UNIVERSITE ASSANE SECK DE ZIGUINCHOR

U.F.R DES SCIENCES ET TECHNOLOGIES

DÉPARTEMENT DE MATHÉMATIQUES

Mémoire de Master

DOMAINE : **Sciences et Technologies**
MENTION : **Mathématiques et Applications**
SPÉCIALITÉ : **Mathématiques Pures**
OPTION : **Géométrie Algébrique**

Théme :

Conjectures de Weil

Présenté et soutenu par :
Johnathan DJELLA LEGNONGO

Sous la direction de :
Dr Tony Ezome : Université des Sciences et Techniques de Masuku, Franceville Gabon

Sous la supervision de :
Pr. Oumar SALL : Université Assane Seck de Ziguinchor, Ziguinchor Sénégal

Devant le jury ci-après :

Nom(s) et Prénom(s)	Grade	Qualité	Établissement
Amoussou Thomas GUEDENON	Maître de conférences	Examinateur	UASZ
Oumar SALL	Professeur titulaire	Co-directeur	UASZ
Salomon SAMBOU	Professeur titulaire	Président du jury	UASZ
Tony EZOME	Maître assistant	Directeur	USTM (Gabon)

Année universitaire : 2018 – 2019

Conjectures de Weil

Johnathan DJELLA LEGNONGO

Soutenu publiquement le 14 Juillet 2020

Résumé

Le but de ce travail est de présenter une série de conjectures remarquables énoncées par André Weil [1] en 1949. Ces conjectures ont été formulées à partir des calculs sur le nombre de solutions de certains systèmes d'équations polynomiales. Toutefois, Weil s'est beaucoup inspiré de la fonction zêta de Riemann et de l'hypothèse de Riemann pour les deux dernières. Ainsi pour une variété projective lisse V définie sur un corps fini $\mathbb{F}_{p^r}$, les conjectures de Weil :

1. affirment que la fonction zêta $Z(t)$ de V est une fraction rationnelle de la forme $\frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$ où les $P_i(t)$ sont des polynômes à coefficients dans $\mathbb{Z}$;
2. proposent une équation fonctionnelle pour $Z(t)$;
3. affirment que les inverses des zéros des $P_i(t)$ pour $1 \leq i \leq 2n-1$ sont des nombres complexes dont le module est égal à $\sqrt{p^r}$;
4. donnent certaines propriétés topologiques (en fonction des degrés des polynômes $P_i(t)$) de toute variété algébrique $\mathcal{X}$ définie sur un corps de nombres dont V serait la réduction modulo p.

Par cela, André Weil a jeté les bases de tout un programme qui servira de boussole pour les fondateurs de la géométrie algébrique moderne. Précisons que ces conjectures ont toutes été démontées : Bernard Dwork a démontré la première conjecture, Alexander Grothendieck avec son équipe a prouvé la première, la deuxième et la quatrième conjecture, et enfin Pierre Deligne a démontré la troisième conjecture.

Le sujet étant bien trop large pour être présenter intégralement dans un mémoire de master, nous nous concentrons essentiellement sur les trois premières conjectures dans le cas des courbes algébriques et leurs jacobiennes. Pour cela nous allons commencer par recenser un bon nombre de résultats de théorie des corps, de théorie de Galois et de géométrie algébrique liés à ce sujet.

1. André Weil : mathématicien français (1906-1998).

Remerciements

J'aimerai profiter de cette occasion pour exprimer ma gratitude envers Monsieur Tony EZOME mon directeur de mémoire qui m'a motivé, encouragé, et surtout m'a passionné pour ce domaine. Il est resté constamment disponible pour me guider et répondre à mes questions.

Merci à Monsieur Oumar SALL pour avoir accepté de co-encadrer ce mémoire, et d'avoir donner de son précieux temps pour m'écouter, me corriger, et me guider.

La soutenance de Mémoire est un évènement important, qui marque la fin d'un cycle. dans ces conditions, le jury tient un rôle extrêmement important, d'où ma reconnaissance et ma gratitude envers ces personnes qui ont accepté du constituer ce jury. Monsieur Salomon SAMBOU qui a présidé le jury, et Monsieur Amoussou Thomas GUEDENON qui a été examinateur.

- Je remercie tous les enseignants du département de mathématiques de l'Université Assane SECK de Ziguinchor, pour la qualité des enseignements qu'ils m'ont dispensé, il s'agit de Salomon SAMBOU, Oumar SALL, Amoussou Thomas GUEDENON, Mansour SANE, Alassane DIEDHIOU, Daouda Niang DIATTA, Timack NGOM, Clément MANGA et Emmanuel CABRAL. Je n'oublie pas l'administration de l'Université Assane SECK de Ziguinchor pour son professionnalisme et son dynamisme.
- Je n'oublie pas mes enseignants du département de mathématiques et informatique de la faculté des sciences de l'Université des Sciences et Techniques de Masuku au Gabon, Tony EZOME, Octave MOUTINGA, Jules TINZOGHO NTSIRI , Henri BOUYTIVOUBOU, Alban MBINA MBINA, Florent NGUEMA NDONG, Brice DOUMBE, Andami OVONO, Frédéric EYI MINKO, Flugence EYI MINKO, Souleymane BA, Théophile MAVOUNGOU et Dossou AKIOLA.
- Merci à Monsieur Daouda Niang DIATTA pour son rôle de tuteur.
- Merci à mes aînés et camarades de l'Université Assane SECK de Ziguinchor ; il s'agit de Winnie OSSETE INGOBA, Sény DIATTA, Souhaibou SAMBOU, Eramane BODIAN, Nestor DJINTELBE, Chérif Mamina COLY, pour leur aide et encouragements.
- Merci à Winnie OSSETE INGOBA, je ne sais pas ce que serait mon séjour ici si tu n'avais pas été là. Je n'oublie pas Jean Eudes, Marcie, Ferdie, Malva, Anna DIAKOUNDILA, Orphelia, et Rita DADOTE.
- Merci à ma famille DJELLA, puisses-tu me guider encore vers la réussite. Merci à la famille GOUDIABI pour son acceuil et son soutien.
- Et aux personnes oubliées...

Sommaire

Introduction

Achevant le travail commencé par Hasse à propos du nombre de points rationnels sur une courbe elliptique définie sur un corps fini, André Weil a eu la perspicacité de développer toute la théorie, en partant des courbes elliptiques jusqu'aux généralisations concernant les variétés abéliennes. Il a commencé par écrire méthodiquement tous les fondements nécessaires. Dans la période $1946-1948$, il a rédigé la preuve pour les courbes algébriques de genre arbitraire et pour les variétés abéliennes. Ses travaux partent de l'observation simple mais fondamentale suivante :

Pour une variété algébrique $\mathcal{V} \subset \mathbb{A}^n$ définie sur un corps fini $\mathbf{K} = \mathbb{F}_q$, l'application

$$\begin{aligned} \phi_{q^m} : \mathcal{V} &\longrightarrow \mathcal{V} \\ (x_1, \ldots, x_n) &\longmapsto (x_1^{q^m}, \ldots, x_n^{q^m}) \end{aligned}$$

est un morphisme de variétés dont les points fixes sont exactement les points $\mathbb{F}_{q^m}$-rationnels de $\mathcal{V}$.

Donc si en plus, $\mathcal{V}$ est muni d'une structure de groupe telle que ϕ_{q^m} est également un morphisme de groupes, alors les points $\mathbb{F}_{q^m}$-rationnels sont exactement les éléments du noyau $\mathrm{Ker}(\phi_{q^m} - \mathrm{Id})$.

Notre mémoire est réparti en 4 chapitres. Au chapitre 1, nous rappelons quelques notions de la théorie des corps et de la théorie de Galois, en commençant par les corps et leurs extensions. On présente aussi le cas particulier des extensions des corps finis et nous décrivons le groupe de Galois dans ce contexte. Le chapitre 2 est consacré aux notions de base de la géométrie algébrique. Il s'agit ici de définir les ensembles algébriques (affines et projectifs), les variétés algébriques (affines et projectives). Nous discutons des courbes non-singulières (affines ou projectives), et nous explicitons le lien qu'il y a entre l'étude des variétés affines et celle des variétés projectives. Enfin nous précisons le cas des variétés définies sur un corps fini. Dans le chapitre 3, nous présentons un résultat central : le théorème de Riemann-Roch. Il est incontournable en géométrie algébrique. Nous entamons le chapitre avec la notion de diviseur (effectif, premier, principal) sur une courbe algébrique. Ensuite, nous abordons la notion de jacobienne d'une courbe algébrique, qui est là aussi un élément très important pour notre étude. Puis on présente le théorème de Riemann-Roch, et on définit les courbes elliptiques. Dans le chapitre 4, nous commençons par aborder les notions de groupes algébriques, de variétés abéliennes et d'isogénies, avant de décrire le cas particulier des courbes elliptiques. Puis nous définissons la fonction zêta associée à une courbe, notion fondamentale, et même centrale des conjectures de Weil qui sont le thème de notre mémoire. Nous clôturons le chapitre en présentant un interêt des conjectures de Weil dans le domaine de la sécurité informatique.

La plupart des résultats énoncés dans ce mémoire ne seront pas démontrés en raison de la longueur des preuves. Le cas échéant, nous renverrons le lecteur vers une ou deux références.

Chapitre 1

Rappels sur la théorie de Galois

Dans ce chapitre, nous rappelons brièvement certaines notions de la théorie de Galois, notamment celles qui sont utiles à notre étude. Nous nous sommes inspirés des ouvrages [LN97], [Lan02] et [Sam71]. Le lecteur intéressé par des exposés et des discussions plus larges est invité à consulter ces références.

Dans ce manuscrit, tous les anneaux, sauf mention explicite du contraire, sont supposés commutatifs et unitaires.

1.1 Généralités

1.1.1 Extensions de corps

Étant donné un anneau A, il existe un unique morphisme d'anneaux $\psi : \mathbb{Z} \longrightarrow A$ défini de la manière suivante :

$$\psi(n) = \begin{cases} 1 + \ldots + 1 & n \text{ fois si } n > 0 \quad (1.1) \\ 0 & \text{si } n = 0 \quad (1.1) \\ -(1 + \ldots + 1) & -n \text{ fois si } n < 0 \quad (1.1) \end{cases}$$

Le noyau de ψ est un idéal de $\mathbb{Z}$, et si les multiples de 1 sont tous non nuls alors $\ker(\psi) = \{0\}$ et on dit que A est de caractéristique nulle. Si ψ n'est pas injectif (c'est par exemple le cas lorsque A est un anneau fini), le noyau de ψ est un idéal de $\mathbb{Z}$ engendré par un entier strictement positif : c'est la caractéristique de A que l'on note $\mathrm{Char}(A)$.

Remarque 1.1.1. *La caractéristique d'un anneau commutatif unitaire intègre est soit nulle soit égale à est un nombre premier p. La formule du binôme de Newton liée à l'exponentiation par p^n dans un tel anneau est simplement donnée par :*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, \text{ pour tout } a, b \in A \text{ et } n \in \mathbb{N}^*. \quad (1.2)$$

Rappelons qu'un corps commutatif $\mathbf{K}$ est un anneau commutatif unitaire dans lequel tout élément non nul est inversible. Un corps commutatif est donc un anneau intègre.

Dans ce manuscrit, tous les corps, sauf mention explicite du contraire, sont commutatifs.

Étant donné un anneau intègre A, une façon courante d'obtenir un corps à partir de A est d'ajouter à A les inverses formels de tous ses éléments non nuls. L'ensemble obtenu est le corps des fractions de A. Par exemple, $\mathbf{K}(X)$ est le corps des fractions de l'anneau des polynômes $\mathbf{K}[X]$. Une extension d'un corps $\mathbf{K}$ est un corps $\mathbf{L}$ tel que $\mathbf{K}$ est un sous-corps de $\mathbf{L}$, dans ce cas, on note $\mathbf{L}/\mathbf{K}$. Le degré de $\mathbf{L}$ sur $\mathbf{K}$, noté $[\mathbf{L} : \mathbf{K}]$, est par définition égal à la dimension du $\mathbf{K}$-espace vectoriel $\mathbf{L}$. Puisqu'un homomorphisme de corps est toujours injectif, deux corps $\mathbf{K}$ et

$\mathbf{L}$ sont tels que $\mathbf{L}$ est une extension de $\mathbf{K}$ s'il existe un homomorphisme de corps de $\mathbf{K}$ dans $\mathbf{L}$. Dans ce cas, on identifie $\mathbf{K}$ au sous-corps de $\mathbf{L}$ correspondant. On voit aisément que $\mathbb{Q}(\sqrt[3]{5})$ est une extension de degré 3 sur $\mathbb{Q}$, que $\mathbb{C}$ est une extension de degré 2 sur $\mathbb{R}$ et que $\mathbb{C}(X)$ est une extension de degré infini sur $\mathbb{C}$. Le principe de la base télescopique assure que si $\mathbf{L}/\mathbf{K}$ et $\mathbf{M}/\mathbf{L}$ sont deux extensions finies (*i.e* de degrés respectifs finis), alors $\mathbf{M}/\mathbf{K}$ est aussi une extension finie, et on a

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}].$$

Définition 1.1.1. Soient $\mathbf{L}$ et $\mathbf{L}'$ deux extensions d'un même corps $\mathbf{K}$ et σ un isomorphisme de corps de $\mathbf{L}$ sur $\mathbf{L}'$. On dit que σ est un $\mathbf{K}$-isomorphisme si $\sigma(x) = x$ pour tout $x \in \mathbf{K}$, dans ce cas, on dit aussi que les corps $\mathbf{L}$ et $\mathbf{L}'$ sont $\mathbf{K}$-conjugués.

Par exemple la conjugaison complexe

$$\begin{array}{rccc} \sigma : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \overline{z} \end{array}$$

est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

1.1.2 Extensions algébriques

Les extensions et éléments algébriques font partie des éléments fondamentaux de notre étude.

Définition 1.1.2. Soient $\mathbf{L}/\mathbf{K}$ une extension de corps et θ un élément de $\mathbf{L}$.

1. On appelle équation polynômiale de θ sur $\mathbf{K}$ toute équation de la forme $P(\theta) = 0$, où $P(X) \in \mathbf{K}[X]$. Le degré de cette équation est le degré de $P(X)$.
2. On dit que $\theta \in \mathbf{L}$ est algébrique sur $\mathbf{K}$ s'il existe un polynôme non-constant $P(X) \in \mathbf{K}[X]$ tel que $P(\theta) = 0$. Un élément qui n'est pas algébrique est dit transcendant.
3. On dit qu'une extension de corps $\mathbf{L}/\mathbf{K}$ est algébrique si tout élément de $\mathbf{L}$ est algébrique sur $\mathbf{K}$.
4. S'il existe un élément de $\mathbf{L}$ qui n'est pas algébrique sur $\mathbf{K}$, alors on dit que $\mathbf{L}/\mathbf{K}$ est une extension transcendante.
5. Soit S un sous-ensemble de $\mathbf{L}$. On dit que S est algébriquement indépendant si toute combinaison linéaire nulle de produits d'éléments de S de la forme

$$\sum a_v \prod_{x \in S} x^{v(x)} = 0$$

à coefficients dans $\mathbf{K}$ où presque tous les a_v sont nuls, implique que tous les a_v sont nuls.

6. Si S est une partie de $\mathbf{L}$ algébriquement indépendante telle que S a le plus grand cardinal parmi tous les sous-ensembles de $\mathbf{L}$ algébriquement indépendants, alors on dit que le cardinal de S est le degré de transcendance de $\mathbf{L}$ sur $\mathbf{K}$.

Considérons une extension de corps $\mathbf{L}/\mathbf{K}$ et θ un élément de $\mathbf{L}$ algébrique sur $\mathbf{K}$. Soit $\varphi : \mathbf{K}[X] \longrightarrow \mathbf{L}$ l'unique homomorphisme d'anneaux tel que $\varphi(X) = \theta$ et pour tout $a \in \mathbf{K}$, $\varphi(a) = a$. Le noyau $\ker(\varphi)$ est un idéal maximal de $\mathbf{K}[X]$. Puisque $\mathbf{K}[X]$ est un anneau principal, il est engendré par un unique polynôme unitaire irréductible $\mathrm{Irr}_{\theta,\mathbf{K}}$: c'est le polynôme minimal de θ sur $\mathbf{K}$. L'image $\varphi(\mathbf{K}[X]) = \mathbf{K}[\theta]$ est isomorphe à $\mathbf{K}[X]/\ker(\varphi)$ et c'est un sous-corps de $\mathbf{L}$.

Exemple 1.1.1.

1. *Pour $n \in \mathbb{N}^*$, les nombres complexes $z = \exp(\frac{2i\pi}{n})$ sont algébriques sur $\mathbb{Q}$, car ils vérifient $z^n = 1$.*
2. *Le corps $\overline{\mathbb{Q}}$ des nombres complexes $z \in \mathbb{C}$ algébriques sur $\mathbb{Q}$ est appelé le corps des nombres algébriques. Il a les propriétés suivantes :*

(i) $\overline{\mathbb{Q}}$ *est dénombrable du fait que* $\mathbb{Q}[X]$ *est dénombrable (en effet un polynôme de degré* n *sur un corps a au plus* n *racines) ;*

(ii) l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ *n'est pas finie car, il existe dans* $\mathbb{Q}[X]$ *des polynômes irréductibles de degré aussi grand que l'on veut. Par exemple* $\sqrt[n]{2}$ *est de degré* n *: en effet, c'est un zéro du polynôme minimal* $X^n - 2$.

3. *Puisque le corps* $\mathbb{R}$ *n'est pas dénombrable, il existe des nombres réels qui ne sont pas algébriques ; par exemple* e *et* π *sont transcendants.*

Notons que toutes les extensions algébriques ne sont pas finies, mais une extension finie est toujours algébrique. Il est établie que si $\mathbf{L}/\mathbf{K}$ est une extension finie alors il existe une suite finie d'éléments algébriques $x_1, \ldots, x_n \in \mathbf{L}$ tel que $\mathbf{L} = \mathbf{K}(x_1, \ldots, x_n)$.

Définition 1.1.3. *Une extension de corps* $\mathbf{L}/\mathbf{K}$ *est dite simple ou monogène s'il existe* $x \in \mathbf{L}$ *telle que* $\mathbf{L} = \mathbf{K}(x)$. *Dans ce cas, on dit que* x *est un élément primitif de* $\mathbf{L}/\mathbf{K}$.

Exemple 1.1.2.

1. $\mathbb{C}$ *est une extension simple de* $\mathbb{R}$, *car* $\mathbb{C} = \mathbb{R}(i)$.
2. $\mathbf{K}(X)$ *est une extension monogène de* $\mathbf{K}$.
3. *Toute extension quadratique* $\mathbf{K}$ *de* $\mathbb{Q}$ *est monogène : il existe un entier* $d \in \mathbb{Z}$ *sans facteur carré tel que* $\mathbf{K} = \mathbb{Q}(\sqrt{d})$.

Soient $\mathbf{L}/\mathbf{K}$ une extension de corps et x un élément de $\mathbf{L}$. Considérons l'application de multiplication par x :

$$\begin{array}{rccc} m_x : & \mathbf{L} & \longrightarrow & \mathbf{L}. \\ & y & \longmapsto & xy \end{array}$$

C'est une application $\mathbf{K}$-linéaire, autrement dit c'est un endomorphisme du $\mathbf{K}$-espace vectoriel $\mathbf{L}$. On note $\chi_{\mathbf{L}/\mathbf{K}}(m_x) \in \mathbf{K}[X]$ le polynôme caractéristique de m_x, $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x)$ sa trace, et $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(x)$ son déterminant.

Définition et proposition 1.1.1. L'application $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}} : \mathbf{L} \longrightarrow \mathbf{K}$ ainsi définie est $\mathbf{K}$-linéaire, on l'appelle la trace de $\mathbf{L}/\mathbf{K}$. De même, l'application $\mathrm{N}_{\mathbf{L}/\mathbf{K}} : \mathbf{L} \longrightarrow \mathbf{K}$ est multiplicative : $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(xy) = \mathrm{N}_{\mathbf{L}/\mathbf{K}}(x)\mathrm{N}_{\mathbf{L}/\mathbf{K}}(y)$ pour tout $x, y \in \mathbf{L}$, on l'appelle la norme de $\mathbf{L}/\mathbf{K}$.

Exemple 1.1.3. *Considérons par exemple le cas du corps quadratique* $\mathbf{L} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Q}$ *non carré, et* $\mathbf{K} = \mathbb{Q}$. *Alors* $\{1, \sqrt{d}\}$ *est une* $\mathbb{Q}$*-base de* $\mathbb{Q}(\sqrt{d})$. *La matrice de la multiplication par* $x = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$ *dans cette base est visiblement*

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

et donc $Tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = 2a$ *et* $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = a^2 - db^2$. *Remarquons que la multiplicativité de la norme explique notamment l'identité remarquable* $(a^2 - db^2) \times (a'^2 - db'^2) = (aa' + dbb')^2 - d(ab' + a'b)^2$ *pour tous* $a, a', b, b' \in \mathbb{Q}$, *car* $(a + b\sqrt{d}) \times (a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + a'b)\sqrt{d}$.

Si x est un élément générateur de $\mathbf{L}/\mathbf{K}$ avec un polynôme minimal

$$\mathrm{Irr}_{x,\mathbf{K}} = X^d + a_{d-1}X^{d-1} + \cdots + a_0,$$

alors $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x) = -a_{d-1}$ et $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(x) = (-1)^d a_0$. Nous utiliserons les notations $\mathrm{Tr}(x)$ et $\mathrm{N}(x)$ s'il n'y a pas de confusion possible.

Lemme 1.1.1. *Soit* $\mathbf{L}/\mathbf{K}$ *une extension algébrique de degré fini* d. *Pour* $x, y \in \mathbf{L}$ *et* $a \in \mathbf{K}$, *on a*

$$\begin{array}{cc} Tr(x+y) = Tr(x) + Tr(y), & N(xy) = N(x)N(y) \\ Tr(a) = da, & N(a) = a^d \\ Tr(ax) = a\,Tr(x), & N(x) = 0 \ \Rightarrow x = 0. \end{array}$$

Soient $\mathbf{L}/\mathbf{K}$ *et* $\mathbf{M}/\mathbf{L}$ *deux extensions algébriques finies, soit* x *un élément de* M. *Alors* $Tr_{\mathbf{M}/\mathbf{K}}(x) = Tr_{\mathbf{L}/\mathbf{K}}(Tr_{\mathbf{M}/\mathbf{L}}(x))$ *et* $N_{\mathbf{M}/\mathbf{K}}(x) = N_{\mathbf{L}/\mathbf{K}}(N_{\mathbf{M}/\mathbf{L}}(x))$.

1.1.3 Clôture algébrique

Soit $\mathbf{K}(x)/\mathbf{K}$ une extension algébrique monogène de corps. Le polynôme $\mathrm{Irr}_{x,\mathbf{K}}(X)$ se décompose en produit $\prod_i P_i(X)$ de polynômes irréductibles sur $\mathbf{K}(x)$. En effet, par construction x est une racine de $\mathrm{Irr}_{x,\mathbf{K}}(X)$ dans $\mathbf{K}(x)$. Donc $(X-x)$ est un facteur irréductible de $\mathrm{Irr}_{x,\mathbf{K}}(X)$. Par conséquent pour chaque i, $\deg(P_i) < \deg(\mathrm{Irr}_{x,\mathbf{K}})$. Si les $P_i(X)$ sont tous de degré 1 alors on dit que $\mathrm{Irr}_{x,\mathbf{K}}(X)$ se factorise complètement dans $\mathbf{K}(x)$. Dans le cas où le polynôme $\mathrm{Irr}_{x,\mathbf{K}}(X)$ ne se factorise pas complètement dans $\mathbf{K}(x)$, il admet un facteur $P_{i_1}(X)$ irréductible sur $\mathbf{K}(x)$ de degré supérieur ou égal à 2 et on peut considérer l'extension $\mathbf{K}(x,y)/\mathbf{K}(x)$ définie par $P_{i_1}(X)$ (*i.e* $\mathbf{K}(x,y) = \mathbf{K}(x)[Y]/(P_{i_1}(Y))$. En répétant ce processus, on peut construire récursivement une extension de $\mathbf{K}$ dans laquelle $\mathrm{Irr}_{x,\mathbf{K}}(X)$ se factorise complètement.

