}} b_i\left(\frac{x^i + \nu^i}{x}\right)\right)^2 = 109\left(\sum_{j=0}^{\frac{\ell-5}{2}} c_i x^{\frac{2j-1}{2}}\right)^2 (x^2 - 2)(x^2 + x)(x^2 + 1)$$

avec

$$\mu = -\frac{1}{2}\left((\zeta)^{\frac{5}{2}} + (-\zeta)^{\frac{5}{2}}\right) \quad \text{et} \quad \nu^i = -\frac{1}{2}\left((\zeta)^i + (-\zeta)^i\right) \Bigg\}$$

Conclusion : L'ensemble des points algébriques de degré au-plus ℓ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 109(x^2 - 2)(x^2 + x)(x^2 + 1)$ est donné par :

$$\mathcal{S} = \mathcal{S}_1 \bigcup \mathcal{S}_2 \bigcup \mathcal{S}_3 \bigcup \mathcal{S}_4$$

CQFD

3.2 Points algébriques de degré donné quelconque sur la courbe d'équation affine : $y^2 = (x - 74)(x^2 - 2738)(x^2 + 5476)$

3.2.1 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 sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leqslant\ell} \mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire qu'on a $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera par $\mathcal{J}$ la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien :

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

où $\mathcal{J}(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (voir [6]).
Notre courbe $\mathcal{C}$ qui est lisse d'équation affine $y^2 = (x - 74)(x^2 - 2730)(x^2 + 5476)$ est un cas spécial de famille de courbes

$$\mathcal{C}_q : y^2 = (x - 2q)(x^2 - 2q^2)(x^2 + 2^2q^2), \qquad \text{avec} \qquad q \equiv 13[24]$$

et q un nombre premier, étudiées dans [6, page 8].
Notre courbe $\mathcal{C} : y^2 = (x - 74)(x^2 - 2730)(x^2 + 5476)$ est d'équations projectives

$$Z^3Y^2 = (X - 74Z)(X^2 - 2730Z^2)(X^2 + 5476Z^2) \qquad (*)$$

qui peut s'ecrire

$$\mathcal{C} : \begin{cases} Z^3\left(Y - 5476\sqrt{37}Z\right)\left(Y + 5476\sqrt{37}Z\right) = X(X^4 - 74X^3Z + 2738X^2Z^2 - 405224XZ^3 \\ \qquad\qquad -14993288Z^4) \qquad (1) \\ \qquad\qquad \text{ou} \\ Z^3Y^2 = (X - 74Z)(X - 37\sqrt{2}Z)(X + 37\sqrt{2}Z)(X - 74\zeta Z)(X + 74\zeta Z) \text{ où } \zeta^2 = -1 \qquad (2) \end{cases}$$

ce qui correspond aussi aux équations affines :

$$\mathcal{C} : \begin{cases} \left(y - 5476\sqrt{37}\right)\left(y + 5476\sqrt{37}\right) = x(x^4 - 74x^3 + 2738x^2 - 405224x - 14993288) \\ \qquad\qquad \text{ou} \\ y^2 = (x - 74)(x - 37\sqrt{2})(x + 37\sqrt{2})(x - 74\zeta)(x + 74\zeta) \text{ avec } \zeta^2 = -1 \end{cases}$$

On note $P_0,\ P_1,\ P_2,\ P_3,\ P_4,\ P_5,\ P_6$ et ∞ les points sur $\mathcal{C}$, définis par : $P_0 = [74 : 0 : 1]$, $P_1 = [37\sqrt{2} : 0 : 1]$, $P_2 = [-37\sqrt{2} : 0 : 1]$, $P_3 = [74\zeta : 0 : 1]$, $P_4 = [-74\zeta : 0 : 1]$, $P_5 = [0 : 5476\sqrt{37} : 1]$, $P_6 = [0 : -5476\sqrt{37} : 1]$ et $\infty = [0 : 1 : 0]$.
Dans cette note, on détermine l'ensemble :

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

Notre résultat principal est s'énonce comme suit :

Théorème 2
L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = (x - 74)(x^2 - 2730)(x^2 + 5476)$ est donné par :

$$\mathcal{M} = \mathcal{M}_1 \bigcup \mathcal{M}_2 \bigcup \mathcal{M}_3 \bigcup \mathcal{M}_4$$

avec

$$\mathcal{M}_1 = \left\{ \left(x,\ -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair,} \\ b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \end{array} \right\}$$

$$\mathcal{M}_2 = \left\{ \left(x,\ -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i)}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \middle| \begin{array}{l} a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-4}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right.$$
$$\left. \left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i \left(\frac{x^i - (74)^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \right\}$$

$$\mathcal{M}_3 = \left\{ \left(x,\ -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair , } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right.$$
$$\left. \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \xi^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \right\}$$
$$\text{avec}$$
$$\xi^i = -\frac{1}{2}\left((37\sqrt{2})^i + (-37\sqrt{2})^i\right)$$

$$\mathcal{M}_4 = \left\{ \left(x,\ -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair , } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right.$$
$$\left. \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \gamma^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \right\}$$
$$\text{avec}$$
$$\gamma^i = -\frac{1}{2}\left((74\zeta)^i + (-74\zeta)^i\right)$$

3.2.2 Résultats auxiliaires

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

Lemme 3.2.1
On a : $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Démonstration : (voir [6, page 8])

Lemme 3.2.2
Pour notre courbe $\mathcal{C} : y^2 = (x - 74)(x^2 - 2730)(x^2 + 5476)$ *qui est aussi donnée par :*

$$\mathcal{C} : \begin{cases} \left(y - 5476\sqrt{37}\right)\left(y + 5476\sqrt{37}\right) = x(x^4 - 74x^3 + 2738x^2 - 405224x - 14993288) \\ \qquad\qquad ou \\ y^2 = (x - 74)(x - 37\sqrt{2})(x + 37\sqrt{2})(x - 74\zeta)(x + 74\zeta) \text{ avec } \zeta^2 = -1 \end{cases}$$

On a :

(i) $div(x) = P_5 + P_6 - 2\infty$,

(ii) $div(x - 74) = 2P_0 - 2\infty$,

(iii) $div(x - 37\sqrt{2}) = 2P_1 - 2\infty$,

(iv) $div(x + 37\sqrt{2}) = 2P_2 - 2\infty$,

(v) $div(x - 74\zeta) = 2P_3 - 2\infty$,

(vi) $div(x + 74\zeta) = 2P_4 - 2\infty$,

(vii) $div(y) = P_0 + P_1 + P_2 + P_3 + P_4 - 5\infty$.

Démonstration :
Notons x et y les coordonnées affines et X, Y, Z les coordonnées projectives. Posons : $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$.

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

- Pour $X = 0$, on déduit de (1) que : $Z^3\left(Y - 5476\sqrt{37}Z\right)\left(Y + 5476\sqrt{37}Z\right) = 0$.
  On obtient donc les points $P_5 = [0 : 5476\sqrt{37} : 1]$, $P_6 = [0 : -5476\sqrt{37} : 1]$ et $\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 1, 1 et 3 respectivement.
  D'où
  $$(X = 0) \cdot \mathcal{C} = P_5 + P_6 + 3\infty. \tag{3.2.1}$$

- De même pour $Z = 0$, on déduit de (2) que : $X^5 = 0$.
  On obtient donc le point $\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal 5. D'où
  $$(Z = 0) \cdot \mathcal{C} = 5\infty. \tag{3.2.2}$$

Des relations (3.2.1) et (3.2.2), induisent que :

$$div(x) = P_5 + P_6 - 2\infty.$$

(ii) $div(x - 74) = (X = 74Z) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C}$.

- Pour $X = 74Z$, on déduit de (2) que : $Y^2 = 0$ ou $Z^3 = 0$.
  On obtient donc les points $P_0 = [74 : 0 : 1]$ et $\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 3 respectivement. D'où

$$(X = 74Z) \cdot \mathcal{C} = 2P_0 + 3\infty. \tag{3.2.3}$$

- Pour $Z = 0$, on obtient la relation (3.2.2).

$$(Z = 0) \cdot \mathcal{C} = 5\infty. \tag{3.2.4}$$

Des relations (3.2.3) et (3.2.4), induisent que :

$$div(x - 74) = 2P_0 - 2\infty$$

.

NB : On procède de la même manière pour les cas (iii), (iv), (v) et (vi).

(ii) $div(y) = div(\frac{Y}{Z}) = (Y = 0) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C}$.

- Pour $Y = 0$, (2) implique que :

$$(X - 74Z)(X - 37\sqrt{2}Z)(X + 37\sqrt{2}Z)(X - 74\zeta Z)(X + 74\zeta Z) = 0.$$

On obtient donc les points : $P_0 = [74 : 0 : 1]$, $P_1 = [37\sqrt{2} : 0 : 1]$, $P_2 = [-37\sqrt{2} : 0 : 1]$, $P_3 = [74\zeta : 0 : 1]$ et $P_4 = [-74\zeta : 0 : 1]$ avec un ordre multiplicité égal 1 pour chaque points. D'où

$$(Y = 0) \cdot \mathcal{C} = P_0 + P_1 + P_2 + P_3 + P_4 \tag{3.2.5}$$

- Pour $Z = 0$, revient à l'obtention de la relation (3.2.2).
  Ainsi des relations (3.2.5) et (3.2.2), entraînent donc que :

$$div(y) = P_0 + P_1 + P_2 + P_3 + P_4 - 5\infty.$$

CQFD

Corollaire 3.2.3

Les résultats suivants sont les conséquences du Lemme 3.2.2 :

- $j(P_5) + j(P_6) = 0$,
- $j(P_0) + j(P_1) + j(P_2) + j(P_3) + j(P_4) = 0$.
- $2j(P_0) = 2j(P_1) = 2j(P_3) = 2j(P_4) = 0$.

