Institut de Mathématiques de Marseille

École doctorale en Mathématiques et Informatique de Marseille
Discipline : Mathématiques

THÈSE DE DOCTORAT

Présentée par

Annamaria Iezzi

Pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ D'AIX-MARSEILLE

Nombre de points rationnels des courbes singulières sur les corps finis

---

Dirigée par Yves AUBRY
Rapportée par Marc HINDRY et James W. P. HIRSCHFELD

Soutenue publiquement le mercredi 6 juillet 2016 devant le jury composé de :

Yves AUBRY	Université de Toulon	Directeur de thèse
Massimo GIULIETTI	Università degli Studi di Perugia	Examinateur
Marc HINDRY	Université Paris Diderot	Rapporteur
James W. P. HIRSCHFELD	University of Sussex	Rapporteur
David KOHEL	Aix-Marseille Université	Examinateur
Marc PERRET	Université de Toulouse II	Examinateur
Serge VLADUTS	Aix-Marseille Université	Examinateur

Merci !

Pendant des années j'ai rêvé d'en être là, devant ce chapitre plus communément intitulé *remerciements*. L'émotion est grande et la tâche difficile. Résumer « trois ans » en ces quelques pages est finalement le plus grand défi de cette thèse.

Bien consciente de que le niveau de ces remerciements n'atteindra à aucun moment la perfection de ceux de la thèse de Virgile [1], je souhaite, par eux, adresser ma plus grande gratitude à toutes les personnes qui m'ont accompagnée dans ce singulier parcours. Conformément au caractère international de cette aventure, et en tant que responsable autonommée du *Café des Langues Luminy*, j'adapterai, lorsque possible, la langue de chacune de ces lignes à leur(s) destinataire(s). J'ai évidemment glissé quelques typos par-ci, par-là, histoire de donner à Pierre-O la possibilité de se venger sur mon français. Bref, comme Paolo le dirait, c'est parti !

Pour une thèse il faut bien un directeur, et c'est à toi, Yves, que j'adresse mon premier grand merci. Depuis le début, tu m'as guidée dans les méandres de la recherche, toujours avec patience, humour, énergie et optimisme. Tu as su me motiver et me donner confiance lorsque je me sentais le plus égarée. Merci pour tes conseils, ta disponibilité, ta ponctualité et aussi la liberté que tu m'as laissée. Ton approche aux mathématiques, rigoureuse, enthousiaste et pleine d'anecdotes, sera toujours pour moi une source d'inspiration. Je suis très contente d'avoir partagé ce parcours avec un directeur cool comme toi, et plus que ça : un ami.

My most sincere thanks to Marc Hindry and James Hirschfeld for having accepted the heavy task of reviewing this manuscript. I'm very grateful for their interest in my work, their careful read-through as well as for their precious remarks. Mes remerciements vont également à Massimo Giulietti, David Kohel, Marc Perret et Serge Vladuts pour me faire l'honneur d'être membres de mon jury.

Une rédaction en français par une italienne nécessite de plusieurs relectures et relecteurs. Merci alors à mon équipe sélectionnée de l'Académie française, spécialité mathématiques : Joël Cohen, Guillaume Geoffroy, Pierre-Olivier Goffard et Marc Munsch. Votre minutieux travail (dont les effets seront visibles lorsque l'on retrouvera des fonctions zêta dans l'actuariat ou dans la logique) a été indispensable à l'amélioration de la qualité et du swag de ce texte. Aussi je n'oublierai pas la ponctualité et la rapidité avec laquelle vous avez répondu à toutes mes nombreuses et variées questions (sur les mathématiques, le français, le latex, etc.). Vous pourrez évidemment compter sur moi pour vos prochaines rédactions en italien.

1. « Mes remerciements, c'est génial ! »

Mais une thèse va bien au delà d'un manuscrit et d'une soutenance. Et c'est là que la petite larme d'émotion est prête à sortir...

La primera persona a agradecer eres tú, Dani, porque sin ti esta experiencia nunca habría empezado.

Je remercie toute mon équipe ATI [2] pour l'accueil chaleureuse qu'elle m'a toujours réservée. Une pensée particulière à Stéphane B., esprit combattant et déterminé, mais qui n'a jamais accepté la défaite de la France lors de la rencontre internationale YACC 2014 (Yves Aubry Conference on Cryptography) ; à Alexis, unique professeur à avoir été aussi mon élève, en italien ; à Christophe, dont j'admire, entre autres, l'énorme dynamisme et l'esprit organisationnel (Antalya, quel bon souvenir !) ; à David, Gilles, François et Serge, pour leur gentillesse et leur soutien constants. Un remerciement spécial à Stéphane L., compagnie fidèle pendant mes week-ends et nuits passés au laboratoire, surtout en fin de rédaction ; je le remercie également pour toutes ses blagues, sur lesquelles j'ai pu m'entraîner pendant les années et que, enfin, je trouve drôles.

Je remercie l'Institut de Mathématiques de Marseille, et en particulier le site sud, pour m'avoir donné des excellentes conditions de travail et pour avoir supporté ma présence assidue et parfois bruyante au laboratoire. Beaucoup de collègues sont devenus pour moi plus que ça, et je les remercie pour leur amitié, les bavardages dans les couloirs et les pauses café. Dans ce cadre, je tiens en particulier à exprimer ma reconnaissance à Yves Lafont, pour son encouragement constant aux doctorants et promotion de leurs activités, et à Tomasz Miernowski, pour tous les conseils qu'il m'a dispensés en matière d'enseignement et de pédagogie. Aussi je n'oublie pas la disponibilité, la compétence et la bonne humeur du personnel administratif et informatique : merci à Aurelia, Corinne, Éric, Jean-Bruno et Jessica.

Je suis extrêmement reconnaissante à l'École Doctorale 184. Merci à Nadia Creignou, Thierry Gallouet et Sonia Asseum pour la confiance qu'ils m'ont toujours accordée et pour tout le soin et toute l'attention qu'ils portent aux doctorants.

Merci également à l'IREM et au CIRM, et à l'ensemble du personnel qui y travaille. C'est une chance de vous avoir à côté et c'est toujours un plaisir de passer vous voir, que ce soit pour un livre de maths, ou un stage hippocampe.

Sinon, pour le reste, l'ambiance au labo, pendant ces années, a toujours été plate et monotone, en raison des doctorants renfermés et des rares infiltrés qui ont mis les pieds dans mon bureau [3] : Marc « Je suis trop fort à la belote » et ses vaines tentatives d'apprendre de l'italien « Sei una busta ! », « Non ne posso più ! » ; Virgile, l'unique médecin chinois avec des compétences en mathématiques, et son humour rarement drôle ; Joël, le plus grand fan de π de l'histoire (après Archimède) et magicien à ses heures perdues « je peux te faire un tour de cartes ? » ; Émilie, mon amie commère « Viens, je dois te raconter un truc », à remercier avec π points exclamatifs ! ! !. ; Pierre-O, infatigable mangeur de mes pâtes (même celles passées ou notées 5) et sa brusque franchise « tu n'as rien d'autre à faire là ? » ; Paolo1, filosofo, scenografo, logico, airbienbista, dall'enorme gusto estetico « J'ai changé la couleur de l'année » ; Irene, mi mozzarella preferida, pero a renegar cada vez que me pregunte « ¿Tienes leche por el café ? » ; Joooordi, el catalá de Marsella « u, dos, tres, quatre,..., i quinze ! Oeoeo... », professor de guitarra de un estudiant

2. Arithmétique et Théorie de l'Information, pour les moins habitués aux acronymes.
3. avec des conséquences irréversibles sur ma thèse.

peresós ; Jb « Salut Anna, t'es pas trop fatiguée ? » ; Marc, le capitain d'un foot qui s'est arrêté après son départ ; Eugenia, la fantasista delle espressioni romane ; Lionel, acteur studio et « ça vous dit pas un sushi ? » ; Florian, le laveur des vitres du labo ; Stéphanie « Tu mets 6 œux dans le tiramisu ? ? ? » ; Florent « oooh quel dommaaage ! » ; Pascale ; Yih-Dar « ça va bien la chemise aujourd'hui ? » ; Marcelo, Jaqui, as capirinhas, les frescurés i « Sondaaaage ! » ; Fabio e le melanzane di Chez Étienne ; Francesca (Ludovica per gli amici), la pittrice incompresa ; Matteo, la mucca, la gallina e *le théorème de Riemann Rock !* ; Sarah, the superwoman ; Tammam ; Paolo2 "La vita è bella" ; Diogo, o Português inglês com acento sexy em francês i ao qual este capítulo está dedicado ; Alejandro « il y a café des langues aujourd'hui ? » ; Lamia, toujours prête à défourner une tarte pour π ; Andrea, il re delle gif su Facebook ; Serena e la renna Avogadro ; Marianna la giocoliera ; Sarah, la squatter du CIRM. Sans oublier mes co-bureaux, qui m'ont convaincue qu'il est possible de partager un bureau à 5 tout en travaillant concentrés : Elena e l'ossimoro dei salsicciotti e delle operazioni bikini ; Alberto y la paella que esperamos todavía (y su infinita patiencia de cada mañana) ; Firas « demain je vais faire un montage vidéo » ; Guillaume, l'homme de la forêt qui hypnotise les sangliers avec son ukulele.

Merci à vous tous, et à ceux qui j'ai oubliés, pour les indénombrables moments que l'on a partagés ensemble : merci pour[4] les cours d'argot français et de belote ; pour les soirées interminables chez Joël, le Barberousse, les silent discos, et les tonneaux ; pour les machines à pâtes au labo et les petits déj, bizarrement passés, avec l'avancée de la thèse, de 10h à 8h30, ce qui a comporté une grosse baisse de la qualité (pâtes à tartiner maison, toasts et jus de fruits mixés sur place remplacés par des tristes croissants du Crous) ; merci pour les journées au labo assorties ; pour les journées de π[5], les pie meetings (ou pie eating ?), les tartes et les comédies musicales ; pour les cafés, les pastis, les apéros porto cachés et les semibières ; pour le loft de Barcelone, le grand appart et les chats d'Amsterdam, la villa de Molliets, Madame Moustache de Bruxelles, Roma, Lorient, Teramo beach et le Salento ; pour les foot, les tennis, les escalades, les randonnées et les essaies infructueux de surf aux pays bretons ; merci pour m'avoir suivie dans mes projets, sans aucune pression de ma part (« Tu veux pas nous aider ? »), pour m'avoir partagé les vôtres et pour en avoir construits ensemble ; enfin, plus important, merci infiniment pour la « motivation ! ! » que vous m'avez transmise sans faille lorsque j'en avais le plus besoin.

Et quand le ton se fait plus romantique... J'adresse des remerciements spéciaux : à Marc, pour toute la patience envers moi dont tu as fait preuve et pour la gentillesse envers tout le monde qui te caractérise ; à Joël, parce que tu as toujours mis les nécessités des autres devant les tiennes, sans rien prétendre en échange ; à Émilie (bon anniversaire ! !), car j'ai beaucoup souffert de ton absence au labo et ton enthousiasme m'a beaucoup manqué ; a Paolo, perché con il tuo temperamento e la tua saggezza, hai sempre avuto una soluzione pronta e razionale ai miei problemi e alle mie ansie ; à Pierre-O, pour ton énorme générosité et ton grand sens d'amitié cachés aux yeux de ceux qui ne te connaissent pas ; a Irene y Jordi, por ser dos puntos de referencia desde mis primeros días en Luminy ; à Guillaume, car ton arrivée a rapporté un gros dynamisme dans notre groupe, et parce que ton irrépressible disponibilité aux demandes des gens est juste enviable.

Une pensée particulière va aussi au CIELL, le Centre des Langues de Luminy, et à tous les gens que j'ai rencontrés dans ses murs. Merci à Cathy et Tom, respectivement maman et père des

4. liste non exhaustive.
5. grâce auxquelles maintenant je retiens 9 décimales de π.

Erasmus, pour avoir été les premiers à m'accueillir à Marseille (après le Crous, évidemment), et pour l'avoir fait avec tant d'enthousiasme ; merci pour les dîners internationaux et les karaokes jusqu'à pas d'heures « Roooooxane ! » ; merci à Daveen et Mathias et aux autres membres de ESN Marseille pour continuer à s'occuper des étudiants internationaux avec tant de passion. Merci au Café des Langues Luminy, à ses animateurs et ses participants, pour m'avoir donné chaque jour l'occasion de partager un bon café tout en m'amusant et en apprenant. Cela a été aussi l'occasion de faire de jolies rencontres sur le campus, et je ne peux en citer que quelques-uns : Alice, Ante, Antoine, Ariana, Elena, Jaime, Jean-Michel, Julie, Marianna, Milton, Mónica, Pascal, etc.

Merci également aux doctorants du site nord, dont, pour certains, notre relation a été uniquement limitée par des questions géographiques ; merci à l'équipe des Treize Minutes Jeunes Chercheurs, qui m'a confirmé l'importance de regarder aussi aux domaines au-delà des mathématiques ; merci à mes étudiants, les bons et les moins bons, pour m'apprendre des choses chaque jour, et pour faire en sorte que le défi de les passionner avec les maths reste toujours parmi mes priorités ; grazie a tutti quei professori che per primi mi hanno comunicato quest'entusiasmo per la matematica ; merci aux 5 générations Erasmus que j'ai vues débarquer à Luminy et, souvent, en repartir ; merci à l'ennuyante bureaucratie française et à tous les gestionnaires et secrétaires qui m'ont donné un coup de main pour la vaincre ; merci à l'arracheur des affiches pour nous avoir fait plus de pub de ce qu'il s'imaginait ; merci à Marseille, et plus particulièrement à Luminy, pour avoir été le magnifique cadre de cette expérience ; merci à π ; merci à vous tous qui êtes là aujourd'hui !

E infine tocca a voi, cari amici e parenti italiani...

Ringrazio innanzitutto la mia fedele e amata combriccola di amici di Teramo [6], per esserci sempre stata e per aver dimostrato, negli anni, che le migliaia di chilometri che ci separano sono facilmente abbattibili, soprattutto quando si dispone dei voucher EasyJet (grazie Felice!) : grazie in particolare ad Halenya, Silvia, Felice, Ilaria, Giada, Zek, Graziana e Andrea e alle svariate città che ci hanno ospitato (Lione, Stoccolma, Marbella, Liverpool, Marsiglia, Milano e prossimamente Berlino). Grazie a Graziana per non essere mai mancata nei momenti importanti e per il tuo aiuto incondizionato nei confronti di tutti e comunque. Grazie ad Andrea perché, nonostante i frequenti bisticci, ci vogliamo tanto bene.

Un grazie di cuore alla mia famiglia, per aver accettato (serenamente?!?) la mia lontananza in tutti questi anni [7] e per essere stati, al tempo stesso, sempre puntualmente presenti. Grazie a zio Marcello per avermi trasmesso, fin da piccola, la passione per la matematica. Grazie al nonno per il suo entusiasmo ad ogni mio ritorno, nonostante non abbia ancora ben capito cosa ci faccia in Francia "'Nnamarí, duva stí? E che stí a fá?". Grazie alla mamma per non aver mai posto la fatidica domanda: "Allora, come va con la tesi?" e per non essersi mai interessata al mio tema di ricerca, ma per aver in cambio assistito a tutte le journée de π.

E infine, grazie a te, per essere con me anche quando non ci sei, per il tuo amore che non svanirà mai...

6. Teramo - Petite ville d'environ 50000 habitants située dans la région des Abruzzes, au centre de l'Italie, côté Adriatique. Elle est notamment connue à l'international pour sa production, pendant le mois d'août, de tonnes de sauces tomates (ou dans un langage plus soutenu des *buttije di pummadore*).

7. però non che da domani torni a casa, eh!

... al mio papà

Table des matières

Introduction

Le problème de déterminer l'ensemble des solutions d'un système d'équations polynomiales dans un « certain domaine de rationalité » trouve ses racines les plus anciennes en Grèce antique, à une période indéterminée entre le I^{er} et le IV^{e} siècle av. J.-C. À cette époque, le mathématicien Diophante d'Alexandrie se dédie à la recherche de solutions rationnelles positives d'équations à coefficients entiers, et recueille 130 de ces problèmes, ainsi que leurs résolutions, dans son ouvrage *Arithmetica*.

Dans sa forme la plus simple, une *équation diophantienne* est ainsi une équation polynomiale à deux variables à coefficients entiers

$$f(x, y) = 0,$$

dont on recherche les solutions rationnelles (x, y). Dans le langage géométrique, probablement inconnu de Diophante, cela se traduit par la recherche des *points rationnels* appartenant à la courbe algébrique plane correspondante. Cette recherche devient donc un problème de *géométrie arithmétique*.

En effet, comme André Weil le dit dans l'introduction de sa thèse (voir [51]), l'*arithmétique sur une courbe* définie sur un « domaine de rationalité k », consiste en l'étude des « propriétés qui sont invariantes par rapport aux transformations birationnelles à coefficients rationnels », et effectivement, d'après les résultats d'Hilbert et Hurwitz (voir [24]), le problème de la recherche des points rationnels rentre dans ce cadre. Ainsi, l'*invariant* qui gouverne les questions sur les points rationnels est le *genre*, et non pas le degré de la courbe.

Historiquement, la résolution des équations diophantiennes sur les rationnels a amené les mathématiciens à s'intéresser au problème, d'apparence plus simple, d'étudier les solutions modulo un nombre premier. Bien souvent, cela permet de déterminer l'existence, ou non, de solutions rationnelles. Progressivement, l'étude des points rationnels des courbes modulo un nombre premier, et plus généralement sur les corps finis, est devenue un sujet d'étude en lui même.

Si $k = \mathbb{F}_q$ est un corps fini, toute courbe algébrique définie sur $\mathbb{F}_q$ a un nombre fini de points rationnels, et il est donc possible, au pire par « force brute », de tous les déterminer. Cependant, lorsque q devient grand, ce problème est hors d'atteinte, et on peut s'intéresser au problème plus simple de compter le nombre de solutions, plutôt que de les calculer explicitement. Dans ce sens, des études ont été entreprises pour donner une estimation précise du nombre maximum de points rationnels d'une courbe algébrique définie sur un corps fini et d'un genre donné.

Concernant celles-ci, les résultats fondamentaux, avec comme acteurs principaux Hasse (voir [22], [23]), Weil (voir [52]) et Serre (voir [41]), sont tous formulés pour des courbes algébriques,

projectives, absolument irréductibles et lisses, et peuvent être grossièrement résumés dans l'inégalité

$$N_q(g) \leq q + 1 + g[2\sqrt{q}],$$

où $N_q(g)$ désigne le nombre maximum de points rationnels d'une courbe algébrique, projective, absolument irréductible et lisse de genre g. Tous ces résultats reposent sur l'étude des zéros d'une fonction génératrice encodant le nombre de points rationnels de la courbe sur les extensions du corps de base, introduite par Artin dans les années 20 (thèse de doctorat, 1924), et appelée la *fonction zêta* de la courbe. On peut voir cette fonction zêta comme un analogue pour les courbes de la fonction zêta de Riemann classique. Dans ce cadre, Weil a démontré , dans [52], ce que l'on appelle communément l'*hypothèse de Riemann pour les courbes sur les corps finis*, et qui est le point crucial de l'inégalité précédemment citée.

Nous allons nous intéresser dans cette thèse au cas plus général du nombre de points d'une courbe singulière sur un corps fini. Dans la suite de l'introduction, le mot *courbe* désignera une courbe algébrique, projective, absolument irréductible.

Les résultats précédemment évoqués pour les courbes lisses sont utiles pour l'étude du nombre de points rationnels d'une courbe *singulière*, étant donné que toute courbe définie sur $\mathbb{F}_q$ est birationnellement équivalente à une courbe lisse sur $\mathbb{F}_q$, à savoir sa *normalisée*. Néanmoins, il faut remarquer qu'un point singulier peut correspondre à plusieurs points dans la normalisée, et que donc, en particulier, le nombre de points rationnels n'est pas en général le même sur les deux courbes.

La borne d'Hasse-Weil-Serre peut alors être étendue au cas d'une courbe singulière, en faisant intervenir un nouvel invariant appelé *genre arithmétique*. Aubry et Perret ont en effet montré dans [6] que, si X est une courbe définie sur $\mathbb{F}_q$, de genre géométrique g et de genre arithmétique π, alors

$$\sharp X(\mathbb{F}_q) \leq (q+1) + g[2\sqrt{q}] + \pi - g, \tag{1}$$

ou, ce qui est plus fort,

$$\sharp X(\mathbb{F}_q) \leq N_q(g) + \pi - g. \tag{2}$$

Ces bornes sont le point de départ de cette thèse, dans laquelle on s'intéresse à des questions concernant le nombre maximum de points rationnels d'une courbe singulière définie sur un corps fini.

À cet effet, pour q une puissance d'un nombre premier, g et π deux entiers positifs tels que $\pi \geq g$, nous introduisons la quantité

$$N_q(g, \pi)$$

définie, par analogie avec le cas lisse, comme le nombre maximum de points rationnels d'une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π. De plus, nous appelons *maximales* les courbes qui atteignent la borne (1) et *δ-optimales* les courbes qui atteignent la borne (2).

Le problème de déterminer $N_q(g, \pi)$ nous amène donc à construire des courbes singulières de genres et corps de base donnés, possédant un grand nombre de points rationnels. Pour ce faire,

en suivant les idées développées par Rosenlicht dans [36], et reprises par Serre dans [39, Ch. IV], nous partons d'une courbe lisse X, pour construire une courbe à singularités X', de telle sorte que X soit la normalisée de X', et que les singularités « construites » soient rationnelles sur le corps de base, et de degré de singularité prescrit (voir théorème 3.1.3).