Définition 1.1.4.
1. La plus petite extension de $\mathbf{K}$ dans laquelle $\mathrm{Irr}_{x,\mathbf{K}}$ se factorise complètement est appelée le corps de décomposition de $\mathrm{Irr}_{x,\mathbf{K}}$. Elle est unique à $\mathbf{K}$-isomorphisme près.
2. Une extension $\mathbf{L}/\mathbf{K}$ est appelée corps de rupture pour un polynôme $P(X) \in \mathbf{K}[X]$, si $\mathbf{L}$ contient au moins une racine de P.

Exemple 1.1.4.
1. $\mathbb{C}$ est un corps de rupture et de décomposition du polynôme X^2+1 sur $\mathbb{R}$.
2. $\mathbb{Q}$ est un corps de rupture et de décomposition du polynôme X^2-1 sur $\mathbb{Q}$.
3. $\mathbb{R}$ et $\mathbb{Q}(\sqrt{2})$ sont respectivement des corps de rupture et de décomposition du polynôme X^2-2 sur $\mathbb{Q}$.

Il est bien connu que tout polynôme à coefficients dans $\mathbb{R}$ se factorise complètement dans $\mathbb{C}$. Plus généralement, si $\mathbf{K}$ est un corps, nous voudrions considérer une extension algébrique de $\mathbf{K}$ dans laquelle chaque extension algébrique de $\mathbf{K}$ pourrait être incluse. Une telle extension a la propriété que tout polynôme de $\mathbf{K}[X]$ s'y factorise complètement. Le théorème suivant affirme son existence.

Définition et proposition 1.1.2. *Soit* $\mathbf{K}$ *un corps, les propriétés suivantes sont équivalentes :*
1. $\mathbf{K}$ *n'admet pas d'extension algébrique* $\mathbf{L}$ *telle que* $\mathbf{K} \neq \mathbf{L}$ *;*
2. *les polynômes irréductibles de* $\mathbf{K}[X]$ *sont les polynômes de degré* 1 *;*
3. *tout polynôme non constant à coefficients dans* $\mathbf{K}$ *possède une racine dans* $\mathbf{K}$ *;*
4. *tout polynôme non constant à coefficients dans* $\mathbf{K}$ *se factorise complètement dans* $\mathbf{K}$*.*

On dit que $\mathbf{K}$ *est un corps algébriquement clos s'il possède une des propriétés ci-dessus.*

Une clôture algébrique d'un corps $\mathbf{K}$ est une extension algébrique $\mathbf{L}/\mathbf{K}$ telle que $\mathbf{L}$ est algébriquement clos.

Théorème 1.1.1 (Steinitz). *Il existe une extension algébrique de* $\mathbf{K}$ *(unique à* $\mathbf{K}$*-isomorphisme près) dans laquelle chaque polynôme* $\mathrm{Irr}_{x,\mathbf{K}} \in \mathbf{K}[X]$ *se factorise complètement. Cette extension appelée la clôture algébrique de* $\mathbf{K}$ *est notée par* $\overline{\mathbf{K}}$*.*

Exemple 1.1.5.
1. $\mathbb{C}$ est algébriquement clos. C'est le théorème de d'Alembert-Gauss, aussi appelé théorème fondamental de l'algèbre.
2. $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

Maintenant, nous pouvons passer en revue certaines propriétés de base des extensions algébriques afin d'énoncer le théorème fondamental de la théorie de Galois.

1.1.4 Théorème fondamental de la théorie de Galois

À de partir de cette section, et ce jusqu'à la fin du document, nous ne considérons que des extensions algébriques finies. Par conséquent, nous restreignons la discussion de la théorie de Galois à ce cas.

Définition 1.1.5. Soit $\mathbf{L}/\mathbf{K}$ une extension de corps.

1. Une extension $\mathbf{L}/\mathbf{K}$ est dite normale si tout polynôme irréductible sur $\mathbf{K}$ qui a une racine dans $\mathbf{L}$ se factorise complètement dans $\mathbf{L}$.
2. Une clôture normale de $\mathbf{L}$ est une extension normale $\mathbf{N}/\mathbf{K}$ qui satisfait les conditions suivantes :
   i) $\mathbf{K} \subset \mathbf{L} \subset \mathbf{N}$;
   ii) si $\mathbf{M}/\mathbf{K}$ est une extension normale vérifiant $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M} \subset \mathbf{N}$, alors $\mathbf{M} = \mathbf{N}$

Exemple 1.1.6 (exemple et contre exemple)**.**

1. $\mathbb{C}$ est une extension normale de degré 2 de $\mathbb{R}$ (en effet $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$).
2. L'extension $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ n'est pas une extension normale, car le polynôme $X^3 - 5 \in \mathbb{Q}[X]$ possède une racine dans $\mathbb{Q}(\sqrt[3]{5})$ sans se décomposer en produit de polynômes linéaires dans $\mathbb{Q}(\sqrt[3]{5})[X]$ (en effet ni $e^{\frac{2i\pi}{3}}\sqrt[3]{5}$, ni $e^{\frac{4i\pi}{3}}\sqrt[3]{5}$ n'appartiennent à $\mathbb{Q}(\sqrt[3]{5})$).
3. $\mathbb{C}$ est la clôture normale de l'extension $\mathbb{R}/\mathbb{Q}$.

Tout $\mathbf{K}$-automorphisme du corps $\mathbf{L}$ laisse $\mathbf{L}$ invariant. Soient $\mathbf{K}$ un corps, $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$, et σ un plongement [1] de $\mathbf{K}$ dans $\overline{\mathbf{K}}$. Étant donné un élément $x \in \overline{\mathbf{K}}$, on note $\mathbf{K}(x)$ le sous-corps de $\overline{\mathbf{K}}$ engendré par x sur $\mathbf{K}$. C'est une extension simple de $\mathbf{K}$ définie par le polynôme $\mathrm{Irr}_{x,\mathbf{K}}(X)$, on note d le degré de $\mathbf{K}(x)$ sur $\mathbf{K}$. Soient $x = x_1, x_2, \ldots, x_r$ les différentes racines de $\mathrm{Irr}_{x,\mathbf{K}}$ dans $\overline{\mathbf{K}}$. Alors on dit que les x_i sont les conjugués de x. En effet pour chaque $i \in \{1, \ldots, r\}$, il existe un unique plongement σ_i de $\mathbf{K}(x)$ dans $\overline{\mathbf{K}}$ tel que la restriction de σ_i à $\mathbf{K}$ soit égale à σ et $\sigma_i(x) = x_i$. Les σ_i sont tous des plongements de $\mathbf{K}(x)$ dans $\overline{\mathbf{K}}$, dont la restriction sur $\mathbf{K}$ est égale à σ. Il est clair que r est inférieur ou égal à d. L'entier r est appelé le degré de séparabilité de $\mathbf{K}(x)$ sur $\mathbf{K}$ ou le degré de séparabilité de x. Plus généralement, nous avons :

Définition 1.1.6. Soient $\mathbf{L}/\mathbf{K}$ une extension algébrique finie, $\overline{\mathbf{K}}$ la clôture algébrique de $\mathbf{K}$ et σ un plongement de $\mathbf{K}$ dans $\overline{\mathbf{K}}$. Alors, le degré de séparabilité de $\mathbf{L}$ sur $\mathbf{K}$ noté $\deg_s(\mathbf{L}/\mathbf{K})$ est le nombre r de plongements distincts $\sigma_i,\ i = 1, \ldots, r$ de $\mathbf{L}$ dans $\overline{\mathbf{K}}$ dont la restriction à $\mathbf{K}$ est égale à σ. Lorsque $\deg_s(\mathbf{L}/\mathbf{K}) = \deg(\mathbf{L}/\mathbf{K})$, on dit que $\mathbf{L}/\mathbf{K}$ est séparable.
Un élément $x \in \mathbf{L}$ est dit séparable sur $\mathbf{K}$ si, toutes les racines de son polynôme minimal $\mathrm{Irr}_{x,\mathbf{K}}$ sont simples.

Une conséquence immédiate de la définition et de la discussion précédente est :

Lemme 1.1.2. *Une extension simple* $\mathbf{K}(x)/\mathbf{K}$ *définie par un polynôme minimal* $\mathrm{Irr}_{x,\mathbf{K}}$ *est séparable si et seulement si* $\mathrm{Irr}_{x,\mathbf{K}}$ *est premier à sa dérivée* $\mathrm{Irr}'_{x,\mathbf{K}}$.

En ce qui concerne la séparabilité dans une tour d'extensions, nous avons

Proposition 1.1.1. *Soit* $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$ *une tour d'extensions, alors*

$$\deg_s(\mathbf{M}/\mathbf{K}) = \deg(\mathbf{L}/\mathbf{K})_s \times \deg(\mathbf{M}/\mathbf{L})_s.$$

De la proposition précédente, nous déduisons qu'une extension algébrique finie est séparable si et seulement si elle peut être écrite comme une tour d'extensions monogènes séparables.

1. Un homomorphisme de $\mathbf{K}$ dans sa clôture algébrique.

Proposition 1.1.2. *1. Une extension algébrique finie* $\mathbf{L}/\mathbf{K}$ *est séparable si et seulement si chaque* $x \in \mathbf{L}$ *est séparable sur* $\mathbf{K}$.

2. Soit $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$ *une tour d'extensions telle que* $\mathbf{M}$ *est séparable sur* $\mathbf{K}$, *alors* $\mathbf{M}$ *est séparable sur* $\mathbf{L}$ *et* $\mathbf{L}$ *est séparable sur* $\mathbf{K}$.

Définition 1.1.7. Un corps $\mathbf{K}$ tel que chaque extension algébrique de $\mathbf{K}$ est séparable est appelé corps parfait.

On montre qu'un corps $\mathbf{K}$ est parfait si et seulement si l'application $x \mapsto x^p$ est un endomorphisme surjectif de $\mathbf{K}$. Donc un corps $\mathbf{K}$ est parfait si et seulement si l'une des conditions suivantes est réalisée

- $\mathrm{char}(\mathbf{K}) = 0$,
- $\mathrm{char}(\mathbf{K}) = p$ et $\mathbf{K}^p = \mathbf{K}$.

Par conséquent tout corps fini est parfait.

Théorème 1.1.2 (de l'élément primitif)**.** *Soit* $\mathbf{L}/\mathbf{K}$ *une extension algébrique finie et séparable. Alors* $\mathbf{L}/\mathbf{K}$ *est monogène, c'est-à-dire, il existe* $x \in \mathbf{L}$ *tel que* $\mathbf{L} = \mathbf{K}(x)$. *Un tel* x *est appelé élément primitif de* $\mathbf{L}$ *sur* $\mathbf{K}$.

Exemple 1.1.7.

1. $\mathbb{C}/\mathbb{R}$ est une extension séparable car le nombre complexe i est séparable sur $\mathbb{R}$.
2. $\sqrt{2}$ est séparable sur $\mathbb{Q}$.

Définition 1.1.8. Une extension $\mathbf{L}/\mathbf{K}$ est dite galoisienne si elle est normale et séparable. Dans ce cas le groupe de Galois de $\mathbf{L}$ sur $\mathbf{K}$, noté $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$, est le groupe des $\mathbf{K}$-automorphismes de $\mathbf{L}$.

Il existe une action naturelle de $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ sur $\mathbf{L}$ définie par

$$\forall \sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \ \text{ et } \ \forall x \in \mathbf{L},\ \sigma \cdot x = \sigma(x).$$

Par sa définition même, cette action laisse les éléments de $\mathbf{K}$ invariants. Si H est un sous-groupe de $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$, on note $\mathbf{L}^H$ l'ensemble des éléments de $\mathbf{L}$ invariant sous l'action de H. Évidemment $\mathbf{L}^H$ est un sous-corps de $\mathbf{L}$. De plus, $\mathbf{L}^H$ est une extension normale (et donc galoisienne) de $\mathbf{K}$ si et seulement si H est un sous-groupe normal de $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$.

La condition de séparabilité des extensions de Galois implique que l'ordre du groupe de Galois de $\mathbf{L}/\mathbf{K}$ est égal au degré de cette extension. Maintenant nous présentons le résultat le plus important de cette section..

Théorème 1.1.3 (fondamental de la théorie de Galois)**.** *Soit* $\mathbf{L}/\mathbf{K}$ *une extension galoisienne finie. Alors, il y a une bijection entre l'ensemble des sous-corps de* $\mathbf{L}$ *contenant* $\mathbf{K}$ *et les sous-groupes de* $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$. *À un sous-groupe* H *de* $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ *cette bijection associe le sous-corps* $\mathbf{L}^H$ *de* $\mathbf{L}$.

Exemple 1.1.8. $\mathbb{C}/\mathbb{R}$ est une exention galoisienne, en effet : $G_{\mathbb{C}/\mathbb{R}} = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$ où σ est la conjugaison complexe. Plus généralement toute extension quadratique (*i.e* de degré 2) est galoisienne.

1.2 Le cas des corps finis

Les corps finis sont des objets centraux en cryptographie, car ils jouissent de propriétés très particulières. Par exemple, leur groupe multiplicatif est cyclique et leur structure galoisienne est remarquablement simple.

Nous nous sommes inspirés principalement de [Sam71] et [LN97] pour la conception cette section.

La proposition élémentaire suivante est très utilisée dans la pratique pour la construction des corps.

Proposition 1.2.1. *Soient A un anneau et I un idéal de A. Alors le quotient A/I est un corps si et seulement si I est un idéal maximal de A.*

1.2.1 Définitions et propriétés de base

Définition 1.2.1. *On appelle corps fini tout corps ayant un nombre fini d'éléments.*

Pour tout nombre premier p, le quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps fini : c'est le corps à p éléments que l'on note $\mathbb{F}_p$.

Le théorème suivant classifie tous les corps finis.

Théorème 1.2.1 (Théorème fondamental)**.**

1. *La caractéristique d'un corps fini $\mathbf{K}$ est un nombre premier p. Si $d = [\mathbf{K} : \mathbb{F}_p]$, alors le cardinal de $\mathbf{K}$ est égal à p^d.*
2. *Soient $q = p^d$ où p est un nombre premier et $d > 0$ un entier naturel. Alors il existe un corps fini de cardinal q, unique à isomorphisme près : c'est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$, on le note $\mathbb{F}_q$ (autrement dit les éléments x de $\mathbb{F}_q$ vérifient l'équation $x^q = x$.)*
3. *Pour tout corps fini $\mathbb{F}_q$ tel que $q = p^d$, il existe un polynôme unitaire irréductible $f(X) \in \mathbb{F}_p[X]$ de degré d tel que $\mathbb{F}_q \cong \mathbb{F}_p[X]/(f(X))$.*

Définition 1.2.2. Un corps qui ne contient aucun sous-corps propre est appelé un corps premier.

Donc un corps premier $\mathbf{K}$ est soit isomorphe au corps $\mathbb{Q}$ des nombres rationnels, ou bien $\mathbf{K}$ est isomorphe à un corps fini $\mathbb{F}_p$ où p est un nombre premier . Par ailleurs, il y a une bijection entre les sous-corps de $\mathbb{F}_{p^d}$ et les diviseurs de d :

$$\mathbb{F}_{p^c} \subset \mathbb{F}_{p^d} \quad \text{si et seulement si} \quad c \mid d.$$

Ainsi

$$\mathbb{F}_{p_1^d} \cap \mathbb{F}_{p_2^d} = \mathbb{F}_{p^{\mathrm{pgcd}(d_1,d_2)}} \quad \text{et} \quad \mathbb{F}_{p_1^d} \cdot \mathbb{F}_{p_2^d} = \mathbb{F}_{p^{\mathrm{ppcm}(d_1,d_2)}}.$$

où $\mathbb{F}_{p_1^d} \cdot \mathbb{F}_{p_2^d}$ désigne le compositum des corps $\mathbb{F}_{p_1^d}$ et $\mathbb{F}_{p_2^d}$, c'est-à-dire le plus petit corps contenant $\mathbb{F}_{p_1^d}$ et $\mathbb{F}_{p_2^d}$ dans une clôture algébrique de $\mathbb{F}_p$.

D'après le théorème de Lagrange

$$a^{q-1} = 1 \quad \text{pour tout} \quad a \in \mathbb{F}_q^*.$$

C'est en quelque sorte une généralisation du petit théorème de Fermat, et cela a des conséquences importantes. Par exemple, cela implique que tout corps fini n'est pas algébriquement clos. En effet le polynôme $X^q - X + 1 \in \mathbb{F}_q[X]$ n'a pas de racine dans $\mathbb{F}_q$.

Théorème 1.2.2. *Soit $\mathbb{F}_q$ un corps fini. Le groupe $\mathbb{F}_q^*$ est cyclique.*

Un générateur γ de $\mathbb{F}_q^*$, c'est-à-dire un élément tel que $\mathbb{F}_q^* = \langle\gamma\rangle$, est appelé élément primitif.

Remarque 1.2.1. Il est facile de voir qu'il existe $\varphi(q-1)$ éléments primitifs, où φ est la fonction indicatrice d'Euler. Plus généralement, si $l \mid (q-1)$ alors il y a exactement $\varphi(l)$ éléments d'ordre l dans $\mathbb{F}_q$. Notez également que l'application $a \to a^l$ est une bijection de $\mathbb{F}_q^*$ si et seulement si $\mathrm{pgcd}(l, q-1) = 1$.

Les corps finis ont des extensions transcendantes. Par exemple, $\mathbb{F}_q(X)$ est une extension du corps $\mathbb{F}_q$,qui n'est pas algébrique sur $\mathbb{F}_q$. Cependant, dans la suite, nous nous focalisons sur les extensions algébriques d'un corps fini.

1.2.2 Extensions algébriques d'un corps fini

Il existe des extensions algébriques de $\mathbb{F}_q$ de degré infini, le premier exemple étant $\overline{\mathbb{F}}_q$, la clôture algébrique de $\mathbb{F}_q$. Concernant les extensions finies, le corps $\mathbb{F}_q$ étant parfait, (voir page 11), cela implique que $\mathbb{F}_{q^k}/\mathbb{F}_q$ peut toujours s'écrire $\mathbb{F}_q(\alpha)$, où α est un élément algébrique de degré k sur $\mathbb{F}_q$ (cf. Théorème 1.1.2 de l'élément primitif).

La représentation polynomiale d'une extension de $\mathbb{F}_q$ donne un moyen pratique de construire $\mathbb{F}_{q^k}$. Puisqu'il existe un corps fini unique de cardinal q^k contenu dans $\overline{\mathbb{F}}_q$, il suffit de trouver un polynôme de degré k irréductible sur $\mathbb{F}_q$. Gauss a établi l'égalité

$$X^{q^k} - X = \prod_{j \mid k} \prod_{P \in \mathcal{I}_j} P(X) \tag{1.3}$$

où $\mathcal{I}_j$ est l'ensemble de tous les polynômes unitaires irréductibles de degré j dans $\mathbb{F}_q[X]$. Il s'ensuit que le le nombre de polynômes unitaires irréductibles de degré k sur $\mathbb{F}_q$ est donné par la formule

$$\frac{1}{k} \sum_{j \mid k} \mu(j) q^{k/j} \tag{1.4}$$

où μ est la fonction de Möbius [2] . En conséquence, il existe au moins un polynôme irréductible de degré k sur $\mathbb{F}_q$, pour tout $k \geq 1$.

La relation (1.2) (page 6) montre que l'appliation $\alpha \longmapsto \alpha^p$ est un automorphisme de $\mathbb{F}_p$.

Définition 1.2.3. Soient p un nombre premier et α un élément de $\mathbb{F}_{q^k}$. L'application $\phi_p : \alpha \longmapsto \alpha^p$, est un $\mathbb{F}_p$-automorphisme appelé automorphisme absolu de Frobenius de $\mathbb{F}_{q^k}$. Plus généralement, l'application

$$\begin{array}{rccc} \phi_q : & \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_{q^k} \\ & \alpha & \longmapsto & \alpha^q \end{array}$$

est un $\mathbb{F}_q$-automorphisme de $\mathbb{F}_{q^k}$ appelé automorphisme Frobenius relatif de $\mathbb{F}_{q^k}/\mathbb{F}_q$.

Théorème 1.2.3. *Chaque extension finie $\mathbb{F}_{q^k}/\mathbb{F}_q$ est galoisienne et le groupe* $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ *de Galois est un groupe cyclique d'ordre k engendré par ϕ_q.*

Si $\mathrm{Irr}_{x,\mathbf{K}} \in \mathbb{F}_q[X]$ est un polynôme irréductible de degré k, il se décompose complètement en $\mathbb{F}_{q^k}$. Si α est une racine de $\mathrm{Irr}_{x,\mathbf{K}}$ dans $\mathbb{F}_{q^k}$, on voit par calcul direct que les conjugués de α sont les éléments distincts $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}}$ de $\mathbb{F}_{q^k}$.

2. La fonction de Möbius μ est définie de $\mathbb{N}^*$ dans $\{-1, 0, 1\}$.
L'image $\mu(n)$ d'un entier $n > 0$ vaut :

- 0 si n est divisible par un carré parfait différent de 1 ;
- 1 si n est le produit d'un nombre pair de nombres premiers distincts ;
- -1 si n est le produit d'un nombre impair de nombres premiers distincts.

Chapitre 2

Rappels sur la géométrie algébrique

Tout au long de ce chapitre, $\mathbf{K}$ désigne un corps parfait (cf. chapitre 1) et $\overline{\mathbf{K}}$ une clôture algébrique fixée de $\mathbf{K}$, $\mathbf{L}$ désigne une extension de $\mathbf{K}$ contenue dans $\overline{\mathbf{K}}$. On note $\mathrm{Aut}_{\mathbf{L}}\left(\overline{\mathbf{K}}\right)$ (ou bien $G_{\mathbf{L}}$) son groupe de Galois absolu.

2.1 Variétés affines

Terminologies

1. On appelle espace affine de dimension n sur $\mathbf{K}$, et on note $\mathbb{A}^n(\overline{\mathbf{K}})$ ou encore $\mathbb{A}^n$, l'ensemble $\overline{\mathbf{K}}^n$, produit cartésien itéré n fois du corps $\overline{\mathbf{K}}$.
2. Les éléments de l'espace affine sont appelés points.
3. $\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement la droite et le plan affine.
4. Un point a de $\mathbb{A}^n$ est dit zéro d'un polynôme $P(X) \in \mathbf{K}[X_1, \ldots, X_n]$ si $P(a) = 0$.

Définition 2.1.1. Soit $\mathbf{L}/\mathbf{K}$ une extension de corps. L'ensemble des points $\overline{\mathbf{K}}$-rationnels de l'espace affine de dimension n sur $\mathbf{K}$ est l'ensemble des n-uplets

$$\mathbb{A}^n(\overline{\mathbf{K}}) := \{\ (x_1, \ldots, x_n) \mid x_i \in \overline{\mathbf{K}},\ i = 1, \ldots, n\ \}.$$

L'ensemble des points $\mathbf{L}$-rationnels est donné par

$$\mathbb{A}^n(\mathbf{L}) := \{\ (x_1, \ldots, x_n) \mid x_i \in \mathbf{L},\ i = 1, \ldots, n\ \}.$$

qui est l'ensemble des points de $\mathbb{A}^n(\overline{\mathbf{K}})$ G_L-invariants sous l'action naturelle sur les coordonnées.

Soit S une partie quelconque de $\mathbf{K}[X_1, \ldots, X_n]$. On pose :

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

de sorte que les $a \in \mathcal{V}(S)$ sont les zéros communs à tous les polynômes de S.

Définition 2.1.2. On dit que $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S.

On notera souvent, dans le cas d'un ensemble fini, $\mathcal{V}(P_1, \ldots, P_r)$ au lieu de $\mathcal{V}(\{P_1, \ldots, P_r\})$, pour $S = (P_i)_{i=1,\ldots,r}$ une famille d'éléments de $\mathbf{K}[X_1, \ldots, X_n]$.