Donc les $2j(P_i)$ pour $i \in \{0, 1, 2, 3, 4\}$ engendrent le même sous-groupe $\mathcal{J}(\mathbb{Q})$.

Lemme 3.2.4
On a :

$$\begin{aligned}\mathcal{J}(\mathbb{Q}) &= \langle [P_0 - \infty] \ , \ [P_1 + P_2 - 2\infty] \rangle \\ &= \{\alpha j(P_0) + \beta\,(j(P_2) + j(P_3))\,, \ avec \ \alpha, \ \beta \in \{0 \ , \ 1\}\}\end{aligned}$$

Démonstration : (voir [6, page 8]).

Lemme 3.2.5
Une $\mathbb{Q}$-base de $\mathcal{L}(mP_\infty)$ est donnée par :

$$\mathcal{B}_m = \left\{ x^i \;\middle|\; i \in \mathbb{N},\ i \leq \frac{m}{2} \right\} \bigcup \left\{ yx^j \;\middle|\; j \in \mathbb{N},\ j \leq \frac{m-5}{2} \right\}$$

Démonstration :
On montre aisément que $\mathcal{B}_m$ est une famille libre, il reste alors à montrer que card $\mathcal{B}_m = \dim \mathcal{L}(m\infty)$. On sait que le genre de $\mathcal{C}$ est $g = 2$ (voir [6]). La courbe étant de genre 2, d'après le théorème de Riemann-Roch, on a $\dim \mathcal{L}(m\infty) = m - g + 1 = m - 1$ dès que $m \geq 2g - 1 = 3$.
Deux cas sont possibles :

1^{er} **cas :** supposons que m est pair, on pose alors $m = 2h$, on obtient ainsi :
$i \leq \dfrac{m}{2} \Leftrightarrow i \leq \dfrac{2h}{2} = h$ de même $j \leq \dfrac{m-5}{2} \Leftrightarrow j \leq \dfrac{2h-5}{2} \Leftrightarrow j \leq h - \dfrac{5}{2}$
$\Longrightarrow j < h - \dfrac{4}{2} = h - 2 \Longrightarrow j \leqslant h - 3$. Donc on a :

$$\mathcal{B}_m = \left\{1,\ x,\ \ldots\ldots,x^h\right\} \bigcup \left\{y,\ yx,\ \ldots\ldots,yx^{h-3}\right\}.$$

On en déduit que :

$$\text{card } \mathcal{B}_m = h + 1 + h - 3 + 1 = 2h - 1 = m - 1 = \dim \mathcal{L}(m\infty).$$

$2^{éme}$ **cas :** supposons que m est impair, on pose alors $m = 2h + 1$, on obtient ainsi :
$i \leq \dfrac{m}{2} \Leftrightarrow i \leq \dfrac{2h+1}{2} \Leftrightarrow i \leq h + \dfrac{1}{2} \Longrightarrow i < h + 1 \Longrightarrow i \leqslant h$ de même $j \leq \dfrac{m-5}{2} \Leftrightarrow j \leq \dfrac{2h-4}{2} = h - 2$. Donc on a :

$$\mathcal{B}_m = \left\{1,\ x,\ \ldots\ldots,x^h\right\} \bigcup \left\{y,\ yx,\ \ldots\ldots,yx^{h-3}\right\}.$$

On en déduit que :

$$\text{card}\,\mathcal{B}_m = h + 1 + h - 3 + 1 = 2h - 1 = m - 1 = \dim \mathcal{L}(m\infty).$$

CQFD

3.2.3 Démonstration du Théorème 2

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = \ell$. Considérons $R_1, \ldots\ldots, R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots + R_\ell - \ell\infty] \in \mathcal{J}(\mathbb{Q})$. D'après le Lemme 3.2.4, on a $[R_1 + \ldots + R_\ell - \ell\infty] = -\alpha j(P_0) - \beta\,(j(P_1) + j(P_2))$ avec $\alpha,\ \beta \in \{0\ ,\ 1\}$ et par suite

$$[R_1{+}\ldots{+}R_\ell{-}\ell\infty] = [(\alpha + 2\beta)\infty - \alpha P_0 - \beta\,(P_1 + P_2)]\,,\ \text{avec}\ \alpha,\ \beta \in \{0,\ 1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots\ldots + R_\ell + \alpha P_0 + \beta\,(P_1 + P_2) - (\ell + \alpha + 2\beta)\infty] = 0$$

D'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots\ldots + R_\ell + \alpha P_0 + \beta\,(P_1 + P_2) - (\ell + \alpha + 2\beta)\infty \qquad (\star)$$

Quatre cas sont possibles :

1^{er} **cas :** $\alpha = 0$ **et** $\beta = 0$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell - \ell\infty$, donc $f \in \mathcal{L}(\ell\infty)$, d'après le Lemme 3.2.5, on a : $f = \sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde), $a_{\frac{\ell}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à ∞, ce qui serait absurde) et $b_{\frac{\ell-5}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à ∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y x^j = 0$, ce qui implique que : $y = -\dfrac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on

obtient :

$$\left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right)^2 = (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \qquad (3.2.6)$$

L'équation (3.2.6) est une équation de degré ℓ en x :
En effet, quelque soit la parité de ℓ, le membre de l'équation est de degré égal à $2\left(\frac{\ell}{2}\right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\frac{\ell-5}{2}\right) + 5 = \ell$.
On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{M}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right) \middle| \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair ,} \\ b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \end{array} \right\}$$

$2^{éme}$ **cas : $\alpha = 1$ et $\beta = 0$.**
La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_0 - (\ell + 1)\infty$, donc $f \in \mathcal{L}((\ell + 1)\infty)$, d'après le Lemme 3.2.5, on a $f = \sum_{i=0}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j$, et puisque $ord_{P_0} = 1$, entraine donc que $a_0 = -\sum_{i=1}^{\frac{\ell+1}{2}} a_i (74)^i$, impliquant ainsi que $f = \sum_{i=1}^{\frac{\ell+1}{2}} a_i (x^i - (74)^i) + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j$ avec $a_{\frac{\ell+1}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-4}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux

points R_i, on a : $\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i) + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j = 0$, ce qui implique que

$$y = -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i)}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j}.$$

En remplaçant la valeur de y dans l'expression de l'équation, on obtient :

$$\left(-\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i)}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j}\right)^2 = (x-74)\left(x^2-2730\right)\left(x^2+5476\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i)\right)^2 = \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j\right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i\left(\frac{x^i-(74)^i}{x}\right)\right)^2 = \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^{j-1}\right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \quad (3.2.7)$$

L'expression (3.2.7) est une équation de degré ℓ en x.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation est de degré égal à $2 \times \left(\frac{\ell+1}{2} - 1\right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\frac{\ell-4}{2} - 1\right) + 5 = \ell$. On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{M}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i(x^i - (74)^i)}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \middle| \begin{array}{l} a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair , } b_{\frac{\ell-4}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i\left(\frac{x^i-(74)^i}{x}\right)\right)^2 = \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^{j-1}\right)^2 (x-74)\left(x^2-2730\right)\left(x^2+5476\right) \end{array} \right\}$$

$3^{éme}$ cas : $\alpha = 0$ et $\beta = 1$.

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_1 + P_2 - (\ell+2)\infty$, donc $f \in \mathcal{L}((\ell+2)\infty)$, d'après le Lemme 3.2.5, on a $f = \sum_{i=0}^{\frac{\ell+2}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j$, et puisque $ord_{P_1} f = ord_{P_2} f = 1$, entraine donc que

$a_0 = -\frac{1}{2}\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left((37\sqrt{2})^i + (-37\sqrt{2})^i\right)\right)$ en posant

$\xi^i = -\frac{1}{2}\left((37\sqrt{2})^i + (-37\sqrt{2})^i\right)$, on obtient $a_0 = \sum_{i=1}^{\frac{\ell+2}{2}} a_i \xi^i$, impliquant ainsi que $f = \sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j$ avec $a_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-3}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à ∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j = 0$, ce qui implique que

$$y = -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j}.$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j}\right)^2 = (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i)\right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j\right)^2 (x-74)\left(x^2 - 2730\right)\left(x^2 + 5476\right)$$

Ce qui équivaux à l'équation :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i\left(\frac{x^i + \xi^i}{x}\right)\right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1}\right)^2 (x-74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \quad (3.2.8)$$

L'expression (3.2.8) est une équation de degré ℓ en x :
En effet, quelque soit la parité de ℓ, le premier membre de l'équation est de

degré égal à $2 \times \left(\frac{\ell+2}{2} - 1\right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\frac{\ell-3}{2} - 1\right) + 5 = \ell$.