En remarquant que le degré de singularité d'un point singulier dépend, entre autres, du degré des points dans sa fibre via la normalisation, cette construction prend la forme d'une sorte de « bataille » entre nombre de points rationnels et genre arithmétique (voir théorème 3.2.1), et on s'aperçoit que ce sont les points de degré 2 de la courbe lisse de départ qui font gagner la « partie » !

Nous en déduisons le résultat suivant (voir théorème 4.3.1), qui caractérise l'existence d'une courbe δ-optimale définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π :

$$N_q(g,\pi) = N_q(g) + \pi - g \iff g \leq \pi \leq g + B_2(\mathcal{X}_q(g)) \tag{3}$$

où $\mathcal{X}_q(g)$ désigne l'ensemble des courbes optimales lisses définies sur $\mathbb{F}_q$ de genre g (i.e. avec $N_q(g)$ points rationnels), et $B_2(\mathcal{X}_q(g))$ est le nombre maximum de points de degré 2 d'une courbe de $\mathcal{X}_q(g)$.

La quantité $B_2(\mathcal{X}_q(g))$ est explicite lorsque g est égal à 0 ou 1 et pour tous les g tels que $N_q(g) = q + 1 + g\lfloor 2\sqrt{q} \rfloor$. Dans les autres cas, en utilisant l'approche euclidienne présentée par Hallouin et Perret dans [20], nous en déterminons des bornes inférieures et supérieures. Bien que ces résultats sur le nombre de points de degré 2 d'une courbe lisse aient un intérêt propre, nous les utilisons pour préciser l'équivalence (3), et pour déterminer quelques valeurs exactes de $N_q(g,\pi)$, pour des valeurs spécifiques de q, de g et de π (voir proposition 4.5.1).

La thèse se termine par l'étude des propriétés et du spectre de genres des courbes maximales (voir théorème 4.6.4), et par un résultat sur les revêtements de courbes singulières (voir théorème 4.7.2).

Notre étude des courbes singulières sur les corps finis est également motivée par leurs nombreuses occurrences dans divers problèmes mathématiques. Un exemple nous vient de la théorie des codes avec la construction géométrique de codes correcteurs d'erreurs définis par évaluation de points sur des variétés algébriques (voir [31]). La détermination des paramètres fondamentaux de ces codes nécessite l'étude de sections hyperplanes ou plus généralement de sections de variétés algébriques, qui donnent bien souvent des variétés singulières.

Un autre exemple provient de la théorie des fonctions booléennes pour lesquelles la propriété Almost Perfect Nonlinear (APN) est caractérisée par l'inclusion des points rationnels d'un certain ensemble algébrique (qui est une courbe singulière ou une surface singulière) dans une réunion d'hyperplans (voir [9]).

Ce travail a été réalisé grâce à la participation du LabEx Archimède (ANR-11-LABX- 0033) et de la fondation A*MIDEX (ANR-11-IDEX-0001-02), financés par le programme « Investissements d'Avenir » mené par l'ANR.

Plan de la thèse

Cette thèse est organisée de la manière suivante.

Le Chapitre 1 est dédié à des rappels sur les objets et les notions de base, ainsi que les principaux résultats qui interviennent dans l'étude d'une courbe algébrique singulière définie sur un corps fini.

Dans le Chapitre 2 on passe en revue, dans le cas lisse, puis singulier, les résultats fondamentaux concernant les bornes sur le nombre de points rationnels d'une courbe définie sur un corps fini.

On présente, dans le Chapitre 3, une construction de courbes singulières de genres et corps de base donnés, ayant un grand nombre de points rationnels.

Le Chapitre 4 concerne l'étude des propriétés et des conditions d'existence d'une courbe δ-optimale et d'une courbe maximale. Il contient également des résultats sur le nombre de points de degré 2 d'une courbe lisse, ainsi que sur les revêtements de courbes singulières.

Chapitre 1

Propriétés locales des points d'une courbe algébrique

La propriété pour un point Q d'une variété algébrique X d'être singulier est une propriété locale, c'est-à-dire une propriété qui demeure inchangée si X est remplacée par un voisinage quelconque de Q. Cette notion géométrique de concentrer l'attention « près d'un point » a son analogue algébrique dans le procédé de localisation d'un anneau en un idéal premier.

En gardant un niveau de généralisation propre à nos objectifs, nous rappelons dans ce chapitre les objets et les notions de base, ainsi que les principaux résultats qui interviennent dans l'étude d'une courbe algébrique singulière définie sur un corps fini, et qui seront utilisés tout au long de cette thèse.

Nous nous inspirerons principalement de [21], [27], [34], [39], [44], [45] et [47], en réadaptant éventuellement les définitions et les résultats dans le cas où le corps de base n'est pas algébriquement clos. Pour toutes les notions d'algèbre commutative nous renvoyons à [2].

1.1 Notations

Nous fixons les notations suivantes :

q	une puissance d'un nombre premier,
$\mathbb{F}_q$	le corps fini à q éléments,
$\overline{\mathbb{F}}_q$	la clôture algébrique de $\mathbb{F}_q$,
$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$	le groupe de Galois de l'extension $\overline{\mathbb{F}}_q/\mathbb{F}_q$.

À noter que les définitions et résultats de ce chapitre restent valables si on remplace $\mathbb{F}_q$ par un autre corps parfait, c'est-à-dire un corps dont toute extension algébrique est séparable.

1.2 L'anneau local en un point

Commençons par examiner les objets algébriques associés aux points d'une courbe algébrique. Dans cette section, nous nous limitons au cas des courbes affines. Cela peut se faire sans perte de généralité, car chaque point d'une courbe projective admet un voisinage affine, c'est-à-dire un ouvert affine qui le contient.

Soit $X \subset \mathbb{A}^n(\overline{\mathbb{F}}_q) := \{(x_1, \ldots, x_n) : x_i \in \overline{\mathbb{F}}_q\}$ une *courbe algébrique affine*, c'est-à-dire une variété algébrique affine de dimension 1.

Définition 1.2.1. On dit que X est *définie sur* $\mathbb{F}_q$ si l'idéal

$$\mathcal{I}(X) := \{F \in \overline{\mathbb{F}}_q[X_1, \ldots, X_n] : F(Q) = 0 \text{ pour tout } Q \in X(\overline{\mathbb{F}}_q)\}$$

peut être engendré par des polynômes de $\mathbb{F}_q[X_1, \ldots, X_n]$.

Remarque 1.2.2. Considérons l'idéal

$$\mathcal{I}(X/\mathbb{F}_q) := \{F \in \mathbb{F}_q[X_1, \ldots, X_n] : F(Q) = 0 \text{ pour tout } Q \in X\} = \mathcal{I}(X) \cap \mathbb{F}_q[X_1, \ldots, X_n].$$

Alors X est définie sur $\mathbb{F}_q$ si et seulement si :

$$\mathcal{I}(X) = \mathcal{I}(X/\mathbb{F}_q)\ \overline{\mathbb{F}}_q[X_1, \ldots, X_n].$$

Définition 1.2.3. Une courbe algébrique X définie sur $\mathbb{F}_q$ est dite *irréductible sur* $\mathbb{F}_q$ si $\mathcal{I}(X/\mathbb{F}_q)$ est un idéal premier de $\mathbb{F}_q[X_1, \ldots, X_n]$. Elle est dite *absolument irréductible* (ou *géométriquement irréductible)* si elle est irréductible sur $\overline{\mathbb{F}}_q$, c'est-à-dire si $\mathcal{I}(X)$ est un idéal premier de $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$.

Exemple 1.2.4. La courbe $X^2 + XY + Y^2 = 0$ est irréductible sur $\mathbb{F}_2$, mais pas absolument irréductible. En effet dans $\mathbb{F}_{2^2}$ elle est la réunion des deux droites :

$$\mathcal{D}_1 : X - \zeta Y = 0 \quad \text{et} \quad \mathcal{D}_2 : X - \zeta^2 Y = 0,$$

où $\zeta \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$ est une racine primitive 3-ème de l'unité.

Définition 1.2.5. Soit X une courbe définie sur $\mathbb{F}_q$. L'ensemble des *points rationnels sur* $\mathbb{F}_q$ de X est l'ensemble

$$X(\mathbb{F}_q) = X \cap \mathbb{A}^n(\mathbb{F}_q).$$

Remarque 1.2.6. Si X est définie sur $\mathbb{F}_q$, pout tout $n \geq 1$ on peut aussi définir l'ensemble des points de X rationnels sur $\mathbb{F}_{q^n}$ par

$$X(\mathbb{F}_{q^n}) = X \cap \mathbb{A}^n(\mathbb{F}_{q^n}).$$

L'ensemble $X(\mathbb{F}_{q^n})$ correspond ainsi aux points de $X(\overline{\mathbb{F}}_q)$ à coordonnées dans $\mathbb{F}_{q^n}$. Si l'on ne précise pas l'extension, un *point rationnel* désignera un point rationnel sur $\mathbb{F}_q$.

Dans la suite on supposera X définie sur $\mathbb{F}_q$.

Soient $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ des polynômes générateurs de $\mathcal{I}(X/\mathbb{F}_q)$ (l'anneau $\mathbb{F}_q[X_1, \ldots, X_n]$ étant noetherien, ses idéaux sont tous de type fini). Alors $X(\mathbb{F}_q)$ est constitué par l'ensemble des solutions $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ du système d'équations polynomiales :

$$\begin{cases} F_1(X_1, \ldots, X_n) = 0 \\ \vdots \\ F_m(X_1, \ldots, X_n) = 0. \end{cases}$$

On remarque que si $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ et $Q = (x_1, \ldots, x_n) \in \mathbb{A}^n(\overline{\mathbb{F}}_q)$, alors pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on a

$$F(Q^\sigma) = F(Q)^\sigma, \tag{1.1}$$

où $Q^\sigma = (\sigma(x_1), \ldots, \sigma(x_n))$ et $F(Q)^\sigma = \sigma(F(Q))$. Ainsi $F(Q^\sigma) = 0$ si et seulement si $F(Q)^\sigma = 0$, et $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ induit une action sur $X(\overline{\mathbb{F}}_q)$. Il est immédiat de vérifier que

$$X(\mathbb{F}_q) = \{Q \in X(\overline{\mathbb{F}}_q) : Q = Q^\sigma, \text{ pour tout } \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\}.$$

Définition 1.2.7. Soit X une courbe algébrique définie sur $\mathbb{F}_q$. Un *point fermé* Q de X est une orbite de l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ sur $X(\overline{\mathbb{F}}_q)$:

$$Q = \left\{ \overline{Q}^\sigma : \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \right\},$$

où $\overline{Q} \in X(\overline{\mathbb{F}}_q)$. Le *degré* $\deg Q$ de Q est le cardinal de son orbite. Le *corps de décomposition* de Q est la plus petite extension de $\mathbb{F}_q$ sur laquelle l'orbite se décompose en points séparés.

Remarque 1.2.8.

1. Le degré d'un point fermé Q est le degré de son corps de décomposition sur $\mathbb{F}_q$. Autrement dit, c'est le degré de la plus petite extension de $\mathbb{F}_q$ qui contienne les coordonnées de tous les éléments de l'orbite. Ainsi le degré d'un point est toujours fini.
   Si Q est un point de degré d alors $Q = \{\overline{Q}, \overline{Q}^\varphi, \ldots, \overline{Q}^{\varphi^{d-1}}\}$ où $\overline{Q} \in X(\overline{\mathbb{F}}_q)$ et $\varphi \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ est l'*automorphisme de Frobenius* défini par :
   $$\begin{array}{rccc} \varphi : & \overline{\mathbb{F}}_q & \to & \overline{\mathbb{F}}_q \\ & \alpha & \mapsto & \alpha^q \end{array}. \tag{1.2}$$
2. Un point rationnel sur $\mathbb{F}_q$ est un point fermé de degré 1.
3. Soit $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ et $Q = \{\overline{Q}, \overline{Q}^\varphi, \ldots, \overline{Q}^{\varphi^{d-1}}\}$ un point fermé de degré d. D'après (1.1), s'il existe $i_0 \in \{0, \ldots, d-1\}$ tel que $F(\overline{Q}^{\varphi^{i_0}}) = 0$, alors $F(\overline{Q}^{\varphi^i}) = 0$ pour tout $i = 0, \ldots, d-1$. Ainsi, dans ce cas, on pourra se permettre l'abus de notation $F(Q) = 0$. Cela justifiera aussi le fait de considérer les fonctions s'annulant en un point fermé.

Notations. Soit X une courbe algébrique définie sur $\mathbb{F}_q$. On note

$$B_d(X)$$

le nombre de points fermés de degré d de X.

Remarque 1.2.9. Puisque chaque point de degré d de X engendre exactement d points de $X(\mathbb{F}_{q^d})$, pour tout $n \geq 1$ on a la formule suivante :

$$X(\mathbb{F}_{q^n}) = \sum_{d|n} dB_d(X). \tag{1.3}$$

À partir de maintenant, un point fermé sera plus simplement appelé point, sauf indication contraire.

Définition 1.2.10. Soit X une courbe algébrique définie sur $\mathbb{F}_q$ et Q l'un de ses points. Soit $\mathcal{I}(X/\mathbb{F}_q) = (F_1, \ldots, F_m) \subset \mathbb{F}_q[X_1, \ldots, X_n]$. On dit que X est *non singulière* en Q si la matrice de taille $m \times n$

$$\left(\frac{\partial F_i}{\partial X_j}(Q)\right)_{\substack{1\leq i\leq m\\ 1\leq j\leq n}},$$

appelée *matrice Jacobienne en* Q, est de rang $n-1$. On dit que X est *non singulière* (ou *lisse*) si elle est non singulière en tout point.

Exemple 1.2.11. Soit q impair. Considérons dans le plan affine $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ les courbes décrites par les équations :

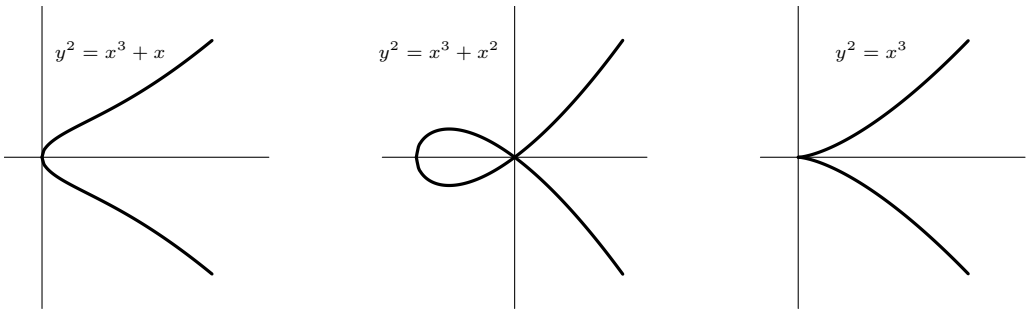
$$\mathcal{C}_0 : y^2 = x^3 + x, \qquad \mathcal{C}_1 : y^2 = x^3 + x^2, \qquad \mathcal{C}_2 : y^2 = x^3.$$

Au point $Q_0 = (0,0)$ les trois matrices Jacobiennes

$$\mathcal{J}_0 = (-3x^2 - 1,\ 2y), \qquad \mathcal{J}_1 = (-3x^2 - 2x,\ 2y), \qquad \mathcal{J}_2 = (-3x^2,\ 2y)$$

ont pour rangs respectifs 1, 0 et 0. Il s'ensuit que Q_0 est un point non singulier pour $\mathcal{C}_0$ et singulier pour $\mathcal{C}_1$ et $\mathcal{C}_2$.

Pour avoir une vision géométrique du comportement local des trois courbes autour du point $(0,0)$, représentons $\mathcal{C}_0$, $\mathcal{C}_1$ et $\mathcal{C}_2$ dans le plan affine réel :



Nous examinerons plus en détails, dans la section 1.6, les propriétés algébriques locales « responsables » de la nature du point (0,0) dans les cas des courbes $\mathcal{C}_1$, et $\mathcal{C}_2$.

Remarque 1.2.12. L'ensemble des points singuliers d'une courbe algébrique irréductible X, noté $\mathrm{Sing}(X)$, est un ensemble propre et fermé dans la topologie de Zariski [21, Ch.I, Th. 5.3]. Ainsi une courbe algébrique irréductible a un nombre fini de points singuliers.

Remarque 1.2.13. Soit Q un point de X de degré d et soient $Q_1, \ldots, Q_d \in X(\overline{\mathbb{F}}_q)$, tels que $Q = \{Q_1, \ldots, Q_d\}$. Il est clair que Q est un point singulier de X si et seulement si Q_i est un point singulier de $X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, pour tout $i = 1, \ldots, d$.

La définition 1.2.10 semble dépendre du plongement de X dans un espace affine. Toutefois, on verra que l'on peut décrire intrinsèquement la propriété de non singularité, en termes des fonctions sur la courbe X (voir [53]).

Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$. Notons $\mathbb{F}_q[X]$ l'*anneau des coordonnées affines* de X sur $\mathbb{F}_q$:

$$\mathbb{F}_q[X] = \frac{\mathbb{F}_q[X_1, \ldots, X_n]}{\mathcal{I}(X/\mathbb{F}_q)}.$$

C'est un anneau intègre (car $\mathcal{I}(X/\mathbb{F}_q)$ est un idéal premier) de dimension de Krull égale à 1. Son corps des fractions, noté $\mathbb{F}_q(X)$, est appelé le *corps des fonctions rationnelles* de X sur $\mathbb{F}_q$. Ce dernier est une extension de type fini de $\mathbb{F}_q$, de degré de transcendance égal à 1. On définit, de façon similaire, $\overline{\mathbb{F}}_q[X]$ et $\overline{\mathbb{F}}_q(X)$, en remplaçant $\mathbb{F}_q$ par $\overline{\mathbb{F}}_q$.

Soit Q un point de X de degré d. Considérons le sous-ensemble $\mathcal{O}_Q$ de $\mathbb{F}_q(X)$ constitué par les fonctions rationnelles de X définies en Q :

$$\mathcal{O}_Q := \left\{ \frac{G}{H} \in \mathbb{F}_q(X) \ : \ H(Q) \neq 0 \right\}.$$

Si $f = G/H \in \mathcal{O}_Q$, alors $f(Q) = G(Q)/H(Q)$ est bien défini. Ainsi les éléments de $\mathcal{O}_Q$ sont appelés les *fonctions régulières en* Q. On montre aisément que $Q \neq Q'$ si et seulement si $\mathcal{O}_Q \neq \mathcal{O}_{Q'}$.

On remarque facilement que $\mathcal{O}_Q$ est le localisé de $\mathbb{F}_q[X]$ en l'idéal maximal

$$M_Q = \{F \in \mathbb{F}_q[X] : F(Q) = 0\}.$$

Il s'ensuit [2, Ex. 1 Ch. 3] que $\mathcal{O}_Q$ est un anneau local d'idéal maximal

$$\mathcal{M}_Q := \left\{ \frac{G}{H} \in \mathcal{O}_Q \ : \ G(Q) = 0 \right\}.$$

De plus, $\mathcal{O}_Q$ est de dimension de Krull 1, c'est-à-dire qu'il ne possède pas d'autres idéaux premiers que (0) et $\mathcal{M}_Q$ (cela vient du fait que $\mathbb{F}_q[X]$ est de dimension de Krull égale à 1). On a :

$$\frac{\mathcal{O}_Q}{\mathcal{M}_Q} \cong \frac{\mathbb{F}_q[X]}{M_Q} \cong \mathbb{F}_{q^d},$$

où le dernier isomorphisme est donné par l'application :

$$\begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_{q^d} \\ F & \mapsto & F(\overline{Q}) \end{array},$$

avec $\overline{Q}$ l'un des points de $X(\overline{\mathbb{F}}_q)$ dans l'orbite de Q.

L'anneau $\mathcal{O}_Q$ est appelé *anneau local de* X *en* Q.

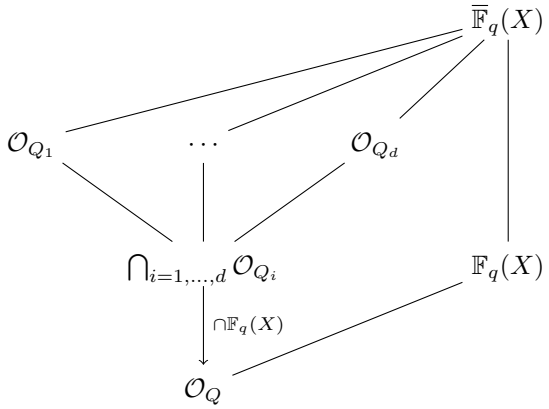
Remarque 1.2.14. Si l'on considère l'extension de corps de fonctions $\overline{\mathbb{F}}_q(X)/\mathbb{F}_q(X)$, il existe exactement d anneaux locaux qui contiennent $\mathcal{O}_Q$. Ils correspondent aux d points $Q_1, \ldots, Q_d \in X(\overline{\mathbb{F}}_q)$, tels que $Q = \{Q_1, \ldots, Q_d\}$. Il en découle que $\mathcal{O}_Q \subseteq \bigcap_{i=1,\ldots,d} \mathcal{O}_{Q_i} \subset \overline{\mathbb{F}}_q(X)$, et plus précisément

$$\mathcal{O}_Q = \left(\bigcap_{i=1,\ldots,d} \mathcal{O}_{Q_i} \right) \cap \mathbb{F}_q(X).$$

De plus, on a

$$\mathcal{M}_Q = \mathcal{M}_{Q_i} \cap \mathcal{O}_Q, \text{ pour tout } i = 1, \ldots d.$$

On peut illustrer cela de la manière suivante :



Le quotient $\mathcal{M}_Q/(\mathcal{M}_Q)^2$ est un $\mathcal{O}_Q/\mathcal{M}_Q$-espace vectoriel dont la dimension gouverne la nature du point Q. On a, en fait, le résultat suivant :

Théorème 1.2.15. *Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$ et Q un point de X. Alors X est non singulière en Q si et seulement si l'anneau local $\mathcal{O}_Q$ est un anneau local régulier, c'est-à-dire*

$$\dim_{\mathcal{O}_Q/\mathcal{M}_Q} \frac{\mathcal{M}_Q}{(\mathcal{M}_Q)^2} = \dim(\mathcal{O}_Q) = 1, \tag{1.4}$$

où le premier symbole dim *désigne la dimension d'un espace vectoriel et le second la dimension de Krull d'un anneau.*

Démonstration. Le résultat découle directement de [21, Ch. I, Th. 5.1], en remarquant qu'une courbe est une variété de dimension 1. □

La propriété (1.4) est équivalente à la condition que $\mathcal{M}_Q$ peut être engendré par un seul élément $t \in \mathcal{O}_Q$ appelé une *uniformisante locale en Q* [2, Th. 11.22].