Définition 2.1.3. On appelle hypersurface définie par $P \in \mathbf{K}[X_1, \ldots, X_n]$, et on note $\mathcal{V}(P)$, l'ensemble des zéros de P dans $\mathbb{A}^n$. Le degré de $\mathcal{V}(P)$ est le degré de P.

Une courbe plane affine est une hypersurface du plan affine. Une courbe plane affine est dite conique, cubique, quartique,... si le degré est respectivement 2, 3, 4, ...

Un hyperplan est une hypersurface définie par un polynôme de degré 1. Une droite est un hyperplan de $\mathbb{A}^2$.

Exemple 2.1.1.

1. Le vide et l'espace tout entier sont des ensembles algébriques affines. En effet, on a :
   — $\mathcal{V}(k) = \emptyset$, car le polynôme constant égal à k ne s'annule jamais pour $k \in \mathbf{K} - \{0\}$.
   — $\mathcal{V}(0) = \mathbf{K}^n$, car le polynôme constant 0 est identiquement nul.
2. Si $n = 1$ et si S n'est pas réduit à 0, $\mathcal{V}(S)$ est un ensemble fini : les ensembles algébriques affines de la droite affine sont l'ensemble vide, la droite affine elle-même et les ensembles finis.

Remarques 2.1.1.

1. Soit $\mathcal{V}(S) = \{a \in \mathbb{A}^n \mid \forall\ P \in S,\ P(a) = 0\}$.
   Si deux polynômes P_1 et P_2 s'annulent sur $\mathcal{V}(S)$, il en sera de même pour $P_1 + P_2$ et λP_1 pour tout $\lambda \in \mathbf{K}$. Ainsi, au lieu d'une famille quelconque de polynômes, on s'intéresse aux idéaux de $\mathbf{K}[X_1, \ldots, X_n]$.
2. L'application $\mathcal{V}$ est décroissante : si $S_1 \subset S_2$, alors $\mathcal{V}(S_2) \subset \mathcal{V}(S_1)$.
3. Si $S \subset \mathbf{K}[X_1, \ldots, X_n]$, notons $\langle S \rangle$ l'idéal engendré par S :
$$\langle S \rangle = \{P \mid P = \sum_{i=1}^{r} \lambda_i P_i \text{ avec } P_i \in S \text{ et } \lambda_i \in \mathbf{K}\}.$$
   Alors , par décroissance de $\mathcal{V}$, on a $\mathcal{V}(\langle S \rangle) \subset \mathcal{V}(S)$. Réciproquement, si $a \in \mathcal{V}(S)$, il annule les $P_i \in S$, donc aussi les $P \in \langle S \rangle$.
   Ainsi, on a $\mathcal{V}(\langle S \rangle) = \mathcal{V}(S)$; on peut donc, pour étudier les ensembles algébriques affines, se limiter aux S qui sont des idéaux, ou simplement aux générateurs de ceux-ci.
4. Comme $\mathbf{K}[X_1, \ldots, X_n]$ est noethérien, tout idéal I est de type fini : $I = \langle P_1, \ldots, P_r \rangle$.
   Donc tout ensemble algébrique affine est défini par un nombre fini d'équations : $\mathcal{V}(I) = \mathcal{V}(P_1, \ldots, P_r)$.

Proposition 2.1.1.

1. *Un point de $\mathbb{A}^n$ est un ensemble algébrique affine.*
2. *Une intersection quelconque d'ensembles algébriques affines est un ensemble algébrique affine :*
$$\bigcap_i \mathcal{V}(S_i) = \mathcal{V}\left(\bigcup_i S_i\right).$$
3. *Une réunion finie d'ensembles algébriques affines est un ensemble algébrique affine.*

Conséquences

1. Tout ensemble fini est algébrique.
   En effet, il suffit d'appliquer 1) et 3) de la proposition précédente.
2. Tout sous-ensemble algébrique propre est une intersection d'hypersurfaces.

En effet, on a
$$\mathcal{V}(S) = \mathcal{V}(\bigcup_{P \in S} \{P\}) = \bigcap_{P \in S} \mathcal{V}(P).$$

Puisque $\mathcal{V}(S)$ est non vide, aucun des $P \in S \backslash \{0\}$ n'est constant et les $\mathcal{V}(P)$ sont donc bien des hypersurfaces.

Remarque 2.1.1. Un ensemble algébrique peut être défini par plusieurs idéaux.

Par exemple, les idéaux
$$I = \langle\ X^2 + Y^2, XY^3 \rangle \text{ et } J = \langle X^2, Y^3 \rangle$$
de $\mathbb{C}[X, Y]$ définissent tous deux $(0, 0)$ dans $\mathbb{A}^n(\mathbb{C})$.

Définition 2.1.4. Les ensembles algébriques de $\mathbb{A}^n$ définissent une topologie sur $\mathbb{A}^n$, dite topologie de Zariski, dont ils sont les fermés.

2.1.1 Idéal d'un ensemble de points

Définition 2.1.5. 1. Soient A un anneau et I un idéal de A. Le radical de I est l'ensemble noté $\sqrt{I}$ défini par

$$\sqrt{I} = \{x \in A | \exists m \in \mathbb{N}^\star, x^m \in I\}.$$

En fait $\sqrt{I}$ est aussi un idéal de A et I est contenu dans $\sqrt{I}$. On dit qu'un idéal I est radical s'il est égal à $\sqrt{I}$.

2. Soit A une partie de $\mathbb{A}^n$. On appelle idéal de A, l'ensemble noté $\mathfrak{I}(A)$ défini par

$$\mathfrak{I}(A) = \{P \in \mathbf{K}[X_1, \ldots, X_n] \mid \forall\, a \in A,\ P(a) = 0\}.$$

On voit clairement que $\mathfrak{I}(A)$ est l'ensemble des polynômes nuls sur A. Donc l'élément neutre de l'addition dans $\mathbf{K}[X_1, \ldots, X_n]$ appartient à $\mathfrak{I}(A)$. En fait $\mathfrak{I}(A)$ est un idéal radical de $\mathbf{K}[X_1, \ldots, X_n]$ car :

(a) si $F, G \in \mathfrak{I}(A)$ et $a \in A$, alors $(F+G)(a) = F(a) + G(a) = 0$;

(b) si $F \in \mathbf{K}[X_1, \ldots, X_n]$, $G \in \mathfrak{I}(A)$ et $a \in A$, alors $(FG)(a) = F(a)G(a) = 0$;

(c) si $F^r \in \mathfrak{I}(A)$, pour $r \in \mathbb{N}^*$ et $a \in A$, alors $F^r(a) = F(a)^r = 0$, donc $F(a) = 0$ et par conséquent, $F \in \mathfrak{I}(A)$.

Définition 2.1.6. Soient $V \subset \mathbb{A}^n$ un ensemble algébrique et $\mathfrak{I}(V)$ l'idéal de V. L'anneau des fonctions régulières sur V, noté $\mathbf{K}[V]$, est égal à l'anneau quotient $\mathbf{K}[X_1, \ldots, X_n]/\mathfrak{I}(V)$.

Proposition 2.1.2.

i) On a $\mathfrak{I}(\varnothing) = \mathbf{K}[X_1, \ldots, X_n]$ *et* $\mathfrak{I}(\mathbb{A}^n) = 0$.

ii) Si $\{A_i\}_{i \in I}$ *est un ensemble de parties de* $\mathbb{A}^n$, *alors* $\mathfrak{I}(\bigcup_i A_i) = \bigcap_i \mathfrak{I}(A_i)$.

iii) Si $A \subset B \subset \mathbb{A}^n$, *alors* $\mathfrak{I}(B) \subset \mathfrak{I}(A)$.

On a les propriétés suivantes :
— Pour toute partie $S \subset \mathbf{K}[X_1, \ldots, X_n]$, on a $S \subset \mathfrak{I}(\mathcal{V}(S))$; mais il n'y a en général pas égalité, même lorsque S est un idéal.
— Pour toute partie $A \subset \mathbb{A}^n$, on a $A \subset \mathcal{V}(\mathfrak{I}(A))$; avec égalité si et seulement si A est algébrique. En fait, $\mathcal{V}(\mathfrak{I}(A))$ est l'adhérence de A (pour la topologie de Zariski).

2.1.2 Irréductibilité

Définition 2.1.7. 1. On dit qu'un espace topologique E est irréductible s'il n'est pas vide et qu'il n'est pas réunion de deux fermés distincts de E.

2. Un ensemble algébrique non vide est dit irréductible s'il est irréductible pour la topologie de Zariski.

On montre facilement que si E est non vide, E est irréductible si et seulement si deux ouverts non vides quelconques se rencontrent, i.e si et seulement si tout ouvert non vide est dense.

Proposition 2.1.3. *Un ensemble algébrique V est irréductible si et seulement si son idéal $\mathfrak{I}(V)$ est premier.*

Autrement dit un ensemble algébrique V est irréductible si la $\mathbf{K}$-algèbre $\mathbf{K}[X_1, \ldots, X_n]/\mathfrak{I}(V)$ est intègre. Donc $\mathbb{A}^n$ est un espace topologique irréductible. En effet, un polynôme de $\mathbf{K}[X_1, \ldots, X_n]$ est nul sur $\mathbb{A}^n$ si et seulement s'il est identiquement nul, de sorte que $\mathfrak{I}(\mathbb{A}^n) = (0)$, qui est premier.

Définition et théoreme 2.1.1. *Tout ensemble algébrique non vide V se décompose de façon unique (à permutation près) en une réunion finie d'ensembles algébriques irréductibles $V_1, \ldots, V_p$, non contenus l'un dans l'autre. Les $V_1, \ldots, V_p$ sont appelés les composantes irréductibles de V.*

Si W est un fermé irréductible d'un ensemble algébrique V , alors W est contenu dans une composante irréductible de V. Il en résulte que les composantes irréductibles sont exactement les sous-ensembles fermés irréductibles maximaux de V.

Définition 2.1.8.

1. On appelle variété algébrique affine tout ensemble algébrique affine irréductible.
2. Une variété algébrique affine V sur $\mathbf{K}$ est dite absolument irréductible si elle est irréductible en tant qu'ensemble fermé par rapport à la topologie Zariski de l'espace affine $\mathbb{A}^n(\overline{\mathbf{K}})$.
3. Soient $V \subset \mathbb{A}^n$ un ensemble algébrique affine et $\mathfrak{I}(V)$ l'idéal de V.
   (a) Le corps des fonctions sur V, noté $\mathbf{K}(V)$, est égal au corps des fractions de son anneau de fonctions régulières :
   $$\mathbf{K}(V) = \mathrm{Frac}(\mathbf{K}[V]).$$
   (b) La dimension de V est égal au degré de transcendance de $\mathbf{K}(V)$ sur $\mathbf{K}$.

2.1.3 Le Nullstellensatz

Le Nullstellensatz, ou théorème des zéros de Hilbert, nous dit précisément la relation qui existe entre les idéaux et les ensembles algébriques. Nous allons commencer par la version faible avant d'énoncer le théorème lui-même. Nous allons montrer comment la réduire à un fait purement algébrique, et terminons par quelques conséquences. Nous supposons tout au long de cette section que $\mathbf{K}$ est algébriquement clos.

Pour tout idéal I de $\mathbf{K}[X_1, \ldots, X_n]$ on a : $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.
En particulier, $\sqrt{I} \subset \mathfrak{I}(\mathcal{V}(I))$;
en effet, $\sqrt{I} \subset \ \mathfrak{I}(\mathcal{V}(\sqrt{I})) = \mathfrak{I}(\mathcal{V}(I))$.

Théorème 2.1.1 (Nullstellensatz faible)**.** *Si I est un idéal propre de $\mathbf{K}[X_1, \ldots, X_n]$, alors $\mathcal{V}(I) \neq \varnothing$.*

Nous pouvons trouver une preuve de ce résultat dans [Ful69], p.20.

Théorème 2.1.2 (Nullstellensatz)**.** *Pour tout idéal I de $\mathbf{K}[X_1, \ldots, X_n]$, on a*

$$\mathfrak{I}(\mathcal{V}(I)) = \sqrt{I}.$$

Là encore, nous renvoyons à [Ful69], (p.21) ou [Per01] (p.18) pour la preuve.

Corollaire 2.1.1. *Si I est un idéal radical de $\mathbf{K}[X_1, \ldots, X_n]$, alors $\mathfrak{I}(\mathcal{V}(I)) = I$. Il y a donc une correspondance biunivoque entre idéaux radicaux et ensembles algébriques.*

Corollaire 2.1.2. *Si I est un idéal premier de $\mathbf{K}[X_1, \ldots, X_n]$, alors $\mathcal{V}(I)$ est une variété algébrique. Il y a une correspondance entre idéaux premiers de $\mathbf{K}[X_1, \ldots, X_n]$ et variétés algébriques affines. Les idéaux maximaux correspondent à des points.*

Corollaire 2.1.3. *Soit F un polynôme non constant dans $\mathbf{K}[X_1, \ldots, X_n]$, $F = F_1^{n_1} \cdots F_r^{n_r}$ la décomposition de F en facteurs irréductibles. Alors $\mathcal{V}(F) = \mathcal{V}(F_1) \cup \ldots \cup \mathcal{V}(F_r)$ est la décomposition de $\mathcal{V}(F)$ en composants irréductibles, et $\mathfrak{I}(\mathcal{V}(F)) = (F_1 \cdots F_r)$. Ainsi, il y a une correspondance entre les polynômes irréductibles $F \in \mathbf{K}[X_1, \ldots, X_n]$ (compté avec la multiplication par un élément non nul de $\mathbf{K}$) et des hypersurfaces irréductibles dans $\mathbb{A}^n(\mathbf{K})$.*

2.1.4 Applications régulières

Définition 2.1.9. Soient $V \subset \mathbf{K}^n$ et $W \subset \mathbf{K}^m$ des variétés affines. Une application $f : V \longrightarrow W$ est dite régulière si elle est la restriction à V d'une application $F : \mathbf{K}^n \longrightarrow \mathbf{K}^m$ dont les composantes sont des fonctions polynômiales.

Exemple 2.1.2. Supposons $\mathbf{K}$ infini.

1. Soit $\mathcal{C}$ l'hypersurface plane d'équation $Y = X^2$.
   L'application
   $$\begin{array}{rccc} f : & \mathcal{C} & \longrightarrow & \mathbf{K} \\ & (x, y) & \longmapsto & x \end{array}$$
   est régulière et bijective ; son inverse $x \longmapsto (x, x^2)$ est aussi régulière : on dit que f est un isomorphisme.
2. Soit $\mathcal{C}$ l'hypersurface plane d'équation $Y^3 = X^2$.
   L'application
   $$\begin{array}{rccc} u : & \mathbf{K} & \longrightarrow & \mathcal{C} \\ & t & \longmapsto & (t^3, t^2) \end{array}$$
   est régulière et bijective.
3. On suppose $\mathbf{K}$ algébriquement clos de caractéristique $p > 0$.
   L'application
   $$\begin{array}{rccc} f : & \mathbf{K} & \longrightarrow & \mathbf{K} \\ & x & \longmapsto & x^p \end{array}$$
   (dite " de Frobenius ") est régulière et bijective.

.

Définition 2.1.10. Une application régulière $u : V \longrightarrow W$ est dite dominante si son image est dense.

Remarque 2.1.2. Soient $V \subset \mathbf{K}^n$ et $W \subset \mathbf{K}^m$ des sous-variétés affines et $u : V \longrightarrow W$ une application régulière. L'ensemble des fonctions régulières de V dans $\mathbf{K}$ s'identifie à l'algèbre $\mathbf{K}[X_1, \ldots, X_n](V) = \mathbf{K}[X_1, \ldots, X_n]/\mathfrak{I}(V)$. On associe à u un morphisme de $\mathbf{K}$-algèbres $u^* : \mathbf{K}[X_1, \ldots, X_n](W) \longrightarrow \mathbf{K}[X_1, \ldots, X_n](V)$ par la règle $f \longmapsto f \circ u$.

$$\begin{array}{ccc} V & \xrightarrow{u} & W. \\ f \circ u \searrow & & \swarrow f \\ & \mathbf{K} & \end{array}$$

Proposition 2.1.4.

i) Une application régulière $u : V \longrightarrow W$ est dominante, si et seulement si, u^* est injectif.

ii) Si u^* est surjectif, alors u est injective.

2.2 Variétés projectives

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

2.2.1 L'espace projectif

Considérons la relation $\mathcal{R}$ sur $\mathbb{A}^{n+1}-\{0\}$ définie par : $x\mathcal{R}y$ si et seulement si ils sont colinéaires i.e

$$x\mathcal{R}y \;\Leftrightarrow\; \exists\lambda\in\mathbf{K}^* : y=\lambda x.$$

On montre que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{A}^{n+1}-\{0\}$.

Définition 2.2.1. On appelle espace projectif de dimension n sur $\mathbf{K}$, et l'on note $\mathbb{P}^n$ (ou $\mathbb{P}^n(\overline{\mathbf{K}})$), l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$.

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

Définition 2.2.2. Soit $\mathbf{L}/\mathbf{K}$ une extension contenu dans $\overline{\mathbf{K}}$. Son groupe de Galois $G_{\mathbf{L}}$ opère sur $\mathbb{P}^n(\overline{\mathbf{K}})$ via l'action sur les coordonnées. Cela préserve l'équivalence des classes pour la relation $\mathcal{R}$.

L'ensemble des points $\mathbf{L}$-rationnels $\mathbb{P}^n(\mathbf{L})$ est défini comme étant égal au sous-ensemble de $\mathbb{P}^n(\overline{\mathbf{K}})$ fixé par $G_{\mathbf{L}}$. En termes de coordonnées, cela signifie :

$$\mathbb{P}^n(\mathbf{L}) := \{\ [x_0:\ldots:x_n]\in\mathbb{P}^n \mid x_i\in\mathbf{L}\ , i=1,\ldots,n\}.$$

Soit $P\in\mathbb{P}^n(\overline{\mathbf{K}})$. La plus petite extension de corps $\mathbf{L}/\mathbf{K}$ tel que $P\in\mathbb{P}^n(\mathbf{L})$ est noté $\mathbf{K}(P)$ et appelé le corps de définition de P. On a

$$\mathbf{K}(P)=\bigcap_{G_{\mathbf{L}}\cdot P=P}\mathbf{L}.$$

Soit $S\subset\mathbb{P}^n(\overline{\mathbf{K}})$ et $\mathbf{L}$ un sous-corps de $\overline{\mathbf{K}}$ contenant $\mathbf{K}$. Alors S est dit défini sur $\mathbf{L}$ si et seulement si pour tout $P\in S$ le corps $\mathbf{K}(P)$ est contenu dans $\mathbf{L}$, ou de manière équivalente, $G_{\mathbf{L}}\cdot P=P$.

Si E est un $\mathbf{K}$-espace vectoriel non nul de dimension finie n, on définit de la même manière l'espace projectif associé à E noté $\mathbb{P}E$ (ou $\mathbb{P}(E)$) de dimension $n-1$.

Si F est un sous-espace vectoriel non nul de E, l'inclusion $F-\{0\}\subset E-\{0\}$ induit une inclusion $\mathbb{P}F\subset\mathbb{P}E$. Les sous-ensembles de $\mathbb{P}E$ ainsi obtenus sont appelés sous-ensembles linéaires de $\mathbb{P}E$; et on a $\mathbb{P}F_1\cap\mathbb{P}F_2=\mathbb{P}(F_1\cap F_2)$. Pour chaque $i=0,1,\ldots,n$, on définit un sous-ensemble U_i de $\mathbb{P}^n$ par :

$$U_i=\{\ P=[x_0:\ldots:x_n]\ \in\mathbb{P}^n \mid x_i\neq 0\}$$

Chacun des U_i est isomorphe à $\mathbb{A}^n$.

$$U_i\approx\mathbb{A}^n,\quad [x_0:\ldots:x_n]\ \longrightarrow\ (\frac{x_0}{x_i},\ldots,\frac{x_n}{x_i})$$

Les U_i recouvrent $\mathbb{P}^n$. Le complémentaire de U_i est le sous-espace linéaire $\mathbb{P}H_i$ où H_i est l'hyperplan d'équation $X_i=0$ dans $\mathbb{A}^{n+1}$. On peut donc voir $\mathbb{P}^n$ comme obtenu à partir de $\mathbb{A}^n$ en adjoignant un "hyperplan à l'infini". Par exemple, la droite projective $\mathbb{P}^1$ est obtenue en adjoignant à $\mathbb{A}^1$ un unique "point à l'infini". Plus généralement, le complémentaire dans $\mathbb{P}^n$ de n'importe quel hyperplan projectif s'identifie naturellement à $\mathbb{A}^n$.

Définition 2.2.3. On dit que des points de $\mathbb{P}^n$ sont linéairement indépendants si les droites de $\mathbf{K}^{n+1}$ qu'ils représentent sont en somme directe.
On dit que des points de $\mathbb{P}^n$ sont en position générale , si pour tout $m\leq n+1$, m quelconques d'entre-eux sont linéairement indépendants.

La proposition suivante, illustre une des propriétés fondamentales de l'espace projectif : il n'y a pas de sous-espaces parallèles, ils se rencontrent à «l'infini».

Proposition 2.2.1. *Soient $\mathbb{P}(F)$ et $\mathbb{P}(F')$ deux sous-espaces linéaires de $\mathbb{P}^n$ de dimension respective r et r' vérifiant $r + r' \geq n$. Alors l'intersection $\mathbb{P}(F) \cap \mathbb{P}(F') = \mathbb{P}(F \cap F')$ est un sous-espace linéaire de dimension supérieure ou égale à $r + r' - n$; il est en particulier non vide.*

2.2.2 Variétés projectives

Définition 2.2.4. Un polynôme F de $R := \mathbf{K}[X_0, \ldots, X_n]$ est dit homogène de degré d si, pour tout $\lambda \in \mathbf{K}$, on a $F(\lambda X_0, \ldots, \lambda X_n) = \lambda^d F(X_0, \ldots, X_n)$.

Une conséquence immédiate est que, si F est homogène, on a pour tout $\lambda \neq 0$, $F(x_0, \ldots, x_n) = 0$ si et seulement si $F(\lambda x_0, \ldots, \lambda x_n) = 0$.

Proposition 2.2.2. *Tout polynôme se décompose de façon unique en somme de polynômes homogènes (autrement dit, $\mathbf{K}[X_0, \ldots, X_n]$ est un anneau gradué).*

Définition 2.2.5. Soit S une partie de $\mathbf{K}[X_0, \ldots, X_n]$ formée de polynômes homogènes. On pose :

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

de sorte que les $P \in \mathcal{V}(S)$ sont les zéros communs à tous les polynômes de S. On dit que $\mathcal{V}(S)$ est l'ensemble algébrique projectif défini par S. Dans le cas d'un ensemble fini, on notera souvent $\mathcal{V}(F_1, \ldots, F_r)$ au lieu de $\mathcal{V}(\{F_1, \ldots, F_r\})$.

Définition 2.2.6.

1. On appelle hypersurface définie par un polynôme homogène F en $n + 1$ variables, et on note $\mathcal{V}(F)$, l'ensemble des zéros de F. Le degré de $\mathcal{V}(F)$ est le degré de F.
2. Une courbe projective plane est une hypersurface du plan projectif. Une courbe projective plane est dite conique (ou quadrique), cubique, quartique, quintique, sextique,... si le degré est respectivement 2, 3, 4, 5, 6,...
3. Un hyperplan est une hypersurface définie par un polynôme homogène de degré 1.
4. On dit qu'un idéal I de R est homogène s'il est engendré par des polynômes homogènes. On note $\mathcal{V}(I)$ le sous-ensemble de $\mathbb{P}^n$ formé des zéros communs à tous les éléments homogènes de I. Pour qu'un idéal I de R soit homogène, il faut et il suffit que pour toute décomposition $F = \sum F_i$ d'un élément F de I en somme de polynômes homogènes, on ait $F_i \in I$ pour tout i.