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{M}_3 = \left\{ \left(x, \ -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \xi^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \middle| \ a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair }, \ b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est impair et } x \text{ solution de l'équation :} \right.$$

$$\left. \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \xi^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \right\}$$

avec

$$\xi^i = -\frac{1}{2}\left((37\sqrt{2})^i + (-37\sqrt{2})^i\right)$$

$4^{éme}$ **cas :** $\alpha = \beta = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_0 + P_1 + P_2 - (\ell + 3)\infty$. Par le Corollaire 3.2.3, on en déduit que : $div(f) = R_1 + \ldots + R_\ell + P_3 + P_4 - (\ell + 2)\infty$, donc $f \in \mathcal{L}((\ell + 2)\infty)$, d'après le Lemme 3.2.5, on a $f = \sum_{i=0}^{\frac{\ell+2}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j$, et puisque $ord_{P_3} f = ord_{P_4} f = 1$, entraine donc que

$a_0 = -\frac{1}{2}\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left((74\zeta)^i + (-74\zeta)^i\right)\right)$ en posant $\gamma^i = -\frac{1}{2}\left((74\zeta)^i + (-74\zeta)^i\right)$, on obtient $a_0 = \sum_{i=1}^{\frac{\ell+2}{2}} a_i \gamma^i$, implique que $f = \sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j$ avec $a_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à ∞, ce qui serait absurde) et $b_{\frac{\ell-3}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à ∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y x^j = 0$, ce qui implique $y = -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on

obtient l'équation :

$$\left(-\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right)^2 = (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right)$$

cette équation peut s'écrire :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right)$$

Cette équation équivaux à :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \gamma^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \quad (3.2.9)$$

L'expression (3.2.9) est une équation de degré ℓ en x :
En effet, quelque soit la parité de ℓ, le premier membre de l'équation est de degré égal à $2 \times \left(\frac{\ell+2}{2} - 1 \right) = \ell$ et le second membre de l'équation est de degré égal à $2 \times \left(\frac{\ell-3}{2} - 1 \right) + 5 = \ell$.
On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{M}_4 = \left\{ \begin{array}{l} \left(x,\ -\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i(x^i + \gamma^i)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^j} \right) \Bigg| \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair },\ b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \\ \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \gamma^i}{x} \right) \right)^2 = \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j-1} \right)^2 (x - 74)\left(x^2 - 2730\right)\left(x^2 + 5476\right) \\ \text{avec} \\ \gamma^i = -\frac{1}{2}\left((74\zeta)^i + (-74\zeta)^i \right) \end{array} \right\}$$

Conclusion : L'ensemble des points algébriques de degré au-plus ℓ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = (x - 74)(x^2 - 2738)(x^2 + 5476)$ est donné par :

$$\mathcal{M} = \mathcal{M}_1 \bigcup \mathcal{M}_2 \bigcup \mathcal{M}_3 \bigcup \mathcal{M}_4$$

CQFD

3.3 Points algébriques de degré donné quelconque sur la courbe d'équation affine : $y^2 = 6x(x^4 + 3)$

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 sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leqslant\ell} \mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire qu'on a $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera par $\mathcal{J}$ la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

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

où $\mathcal{J}(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$.
Notre courbe $\mathcal{C}$ qui est lisse d'équation affine $y^2 = 6x(x^4 + 3)$ est d'écrite dans [13].
Notre courbe $\mathcal{C} : y^2 = 6x(x^4 + 3)$ est d'équation projective

$$Z^3Y^2 = 6X(X^4 + 3) \qquad (*)$$

qui peut s'ecrire

$$Z^3Y^2 = 6X\prod_{k=0}^{3}(X - \eta_k Z) \quad \text{avec} \quad \eta_k = \sqrt[4]{3}\exp^{(\frac{2k+1}{4})\pi i} \qquad (**)$$

ce qui correspond aussi à l'équation affine

$$y^2 = 6x\prod_{k=0}^{3}(x - \eta_k) \quad \text{avec} \quad \eta_k = \sqrt[4]{3}\exp^{(\frac{2k+1}{4})\pi i}$$

On note $P_0,\ P_1,\ P_2,\ P_3,\ P_4$ et P_∞ les points sur $\mathcal{C}$, définis par : $P_0 = [\eta_0 : 0 : 1]$, $P_1 = [\eta_1 : 0 : 1]$, $P_2 = [\eta_2 : 0 : 1]$, $P_3 = [\eta_3 : 0 : 1]$, $P_4 = [0 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$.
Dans cette note on détermine l'ensemble :

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

Notre résultat principal est s'énonce comme suit :

Théorème 3
L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $y^2 = 6x(x^4 + 3)$ est donné par :

$$\mathcal{H} = \mathcal{H}_1 \bigcup \mathcal{H}_2$$

avec

$$\mathcal{H}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair }, b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair} \\ \text{et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = 6x \left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x^4 + 3) \end{array} \right\}$$

$$\mathcal{H}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} b_0 \neq 0, \; a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-4}{2}} \neq 0 \\ \text{si } \ell \text{ est impair et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 = 6 \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_i x^j\right)^2 (x^4 + 3) \end{array} \right\}$$

3.3.2 Résultats auxiliaires

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

Lemme 3.3.1
On a : $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

Lemme 3.3.2
Pour la courbe $\mathcal{C} : y^2 = 6x(x^4 + 3)$ qui est aussi donnée par :

$$\mathcal{C} : y^2 = 6x \prod_{k=0}^{3} (x - \eta_k) \qquad avec \qquad \eta_k = \sqrt[4]{3} \exp^{(\frac{2k+1}{4})\pi i}.$$

On a :

(*i*) $div(x) = 2P_4 - 2P_\infty$,

(*ii*) $div(x + \eta_k) = 2P_k - 2P_\infty$, *avec* $k \in \{0, 1, 2, 3\}$

(iii) $div(y) = P_0 + P_1 + P_2 + P_3 + P_4 - 5P_\infty$.

Démonstration :
Notons x, y les coordonnées affines et X, Y, Z les coordonnes projectives.
Posons : $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$.

(i) $div(x) = div\left(\dfrac{X}{Z}\right) = (X = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = 0$, on déduit de $(**)$ que : $Y^2 = 0$ ou $Z^3 = 0$.
  On obtient donc les points : $P_4 = [0 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 4 respectivement. D'où

$$(X = 0)\cdot\mathcal{C} = 2P_4 + 3P_\infty \tag{3.3.1}$$

- De même pour $Z = 0$, on déduit de $(**)$ que : $X^5 = 0$.
  On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal 5. D'où

$$(Z = 0)\cdot\mathcal{C} = 5P_\infty. \tag{3.3.2}$$

  Des relations (3.3.1) et (3.3.2), induisent que :

$$div(x) = 2P_4 - 2P_\infty.$$

(ii) Notons que :
$div(x - \eta_i) = div(X - \eta_k Z) - div(Z) = (X = \eta_k Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = -\eta_k Z$, on déduit de $(**)$ que : $Y^2 = 0$ ou $Z^3 = 0$.
  On obtient donc les points $P_k = [\eta_k : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 3 respectivement. D'où

$$(X = \eta_k Z)\cdot\mathcal{C} = 2P_k + 3P_\infty. \tag{3.3.3}$$

- Pour $Z = 0$, on retrouve la relation (3.3.2).
  Ainsi des relations (3.3.2) et (3.3.3), entraînent donc que :

$$div(x + \eta_k) = 2P_k - 2P_\infty.$$

(vi) $div(y) = div\left(\dfrac{Y}{Z}\right) = (Y = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $Y = 0$, équivaux à : $6X\prod_{k=0}^{3}(X + \eta_k Z) = 0$.
  On obtient donc les points : $P_0 = [\eta_0 : 0 : 1]$, $P_1 = [\eta_1 : 0 : 1]$,

$P_2 = [\eta_2 : 0 : 1]$, $P_3 = [\eta_3 : 0 : 1]$ et $P_4 = [0 : 0 : 1]$ avec un ordre multiplicité égal 1 pour chaque points. D'où

$$(Y = 0) \cdot \mathcal{C} = P_0 + P_1 + P_2 + P_3 + P_4 \tag{3.3.4}$$

- Pour $Z = 0$, on retrouve la relation (3.3.2).
  Ainsi les relations (3.3.2) et (3.3.4), on déduit que :

$$div(y) = P_0 + P_1 + P_2 + P_3 + P_4 - 5P_\infty.$$

CQFD

Corollaire 3.3.3
Les résultats suivants sont les conséquences du Lemme 3.3.2 :

- $j(P_0) + j(P_1) = -(j(P_2) + j(P_3) + j(P_4) + j(P_5))$,
- $2j(P_0) = 2j(P_1) = 2j(P_3) = 2j(P_4) = 2j(P_5) = 0$

Donc les $j(P_k)$ où $k \in \{0, \ldots, 5\}$ engendrent le même sous-groupe $\mathcal{J}(\mathbb{Q})$

Lemme 3.3.4
On a :

$$\mathcal{J}(\mathbb{Q}) = \langle j(P_4) \rangle = \{\alpha j(P_4), \text{ avec } \alpha \in \{0, 1\}\}$$

Démonstration : (voir [13, page 8], *Lemme 1.1.1*)