Remarque 1.2.16. Les propriétés suivantes sont équivalentes pour un anneau local noethérien $\mathcal{O}$ d'idéal maximal $\mathcal{M}$ et de corps résiduel $\mathcal{O}/\mathcal{M}$ [2, Prop. 9.2] :

- $\mathcal{O}$ est un anneau de valuation discrète ;
- $\mathcal{O}$ est intégralement clos ;

- $\mathcal{M}$ est un idéal principal ;
- $\dim_{\mathcal{O}/\mathcal{M}}(\mathcal{M}/\mathcal{M}^2) = 1$;
- tout idéal non nul est une puissance de $\mathcal{M}$;
- il existe $t \in \mathcal{O}$ tel que tout idéal non nul est de la forme $t^k\mathcal{O}$, $k \geq 0$.

D'après la remarque précédente, un anneau local régulier de dimension 1 est un anneau de valuation discrète. On peut donc réécrire le théorème 1.2.15 sous la forme suivante :

Théorème 1.2.17. *Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$ et Q un point de X. Alors X est non singulière en Q si et seulement si $\mathcal{O}_Q$ est un anneau de valuation discrète.*

Si $Q \in X$ est non singulier, notons v_Q la valuation (à valeurs dans $\mathbb{Z}$) associée à $\mathcal{O}_Q$: si f est un élément non nul de $\mathbb{F}_q(X)$, la relation $v_Q(f) = n, n \in \mathbb{Z}$, signifie que f peut s'écrire sous la forme $f = t^n u$, où u est un élément inversible de $\mathcal{O}_Q$.

Remarque 1.2.18. Comme pour toute variété algébrique, les $\mathcal{O}_Q$ forment un faisceau d'anneaux sur X, à condition de munir X de la topologie de Zariski [38, Ch. II] ; rappelons que les sous-ensembles fermés d'une courbe X pour cette topologie sont les sous-ensembles finis et X lui-même. Le faisceau des anneaux locaux $\mathcal{O}_Q$ sera noté $\mathcal{O}_X$; c'est un sous-faisceau du faisceau constant $\mathbb{F}_q(X)$.

1.3 La normalisée d'une courbe

Commençons par résumer les propriétés fondamentales de la normalisée d'une courbe algébrique, en partant de sa définition.

Définition 1.3.1. Une *normalisée* d'une courbe algébrique irréductible X est une courbe algébrique irréductible lisse $\tilde{X}$ pour laquelle il existe une application régulière

$$\nu : \tilde{X} \to X,$$

telle que ν est finie et birationnelle. L'application ν est appelée *normalisation*.

Remarque 1.3.2.

1. Si $X = \bigcup_i X_i$ est une courbe réductible alors on peut définir $\tilde{X} = \bigcup_i \tilde{X}_i$. Pour cette raison il n'est pas contraignant de supposer X irréductible.
2. Une courbe affine a une normalisée qui est aussi affine [44, Th. 4 Ch. II].
3. Si X est définie sur $\mathbb{F}_q$, alors il en va de même pour $\tilde{X}$ et ν.
4. Puisque ν est birationnelle, on a que $\mathbb{F}_q(\tilde{X})$ et $\mathbb{F}_q(X)$ sont isomorphes en tant $\mathbb{F}_q$-algèbres [21, Ch. I, Cor. 4.5]. Un isomorphisme est donné par l'application :

$$\begin{array}{rccc} \nu^* : & \mathbb{F}_q(X) & \to & \mathbb{F}_q(\tilde{X}) \\ & f & \mapsto & f \circ \nu \end{array}$$

5. Par définition des applications régulières finies, on a que si $\tilde{X}$ est une normalisée de X, alors $\mathbb{F}_q[\tilde{X}]$ est entier sur $\mathbb{F}_q[X]$. Or, l'anneau $\mathbb{F}_q[\tilde{X}]$ est intégralement clos (ou normal),

puisque $\tilde{X}$ est une courbe lisse, et donc normale [44, Th. 1 Ch. 5]. Il s'ensuit que $\mathbb{F}_q[\tilde{X}]$ est la fermeture intégrale de $\mathbb{F}_q[X]$ dans son corps des fractions $\mathbb{F}_q(X)$, c'est-à-dire la clôture intégrale de $\mathbb{F}_q[X]$.

6. Le fait que ν soit finie entraîne aussi que, pour tout $Q \in X$, la fibre $\nu^{-1}(Q) \subset \tilde{X}$ de ν au-dessus de Q est finie. Autrement dit, il existe un nombre fini de points $P_1, \ldots, P_s \in \tilde{X}$ tels que $\nu(P_i) = Q$. Si $\nu(P) = Q$, on écrira aussi $P \to Q$.

La courbe normalisée est unique à isomorphisme près :

Théorème 1.3.3. [44, Cor. Ch. 5] *La normalisation d'une courbe algébrique affine irréductible X est unique. Plus précisément, si $\nu : \tilde{X} \to X$ et $\nu' : \tilde{X}' \to X$ sont deux normalisations, alors il existe un isomorphisme $\phi : \tilde{X} \to \tilde{X}'$.*

Théorème 1.3.4. [44, Th. 7 Ch. II] *La normalisée d'une courbe projective est une courbe projective.*

Il est intéressant d'examiner les relations entre les points de X et $\tilde{X}$, et les anneaux locaux de $\mathbb{F}_q(X)$ et $\mathbb{F}_q(\tilde{X})$.

Proposition 1.3.5. *Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$, $\tilde{X}$ sa courbe normalisée et $\nu : \tilde{X} \to X$ l'application de normalisation. Alors $P \to Q$ si et seulement si $\nu^*(\mathcal{O}_Q) \subseteq \mathcal{O}_P$.*

Démonstration. Supposons d'abord que $\nu(P) = Q$. Soit donc $f = G/H \in \mathcal{O}_Q$. On a :

$$\nu^*(f) = \frac{\nu^*(G)}{\nu^*(H)} = \frac{G \circ \nu}{H \circ \nu},$$

avec $H \circ \nu(P) = H(\nu(P)) = H(Q) \neq 0$. Donc $\nu^*(f) \in O_P$.

Supposons réciproquement que $\nu^*(\mathcal{O}_Q) \subseteq \mathcal{O}_P$. Alors pour tout $f = G/H \in \mathcal{O}_Q$ on a $\nu^*(f) = (G \circ \nu)/(H \circ \nu) \in \mathcal{O}_P$. En particulier, on obtient $H(\nu(P)) = H(Q) \neq 0$ qui implique $f \in \mathcal{O}_{\nu(P)}$. Ainsi $\mathcal{O}_Q \subseteq \mathcal{O}_{\nu(P)}$, d'où $Q = \nu(P)$. □

En vertu de l'isomorphisme ν^*, à partir de maintenant nous considérerons $\mathbb{F}_q[X]$ comme un sous-anneau de $\mathbb{F}_q[\tilde{X}]$ et $\mathbb{F}_q(X) = \mathbb{F}_q(\tilde{X})$. Ainsi, pour tout $P \to Q$ nous verrons $\mathcal{O}_P$ comme un sur-anneau de $\mathcal{O}_Q$. Avec cette convention, on a le corollaire suivant :

Corollaire 1.3.6. *Soit $\mathcal{O}_Q$ un anneau local de $\mathbb{F}_q(X)$. Il existe un nombre fini d'anneaux de valuation discrète de $\mathbb{F}_q(X)$ qui contiennent $\mathcal{O}_Q$. Ce sont précisément les anneaux locaux des points P de $\tilde{X}$ tels que $P \to Q$.*

Soit Q un point de X et soient $P_1, \ldots, P_s$ les points de $\tilde{X}$ tels que $P_i \to Q$ pour tout $i = 1, \ldots, s$. On peut illustrer la proposition 1.3.5 et le corollaire 1.3.6 avec le diagramme suivant :

Remarque 1.3.7. Le faisceau $\mathcal{O}_X$ sur X est donc l'*image directe* $\nu(\mathcal{O}_{\tilde{X}})$ du faisceau $\mathcal{O}_{\tilde{X}}$ des anneaux locaux sur $\tilde{X}$.

Le corollaire précédent permet aussi de définir des relations entre les degrés des points sur X et $\tilde{X}$ qui se correspondent à travers ν :

Proposition 1.3.8. *Soient $Q \in X$ et $P_1, \ldots, P_s \in \tilde{X}$ tels que $P_i \to Q$. Alors*

$$\deg Q \mid \deg P_i, \quad \textit{pour tout } i = 1, \ldots, s.$$

En particulier, s'il existe $i = 1, \ldots, s$ tel que P_i soit rationnel, alors Q est rationnel. De plus, si Q est non singulier, alors Q et $P = \nu^{-1}(Q)$ ont le même degré.

Démonstration. Si $P \to Q$, alors $\mathcal{O}_Q \subseteq \mathcal{O}_P$ et l'application

$$\begin{array}{ccc} \dfrac{\mathcal{O}_Q}{\mathcal{M}_Q} & \longrightarrow & \dfrac{\mathcal{O}_P}{\mathcal{M}_P} \\ f + \mathcal{M}_Q & \longmapsto & f + \mathcal{M}_P \end{array},$$

est un plongement de corps. Ainsi

$$\deg P = \left[\frac{\mathcal{O}_P}{\mathcal{M}_P} : \mathbb{F}_q\right] = \left[\frac{\mathcal{O}_P}{\mathcal{M}_P} : \frac{\mathcal{O}_Q}{\mathcal{M}_Q}\right]\left[\frac{\mathcal{O}_Q}{\mathcal{M}_Q} : \mathbb{F}_q\right] = \left[\frac{\mathcal{O}_P}{\mathcal{M}_P} : \frac{\mathcal{O}_Q}{\mathcal{M}_Q}\right] \cdot \deg Q.$$

Si Q est non singulier, alors $\mathcal{O}_Q = \mathcal{O}_P$, d'où $\deg Q = \deg P$. □

Remarque 1.3.9. Une conséquence immédiate de la proposition 1.3.8 est que

$$\nu\left(\tilde{X}(\mathbb{F}_{q^n})\right) \subseteq X(\mathbb{F}_{q^n}).$$

Proposition 1.3.10. *Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$ et $\nu : \tilde{X} \to X$ la normalisation de X. Si Q est non singulier, alors il existe un unique point P tel que $\nu(P) = Q$. Autrement dit, si $Q \in X$ est tel que $|\nu^{-1}(Q)| > 1$, alors Q est singulier.*

Démonstration. Si Q est non singulier, alors $\mathcal{O}_Q$ est un anneau de valuation discrète, et un anneau de valuation discrète n'a pas de sur-anneau de valuation discrète propre. □

Proposition 1.3.11. *L'application de normalisation $\nu : \tilde{X} \to X$ est un isomorphisme birégulier de $\tilde{X} \setminus \nu^{-1}(\mathrm{Sing}(X))$ sur $X \setminus \mathrm{Sing(X)}$.*

Démonstration. Cela découle directement du fait qu'une application rationnelle entre courbes est régulière en les points non singuliers [45, Prop. 2.1]. □

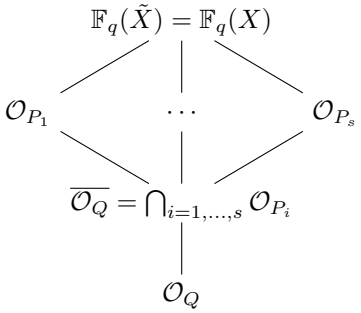
1.4 Invariants locaux d'un point

Dans la section 1.2, on a déjà vu que les informations sur la nature d'un point d'une courbe (comme la propriété d'être singulier) sont contenues dans son anneau local. Dans cette section, nous examinons plus en détails les caractéristiques d'un point qui dépendent de son anneau local et qui sont appelées *invariants locaux* du point.

Soient X une courbe algébrique irréductible définie sur $\mathbb{F}_q$, $\tilde{X}$ sa courbe normalisée et $\nu : \tilde{X} \to X$ une application de normalisation. Soit $Q \in \mathrm{Sing}(X)$. D'après la remarque 1.2.16 et le théorème 1.2.17, l'anneau local $\mathcal{O}_Q$ n'est pas intégralement clos. Ainsi, on peut considérer la clôture intégrale $\overline{\mathcal{O}_Q}$ de $\mathcal{O}_Q$. Soient $P_1, \ldots, P_s \in \tilde{X}$ tels que $P_i \to Q$ pour tout $i = 1, \ldots, s$. D'après [2, Cor. 5.22] et le corollaire 1.3.6, on a :

$$\overline{\mathcal{O}_Q} = \bigcap_{P \to Q} \mathcal{O}_P = \bigcap_{i=1,\ldots,s} \mathcal{O}_{P_i}.$$

La situation est illustrée dans le diagramme suivant :



L'anneau $\overline{\mathcal{O}_Q}$ est ainsi une intersection finie d'anneaux de valuation discrète. Il est bien connu (voir [46, Prop. 3.2.9]) que cela entraîne que $\overline{\mathcal{O}_Q}$ est un anneau semi-local, c'est-à-dire qu'il a un nombre fini d'idéaux maximaux. Ce sont précisément les idéaux $\mathcal{N}_i$ donnés par

$$\mathcal{N}_i = \mathcal{M}_{P_i} \cap \overline{\mathcal{O}_Q}, \quad i = 1, \ldots, s.$$

De plus les corps $\mathcal{O}_{P_i}/\mathcal{M}_{P_i}$ et $\overline{\mathcal{O}_Q}/\mathcal{N}_i$ sont isomorphes.

Plus exactement, $\overline{\mathcal{O}_Q}$ est un anneau principal [46, Prop. 3.2.10], et donc, en particulier, un anneau de Dedekind.

Considérons le $\mathcal{O}_Q$-module $\overline{\mathcal{O}_Q}/\mathcal{O}_Q$. C'est un $\mathbb{F}_q$-espace vectoriel de dimension finie [36, Th.1].

Soit $\mathcal{C}_Q$ l'*annulateur* de $\overline{\mathcal{O}_Q}/\mathcal{O}_Q$, à savoir :

$$\mathcal{C}_Q = \{f \in \mathcal{O}_Q : f\overline{\mathcal{O}_Q} \subseteq \mathcal{O}_Q\}.$$

Il est clair que $\mathcal{C}_Q$ est un idéal à la fois de $\mathcal{O}_Q$ et de $\overline{\mathcal{O}_Q}$. Plus précisément, $\mathcal{C}_Q$ est le plus grand idéal de $\mathcal{O}_Q$ qui soit un idéal de $\overline{\mathcal{O}_Q}$. L idéal $\mathcal{C}_Q$ est appelé le *conducteur* de l'extension $\overline{\mathcal{O}_Q}/\mathcal{O}_Q$.

On définit ainsi les *invariants locaux fondamentaux* d'un point Q :

Définition 1.4.1. Soit X une courbe algébrique irréductible définie sur $\mathbb{F}_q$ et Q l'un de ses points. Considérons les entiers positifs :

$$\delta_Q := \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{O}_Q, \qquad n_Q := \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{C}_Q.$$

On appelle n_Q et δ_Q les *invariants locaux fondamentaux* de Q. En particulier δ_Q est appelé le *degré de singularité* en Q.

Remarque 1.4.2. Les assertions suivantes sont équivalentes :

- Q est non singulier ;
- $\delta_Q = 0$;
- $n_Q = 0$.

Cela découle directement du fait que Q est non singulier si et seulement si $\overline{\mathcal{O}_Q} = \mathcal{O}_Q$.

Remarque 1.4.3. En vertu du troisième théorème d'isomorphisme pour les $\mathbb{F}_q$-modules $\overline{\mathcal{O}_Q} \supseteq \mathcal{O}_Q \supseteq \mathcal{C}_Q$ [2, Prop. 2.1] :

$$\overline{\mathcal{O}_Q}/\mathcal{O}_Q \cong (\overline{\mathcal{O}_Q}/\mathcal{C}_Q)(\mathcal{O}_Q/\mathcal{C}_Q),$$

on a que si $\delta_Q > 0$, alors $\mathcal{C}_Q$ est un idéal propre. Ainsi, dans l'anneau de Dedekind $\overline{\mathcal{O}}_Q$, il possède une factorisation unique comme produit des idéaux maximaux $\mathcal{N}_1, \ldots, \mathcal{N}_s$ de $\overline{\mathcal{O}}_Q$ [2, Cor. 9.4], c'est-à-dire qu'il existe $n_1, \ldots, n_s$ strictement positifs tels que :

$$\mathcal{C}_Q = \mathcal{N}_1^{n_1} \cdots \mathcal{N}_s^{n_s}.$$

Or

$$\overline{\mathcal{O}_Q}/\mathcal{C}_Q = \overline{\mathcal{O}_Q}/(\mathcal{N}_1^{n_1} \cdots \mathcal{N}_s^{n_s}) \cong \bigoplus_{i=1,\ldots,s} \overline{\mathcal{O}_Q}/\mathcal{N}_i^{n_i} \cong \bigoplus_{i=1,\ldots,s} (\mathcal{O}_{P_i}/\mathcal{M}_{P_i})^{n_i},$$

donc

$$\delta_Q = \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{C}_Q - \dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q = \sum_{i=1,\ldots,s} n_i \deg P_i - \dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q.$$

Cela montre comment, dans le cas non algébriquement clos, le degré de singularité d'un point dépend aussi du degré des points qui appartiennent à la fibre, via l'application de normalisation.

Proposition 1.4.4. *Si $\delta_Q \neq 0$, alors $\delta_Q \leq n_Q - 1$.*

Démonstration. On a

$$\delta_Q = n_Q - \dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q.$$

Si $\delta_Q \neq 0$, alors $\mathcal{O}_Q \subsetneq \overline{\mathcal{O}_Q}$, et $\mathcal{C}_Q \subsetneq \mathcal{O}_Q$. On a $\mathbb{F}_q + \mathcal{C}_Q \subseteq \mathcal{O}_Q$, d'où

$$\dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q \geq \dim_{\mathbb{F}_q} (\mathbb{F}_q + \mathcal{C}_Q)/\mathcal{C}_Q = 1.$$

□

1.5 Le genre arithmétique

Un *invariant birationnel* est une quantité ou un objet qui est bien défini sur une classe d'équivalence birationnelle de variétés algébriques. Autrement dit, il dépend seulement du corps des fonctions de la variété.

Dans le cas des courbes algébriques projectives irréductibles lisses, l'invariant birationnel numérique le plus important est le *genre* g, dont une définition peut être donnée à partir du théorème de Riemann-Roch (voir par exemple [45, Th. 5.4]), et qui prend toutes les valeurs entières positives $g \geq 0$. C'est un entier qui, d'une certaine façon, mesure la complexité de la courbe. Pour $g = 0$, par exemple, il existe exactement une classe d'équivalence birationnelle, celle des *courbes rationnelles*, c'est-à-dire des courbes qui sont birationnellement équivalentes à la droite projective $\mathbb{P}^1$.

Il est possible d'étendre la définition de genre à une courbe singulière, en définissant le genre d'une courbe singulière comme celui de la courbe lisse qui lui est birationnellement équivalente :

Définition 1.5.1. Le *genre géométrique* d'une courbe algébrique projective irréductible est le genre de sa normalisée.

Par définition, le genre géométrique est donc un invariant birationnel aussi des courbes singulières.

On peut associer à une courbe un autre entier naturel, le *genre arithmétique*, qui, comme on le verra, mesure, dans un certain sens, combien la courbe est « loin » d'être lisse.

Le genre arithmétique d'une courbe algébrique projective X plongée dans $\mathbb{P}^n$ est par définition (voir [32], [43], [54], où la définition pour une variété de dimension quelconque) l'entier π [1] tel que :

$$1 - \pi = \chi(X),$$

où $\chi(X)$ est le terme constant du polynôme caractéristique d'Hilbert de X dans $\mathbb{P}^n$. Si X est lisse, alors π est un invariant birationnel. Plus généralement, le genre arithmétique est un invariant numérique qui est indépendant du plongement projectif de X (voir [21, Ch. III, Ex. 5.3]).

Pour nos besoins, il sera plus utile de travailler avec une définition équivalente du genre arithmétique qui mette en évidence la dépendance de ce dernier par rapport au degré de singularité de la courbe (voir [39, Ch. IV n. 7]).