Remarque 2.2.1. *On retrouve beaucoup de résultats obtenus dans le cas de l'espace affine (mais pas tous !) :*

1. *L'application $S \longrightarrow \mathcal{V}(S)$ est décroissante pour l'inclusion.*
2. *Si S est formé de polynômes homogènes, l'idéal $\langle S \rangle$ engendré par S est homogène, et l'on a $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$.*
3. *L'anneau $R := \mathbf{K}[X_0, \ldots, X_n]$ étant noethérien, on vérifie que l'idéal $\langle S \rangle$ est engendré par un nombre fini de polynômes homogènes $F_1, \ldots, F_r$, de sorte que $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle) = \mathcal{V}(F_1, \ldots, F_r)$. En d'autres termes, tout ensemble algébrique projectif peut être défini par un nombre fini d'équations.*
4. *Une intersection quelconque d'ensembles algébriques projectifs est un ensemble algébrique projectif :*
$$\bigcap_i \mathcal{V}(S_i) = \mathcal{V}(\bigcup_i S_i).$$
5. *Une réunion finie d'ensembles algébriques projectifs est un ensemble algébrique projectif.*

6. *La topologie de Zariski sur $\mathbb{P}^n$ est celle dont les fermés sont les ensembles algébriques projectifs.*

Définition 2.2.7. Soit A une partie de $\mathbb{P}^n$. On appelle idéal de A dans $\mathbb{P}^n$, l'ensemble noté $\mathfrak{I}(A)$ défini par

$$\mathfrak{I}(A) = \{\text{Polynômes homogènes } F \in \mathbf{K}[X_0, \ldots, X_n] \mid \forall P \in A,\ F(P) = 0\}.$$

On voit clairement que $\mathfrak{I}(A)$ est l'ensemble des polynômes homogènes nuls sur A. On a $\mathcal{V}(\mathfrak{I}(A))$ est l'adhérence de A (pour la topologie de Zariski). Les résultats sur la décomposition d'un ensemble algébrique affine en composantes irréductibles se transportent tels quels au cadre projectif.

Définition 2.2.8.

1. Un ensemble algébrique projectif $\mathcal{V}$ est dit irréductible s'il est irréductible pour la topologie de Zariski. Comme en affine, $\mathcal{V}$ est irréductible si, et seulement si $\mathfrak{I}(\mathcal{V})$ est premier. Un tel $\mathcal{V}$ est appelé variété projective.
2. Un ensemble projectif $\mathcal{V}$ est appelé variété projective si l'idéal homogène $\mathfrak{I}(\mathcal{V})$ est premier dans $\mathbf{K}[X_0, \ldots, X_n]$. Une variété quasi-projective est un sous-ensemble ouvert (de Zariski) d'une variété projective.

Une variété algébrique projective $\mathcal{V}$ sur $\mathbf{K}$ est dite absolument irréductible si elle est irréductible en tant qu'ensemble fermé par rapport à la topologie Zariski de l'espace projectif $\mathbb{P}^n(\overline{\mathbf{K}})$. On a aussi le Nullstellensatz projectif.

Théorème 2.2.1 (Nullstellensatz)**.** *On suppose* $\mathbf{K}$ *algébriquement clos. Soit* I *un idéal homogène de* $\mathbf{K}[X_0, \ldots, X_n]$. *Si* $\mathcal{V}(I)$ *n'est pas vide, on a* $\mathfrak{I}(\mathcal{V}(I)) = \sqrt{I}$.

2.2.3 Applications régulières

Dans cette partie, $\mathbf{K}$ désigne un corps algébriquement clos.

Définition 2.2.9. On appelle variété quasi-projective, tout ouvert (de Zariski) d'une variété projective.

Pour étudier des applications régulières définies sur une variété projective, le constat de base est qu'un polynôme, même homogène, ne définit pas de fonction sur $\mathbb{P}^n$. Mais le quotient F/G de polynômes homogènes de même degré définit une fonction sur l'ouvert où G ne s'annule pas.

Définition 2.2.10. Soient X une sous-variété quasi-projective de $\mathbb{P}^n$ et $x \in X$. Une fonction $f : X \longrightarrow \mathbf{K}$ est dite régulière en x, s'il existe des polynômes homogènes F et G de même degré avec $G(x) \neq 0$ et $f = F/G$ dans un voisinage de x dans X. On dit que f est régulière sur X, si elle est régulière en tout point de X.

Définition 2.2.11. Soient X et Y des variétés quasi-projectives. On dit qu'une application $u : X \longrightarrow Y$ est régulière si elle est continue et si, pour tout ouvert U de Y et toute fonction régulière $f : U \longrightarrow \mathbf{K}$, la composée $f \circ u$ est régulière sur $u^{-1}(U)$.

$$\begin{array}{ccc} u^{-1}(U) \subset X & \xrightarrow{u} & Y \supset U \\ & f \circ u \searrow \quad \swarrow f & \\ & \mathbf{K} & \end{array}$$

Exemple 2.2.1. L'application $u : \mathbb{P}^1 \longrightarrow \mathbb{P}^3$ définie par $u(x_0, x_1) = (x_0^3\ ,\ x_0^2x_1,\ x_0x_1^2,\ x_1^3)$ est régulière. Plus généralement, si on se donne des polynômes homogènes $F_0, \ldots, F_m$ de même degré en $n+1$ variables, l'égalité $u(x) = (F_0(x), \ldots, F_m(x))$ définit une application régulière

$$u : \mathbb{P}^n - \mathcal{V}(F_0, \ldots, F_m) \longrightarrow \mathbb{P}^m.$$

En particulier, si $F_0, \ldots, F_m$ ne s'annulent simultanément qu'en $(0, \ldots, 0)$, l'application u est définie sur tout $\mathbb{P}^n$. C'est sous cette forme plus concrète que l'on rencontre le plus souvent les applications régulières.

Exemple 2.2.2 (Applications de Véronese)**.** *Soient $M_0, \ldots, M_N$ tous les monômes de degré d en $X_0, \ldots, X_n$. Ils forment un espace vectoriel de dimension C_{n+d}^d, donc $N = C_{n+d}^d - 1$. On obtient une application régulière injective*

$$u_d : \mathbb{P}^n \longrightarrow \mathbb{P}^N$$

$$[x_0 : \ldots : x_n] \longmapsto [M_0(x_0, \ldots, x_n) : \ldots : M_N(x_0, \ldots, x_n)].$$

La proposition suivante montre qu'une application régulière est toujours définie localement comme dans l'exemple 2.2.1.

Proposition 2.2.3. *Soient X une sous-variété quasi-projective de $\mathbb{P}^n$ et $u : X \longrightarrow \mathbb{P}^m$ une application régulière. Pour tout point $x_0 \in X$, il existe un voisinage ouvert U de x_0 dans X et des polynômes homogènes $F_0, \ldots, F_m$ de même degré en $n+1$ variables qui ne s'annulent simultanément en aucun point de U, tels que pour tout $x \in U$, on ait*

$$u(x) = (F_0(x), \ldots, F_m(x)) \tag{2.1}$$

en coordonnées homogènes.

On peut trouver la preuve dans [Per01] ou [Ful69].

2.3 Points et courbes lisses

Cette section concerne les ensembles algébriques affines et projectifs. Nous omettrons donc les adjectifs affines et projectifs dans les différents énoncés pour signifier que les résultats annoncés sont vrais pour les deux familles.

2.3.1 Dimension d'une variété algébrique projective

L'approche de la géométrie différentielle, basée sur des "cartes", ne convient pas ici : en général, une variété algébrique ne contient pas d'ouvert non vide isomorphe à un ouvert d'un espace affine.

Définition 2.3.1. Soit X un espace topologique. La dimension de X est le maximum des entiers n pour lesquels il existe des parties irréductibles fermées $X_0, \ldots, X_n$ de X vérifiant $X_0 \subsetneq \ldots \subsetneq X_n$. La dimension de X est donc un entier positif, ou bien $+\infty$, ou même $-\infty$ dans le cas où X est l'ensemble vide.

Si X est une réunion de fermés $X_1, \ldots, X_l$, on a $\dim X = \max_{1 \leq i \leq l}(\dim X_i)$. On voit donc que la dimension d'un ensemble algébrique est le maximum des dimensions de ses composantes irréductibles.

Proposition 2.3.1. *Un ensemble algébrique est de dimension 0 si et seulement si il consiste en un nombre fini de points.*

Démonstration. Soit X un ensemble algébrique de dimension 0. Tout fermé irréductible contenant un point est réduit à ce point, donc les composantes irréductibles de X sont des points. La condition suffisante est évidente. □

Définition 2.3.2. On dit qu'un ensemble algébrique est de dimension pure n, ou équidimensionnelle de dimension n, si chaque composante irréductible est de dimension n.
Si x est un point de X, on appelle dimension de X en x, et l'on note $\dim_x X$, le maximum des dimensions des composantes irréductibles de X passant par x.

On admet le résultat suivant :

Proposition 2.3.2. *Tout ensemble algébrique X est de dimension finie, et tout ouvert dense dans X est de même dimension que X.*

Exemple 2.3.1. 1. $\dim \mathbb{A}^n = n$; $\dim \mathbb{P}^n = n$.

2. Le produit $\mathbb{P}^m \times \mathbb{P}^n$ contient un ouvert dense isomorphe à $\mathbb{A}^m \times \mathbb{A}^n$, donc à $\mathbb{A}^{m+n}$; il est alors de dimension $m + n$.

2.3.2 Critère de Jacobi

Commençons par une approche de géométrie différentielle. Considérons une courbe $\mathcal{C}$ dans $\mathbb{R}^2$ d'équation affine $F(x, y) = 0$ et $M = (x_0, y_0)$ un point de $\mathcal{C}$. Supposons $\dfrac{\partial F}{\partial y}(x_0, y_0) \neq 0$. Alors on peut paramétrer localement la courbe $\mathcal{C}$ par une fonction g qui vérifie $g(x_0) = y_0$ et $F(t, g(t)) = 0$ pour tout t. La tangente à $\mathcal{C}$ en M est la droite d'équation affine :

$$y - y_0 = g'(x_0)(x - x_0).$$

Soit encore

$$(x - x_0)\frac{\partial F}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial F}{\partial y}(x_0, y_0) = 0.$$

Cette équation définit toujours une droite sauf si $\dfrac{\partial F}{\partial x}(x_0, y_0) = \dfrac{\partial F}{\partial y}(x_0, y_0) = 0.$

Définition 2.3.3. Soit H une hypersurface de $\mathbb{R}^n$ d'équation $F(x_1, \ldots, x_n) = 0$. L'espace défini par l'équation

$$(x_1 - p_1)\frac{\partial F}{\partial x_1}(P) + \ldots + (x_n - p_n)\frac{\partial F}{\partial x_n}(P) = 0$$

est appelé espace tangent affine en $P = (p_1, \ldots, p_n)$. C'est un hyperplan sauf si toutes les dérivées partielles de F en P sont nulles.

Définition 2.3.4 (Critère de Jacobi)**.**

1. Soient V une sous-variété algébrique affine de $\mathbb{A}^n$, $P = (x_1, \ldots, x_n)$ un point de V et $F_1, \ldots, F_r$ des générateurs de l'idéal $\mathfrak{I}(V)$ de V. On dit que V est non-singulière ou bien lisse en P (on dit aussi que P est un point lisse) si la matrice

$$\left(\frac{\partial F_i}{\partial X_j}(P))\right)_{1 \leq i \leq r,\ 1 \leq j \leq n}$$

est de rang $n - dim(V)$.

2. Un point qui n'est pas lisse est dit point singulier. Un point lisse est aussi appelé point régulier.
3. On dit que V est non-singulière (ou lisse) si elle l'est en chacun de ses points.

L'ensemble des points singuliers de X est un fermé propre de X, appelé lieu singulier de X et noté Sing$X$. L'ouvert complémentaire de Sing$X$ est noté X_{lisse}. Lorsque X est un ensemble algébrique réductible, tout point situé sur au moins deux composantes est singulier.

Exemple 2.3.2.

1. Les points singuliers d'une hypersurface dans $\mathbb{A}^n$ d'idéal engendré par un polynôme F sont définis par les équations
$$F(x) = \frac{\partial F}{\partial x_1}(x) = \cdots = \frac{\partial F}{\partial x_n}(x) = 0.$$
On voit bien dans ce cas que si $F = F_1 \cdots F_s$, les points situés à l'intersection de $\mathcal{V}(F_i)$ et $\mathcal{V}(F_j)$ sont singuliers.
2. Les points singuliers d'une hypersurface X dans $\mathbb{P}^n$ d'idéal engendré par un polynôme homogène F de degré d sont définis par les équations
$$F(x) = \frac{\partial F}{\partial x_0}(x) = \ \cdots \ = \frac{\partial F}{\partial x_n}(x) = 0.$$
Il faut noter que si la caractéristique de $\mathbf{K}$ ne divise pas d, les points singuliers sont définis par les $n+1$ équations
$$\frac{\partial F}{\partial x_0}(x) = \ \cdots \ = \frac{\partial F}{\partial x_n}(x) = 0.$$

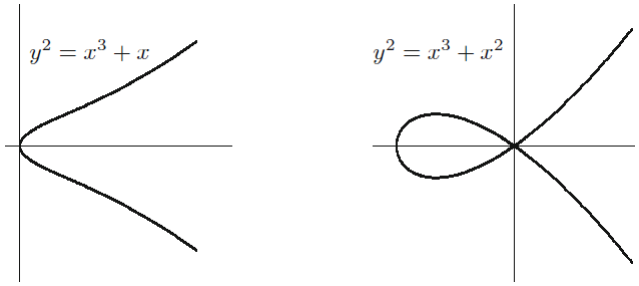

FIGURE 2.1 – Une courbe régulière et une courbe singulière (cf. [Sil86] p.5).

2.3.3 Homogénéisation et déshomogénéisation

A tout fermé $\mathcal{V}$ de $\mathbb{P}^n$, on peut associer l'idéal homogène que l'on note $\mathfrak{I}(\mathcal{V})$ engendré par des polynômes homogènes $F_1, \ldots, F_p$ s'annulant en tous les points de $\mathcal{V}$.

Définition 2.3.5. On dit que $\mathcal{V}$ est défini sur $\mathbf{K}$, et on note $\mathcal{V}/\mathbf{K}$, si on peut choisir les F_i comme polynômes homogènes à coefficients dans $\mathbf{K}$. Si $\mathcal{V}$ est défini sur $\mathbf{K}$, l'ensemble des points $\mathbf{K}$-rationnels de $\mathcal{V}$ est
$$\mathcal{V}(\mathbf{K}) = \mathcal{V} \cap \mathbb{P}^n(\mathbf{K}).$$

Cas particulier. Soit $\mathcal{C} = \mathcal{V}(F)$ une courbe projective plane. On dit que $\mathcal{C}$ est définie sur $\mathbf{K}$, et l'on note $\mathcal{C}/\mathbf{K}$, si F est à coefficients dans $\mathbf{K}$.
L'ensemble des points $\mathbf{K}$-rationnels de $\mathcal{C}$ est
$$\mathcal{C}(\mathbf{K}) = \mathcal{C} \cap \mathbb{P}^n(\mathbf{K}).$$
Soient U_2 et L_∞ les ensembles définis par
$$U_2 = \left\{ [X : Y : Z] \in \mathbb{P}^2 \mid Z \neq 0 \right\},$$

$$L_\infty = \left\{ [X : Y : Z] \in \mathbb{P}^2 \mid Z = 0 \right\}.$$

On introduit les coordonnées x, y telles que

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

L'application définie par

$$\begin{array}{rccc} \phi_2 : & \mathbb{A}^2 & \longrightarrow & U_2 \\ & (x, y) & \longmapsto & [x : y : 1] \end{array}$$

est un homéomorphisme ($i.e$ bijection bicontinue) sa réciproque est

$$\begin{array}{rccc} \phi_2^{-1} : & U_2 & \longrightarrow & \mathbb{A}^2. \\ & [X : Y : Z] & \longmapsto & \left(\dfrac{X}{Z}, \dfrac{Y}{Z} \right) \end{array}$$

On voit clairement que $\mathbb{P}^2$ est la réunion disjointe

$$\mathbb{P}^2 = U_2 \cup L_\infty$$

du "plan affine" U_2 et de la " droite à l'infini " L_∞.

Un point de L_∞ est appelé point à l'infini que l'on notera P_∞. Le plan projectif $\mathbb{P}^2$ peut donc être identifié au plan affine auquel on adjoint une droite à l'infini.

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

$$U_0 = \{[X : Y : Z] \in \mathbb{P}^2 \mid X \neq 0\} \quad \text{et} \quad U_1 = \{[X : Y : Z] \in \mathbb{P}^2 \mid Y \neq 0\},$$

et des bijections

$$\begin{array}{rccc} \phi_0^{-1} : & U_0 & \longrightarrow & \mathbb{A}^2 \\ & [X : Y : Z] & \longmapsto & \left(\dfrac{Y}{X}, \dfrac{Z}{X} \right) \end{array}$$

et

$$\begin{array}{rccc} \phi_1^{-1} : & U_1 & \longrightarrow & \mathbb{A}^2. \\ & [X : Y : Z] & \longmapsto & \left(\dfrac{X}{Y}, \dfrac{Z}{Y} \right) \end{array}$$

Les applications ϕ_i^{-1} permettent d'identifier le plan affine $\mathbb{A}^2$ avec un ouvert U_i de $\mathbb{P}^2$. Il faut noter que la réunion des U_i recouvre $\mathbb{P}^2$:

$$\mathbb{P}^2 = U_0 \cup U_1 \cup U_2.$$

Une courbe projective plane $\mathcal{C}$ est la réunion de trois courbes affines planes :

$$\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2,$$

avec $\mathcal{C}_i = \mathcal{C} \cap U_i$. Lorsque nous identifions U_i avec $\mathbb{A}^2$, alors $\mathcal{C}_0$, $\mathcal{C}_1$ et $\mathcal{C}_2$ s'identifient avec les courbes affines définies respectivement par les polynômes

$$F_*(Y, Z) = F(1, Y, Z)\,; \quad F_*(X, Z) = F(X, 1, Z) \quad \text{et} \quad F_*(X, Y) = F(X, Y, 1).$$

Le fait de remplacer $F(X, Y, Z)$ par $F(1, Y, Z)$, $F(X, 1, Z)$ ou $F(X, Y, 1)$ est appelé déshomogénéisation suivant respectivement X, Y, et Z. Inversement, à tout polynôme non nul $F(X, Y) \in \mathbf{K}[X, Y]$ on associe le polynôme homogène F^* tel que :

$$F^*(X,Y,Z) = Z^d F\left(\frac{X}{Z}, \frac{Y}{Z}\right), \text{ où } d = \deg(F).$$

Le polynôme F^* est appelé l'homogénéisé de F par rapport à Z.

Remarque 2.3.1. Soit $\mathcal{C} = \mathcal{V}(F)$ une courbe projective plane. Les situations suivantes sont équivalentes :

1. $\mathcal{C}$ est irréductible.
2. $\mathcal{C}$ est une variété projective.
3. F est irréductible.

Définition 2.3.6. Soit $\mathcal{C} = \mathcal{V}(F)$ une courbe affine plane avec $d = \deg F \geq 1$.
La clôture projective de $\mathcal{C}$, que l'on note $\overline{\mathcal{C}}$, est la courbe plane projective $\overline{\mathcal{C}} = \mathcal{V}(H)$ où H est l'homogénéisé de F.

Les points $(\overline{\mathcal{C}} - \mathcal{C})$ sont les points à l'infini de $\mathcal{C}$.

2.4 Cas des variétés algébriques sur des corps finis

Dans cette section, nous traiterons des variétés définies sur un corps fini $\mathbb{F}_q$, avec $q = p^d$, i.e. une extension de degré d du corps $\mathbb{F}_p$, avec p un nombre premier et $d \geq 1$.

2.4.1 Homomorphisme de Frobenius

Pour $k \geq 1$, nous nous intéressons au k-ième itéré ϕ_p^k du $\mathbb{F}_p$-automorphisme absolu de Frobenius $\phi_p : a \longrightarrow a^p$, qui fixe les éléments de $\mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_p$. L'application ϕ_p^k est donc un $\mathbb{F}_{p^k}$-automorphisme de $\overline{\mathbb{F}}_p$. Il induit un endomorphisme de l'espace projectif $\mathbb{P}^n(\overline{\mathbb{F}}_p)$ qui à tout point $[x_0 : \ldots : x_n]$ fait correspondre $[x_0^p : \ldots : x_n^p]$. Par ailleurs ϕ_p opère sur $\overline{\mathbb{F}}_p[X_0, \ldots, X_n]$ en agissant sur les coefficients. Plus généralement, si $\mathcal{V}$ est une variété projective définie sur $\mathbf{K}$ de caractéristique p, d'idéal $\mathfrak{I}(\mathcal{V})$, alors nous pouvons appliquer ϕ_p à $\mathfrak{I}(\mathcal{V})$ et obtenir une variété $\phi_p(\mathcal{V})$ définie sur $\phi_p(\mathbf{K})$ ayant $\phi_p(\mathfrak{I}(\mathcal{V}))$ pour idéal. Les points de $\mathcal{V}$ sont envoyés vers des points sur $\phi_p(\mathcal{V})$. L'application de $\mathcal{V} \to \phi_p(\mathcal{V})$ qui à $[x_0 : \ldots : x_n]$ fait correspondre $[x_0^p : \ldots : x_n^p]$ est appelée morphisme de Frobenius et est à nouveau notée ϕ_p. De même pour tout $k \in \mathbb{N}^*$, le k-ième itéré de l'automorphisme de Frobenius ϕ_{p^k} induit un endomorphisme de $\mathcal{V}$ vers $\phi_{p^k}(\mathcal{V})$ qui à $[x_0 : \ldots : x_n]$ fait correspondre $[x_0^{p^k} : \ldots : x_n^{p^k}]$ que nous notons encore ϕ_{p^k}.

Chapitre 3

Résultats fondamentaux concernant les courbes algébriques

Ce chapitre théorique nous présente la notion de diviseur d'une courbe, survole rapidement la construction de la Jacobienne d'une courbe, et nous présente un résultat important de la géométrie algébrique : le théorème de Riemann-Roch. On boucle le chapitre avec une petite discussion sur les courbes elliptiques. Nous nous sommes inspirés des ouvrages [Ful69], et [Sil86].

Tout au long de ce chapitre, $\mathbf{K}$ désigne un corps parfait (cf. chapitre 1) et $\overline{\mathbf{K}}$ une clôture algébrique fixée de $\mathbf{K}$, $\mathbf{L}$ désigne une extension de $\mathbf{K}$ contenue dans $\overline{\mathbf{K}}$. On note $\mathrm{Aut}_{\mathbf{L}}\left(\overline{\mathbf{K}}\right)$ (ou bien $G_{\mathbf{L}}$) son groupe de Galois absolu. Sauf mention contraire toutes les courbes seront supposées lisses.

3.1 Diviseurs

3.1.1 Diviseurs sur une courbe

Soit $\mathcal{C}$ une courbe projective lisse définie sur un corps $\mathbf{K}$ algébriquement clos.

Définition 3.1.1. Un diviseur D sur $\mathcal{C}$ est une somme formelle de points appartenant à $\mathcal{C}$:

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

où les n_P sont des entiers nuls sauf un nombre fini d'entre eux.
L'ensemble des diviseurs sur $\mathcal{C}$ est un groupe commutatif noté $\mathrm{Div}(\mathcal{C})$, où la loi de groupe est l'addition formelle de points : si $D = \sum_{P \in \mathcal{C}} n_P P$ et $D' = \sum_{P \in \mathcal{C}} n'_P P$ sont deux diviseurs sur $\mathcal{C}$, alors

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

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

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

Le support de $\sum_{P \in \mathcal{C}} n_P P$ est l'ensemble des points $P \in \mathcal{C}$ tels que $n_P \neq 0$.

Le degré est un homomorphisme de groupes de $\mathrm{Div}(\mathcal{C})$ dans $\mathbb{Z}$; le noyau de cet homomorphisme est l'ensemble des diviseurs de degré 0, noté $\mathrm{Div}^0(\mathcal{C})$, c'est un sous-groupe de $\mathrm{Div}(\mathcal{C})$.

Définition 3.1.2. On dit qu'un diviseur $D = \sum_{P \in \mathcal{C}} n_P P$ est effectif et on note $D \geq 0$, si $n_P \geq 0$ pour tout $P \in \mathcal{C}$.