Lemme 3.3.5
Une $\mathbb{Q}$-base de $\mathcal{L}(mP_\infty)$ est donnée par :

$$\mathcal{B}_d = \left\{ x^i \;\middle|\; i \in \mathbb{N},\ i \leq \frac{m}{2} \right\} \bigcup \left\{ yx^j \;\middle|\; j \in \mathbb{N},\ j \leq \frac{m-5}{2} \right\}$$

Démonstration :
On montre aisément que $\mathcal{B}_m$ est une famille libre, il reste alors à montrer que card $\mathcal{B}_m = \dim \mathcal{L}(mP_\infty)$. On sait que le genre de $\mathcal{C}$ est $g = 2$ (voir [13]). La courbe étant de genre 2, d'après le théorème de Riemann-Roch, on a $\dim \mathcal{L}(mP_\infty) = m - g + 1 = m - 1$ dès que $m \geq 2g - 1 = 3$.
Deux cas sont possibles :

1^{er} **cas :** supposons que d est pair, on pose alors $m = 2h$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h}{2} = h$ de même $j \leq \frac{m-5}{2} \Leftrightarrow j \leq \frac{2h-5}{2} \Leftrightarrow j \leq h - \frac{5}{2}$
$\Longrightarrow j < h - \frac{4}{2} = h - 2 \Longrightarrow j \leqslant h - 3$. Donc on a :

$$\mathcal{B}_m = \left\{1, x, \ldots\ldots, x^h\right\} \bigcup \left\{y, yx, \ldots\ldots, yx^{h-3}\right\}.$$

On en déduit que :

$$\text{card}\,\mathcal{B}_m = h + 1 + h - 3 + 1 = 2h-1 = m-1 = \dim \mathcal{L}(mP_\infty).$$

$2^{éme}$ **cas :** supposons que m est impair, on pose alors $m = 2h+1$, on obtient ainsi :
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Longrightarrow i < h+1 \Longrightarrow i \leqslant h$ de même $j \leq \frac{m-5}{2} \Leftrightarrow j \leq \frac{2h-4}{2} = h - 2$. Donc on a :

$$\mathcal{B}_m = \left\{1,\ x,\ \ldots\ldots\ ,x^h\right\} \bigcup \left\{y,\ yx,\ \ldots\ldots\ ,yx^{h-2}\right\}.$$

On en déduit que :

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

CQFD

3.3.3 Démonstration du Théorème 3

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = \ell$. Considérons $R_1, \ldots\ldots, R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots + R_\ell - \ell P_\infty] \in \mathcal{J}(\mathbb{Q})$. D'après le Lemme 3.3.4, on a $t = -\alpha j(P_4)$, avec $\alpha \in \{0,\ 1\}$ et par suite

$$[R_1 + \ldots + R_\ell - \ell P_\infty] = [\alpha P_\infty - \alpha P_4]$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots + R_\ell + \alpha P_4 - (\alpha + \ell)P_\infty] = 0 \quad \text{avec } \alpha \in \{0,\ 1\}$$

d'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots + R_\ell + \alpha P_4 - (\alpha + \ell)P_\infty \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $\alpha = 0$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell - \ell P_\infty$, donc $f \in \mathcal{L}(\ell P_\infty)$. D'après le Lemme 3.3.5, on a : $f = \sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y x^j$ avec a_0, a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_4, ce qui serais

absurde), $a_{\frac{\ell}{2}} \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serais absurde) et $b_{\frac{\ell-5}{2}} \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serais absurde). Aux points R_1, on a : $\sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y x^j = 0$, impliquant ainsi,

$$y = -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j}.$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j}\right)^2 = 6x(x^4 + 3).$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = 6x\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x^4 + 3). \tag{3.3.5}$$

L'expression (3.3.5) est une équation de degré ℓ en x.

En effet : quelque soit la parité de ℓ, le premier membre de l'équation (3.3.5) est de degré $2 \times \left(\frac{\ell}{2}\right) = \ell$ et le second membre est de degré

$2 \times \left(\frac{2 \times (\frac{\ell-5}{2}) + 1}{2}\right) + 5 = \ell.$

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{H}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \\ \text{si } \ell \text{ est pair }, b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair} \\ \text{et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i\right)^2 = 6x\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j\right)^2 (x^4 + 3) \end{array} \right\}$$

$2^{éme}$ **cas :** $\alpha = 1$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_4 - (\ell + 1)P_\infty$, donc $f \in \mathcal{L}((\ell+1)P_\infty)$, d'après le Lemme 3.3.5, on a : $f = \sum_{i=0}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j$, et puisque $ord_{P_4} f = 1$, donc $f(P_4) = 0$ entraîne donc que $a_0 = 0$, impliquant

ainsi que $f = \sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j$ avec b_0 non nul (sinon un des R_i devrait être égal à P_4, ce qui serais absurde) $a_{\frac{\ell+1}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-4}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j = 0$, ce qui implique que $y = -\dfrac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j}$.

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$\left(\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j y x^j} \right)^2 = 6x(x^4 + 3)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i \right)^2 = 6 \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_i x^j \right)^2 x(x^4 + 3)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^{i-\frac{1}{2}} \right)^2 = 6 \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_i x^j \right)^2 (x^4 + 3) \tag{3.3.6}$$

L'expression (3.3.6) est une équation de degré ℓ en x.

En effet : quelque soit la parité de ℓ, le premier membre de l'équation (3.3.6) est de degré $2 \times \left(\dfrac{\ell+1}{2} - \dfrac{1}{2} \right) = \ell$ et le second membre est de degré $2 \times \left(\dfrac{\ell-4}{2} \right) + 4 = \ell$.

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{H}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-4}{2}} b_j x^j} \right) \;\middle|\; \begin{array}{c} b_0 \neq 0,\ a_{\frac{\ell+1}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-4}{2}} \neq 0 \\ \text{si } \ell \text{ est impair et } x \text{ solution} \\ \text{de l'équation :} \\ \left(\sum_{i=1}^{\frac{\ell+1}{2}} a_i x^{i-\frac{1}{2}} \right)^2 = 6 \left(\sum_{j=0}^{\frac{\ell-4}{2}} b_i x^j \right)^2 (x^4 + 3) \end{array} \right\}$$

Conclusion : L'ensemble des points algébriques de degré au-plus ℓ sur la courbe $\mathcal{C}$

d'équation affine $y^2 = 6x(x^4 + 3)$ est donné par :

$$\mathcal{H} = \mathcal{H}_1 \bigcup \mathcal{H}_2$$

CQFD

3.4 Points algébriques de degré donné quelconque sur la courbe d'équation affine : $-y^2 = x^6 - 20x^3 - 8$

3.4.1 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 sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{K}:\mathbb{Q}]\leqslant\ell} \mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus ℓ sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire qu'on a $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. On désignera par $\mathcal{J}$ la jacobienne de $\mathcal{C}$ et par $j(P)$ la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

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

où $\mathcal{J}(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (cf [13]).
Notre courbe $\mathcal{C}$ d'équation affine $-y^2 = x^6 - 20x^3 - 8$ est étudiées dans [13].
Notre courbe $\mathcal{C} : -y^2 = x^6 - 20x^3 - 8$ est d'équation projective

$$-Z^4Y^2 = X^6 - 20X^3Z^3 - 8Z^6 \qquad (*)$$

qui peut s'ecrire

$$\mathcal{C} : \begin{cases} Z^4(Y - 2\sqrt{2}Z)(Y + 2\sqrt{2}Z) = -X^3\left(X^3 - 20Z^3\right) & (1) \\ \text{ou} \\ -Z^4Y^2 = (X - (1+\sqrt{3})Z)(X - (1-\sqrt{3})Z)\prod_{k=0}^{3}(X - \eta_k Z) & (2) \end{cases}$$

avec les η_k sont solutions de l'équation : $x^4 + 2x^3 + 6x^2 - 4x + 4 = 0$.

Ce qui correspond aussi à la forme affine suivante

$$\mathcal{C} : \begin{cases} (y - 2\sqrt{2})(y + 2\sqrt{2}) = -x^3\left(x^3 - 20\right) \\ \text{ou} \\ -y^2 = (y - (1 + \sqrt{3}))(x - (1 - \sqrt{3}))\prod_{k=0}^{3}(x - \eta_k) \end{cases}$$

avec les η_k sont solutions de l'équation : $x^4 + 2x^3 + 6x^2 - 4x + 4 = 0$.
On note $P_{k,\ k\in\{0,\ldots 1,\ 3\}}$, P_4, P_5, P_6, P_7 et P_∞ les points de $\mathcal{C}$, définis par : $P_k = [\eta_k : 0 : 1]$, $P_4 = [1+\sqrt{3} : 0 : 1]$, $P_5 = [1-\sqrt{3} : 0 : 1]$, $P_6 = [0 : 2\sqrt{2} : 1]$, $P_7 = [0 : -2\sqrt{2} : 1]$ et $P_\infty = [0 : 1 : 0]$.
Dans cette note on détermine l'ensemble :

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

Notre résultat principal est s'énonce comme suit :