Définition 1.5.2. Soit X une courbe algébrique projective irréductible définie sur $\mathbb{F}_q$. Le *degré de singularité de* X, noté δ, est défini par la formule

$$\delta = \sum_{Q \in X} \delta_Q. \tag{1.5}$$

Remarque 1.5.3. Le degré de singularité de la courbe est ainsi naturellement défini comme la somme des degrés de singularité de ses points. D'après la remarque 1.4.2, la somme (1.5) peut

1. Dans la littérature, le genre arithmétique est plus souvent noté p_a. Nous adoptons ici la notation de Serre dans [39, Ch. IV n. 6])

être restreinte aux points $Q \in \mathrm{Sing}(X)$:

$$\delta = \sum_{Q \in \mathrm{Sing}(X)} \delta_Q. \tag{1.6}$$

En particulier X est lisse si et seulement si $\delta = 0$.

On remarque aussi que si on pose

$$\mathcal{O} := \bigcap_{Q \in \mathrm{Sing}(X)} \mathcal{O}_Q,$$

et si $\overline{\mathcal{O}}$ est la clôture intégrale de $\mathcal{O}$, alors, d'après [36, Lemma], on a

$$\delta = \dim_{\mathbb{F}_q} \overline{\mathcal{O}}/\mathcal{O}.$$

L'anneau $\mathcal{O}$, intersection des anneaux locaux des points singuliers de X, est appelé dans [36] l'*anneau semi-local de* X.

Définition 1.5.4. Soit X une courbe algébrique projective irréductible définie sur $\mathbb{F}_q$. Le *genre arithmétique* π de X est l'entier :

$$\pi := g + \delta,$$

où g est le genre géométrique de X.

Remarque 1.5.5.

1. Il est évident que $\pi \geq g$, et $\pi = g$ si et seulement si X est une courbe lisse.
2. Si X est une courbe plane de degré d alors (voir [21, Ch. I, Ex. 7.2])

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

Il s'ensuit que dans ce cas le genre géométrique de X est donné par la formule :

$$g = \frac{(d-1)(d-2)}{2} - \sum_{Q \in \mathrm{Sing}(X)} \delta_Q.$$

1.6 Exemples

Reprenons les courbes $\mathcal{C}_1,\ \mathcal{C}_2 \subseteq \mathbb{A}^2(\overline{\mathbb{F}}_q)$, avec q impair, introduites dans l'exemple 1.2.11 :

$$\mathcal{C}_1 : y^2 = x^3 + x^2, \qquad \mathcal{C}_2 : y^2 = x^3.$$

On a montré que le point $Q_0 = (0,0)$ est l'unique point singulier pour $\mathcal{C}_1$ et $\mathcal{C}_2$. On verra par la suite que les propriétés locales de ce point diffèrent suivant la courbe.

1) Considérons l'anneau des coordonnées affines de $\mathcal{C}_1$ sur $\mathbb{F}_q$

$$\mathbb{F}_q[\mathcal{C}_1] = \frac{\mathbb{F}_q[x,y]}{(y^2 - x^2 - x^3)} = \mathbb{F}_q[\overline{x}, \overline{y}],$$

où $\overline{x} = x + (y^2 - x^2 - x^3)\mathbb{F}_q[x,y]$ et $\overline{y} = y + (y^2 - x^2 - x^3)\mathbb{F}_q[x,y]$. L'élément $\overline{y}/\overline{x} \in \mathbb{F}_q(\mathcal{C}_1)$ est racine du polynôme unitaire $t^2 - (x+1) \in \mathbb{F}_q[\mathcal{C}_1][t]$. Ainsi $\overline{y}/\overline{x}$ est un élément entier sur $\mathbb{F}_q[\mathcal{C}_1]$ qui n'appartient pas à $\mathbb{F}_q[\mathcal{C}_1]$, d'où $\mathbb{F}_q[\mathcal{C}_1]$ n'est pas un anneau intégralement clos (en effet $\mathcal{C}_1$ n'est pas normale). On obtient que dans l'algèbre $\mathbb{F}_q[\mathcal{C}_1]\,[\overline{y}/\overline{x}]$ on a :

$$\overline{x} = \left(\frac{\overline{y}}{\overline{x}}\right)^2 - 1 \quad \text{et} \quad \overline{y} = \overline{x}\frac{\overline{y}}{\overline{x}} = \left(\left(\frac{\overline{y}}{\overline{x}}\right)^2 - 1\right)\frac{\overline{y}}{\overline{x}}.$$

Ainsi l'application

$$\begin{array}{rccc} \nu^* : & \mathbb{F}_q[\mathcal{C}_1]\,[\overline{y}/\overline{x}] & \longrightarrow & \mathbb{F}_q[t] \\ & \overline{x} & \longmapsto & t^2 - 1 \\ & \overline{y} & \longmapsto & (t^2-1)t \end{array}$$

est un isomorphisme et $\mathbb{F}_q[\mathcal{C}_1][\overline{y}/\overline{x}] \cong \mathbb{F}_q[t]$ est donc intégralement clos. Il s'ensuit que $\mathbb{A}^1(\mathbb{F}_q)$ est la normalisation de $\mathcal{C}_1$ et une application de normalisation est donnée par

$$\begin{array}{rccc} \nu : & \mathbb{A}^1 & \longrightarrow & \mathcal{C}_1 \\ & t & \longmapsto & (t^2-1, (t^2-1)t). \end{array}$$

Soit $Q_0 = (0,0) \in \mathcal{C}_1$ et

$$\mathcal{O}_{Q_0} = \mathbb{F}_q[\mathcal{C}_1]_{(\overline{x},\overline{y})} = \left\{ \frac{F}{G} \mid F, G \in \mathbb{F}_q[\mathcal{C}_1] \text{ et } G \notin (\overline{x},\overline{y})\mathbb{F}_q[\mathcal{C}_1] \right\}$$

l'anneau local de Q_0. En remarquant que

$$\nu^*(\mathbb{F}_q[\mathcal{C}_1]) = \mathbb{F}_q[t^2, t^3 - t] \qquad \text{et} \qquad (t^2-1, t(t^2-1))\mathbb{F}_q[t^2-1, t(t^2-1)] = (t^2-1)\mathbb{F}_q[t],$$

on a :

$$\begin{aligned} \nu^*(\mathcal{O}_{Q_0}) &= \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}_q[t^2, t^3 - t^2] \text{ et } g \notin (t^2-1)\mathbb{F}_q[t] \right\} \\ &= \mathbb{F}_q + (t^2-1)\left(\mathbb{F}_q[t]_{(t-1)} \cap \mathbb{F}_q[t]_{(t+1)}\right). \end{aligned}$$

Par abus de notation nous écrirons $\mathcal{O}_{Q_0}$ plutôt que $\nu^*(\mathcal{O}_{Q_0})$.

La fibre au-dessus de Q_0 est constituée de deux points rationnels de $\mathbb{A}^1$, $P_1 = 1$ et $P_2 = -1$:

$$\begin{array}{rccc} \nu : & \mathbb{A}_1 & \longrightarrow & \mathcal{C}_1 \\ & 1 & \searrow & \\ & & & Q_0 = (0,0) \\ & -1 & \nearrow & \end{array}$$

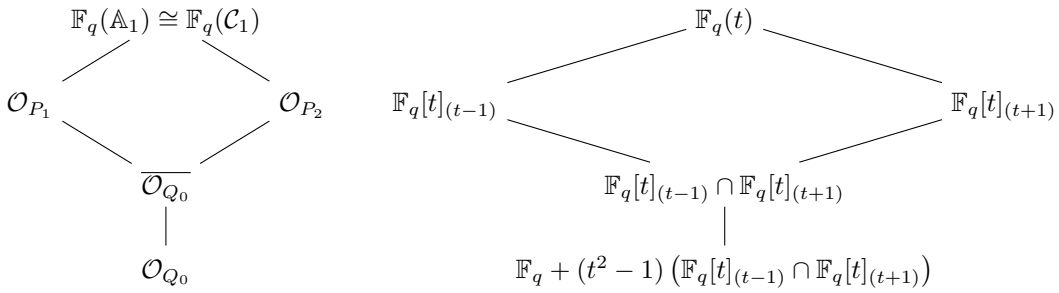
d'où

$$\overline{\mathcal{O}_{Q_0}} = \mathcal{O}_{P_1} \cap \mathcal{O}_{P_2} = \mathbb{F}_q[t]_{(t-1)} \cap \mathbb{F}_q[t]_{(t+1)}.$$

Ce dernier est un anneau semi-local, dont les idéaux maximaux sont précisément :

$$\mathcal{N}_1 = (t-1)\overline{\mathcal{O}_{Q_0}} \quad \text{et} \quad \mathcal{N}_2 = (t+1)\overline{\mathcal{O}_{Q_0}}.$$

Si l'on pose $\mathcal{C}_{Q_0} = (t^2-1)\overline{\mathcal{O}_{Q_0}} = \mathcal{N}_1\mathcal{N}_2$, on a que $\mathcal{O}_{Q_0} = \mathbb{F}_q + \mathcal{C}_{Q_0}$. On peut résumer la situation par les diagrammes suivants :



L'idéal $\mathcal{C}_{Q_0}$ est ainsi le conducteur de l'extension $\overline{\mathcal{O}_{Q_0}}/\mathcal{O}_{Q_0}$ et le degré de singularité en Q_0 est donné par

$$\delta_{Q_0} = \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{C}_Q - \dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q = \deg P_1 + \deg P_2 - 1 = 1.$$

2) Considérons l'anneau des coordonnées affines de $\mathcal{C}_2$ sur $\mathbb{F}_q$

$$\mathbb{F}_q[\mathcal{C}_2] = \frac{\mathbb{F}_q[x,y]}{(y^2-x^3)} = \mathbb{F}_q[\overline{x},\overline{y}],$$

où $\overline{x} = x + (y^2-x^3)$ et $\overline{y} = y + (y^2-x^3)$. On remarque que $\mathbb{F}_q[\mathcal{C}_2] \cong \mathbb{F}_q[t^2,t^3]$ puisque l'application

$$\begin{array}{rccc} \nu^* : & \mathbb{F}_q[\mathcal{C}_1] & \longrightarrow & \mathbb{F}_q[t^2,t^3] \\ & \overline{x} & \longmapsto & t^2 \\ & \overline{y} & \longmapsto & t^3 \end{array}$$

est un isomorphisme. Il est simple de montrer que $\mathbb{F}_q[t]$ est la clôture intégrale de $\mathbb{F}_q[t^2,t^3]$, car $t \in \mathrm{Frac}(\mathbb{F}_q[t^2,t^3]) = \mathbb{F}_q(t)$ est racine du polynôme unitaire $X^2 - t^2 \in \mathbb{F}_q[t^2,t^3][X]$ et $\mathbb{F}_q[t]$ est intégralement clos.
Il s'ensuit que $\mathbb{A}^1$ est la normalisation de $\mathcal{C}_2$ dans ce cas aussi, et une application de normalisation est donnée par

$$\begin{array}{rccc} \nu : & \mathbb{A}^1 & \longrightarrow & \mathcal{C}_2 \\ & t & \longmapsto & (t^2,t^3). \end{array}$$

Soit $Q_0 = (0,0) \in \mathcal{C}_2$ et

$$\mathcal{O}_{Q_0} = \mathbb{F}_q[\mathcal{C}_2]_{(\overline{x},\overline{y})} = \left\{ \frac{F}{G} \mid F, G \in \mathbb{F}_q[\mathcal{C}_2] \text{ et } G \notin (\overline{x},\overline{y})\mathbb{F}_q[\mathcal{C}_2] \right\}$$

l'anneau local de Q_0. En remarquant que

$$(t^2, t^3)\mathbb{F}_q[t^2, t^3] = t^2\mathbb{F}_q[t],$$

on a :

$$\begin{aligned}\nu^*(\mathcal{O}_{Q_0}) &= \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}_q[t^2, t^3] \text{ et } g \notin t^2\mathbb{F}_q[t] \right\} \\ &= \mathbb{F}_q + t^2\mathbb{F}_q[t]_{(t)}.\end{aligned}$$

Comme précédemment nous écrirons $\mathcal{O}_{Q_0}$ plutôt que $\nu^*(\mathcal{O}_{Q_0})$.
La fibre au-dessus de Q_0 est constituée du point rationnel $P = 0$, d'où

$$\overline{\mathcal{O}_{Q_0}} = \mathcal{O}_P = \mathbb{F}_q[t]_{(t)}.$$

Ce dernier est un anneau local d'idéal maximal $\mathcal{M}_P = t\mathbb{F}_q[t]_{(t)}$. Si l'on pose $\mathcal{C}_{Q_0} = t^2\mathcal{O}_P = (\mathcal{M}_P)^2$, on a que $\mathcal{O}_{Q_0} = \mathbb{F}_q + \mathcal{C}_{Q_0}$. On peut résumer la situation par les diagrammes suivants :

$$\begin{array}{c} \mathbb{F}_q(\mathbb{A}_1) \cong \mathbb{F}_q(\mathcal{C}_2) \\ | \\ \mathcal{O}_P = \overline{\mathcal{O}_{Q_0}} \\ | \\ \mathcal{O}_{Q_0} \end{array} \qquad\qquad \begin{array}{c} \mathbb{F}_q(t) \\ | \\ \mathbb{F}_q[t]_{(t)} \\ | \\ \mathbb{F}_q + t^2\mathbb{F}_q[t]_{(t)} \end{array}$$

L'idéal $\mathcal{C}_{Q_0}$ est ainsi le conducteur de l'extension $\overline{\mathcal{O}_{Q_0}}/\mathcal{O}_{Q_0}$ et le degré de singularité en Q_0 est donné par

$$\delta_{Q_0} = \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{C}_Q - \dim_{\mathbb{F}_q} \mathcal{O}_Q/\mathcal{C}_Q = 2\deg P - 1 = 1.$$

Chapitre 2

Bornes sur le nombre de points rationnels des courbes

Une courbe définie sur un corps fini a un nombre fini de points rationnels, car ce dernier est trivialement borné par le nombre de points rationnels de l'espace projectif dans lequel la courbe est plongée : un aspect arithmétique de la géométrie algébrique, qui a influencé de façon prépondérante des domaines d'application tels que la cryptographie et la théorie des codes.

La fonction zêta associée à une courbe joue un rôle central dans le comptage de son nombre de points rationnels. En partant du théorème de Weil pour les courbes lisses, nous parcourrons dans ce chapitre les résultats fondamentaux concernant les bornes sur le nombre de points rationnels d'une courbe algébrique projective absolument irréductible définie sur un corps fini, avec pour point culminant le cas des courbes singulières.

Sauf indication contraire, par la suite on utilisera le mot *courbe* pour désigner une courbe algébrique, projective, absolument irréductible.

2.1 Le cas lisse

On pourra se référer, pour cette section, à [25], [26], [33] et [49].

2.1.1 La borne de Serre-Weil

Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. Notons $\sharp X(\mathbb{F}_{q^n})$ le nombre de points de X rationnels sur $\mathbb{F}_{q^n}$. La fonction zêta de X, notée $Z_X(T)$, est définie par :

$$Z_X(T) := \exp\left(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right). \tag{2.1}$$

Exemple 2.1.1. Considérons $\mathbb{P}^1$, la droite projective définie sur $\mathbb{F}_q$. Pour tout $n \geq 1$, on a

$$\sharp \mathbb{P}^1(\mathbb{F}_{q^n}) = q^n + 1.$$

Ainsi, dans ce cas, la fonction zêta est donnée par :

$$Z_{\mathbb{P}^1}(T) = \exp\left(\sum_{n=1}^{\infty}(q^n+1)\frac{T^n}{n}\right) = \exp\left(\sum_{n=1}^{\infty}\frac{T^n}{n}\right)\exp\left(\sum_{n=1}^{\infty}\frac{(qT)^n}{n}\right) = \frac{1}{(1-T)(1-qT)}.$$

Il est bien connu que $Z_X(T)$ est une fonction rationnelle de $\mathbb{Q}(T)$ (la rationalité de $Z_X(T)$ vaut plus généralement pour tout schéma X défini sur $\mathbb{F}_q$, comme l'ont montré Dwork dans [11] et Grothendieck dans [19]). Plus précisément, on a le résultat suivant, aussi connu sous le nom d'*hypothèse de Riemann* pour les courbes sur les corps finis.

Théorème 2.1.2 (Weil, 1948 [1], [52])**.** *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. Alors la fonction zêta $Z_X(T)$ prend la forme :*

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)}, \tag{2.2}$$

où

$$P(T) = \prod_{i=1}^{2g}(1-\omega_i T) \in \mathbb{Z}[T]$$

est un polynôme de degré $2g$ dont les racines inverses $\omega_i \in \mathbb{C}$ sont des entiers algébriques de module $\sqrt{q}$.

De plus, la fonction zêta $Z_X(T)$ satisfait l'équation fonctionnelle

$$Z_X\left(\frac{1}{qT}\right) = \frac{Z_X(T)}{(qT^2)^{g-1}}.$$

Remarque 2.1.3.

1. Le théorème précédent montre en particulier que toutes les informations sur la courbe contenues dans la fonction zêta sont aussi contenues dans le polynôme $P(T)$.
2. Les ω_i sont deux à deux conjugués [46, Th. 5.1.15], et peuvent donc être ordonnés de façon à ce que $\omega_{i+g} = \overline{\omega}_i$. Si pour tout $i = 1, \ldots, g$ on note :

   $$\alpha_i = \omega_i + \overline{\omega}_i,$$

   on a

   $$Z_X(T) = \frac{\prod_{i=1}^{g}(1-\omega_i T)(1-\overline{\omega}_i T)}{(1-T)(1-qT)} = \frac{\prod_{i=1}^{g}(qT^2-\alpha_i T+1)}{(1-T)(1-qT)}. \tag{2.3}$$

Le théorème 2.1.2 entraîne le résultat suivant sur le nombre de points rationnels d'une courbe lisse définie sur $\mathbb{F}_q$:

1. La note originale de trois pages sur *l'hypothèse de Riemann pour une courbe sur un corps fini*, présentée par André Weil aux Comptes rendus de l'Académie des Sciences par l'intermédiaire d'Élie Cartan, est en vérité datée de 1940, mais il manque à cette note la preuve d'un *lemme important*, qui arrivera seulement 8 ans et 500 pages plus tard.
Pour plus de détails, le lecteur curieux pourra trouver dans [25] une référence intéressante sur le contexte historique et mathématique de la preuve par André Weil.

Proposition 2.1.4. *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. On a :*

$$\sharp X(\mathbb{F}_q) = q + 1 - \sum_{n=1}^{2g} \omega_i = q + 1 - \sum_{n=1}^{g} \alpha_i. \tag{2.4}$$

Démonstration. D'après la définition (2.1) de la fonction zêta, on pose :

$$\left.\frac{dZ_X(T)}{dT}\right|_{T=0} = \sharp X(\mathbb{F}_q).$$

D'autre part, en dérivant (2.2), on obtient :

$$\left.\frac{dZ_X(T)}{dT}\right|_{T=0} = q + 1 + P'(0) = q + 1 - \sum_{i=1}^{2g} \omega_i,$$

ce qui donne l'expression voulue pour $\sharp X(\mathbb{F}_q)$. □

Remarque 2.1.5. Plus généralement, pour tout entier $n \geq 1$ on a [46, Cor. 5.1.16] :

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{n=1}^{2g} \omega_i^n. \tag{2.5}$$

Une conséquence immédiate du théorème 2.1.2 et de l'équation (2.4) est la *borne de Weil*[2] pour le nombre de points rationnels d'une courbe lisse définie sur un corps fini :

Théorème 2.1.6. *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. On a*

$$|\sharp X(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}. \tag{2.6}$$

Remarque 2.1.7. En réécrivant la borne (2.6) sous la forme :

$$|\sharp X(\mathbb{F}_q) - \sharp \mathbb{P}^1(\mathbb{F}_q)| \leq 2(g_X - g_{\mathbb{P}^1})\sqrt{q},$$

le théorème 2.1.6 dit, d'une certaine façon, que le nombre de points rationnels d'une courbe définie sur $\mathbb{F}_q$ est « proche » du nombre de points rationnels de la droite projective sur le même corps fini.

Une amélioration significative de (2.6) lorsque q n'est pas un carré a été donnée par Serre en 1983. Cette nouvelle borne, qui est d'autant meilleure que le genre est grand, est traditionnellement appelée *borne de Serre-Weil* :

Théorème 2.1.8 (Serre, 1983, [41])**.** *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. On a*

$$|\sharp X(\mathbb{F}_q) - (q + 1)| \leq g[2\sqrt{q}]. \tag{2.7}$$

2. Dans la littérature la borne de Weil est parfois appelée *borne de Hasse-Weil*, car elle avait déjà été démontrée par Hasse dans les années 30, dans le cas des courbes elliptiques (voir [22] et [23]).