Plus généralement, on définit la relation d'ordre partiel " $\geq$ " sur les diviseurs par :
$D_1 \geq D_2$ si et seulement si $D_1 - D_2 \geq 0$.

3.1.2 Diviseurs principaux

Soit $\mathcal{C}$ une courbe projective lisse définie sur un corps $\mathbf{K}$ algébriquement clos. Alors $\mathcal{C}$ est nécessairement irréductible. On note $\mathbf{K}[\mathcal{C}]$ l'anneau des fonctions régulières sur $\mathcal{C}$ et $\mathbf{K}(\mathcal{C})$ son corps des fonctions.

Théorème 3.1.1. *Deux courbes sont isomorphes si et seulement si elles ont deux corps de fonctions isomorphes.*

On trouve une démonstration de ce théorème dans [Ful69], p.180. Il indique qu'il est complètement équivalent de travailler avec une vision géométrique des choses : courbes, points, etc... ou de travailler algébriquement, *i.e* avec les corps de fonctions. Nous préférons la première approche, plus proche de l'intuition (on peut faire des dessins).

Quelle que soit l'approche choisie, les diviseurs principaux sont intrinsèquement liés au corps de fonctions de $\mathcal{C}$. Pour les définir, il est nécessaire de faire une étude locale de la courbe. Le but est de donner une définition algébrique du fait qu'une fonction s'annule ou a un pôle en un point, éventuellement avec multiplicité.

Soient f une fonction sur $\mathcal{C}$ et P un point de $\mathcal{C}$. On dit que f est régulière (ou est définie) au point P s'il existe $g, h \in \mathbf{K}[\mathcal{C}]$ avec $h(P) \neq 0$ telle que $f = \frac{g}{h}$. L'ensemble des fonctions régulières en P est noté $\mathcal{O}_P(\mathcal{C})$ et appelé l'anneau local de $\mathcal{C}$ en P. L'ensemble des points de $\mathcal{C}$ où la fonction rationnelle f n'est pas définie est appelé l'ensemble des pôles de f sur $\mathcal{C}$. Si f est régulière et s'annule en $P = (a, b)$, on dit que P est un zéro de f. On note $\mathcal{M}_P$ l'ensemble des fonctions sur $\mathcal{C}$ qui s'annule en P :

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

L'ensemble $\mathcal{M}_P$ est l'unique idéal maximal de $\mathcal{O}_P$ et il est de la forme $\langle x-a, y-b\rangle$. Le corps $\mathcal{O}_P(\mathcal{C})\ /\mathcal{M}_P(\mathcal{C})$ est appelé corps résiduel de $\mathcal{C}$ en P. Les éléments inversibles de $\mathcal{O}_P(\mathcal{C})$ sont ceux qui n'appartiennent pas à $\mathcal{M}_P(\mathcal{C})$, on les appelle les unités de $\mathcal{O}_P(\mathcal{C})$ et ils forment un groupe multiplicatif. En fait $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète, *i.e* il existe $t \in \mathcal{M}_P(\mathcal{C})$ une fonction non nulle telle que tout élément non nul $f \in \mathcal{O}_P(\mathcal{C})$ s'écrit de manière unique $f = u.t^n$, où u est une unité de $\mathcal{O}_P(\mathcal{C})$ et n un entier naturel appelé la valuation (ou l'ordre) de f en P et noté $ord_P(f)$. Cet entier ne dépend pas du choix de t. La fonction t est appelée uniformisante de $\mathcal{O}_P(\mathcal{C})$. On a les propriétés suivantes :

(i) L'application $\mathrm{ord}_P : \mathcal{O}_P(\mathcal{C}) \to \mathbb{Z} \cup \{\infty\}$ définie par

$$\mathrm{ord}_P(u.t^n) = n,\ \ \mathrm{ord}_P(t) = 1,\ \ \mathrm{ord}_P(u) = 0 \text{ et } \mathrm{ord}_P(0) = \infty,$$

est un morphisme de groupes surjectif, où $\infty + k = \infty$ pour tout $k \in \mathbb{Z}$.

(ii) $\mathrm{ord}_P(f) = \infty$ si et seulement si $f = 0$.

(iii) $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$.

(iv) $\mathrm{ord}_P\left(\frac{f}{g}\right) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.

(v) $\mathrm{ord}_P(f + g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$.

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

$$\mathcal{O}_P(\mathcal{C}) = \{f \in \mathbf{K}(\mathcal{C})\ ;\ \mathrm{ord}_P(f) \geq 0\ \},$$

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

Remarque 3.1.1. Soient $\mathcal{C}$ une courbe plane irréductible et lisse en P, et f une fonction non nulle de $\mathbf{K}(\mathcal{C})$.

— Si f est régulière en P et $f(P) \neq 0$, alors $\text{ord}_P(f) = 0$.
— Si f est régulière en P et $f(P) = 0$, alors $\text{ord}_P(f) > 0$.
— Si P est un pôle de f, alors $\text{ord}_P(f) = -\text{ord}_P\left(\frac{1}{f}\right)$.

Intuitivement, la valuation d'une fonction en un point mesure la multiplicité du zéro de la fonction. Géométriquement, cela correspond à la tangente entre la courbe $\mathcal{C}$ et la courbe $f = 0$.

Exemple 3.1.1. Considérons $\mathcal{C}$ la courbe affine plane irréductible et lisse définie sur $\mathbb{Q}$ d'équation affine

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

Soit $P_i = (i, 0)$ où $i \in \{0, 1, 2, 3\}$. On sait que $\mathcal{M}_{P_i}(\mathcal{C})$ est engendré par $< x - i, y >$, et les éléments $x - j$ sont inversibles dans l'anneau local $\mathcal{O}_{P_i}(\mathcal{C})$, avec $j \in \{0, 1, 2, 3\}$ et $j \neq i$, d'où $(x - i) = uy^3$. Donc y est une uniformisante de $\mathcal{O}_{P_i}(\mathcal{C})$, $\text{ord}_{P_i}(y) = 1$ et $\text{ord}_{P_i}(x - i) = 3$.

Ainsi, à chaque point P d'une courbe lisse $\mathcal{C}$, on peut associer une valuation ord_P qui à toute fonction f bien définie en P fait correspondre son ordre en P. Cette valuation peut être étendue aux fonctions qui ont un pôle au point considéré (d'après la remarque précédente).

Théorème 3.1.2. *Soit f une fonction non nulle de $\mathbf{K}(\mathcal{C})$. Alors les points P pour lesquels $\text{ord}_P(f)$ est non nul sont en nombre fini. De plus, le diviseur*

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

est de degré 0.

Nous renvoyons à [Ful69], (p.188) pour une preuve.
Ce dernier résultat peut-être reformulé en « une fonction rationnelle a autant de zéros que de pôles ».

Définition 3.1.3. Un diviseur principal de $\mathcal{C}$ est un diviseur D tel qu'il existe une fonction rationnelle $f \in \mathbf{K}(\mathcal{C})$ pour laquelle

$$D = \text{div}(f).$$

Proposition 3.1.1. *L'application* div *est un homomorphisme du groupe multiplicatif des fonctions non nulles de $\mathbf{K}(\mathcal{C})$ vers les diviseurs de degré 0 sur $\mathcal{C}$.*

Démonstration. Cela découle directement des propriétés de la valuation en un point. □

L'ensemble des diviseurs principaux est donc un sous-groupe des diviseurs de degré 0. On le note $\text{Pr}(\mathcal{C})$. Soit f une fonction. On découpe souvent $\text{div}(f)$ en la différence de deux diviseurs effectifs :

$$\text{div}(f) = \text{div}_0(f) - \text{div}_\infty(f),$$

où $\text{div}_0(f)$ correspond à l'intersection de $\mathcal{C}$ avec la courbe $f = 0$, et $\text{div}_\infty(f)$ à l'intersection avec $\frac{1}{f} = 0$. Sur le dessin ci-dessous on a ainsi

$$\text{div}(f) = P_1 + P_2 + P_3 + P_4 - (2Q_1 + 2Q_2).$$

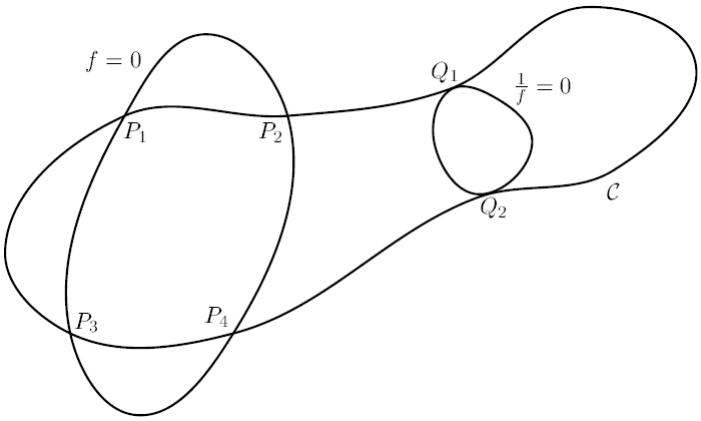

FIGURE 3.1 – (cf. [Gau00] p.11)

3.2 Jacobienne

3.2.1 Jacobienne et corps de définition

En général les diviseurs de degré 0 ne sont pas tous principaux, les diviseurs principaux forment un sous-groupe de $\mathrm{Div}^0(\mathcal{C})$.

Définition 3.2.1. La Jacobienne de $\mathcal{C}$ est le groupe des diviseurs de degré 0 quotienté par celui des diviseurs principaux :

$$\mathrm{Jac}(\mathcal{C}) = \mathrm{Div}^0(\mathcal{C})/\mathrm{Pr}(\mathcal{C}).$$

Deux diviseurs D et D' qui sont dans la même classe sont dits linéairement équivalents ; on le note

$$D \sim D'.$$

Avant de donner quelques exemples concrets, nous allons préciser ce qu'il faut adapter dans les définitions précédentes si l'on veut travailler sur un corps non algébriquement clos. Soit donc $\mathbf{K}$ un corps quelconque contenant les coefficients de l'équation de la courbe $\mathcal{C}$ et $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. De manière générale, un objet sera dit défini sur $\mathbf{K}$ s'il est invariant sous l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{K}}/\mathbf{K})$.

Un point de la courbe $\mathcal{C}$ est défini sur $\mathbf{K}$ si ses coordonnées sont dans $\mathbf{K}$. Un diviseur est défini sur $\mathbf{K}$ s'il est invariant sous l'action du groupe de Galois. Cela ne signifie pas que tous les points qui le composent sont définis sur $\mathbf{K}$; en effet, l'action de Galois peut permuter les points. Un diviseur sur $\mathbf{K}$ est donc une somme de cycle de conjugués de points : si un point défini sur une extension de $\mathbf{K}$ est dans le support du diviseur, alors tous ses conjugués y sont aussi avec le même coefficient.

Une fonction est définie sur $\mathbf{K}$ si ses coefficients sont dans $\mathbf{K}$; et il s'ensuit immédiatement que le diviseur d'une fonction sur $\mathbf{K}$ est défini sur $\mathbf{K}$. On note avec l'indice $\mathbf{K}$ tous les ensembles d'objets définis sur $\mathbf{K}$: $\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$, $\mathrm{Div}_{\mathbf{K}}(\mathcal{C})$, $\mathrm{Div}^0_{\mathbf{K}}(\mathcal{C})$, $\mathrm{Pr}_{\mathbf{K}}(\mathcal{C})$.

Définir sans ambiguïté la Jacobienne sur $\mathbf{K}$ nécessite un résultat qui prouve que les éléments de la Jacobienne qui sont invariants sous l'action de Galois forment exactement le groupe quotient $\mathrm{Div}^0_{\mathbf{K}}(\mathcal{C})/\mathrm{Pr}_{\mathbf{K}}(\mathcal{C})$.

Théorème 3.2.1. *Soit $\mathcal{C}$ une courbe définie sur $\mathbf{K}$ possédant un point défini sur $\mathbf{K}$ et D un diviseur de degré 0 sur $\mathbf{K}$. S'il existe un diviseur principal* $\mathrm{div}(f)$ *défini sur $\overline{\mathbf{K}}$ tel que $D' = D + \mathrm{div}(f)$ soit défini sur $\mathbf{K}$ alors il existe une fonction F définie sur $\mathbf{K}$ telle que* $\mathrm{div}(f) = \mathrm{div}(F)$.

La preuve de ce résultat repose sur le théorème de Riemann-Roch qui sera énoncé à la section suivante. La conséquence est que

$$\mathrm{Jac}_{\mathbf{K}}(\mathcal{C}) = \mathrm{Div}^0_{\mathbf{K}}(\mathcal{C})/\mathrm{Pr}_{\mathbf{K}}(\mathcal{C}).$$

L'étude sur un corps non algébriquement clos nécessite l'introduction d'une notion supplémentaire pour les diviseurs.

Définition 3.2.2. Un diviseur D défini sur $\mathbf{K}$ est dit premier si

1. D est effectif,
2. Si D' est effectif, défini sur $\mathbf{K}$ et $D' \leq D$, alors D' est nul ou égal à D.

Les diviseurs premiers sont en fait les sommes de tous les conjugués d'un point défini sur une extension de $\mathbf{K}$. Dans le cas d'un corps algébriquement clos, les diviseurs premiers sont exactement les points de la courbe.

Exemple 3.2.1. Considérons la courbe sur $\mathbb{Q}$ d'équation $y^2 + xy + 2y = x^3 + x^2 - 3x - 1$. Son allure lorsqu'on la trace sur $\mathbb{R}$ est la suivante

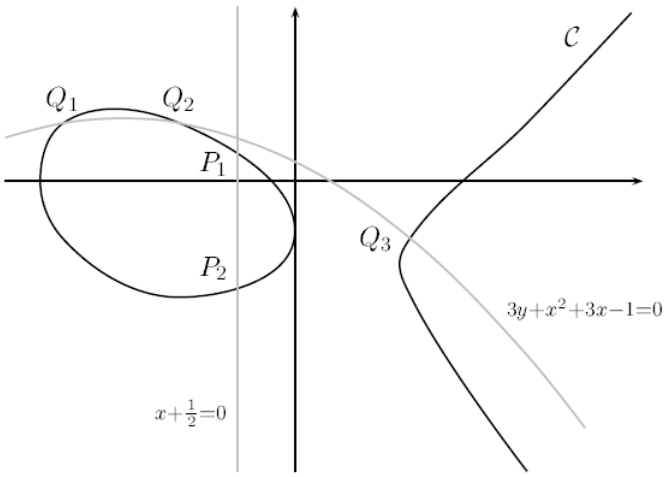

FIGURE 3.2 – (cf. [Gau00] p.13)

Pour illustrer les définitions précédentes, il est nécessaire d'avoir une courbe projective. On rajoute donc le point à l'infini, noté P_∞ qui complète notre courbe affine en une courbe projective $\mathcal{C}$. Il est facile de vérifier que $\mathcal{C}$ est lisse, même en P_∞. La plupart du temps, on opérera ainsi : on travaille avec des modèles affines de courbes planes, et l'on manipule les points à l'infini formellement.

Soient P_1 et P_2 les deux points de $\mathcal{C}$ de coordonnées

$$P_1 = \left(-\frac{1}{2}, \frac{-3+\sqrt{19}}{4}\right) \quad \text{et} \quad P_2 = \left(-\frac{1}{2}, \frac{-3-\sqrt{19}}{4}\right).$$

Ces deux points sont conjugués sur $\mathbb{Q}$ et le diviseur $D = P_1 + P_2$ est un diviseur premier de degré 2 défini sur $\mathbb{Q}$. Soit la fonction f sur $\mathcal{C}$ définie par

$$f = \frac{3y + x^2 + 3x - 1}{x + \frac{1}{2}}.$$

La courbe correspondant à l'annulation du numérateur coupe $\mathcal{C}$ en les trois points $Q_1 = (2,1),\ Q_2 = (1,1),\ Q_3 = (1,1)$, et celle correspondant au dénominateur coupe $\mathcal{C}$ en P_1 et P_2. Si l'on tient compte des intersections à l'infini, on obtient ainsi

$$\mathrm{div}(f) = Q_1 + Q_2 + Q_3 - P_1 - P_2 - P_\infty.$$

Ainsi par exemple les deux diviseurs de degré 0 suivants sont linéairement équivalents :

$$P_1 + P_2 - Q_1 - Q_2 \ \sim\ Q_3 - P_\infty.$$

3.2.2 Théorème de Riemann-Roch

Le théorème de Riemann-Roch est un outil très important pour l'étude des courbes algébriques. Il permet de définir le genre de la courbe qui est un invariant fondamental et il fournit l'existence de représentants agréables dans chaque classe de la Jacobienne.

Soit $D = \sum_{P \in \mathcal{C}} n_P P$ un diviseur sur $\mathcal{C}$. Chaque D sélectionne un nombre fini de points, et leur attribue des entiers. Nous voulons déterminer quand il y a une fonction rationnelle avec des pôles uniquement aux points choisis, et avec des pôles pas «pires» que l'ordre n_P en P.

Soit $L(D)$ l'ensemble $\left\{ f \in \mathbf{K}(\mathcal{C})^*,\ \mathrm{ord}_P(f) \geq -n_P,\ \forall P \in \mathcal{C} \right\} \cup \{0\}$, où $D = \sum_{P \in \mathcal{C}} n_P P$.

Une fonction rationnelle f appartient à $L(D)$ si $\mathrm{div}(f) - D \geq 0$, ou si $f = 0$. On peut donc redéfinir $L(D)$ de la manière suivante :

Définition 3.2.3. Soit $\mathcal{C}$ une courbe définie sur $\mathbf{K}$ et D un diviseur sur $\mathbf{K}$. On note $L(D)$ l'ensemble des fonctions de $\mathbf{K}(\mathcal{C})$, qui sont soit nulles, soit de diviseur plus grand que $-D$:

$$L(D) = \{\ f \in \mathbf{K}(\mathcal{C}) \mid \mathrm{div}(f) \geq -D \text{ ou } f = 0\}.$$

Le lemme suivant nous renseigne sur la nature de $L(D)$.

Lemme 3.2.1. *Soit D un diviseur.*

(1) *Si $D \leq D'$, alors $L(D) \subset L(D')$, et $\dim_{\mathbf{K}}((L(D')/L(D)) \leq deg(D' - D)$, pour D' un diviseur.*

(2) *L'ensemble $L(D)$ est un espace vectoriel de dimension finie. Sa dimension est notée $l(D)$.*

Démonstration.

(1) On a $D' = D + P_1 + \ldots + P_s$, donc $L(D) \subset L(D + P_1) \subset \ldots \subset L(D + P_1 + \ldots + P_s)$, ainsi il suffit de montrer que $\dim(L(D + P)/L(D)) \leq 1$. Pour prouver cela, soit t une uniformisante dans $\mathcal{O}_P(\mathcal{C})$, et soit $r = n_P$ le coefficient de P dans D.
définissons $\varphi : L(D + P) \longrightarrow \mathbf{K}$ par $\varphi(f) = (t^{r+1} f)(P)$. Puisque $\mathrm{ord}_P(f) \geq -r - 1$, φ est bien défini, φ est une application linéaire, et $\ker(\varphi) = L(D)$, ainsi φ induit une unique application linéaire $\overline{\varphi} : L(D + P)/L(D) \longrightarrow \mathbf{K}$, ce qui donne le résultat.

(2) La seule chose à montrer est que la dimension est finie.
Si $\deg(D) = n \geq 0$, choisissons $P \in \mathcal{C}$, et soit $D' = D - (n + 1)P$. Alors $L(D') = 0$, et d'après (1), $\dim(L(D)/L(D')) \leq n + 1$, ainsi $l(D) \leq n + 1$.

□

Le principe sous-jacent est que lorsque l'on rajoute un point à un diviseur, le degré augmente de un, et la dimension de l'espace L(D) augmente d'au plus un. Dans le lemme précédent, le résultat qui nous intéresse est le (2).

Théorème 3.2.2 (Riemann-Roch)**.** *Soit $\mathcal{C}$ une courbe sur un corps $\mathbf{K}$. Il existe un entier g et un diviseur W tels que pour tout diviseur D*

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

L'entier g est appelé le genre de la courbe et W est un diviseur canonique.

Pour une courbe donnée, un diviseur canonique peut être calculé, et donc le théorème de Riemann-Roch donne une valeur exacte pour $l(D)$. Toutefois, dans de nombreux cas, il suffit de minorer le terme $l(W - D)$ par zéro pour obtenir ce que l'on veut. Cette forme un peu plus faible est ce qu'on appelle le théorème de Riemann.

Le genre g de la courbe est une notion qui admet une interprétation intuitive simple. Si le corps de base est le corps des complexes, alors une courbe projective lisse est en fait une surface

de Riemann, et le genre est alors le « nombre de trous » dans cette surface. Par exemple, la sphère de Riemann $\mathbb{P}^1(\mathcal{C})$ est de genre 0 et un tore à un trou est une courbe elliptique (de genre 1). Revenons à la Jacobienne de $\mathcal{C}$: c'est un groupe de classes, et le problème se pose donc de trouver un représentant canonique pour chaque classe. Le théorème suivant donne déjà l'existence d'une forme agréable d'un représentant.

Théorème 3.2.3. *Soit P_∞ un point de la courbe $\mathcal{C}$ fixé à l'avance. Pour tout diviseur D de degré zéro, il existe un diviseur effectif E de degré $r \leq g$, ne contenant pas P_∞ tel que*

$$D \sim E - rP_\infty.$$

Démonstration. Considérons le diviseur $D' = D + gP_\infty$ de degré g. Le théorème de Riemann-Roch donne $l(D') = 1 + l(W - D') \geq 1$, et assure donc l'existence d'une fonction f non nulle telle que $\mathrm{div}(f) + D' \geq 0$; notons E' le diviseur effectif $\mathrm{div}(f) + D'$. On a $D + div(f) = E' - gP_\infty$, donc

$$D \sim E' - gP_\infty.$$

Si l'on prend en compte le fait qu'il faut éliminer les éventuels P_∞ intervenant dans E', on a le résultat.

□

Exemple 3.2.2. Une courbe elliptique[1] est une courbe de genre 1. On peut montrer qu'une telle courbe est isomorphe à une courbe admettant un modèle affine sous forme de Weierstrass, c'est-à-dire une équation de la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, tout comme dans l'exemple 3.2.1 page 31. Appliquons le théorème précédent en prenant pour P_∞ l'unique point à l'infini de la courbe sous cette forme. Chaque classe de la Jacobienne contient un diviseur de la forme $P - P_\infty$ ou bien 0. Le deuxième cas signifie qu'il s'agit de la classe triviale, et dans le cas général, toute classe peut-être représentée par un point de la courbe. Réciproquement, soient P et Q deux points de la courbe, alors $P - P_\infty$ et $Q - P_\infty$ définissent la même classe si et seulement si P et Q sont égaux.

Ainsi la Jacobienne d'une courbe elliptique est la courbe elle-même. Quand on trace une droite, on considère le diviseur principal de la fonction donnée par l'équation de cette droite.

Nous donnons un résultat plus précis que le théorème précédent, dû à Galbraith, Paulus et Smart et qui fournit un représentant unique dans chaque classe.

Théorème 3.2.4. *Soit P_∞ un point de la courbe $\mathcal{C}$ fixé à l'avance. Pour tout diviseur D de degré zéro, il existe un unique diviseur effectif E de degré minimal m, ne contenant pas P_∞, tel que*

$$D \sim E - mP_\infty.$$

Un tel diviseur minimal est appelé diviseur réduit, l'entier m est appelé le poids du diviseur.