Théorème 4
L'ensemble des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine $-y^2 = x^6 - 20x^3 - 8$ est donné par :

$$\mathcal{R} = \mathcal{R}_1 \bigcup \mathcal{R}_2$$

avec

$$\mathcal{R}_1 = \left\{ \left(x,\ \left(\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right)^6 \right) \ \middle|\ \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \\ \text{est pair , } b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair et } x \\ \text{solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^{i-\frac{5\ell}{12}}\right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2-\frac{5\ell}{12}}\right)^{12}\left(x^6 - 20x^3 - 8\right) \end{array} \right\}$$

$$\mathcal{R}_2 = \left\{ \begin{array}{l} \left(x, \left(\dfrac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i \right)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+2}} \right)^6 \right) \quad \left| \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \\ \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\dfrac{x^i + \rho^i}{x^{\frac{\ell}{12}+1}} \right) \right)^{12} = - \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+1-\frac{\ell}{12}} \right)^{12} \left(x^6 - 20x^3 - 8 \right) \\ \\ \text{avec} \\ \\ \rho^i = -\dfrac{1}{2} \left(\left(1 + \sqrt{3} \right)^i + \left(1 - \sqrt{3} \right)^i \right) \end{array} \right\}$$

3.4.2 Résultats auxiliaires

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

Lemme 3.4.1
On a : $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

Lemme 3.4.2
Pour la courbe $\mathcal{C} : -y^2 = x^6 - 20x^3 - 8$ *qui est donnée aussi par :*

$$\mathcal{C} : \left\{ \begin{array}{c} (y - 2\sqrt{2})(y + 2\sqrt{2}) = -x^3 \left(x^3 - 20 \right) \\ ou \\ -y^2 = (y - (1 + \sqrt{3}))(x - (1 - \sqrt{3})) \prod_{k=0}^{3} (x - \eta_k) \end{array} \right.$$

On a :

(i) $div(x) = P_6 + P_7 - 2P_\infty$,

(ii) $div(x - \eta_k) = 2P_k - 2P_\infty, \qquad k \in \{0, 1, 2, 3\}$,

(iii) $div(x - (1 + \sqrt{3})) = 2P_4 - 2P_\infty$,

(iv) $div(x - (1 - \sqrt{3})) = 2P_5 - 2P_\infty$,

(v) $div(y) = \sum_{k=0}^{3} P_k + P_4 + P_5 - 6P_\infty$.

Démonstration :
Notons x, y les coordonnées affines et X, Y et Z les coordonnées affines projectives. Posons : $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$. On a :

(i) $div(x) = div\left(\frac{X}{Z}\right) = (X = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = 0$, on déduit de (1) que : $Y = 2\sqrt{2}Z$ ou $Y = -2\sqrt{2}Z$ ou $Z^4 = 0$.
  On obtient donc les points : $P_6 = [0 : 2\sqrt{2} : 1]$, $P_7 = [0 : -2\sqrt{2} : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 1, 1 et 4 respectivement. D'où
  $$(X = 0)\cdot\mathcal{C} = P_6 + P_7 + 4P_\infty \tag{3.4.1}$$
- De même pour $Z = 0$, on déduit de (1) que : $X^6 = 0$.
  On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal 6. D'où
  $$(Z = 0)\cdot\mathcal{C} = 6P_\infty. \tag{3.4.2}$$
  Des relations (3.4.1) et (3.4.2), induisent que :
  $$div(x) = P_6 + P_7 - 2P_\infty.$$

(ii) Notons que :
$div(x - \eta_k) = div(X - \eta_k Z) - div(Z) = (X = \eta_k Z)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $X = \eta_k Z$, on déduit de (2) que : $Y^2 = 0$ or $Z^4 = 0$.
  On obtient donc les points : $P_k = [\eta_k : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égal à 2 et 4 respectivement. D'où
  $$(X = \eta_k Z)\cdot\mathcal{C} = 2P_k + 4P_\infty. \tag{3.4.3}$$
- Pour $Z = 0$, revient à l'obtention de la relation (3.4.2).
  Ainsi des relations (3.4.2) et (3.4.3), entraînent donc que :
  $$div(x + \eta_k) = 2P_k - 2P_\infty. \quad \text{avec} \quad k \in \{0, 1, 2, 3\}$$

NB : On procède de la même manière pour les cas (iii) et (iv).

(v) $div(y) = div(\frac{Y}{Z}) = (Y = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}$.

- Pour $Y = 0$, on déduit de (2) que :
  $$(X - (1+\sqrt{3})Z)(X - (1-\sqrt{3})Z)\prod_{k=0}^{3}(X - \eta_k Z) = 0.$$
  On obtient donc les points : $P_{k,\ k\in\{0,\ldots,3\}} = [\eta_k : 0 : 1]$, $P_4 = [1 + \sqrt{3} : 0 : 1]$, $P_5 = [1+\sqrt{3} : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre

multiplicité égal 1 pour chaque points. D'où

$$(Y = 0)\cdot\mathcal{C} = \sum_{k=0}^{3} P_k + P_4 + P_5 \tag{3.4.4}$$

- Pour $Z = 0$, on retrouve la relation (3.4.2).
  Ainsi les relations (3.4.2) et (3.4.4), on déduit que :

$$div(y) = \sum_{k=0}^{3} P_k + P_4 + P_5 - 6P_\infty.$$

CQFD

Corollaire 3.4.3

Les résultats suivants sont les conséquences du Lemme 3.4.2 :

- $2j(P_k) = 0 \qquad avec \qquad k \in \{0, \ldots, 5\}$,
- $j(P_6) + j(P_7) = 0$,
- $\sum_{k=0}^{3} j(P_k) + j(P_4) + j(P_5) = 0$

Donc les $j(P_k)$ où $k \in \{0, \ldots, 5\}$ engendrent le même sous-groupe $\mathcal{J}(\mathbb{Q})$.

Lemme 3.4.4

On a :

$$\mathcal{J}(\mathbb{Q}) = \langle j(P_4) + j(P_5)\rangle = \{n\,(j(P_4) + j(P_5)),\ avec\ n \in \{0, 1\}\}$$

Lemme 3.4.5

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

$$\mathcal{B}_d = \left\{ x^i \;\middle|\; i \in \mathbb{N},\ i \leq \frac{d}{2} \right\} \bigcup \left\{ y^{\frac{1}{6}} x^{j+2} \;\middle|\; j \in \mathbb{N},\ j \leq \frac{d-5}{2} \right\}$$

Démonstration :

On montre aisément que $\mathcal{B}_d$ est une famille libre, il reste alors à montrer que card $\mathcal{B}_d = \dim \mathcal{L}(dP_\infty)$. On sait que le genre de $\mathcal{C}$ est $g = 2$ (voir [5]). La courbe étant de genre 2, d'après le théorème de Riemann-Roch, on a $\dim \mathcal{L}(dP_\infty) = d - g + 1 = d - 1$ dès que $d \geq 2g - 1 = 3$. Deux cas sont possibles :

1^{er} **cas :** supposons que d est pair, on pose alors $d = 2h$, on obtient ainsi :
$i \leq \frac{d}{2} \Leftrightarrow i \leq \frac{2h}{2} = h$ de même $j \leq \frac{d-5}{2} \Leftrightarrow j \leq \frac{2h-5}{2} \Leftrightarrow j \leq h - \frac{5}{2}$
$\Longrightarrow j < h - \frac{4}{2} = h - 2 \Longrightarrow j \leqslant h - 3$. Donc on a :

$$\mathcal{B}_d = \left\{1, x, \ldots\ldots, x^h\right\} \bigcup \left\{y^{\frac{1}{6}}, y^{\frac{1}{6}}x, \ldots\ldots, y^{\frac{1}{6}}x^{h-3}\right\}.$$

On en déduit que :

$$\text{card } \mathcal{B}_d = h + 1 + h - 3 + 1 = 2h-1 = d-1 = \dim \mathcal{L}(dP_\infty).$$

$2^{éme}$ **cas :** supposons que d est impair, on pose alors $d = 2h+1$, on obtient ainsi : $i \leq \frac{d}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Longrightarrow i < h+1 \Longrightarrow i \leqslant h$ de même $j \leq \frac{d-5}{2} \Leftrightarrow j \leq \frac{2h-4}{2} = h - 2$. Donc on a :

$$\mathcal{B}_d = \left\{1,\ x,\ \ldots\ldots,x^h\right\} \bigcup \left\{y^{\frac{1}{6}},\ y^{\frac{1}{6}}x,\ \ldots\ldots,y^{\frac{1}{6}}x^{h-2}\right\}.$$

On en déduit que :

$$\text{card } \mathcal{B}_d = h + 1 + h - 2 + 1 = (2h+1)-1 = d-1 = \dim \mathcal{L}(dP_\infty).$$

CQFD

3.4.3 Démonstration du Théorème 4

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R):\mathbb{Q}] = \ell$. Considérons $R_1,\ldots\ldots,R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots + R_\ell - \ell P_\infty] \in \mathcal{J}(\mathbb{Q})$. D'après le Lemme 3.4.4, on a $t = -n\,(j(P_4) + j(P_5))$, $n \in \{0,\ 1\}$, et par suite :

$$[R_1 + \ldots\ldots + R_\ell - \ell P_\infty] = [2nP_\infty - n\,(P_4 + P_5)] \qquad \text{avec } n \in \{0,\ 1\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots + R_\ell + n\,(P_4 + P_5) - (\ell + 2n)\,P_\infty] = 0 \qquad \text{avec } n \in \{0,\ 1\}$$