Démonstration. On peut supposer $g > 0$. D'après (2.4), il suffit de montrer que

$$\left|\sum_{i=1}^{g} \alpha_i\right| \leq g[2\sqrt{q}].$$

Pour $i = 1, \ldots, g$, on pose :

$$\gamma_i = \alpha_i + [2\sqrt{q}] + 1.$$

Les nombres γ_i sont des entiers algébriques réels qui forment un ensemble stable sous l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et tels que $\gamma_i > 0$ (puisque $\alpha_i \geq -2\sqrt{q}$). Ainsi, $\prod_{i=1}^{g} \gamma_i > 0$ est un entier. Si l'on applique l'inégalité arithmético-géométrique :

$$\frac{1}{g}\sum_{i=1}^{g} \gamma_i \geq \left(\prod_{i=1}^{g} \gamma_i\right)^{1/g} \geq 1,$$

il s'ensuit que

$$g \leq \sum_{i=1}^{g} \gamma_i = g([2\sqrt{q}] + 1) + \sum_{i=1}^{g} \alpha_i,$$

ou, autrement dit,

$$-\sum_{i=1}^{g} \alpha_i \leq g[2\sqrt{q}].$$

Pour l'autre inégalité, il suffit de remplacer α_i par $-\alpha_i$ dans la définition des γ_i. □

Exemple 2.1.9. Pour $g = 2$ et $q = 23$, la borne (2.6) donne $|\sharp X(\mathbb{F}_q) - 24| \leq 19$, alors que (2.7) donne $|\sharp X(\mathbb{F}_q) - 24| \leq 18$.

Notations. Nous notons de façon usuelle

$$N_q(g)$$

le nombre maximum de points rationnels d'une courbe lisse de genre g définie sur $\mathbb{F}_q$.

Le corollaire suivant découle directement de la borne de Serre-Weil.

Corollaire 2.1.10. *On a l'inégalité*

$$N_q(g) \leq q + 1 + g[2\sqrt{q}]. \tag{2.8}$$

2.1.2 La borne de Ihara

Quand le genre g est suffisamment grand par rapport à q, on a une amélioration significative de la borne de Serre-Weil, donnée par la *borne de Ihara*.

Théorème 2.1.11 (Ihara, 1981, [28])**.** *On a*

$$N_q(g) \leq q + 1 + \frac{1}{2}\left(\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - g\right). \tag{2.9}$$

Démonstration. Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. D'après l'inégalité, évidente,

$$\sharp X(\mathbb{F}_q) \leq \sharp X(\mathbb{F}_{q^2}),$$

remarquée et utilisée par Ihara dans [28], les formules (2.5) et le fait que $\omega_i\overline{\omega}_i = q$, on a :

$$q+1-\sum_{i=1}^{g}\alpha_i = \sharp X(\mathbb{F}_q) \leq \sharp X(\mathbb{F}_{q^2}) = q^2+1+2qg-\sum_{i=1}^{g}\alpha_i^2.$$

En appliquant la borne de Cauchy-Schwarz aux vecteurs $(\alpha_1,\ldots,\alpha_g)$ et $(1,\ldots,1)$ dans $\mathbb{R}^g$, on obtient :

$$\left(\sum_{i=1}^{g}\alpha_i\right)^2 \leq g\sum_{i=1}^{g}\alpha_i^2$$

et donc

$$\sharp X(\mathbb{F}_q) \leq q^2+1+2qg-\sum_{i=1}^{g}\alpha_i^2 \leq q^2+1+2qg-\frac{1}{g}\left(\sum_{i=1}^{g}\alpha_i\right)^2 = q^2+1+2qg-\frac{1}{g}(q+1-\sharp X(\mathbb{F}_q))^2.$$

Nous obtenons ainsi une inéquation de second degré en $\sharp X(\mathbb{F}_q)$:

$$(\sharp X(\mathbb{F}_q))^2-(2(q+1)-g)\sharp X(\mathbb{F}_q)+(q+1)^2-(q^2+2qg+1)g \leq 0,$$

dont la résolution donne la borne voulue.

□

Remarque 2.1.12. La borne de Ihara est meilleure que la borne de Weil dès que

$$2(q+1+2g\sqrt{q}) > \left(\sqrt{(8q+1)g^2+(4q^2-4q)g}-(g-2q-2)\right),$$

c'est-à-dire dès que

$$g > \frac{\sqrt{q}(\sqrt{q}-1)}{2},$$

ou, autrement dit, quand le genre est grand par rapport à la cardinalité du corps sur lequel la courbe est définie. Pour $q=4$, la borne de Ihara est déjà meilleure lorsque $g \geq 1$.

Exemple 2.1.13. La borne de Weil nous dit que $N_2(100) \leq 285$ alors que la borne de Ihara donne $N_2(100) \leq 159$.

Remarque 2.1.14. Pour g suffisamment grand par rapport à q, les bornes de Serre-Weil et Ihara sont améliorées par la *borne d'Oesterlé*[3] (voir [49]). Cette borne consiste en une optimisation de la méthode des « formules explicites » à travers laquelle Serre, dans [41], obtient des minorations du genre d'une courbe en fonction de son nombre de points rationnels.

3. Le résultat fut exposé par Oesterlé au séminaire 1982-1983 que dirigeait Serre au Collège de France, mais sa démonstration n'a jamais été publiée. Néanmoins, on peut trouver des indications sur l'énoncé et la démonstration du théorème d'Oesterlé dans les notes manuscrites de F. Q. Gouvea d'un cours de Serre à Harvard en 1985 (voir [42]).

2.1.3 Le cas des petits genres

Pour $g = 0, 1$, ou 2, la valeur de $N_q(g)$ est connue explicitement.

Dans le cas des courbes rationnelles, c'est-à-dire lorsque $g = 0$, le théorème 2.1.6 montre qu'une telle courbe a toujours $q + 1$ points rationnels :

$$N_q(0) = q + 1.$$

Le cas où $g = 1$, c'est-à-dire celui des courbes elliptiques, est moins trivial. Le résultat suivant est connu depuis les travaux de Hasse et Deuring (voir par exemple [10]).

Théorème 2.1.15. [50, Th. 4.1] *Soit $q = p^n$ avec p premier. Alors*

$$N_q(1) = \begin{cases} q + [2\sqrt{q}] & \text{si } p \text{ divise } [2\sqrt{q}], \text{ et si } n \geq 3, \\ q + 1 + [2\sqrt{q}] & \text{sinon.} \end{cases}$$

Le cas $g = 2$ a été entièrement résolu par Serre. Pour cela, nous disons que $q = p^r$ est *spécial* si q vérifie l'une des quatre conditions suivantes :

- q divise $[2\sqrt{q}]$;
- il existe un entier x tel que $q = x^2 + 1$;
- il existe un entier x tel que $q = x^2 + x + 1$;
- il existe un entier x tel que $q = x^2 + x + 2$.

Théorème 2.1.16 (Serre, [40])**.** *Si q est un carré et $q \neq 4, 9$, alors*

$$N_q(2) = q + 1 + 4\sqrt{q}.$$

De plus, on a $N_4(2) = 10$ et $N_9(2) = 20$. Si q n'est pas un carré, alors

$$N_q(2) = \begin{cases} q + 1 + 2[2\sqrt{q}] & \text{si } q \text{ n'est pas spécial ;} \\ q + 2[2\sqrt{q}] & \text{si } q \text{ est spécial et } 2\sqrt{q} - [2\sqrt{q}] > (\sqrt{5} - 1)/2 ; \\ q - 1 + 2[2\sqrt{q}], & \text{sinon.} \end{cases}$$

Déterminer $N_q(g)$ devient tout de suite un problème difficile pour $g \geq 3$. Pour $g = 3$ les principales idées et techniques qui ont été développées pour traiter le problème sont résumées dans [35].

Pour un tableau sur la meilleure évaluation de $N_q(g)$ lorsque q est petit, on peut consulter le site web `www.manypoints.org` [48].

2.1.4 Courbes lisses maximales

En vertu aussi des applications à la cryptographie et à la théorie des codes, les courbes avec beaucoup de points rationnels ont suscité un intérêt particulier de la part de la communauté mathématique. En 1981, Goppa a montré, par exemple, qu'il est possible d'associer à une courbe lisse sur un corps fini un code correcteur d'erreurs, et que les paramètres de ce code sont meilleurs quand le nombre de points rationnels de la courbe est large (voir [17] et [18]).

Ici nous rappelons le vocabulaire suivant.

Définition 2.1.17. Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. On dit que X est :

(i) *optimale* si
$$\sharp X(\mathbb{F}_q) = N_q(g)\,;$$

(ii) *maximale* si
$$\sharp X(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}].$$

Il faut remarquer que cette terminologie n'est pas universellement acceptée, et quelques auteurs appellent *courbe optimale* ce que nous appelons, ici, *courbe maximale*, et vice-versa.

Dans le cas des courbes maximales, la fonction zêta est explicite, comme énoncé dans la proposition suivante.

Proposition 2.1.18. *Soit X une courbe lisse maximale de genre g définie sur $\mathbb{F}_q$. Si $\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g$ sont les racines inverses du numérateur de la fonction zêta $Z_X(T)$ de X, alors*

$$\alpha_i = \omega_i + \overline{\omega}_i = -[2\sqrt{q}],$$

pour $1 \leq i \leq g$. En particulier on obtient

$$Z_X(T) = \frac{(qT^2 + [2\sqrt{q}]T + 1)^g}{(1-T)(1-qT)}.$$

Démonstration. En reprenant l'idée de la preuve de l'amélioration de Serre à la borne de Weil (théorème 2.1.8), l'inégalité arithmético-géométrique donne

$$\frac{1}{g}\sum_{i=1}^{g}([2\sqrt{q}] + 1 + \alpha_i) \geq \left(\prod_{i=1}^{g}([2\sqrt{q}] + 1 + \alpha_i)\right)^{1/g} \geq 1.$$

La maximalité de X entraîne que la moyenne arithmétique est égale à la moyenne géométrique. Ainsi, nous trouvons que $\alpha_i = -[2\sqrt{q}]$ pour tout $1 \leq i \leq g$.

La forme de la fonction zêta découle, alors, directement de l'équation (2.3). □

Or, si q est un carré, l'hypothèse de Riemann donne $\omega_i = -\sqrt{q}$ pour tout $i = 1, \ldots, g$. Par conséquent, l'expression de la fonction zêta se simplifie et devient :

$$Z_X(T) = \frac{(1 + \sqrt{q}T)^{2g}}{(1-T)(1-qT)}.$$

Deux problématiques, en particulier, se posent.

- Pour quels genres existe-t-il une courbe maximale ?
- Classifier les courbes maximales d'un genre donné.

Ces questions ont été largement étudiées dans le cas particulier où q est un carré. Ainsi, dans la suite de cette section nous supposerons q carré.

La proposition suivante, prouvée dans la remarque 2.1.12, nous dit que, à q fixé, le *spectre des genres* de courbes lisses maximales, c'est-à-dire l'ensemble des genres pour lesquels il existe une courbe lisse maximale définie sur $\mathbb{F}_q$, est fini.

Proposition 2.1.19 (Ihara, [28]). *Soit X une courbe lisse maximale de genre g définie sur $\mathbb{F}_q$. On a*

$$g \leq \frac{\sqrt{q}(\sqrt{q}-1)}{2}. \tag{2.10}$$

Rück et Stichtenoth ont montré dans [37] que g atteint la borne (2.10) si et seulement si X est $\mathbb{F}_q$-isomorphe à la *courbe Hermitienne*

$$x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + 1 = 0.$$

Nous listons d'autres résultats dans cette même direction.

Théorème 2.1.20 (Fuhrmann et Garcia, [13]). *Soit X une courbe lisse maximale de genre g définie sur $\mathbb{F}_q$. Alors*

$$ou \quad g \leq \left[\frac{(\sqrt{q}-1)^2}{4}\right], \qquad ou \quad g = \frac{\sqrt{q}(\sqrt{q}-1)}{2}. \tag{2.11}$$

L'inégalité (2.11) donne ce que l'on appelle le *first gap* dans le spectre des genres de courbes maximales lisses définies sur $\mathbb{F}_q$. Pour q impair, Fuhrmann, Garcia et Torres ont montré dans [12] que

$$g = \frac{(\sqrt{q}-1)^2}{4}$$

si et seulement si X est $\mathbb{F}_q$-isomorphe au modèle non singulier de la courbe plane d'équation affine

$$y^{\sqrt{q}} + y = x^{\frac{\sqrt{q}+1}{2}}.$$

Pour q pair, Abdón et Torres ont établi un résultat similaire dans [1], sous la condition d ?existence d ?un point de Weierstrass d ?un type particulier. Dans ce cas,

$$g = \frac{\sqrt{q}(\sqrt{q}-2)}{4}$$

si et seulement si X est $\mathbb{F}_q$-isomorphe au modèle non singulier de la courbe plane d'équation affine

$$y^{\sqrt{q}/2} + \cdots + y^2 + y = x^{(\sqrt{q}+1)}.$$

Une amélioration de (2.11) a été donnée par Korchmáros et Torres dans [29] :

Théorème 2.1.21 (Korchmáros et Torres, [29]). *Soit X une courbe lisse maximale de genre g définie sur $\mathbb{F}_q$. Alors*

$$ou \quad g \leq \left[\frac{q-\sqrt{q}+4}{6}\right], \qquad ou \quad g = \left[\frac{(\sqrt{q}-1)^2}{4}\right], \qquad ou \quad g = \frac{\sqrt{q}(\sqrt{q}-1)}{2}. \tag{2.12}$$

Ainsi, le deuxième saut (*second gap*) dans le spectre des genres de courbes lisses maximales définies sur $\mathbb{F}_q$ est aussi connu. Dans le même article, les auteurs fournissent également des modèles maximaux définis sur $\mathbb{F}_q$ de genre $\left[\frac{q-\sqrt{q}+4}{6}\right]$.

2.2 Le cas singulier

Dans le cas des courbes singulières, il existe notamment un analogue de la borne de Serre-Weil pour estimer le nombre de points rationnels. Nous verrons que cela découle du lien étroit entre une courbe singulière et sa normalisée, en particulier en termes de leurs fonctions zêta.

Les résultats rappelés par la suite sont contenus dans [6].

2.2.1 La fonction zêta d'une courbe singulière

Soient X une courbe (non nécessairement lisse) définie sur $\mathbb{F}_q$, $\tilde{X}$ la courbe normalisée de X et $\nu : \tilde{X} \to X$ une application de normalisation.

Théorème 2.2.1. *Soit* $\mathrm{Sing}(X)$ *l'ensemble (fini) des points singuliers de* X*. Alors*

$$Z_X(T) = \frac{P_X(T)}{(1-T)(1-qT)},$$

où

$$P_X(T) = P_{\tilde{X}}(T) \prod_{Q \in \mathrm{Sing}\, X} \left(\frac{\prod_{P \in \nu^{-1}(Q)} (1 - T^{\deg P})}{1 - T^{\deg Q}} \right) \tag{2.13}$$

et $P_{\tilde{X}}$ *est le numérateur de la fonction zêta* $Z_{\tilde{X}}$ *de* $\tilde{X}$*.*

Démonstration. Considérons le rapport des fonctions zêta Z_X et $Z_{\tilde{X}}$:

$$\frac{Z_X(T)}{Z_{\tilde{X}(T)}} = \exp\left(-\sum_{n=1}^{\infty} (\sharp \tilde{X}(\mathbb{F}_{q^n}) - \sharp X(\mathbb{F}_{q^n})) \frac{T^n}{n} \right). \tag{2.14}$$

Soit $Q \in \mathrm{Sing}(X)$. Notons $\alpha_Q(n)$ le nombre de points dans la fibre de Q via ν qui sont rationnels sur $\mathbb{F}_{q^n}$. Soit $\delta_{m|n}$ la fonction qui vaut 1 si m divise n, et 0 sinon.

D'après la proposition 1.3.8, un point non singulier de X et son antécédent dans $\tilde{X}$ ont même degré, le membre de droite de l'équation (2.14) se réduit donc à un produit sur les points singuliers

de X. Par conséquent,

$$\begin{aligned}\frac{Z_X(T)}{Z_{\tilde{X}(T)}} &= \prod_{Q\in \operatorname{Sing} X} \exp\left(-\sum_{n=1}^{\infty}(\alpha_Q(n)-\deg Q)\delta_{\deg Q|n}\frac{T^n}{n}\right)\\ &= \prod_{Q\in \operatorname{Sing} X} \exp\left(-\sum_{m=1}^{\infty}(\alpha_Q(m\deg Q)-\deg Q)\frac{T^{m\deg Q}}{m\deg Q}\right)\\ &= \prod_{Q\in \operatorname{Sing} X} \exp\left(-\sum_{m=1}^{\infty}\alpha_Q(m\deg Q)\frac{T^{m\deg Q}}{m\deg Q}+\sum_{m=1}^{\infty}\frac{(T^{\deg Q})^m}{m}\right)\\ &= \prod_{Q\in \operatorname{Sing} X} \frac{\exp\left(-\sum_{m=1}^{\infty}\alpha_Q(m\deg Q)\frac{T^{m\deg Q}}{m\deg Q}\right)}{1-T^{\deg Q}}\end{aligned}$$

Or

$$\alpha_Q(m\deg Q)=\sum_{P\in\nu^{-1}(Q)}\deg P\delta_{\deg P|m\deg Q},$$

donc

$$\begin{aligned}\frac{Z_X(T)}{Z_{\tilde{X}(T)}} &= \prod_{Q\in \operatorname{Sing} X} \frac{\prod_{P\in\nu^{-1}(Q)}\exp\left(-\sum_{m=1}^{\infty}\deg P\delta_{\deg P|m\deg Q}\frac{T^{m\deg Q}}{m\deg Q}\right)}{1-T^{\deg Q}}\\ &= \prod_{Q\in \operatorname{Sing} X} \frac{\prod_{P\in\nu^{-1}(Q)}\exp\left(-\sum_{l=1}^{\infty}\frac{T^{l\deg P}}{l}\right)}{1-T^{\deg Q}}\\ &= \prod_{Q\in \operatorname{Sing} X} \frac{\prod_{P\in\nu^{-1}(Q)}(1-T^{\deg P})}{1-T^{\deg Q}}\end{aligned}$$

et le théorème est prouvé. □

Exemple 2.2.2. Le théorème 2.2.1 permet de déterminer aisément les fonctions zêta des courbes traitées dans les exemples du premier chapitre (voir la sous-section 1.6). En effet, si l'application de normalisation est explicite pour une courbe, il est alors simple de trouver la partie cyclotomique de le fonction zêta associée à cette courbe. Dans ce cas, il suffit donc de connaître la fonction zêta de la courbe normalisée pour déterminer la fonction zêta de la courbe en question.

1. Soit $\overline{\mathcal{C}}_1$ la clôture projective de la courbe $\mathcal{C}_1 : y^2 = x^3 + x^2$, à savoir

$$\overline{\mathcal{C}}_1 : Y^2Z - X^3 - X^2Z = 0.$$

Le point à l'infini $(0:1:0)$ n'est pas un point singulier pour $\overline{\mathcal{C}}_1$, ainsi $\mathbb{P}_1$ est la normalisée de $\overline{\mathcal{C}}_1$. La fibre de $(0:0:1)$, via la normalisation

$$\begin{array}{rccc}\nu: & \mathbb{P}^1 & \longrightarrow & \overline{\mathcal{C}}_1\\ & (s:t) & \longmapsto & (t(s^2-t^2):(s^2-t^2)s:t^3),\end{array} \tag{2.15}$$

est constituée par deux points rationnels, $P_1 = (1:1)$ et $P_2 = (-1:1)$ d'où :

$$Z_{\overline{\mathcal{C}}_1}(T) = Z_{\mathbb{P}^1}(T)\frac{(1-T)^2}{1-T} = \frac{1-T}{1-qT}.$$

2. La clôture projective $\overline{\mathcal{C}}_2$ de $\mathcal{C}_2 : y^2 = x^3$ est donnée par

$$\overline{\mathcal{C}}_2 : Y^2Z - X^3 = 0.$$

Là encore le point à l'infini $(0:1:0)$ n'est pas un point singulier pour $\overline{\mathcal{C}}_2$, ainsi $\mathbb{P}_1$ est la normalisée de $\overline{\mathcal{C}}_2$. La fibre de $(0:0:1)$ via la normalisation

$$\begin{array}{rccc} \nu : & \mathbb{P}^1 & \longrightarrow & \overline{\mathcal{C}}_2 \\ & (s:t) & \longmapsto & (s^2t : s^3 : t^3) \end{array} \tag{2.16}$$

est constituée par le point rationnel $P = (0:1)$ d'où :

$$Z_{\overline{\mathcal{C}}_2}(T) = Z_{\mathbb{P}^1}(T)\frac{1-T}{1-T} = \frac{1}{(1-qT)(1-T)}.$$

Donc $\overline{\mathcal{C}}_2$ et $\mathbb{P}^1$ ont la même fonction zêta, et, par conséquent, le même nombre de points rationnels sur les différentes extensions de $\mathbb{F}_q$.

Remarque 2.2.3. La fonction zêta d'une courbe, éventuellement singulière, est ainsi donnée par le produit de la fonction zêta de sa normalisée par un produit explicite de polynômes cyclotomiques. Plus précisément, si X est une courbe de genre géométrique g et genre arithmétique π, alors

$$Z_X(T) = \frac{P_X(T)}{(1-T)(1-qT)},$$

où le numérateur $P_X(T) \in \mathbb{Z}[T]$ est le produit d'un polynôme de degré $2g$ (le numérateur de la fonction zêta de sa courbe normalisée) par un polynôme de degré

$$\Delta_X = \sharp\tilde{X}(\overline{\mathbb{F}}_q) - \sharp X(\overline{\mathbb{F}}_q),$$

dont toutes les racines sont des racines de l'unité. Notons que la quantité Δ_X est bien définie, puisque l'ensemble des points singuliers de X est fini, et la fibre de chacun de ces points aussi.