Démonstration. L'existence d'un tel diviseur est assuré par le théorème précédent. Si $m = 0$ alors D est principal et il n'y a rien à montrer. Nous allons prouver l'unicité dans le cas $m \geq 1$. Soit $D_0 = E - mP_\infty$ une représentation de D avec m minimal. Montrons d'abord que $l(E) = 1$. Supposons que $l(D_0 + (m-1)P_\infty)$ soit non nul. Alors il existe une fonction f telle que $\mathrm{div}(f) + D_0 + (m-1)P_\infty = E' \geq 0$, et donc $E' - (m-1)P_\infty$ est une représentation de poids $m-1$ de D, ce qui contredit la minimalité de m. Ainsi $l(D_0 + (m-1)P_\infty) = 0$. Le fait de rajouter un point à un diviseur fait augmenter la dimension de l'espace associé d'au plus une unité, donc $l(D_0 + mP_\infty) \leq 1$. Or $D_0 + mP_\infty = E$ est un diviseur effectif et les constantes forment un sous-espace vectoriel de $l(D_0 + mP_\infty)$. Il s'ensuit que

$$l(E) = 1.$$

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

□

1. Cette notion sera présentée plus formellement dans la prochaine section.

3.3 Courbes elliptiques

L'une des applications les plus importantes du théorème de Riemann-Roch est de trouver des équations affines pour une courbe avec un corps de fonctions donné. Nous le démontrerons dans deux cas particuliers qui sont les centres d'intérêts dans bien de domaines de mathématiques. On peut citer [Sil86] comme référence pour ce chapitre, et [CFA+06] nous fait un bon rappel.

3.3.1 Première approche

Définition 3.3.1. Une courbe elliptique définie sur un corps $\mathbf{K}$ est une courbe projective sur $\mathbf{K}$ lisse absolument irréductible, de genre 1, et possédant au moins un point $\mathbf{K}$-rationnel.

Soit $\mathcal{C}$ une courbe lisse et absolument irréductible, de genre 1 possédant au moins un point $\mathbf{K}$-rationnel P_∞ et $\mathbf{K}(\mathcal{C})$ son corps de fonctions. Comme $l(P_\infty) = 1$ nous avons donc $L(P_\infty) = \mathbf{K}$.

Le théorème de Riemann-Roch garantit que $l(2P_\infty) = 2$, donc il existe une fonction $x \in \mathbf{K}(\mathcal{C})$ telle que $\{1, x\}$ soit une base de $L(2P_\infty)$ sur $\mathbf{K}$. Il existe également $y \in \mathbf{K}(\mathcal{C})$ tel que $\{1, x, y\}$ est une base de $L(3P_\infty)$ sur $\mathbf{K}$. Nous trouvons facilement que $\{1, x, y, x^2\}$ est une base de $L(4P_\infty)$ et que $\{1, x, y, x^2, xy\}$ est une base de $L(5P_\infty)$. L'espace $L(6P_\infty) \supset \langle\{1, x, y, x^2, xy, x^3, y^2\}\rangle$ est de dimension 6, il doit donc y avoir une dépendance linéaire entre ces sept fonctions. Dans cette relation, y^2 doit avoir un coefficient non trivial a. En multipliant la relation par a et en remplaçant y par $a^{-1}y$, nous pouvons supposer que $a = 1$. La fonction x^3 doit également apparaître de manière non triviale, avec un certain coefficient b. Multiplions la relation par b^2 et remplaçons x par $b^{-1}x$, y par $b^{-1}y$. Ensuite, les coefficients de y^2 et x^3 sont égaux à 1 et nous obtenons une relation

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,\ a_i \in \mathbf{K}.$$

C'est l'équation d'une courbe affine plane absolument irréductible. C'est un fait (encore obtenu par l'utilisation du théorème de Riemann-Roch) que cette courbe est lisse. La fermeture projective $\overline{\mathcal{C}}$ de $\mathcal{C}$ est donnée par

$$Y^2Z + a_1XYZ + a_3XZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in \mathbf{K}$$

avec des coordonnées projectives planes $[X : Y : Z]$. On voit que $\overline{\mathcal{C}} \setminus \mathcal{C} = \{[0 : 1 : 0]\}$ et que $P_\infty := [0 : 1 : 0]$ est lisse. $\overline{\mathcal{C}}$ est donc une courbe projective plane lisse, absolument irréductible, de genre 1.

Encore une fois, en utilisant le théorème de Riemann-Roch, on peut prouver que l'inverse est également valable. La courbe projective donnée par

$$Y^2Z + a_1XYZ + a_3XZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in \mathbf{K}$$

est une courbe de genre 1 si et seulement si elle est lisse. Nous avons vu que le théorème de Riemann-Roch donne :

Théorème 3.3.1. *Un corps de fonctions $\mathbf{K}(\mathcal{C})$ de genre 1 avec un diviseur premier de degré 1 est le corps des fonctions d'une courbe elliptique E. Cette courbe est isomorphe à une courbe projective plane lisse donnée par une équation de Weierstrass*

$$E:\ Y^2Z + a_1XYZ + a_3XZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in \mathbf{K}.$$

Une partie affine non singulière plane E_a de E est donnée par

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,\ a_i \in \mathbf{K}.$$

$E \setminus E_a$ se compose d'un unique point avec des coordonnées homogènes $[0 : 1 : 0]$.

Inversement, des courbes non singulières données par des équations du type

$$E:\ Y^2Z + a_1XYZ + a_3XZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in \mathbf{K}$$

ont des corps de fonctions de genre 1 avec au moins un diviseur premier de degré 1, tout comme les courbes elliptiques.

Chapitre 4

Courbes définies sur un corps fini et conjectures de Weil

Dans ce chapitre, nous verrons quelques résultats autour des variétés abéliennes, et présenterons les conjectures de Weil.

Tout au long de ce chapitre, $\mathbf{K}$ désigne un corps parfait (cf. chapitre 1) et $\overline{\mathbf{K}}$ une clôture algébrique fixée de $\mathbf{K}$, $\mathbf{L}$ désigne une extension de $\mathbf{K}$ contenue dans $\overline{\mathbf{K}}$. On note $\mathrm{Aut}_{\mathbf{L}}\left(\overline{\mathbf{K}}\right)$ (ou bien $G_{\mathbf{L}}$) son groupe de Galois absolu.

4.1 Variétés abéliennes

La Jacobienne d'une courbe de genre g est une variété algébrique projective de dimension g munie d'une loi de groupe. De plus cette loi s'exprime localement par des formules algébriques. Un tel objet est appelé une variété abélienne et possède de riches propriétés. Nous en donnerons ici quelques unes. Le sujet est largement traité dans [Lan83] et dans [Mum74].

4.1.1 Groupes algébriques

L'idée est de combiner la structure de groupe avec le celle de variété.

Définition 4.1.1. Un groupe algébrique $\mathcal{G}$ est une variété (affine ou projective) munie de deux applications régulières

$$\begin{array}{rccc} m: & \mathcal{G}\times\mathcal{G} & \longrightarrow & \mathcal{G} \\ & (P,Q) & \longmapsto & m(P,Q) \end{array} \qquad \text{et} \qquad \begin{array}{rccc} i: & \mathcal{G} & \longrightarrow & \mathcal{G} \\ & P & \longmapsto & i(P) \end{array}$$

satisfaisant aux axiomes de groupes suivants :

- (i) Il existe un point $O \in \mathcal{G}$ tel que $m(P,O) = m(O,P) = P$ pour tout $P \in \mathcal{G}$.
- (ii) $m(P,i(P)) = m(i(P),P) = O$ pour tout $P \in \mathcal{G}$.
- (iii) $m(P,m(Q,R)) = m(m(P,Q),R)$ pour tout $P,Q,R \in \mathcal{G}$.

  $\mathcal{G}$ est un groupe algébrique commutatif s'il satisfait en outre
- (iv) $m(P,Q) = m(Q,P)$ pour tout $P,Q \in \mathcal{G}$.

Le groupe algébrique $\mathcal{G}$ est défini sur $\mathbf{K}$ si $\mathcal{G}$ est défini sur $\mathbf{K}$, les applications m et i sont définies sur $\mathbf{K}$, et $O \in \mathcal{G}(\mathbf{K})$. Soit $\mathbf{L}/\mathbf{K}$ une extension. Soit $\mathcal{G}(\mathbf{L})$ l'ensemble des points $\mathbf{L}$-rationnels. L'ensemble $\mathcal{G}(\mathbf{L})$ est un groupe dans lequel la somme et l'inverse des éléments sont calculés en évaluant les morphismes qui sont définis sur $\mathbf{K}$, qui ne dépendent pas de $\mathbf{L}$, et dans lequel l'élément neutre est le point O.

Exemple 4.1.1. Le groupe additif $\mathbb{G}_a$ est un groupe algébrique commutatif

$$\mathbb{G}_a \cong \mathbb{A}^1 = \mathbf{K}.$$

Le groupe additif $\mathbb{G}_a$ est clairement une variété affine. La loi de groupe sur $\mathbb{G}_a$ est définie par les applications régulières

$$\begin{array}{rccc} m: & \mathbb{G}_a \times \mathbb{G}_a & \longrightarrow & \mathbb{G}_a \\ & (x,y) & \longmapsto & x+y \end{array} \qquad \text{et} \qquad \begin{array}{rccc} i: & \mathbb{G}_a & \longrightarrow & \mathbb{G}_a \\ & x & \longmapsto & -x. \end{array}$$

Loi de groupes sur des courbes elliptiques

On suppose que $\mathbf{K}$ est algébriquement clos. Soit E une courbe elliptique donnée par une équation de Weierstrass. Ainsi $E \subset \mathbb{P}^2$ consiste en des points $P = (x, y)$ satisfaisant l'équation de Weierstrass, ainsi que le point $O = [0 : 1 : 0]$ à l'infini. Soit $L \subset \mathbb{P}^2$ une droite. Puisque l'équation est de degré 3, la droite L coupe E en exactement trois points, disons P, Q, R. Bien sûr, si L est tangent à E, alors P, Q, R n'ont pas besoin d'être distincts. Le fait que $L \cap E$, pris avec des multiplicités, se compose d'exactement trois points est un cas particulier du théorème de Bezout [1]. Cependant, puisque nous donnons des formules explicites plus loin dans cette partie, il n'est pas nécessaire d'utiliser un théorème général.

On définit une loi de composition $\oplus$ sur E par la règle suivante :

Loi de composition : Soit $P, Q \in E$, soit L la droite passant par P et Q (si $P = Q$, soit L la tangente à E en P), et soit R le troisième point d'intersection de L avec E. Soit L' la droite passant par R et O. Alors L' coupe E en R, O et un troisième point. On note ce troisième point par $P \oplus Q$.

Divers exemples de cette loi de composition sont illustrés à la figure 6.1.

Nous justifions maintenant l'utilisation du symbole $\oplus$.

Proposition 4.1.1.

La loi de composition $\oplus$ a les propriétés suivantes :

(*i*) *Si une droite L coupe E aux points (pas nécessairement distincts) P, Q et R, alors*

$$P \oplus Q \oplus R = O.$$

(*ii*) $P \oplus O = P$ *pour tout* $P \in E$.

(*iii*) $P \oplus Q = Q \oplus P$ *pour tout* $P, Q \in E$.

(*iv*) *Soit $P \in E$. Il existe un point de E, noté $\ominus P$, satisfaisant*

$$P \oplus (\ominus P) = O.$$

(*v*) *Soient $P, Q, R \in E$. Alors*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

En d'autres termes, la loi de composition $\oplus$ fait de E un groupe abélien avec O pour élément neutre. En outre :

(*vi*) *Supposons que E soit défini sur $\mathbf{K}$. Alors,*

$$E(\mathbf{K}) = E_a = \{(x, y) \in \mathbf{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x_2 + a_4x + a_6\} \cup \{O\}$$

est un sous-groupe de E.

1. Deux courbes algébriques Projectives planes, sans composantes communes, respectivement de degré n et de degré m, ont au plus $n \times m$ points d'intersections , comptés avec leur multiplicité. Si le corps de base est algébriquement clos (exemple $\mathbb{C}$), alors il ya exactement $n \times m$ points d'intersections.

On peut consulter [Sil86] p.52 pour la preuve.

Notation. À partir de là, nous remplaçons les symboles $\oplus$ et $\ominus$ par $+$ et $-$ pour l'opération de groupe sur une courbe elliptique E. Pour $m \in \mathbb{Z}$ et $P \in E$, on pose

$$[m]P = \overbrace{P + \cdots + P}^{m \text{ fois si } m > 0}, \qquad [m]P = \overbrace{-P - \cdots - P}^{|m| \text{ fois si } m < 0}, \qquad [0]P = O.$$

Nous dérivons maintenant des formules explicites pour les opérations de groupe sur E. Tout cela est résumé dans l'algorithme suivant

Proposition 4.1.2 (Algorithme de loi de groupe)**.**
Soit E une courbe elliptique donnée par une équation de Weierstrass

$$E : y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_4.$$

(*i*) *Soit $P_0 = (x_0, y_0)$. Alors*

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

(*ii*) *Soit ensuite*

$$P_1 + P_2 = P_3 \;\text{ avec } P_i = (x_i, y_i) \in E \text{ pour tout } i = 1, 2, 3.$$

Si $x_1 = x_2$ et $y_1 + y_2 + a_1x_2 + a_3 = 0$, alors

$$P_1 + P_2 = O.$$

Autrement, définissons λ et ν par les formules suivantes :

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Alors $y = \lambda x + \nu$ est la droite passant par P_1 et P_2 ou la tangente à E si $P_1 = P_2$.

(*iii*) *Avec les notations comme en (ii), $P_3 = P_1 + P_2$ a pour coordonnées*

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned}$$

Exemple 4.1.2. Soit E la courbe elliptique sur $\mathbb{Q}$

$$E : y^2 = x^3 + 17.$$

Une brève inspection révèle certains points ayant des coordonnées entières,

$$P_1 = (-2, 3), \quad P_2 = (-1, 4), \quad P_3 = (2, 5), \quad P_4 = (4, 9), \quad P_5 = (8, 23),$$

et une recherche informatique en donne d'autres,

$$P_6 = (43, 282), \quad P_7 = (52, 375), \quad P_8 = (5234, 378661).$$

En utilisant la formule d'addition, on vérifie des relations telles que

$$P_5 = [-2]P_1, \quad P_4 = P_1 - P_3, \quad [3]P_1 - P_3 = P_7.$$

Il y a aussi beaucoup de points avec des coordonnées rationnelles non entières, par exemple

$$[2]P_2 = \left(\frac{127}{64}, -\frac{2651}{512}\right), \quad P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Définition 4.1.2. Une variété abélienne est une variété projective lisse munie d'une loi de groupe commutatif.

Remarque 4.1.1.

1. Il n'est pas nécessaire de mettre la commutativité dans la définition, car celle-ci découle des autres propriétés (cf [Lan83], p.20).
2. Pour faire la connexion avec les groupes abéliens plus évidents, nous remplaçons $m(P, Q)$ par la notation $P \oplus Q$ pour $P, Q \in \mathcal{G}(\overline{\mathbf{K}})$ et $i(P)$ par $-P$.

Nous nous concentrerons désormais sur les variétés abéliennes et utiliserons plutôt la notation standard $\mathcal{A}$ au lieu de $\mathcal{G}$.

4.1.2 Homomorphismes des variétés abéliennes

Nous supposons que $\mathcal{A}$ et $\mathcal{B}$ sont des variétés abéliennes sur $\mathbf{K}$ avec des lois d'addition respectives $\oplus$ et $\oplus'$. Soit f un élément de $\mathrm{Mor}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$ [2].

Exemple 4.1.3. Soit $P \in \mathcal{A}$ et définissons

$$\begin{array}{rccc} t_P : & \mathcal{A} & \longrightarrow & \mathcal{A} \\ & Q & \longmapsto & P \oplus Q. \end{array}$$

Ici, t_P est appelé la translation par P et est un élément de $\mathrm{Mor}_{\mathbf{K}}(\mathcal{A}, \mathcal{A})$.

Un fait intéressant est que pour tout $f \in \mathrm{Mor}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$, nous avons

$$f(P \oplus Q) = f(P) \oplus' f(Q)$$

pour tous points $P, Q \in \mathcal{A}$ si et seulement si $f(0)$ est l'élément neutre de $\mathcal{B}$. En d'autres termes, toute application régulière $f : \mathcal{A} \longrightarrow \mathcal{B}$ est un homomorphisme par rapport aux lois d'addition à translation $t_{(-f(0))}$ en $\mathcal{B}$ près (cf [Lan83], p.24). L'ensemble des homomorphismes de $\mathcal{A}$ vers $\mathcal{B}$ est noté $\mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$.

Soit $\mathbf{L}/\mathbf{K}$ une extension de corps et prenons $f \in \mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$. On obtient un homomorphisme de groupes $f_{\mathbf{L}} : \mathcal{A}(\mathbf{L}) \longrightarrow \mathcal{B}(\mathbf{L})$ qui est donné en évaluant les polynômes à coefficients dans $\mathbf{K}$. Une observation importante est que $f_{\mathbf{L}}$ commute avec l'action du groupe de Galois $G_{\mathbf{K}}$ de $\mathbf{K}$.

L'ensemble des homomorphismes $\mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$ devient un $\mathbb{Z}$-module de la manière habituelle : pour $f_1, f_2 \in \mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})$ et $P \in \mathcal{A}$, définissons

$$(f_1 + f_2)(P) := f_1(P) \oplus' f_2(P).$$

Dans de nombreux cas, il est utile de travailler avec des espaces vectoriels au lieu de modules, d'où nous définissons donc

$$\mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})^0 := \mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

$\mathrm{Hom}_{\mathbf{K}}(\mathcal{A}, \mathcal{B})^0$ est un $\mathbb{Q}$-espace vectoriel de dimension finie (cf [CFA+06]).

2. L'ensemble des applications régulières de $\mathcal{A}$ dans $\mathcal{B}$.

Remarque 4.1.2. Les homomorphismes des variétés abéliennes se comportent de manière naturelle lors d'un changement de base : soit $\mathbf{L}/\mathbf{K}$ une extension de corps et soit $\mathcal{A}_\mathbf{L}$, $\mathcal{B}_\mathbf{L}$ les variétés abéliennes obtenues par extension scalaire à $\mathbf{L}$, $\mathrm{Hom}_\mathbf{L}(\mathcal{A},\mathcal{B}) := \mathrm{Hom}_\mathbf{L}(\mathcal{A}_\mathbf{L},\mathcal{B}_\mathbf{L})$. Le groupe Galois $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ agit naturellement sur $\mathrm{Mor}_\mathbf{L}(\mathcal{A}_\mathbf{L},\mathcal{B}_\mathbf{L})$ et donc sur $\mathrm{Hom}_\mathbf{L}(\mathcal{A},\mathcal{B})$.

Lemme 4.1.1. *Avec les notations précédentes, nous avons*

(*i*) *Soit* $\mathbf{L}_0$ *la clôture algébrique de* $\mathbf{K}$ *dans* $\mathbf{L}$. *Alors* $\mathrm{Hom}_\mathbf{L}(\mathcal{A},\mathcal{B}) = \mathrm{Hom}_{\mathbf{L}_0}(\mathcal{A},\mathcal{B})$.

(*ii*) *Pour* $\mathbf{L}$ *contenu dans* $\overline{\mathbf{K}}$, *on a* $\mathrm{Hom}_\mathbf{L}(\mathcal{A},\mathcal{B}) = \mathrm{Hom}_{\overline{\mathbf{K}}}(\mathcal{A},\mathcal{B})^{G_\mathbf{L}}$.

En raison des résultats suivants, nous pouvons penser que les variétés abéliennes se comportent comme des groupes abéliens.

Proposition 4.1.3. *Soit* $f \in \mathrm{Hom}_\mathbf{K}(\mathcal{A},\mathcal{B})$.

(*i*) *L'image* $\mathrm{Im}(f)$ *de* f *est une sous-variété de* $\mathcal{B}$, *qui devient une variété abélienne en restreignant la loi d'addition de* $\mathcal{B}$, *c'est-à-dire qu'il s'agit d'une sous-variété abélienne de* $\mathcal{B}$.

(*ii*) *Le noyau* $\ker(f)$ *de* f *est par définition l'image inverse de* $O_\mathcal{B}$. *C'est un fermé (par rapport à la topologie de Zariski) de* $\mathcal{A}$. *Ses points sont constitués de tous les points* P *de* $\mathcal{A}(\overline{\mathbf{K}})$ *tels que* $f_{\overline{\mathbf{K}}}(P) = O_\mathcal{B}$ *; et forment donc un sous-groupe de* $\mathcal{A}(\overline{\mathbf{K}})$.

(*iii*) *Le noyau* $\ker(f)$ *contient une sous-variété maximale absolument irréductible* $\ker(f)^0$ *contenant* $O_\mathcal{A}$. *Cette sous-variété est appelée la composante connexe de l'unité de* $\ker(f)$. *C'est une sous-variété abélienne de* $\mathcal{A}$.

(*iv*) *En termes de dimension, on a*

$$\dim(\mathrm{Im}(f)) + \dim(\ker(f)^0) = \dim(\mathcal{A}).$$

4.1.3 Isomorphismes et isogénies

Pour étudier les variétés abéliennes (du point de vue des ensembles), il est (comme d'habitude) important d'avoir un aperçu des isomorphismes entre eux. Les homomorphismes qui préservent la dimension de la variété abélienne sont très étroitement liés aux isomorphismes. Ils sont intensivement utilisés à la fois pour l'étude théorique et dans les applications de la cryptographie.

Définition 4.1.3. Soient $\mathcal{A}$ et $\mathcal{B}$ des variétés abéliennes sur $\mathbf{K}$. On appelle isogénie tout morphisme $\mathcal{I} \in \mathrm{Hom}_\mathbf{K}(\mathcal{A},\mathcal{B})$ telle que $\mathrm{Im}(\mathcal{I}) = \mathcal{B}$ et $\ker(\mathcal{I})$ est fini.

Proposition 4.1.4. *Un homomorphisme* $\mathcal{I} \in \mathrm{Hom}_\mathbf{K}(\mathcal{A},\mathcal{B})$ *est une isogénie si et seulement si* $\dim(\mathcal{A}) = \dim(\mathcal{B})$ *et* $\dim(\ker(\mathcal{I})^0) = 0$.

Le degré d'une isogénie est son degré en tant que morphisme de variété algébrique. Soit $\mathcal{I}$ une isogénie de $\mathcal{A}$ vers $\mathcal{B}$ et soit x un point générique sur $\mathcal{A}$, tous définis sur un corps $\mathbf{K}$. Alors le degré de $\mathcal{I}$ est le degré de l'extension de corps $[\mathbf{K}(x) : \mathbf{K}(\mathcal{I}(x))]$. Cette extension se décompose en une extension purement inséparable et une extension séparable. On appelle degré inséparable et degré séparable de $\mathcal{I}$ les degrés respectifs de ces extensions, dont le produit est le degré de l'isogénie.

Définition 4.1.4. Les homomorphismes $\mathrm{End}_\mathbf{K}(\mathcal{A}) := \mathrm{Hom}_\mathbf{K}(\mathcal{A},\mathcal{A})$ sont les endomorphismes de $\mathcal{A}$.

L'ensemble $\mathrm{End}_\mathbf{K}(\mathcal{A})$ est un anneau dont la composition est la loi multiplicative.

Exemple 4.1.4. Supposons que $\mathbf{K} = \mathbb{F}_p$. Alors ϕ_p induit l'application identité sur l'ensemble des polynômes à coefficients dans $\mathbf{K}$ et donc $\phi_p(\mathcal{A}) = \mathcal{A}$. Par conséquent, $\phi_p \in \mathrm{End}_{\mathbf{K}}(\mathcal{A})$; c'est l'endomorphisme de Frobenius. Une généralisation légère mais importante est de considérer $\mathbf{K} = \mathbb{F}_q$ avec $q = p^d$, pour $d \geq 1$. Alors $\phi_q := \phi_P^d$ est l'automorphisme relatif de Frobenius laissant fixes les éléments de $\mathbf{K}$. Nous pouvons appliquer les considérations faites ci-dessus à ϕ_q et obtenir un endomorphisme totalement inséparable de $\mathcal{A}$ de degré $p^{d\dim(\mathcal{A})}$ qui est appelé l'endomorphisme (relatif) de Frobenius de $\mathcal{A}$.

Un autre exemple d'isogénie est le suivant : soit $\mathcal{A}$ une variété abélienne de dimension g, et soit n un entier premier à la caractéristique du corps. Alors la multiplication par n, notée $[n]_{\mathcal{A}}$ et définie par

$$[n]_{\mathcal{A}}(x) = x + x + \ldots + x \quad (n\ fois),$$

est une isogénie de $\mathcal{A}$ vers $\mathcal{A}$ dont le noyau est de cardinal n^{2g} (cf [Lan83] ou [CFA+06] p.60).