D'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots + R_\ell + n\,(P_4 + P_5) - (\ell + 2n)\,P_\infty \qquad (\star)$$

Deux cas sont possibles :

1^{er} **cas :** $n = 0$**.**

La formule $(\star)$ devient : $div(f) = R_1 + \ldots\ldots + R_\ell - \ell P_\infty$, donc $f \in \mathcal{L}(\ell P_\infty)$. D'après le Lemme 3.4.5, on a : $f = \sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y^{\frac{1}{6}} x^{j+2}$ avec a_0, et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_6 ou P_7, ce qui serais absurde), $a_{\frac{\ell}{2}} \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serais

absurde) et $b_{\frac{\ell-5}{2}} \neq 0$ (sinon un des R_i devrait être égal à P_∞, ce qui serais absurde). Aux points R_1, on a : $\sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y^{\frac{1}{6}} x^{j+2} = 0$, impliquant ainsi

$$y = \left(\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2}} \right)^6 .$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$-\left(\left(\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2}} \right)^6 \right)^2 = \left(x^6 - 20x^3 - 8\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^i \right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2} \right)^{12} \left(x^6 - 20x^3 - 8\right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^{i-\frac{5\ell}{12}} \right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2-\frac{5\ell}{12}} \right)^{12} \left(x^6 - 20x^3 - 8\right) \qquad (3.4.5)$$

L'expression (3.4.5) est une équation de degré ℓ en x.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation (3.4.5) est de degré $12 \times \left(\frac{\ell}{2} - \frac{5\ell}{12}\right) = \ell$ et le second membre est de degré $12 \times \left(\left(\frac{\ell-5}{2}\right) + 2 - \frac{5\ell}{12}\right) = \ell$.

On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{R}_1 = \left\{ \left(x, \left(\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i x^i}{\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^j} \right)^6 \right) \;\middle|\; \begin{array}{c} a_0 \text{ et } b_0 \text{ non simultanément nuls, } a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \\ \text{est pair , } b_{\frac{\ell-5}{2}} \neq 0 \text{ si } \ell \text{ est impair et } x \\ \text{solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{\ell}{2}} a_i x^{i-\frac{5\ell}{12}} \right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-5}{2}} b_j x^{j+2-\frac{5\ell}{12}} \right)^{12} \left(x^6 - 20x^3 - 8\right) \end{array} \right\}$$

$2^{éme}$ **cas :** $n = 1$.

La formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell + P_4 + P_5 - (\ell+2)P_\infty$, donc $f \in \mathcal{L}((\ell+2)P_\infty)$, d'après le Lemme 3.4.5, on a : $f = \sum_{i=0}^{\frac{\ell+2}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y^{\frac{1}{6}} x^{j+2}$, et puisque $ord_{P_4} f = ord_{P_5} f = 1$, donc $f(P_4) = f(P_5) = 0$ entraîne donc que $a_0 = -\frac{1}{2}\sum_{i=0}^{\frac{\ell+1}{2}} a_i \left(\left(1+\sqrt{3}\right)^i + \left(1-\sqrt{3}\right)^i\right)$. En posant $\rho^i = -\frac{1}{2}\left(\left(1+\sqrt{3}\right)^i + \left(1-\sqrt{3}\right)^i\right)$, on obtient $a_0 = -\sum_{i=1}^{\frac{\ell+2}{2}} a_i \rho^i$ impliquant ainsi que $f = \sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i\right) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y^{\frac{1}{6}} x^{j+2}$ avec $a_{\frac{\ell+2}{2}} \neq 0$ si ℓ est pair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-3}{2}} \neq 0$ si ℓ est impair (sinon un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux points R_i, on a : $\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i\right) + \sum_{j=0}^{\frac{\ell-3}{2}} b_j y^{\frac{1}{6}} x^{j+2} = 0$, impliquant ainsi :

$$y = \left(\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i\right)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+2}}\right)^6.$$

En remplaçant la valeur de y dans l'expression de l'équation de la courbe, on obtient :

$$-\left(\left(\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i\right)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+2}}\right)^6\right)^2 = \left(x^6 - 20x^3 - 8\right)$$

cette équation peut s'ecrire :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i\right)\right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-2}{2}} b_j x^{j+2}\right)^{12} \left(x^6 - 20x^3 - 8\right)$$

ce qui correspond aussi à l'équation :

$$\left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \rho^i}{x^{\frac{\ell}{12}+1}}\right)\right)^{12} = -\left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+1-\frac{\ell}{12}}\right)^{12} \left(x^6 - 20x^3 - 8\right) \quad (3.4.6)$$

L'expression (3.4.6) est une équation de degré ℓ en x.

En effet, quelque soit la parité de ℓ, le premier membre de l'équation (3.4.6)

est de degré $12 \times \left(\frac{\ell+2}{2} - \frac{\ell}{12} - 1 \right) = \ell$ et le second membre est de degré $12 \times \left(\frac{\ell-3}{2} + 1 - \frac{\ell}{12} \right) + 6 = \ell$.
On obtient ainsi une famille de points de degré ℓ :

$$\mathcal{R}_2 = \left\{ \begin{array}{l} \left(x, \left(\frac{\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(x^i + \rho^i \right)}{\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+2}} \right)^6 \right) \left| \begin{array}{l} a_{\frac{\ell+2}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-3}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \\ \text{impair et } x \text{ solution de l'équation :} \end{array} \right. \\ \\ \left(\sum_{i=1}^{\frac{\ell+2}{2}} a_i \left(\frac{x^i + \rho^i}{x^{\frac{\ell}{12}+1}} \right) \right)^{12} = - \left(\sum_{j=0}^{\frac{\ell-3}{2}} b_j x^{j+1-\frac{\ell}{12}} \right)^{12} \left(x^6 - 20x^3 - 8 \right) \\ \\ \text{avec} \\ \\ \rho^i = -\frac{1}{2} \left(\left(1 + \sqrt{3} \right)^i + \left(1 - \sqrt{3} \right)^i \right) \end{array} \right\}$$

Conclusion : L'ensemble des points algébriques de degré au-plus ℓ sur la courbe $\mathcal{C}$ d'équation affine $-y^2 = x^6 - 20x^3 - 8$ est donné par :

$$\mathcal{R} = \mathcal{R}_1 \bigcup \mathcal{R}_2$$

CQFD

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

3.5.1 Introduction

Soit $\mathcal{C}$ une courbe algébrique définie sur un corps de nombres $\mathbb{K}$. On note $\mathcal{C}(\mathbb{K})$ l'ensemble des points algébriques sur $\mathcal{C}$ définis sur $\mathbb{K}$. Le degré d'un point algébrique R est le degré de son corps de définition sur $\mathbb{Q}$, i.e $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Un théorème célèbre de Faltings 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. Une généralisation aux sous-variétés d'une variété abélienne permet une étude qualitative de l'ensemble $\bigcup_{[\mathbb{K}:\mathbb{Q}] \leq \ell} \mathcal{C}(\mathbb{K})$ des points algébriques sur $\mathcal{C}$ de degré au plus ℓ donnée sur $\mathbb{Q}$. La situation est plus favorable dans le cas où le rang du groupe de Mordell–Weil $\mathcal{J}(\mathbb{Q})$ de la jacobienne de $\mathcal{C}$ est nul.
Notre courbe d'équation affine $\mathcal{C}_3(11) : y^{11} = x^3(x - 1)^3$ est un cas spécial des

quotients de courbes de Fermat d'équations affine :

$$\mathcal{C}_{r,s}(p) \ : \ y^p \ = \ x^r(x-1)^s, \qquad \text{avec} \qquad 1 \ \leq \ r, \ s, \ r+s \ \leq \ p-1$$

étudiées dans [3] pour $r \ = \ s \ = \ 3$.
Nous nous proposons d'étudier en détail les points algébriques de degré quelconque donnée sur le corps $\mathbb{Q}$ de la courbe $\mathcal{C}_3(11)$ d'équation affine : $y^{11} \ = \ x^3(x \ - \ 1)^3$.
La courbe $\mathcal{C}_3(11)$ est hyper-elliptique de genre $g \ = \ 5$ et de rang nul. Dans ([3]), le groupe de Mordell-Weil $\mathcal{J}(\mathbb{Q})$ des points rationnels de la jacobienne J de $\mathcal{C}_3(11) \ : \ y^{11} \ = \ x^3(x \ - \ 1)^3$ est fini et donné par $\mathcal{J}(\mathbb{Q}) \ = \ \mathbb{Z}/11\mathbb{Z}$.
Notre objectif est de donner une description géométrique de l'ensemble des points algébriques de $\mathcal{C}$ de degré quelconque ℓ donné sur $\mathbb{Q}$. On note $P_0 \ = \ [0 : \ 0 \ : \ 0]$, $P_1 \ = \ [1 \ : \ 0 \ : \ 1]$ et $P_\infty \ = \ [1 \ : \ 0 \ : \ 0]$ le point à infini de $\mathcal{C}_3(11)$ et considérons le plongement jacobien :

$$\begin{array}{rccl} j & : & \mathcal{C}_3(11)(\mathbb{Q}) & \longrightarrow \ \mathcal{J}(\mathbb{Q}), \\ & & P & \longmapsto \ [P \ - \ P_\infty]\,. \end{array}$$