Si $\omega_1, \ldots, \omega_{2g}$ sont les racines inverses de $P_{\tilde{X}}$ et $\beta_1, \ldots, \beta_{\Delta_X}$ les racines inverses de la partie cyclotomique de P_X alors on a :

$$P_X(T) = \prod_{i=1}^{2g}(1-\omega_i T)\prod_{j=1}^{\Delta_X}(1-\beta_j T). \tag{2.17}$$

Il est clair que pour pouvoir arriver à un analogue de la borne de Serre-Weil, il faut trouver une estimation de Δ_X, ce que nous développerons par la suite.

2.2.2 La borne d'Aubry-Perret

Soit $Q \in X(\overline{\mathbb{F}}_q)$. Notons $\alpha_Q(\infty)$ le nombre de points dans la fibre de Q et rationnels sur $\overline{\mathbb{F}}_q$:

$$\alpha_Q(\infty) := \{P \in \tilde{X}(\overline{\mathbb{F}}_q) : P \in \nu^{-1}(Q)\}.$$

On a le lemme suivant :

Lemme 2.2.4. *Soit $Q \in X(\overline{\mathbb{F}}_q)$. Alors*

$$\alpha_Q(\infty) - 1 \leq \delta_Q.$$

Démonstration. Soient $P_1, \ldots, P_{\alpha_Q(\infty)}$ les points de $\tilde{X}(\overline{\mathbb{F}}_q)$ qui sont dans la fibre de Q via la normalisation ν. Soit $\mathcal{O}_Q \subset \overline{\mathbb{F}}_q(X) = \mathbb{F}_q(X) \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ l'anneau local de $X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ en Q et $\overline{\mathcal{O}_Q}$ sa clôture intégrale dans le corps des fonctions $\overline{\mathbb{F}}_q(X)$. On a

$$\overline{\mathcal{O}_Q} = \bigcap_{1 \leq i \leq \alpha_Q(\infty)} \mathcal{O}_{P_i}$$

et

$$\delta_Q = \dim_{\overline{\mathbb{F}}_q} \overline{\mathcal{O}_Q}/\mathcal{O}_Q.$$

Soit ϕ l'application linéaire de $\overline{\mathbb{F}}_q$-espaces vectoriels

$$\begin{array}{rccc} \phi : & \overline{\mathcal{O}_Q} & \to & \overline{\mathbb{F}}_q{}^{\alpha_Q(\infty)} \\ & f & \mapsto & (f(P_i))_{1 \leq i \leq \alpha_Q(\infty)} \end{array}$$

Montrons que ϕ est surjective. Soit $(x_1, \ldots, x_{\alpha_Q(\infty)}) \in \overline{\mathbb{F}}_q{}^{\alpha_Q(\infty)}$ et $f_i = x_i \in \overline{\mathbb{F}}_q \subset \overline{\mathbb{F}}_q(X)$ pour $1 \leq i \leq \alpha_Q(\infty)$. D'après le théorème d'approximation faible [46, Th. 1.3.1], il existe une fonction $g \in \overline{\mathbb{F}}_q(X)$ telle que $v_{P_i}(g - f_i) \geq 1$ pour $1 \leq i \leq \alpha_Q(\infty)$, ou, autrement dit, telle que :

$$g(P_i) = f_i(P_i) = x_i, \text{ pour tout } 1 \leq i \leq \alpha_Q(\infty).$$

Donc $\phi(g) = (x_1, \ldots, x_{\alpha_Q(\infty)})$. De plus, g est régulière en P_i pour $1 \leq i \leq \alpha_Q(\infty)$, et ainsi

$$g \in \bigcap_{1 \leq i \leq \alpha_Q(\infty)} \mathcal{O}_{P_i} = \overline{\mathcal{O}_Q}.$$

Comme $f(P_1) = \cdots = f(P_{\alpha_Q(\infty)})$ pour $f \in \mathcal{O}_Q$, nous avons que $\phi(\mathcal{O}_Q)$ est contenu dans un espace vectoriel $L \subseteq \overline{\mathbb{F}}_q{}^{\alpha_Q(\infty)}$ de dimension 1. Ainsi, l'application linéaire

$$\tilde{\phi} : \overline{\mathcal{O}_Q}/\mathcal{O}_Q \to \overline{\mathbb{F}_q}^{\alpha_Q(\infty)}/L$$

est surjective, et le lemme est prouvé. □

Nous pouvons utiliser le lemme 2.2.4 pour borner $\Delta_X = \sharp\tilde{X}(\overline{\mathbb{F}}_q) - \sharp X(\overline{\mathbb{F}}_q)$.

Proposition 2.2.5. *Soit X une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π, alors*

$$\Delta_X = \sharp\tilde{X}(\overline{\mathbb{F}}_q) - \sharp X(\overline{\mathbb{F}}_q) \leq \pi - g.$$

Démonstration. On a d'après le lemme 2.2.4 :

$$\Delta_X = \sharp\tilde{X}(\overline{\mathbb{F}}_q) - \sharp X(\overline{\mathbb{F}}_q) = \sum_{Q \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} (\alpha_Q(\infty) - 1) \leq \sum_{Q \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \delta_Q = \pi - g.$$

□

Ainsi la quantité Δ_X est bornée par le degré de singularité $\delta = \pi - g$ de X.

On obtient directement de la proposition précédente et de l'équation (2.17) un analogue de la borne de Serre-Weil pour les courbes singulières, que l'on appellera *borne d'Aubry-Perret.*

Corollaire 2.2.6 (Borne d'Aubry-Perret)**.** *Soit X une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π. Soient $\omega_1, \ldots, \omega_{2g}$ les racines inverses de $P_{\tilde{X}}$ (le numérateur de la fonction zêta de $\tilde{X}$) et $\beta_1, \ldots, \beta_{\Delta_X}$ les racines inverses de la partie cyclotomique de P_X (le numérateur de la fonction zêta de X). Alors, pour tout $n \geq 1$, on a*

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n - \sum_{j=1}^{\Delta_X} \beta_j^n. \tag{2.18}$$

En particulier, on a

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}] + \Delta_X \leq g[2\sqrt{q}] + \pi - g \leq \pi[2\sqrt{q}]. \tag{2.19}$$

Remarque 2.2.7. À l'aide de la proposition 1.3.8, on se convainc facilement que

$$|\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \sharp\tilde{X}(\overline{\mathbb{F}}_q) - \sharp X(\overline{\mathbb{F}}_q),$$

d'où

$$|\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g. \tag{2.20}$$

Ainsi, la borne d'Aubry-Perret peut aussi être obtenue de la façon suivante. On considère :

$$\begin{aligned} \pi - g &\geq |\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| = |\sharp\tilde{X}(\mathbb{F}_q) - (q+1) - (\sharp X(\mathbb{F}_q) - (q+1))| \\ &\geq |\sharp\tilde{X}(\mathbb{F}_q) - (q+1)| - |\sharp X(\mathbb{F}_q) - (q+1)|, \end{aligned}$$

et on applique la borne de Serre-Weil (2.7).

Remarque 2.2.8. L'équation (2.18) implique aussi que, si $\tilde{X}$ est la normalisée de X, alors

$$\sharp X(\mathbb{F}_{q^n}) - \sharp\tilde{X}(\mathbb{F}_{q^n}) = -\sum_{j=1}^{\Delta_X} \beta_j^n. \tag{2.21}$$

2.2.3 La quantité $N_q(g,\pi)$

La borne d'Aubry-Perret nous dit que le nombre de points rationnels d'une courbe singulière est borné par une quantité dépendant de ses genres géométrique et arithmétique, ansi que de la cardinalité de son corps de définition. Il est donc naturel d'introduire un analogue de la quantité $N_q(g)$ dans le cas des courbes singulières :

Définition 2.2.9. Soient g et π deux entiers positifs tels que $\pi \geq g$ et q une puissance d'un nombre premier. On définit

$$N_q(g,\pi)$$

comme le nombre maximum de points rationnels d'une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π.

Remarque 2.2.10. Puisque $g = \pi$ si et seulement si la courbe est lisse (voir remarque 1.5.5), nous avons immédiatement

$$N_q(g,g) = N_q(g).$$

Il existe une borne supérieure évidente pour $N_q(g,\pi)$, donnée par la borne d'Aubry-Perret :

$$N_q(g,\pi) \leq q + 1 + g[2\sqrt{q}] + \pi - g. \qquad (A)$$

On peut raffiner la borne (A). En effet, si X est une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π, on a, d'après (2.20) :

$$\sharp X(\mathbb{F}_q) \leq \sharp \tilde{X}(\mathbb{F}_q) + \pi - g \leq N_q(g) + \pi - g,$$

d'où

$$N_q(g,\pi) \leq N_q(g) + \pi - g. \qquad (B)$$

Il est clair que la borne (B) implique la borne (A).

Ainsi, afin de déterminer $N_q(g,\pi)$, nous essayerons dans les chapitres qui viennent de répondre à la question suivante :

Pour quelles valeurs de q, g et π les bornes (A) et (B) sont-elles atteintes ?

Chapitre 3

Une construction de courbes singulières

Dans le Chapitre 2 nous avons introduit la quantité $N_q(g,\pi)$: on rappelle qu'elle est définie comme le nombre maximum de points rationnels d'une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π. Ainsi, le problème de déterminer $N_q(g,\pi)$ amène à construire des courbes singulières de genres et corps de base fixés, ayant « beaucoup » de points rationnels.

La nécessité d'obtenir des courbes d'invariants donnés nous invite à adopter un point de vue inverse par rapport au procédé de désingularisation [1] qui normalement entre en jeu lorsque l'on travaille avec des courbes singulières : nous partirons donc d'une courbe lisse X pour construire une courbe à singularités X', de sorte que X soit la normalisée de X'. De plus, afin d'atteindre nos objectifs sur le nombre de points rationnels et le degré de singularité de la courbe, nous imposerons que les singularités « construites » soient rationnelles sur le corps de base, et du degré de singularité voulu.

La construction présentée dans ce chapitre se base sur les idées développées par Rosenlicht dans [36] et reprises par Serre dans [39, Chap. IV].

Les résultats de ce chapitre apparaissent dans l'article [3].

3.1 Courbes à singularités prescrites

Le résultat suivant servira de point de départ pour la construction qui sera présentée dans la section 3.2. Il montre que dans n'importe quelle classe birationnelle de courbes, il existe une courbe avec un ensemble de singularités prescrites.

Théorème 3.1.1. [36, Th. 5] *Soit K un corps de fonctions algébriques à une variable sur le corps de base k, où k est un corps commutatif quelconque. Si l'on se donne un nombre fini d'anneaux locaux dans K, deux à deux sans place en commun (c'est à dire deux à deux non contenus dans un*

1. Le problème de *désingularisation* ou de *résolution des singularités* d'une variété X consiste, lorsque cela est possible, à trouver une variété non singulière $\tilde{X}$ et une application birationnelle propre de $\tilde{X}$ vers X. Dans le cas des courbes, cela revient à déterminer la courbe normalisée de X.

même anneau de valuation discrète de K), alors il existe un modèle projectif de K/k qui contient les points ayant les anneaux locaux fixés, et qui est non singulier ailleurs.

Nous utiliserons ce résultat pour montrer l'existence de courbes singulières de genres géométrique et arithmétique donnés, ayant un grand nombre de points rationnels. Ainsi, dans un premier temps, nous devons comprendre comment choisir un anneau local dans un corps de fonctions, de telle sorte que le point qui lui est associé soit rationnel et avec un degré de singularité explicite.

On remarque que, en vertu de l'équivalence de catégories entre les corps de fonctions à une variable et les courbes lisses, le fait de se fixer un corps de fonctions à une variable K sur k, correspond à considérer une courbe lisse X définie sur k. Dans le même esprit, faire des opérations sur les anneaux locaux dans K équivaut à faire des opérations sur les points de X.

Grossièrement, nous allons montrer qu'à partir d'un nombre fini de points de X (i.e. d'anneaux de valuation discrète de K) il est possible de « construire » un point (i.e. un anneau local de K) singulier rationnel pour lequel on peut contrôler le degré de singularité.

Soit $k = \mathbb{F}_q$. Soient X une courbe lisse définie sur $\mathbb{F}_q$ de corps de fonctions $K = \mathbb{F}_q(X)$ et $S = \{P_1, \ldots, P_s\}$ un ensemble fini non vide de points fermés de X. Considérons le sous-anneau $\mathcal{O} \subset \mathbb{F}_q(X)$ défini par :

$$\mathcal{O} = \bigcap_{i=1}^{s} \mathcal{O}_{P_i}.$$

L'anneau $\mathcal{O}$ est une intersection finie d'anneaux de valuation discrète, et donc est un anneau semi-local. Ses idéaux maximaux sont précisément les idéaux donnés par $\mathcal{N}_i := \mathcal{M}_{P_i} \cap \mathcal{O}$ pour $i = 1, \ldots, s$ et les corps $\mathcal{O}_{P_i}/\mathcal{M}_{P_i}$ et $\mathcal{O}/\mathcal{N}_i$ sont isomorphes. En outre, $\mathcal{O}$ est un anneau principal [46, Prop. 3.2.10].

Soient $n_1, \ldots, n_s$ des entiers strictement positifs et

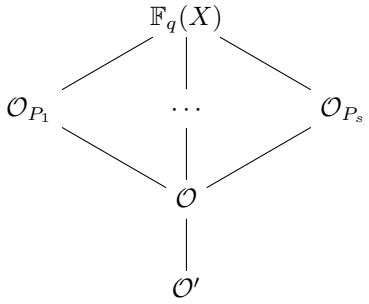
$$\mathcal{N} := \mathcal{N}_1^{n_1} \cdots \mathcal{N}_s^{n_s}.$$

Considérons le sous-anneau $\mathcal{O}' \subseteq \mathcal{O}$ défini par :

$$\mathcal{O}' := \mathbb{F}_q + \mathcal{N}. \tag{3.1}$$

On remarque que, par définition, une fonction dans $\mathcal{O}'$ prend les mêmes valeurs en les points $P_1, \ldots, P_s$.

Nous pouvons illustrer les inclusions précédentes à l'aide du diagramme qui suit :



Proposition 3.1.2. *L'anneau $\mathcal{O}'$ vérifie les propriétés suivantes :*

1. $\mathrm{Frac}(\mathcal{O}') = \mathbb{F}_q(X)$.
2. *$\mathcal{O}$ est la clôture intégrale de $\mathcal{O}'$ (dans $\mathbb{F}_q(X)$).*
3. *$\mathcal{O}'$ est un anneau local d'idéal maximal $\mathcal{N}$ et de corps résiduel $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$. De plus $\mathcal{N}$ est le conducteur de l'extension $\mathcal{O}/\mathcal{O}'$ et, par définition, il contient les fonctions de $\mathcal{O}'$ qui s'annulent en les points $P_1, \ldots, P_s$.*
4. *$\mathcal{O}/\mathcal{O}'$ est un $\mathbb{F}_q$-espace vectoriel tel que*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

Démonstration. 1. On sait, d'après [46, Prop. 3.2.5], que $\mathrm{Frac}(\mathcal{O}) = \mathbb{F}_q(X)$. Il suffit donc de montrer que $\mathcal{O} \subseteq \mathrm{Frac}(\mathcal{O}')$. Puisque $\mathcal{O}$ est un anneau principal, il existe $t \in \mathcal{O}$ tel que $\mathcal{N} = t\mathcal{O}$. Soit donc $x \in \mathcal{O}$. Nous avons $x = \frac{tx^2}{tx}$, de sorte que $x \in \mathrm{Frac}(\mathcal{O}')$.

2. La clôture intégrale $\overline{\mathcal{O}'}$ de $\mathcal{O}'$ est donnée par l'intersection des anneaux de valuation (discrète) de $\mathbb{F}_q(X)$ qui contiennent $\mathcal{O}'$. Donc $\overline{\mathcal{O}'} \subseteq \bigcap_{i=1}^{s} \mathcal{O}_{P_i} = \mathcal{O}$. Par conséquent, il suffit de montrer qu'il n'existe pas d'autres anneaux de valuation contenant $\mathcal{O}'$.

   Soit $\mathcal{O}_P$ un anneau de valuation discrète de $\mathbb{F}_q(X)$ différent de $\mathcal{O}_{P_1}, \ldots, \mathcal{O}_{P_s}$ et soient $v_P, v_{P_1}, \ldots, v_{P_s}$ leurs valuations correspondantes. D'après le théorème d'approximation forte [46, Prop. 1.6.5], il existe un élément $x \in \mathbb{F}_q(X)$ tel que $v_P(x) = -1$ et $v_{P_i}(x) = n_i$ pour tout $i = 1, \ldots, s$. Cela entraîne que $x \in \mathcal{N} \subseteq \mathcal{O}'$ et $x \notin \mathcal{O}_P$. On peut donc conclure que $\overline{\mathcal{O}'} = \mathcal{O}$.

3. On prouve d'abord que $\mathcal{N}$ est un idéal maximal de $\mathcal{O}'$. On a

$$\mathcal{O}' \setminus \mathcal{N} = \{a + n : a \in \mathbb{F}_q^* \text{ et } n \in \mathcal{N}\}.$$

   Si $\mathcal{N}$ n'était pas maximal, par le lemme de Zorn il existerait un idéal maximal $\mathcal{N}'$ tel que $\mathcal{N} \subsetneq \mathcal{N}' \subsetneq \mathcal{O}'$ [2, Cor. 1.4]. Soit $x \neq 0$ un élément de $(\mathcal{O}' \setminus \mathcal{N}) \cap \mathcal{N}'$. Alors $x = a + n$, avec $a \in \mathbb{F}_q^*$ et $n \in \mathcal{N}$. Ainsi $a = x - n \in \mathcal{N}'$ et $\mathcal{N}' = \mathcal{O}'$, ce qui est contradictoire.

   Montrons maintenant que $\mathcal{N}$ est l'unique idéal maximal de $\mathcal{O}'$. S'il existait un autre idéal maximal dans $\mathcal{O}'$, d'après le théorème du Going Up [2, Th. 5.10], il serait la restriction

d'un idéal maximal de $\mathcal{O}$. Or, pour tout $i = 1, \ldots, s$, on a $\mathcal{N} \subseteq (\mathcal{N}_i \cap \mathcal{O}')$ et, puisque $\mathcal{N}$ est un idéal maximal de $\mathcal{O}'$, on obtient $\mathcal{N} = \mathcal{N}_i \cap \mathcal{O}'$. On en conclut que $\mathcal{N}$ est l'unique idéal maximal de $\mathcal{O}'$, et $\mathcal{O}'$ est ainsi un anneau local. Il est évident que $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.
De plus, puisque $\mathcal{N}$ est à la fois un idéal de $\mathcal{O}$ et un idéal maximal de $\mathcal{O}'$, il est le conducteur de l'extension $\mathcal{O}/\mathcal{O}'$.

4. En procédant de la même manière que dans la remarque 1.4.3, d'après le troisième théorème d'isomorphisme des modules on a :

$$\mathcal{O}/\mathcal{O}' \cong \frac{\mathcal{O}/\mathcal{N}}{\mathcal{O}'/\mathcal{N}}.$$

En outre :

$$\mathcal{O}/\mathcal{N} = \frac{\mathcal{O}}{\mathcal{N}_1^{n_1} \cdots \mathcal{N}_s^{n_s}} \cong \prod_{i=1}^{s} \left(\frac{\mathcal{O}_{P_i}}{\mathcal{M}_{P_i}} \right)^{n_i}$$

est un isomorphisme de $\mathbb{F}_q$-espaces vectoriels. Ainsi

$$\dim_{\mathbb{F}_q} \mathcal{O}/\mathcal{N} = \sum_{i=1}^{s} n_i \deg P_i,$$

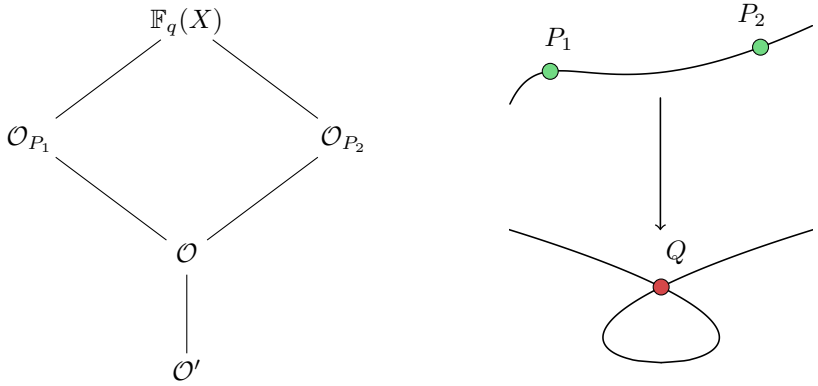
et donc

$$\dim_{\mathbb{F}_q} \mathcal{O}/\mathcal{O}' = \dim_{\mathbb{F}_q} \mathcal{O}/\mathcal{N} - \dim_{\mathbb{F}_q} \mathcal{O}'/\mathcal{N} = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

□

Les opérations sur les anneaux de valuation discrète contenus dans $\mathbb{F}_q(X)$ correspondent à des opérations sur les points de X : grossièrement, le fait de « pincer » ensemble les anneaux de valuation discrète $\mathcal{O}_{P_1}, \ldots, \mathcal{O}_{P_s}$ dans l'anneau local $\mathcal{O}'$ correspond à « pincer » ensemble les points non singuliers $P_1, \ldots, P_s$ dans un point singulier rationnel. De cette façon, en partant d'une courbe lisse X, nous définissons une courbe « pincée » X' qui est birégulièrement équivalente à X sauf en les points $P_1, \ldots, P_s$, et pour laquelle les points non singuliers $P_1, \ldots, P_s$ sont « remplacés » par un point singulier rationnel Q d'un degré de singularité explicite.