Les isogénies sont des objets très importants. Le point crucial est que s'il existe une isogénie entre $\mathcal{A}$ et $\mathcal{B}$, alors il en existe une autre entre $\mathcal{B}$ et $\mathcal{A}$.

Théorème 4.1.1. *Soit $\mathcal{I}$ une isogénie de degré d entre deux variétés abéliennes $\mathcal{A}$ et $\mathcal{B}$. Alors il existe une isogénie, notée $\hat{\mathcal{I}}$, de $\mathcal{B}$ vers $\mathcal{A}$, telle que*

$$\mathcal{I}\hat{\mathcal{I}} = [d]_{\mathcal{A}} \quad et \quad \hat{\mathcal{I}}\mathcal{I} = [d]_{\mathcal{B}},$$

où $[d]\mathcal{A}$ et $[d]\mathcal{B}$ désignent respectivement les multiplications par d sur $\mathcal{A}$ et $\mathcal{B}$.

Ainsi la relation « il existe une isogénie entre deux variétés abéliennes » est symétrique. Elle est par ailleurs transitive car la composée de deux isogénies est une isogénie. Finalement c'est une relation d'équivalence, et l'on dira que deux variétés sont isogènes s'il existe une isogénie entre les deux.

Notation. Si $\mathcal{A}$ et $\mathcal{B}$ sont deux variétés abéliennes isogènes, on note

$$\mathcal{A} \sim \mathcal{B}.$$

Si elles sont isomorphes, ce qui est plus fort, on note

$$\mathcal{A} \cong \mathcal{B}.$$

4.1.4 Théorème de décomposition

La relation d'isogénie étant plus faible que celle d'isomorphisme, on peut introduire une notion «d'irréductibilité» adaptée à cette notion. Toute variété abélienne peut se décomposer de manière unique à isogénie près en produit de variétés abéliennes dites simples.

Théorème 4.1.2. *Soit $\mathcal{A}$ une variété abélienne et $\mathcal{B}$ une variété abélienne strictement incluse dans $\mathcal{A}$. Alors il existe une variété abélienne $\mathcal{C}$ tel le que $\mathcal{A}$ soit isogène au produit $\mathcal{B} \times \mathcal{C}$.*

Nous renvoyons à ([Lan83], p.28) pour une preuve.

Notons que l'on a $\dim(\mathcal{A}) = \dim(\mathcal{B}) + \dim(\mathcal{C})$. Ce théorème dit que dès qu'il existe une sous-variété abélienne propre, alors on peut en trouver une complémentaire.

Définition 4.1.5. Une variété abélienne est dite simple si elle n'admet pas de sous-variété abélienne autre que $\{0\}$ et elle-même.

Le théorème de décomposition est donc le suivant :

Théorème 4.1.3. *Toute variété abélienne est isogène à un produit de variétés abéliennes simples, unique à isogénie près.*

Ainsi toute variété abélienne $\mathcal{A}$ est isogène à un produit

$$(\mathcal{A}_1 \times \ldots \times \mathcal{A}_1) \times \ldots \times (\mathcal{A}_m \times \ldots \times \mathcal{A}_m)$$

où les $\mathcal{A}_i$ sont des variétés abéliennes simples deux-à-deux non isogènes. On peut alors décrire $\mathrm{End}^0(\mathcal{A})$ en fonction des $\mathrm{End}^0(\mathcal{A}_i)$. (cf [Lan83], p. 30)

4.1.5 Corps de définition

Dans tout ce qui précède, nous avons passé sous silence les problèmes de corps de définition. Si le corps $\mathbf{K}$ considéré n'est pas algébriquement clos, deux variétés abéliennes sont dites $\mathbf{K}$-isogènes s'il existe une isogénie définie sur $\mathbf{K}$ entre les deux. Le théorème de décomposition reste vrai sur $\mathbf{K}$, car si une variété abélienne $\mathcal{A}$ contient une sous-variété abélienne propre $\mathcal{B}$ définie sur $\mathbf{K}$, alors on peut trouver une variété abélienne $\mathcal{C}$ définie sur $\mathbf{K}$ telle que $\mathcal{A}$ et $\mathcal{B} \times \mathcal{C}$ sont $\mathbf{K}$-isogènes. Il est toutefois possible qu'une variété abélienne soit simple sur $\mathbf{K}$ mais ne le soit plus sur une clôture algébrique de $\mathbf{K}$. Cela motive la définition suivante :

Définition 4.1.6. Une variété abélienne est absolument simple si elle est simple sur toute extension algébrique de son corps de définition.

4.1.6 Sous-groupes de n-torsion

Nous avons dit précédemment que le cardinal du noyau de la multiplication par n notée $[n]\mathcal{A}$ est n^{2g}. Par ailleurs, ce noyau est un sous-groupe abélien.

Définition 4.1.7. On note $\mathcal{A}[n]$ le noyau de la multiplication par n sur une clôture algébrique

$$\mathcal{A}[n] = \ker([n]\mathcal{A}).$$

Ses éléments sont appelés éléments de n-torsion.

Le théorème suivant donne la structure de la n-torsion :

Théorème 4.1.4. *Soit $\mathcal{A}$ une variété abélienne de dimension g, et n un entier premier à la caractéristique du corps de base. Alors*

$$\mathcal{A}[n] \;\cong\; (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Lorsque n est égal à la caractéristique du corps, le résultat n'est plus vrai.

Théorème 4.1.5. *Soit $\mathcal{A}$ une variété abélienne de dimension g sur un corps $\mathbf{K}$ de caractéristique p. Alors*

$$\mathcal{A}[p](\overline{\mathbf{K}}) \;\cong\; (\mathbb{Z}/p\mathbb{Z})^{r},$$

où r est un entier tel que $0 \leq r \leq g$.

Le lecteur trouvera une preuve dans [Mum74], p. 64.

L'entier r est appelé le p-rang de $\mathcal{A}$ (et par abus de langage, on parle de p-rang d'une courbe pour le p-rang de sa Jacobienne).

Le rang de la p-torsion est un invariant important. Le cas le plus courant est celui où r est maximal. Les autres cas sont des cas particuliers.

Définition 4.1.8. Une courbe $\mathcal{C}$ de p-rang maximal est appelée ordinaire. Une courbe $\mathcal{C}$ dont le p-rang est zéro est appelée très spéciale.

4.2 Conjectures de Weil

Dans cette section, on se fixe un corps fini à $q = p^d$ éléments, noté $\mathbb{F}_q$, et l'on considère une courbe $\mathcal{C}$ de genre g définie sur ce corps. Le nombre de points de la courbe est fini, et la Jacobienne est un groupe fini. L'étude de la fonction Zêta, et les conjectures de Weil donnent des bornes précises sur les cardinalités de ces ensembles. Les preuves de tous les résultats de cette section peuvent être trouvés dans [Sti93].

4.2.1 Fonction Zêta

Proposition 4.2.1. $\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ *est un groupe fini.* $h = \#\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$

Démonstration. Choisissons un diviseur $B \in \mathrm{Div}(\mathcal{C})$ de degré $\geq g$, posons $n := \deg B$, et considérons l'ensemble des classes de diviseurs $\mathrm{Pic}^n := \{[D] \in \mathrm{Pic}(\mathcal{C}) \mid \deg[D] = n\}$. L'application

$$\begin{array}{rccc} f: & \mathrm{Jac}(\mathcal{C}) & \longrightarrow & \mathrm{Pic}^n(\mathcal{C}) \\ & [D] & \longmapsto & [D+B] \end{array}$$

est bijective. Nous allons vérifier que $\mathrm{Pic}^n(\mathcal{C})$ est fini. Par le théorème de Riemann-Roch, pour chaque $D \in \mathrm{Pic}^n(\mathcal{C})$ on a

$$l(D) \geq n - g + 1 \geq 1,$$

ce qui implique que la classe de D contient un diviseur effectif, or le nombre de diviseurs effectifs définis sur $\mathbb{F}_q$ de degré n est fini.

□

La fonction Zêta associée à une courbe $\mathcal{C}$ est une série génératrice liée au nombre de points de $\mathcal{C}$ définis sur une extension de degré n.

Définition 4.2.1. La fonction Zêta de $\mathcal{C}$ est définie par

$$Z(t) = \exp\left(\sum_{n\geq 1} N_n \frac{t^n}{n}\right),$$

où N_n est le nombre de points de $\mathcal{C}$ définis sur $\mathbb{F}_{q^n}$.

En regroupant les points en diviseurs effectifs, on peut réorganiser la série de manière à obtenir une définition équivalente :

Lemme 4.2.1. *La fonction Zêta de* $\mathcal{C}$ *vérifie :*

$$Z(t) = \sum_{n\geq 0}^{\infty} \mathcal{C}_n t^n,$$

où $\mathcal{C}_n = \#\{D \in Div(\mathcal{C});\ D \geq 0;\ \deg(D) = n\}$ *est le nombre de diviseurs effectifs de degré* n *sur* $\mathcal{C}$.

Nous définissons l'entier $\partial > 0$ par

$$\partial := \min\{\deg D \mid D \in \mathrm{Div}(\mathcal{C}) \text{ et } \deg D > 0\}.$$

Etudions les nombres $\mathcal{C}_n$.

Lemme 4.2.2.

a) $\mathcal{C}_n = 0$ *si* $\partial \nmid n$.

b) Pour une classe de diviseurs $[D] \in \mathrm{Pic}(\mathcal{C})$ *fixée, nous avons*

$$\mid \{A \in [D] \mid A \geq 0\} \mid = \frac{q^{l([D])} - 1}{q - 1}.$$

c) Pour chaque entier $n > 2g - 2$ *tel que* $\partial \mid n$ *on a*

$$\mathcal{C}_n = \frac{h}{q-1}(q^{n+1-g} - 1).$$

Démonstration. *a*) ce résultat est trivial.

b) Les conditions $A \in [D]$ et $A \geq 0$ sont équivalentes à

$$A = \mathrm{div}(f) + D, \text{ où } f \in L(\mathcal{C}) \setminus \{0\}.$$

Il y a exactement $q^{l([D])} - 1$ éléments $f \in L(\mathcal{C}) \setminus \{0\}$, et deux d'entre eux donnent le même diviseur si et seulement s'ils diffèrent d'un facteur constant $0 = \alpha \in \mathbb{F}_q$. ce qui prouve *b*).

c) Il ya h classes de diviseurs de degré n, notons les par $[D_1], \ldots, [D_h]$. D'après *b*) et le théorème de Riemann-Roch,

$$\mid \{A \in [D_j] \mid A \geq 0\} \mid = \frac{q^{l([D_j])} - 1}{q-1} = \frac{1}{q-1}(q^{n+1-g} - 1).$$

Chaque diviseur de degré n appartient exactement à l'une des classes de diviseurs $[D_1], \ldots, [D_h]$, d'où

$$\mathcal{C}_n = \sum_{j=1}^{h} \mid \{A \in [D_j] \mid A \geq 0\} \mid = \frac{h}{q-1}(q^{n+1-g} - 1).$$

□

Observons que nous considérons t comme une variable complexe, et $Z(t)$ est une série à variable complexe. Nous allons montrer que cette série converge dans un voisinage de 0.

Proposition 4.2.2. *La série $Z(t) = \sum_{n\geq 0}^{\infty} \mathcal{C}_n t^n$, est convergente pour $|t| < q^{-1}$. Plus précisement pour $|t| < q^{-1}$ on a :*

i) Si $\mathbf{K}(\mathcal{C})$ a pour genre $g = 0$ sur $\mathbb{F}_q$, alors

$$Z(t) = \frac{1}{q-1}\left(\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

ii) Si $g \geq 1$, alors $Z(t) = F(t) + G(t)$ avec

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[D] \leq 2g-2} q^{l([D])} \cdot t^{\deg[D]},$$

(où $[D]$ parcourt toutes les classes de diviseurs $[D] \in \mathrm{Jac}(\mathcal{C})$, avec $0 \leq \deg[D] \leq 2g-2$) et

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

Démonstration. *i)* $g = 0$. Pour commencer, nous montrons qu'un corps de fonctions de genre zéro a le nombre de classe $h = 1$; c'est-à-dire que chaque diviseur A de degré 0 est principal. Ce fait découle du théorème de Riemann-Roch : comme $0 > 2g - 2$, nous avons $l(A) = \deg A + 1 - g = 1$, et on peut donc trouver un élément $x \neq 0$ avec $(x) \geq -A$. Les deux diviseurs sont de degré 0, donc $A = -(x) = (x^{-1})$ est le principal. Maintenant nous appliquons le Lemme 4.2.2 et nous obtenons

$$\begin{aligned}
\sum_{n\geq 0}^{\infty} \mathcal{C}_n t^n &= \sum_{n\geq 0}^{\infty} \mathcal{C}_{\partial n} t^{\partial n} \\
&= \sum_{n\geq 0}^{\infty} \frac{1}{q-1}(q^{\partial n+1} - 1)t^{\partial n} \\
&= \frac{1}{q-1}\left(q\sum_{n\geq 0}^{\infty}(qt)^{\partial n} - \sum_{n\geq 0}^{\infty} t^{\partial n}\right) \\
&= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-(t)^{\partial}}\right)
\end{aligned}$$

pour $|qt| < 1$.

ii) Pour $g \geq 1$, le calcul est assez similaire. On obtient

$\sum_{n\geq 0}^{\infty} \mathcal{C}_n t^n = \sum_{\deg[D]\geq 0} \mid \{A \in [D]; A \geq 0\} \mid \cdot t^{\deg[D]} = \sum_{\deg[D]\geq 0} q^{\deg[D]+1-g} \cdot t^{\deg[D]}$
$- \dfrac{1}{q-1} \sum_{\deg[D]\geq 0} t^{\deg[D]} = F(t) + G(t),$
avec

$$F(t) = \frac{1}{q-1} \sum_{0\leq \deg[D]\leq 2g-2} q^{l([D])} \cdot t^{\deg[D]}$$

et

$$\begin{aligned}(q-1)G(t) &= \sum_{n=((2g-2)/\partial)+1}^{\infty} hq^{n\partial+1-g} \cdot t^{n\partial} - \sum_{n+0}^{\infty} ht^{n\partial} \\ &= hq^{1-g}(qt)^{2g-2+\partial} \frac{1}{1-(qt)^{\partial}} - h\frac{1}{1-(qt)^{\partial}}.\end{aligned}$$

□

Corollaire 4.2.1. *$Z(t)$ peut être étendue à une fonction rationnelle sur $\mathbb{C}$; elle a un pôle simple en $t = 1$.*

Démonstration. Il suffit de voir que $\dfrac{1}{1-t^{\partial}}$ a un pôle simple en $t = 1$.

□

Rappelons qu'un produit infini $\prod_{i=1}^{\infty}(1 + a_i)$ (avec des nombres complexes $a_i \neq -1$) est dit convergent avec la limite $a \in \mathbb{C}$ si $\lim_{n\to\infty} \prod_{i=1}^{n}(1 + a_i) = a \neq 0$. Le produit est dit absolument convergent si $\sum_{i=1}^{\infty} \mid a_i \mid < \infty$. D'après l'analyse, il est bien connu que la convergence absolue implique la convergence du produit, et la limite d'un produit absolument convergent est indépendant de l'ordre des facteurs. De plus, si le produit $\prod_{i=1}^{\infty}(1 + a_i) = a$ est absolument convergent, alors $\prod_{i=1}^{\infty}(1 + a_i)^{-1}$ converge absolument aussi, et $\prod_{i=1}^{\infty}(1 + a_i)^{-1} = a^{-1}$.

De manière analogue à la fonction Zêta ζ de Riemann, on peut transformer cette écriture en un produit Eulérien.

Lemme 4.2.3 (**Produit d'Euler**). *Pour $\mid t \mid < q^{-1}$ la fonction Zêta de $\mathcal{C}$ peut être représentée comme un produit absolument convergent*

$$Z(t) = \prod_{D \text{ premier}} \left(1 - t^{\deg(D)}\right)^{-1}.$$

En particulier $Z(t) \neq 0$ pour $|t| < q^{-1}$.

Démonstration. $\prod_{D \text{ premier}} \left(1 - t^{\deg(D)}\right)^{-1}$ converge absolument pour $|t| < q^{-1}$, puisque $\sum_{D \text{ premier}} |t|^{\deg P} \leq \sum_{n=0}^{\infty} \mathcal{C}_n |t|^n < \infty$ d'après la Proposition 4.2.2. Chaque facteur de $\prod_{D \text{ premier}} \left(1 - t^{\deg(D)}\right)^{-1}$ peut être écrit comme une série géométrique, et nous obtenons

$$\begin{aligned}\prod_{D \text{ premier}} \left(1 - t^{\deg(D)}\right)^{-1} &= \prod_{D \text{ premier}} \sum_{n=0}^{\infty} t^{\deg(nD)} \\ &= \sum_{A \,\in\, Div(\mathcal{C});\ A\geq 0} t^{\deg A} = \sum_{n=0}^{\infty} \mathcal{C}_n t^n = Z(t)\end{aligned}$$

□

Proposition 4.2.3. *Soit $Z(t)$ (resp. $Z_r(t)$) la fonction Zêta de $\mathcal{C}$ (resp. de $\mathbb{F}_{q^r}$). Alors*

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t),$$

pour tout $t \in \mathbb{C}$ (ζ parcourt les racines r-ième de l'unité).

Pour la preuve on peut consulter [Sti93] p.201.

Corollaire 4.2.2 (F.K. Shmidt). $\partial = 1$.

Démonstration. Pour $\zeta^\partial = 1$ nous avons

$$Z(\zeta t) = \prod_{P \text{ premier}} (1 - (\zeta t)^{\deg P})^{-1} = \prod_{P \text{ premier}} (1 - (t)^{\deg P})^{-1} = Z(t),$$

puisque ∂ divise le degré de P pour chaque P un diviseur premier. Donc $Z_\partial(t^\partial) = Z(t)^\partial$ par la proposition 5.2.4. La fonction rationnelle $Z_\partial(t^\partial)$ a un pôle simple à $t = 1$, par le corollaire 4.2.1, et $Z_\partial(t)^\partial$ a un pôle d'ordre ∂ à $t = 1$. D'où $\partial = 1$.

□

Corollaire 4.2.3.

a) toute courbe $\mathcal{C}$ de genre $g = 0$ sur $\mathbb{F}_q$ est rationnelle, et sa fonction zêta est

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

b) Si $\mathcal{C}$ est de genre $g \geq 1$, sa fonction Zêta peut s'écrire sous la forme $Z(t) = F(t) + G(t)$, avec

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[D] \leq 2g-2} q^{l([D])} \cdot t^{\deg[D]},$$

et

$$G(t) = \frac{h}{q-1} \left(q^g (t)^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t} \right).$$

Démonstration. Une courbe de genre 0 ayant un diviseur de degré 1 est rationnel, cf. [Sti93] p.32. Les autres affirmations découlent de la proposition 4.2.2 et $\partial = 1$.

□

Nous donnons ici les détails du calcul afin d'illustrer comment les objets introduits jusqu'ici se manipulent.

Exemple 4.2.1. Pour $\mathbb{P}^1(\mathbb{F}_q)$.

Pour tout $n \geq 1$, le nombre de points sur $\mathbb{P}^1(\mathbb{F}_{q^n})$ est $q^n + 1$, c'est-à-dire le nombre d'éléments dans le corps plus le point à l'infini. La série que l'on obtient est donc

$$Z(t) = \exp\left(\sum_{n \geq 1} (q^n + 1) \frac{t^n}{n} \right).$$

Après simplification, on obtient

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

4.2.2 Les conjectures de Weil

Dans les années 30, Hasse a obtenu des bornes pour le nombre de points sur une courbe elliptique définie sur un corps fini. Généralisant cela, Weil énonça en 1949 de célèbres conjectures concernant la fonction Zêta d'une variété définie sur un corps fini, et les prouva dans le cas particulier des courbes et des variétés abéliennes. Par la suite de nombreux travaux pour étendre ces résultats ont été faits par Dwork, Artin, Grothendieck, et Deligne. Pour le cas des courbes, on peut en trouver une preuve (essentiellement celle de Bombieri) dans [Sti93].

Théorème 4.2.1 (Conjectures de Weil). *Soit $\mathcal{C}$ une courbe de genre g sur un corps fini $\mathbb{F}_q$. Sa fonction Zêta $Z(t)$ possède les propriétés suivantes :*

a) ***Rationalité :*** *$Z(t)$ est une fraction rationnelle.*

b) ***Équation fonctionnelle :*** *$Z(t) = q^{g-1}\ t^{2g-2}\ Z\left(\dfrac{1}{qt}\right)$.*

c) ***Hypothèse de Riemann :*** *Les inverses des zéros de $Z(t)$ ont pour valeur absolue $\sqrt{q}$.*

Plus précisément, la fonction Zêta peut se mettre sous la forme

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

où $L(t)$ est un polynôme qui a les propriétés suivantes :

Théorème 4.2.2. *Le polynôme $L(t) = (1-t)(1-qt)Z(t)$ vérifie :*

i) C'est un polynôme de degré $2g$ à coefficients dans $\mathbb{Z}$.

ii) Le cardinal de la Jacobienne est $\#Jac(\mathcal{C}) = L(1)$.

iii) On a l'équation fonctionnelle $L(t) = q^g\ t^{2g}\ L\left(\dfrac{1}{qt}\right)$.

iv) Si l'on écrit $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$ alors,
   (1) $a_0 = 1$, et $a_{2g} = q^g$,
   (2) $a_{2g-i} = q^{g-i}a_i$, pour $0 \leq i \leq g$.

v) Si on écrit $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, on peut réarranger les indices de telle sorte que $\alpha_i\alpha_{g+i} = q$, et de plus $|\alpha_i| = \sqrt{q}$.

Démonstration. Toutes les assertions sont triviales pour $g = 0$, donc nous pouvons supposer à partir de maintenant que $g \leq 1$.

i) Nous avons déjà remarqué que $L(t)$ est un polynôme de degré $\leq 2g$. Dans *iv)* nous prouverons que son coefficient dominant est q^g, donc $\deg L(t) = 2g$. L'affirmation $L(t) \in \mathbb{Z}[t]$ découle de l'égalité $L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$, en comparant les coefficients.

ii) Avec la notation du corollaire 4.2.3 *b)*, nous avons

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}\left(q^g t^{2g-1}(1-t) - (1-qt)\right).$$

D'où $L(1) = h$.

iii) N'est rien d'autre que l'équation fonctionnelle de la fonction Zêta.

iv) Écrivons $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$. L'équation fonctionnelle *ii)* donne

$$L(t) = q^g\ t^{2g}\ L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \cdots + q^g a_0 t^{2g}.$$

Donc $a_{2g-i} = q^{g-i}a_i$ pour $i = 0, \ldots, g$ et (2) est prouvé. Enfin, $a_{2g} = q^g a_0 = q^g$ par (2).

v) Considérons le polynôme réciproque

$$L^{\perp}(t) := t^{2g}L(\frac{1}{t}) = a_0t^{2g} + a_1t^{2g-1} + \cdots + a_{2g}.$$

$L^{\perp}(t)$ est un polynôme unitaire à coéfficients dans $\mathbb{Z}$, ainsi ses racines sont des entiers algébriques. Posons

$$L^{\perp}(t) = \prod_{i=1}^{2g}(t - \alpha_i), \quad \text{avec} \quad \alpha_i \in \mathbb{C},$$

donc

$$L(t) = t^{2g}L^{\perp}(\frac{1}{t}) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Observons que $L(\alpha_i^{-1}) = 0$ pour $i = 1, \ldots, 2g$, et

$$\prod_{i=1}^{2g}\alpha_i = q^g.$$

En substituant $t = qu$ et en utilisant l'équation fonctionnelle *iii*) on obtient

$$\begin{aligned}
\prod_{i=1}^{2g}(t - \alpha_i) &= L^{\perp}(t) = t^{2g}L(\frac{1}{t}) \\
&= q^{2g}u^{2g}L(\frac{1}{qu}) = q^gL(u) = q^g \cdot \prod_{j=1}^{2g}(1 - \alpha_j u) \\
&= q^g \cdot \prod_{j=1}^{2g}(1 - \frac{\alpha_j}{q}t) = q^g \cdot \prod_{j=1}^{2g}\frac{\alpha_j}{q} \cdot \prod_{j=1}^{2g}(t - \frac{q}{\alpha_j}) \\
&= \prod_{j=1}^{2g}(t - \frac{q}{\alpha_j}).
\end{aligned}$$

On peut donc disposer les racines de $L^{\perp}(t)$ comme

$$\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, q^{1/2}, \ldots, q^{1/2}, -q^{1/2}, \ldots, -q^{1/2},$$

où $q^{1/2}$ se produit m fois et $-q^{1/2}$ se produit n fois. D'après l'écriture polynômiale de $L^{\perp}(t)$,

$$\alpha_1 \cdot \frac{q}{\alpha_1} \cdot \ldots \cdot \alpha_k \cdot \frac{q}{\alpha_k} \cdot (q^{1/2})^m \cdot (-q^{1/2})^n = q^g.$$

Par conséquent, n est pair. Puisque $n+m+2k = 2g$, m est également pair, et nous pouvons réorganiser $\alpha_1, \ldots, \alpha_{2g}$ tel que $\alpha_i\alpha_{g+i} = q$ soit valable pour $i = 1, \ldots, g$.