Notre étude résulte des travaux de Gross-Rohrlich dans [3] 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 $\mathbb{Q}$ par la proposition suivante :

Proposition :
l'ensemble des points algébriques sur $\mathcal{C}_1(11)$ de degré au-plus 2 sur $\mathbb{Q}$ est donné par

$$\bigcup_{[\mathbb{K}:\mathbb{Q}]\leq 2} \mathcal{C}_1(11)(\mathbb{K}) = \left\{ \left(\frac{1}{2} \pm \sqrt{y^{11} + \frac{1}{4}}, y \right) \right\} \left\{ P_\infty \right\}$$

Notre résultats principal s'énonce comme suit :

Théorème 5
L'ensemble des points algébriques de degré au-plus $\ell \ \geq \ 9$ *sur la courbe* $\mathcal{C}_3(11)$ *d'équation affine* $y^{11} \ = \ x^3\,(x \ - \ 1)^3$ *est donné par :*

$$\mathcal{W} \ = \ \mathcal{W}_0 \ \bigcup \ \left(\bigcup_{m=1}^{10} \mathcal{W}_m \right)$$

avec

$$\mathcal{W}_0 = \left\{ \left(\begin{array}{c} \sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}} \\ -\frac{}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}}, \ y \end{array} \right) \middle| \begin{array}{l} a_0 \neq 0, \ a_{\frac{\ell}{2}} \neq 0 \ si \ \ell \ est \ pair, \ b_{\frac{\ell-11}{2}} \neq 0 \ si \\ \ell \ est \ impair \ et \ y \ solution \ de \ l'équation : \\ \\ y^{11} \left(\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^j \right)^6 = \left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^i \right)^3 \left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}} + \sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}} \right)^3 \end{array} \right\}$$

$$\mathcal{W}_m = \left\{ \left(\begin{array}{c} \sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} \\ -\frac{}{\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}}, y \end{array} \right) \middle| \begin{array}{l} a_{\frac{\ell+11-m}{2}} \neq 0 \ \ si \ \ell \ est \ pair, \ \ b_{\frac{\ell-m}{2}} \neq 0 \ si \ \ell \ est \\ impair \ et \ y \ est \ solution \ de \ l'équation : \\ \\ y^{11} \left(\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{2j+m-11}{6}} \right)^6 = \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i+m-11}{3}} \right)^3 \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} + \sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}} \right)^3 \end{array} \right\}$$

3.5.2 Résultats auxiliaires

Pour un diviseur $\mathfrak{D}$ sur $\mathcal{C}_3(11)$, on note $\mathcal{L}(\mathfrak{D})$ le $\mathbb{Q}$-espace vectoriel des fonctions rationnelles f définies sur $\mathbb{Q}$ telles que $f = 0$ ou $div(f) \geq -\mathfrak{D}$; $\mathfrak{l}(\mathfrak{D})$ désigne la $\mathbb{Q}$-dimension de $\mathcal{L}(\mathfrak{D})$.
La courbe $\mathcal{C}_3(11)$ d'équation affine $y^{11} = x^3(x-1)^3$ a pour équation projective $Y^{11} = X^3Z^5(X-Z)^3$.
On a le Lemme suivant :

Lemme 3.5.1
Pour la courbe $\mathcal{C}_3(11) : y^{11} = x^3(x-1)^3$ *; on a les diviseurs rationnels suivants :*

(*i*) $div(x) = 11P_0 - 11P_\infty$;

(*ii*) $div(y) = 3P_0 + 3P_1 - 6P_\infty$;

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

Démonstration :
il s'agit d'un calcul de type

$$div(x-a) = ((X-aZ) = 0) \cdot \mathcal{C}_3(11) - (Z = 0) \cdot \mathcal{C}_3(11)$$

CQFD

Corollaire 3.5.2

Les résultats suivants sont les conséquences du Lemme 3.5.2 :

- $11j(P_0) = 11j(P_1) = 0$,
- $3j(P_0) + 3j(P_1) = 0$.

Donc $j(P_0)$ et $j(P_1)$ engendrent le même sous-groupe $J(\mathbb{Q})$.

Lemme 3.5.3

On a :

$$\mathcal{J}(\mathbb{Q}) = \langle j(P_0)\rangle = \{mj(P_0), \quad avec \quad 0 \leq m \leq 10\}$$

Lemme 3.5.4

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

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

Démonstration :

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

D'après le théorème de Riemann-Roch, on a $\dim(\mathcal{L}(nP_\infty)) = n - g + 1$ dès que $n \geq 2g - 1$ avec $g = \dfrac{11-1}{2} = 5$

Deux cas sont possibles :

1^{er} **cas :** Supposons que n est pair, et posons $n = 2h$. On a alors $i \leq \dfrac{n}{2} = h$ et $j \leq \dfrac{n-11}{2} \Leftrightarrow j \leq \dfrac{2h-11}{2} \Leftrightarrow j \leq \dfrac{2h-11-1}{2} = h - 6 = h - g - 1$.
Donc on a :

$$\mathcal{B} = \left\{1, \ldots, \left(\frac{x^2(x-1)^2}{y^7}\right)^h\right\} \bigcup \left\{x, \ldots, x\left(\frac{x^2(x-1)^2}{y^7}\right)^{h-g-1}\right\}$$

On en déduit que :

$$\dim(\mathcal{B}) = (h+1) + (h-g) = 2h - g + 1 = n - g + 1 = \dim(\mathcal{L}(nP_\infty))$$

$2^{éme}$ **cas :** Supposons que n est impair, et posons $n = 2h+1$. On a alors $i \leq \dfrac{n}{2} \Leftrightarrow i \leq \dfrac{2h+1}{2} \Leftrightarrow i \leq h$ et $j \leq \dfrac{n-11}{2} \Leftrightarrow j \leq \dfrac{2h-10}{2} = h - g$
Donc on a :

$$\mathcal{B} = \left\{1, \ldots, \left(\frac{x^2(x-1)^2}{y^7}\right)^h\right\} \bigcup \left\{x, \ldots, x\left(\frac{x^2(x-1)^2}{y^7}\right)^{h-g}\right\}$$

On en déduit que :

$$\dim(\mathcal{B}) = (h+1)+(h-g+1) = 2h+1-g+1 = n-g+1 = \dim(\mathcal{L}(nP_\infty))$$

CQFD

3.5.3 Démonstration du Théorème 5

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$ avec $[\mathbb{Q}(R):\mathbb{Q}] = \ell$. Considérons $R_1, \ldots\ldots, R_\ell$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots + R_\ell - \ell P_\infty] \in \mathcal{J}(\mathbb{Q})$. D'après le Lemme 3.5.4, on a $t = (m-11)(j(P_0))$, avec $m \in \{0, \ldots, 10\}$, et par suite :

$$[R_1 + \ldots\ldots + R_\ell - \ell P_\infty] = [(m-11)P_\infty - (m-11)P_0] \text{ avec } m \in \{0, \ldots, 10\}$$

Ainsi, on obtient la formule suivante :

$$[R_1 + \ldots + R_\ell + (11-m)P_0 - (\ell + 11 - m)P_\infty] = 0 \qquad \text{avec } m \in \{0, \ldots, 10\}$$

D'après le théorème d'Abel Jacobi ([5, page 156]), il existe une fonction rationnelle f définie sur $\mathbb{Q}$ telle que :

$$div(f) = R_1 + \ldots + R_\ell + (11-m)P_0 - (\ell + 11 - m)P_\infty \qquad (\star)$$

On remarque que $R \notin \left\{P_0, P_1, P_\infty\right\}$.
On regroupe les résultat en deux cas :

1^{er} **cas :** $m = 0$**.**

Par remonté, la formule formule $(\star)$ devient : $div(f) = R_1 + \ldots + R_\ell - \ell P_\infty$, donc $f \in \mathcal{L}(\ell P_\infty)$. D'après le Lemme 3.5.5, on a :

$$f = \sum_{i=0}^{\frac{\ell}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j=0}^{\frac{\ell-11}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j$$

avec $a_0 \neq 0$ (sinon l'un des R_i serait égal à P_0, ce qui serait absurde) $a_{\frac{\ell}{2}} \neq 0$ si ℓ est pair (sinon l'un des R_i serait égal à P_∞, ce qui serait absurde) et $b_{\frac{\ell-11}{2}} \neq 0$ si ℓ est impair (sinon l'un des R_i serait égal à P_∞, ce qui serait absurde).

Aux points R_i on a :

$$\sum_{i=0}^{\frac{\ell}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + \sum_{j=0}^{\frac{\ell-11}{2}} b_j x \left(\frac{x^2(x-1)^2}{y^7}\right)^j = 0$$

d'où $x = -\dfrac{\sum_{i=0}^{\frac{\ell}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j}$ et par suite $y^{11} = x^3(x-1)^3 \Leftrightarrow y^{\frac{1}{3}} = \dfrac{x^2(x-1)^2}{y^7}$, ainsi $x = -\dfrac{\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}}$. Donc l'équation $y^{11} = x^3(x-1)^3$ devient :

$$y^{11} = \left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}}\right)^3 \left(\left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}}\right) - 1\right)^3$$

cette équation peut s'ecrire :

$$y^{11}\left(\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}\right)^6 = \left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}\right)^3 \left(\left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}\right) - \left(\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}\right)\right)^3 \qquad (3.5.1)$$

L'expression (3.5.1) est une équation de degré ℓ en y.