Pour $s = 2$, on pourrait visualiser cette correspondance de la façon suivante :



Formellement :

Théorème 3.1.3. *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$ et soient $P_1, \ldots, P_s$ des points de X. Soient $n_1, \ldots, n_s$ des entiers strictement positifs. Considérons l'anneau local $\mathcal{O}'$ défini comme dans (3.1).*

Alors il existe une courbe X' définie sur $\mathbb{F}_q$ ayant X pour normalisée, et dont l'unique point singulier Q_0 a pour anneau local associé $\mathcal{O}'$. De plus, Q_0 est un point rationnel de degré de singularité $\sum_{i=1}^{s} n_i \deg P_i - 1$ et X' est de genre arithmétique $g + \sum_{i=1}^{s} n_i \deg P_i - 1$.

Démonstration. L'existence de la courbe X' découle du théorème 3.1.1, mais l'approche de Serre dans [39, Chap. IV] permettra de mieux comprendre sa construction.

Soit $S = \{P_1, \ldots, P_s\}$. Considérons sur X la relation d'équivalence $\sim$ définie comme suit. Soient $P, Q \in X$, on pose

$$P \sim Q \Longleftrightarrow P \in S \text{ et } Q \in S, \text{ ou } P = Q.$$

On définit X' comme l'ensemble quotient $X/\sim$. On a donc une projection canonique

$$p : X \longrightarrow X'.$$

Pour $Q_0 = p(S)$, on définit $\mathcal{O}'_{Q_0} := \mathcal{O}'$. Si $Q \in X' \setminus \{Q_0\}$ et $Q = p(P)$, on pose $\mathcal{O}'_Q := \mathcal{O}_P$. Alors, pour $Q \in X'$, les $\mathcal{O}'_Q$ forment un sous-faisceau du faisceau des fonctions de X' sur $\mathbb{F}_q$, que l'on notera $\mathcal{O}_{X'}$.

D'après [39, Prop. 2 Chap. IV] le faisceau $\mathcal{O}_{X'}$ munit l'ensemble X' d'une structure de courbe algébrique définie sur $\mathbb{F}_q$, ayant X pour normalisée, et $\{Q_0\}$ comme ensemble de points singuliers. Ainsi, le genre géométrique de X' est égal à g. La rationalité de Q_0, son degré de singularité et le genre arithmétique de X' découlent de la proposition 3.1.2 et de la définition du genre arithmétique. □

Remarque 3.1.4.

1. Nous remarquons que, par construction, la courbe X' a un nombre de points rationnels donné par

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) - \sharp\{P_i, i = 1, \ldots, s \text{ tels que } P_i \text{ est rationnel sur } \mathbb{F}_q\} + 1.$$

   Ainsi, si aucun des points P_i de départ n'est rationnel, la courbe X' aura un point rationnel supplémentaire par rapport à X. Néanmoins, au cours de la construction, on augmente également le degré de singularité et par conséquent le genre arithmétique de la courbe.

2. Une simple conséquence du théorème 3.1.3 est que pour tout couple d'entiers positifs (g, π) tels que $g \leq \pi$, il existe une courbe de genre géométrique g et genre arithmétique π. Pour cela, il suffit de partir d'une courbe lisse de genre g ayant au moins un point rationnel P et de poser $\mathcal{O}' := \mathbb{F}_q + \mathcal{M}_P^{\pi-g+1}$, où $\mathcal{M}_P$ est l'idéal maximal de $\mathcal{O}_P$.

3. Dans le théorème 3.1.3 nous nous limitons à la construction d'une courbe avec une seule singularité, mais rien ne nous empêche de construire plusieurs singularités en même temps, en se donnant un nombre fini d'anneaux locaux dans $\mathbb{F}_q(X)$, deux à deux sans places en commun. On peut alors aisément modifier la preuve du théorème, en définissant la bonne

relation d'équivalence sur les points de X, et en associant les bons anneaux locaux aux différentes classes d'équivalences de points rationnels.

Ainsi le théorème entraîne aussi que, sans restriction imposée sur le genre arithmétique, on peut construire des courbes singulières ayant un nombre arbitrairement grand de points.

4. L'inconvénient de cette construction, qui résulte du fait de travailler dans un corps de fonctions, est qu'il n'est a priori pas si simple de déterminer la dimension minimale de l'espace projectif dans lequel la courbe X' est plongée.

   Cette dimension n'est pas en général la même que celle de X. Par exemple, si nous partons de la droite projective $X = \mathbb{P}^1$ définie sur $\mathbb{F}_q$, nous pouvons construire une courbe X' avec $q+2$ points rationnels et qui donc ne se plonge pas dans $\mathbb{P}^1$.

   D'autre part, si X est une courbe lisse plongée dans un espace projectif $\mathbb{P}^n$, alors une autre obstruction au plongement d'une pincée X' de X dans $\mathbb{P}^n$ est la dimension de l'espace tangent en un point singulier.

Le cas particulier de la proposition 3.1.2 dans lequel S est le singleton $\{P\}$ sera crucial dans la section suivante :

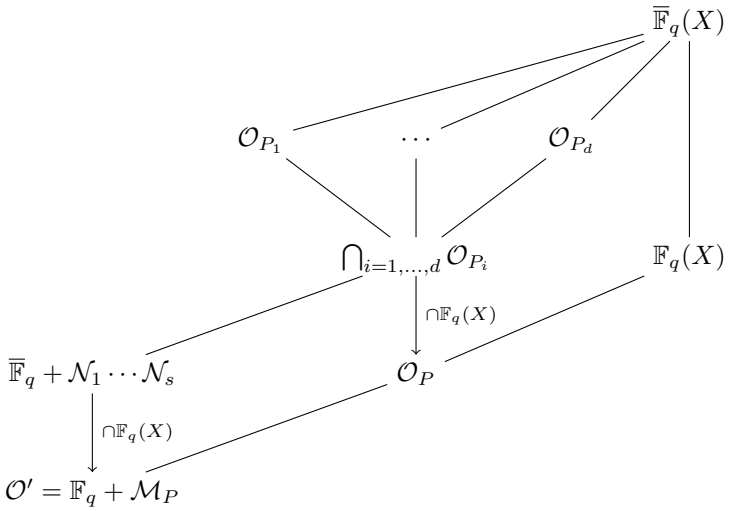
Corollaire 3.1.5. *Soit X une courbe lisse de corps de fonctions $\mathbb{F}_q(X)$ et P un point de X. Considérons $\mathcal{O}_P$, l'anneau local de X en P, d'idéal maximal $\mathcal{M}_P$. Alors l'anneau*

$$\mathcal{O}' := \mathbb{F}_q + \mathcal{M}_P \tag{3.2}$$

est un anneau local contenu dans $\mathcal{O}_P$, d'idéal maximal $\mathcal{M}_P$, et tel que $[\mathcal{O}'/\mathcal{M}_P : \mathbb{F}_q] = 1$. En outre, $\mathcal{O}_P$ est la clôture intégrale de $\mathcal{O}'$ et $\mathcal{O}_P/\mathcal{O}'$ est un $\mathbb{F}_q$-espace vectoriel de dimension $\deg P - 1$.

Remarque 3.1.6. Nous remarquons que l'anneau $\mathcal{O}'$, défini comme dans le corollaire 3.1.5, est le plus grand (pour l'inclusion) anneau local contenu dans $\mathcal{O}_P$ tel que $[\mathcal{O}'/\mathcal{M}_P : \mathbb{F}_q] = 1$. En effet, soit $\mathcal{O}''$ un anneau local contenu dans $\mathcal{O}_P$, d'idéal maximal $\mathcal{M}''$ et tel que $[\mathcal{O}''/\mathcal{M}'' : \mathbb{F}_q] = 1$. Puisque $\mathcal{O}''/\mathcal{M}'' \cong \mathbb{F}_q$, tout élément x dans $\mathcal{O}''$ est de la forme $x = a + m$, avec $a \in \mathbb{F}_q$ et $m \in \mathcal{M}''$. Ainsi $\mathcal{O}'' = \mathbb{F}_q + \mathcal{M}''$. Or, $\mathcal{M}'' = \mathcal{M}_P \cap \mathcal{O}'' \subseteq \mathcal{M}_P$ et par conséquent $\mathcal{O}'' \subseteq \mathcal{O}'$.

Remarque 3.1.7. Lorsque l'on part d'un ensemble constitué d'un seul point fermé, ce qui est le cas du corollaire 3.1.5, le « pincement » effectué sur X devient « visible » si l'on regarde la situation dans $X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Nous illustrerons cela par le dessin suivant, dans lequel on suppose que le point P est de degré d et que $P = \{P_1, \ldots, P_d\}$ avec $P_i \in X(\overline{\mathbb{F}}_q)$:



3.2 Nombre de points rationnels versus genre arithmétique

Nous allons utiliser le théorème 3.1.3 pour étudier la quantité $N_q(g, \pi)$. L'idée est de partir d'une courbe lisse X pour construire une courbe X' de genre géométrique g et genre arithmétique π, dont X est la normalisée, en maximisant le nombre de points rationnels de X'. Il est clair que X doit être choisie parmi les courbes lisses de genre g. De plus, puisque chaque rajout d'un point rationnel implique une augmentation du genre arithmétique, le choix des points de X à « pincer » devra être fait pour que cette augmentation soit minimale.

Nous avons le résultat suivant.

Théorème 3.2.1. *Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$. Soit π un entier de la forme*

$$\pi = g + a_2 + 2a_3 + 3a_4 + \cdots + (n-1)a_n,$$

avec $0 \leq a_i \leq B_i(X)$, où $B_i(X)$ désigne le nombre de points fermés de degré i de la courbe X. Alors il existe une courbe X' définie sur $\mathbb{F}_q$ de genre arithmétique π, ayant X pour normalisée, et telle que

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + a_2 + a_3 + a_4 + \cdots + a_n. \tag{3.3}$$

Démonstration. Pour tout $i \in \{2, \ldots, n\}$, considérons a_i points fermés de degré i de X : $P_1^{(i)}, P_2^{(i)}, \ldots, P_{a_i}^{(i)}$. Ainsi nous obtenons un sous-ensemble $S = \{P_j^{(i)}, 2 \leq i \leq n,\ 1 \leq j \leq a_i\}$ de cardinalité $|S| = a_2 + a_3 + \cdots + a_n$.

Pout tout $P \in S$ on pose $\mathcal{O}'_P := \mathbb{F}_q + \mathcal{M}_P$. D'après le corollaire 3.1.5, nous avons que $\mathcal{O}'_P$ est un anneau local d'idéal maximal $\mathcal{M}_P$ et $[\mathcal{O}'_P/\mathcal{M}_P : \mathbb{F}_q] = 1$. De plus, $\mathcal{O}_P$ est la clôture intégrale de $\mathcal{O}'_P$ et $\mathcal{O}_P/\mathcal{O}'_P$ est un $\mathbb{F}_q$-espace vectoriel de dimension $\deg P - 1$.

Par le théorème 3.1.3, il existe une courbe X' définie sur $\mathbb{F}_q$, ayant X pour courbe normalisée, et telle que :

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + a_2 + a_3 + a_4 + \cdots + a_n.$$

En outre :

$$\pi = g + \sum_{P \in S} \dim_{\mathbb{F}_q} \mathcal{O}_P/\mathcal{O}'_P = g + \sum_{2 \leq i \leq n} \sum_{1 \leq j \leq a_i} (\deg P_j^{(i)} - 1) = g + \sum_{2 \leq i \leq n} \sum_{1 \leq j \leq a_i} (i-1),$$

et donc :

$$\pi = g + \sum_{2 \leq i \leq n} (i-1)a_i.$$

□

Remarque 3.2.2. En d'autres termes, le théorème 3.2.1 montre qu'il est possible de « transformer » un point de degré d d'une courbe lisse en un point singulier rationnel, à condition d'augmenter la valeur du genre arithmétique de $d-1$.

Remarque 3.2.3. La construction décrite dans la preuve du théorème 3.2.1 est « optimale », dans le sens qu'en faisant les bons choix sur l'ensemble S de points de X, elle permet de trouver, parmi les courbes de normalisée X, celles qui maximisent le nombre de points rationnels par rapport à leur genre arithmétique. Plus précisement, si Y_1 est une courbe définie sur $\mathbb{F}_q$ de genre géométrique g, genre arithmétique π et avec N points rationnels et si $\tilde{Y}$ est sa normalisée, alors il existe une courbe Y_2 construite comme dans la démonstration du théorème 3.2.1 de genre arithmétique $\pi' \leq \pi$, avec $N' \geq N$ points rationnels et dont la normalisée est $\tilde{Y}$. En effet d'après la remarque 3.1.6, puisque $\mathcal{O}'_P$ est le plus grand anneau local contenu dans $\mathcal{O}_P$ tel que $[\mathcal{O}'_P/\mathcal{M}_P : \mathbb{F}_q] = 1$, on a que tout point de S est « remplacé » par un point singulier rationnel dont le degré de singularité est le plus petit possible.

En réécrivant l'équation (3.3) sous la forme :

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + \pi - g - (a_3 + 2a_4 + \cdots + (n-2)a_n),$$

on s'aperçoit que les points de degré 2 d'une courbe lisse jouent un rôle clé pour l'étude de la quantité $N_q(g, \pi)$, car ce sont les seuls qui permettent d'augmenter le nombre de points rationnels d'autant que le degré de singularité. On a aussi l'impression que pour obtenir une courbe avec un grand nombre de points rationnels et de petit genre arithmétique, il vaut mieux partir d'une courbe lisse X ayant déjà beaucoup de points rationnels.

Nous développerons ces idées formellement dans le chapitre suivant.

Nous terminons ce chapitre en montrant que le théorème 3.1.3 permet de donner une borne inférieure pour la quantité $N_q(g, \pi)$.

Proposition 3.2.4. *Soient q une puissance d'un nombre premier, g et π deux entiers positifs tels que $\pi \geq g$. Alors on a :*

$$N_q(g, \pi) \geq N_q(g).$$

Démonstration. Soit X une courbe lisse de genre g définie sur $\mathbb{F}_q$ avec $N_q(g)$ points rationnels, et soit P un point rationnel de X. Considérons l'anneau local

$$\mathcal{O}' := \mathbb{F}_q + (\mathcal{M}_P)^{\pi - g + 1}.$$

D'après le théorème 3.1.3, il existe une courbe X' définie sur $\mathbb{F}_q$, ayant X pour normalisée, et possédant un point singulier rationnel Q d'anneau local $\mathcal{O}'$. Ainsi $\sharp X(\mathbb{F}_q) = \sharp X'(\mathbb{F}_q) = N_q(g)$ et X' est de genre géométrique g et de genre arithmétique donné par $g + \pi - g + 1 - 1 = \pi$. Il s'ensuit que $N_q(g, \pi) \geq N_q(g)$. □

Chapitre 4

Courbes optimales, δ-optimales et maximales

Le Chapitre 2 se terminait sur les bornes supérieures suivantes pour $N_q(g,\pi)$:

$$N_q(g,\pi) \leq q+1+g[2\sqrt{q}]+\pi-g, \tag{A}$$

$$N_q(g,\pi) \leq N_q(g)+\pi-g. \tag{B}$$

et laissait en suspens la question :

Pour quelles valeurs de q, g et π les bornes (A) et (B) sont-elles atteintes ?

Or, on se rend facilement compte que, si la borne (B) est atteinte, alors la borne (A) est atteinte si et seulement si $N_q(g) = q+1+g[2\sqrt{q}]$, ou, autrement dit, s'il existe une courbe lisse maximale de genre g définie sur $\mathbb{F}_q$. Ainsi, dans un premier temps nous porterons notre attention sur les conditions d'existence de courbes atteignant la borne (B), et que nous appellerons *courbes δ-optimales*. Les résultats obtenus permettront ainsi d'étudier les propriétés des courbes qui atteignent (A) et qui seront dites *courbes maximales*.

Les résultats de ce chapitre sont contenus dans les articles [3] et [4].

4.1 Définitions

Il est naturel d'introduire le vocabulaire suivant :

Définition 4.1.1. Soit X une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et de genre arithmétique π. On dit que X est une

(i) *courbe optimale* si

$$\sharp X(\mathbb{F}_q) = N_q(g,\pi)\ ;$$

(ii) *courbe δ-optimale* si

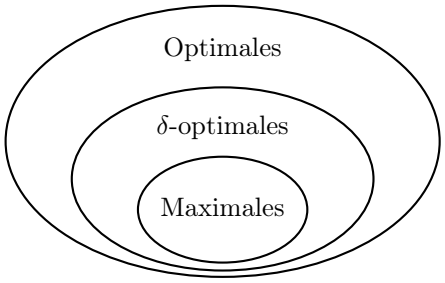
$$\sharp X(\mathbb{F}_q) = N_q(g)+\pi-g\ ;$$

(iii) *courbe maximale* si

$$\sharp X(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}] + \pi - g.$$

En particulier nous retrouvons les définitions usuelles de courbe optimale et maximale lorsque X est lisse (voir la sous-section 2.1.4 pour les rappels).

Il est aussi évident qu'une courbe maximale est δ-optimale, et qu'une courbe δ-optimale est optimale. Ainsi, nous avons les inclusions d'ensembles suivantes :



Remarque 4.1.2. Le choix du terme « courbe δ-optimale » se justifie par le fait qu'une courbe δ-optimale de genre géométrique g et genre arithmétique π possède autant de points supplémentaires que son degré de singularité $\delta = \pi - g$ par rapport à une courbe optimale lisse de genre g.

4.1.1 La courbe maximale de Fukasawa, Homma et Kim

Un exemple non trivial de courbe singulière maximale a été donné en 2011 par Fukasawa, Homma et Kim dans [14]. Nous reproduisons leur exemple ci-dessous.

Considérons la courbe plane B définie comme l'image de l'application

$$\begin{array}{rccc} \nu : & \mathbb{P}^1 & \to & \mathbb{P}^2 \\ & (s:t) & \mapsto & (s^{q+1} : s^q t + s t^q : t^{q+1}). \end{array}$$

L'application ν est birationnelle, de degré $q+1$ et définie sur $\mathbb{F}_q$. Il en découle que B est une courbe plane rationnelle, de degré $q+1$ et définie sur $\mathbb{F}_q$. En particulier, B a pour courbe normalisée la droite projective $\mathbb{P}^1$, et ses genres géométrique et arithmétique sont donnés respectivement par $g = 0$ et $\pi = q(q-1)/2$.

On rappelle quelques propriétés intéressantes de B (pour la preuve voir [14, Th. 2.2]).

1. Pour tout point singulier Q de B on a $\nu^{-1}(Q) = \{P, P^\varphi\}$, où $P \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ et φ est l'automorphisme de Frobenius. Réciproquement, si $P \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ alors $\nu(P)$ est singulier pour X. Autrement dit, $Q \in \mathrm{Sing}(X)$ si et seulement si $\nu^{-1}(Q)$ est un point de degré de 2. Ainsi la courbe B a $q(q-1)/2$ points singuliers :

$$\sharp\,\mathrm{Sing}(B) = B_2(\mathbb{P}_1) = \frac{\sharp\mathbb{P}^1(\mathbb{F}_{q^2}) - \sharp\mathbb{P}^1(\mathbb{F}_q)}{2} = \frac{q^2 + 1 - (q-1)}{2} = \frac{q^2 - q}{2}.$$

2. Tout point singulier de B est de degré de singularité 1, car le degré de singularité de B est égal au nombre de points singuliers.

3. Tous les points singuliers de B sont rationnels sur $\mathbb{F}_q$: $\mathrm{Sing}(B) \subseteq B(\mathbb{F}_q)$.

4. Puisque l'image de tout point rationnel de $\mathbb{P}^1$ reste non singulière et rationnelle dans B, le nombre de points rationnels sur $\mathbb{F}_q$ de B est donné par $\sharp\mathbb{P}^1(\mathbb{F}_q) + \sharp\,\mathrm{Sing}(B)$:

$$\sharp B(\mathbb{F}_q) = q + 1 + \frac{q^2 - q}{2}.$$

Il s'ensuit que la courbe B réalise la borne d'Aubry-Perret, ainsi les bornes (A) et (B) sont atteintes pour $g = 0$ et $\pi = q(q-1)/2$:

$$N_q\left(0, \frac{q^2 - q}{2}\right) = q + 1 + \frac{q^2 - q}{2}.$$

On peut calculer explicitement la fonction zêta de B. D'après l'équation (2.13), elle est donnée par :

$$\frac{(1+T)^{\frac{q^2-q}{2}}}{(1-T)(1-qT)}.$$

De plus, puisque $\mathbb{P}^1$ est birégulièrement équivalente à B en dehors de l'ensemble $\mathbb{P}^1(\mathbb{F}_{q^2})\backslash\mathbb{P}^1(\mathbb{F}_q)$, on obtient que B n'a pas de points de degré 2. Ainsi, la courbe B a été obtenue en « pinçant » tous les points de degré 2 de la droite projective (sa normalisée) en des « nouveaux » points rationnels. On retrouve, donc, que les points de degré 2 jouent un rôle important dans l'existence de courbes qui atteignent la borne d'Aubry-Perret.

Nous verrons dans la section suivante comment la plupart des propriétés de B, listées ci-dessus, sont vérifiées plus généralement pour une courbe δ-optimale quelconque.