□

Démonstration du théorème 4.2.1.

a) **Rationalité :** démontrée dans le corollaire 4.2.3.

b) **Équation fonctionnelle :**
Pour $g = 0$, cela est évident d'après le corollaire 4.2.3 *a*). Pour $g \geq 1$ on écrit $Z(t) = F(t) + G(t)$ comme dans le corollaire 4.2.3 *b*). Soit W un diviseur canonique sur $\mathcal{C}$; on a

$$\begin{aligned}
F(t)(q-1) &= \sum_{0\leq \deg[D]\leq 2g-2} q^{l([D])} \cdot t^{\deg[D]} \\
&= \sum_{0\leq \deg[D]\leq 2g-2} q^{\deg[D]+1-g+l([W-D])} \cdot t^{\deg[D]} \\
&= q^{g-1}t^{2g-2} \sum_{0\leq \deg[D]\leq 2g-2} q^{\deg[D]-(2g-2)+l([W-D])} \cdot t^{\deg[D]-(2g-2)} \\
&= q^{g-1}t^{2g-2} \sum_{0\leq \deg[D]\leq 2g-2} q^{l([W-D])} \cdot t^{\deg[W-D]} \\
&= q^{g-1}t^{2g-2}(q-1)F(\frac{1}{qt}) \\
F(t) &= q^{g-1}t^{2g-2}F(\frac{1}{qt}).
\end{aligned}$$

Nous avons utilisé ce $\deg[W] = 2g-2$ et, si $[D]$ parcourt l'ensemble des classes de diviseurs avec $0 \leq \deg[D] \leq 2g-2$, $[W-D]$ aussi. Pour la fonction $G(t)$ on obtient

$$\begin{aligned}
q^{g-1}t^{2g-2}G(\frac{1}{qt}) &= \frac{h}{q-1}\left(q^g(\frac{1}{qt})^{2g-1}\frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}} \right) \\
&= \frac{h}{q-1}\left(\frac{1}{t})\frac{1}{1-q\frac{1}{t}} - \frac{q^g t^{2g-1}}{qt(1-\frac{1}{qt})} \right) = G(t).
\end{aligned}$$

Finalement on a
$Z(t) = F(t) + G(t) = q^{g-1}t^{2g-2}F(\frac{1}{qt}) + q^{g-1}t^{2g-2}G(\frac{1}{qt}) = q^{g-1}t^{2g-2}\left(F(\frac{1}{qt}) + G(\frac{1}{qt})\right) = q^{g-1}t^{2g-2}Z(\frac{1}{qt})$.

c) **Hypothèse de Riemann :** On peut trouver une preuve dans [Sti93] p.197.

□

Les conséquences des conjectures de Weil sur les cardinalités sont immédiates :

Corollaire 4.2.4. *Soit $\mathcal{C}$ une courbe de genre g définie sur un corps fini $\mathbb{F}_q$. Alors le nombre de points sur la courbe est borné par*

$$|\#\mathcal{C} - (q+1)| \leq 2g\sqrt{q}.$$

Le cardinal de la Jacobienne de $\mathcal{C}$ est quant à lui borné par

$$(\sqrt{q}-1)^{2g} \leq \#Jac(\mathcal{C}) \leq (\sqrt{q}+1)^{2g}.$$

Ces bornes signifient que le nombre de points sur une courbe de genre g est environ q avec un terme d'erreur en $\sqrt{q}$ et le cardinal de sa Jacobienne est environ q^g avec un terme d'erreur en $q^{g-\frac{1}{2}}$.

Un résultat supplémentaire permet de relier la fonction Zêta d'une courbe sur $\mathbb{F}_q$ avec la fonction Zêta de la même courbe, mais considérée sur une extension algébrique finie $\mathbb{F}_{q^r}$.

Théorème 4.2.3. *Soit $\mathcal{C}$ une courbe de genre g définie sur $\mathbb{F}_q$, et soit r un entier non nul. Notons $L(t) = \prod(1-\alpha_i t)$ le polynôme L associé à la fonction Zêta de $\mathcal{C}$. Alors la fonction Zêta $Z_r(t)$ de la courbe $\mathcal{C}$ sur $\mathbb{F}_{q^r}$ est donnée par*

$$Z_r(t) = \frac{\prod(1-\alpha_i^r t)}{(1-t)(1-q^r t)}.$$

4.2.3 Action de l'endomorphisme de Frobenius

Supposons maintenant que $\mathcal{C}$ est une courbe projective lisse absolument irréductible sur $\mathbb{F}_q$ de genre $g \geq 1$. Comme vu précédemment, l'endomorphisme de Frobenius opère sur les fonctions rationnelles sur $\mathcal{C}$, sur les points de $\mathcal{C}$ et « par suite linéaire » sur les diviseurs de $\mathcal{C}$. Il associe les diviseurs principaux aux diviseurs principaux et préserve le degré des diviseurs. Il opère donc de manière naturelle sur le groupe $\mathrm{Div}^0(\mathcal{C})$ des diviseurs de degré 0 de la courbe $\mathcal{C}$ sur $\overline{\mathbb{F}}_q$.

D'après les résultats du dernier paragraphe et du fait que le groupe de Galois de $\mathbb{F}_q/\mathbb{F}_p$ est (topologiquement) généré par ϕ_q.

Dans ce qui suit, on se fixe une courbe $\mathcal{C}$ définie sur $\mathbb{F}_q$ et une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Commençons par un rappel.

Définition 4.2.2. L'automorphisme de Frobenius, noté ϕ_q, est l'automorphisme du corps $\overline{\mathbb{F}}_q$ laissant fixe $\mathbb{F}_q$, défini par

$$\phi_q(x) = x^q.$$

Nous donnons aussi le résultat suivant déjà vu.

Lemme 4.2.4. *L'automorphisme de Frobenius sur $\overline{\mathbb{F}}_q$ s'étend en une action sur les points de la courbe $\mathcal{C}$, puis en un endomorphisme de la Jacobienne. On continue de l'appeler Frobenius et de le noter ϕ_q.*

Un élément de la Jacobienne est défini sur $\mathbb{F}_q$ si et seulement s'il l'est sous l'action de $G_{\overline{\mathbb{F}}_q/\mathbb{F}_q}$, donc si et seulement s'il est invariant sous l'action du Frobenius ϕ_q. En d'autres termes,

$$\ker(\phi_q - \mathrm{Id}) = \mathrm{Jac}(\mathcal{C})/\mathbb{F}_q,$$

et l'on en déduit que $\#\mathrm{Jac}(\mathcal{C})/\mathbb{F}_q = \chi(1)$ où $\chi(t)$ est le polynôme caractéristique du Frobenius dans l'anneau des endomorphismes qui est donné par le théorème suivant :

Théorème 4.2.4. *Le polynôme caractéristique de l'endomorphisme de Frobenius sur $Jac(\mathcal{C})$, noté $\chi(t)$ est le polynôme réciproque du polynôme $L(t)$ défini à partir de la fonction Zêta de la courbe. C'est donc un polynôme de degré $2g$ à coefficients entiers, dont les racines ont pour valeur absolue $\sqrt{q}$ et tel que*

$$\#\mathrm{Jac}(\mathcal{C})/\mathbb{F}_q = \chi(1).$$

Cas du genre 0

Pour la droite projective $\mathbb{P}^1(\mathbb{F}_q)$, le polynôme $L(t)$ est constant, égal à 1, et donc

$$\chi(t) = 1.$$

On retrouve alors le fait que la Jacobienne est le groupe trivial n'ayant qu'une seule classe, celle-ci étant définie sur $\mathbb{F}_q$. Le Frobenius est donc égal à l'identité.

Cas du genre 1

C'est le premier cas non trivial. Le polynôme $L(t)$ s'écrit

$$L(t) = 1 + a_1 t + qt^2 = (1 - \alpha_1 t)(1 - \alpha_2 t),$$

et le polynôme caractéristique du Frobenius est de la forme

$$\chi(t) = t^2 - s_1 t + q = (t - \alpha_1)(t - \alpha_2),$$

où α_1 et α_2 sont conjugués complexes, de valeur absolue $\sqrt{q}$.
On a donc l'inégalité suivante sur l'entier $s_1 = \alpha_1 + \alpha_2$ (la trace de la courbe) :

$$|s_1| \leq 2\sqrt{q}.$$

Il est expliqué plus haut que la Jacobienne d'une courbe elliptique est isomorphe à la courbe elle-même, dès que l'on a choisi un point comme élément neutre. Ainsi, si l'on a une courbe elliptique ε définie sur $\mathbb{F}_q$, l'action du Frobenius sur la courbe est décrite par le polynôme $\chi(t)$: pour tout point P défini sur une extension algébrique, on a

$$\phi_q^2(P) - s_1\phi_q(P) + qP = 0,$$

où l'addition est celle entre points de la courbe héritant de la structure de Jacobienne, et la multiplication par un entier n'est autre que l'application de l'endomorphisme de multiplication dans la Jacobienne. La notation rigoureuse serait donc :

$$\phi_q^2(P) - [s_1]\phi_q(P) + [q]P = 0_{\mathrm{Jac}(\varepsilon)}.$$

Cas du genre 2

Soit $\mathcal{C}$ une courbe de genre 2 sur $\mathbb{F}_q$. Le polynôme caractéristique de l'endomorphisme de Frobenius sur $\mathrm{Jac}(\mathcal{C})$ est de la forme

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - s_1 q t + q^2,$$

et l'hypothèse de Riemann donne les bornes suivantes pour les entiers s_1 et s_2 :

$$|s_1| \leq 4\sqrt{q} \quad \text{et} \quad |s_2| \leq 6q.$$

Ainsi le cardinal de la Jacobienne est donné par

$$q^2 - 4q^{\frac{3}{2}} + 6q - 4q^{\frac{1}{2}} + 1 \leq \ \#\mathrm{Jac}(\mathcal{C}) \ \leq q^2 + 4q^{\frac{3}{2}} + 6q + 4q^{\frac{1}{2}} + 1.$$

Là encore, le polynôme caractéristique du Frobenius traduit son comportement sur les éléments de la Jacobienne : pour tout diviseur réduit D, on a

$$\phi_q^4(D) - [s_1]\phi_q^3(D) + [s_2]\phi_q^2(D) - [s_1 q]\phi_q^4(D) + q^2[D] = 0_{\mathrm{Jac}(\mathcal{C})}.$$

4.2.4 Applications en cryptographie

Dans cette section, nous commençons d'abord par définir une courbe hyperelliptique, ensuite nous énonçons les problème du logarithme discret, avant de discuter des critères de sélection d'une courbe hyperelliptique en cryptographie. le sujet est largement discuté dans l'appendice de [Kob98] dû à Alfred J. Menezes, Yi-Hong Wu et Robert J. Zuccherato.

Définition 4.2.3 (Courbe hyperelliptique). Une courbe hyperelliptique $\mathcal{C}$ de genre g sur $\mathbf{K}$ ($g \geq 2$) est une courbe projective lisse dont le corps des fonctions est isomorphes au corps des fonctions d'une courbe projective définie par une équation de la forme

$$\mathcal{C} : y^2 + h(x)y = f(x),$$

où $h \in \mathbf{K}[X]$ est un polynôme de degré au plus g, $f \in \mathbf{K}[X]$ est un polynôme unitaire de degré $2g+1$, et $\mathcal{C}$ est sans points singuliers dans $\overline{\mathbf{K}} \times \overline{\mathbf{K}}$.

Soit G un groupe cyclique d'ordre n engendré par $g \in G$, i.e. :

$$G = \{g^0, g, \ldots, g^{n-1}\}$$

et $g^n = g^0 = 1$, le neutre de G. On suppose également que les opérations dans G se font rapidement (comme une multiplication d'entiers). Une situation typique est de considérer le groupe $G = (\mathbb{Z}/p\mathbb{Z})^\times$ des éléments inversibles modulo p où p est un nombre premier.

Définition 4.2.4 (Problème du logarithme discret dans G).
Soit G un groupe cyclique d'ordre n engendré par g. Le problème du logarithme discret dans G en base g est le problème, étant donné $y \in G$, de trouver $l \in \mathbb{Z}$ tel que $g^l = y$. On note

$$l = \log_g(y),$$

l'entier l est bien sûr défini modulo n.

Le protocole de base utilisant le problème du logarithme discret est l'échange de clé de Diffie-Hellman. Il est à la base de nombreux cryptosystèmes.

Les premiers groupes proposés pour usage cryptographique furent les groupes $(\mathbb{Z}/p\mathbb{Z})^\times$ où p est un grand nombre premier, puis les groupes de classes de corps quadratiques. Ensuite, Miller et Koblitz montrèrent que l'on pouvait aussi utiliser les courbes elliptiques définies sur un corps fini. Plus généralement, pour toute courbe $\mathcal{C}$ définie sur un corps fini, on peut construire un groupe abélien fini (la Jacobienne de $\mathcal{C}$), avec lequel il est possible de construire des protocoles cryptographiques.

Pour implémenter un Cryptosystème à base du problème du logarithme discret utilisant des courbes hyperelliptiques, parmi les propriétés souhaitables pour la courbe sélectionnée et son corps (fini) de définition (ou une extension) on a :

1. L'arithmétique dans le corps fini sous-jacent $\mathbf{K}$ doit être efficace pour l'implémentation ; un corps fini de caractéristique 2 semble être le choix le plus attractif.
2. L'ordre de la jacobienne $\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ de $\mathcal{C}$, noté $\#\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$, doit être divisible par un grand nombre premier. Compte tenu de l'état actuel de la technologie informatique, une exigence de sécurité est que $\#\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ soit divisible par un nombre premier r d'au moins 45 chiffres. En plus, pour éviter l'attaque de réduction de Frey et Rück qui réduit le problème du logarithme en $\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ au problème du logarithme dans une extension du corps $\mathbf{K} = \mathbb{F}_q$, r ne doit pas diviser $q^k - 1$ pour tous k pour lesquels le problème du logarithme discret dans $\mathbb{F}_{q^k}$ est faisable ($1 \leq k \leq 2000/(\log_2 q)$ suffit).

Une technique pour sélectionner une courbe hyperelliptique et calculer $\#\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ est décrite ci-dessous. Soit $\mathrm{Jac}_{\mathbf{K}}(\mathcal{C})$ la jacobienne de la courbe hyperelliptique $\mathcal{C}$ définie sur $\mathbf{K} = \mathbb{F}_q$, et donnée par l'équation $v^2 + h(u)v = f(u)$. Supposons que $\mathbb{F}_{q^n}$ désigne l'extension de degré n de $\mathbb{F}_q$, et que N_n désigne l'ordre du groupe abélien (fini) $\mathrm{Jac}_{\mathbb{F}_{q^n}}(\mathcal{C})$. Notons M_n le nombre de points $\mathbb{F}_{q^n}$-rationnels sur $\mathcal{C}$. On associe à $\mathcal{C}$ sa fonction zêta

$$Z(t) = \exp\left(\sum_{r \geq 1} M_r \frac{t^r}{r}\right),$$

où $M_r = \#\mathcal{C}(\mathbb{F}_{q^r})$. On a les faits suivants :

(*i*) $Z(t) \in \mathbb{Z}(t)$, et (d'après 3. du théorème sur les conjectures de Weil)

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}, \tag{5.1}$$

avec

$$L(t) = 1 + a_1 t + \ldots + a_g t^g + q a_{g-1} t^{g+1} + q^2 a_{g-2} t^{g+2} + \cdots + q^{g-1} a_1 t^{2g-1} + q^g t^{2g}. \tag{5.2}$$

(*ii*) $L(t)$ se factorise en

$$L(t) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha_i} t), \tag{5.3}$$

où chaque α_i est un nombre complexe de valeur absolue $\sqrt{q}$, et $\overline{\alpha_i}$ désigne le complexe conjugué de α_i.

(*iii*) $N_n = \#\mathrm{Jac}_{\mathbb{F}_{q^n}}(\mathcal{C})$ satisfait

$$N_n = L(1) = \prod_{i=1}^{g} |1 - \alpha_i^n|^2, \tag{5.4}$$

où $|\cdot|$ désigne le module d'un nombre complexe.

Pour calculer N_n, il suffit donc de (*i*) pour déterminer les coefficients a_1, a_2, …, a_g de $L(t)$, déterminant ainsi $L(t)$; d'après (*ii*) la forme factorisée de $L(t)$ permet de déterminer les α_i ; enfin, (*iii*) nous permet de calculer N_n via l'équation (5.4). Maintenant, l'équation (5.1) donne

$$L(t) = (1-t)(1-qt)Z(t).$$

Appliquons la fonction ln de chaque côté de l'égalité puis dérivons le résultat en t, on obtient

$$\frac{L'(t)}{L(t)} = \sum_{r \geq 0} (M_{r+1} - 1 - q^{r+1}) t^r.$$

En égalisant les coefficients de t^0, t^1, …, t^{g-1} des deux côtés, nous voyons que les g premières valeurs M_1, M_2, M_1, …, M_g suffisent pour déterminer les coefficients a_1, a_2, …, a_g, et par conséquent N_n.

La procédure suivante résume la technique de calcul de N_n pour $g = 2$.

1. Par une recherche exhaustive, on calcule M_1 et M_2.
2. Les coefficients de $Z(t)$ sont donnés par $a_1 = M_1 - 1 - q$ et $a_2 = (M_2 - 1 - q^2 + a_1^2)/2$.
3. On résout l'équation quadratique $X^2 + a_1 X + (a_2 - 2q) = 0$, pour obtenir deux solutions γ_1 et γ_2.
4. On résout $X^2 - \gamma_1 X + q = 0$ pour obtenir une solution α_1 et résout $X^2 - \gamma_2 X + q = 0$ pour obtenir une solution α_2.
5. Alors $N_n = |1 - \alpha_1^n|^2 \cdot |1 - \alpha_2^n|^2$.

Les bornes suivantes de l'ordre N_n de la jacobienne sont une conséquence immédiate de (*iii*) vu précédemment :

$$(q^{n/2} - 1)^{2g} \leq N_n \leq (q^{n/2} + 1)^{2g}.$$

Par conséquent, $N_n \approx q^{ng}$.

Exemple 4.2.2 (Sélection d'une courbe hyperelliptique)**.** Considérons la courbe hyperelliptique $\mathcal{C}$ suivante de genre 2 définie sur $\mathbb{F}_2$:

$$\mathcal{C} : y^2 + y = x^5 + x^3 + x.$$

Par une recherche exhaustive, on trouve $M_1 = 3$ et $M_2 = 9$; d'où $a_1 = 0$ et $a_2 = 2$. Les solutions de $X^2 - 2 = 0$ sont $\gamma_1 = \sqrt{2}$ et $\gamma_2 = -\sqrt{2}$. La résolution de $X^2 - \sqrt{2}X + 2 = 0$ donne $\alpha_1 = (\sqrt{2} + i\sqrt{6})/2$; la résolution de $X^2 + \sqrt{2}X + 2 = 0$ donne $\alpha_2 = (-\sqrt{2} + i\sqrt{6})/2$. Donc

$$N_n = |1 - \alpha_1^n|^2 \cdot |1 - \alpha_2^n|^2 = \begin{cases} 2^{2n} + 2^n + 1, & \text{si } n \equiv 1, 5 \pmod 6, \\ (2^n + 2^{n/2} + 1)^2, & \text{si } n \equiv 2, 4 \pmod 6, \\ (2^n - 1)^2, & \text{si } n \equiv 3 \pmod 6, \\ (2^{n/2} - 1)^4, & \text{si } n \equiv 0 \pmod 6. \end{cases}$$

Pour $n = 101$,

$$N_{101} = 642775217703596110216784836936718571128926843393416474761625 7,$$

et sa factorisation en éléments premiers est

$$N_{101} = 7 \cdot 607 \cdot 151276822241373525586440300526410583932437477852063185399 3.$$

Par conséquent, N_{101} est divisible par un nombre premier de 58 chiffres r. Cependant, puisque r divise $(2^{101})^3 - 1$, l'attaque de Frey-Rück nous dit que $\mathcal{C}$ n'offre pas plus de sécurité qu'un système à logarithme discret dans $\mathbb{F}_{2^{303}}$. La courbe $\mathcal{C}$ n'est donc pas adaptée aux applications cryptographiques.

Conclusion

Dans ce mémoire, nous avons présenté les conjectures de Weil pour les courbes algébriques et les variétés abéliennes qui s'en déduisent, la fonction zêta jouant un rôle central. Cela nous a permis de passer en revue plusieurs notions et objets issus de la théorie des corps, de la théorie de Galois et de la géométrie algébrique. Nous avons rappelé ces notions en détaillant quelques illustrations. Nous avons aussi présenté les objets et leurs propriétés. Nous avons également montré comment on peut utiliser les conjectures de Weil pour déterminer le nombre de points rationnels sur une courbe algébrique et sur sa variété jacobienne. En guise d'application, nous avons décrit l'impact que cela a dans le choix d'une courbe hyperelliptique pour la construction de cryptosystèmes sécurisés. Au cours de ce travail, nous avons bien compris la structure de variété abélienne que l'on a sur la variété jacobienne d'une courbe projective. Un problème intéressant serait de chercher à, étant donnée une courbe projective $\mathcal{C}$ définie sur un corps fini $\mathbb{F}_{p^d}$, déterminer le groupe de points rationnels dans les sous-groupes de torsion de la jacobienne $J_{\mathcal{C}}$ de $\mathcal{C}$. C'est une question qui avait déjà été abordée par Jean-Marc Couveignes dans un article publié en 2008, pour la ℓ^s-torsion de $J_{\mathcal{C}}$ où ℓ est un nombre premier différent de p et s un entier naturel arbitraire. Cet article de Couveignes sera un des points de départ pour la suite de nos travaux.

Bibliographie

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Ful69] William Fulton. *Algebraic curves : An introduction to algebraic geometry*. Benjamin, 1969.

[Gau00] Pierrick Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*. PhD thesis, ÉCOLE POLYTECHNIQUE, 2000.

[Kob98] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[Lan83] Serge Lang. *Abelian varieties*. Springer-Verlag, New York, 1983.

[Lan02] Serge Lang. *Algebra, Graduate Texts in Mathematics, vol. 211*. Springer-Verlag, Berlin, third edition, 2002.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields, second edition*. Cambridge University Press,, 1997.

[Mag10] Nöel-Arnaud Maguis. Rédigez des documents de qualités avec latex. Disponible sur www.siteduzero.com, 2010.

[Mum74] David Mumford. *Abelian Varieties, second edition*. Oxford University Press, New York, 1974.

[Per01] Daniel Perrin. *Géométrie algébrique, Une introduction*. Savoirs actuels, EDP Sciences/CNRS EDITIONS, 2001.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres*. HERMANN, ÉDITEURS DES SCIENCES ET DES ARTS, Deuxième édition revue et corrigée, 1971.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106*. Springer-Verlag, Berlin, 1986.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes, Graduate Texts in Mathematics, vol. 254*. Springer-Verlag, Berlin, Second edition, 1993.