En effet, quelque soit la parité de ℓ, le première membre de l'équation (3.5.1) est de degré $11 + 2 \times \left(\dfrac{\ell - 11}{2}\right) = \ell$ et le second membre est de degré $\dfrac{\ell}{2} + 3 \times \left(\dfrac{\ell - 11}{2}\right) = \ell$.

On obtient ainsi une famille de points de degré ℓ.

$$\mathcal{W}_0 = \left\{ \left(-\frac{\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}},\ y \right) \middle| \begin{array}{l} a_0 \neq 0,\ a_{\frac{\ell}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-11}{2}} \neq 0 \text{ si} \\ \ell \text{ est impair et } y \text{ solution de l'équation :} \\ y^{11}\left(\sum_{j=0}^{\frac{\ell-11}{2}} b_j y^j\right)^6 = \left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^i\right)^3 \left(\sum_{i=0}^{\frac{\ell}{2}} a_i y^{\frac{i}{3}} + \sum_{j=0}^{\frac{\ell-11}{2}} b_j y^{\frac{j}{3}}\right)^3 \end{array} \right\}$$

$2^{éme}$ **cas :** $m \in \{1, \ldots, 10\}$**.**

La formule $(*)$ devint : $div(f) = R_1 + \ldots + R_\ell + (11-m)P_0 - (\ell + 11 - m)P_\infty$,

donc $f \in \mathcal{L}(\ell + 11 - m)P_\infty$. D'après le Lemme 3.5.5, on a :

$$f = \sum_{i=0}^{\frac{\ell+11-m}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j=0}^{\frac{l-m}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j;$$

et comme $ordf_{P_0} = 11 - m$, donc

$$f = \sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i + x \sum_{j=0}^{\frac{\ell-m}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j$$

avec $a_{\frac{\ell+11-m}{2}} \neq 0$ si ℓ est pair (sinon les R_i seraient égaux à P_∞, ce qui serait absurde) et $b_{\frac{\ell-m}{2}} \neq 0$ si ℓ est impair (sinon les R_i seraient égaux à P_∞, ce qui serait absurde).

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

d'où $x = -\dfrac{\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i \left(\frac{x^2(x-1)^2}{y^7}\right)^i}{\sum_{j=0}^{\frac{\ell-m}{2}} b_j \left(\frac{x^2(x-1)^2}{y^7}\right)^j}$ et par suite $x = -\dfrac{\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}}$.

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

$$y^{11} = \left(-\frac{\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}}\right)^3 \left(\left(-\frac{\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}}}{\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}}\right) - 1\right)^3$$

cette équation peut s'ecrire :

$$y^{11}\left(\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}\right)^6 = \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}}\right)^3 \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} - \sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}\right)^3$$

Cette équation équivaux à :

$$y^{11}\left(\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{2j+m-11}{6}}\right)^6 = \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i+m-11}{3}}\right)^3 \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} + \sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}}\right)^3 \quad (3.5.2)$$

L'expression (3.5.2) est une équation de degré ℓ en y.

En effet, quelque soit la parité de ℓ, le première membre de l'équation (3.5.2)

est de degré $11 + 6 \times \left(\dfrac{2 \times \dfrac{\ell - m}{2} + m - 11}{6} \right) = \ell$ et le second membre est de degré $3 \times \left(\dfrac{\dfrac{\ell + 11 - m}{2} + m - 11}{3} \right) + 3 \times \left(\dfrac{\dfrac{\ell + 11 - m}{2}}{3} \right) = \ell$.
On obtient ainsi une famille de points de degré ℓ.

$$\mathcal{W}_m = \left\{ \left(\begin{array}{c} \sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} \\ -\dfrac{}{} \\ \sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}} \end{array}, y \right) \middle| \begin{array}{l} a_{\frac{\ell+11-m}{2}} \neq 0 \text{ si } \ell \text{ est pair, } b_{\frac{\ell-m}{2}} \neq 0 \text{ si } \ell \text{ est} \\ \text{impair et } y \text{ est solution de l'équation :} \\ y^{11} \left(\sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{2j+m-11}{6}} \right)^6 = \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i+m-11}{3}} \right)^3 \left(\sum_{i=11-m}^{\frac{\ell+11-m}{2}} a_i y^{\frac{i}{3}} + \sum_{j=0}^{\frac{\ell-m}{2}} b_j y^{\frac{j}{3}} \right)^3 \end{array} \right\}$$

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

$$\mathcal{W} = \mathcal{W}_0 \bigcup \left(\bigcup_{m=1}^{10} \mathcal{W}_m \right)$$

CQFD

CONCLUSION

Les résultats obtenus de cette thèse portent essentiellement sur la détermination explicite des points algébriques de degré au-plus ℓ sur $\mathbb{Q}$ sur quelques courbes algébriques lisses des cas particuliers de courbes qui sont extrêmement utilisées par très nombreux géomètres algébristes. En s'inspirant des travaux de O. Sall et des résultats obtenus dans [7], on a pu au chapitre 2 exhiber les points rationnels jusqu'aux points algébriques de degré au-plus 10 avant d'étendre ce travail aux points algébriques de degré ℓ donné quelconque sur $\mathbb{Q}$, et au dernier chapitre faire une généralisation sur certaines courbes lisses, tout en s'inspirant des travaux de [7] qui a déterminé les points algébriques de degré ℓ donné quelconque sur $\mathbb{Q}$ sur la courbe d'équation affine $y^{3n} = x(x-1)(x-2)(x-3)$.
Malgré les résultats obtenus dans cette thèse, le champ d'investigation reste encore très vaste. En effet

a) Les courbes étudiées pour déterminer les points algébriques de degré au-plus ℓ, sont des courbes dont le Groupe de Mordell-Weil est fini. Le problème reste ouvert pour les courbes dont le Groupe de Mordell-Weil n'est pas fini.

b) La nature explicite des points algébriques peut être rechercher. Par exemple rechercher les points entiers de degré bien spécifique.

c) Retrouver les points de torsion de degré ℓ donné reste un problème ouvert.

d) L'élaboration d'un nouvel algorithme de Deffi-Helmann pourrai faire office de problème ouvert.

Bibliographie

[1] Bruin N. Flynn E.V *Exhibiting SHA[2] on hyperelliptic Jacobians*, Journal of Number Theory 118 (2006) *p.* 266 − 291.

[2] D. Faddeev : *on the divisor class groups of some algebraic curves*, Dokl. Akad. Nauk SSSR 136 (1961) 296 − 298. English translation : Soviet Math. Dokl. 2 (1)(1961) *p.* 67 − 69.

[3] B. Gross, D. Rohrlich, *some results on the Mordell-Weil group of the jacobian of the Fermat curve*, Invent. Math. 44 (1978) *p.* 201 − 224.

[4] M. Hindry, J. Silverman, *Introduction to Diophantine Geometry*, Springer-Verlag (en préparation).

[5] P.A Griffiths : *Introduction to algebric curves*, Translation mathematical monograhs volume 76. (1989). American Matematical Society, Providence (1989).

[6] Anna ARNTH-JENSEN and E. Victor FLYNN : *Non-trivial III in the Jacobian of an infinite family of curves of genus 2*, Journal de Theory des Nombres de Bordeaux, Tome 21, number 1 (2009), *p.* 1 − 13.

[7] O. Sall, M. Fall, *points algébriques de petits degrés sur les courbes d'équations affines* $y^{3n} = x(x-1)(x-2)(x-3)$, Journal 1les Mathématiques Africaines (2015).

[8] M. D. Dillo, B. Baldé, O. Sall, points algébriques de degré donné quelconque sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$, International Journal Of Development Research Vol. 12, Issue, 11, *p.* 53106 − 53110, Janvier, 2022.

[9] E.F. Schaefer, *Rational points on algebraic curves*, lecture II, February 5, 1999, Santa Clara University.

[10] J.-P. Serre, *Représentation des groupes finis*, Hermann, Paris, 1967.

[11] J.-P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin Inc., New York-Amsterdam, 1968.

[12] J.-P. Serre, *Sur les représentations modulaires de degré 2 de Gal(*$\bar{\mathbb{Q}}/\mathbb{Q}$), Duke Math. J. 54, 1987, *p.* $179 - 230$.

[13] N. BRUIN : *On powers as sums of two cubes*, Algorithmic Number Theory, Tome 21, 4th International Symposium, ANTS-IV Leiden, The Netherlands, July 2-7, (2000), *p.* $169 - 184$.

[14] P. Tzermias, *Torsion parts of Mordell-Weil groups of Fermat jacobians*, Internat. Math Res. Notices 7 (1998) *p.* $359 - 369$.

[15] O. Zariski, P. Samuel, *Commutative Algebra*, 2 Vols, Springer-Verlag, Berlin Heidelberg New York 1975.

[16] L. Kulesz, *Courbes algebriques de genre* $\geq$ 2 *possédant de nombreux points rationnels*, ACTA Arithmetica LXXXVII.2 (1998) *p.* $103 - 120$.

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