Remarque 4.1.3. La courbe B étant plane, il est possible de déterminer simplement son équation affine, à partir de la paramétrisation

$$\begin{array}{rccc} \nu : & \mathbb{A}^1 & \to & \mathbb{A}^2 \\ & t & \mapsto & (t^{q+1}, t^q + t). \end{array}$$

En effet, une équation est donnée par $R(X, Y) = 0$, où $R \in \mathbb{F}_q[X, Y]$ est un polynôme non nul qui est le résultant des deux polynômes en t : $X - t^{q+1}$ et $Y - (t^q + t)$.

Selon la valeur de q, on obtient ainsi différentes équations affines de B. Nous en listons quelques unes :

$$\begin{array}{lcl} q = 2 & \to & Y^3 + X^2 + XY + X \\ q = 2^2 & \to & Y^5 + X^4 + XY^3 + X^2Y + X \\ q = 2^3 & \to & Y^9 + X^8 + XY^7 + X^2Y^5 + X^4Y + X \\ q = 2^4 & \to & Y^{17} + X^{16} + XY^{15} + X^2Y^{13} + X^4Y^9 + X^8Y + X \\ q = 3 & \to & 2Y^4 + X^3 + XY^2 + X^2 + X \\ q = 3^2 & \to & 2Y^{10} + X^9 + XY^8 + X^2Y^6 + 2X^3Y^4 + 2X^4Y^2 + 2X^5 + X \\ q = 5 & \to & 4Y^6 + X^5 + XY^4 + X^2Y^2 + 2X^3 + X \end{array}$$

4.2 Propriétés des courbes δ-optimales

Nous énonçons dans le théorème suivant quelques propriétés des courbes δ-optimales.

Théorème 4.2.1. *Soit X une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π. Soit $\tilde{X}$ la courbe normalisée de X et $\nu : \tilde{X} \to X$ une application de normalisation. Alors, si X est δ-optimale, i.e. si*

$$\sharp X(\mathbb{F}_q) = N_q(g) + \pi - g,$$

on a :

1. *$\tilde{X}$ est une courbe lisse optimale ;*
2. *X a $\pi - g$ points singuliers, tous rationnels et de degré de singularité 1 ;*
3. *si Q est un point singulier de X alors $\nu^{-1}(Q) = \{P\}$, où P est un point de degré 2 de $\tilde{X}$;*
4. *$\pi - g \leq B_2(\tilde{X})$;*
5. *$Z_X(T) = Z_{\tilde{X}}(T)(1+T)^{\pi-g}$.*

Démonstration. 1. Si $\tilde{X}$ n'était pas une courbe lisse optimale, à savoir $\sharp\tilde{X}(\mathbb{F}_q) < N_q(g)$, alors on aurait $\sharp X(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q) > \pi - g$, ce qui contredit (2.20).

2. Il découle du point 1 que :

$$\sharp X(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q) = \pi - g.$$

D'autre part, on a :

$$\sharp X(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q) \leq \sharp \operatorname{Sing} X(\mathbb{F}_q) \leq \sharp \operatorname{Sing} X(\overline{\mathbb{F}}_q) \leq \pi - g.$$

Ainsi

$$\sharp \operatorname{Sing} X(\mathbb{F}_q) = \sharp \operatorname{Sing} X(\overline{\mathbb{F}}_q) = \pi - g.$$

En particulier, cela signifie que tous les points singuliers de X sont rationnels sur $\mathbb{F}_q$.

De plus, puisque

$$\pi - g = \sum_{Q \in \operatorname{Sing} X} \delta_Q,$$

nous trouvons $\delta_Q = 1$ pour tout $Q \in \operatorname{Sing} X$.

3. Considérons la fonction zêta de X, qui, d'après (2.13), est donnée par :

$$Z_X(T) = Z_{\tilde{X}}(T) \prod_{Q \in \operatorname{Sing} X} \left(\frac{\prod_{P \in \nu^{-1}(Q)} (1 - T^{\deg P})}{1 - T} \right). \tag{4.1}$$

Or, en utilisant (2.21), on obtient

$$\pi - g = \sharp X(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q) = -\sum_{j=1}^{\Delta_X} \beta_j,$$

ce qui donne $\Delta_X = \pi - g$ et $\beta_j = -1$ pour tout $j = 1, \ldots, \Delta_X$. Ainsi,

$$\prod_{Q \in \mathrm{Sing}\, X} \left(\frac{\prod_{P \in \nu^{-1}(Q)} (1 - T^{\deg P})}{1 - T} \right) = (1+T)^{\pi - g}. \tag{4.2}$$

En particulier, pour tout $Q \in \mathrm{Sing}(X)$, on a

$$\frac{\prod_{P \in \nu^{-1}(Q)} (1 - T^{\deg P})}{1 - T} = 1 + T,$$

d'où $\nu^{-1}(Q) = \{P\}$ avec $\deg P = 2$.

4. Du point 3 on obtient immédiatement que $\sharp \,\mathrm{Sing}\, X \leq B_2(\tilde{X})$, ce qui implique, avec le point 2, l'inégalité $\pi - g \leq B_2(\tilde{X})$.

5. La forme de la fonction zêta $Z_X(T)$ de X découle directement de (4.1) et (4.2).

□

4.3 Théorèmes d'existence de courbes δ-optimales

Nous allons combiner les résultats du théorème 4.2.1 et du théorème 3.2.1 pour obtenir des conditions (respectivement) nécessaires et suffisantes pour l'existence de courbes δ-optimales.

En effet, d'un côté, le théorème 3.2.1 permet de construire, à partir d'une courbe lisse optimale X, une courbe δ-optimale X', pour laquelle la différence entre le nombre de ses points rationnels et ceux de sa normalisée est exactement égal à son degré de singularité : il suffit d'impliquer dans la construction les seuls points de degré 2 de X.

D'autre part, le théorème 4.2.1 montre que ceci est l'unique manière d'obtenir une courbe δ-optimale.

Or, le nombre de points de degré 2 d'une courbe est fini, et, de plus, « assez petit » pour une courbe lisse optimale, et parfois même égal à zéro. Cela contraint l'existence de courbes δ-optimales de genre arithmétique arbitrairement grand.

Pour toutes ces raisons, il est naturel d'introduire la notation suivante.

Notations. Nous notons

$$\mathcal{X}_q(g)$$

l'ensemble des courbes lisses optimales définies sur $\mathbb{F}_q$ de genre g. Nous définissons alors

$$B_2(\mathcal{X}_q(g))$$

comme le nombre maximum de points de degré 2 d'une courbe de $\mathcal{X}_q(g)$.

Théorème 4.3.1. *On a :*

$$N_q(g, \pi) = N_q(g) + \pi - g \iff g \leq \pi \leq g + B_2(\mathcal{X}_q(g)).$$

Démonstration. Soit X une courbe de $\mathcal{X}_q(g)$, ayant $B_2(\mathcal{X}_q(g))$ points de degré 2. Soit π un entier de la forme $\pi = g + a_2$ avec $0 \leq a_2 \leq B_2(X) = B_2(\mathcal{X}_q(g))$. Alors, d'après le théorème 3.2.1, il existe une courbe X' définie sur $\mathbb{F}_q$ de genre arithmétique π, ayant X pour normalisée et telle que

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + a_2 = N_q(g) + a_2.$$

Ainsi, pour tout $g \leq \pi \leq g + B_2(\mathcal{X}_q(g))$, on a $N_q(g, \pi) = N_q(g) + \pi - g$.

L'implication réciproque découle du point 4 du théorème 4.2.1. □

Dans le cas où $g = 0$, c'est-à-dire celui des courbes rationnelles, le théorème 4.3.1 prend la forme du corollaire suivant :

Corollaire 4.3.2. *On a*

$$N_q(0, \pi) = q + 1 + \pi$$

si et seulement si $0 \leq \pi \leq \frac{q^2-q}{2}$.

Démonstration. Puisque toute courbe dans $\mathcal{X}_q(0)$ est isomorphe à la droite projective $\mathbb{P}^1$, la quantité $B_2(\mathcal{X}_q(g))$ correspond au nombre de points de degré 2 de $\mathbb{P}^1$, qui est donné, d'après la formule (1.3), par

$$B_2(\mathbb{P}^1) = \frac{\sharp\mathbb{P}^1(\mathbb{F}_{q^2}) - \sharp\mathbb{P}^1(\mathbb{F}_q)}{2} = \frac{q^2 + 1 - (q+1)}{2} = \frac{q^2 - q}{2}.$$

□

Remarque 4.3.3. La courbe de Fukasawa, Homma et Kim, décrite dans la sous-section 4.1.1, est un exemple explicite de courbe rationnelle singulière qui atteint $N_q\left(0, \frac{q^2-q}{2}\right)$.

Le corollaire précédent montre, plus généralement, qu'il existe une courbe rationnelle δ-optimale définie sur $\mathbb{F}_q$ et de genre arithmétique π pour tout $0 \leq \pi \leq \frac{q^2-q}{2}$.

Considérons maintenant le cas $g = 1$. On a rappelé dans le théorème 2.1.15 que la quantité $N_q(1)$ vaut soit $q + 1 + [2\sqrt{q}]$, soit $q + [2\sqrt{q}]$. Elle vaut $q + 1 + [2\sqrt{q}]$ si et seulement si au moins une des conditions suivantes est vérifiée : p ne divise pas $[2\sqrt{q}]$, q est un carré, ou $q = p$.

Ainsi le théorème 4.3.1 entraîne le corollaire suivant.

Corollaire 4.3.4. *1. Si p ne divise pas $[2\sqrt{q}]$, q est un carré, ou $q = p$ on a :*

$$N_q(1, \pi) = q + 1 + [2\sqrt{q}] + \pi - 1$$

si et seulement si $1 \leq \pi \leq 1 + \frac{q^2+q-[2\sqrt{q}]([2\sqrt{q}]+1)}{2}$.

2. Dans les autres cas, on a

$$N_q(1, \pi) = q + [2\sqrt{q}] + \pi - 1$$

si et seulement si $1 \leq \pi \leq 1 + \frac{q^2+q+[2\sqrt{q}](1-[2\sqrt{q}])}{2}$.

Démonstration. 1. Dans le premier cas, on a $N_q(1) = q + 1 + [2\sqrt{q}]$. Soit X une courbe lisse de genre 1 définie sur $\mathbb{F}_q$ avec $q + 1 + [2\sqrt{q}]$ points rationnels. Si l'on note ω et $\overline{\omega}$ les racines

inverses du numérateur de la fonction zêta de X, alors on obtient, d'après la formule (2.5) :

$$\sharp X(\mathbb{F}_q) = q + 1 + [2\sqrt{q}] = q + 1 - (\omega + \overline{\omega}), \tag{4.3}$$

et

$$\sharp X(\mathbb{F}_{q^2}) = q^2 + 1 - (\omega^2 + \overline{\omega}^2).$$

De (4.3) nous obtenons $\omega + \overline{\omega} = -[2\sqrt{q}]$. Puisque ω est de module $\sqrt{q}$, on a aussi :

$$\omega^2 + \overline{\omega}^2 = (\omega + \overline{\omega})^2 - 2\omega\overline{\omega} = (\omega + \overline{\omega})^2 - 2|\omega|^2 = [2\sqrt{q}]^2 - 2q,$$

ce qui donne

$$\sharp X(\mathbb{F}_{q^2}) = q^2 + 1 - ([2\sqrt{q}]^2 - 2q).$$

De cette façon, nous obtenons que, pour toute courbe maximale lisse de genre 1 définie sur $\mathbb{F}_q$, le nombre de points de degré 2 est égal à :

$$B_2(\mathcal{X}_q(1)) = B_2(X) = \frac{\sharp X(\mathbb{F}_{q^2}) - \sharp X(\mathbb{F}_q)}{2} = \frac{q^2 + q - [2\sqrt{q}]([2\sqrt{q}] + 1)}{2}.$$

La conclusion découle du théorème 4.3.1.

2. Dans ce cas on a $N_q(1) = q + [2\sqrt{q}]$. En utilisant un raisonnement similaire, on obtient $\omega + \overline{\omega} = 1 - [2\sqrt{q}]$ et $\omega^2 + \overline{\omega}^2 = [2\sqrt{q}]^2 - 2[2\sqrt{q}] - 2q + 1$, d'où

$$B_2(\mathcal{X}_q(1)) = \frac{q^2 + q + [2\sqrt{q}](1 - [2\sqrt{q}])}{2}.$$

□

Remarque 4.3.5. Puisque pour $q = 2, 3$ ou 4 la quantité

$$\frac{q^2 + q - [2\sqrt{q}]([2\sqrt{q}] + 1)}{2}$$

est égale à 0, on remarque qu'il n'existe pas de courbe singulière δ-optimale définie sur $\mathbb{F}_q$ de genre géométrique 1.

Remarque 4.3.6. Nous avons vu dans le théorème 4.2.1 qu'une courbe (singulière) δ-optimale a nécessairement une normalisée optimale. En revanche, une courbe singulière optimale n'admet généralement pas une normalisée optimale. On peut illustrer ce fait sur un exemple.

Considérons l'ensemble des courbes définies sur $\mathbb{F}_2$ de genre géométrique 1 et genre arithmétique 3, et commençons par montrer que $N_2(1, 3) = 6$.

On a $N_2(1, 3) \geq N_2(1) = 5$ d'après la proposition 3.2.4, et $N_2(1, 3) < 7$ par le corollaire 4.3.4. Maintenant, soit X une courbe lisse de genre 1 définie sur $\mathbb{F}_2$ avec exactement 4 points rationnels (dont l'existence est assurée par [50, Th. 4.1]). Il est simple de montrer qu'une telle courbe a 3 points de degré 2. En appliquant le théorème 3.2.1 avec $a_2 = 2$, nous obtenons une courbe singulière X' définie sur $\mathbb{F}_2$ de genre géométrique 1 et genre arithmétique 3, ayant 6 points

rationnels et X pour normalisée. Ainsi, $N_2(1,3) = 6$, et X' est un exemple de courbe singulière optimale dont la normalisée n'est pas optimale.

Plus encore, il n'existe pas de courbe définie sur $\mathbb{F}_2$ de genre géométrique 1 et genre arithmétique 3 dont la normalisée est optimale. C'est une conséquence du fait qu'une courbe lisse optimale de genre 1 n'a pas de points de degré 2, ni de degré 3.

À partir de $g \geq 2$, il est plus difficile de rendre le théorème 4.3.1 explicite, comme on l'a fait dans les cas $g = 0$ et $g = 1$ (voir les corollaires 4.3.2 et 4.3.4). En effet, pour $g = 0$ et $g = 1$, la quantité $B_2(\mathcal{X}_q(g))$ peut être aisément calculée en fonction de q et g : cela vient du fait que, dans ces cas, la connaissance du nombre de points rationnels sur $\mathbb{F}_q$ d'une courbe lisse X suffit pour déterminer les racines inverses du numérateur de la fonction zêta de X, et donc le nombre de points de X rationnels sur une extension quelconque de $\mathbb{F}_q$. Or, cela n'est plus vrai, en général, dès que $g \geq 2$.

Néanmoins, nous pourrons déterminer des bornes supérieures et inférieures pour $B_2(\mathcal{X}_q(g))$. Cela permettra, entre autres, de donner des valeurs exactes de $N_q(g,\pi)$ pour certaines valeurs de q, g et π.

4.4 Bornes sur le nombre de points de degré 2 d'une courbe lisse

Soit X une courbe lisse définie sur $\mathbb{F}_q$ de genre $g > 0$. Pour tout entier $n > 0$, on associe à X le n-uplet $(x_1, \ldots, x_n)$ défini comme suit :

$$x_i := \frac{(q^i + 1) - \sharp X(\mathbb{F}_{q^i})}{2g\sqrt{q^i}}, \quad i = 1, \ldots, n. \tag{4.4}$$

D'après les formules (2.5), on a :

$$x_i = \frac{\sum_{j=1}^{2g} \omega_j^i}{2g\sqrt{q^i}}.$$

Or, en appliquant l'hypothèse de Riemann (voir théorème 2.1.2), on obtient pour tout $i = 1, \ldots, n$:

$$|x_i| = \left| \frac{\sum_{j=1}^{2g} \omega_j^i}{2g\sqrt{q^i}} \right| \leq \frac{2g\sqrt{q^i}}{2g\sqrt{q^i}} = 1.$$

Autrement dit, le n-uplet $(x_1, \ldots, x_n)$ appartient à l'hypercube

$$\mathcal{C}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | -1 \leq x_i \leq 1, \ \forall\, i = 1, \ldots, n\}. \tag{4.5}$$

On remarque que toute borne inférieure pour x_i correspond à une borne supérieure pour $\sharp X(\mathbb{F}_{q^i})$ et, inversement, toute borne supérieure pour x_i correspond à une borne inférieure pour $\sharp X(\mathbb{F}_{q^i})$.

Ainsi, pour trouver des bonnes bornes pour le nombre de points de degré 2 de X, il faudra arriver à restreindre le plus possible la région du plan à laquelle x_1 et x_2 appartiennent, en utilisant la double nature, géométrique et arithmétique, de la courbe X.

Nous empruntons cette approche euclidienne à Hallouin et Perret, qui, dans [20], l'utilisent pour donner de nouvelles bornes pour le nombre de points rationnels d'une courbe lisse, lorsque le genre est assez grand par rapport à la cardinalité du corps de base.

4.4.1 L'approche d'Hallouin-Perret

On utilise en premier lieu la nature géométrique de X.

Considérons la surface algébrique lisse $X \times X$ et, en particulier, son espace de Néron-Severi sur $\mathbb{R}$:

$$\mathrm{NS}(X \times X)_{\mathbb{R}} = \mathrm{NS}(X \times X) \otimes_{\mathbb{Z}} \mathbb{R}.$$

Soient $H = X \times \{*\}$ et $V = \{*\} \times X$ les classes respectivement horizontale et verticale de $X \times X$. Soit $\mathrm{Vect}(H, V)$ le plan engendré par H et V. On a :

$$\mathrm{NS}(X \times X)_{\mathbb{R}} = \mathrm{Vect}(H, V) \oplus \mathrm{Vect}(H, V)^{\perp}.$$

Soit p la projection orthogonale de $\mathrm{NS}(X \times X)_{\mathbb{R}}$ sur $\mathrm{Vect}(H, V)^{\perp}$:

$$\begin{array}{rccc} p : & \mathrm{NS}(X \times X)_{\mathbb{R}} & \longrightarrow & \mathrm{Vect}(H, V)^{\perp} \\ & \Gamma & \longmapsto & \Gamma - (\Gamma \cdot V)H - (\Gamma \cdot H)V. \end{array}$$

Puisque $H + V$ est un diviseur ample, le *théorème d'indice de Hodge* [21, Th. 1.9, Ch. 5] entraîne que le produit d'intersection sur l'espace $\mathrm{NS}(X \times X)_{\mathbb{R}}$ est défini négatif sur $\mathrm{Vect}(H, V)^{\perp}$. Ainsi, $\mathrm{Vect}(H, V)^{\perp}$ peut être muni d'une structure d'espace euclidien, en définissant un produit scalaire $\langle \cdot, \cdot \rangle$ comme l'opposé du produit d'intersection :

$$\langle \gamma, \gamma' \rangle := -\gamma \cdot \gamma', \qquad \forall\, \gamma, \gamma' \in \mathrm{Vect}(H, V)^{\perp}.$$

Considérons le morphisme de Frobenius de X

$$\begin{array}{rccc} F : & X & \longrightarrow & X \\ & P & \longmapsto & P^{\varphi} \end{array},$$

où φ est l'automorphisme de Frobenius défini en (1.2). Notons, pour tout $k \geq 0$, $F^k = F \circ \cdots \circ F$ le k-ème itéré de F, avec la convention usuelle $F^0 = \mathrm{Id}_X$. Alors, si Γ^k désigne la classe de F^k dans $\mathrm{NS}(X \times X)_{\mathbb{R}}$, on a :

Lemme 4.4.1. [20, Lemme 3]

$$\begin{cases} \langle p(\Gamma^k), p(\Gamma^k) \rangle = 2gq^k & \forall\, k \geq 0 \\ \langle p(\Gamma^k), p(\Gamma^{k+i}) \rangle = q^k((q+1) - \sharp X(\mathbb{F}_q^i)) & \forall\, k \geq 0,\ \forall i \geq 1. \end{cases}$$

Si maintenant on considère les normalisées des classes de Néron-Severi des itérés du morphisme

de Frobenius :

$$\gamma^k = \frac{1}{\sqrt{2gq^k}} p(\Gamma^k),$$

on obtient, d'après le lemme 4.4.1, que les x_i définis dans (4.4) vérifient

$$x_i = \langle \gamma^k, \gamma^{k+i} \rangle.$$

Avec cette interprétation géométrique, on trouve que la matrice

$$G_n = \begin{pmatrix} 1 & x_1 & \cdots & x_{n-1} & x_n \\ x_1 & 1 & x_1 & \ddots & x_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{n-1} & \ddots & \ddots & 1 & x_1 \\ x_n & x_{n-1} & \cdots & x_1 & 1 \end{pmatrix}$$

est la matrice de Gram [1] de la famille $\gamma^0, \ldots, \gamma^n$ dans $\mathrm{Vect}(H, V)^\perp$, et donc semi-définie positive. Or, une matrice est semi-définie positive si et seulement si tous ses mineurs principaux sont positifs. Il en découle que le n-uplet $(x_1, \ldots, x_n)$ appartient à l'ensemble

$$\mathcal{W}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | \, G_{n,I} \geq 0, \, \forall \, I \subset \{1, \ldots, n+1\}\}, \tag{4.6}$$

où $G_{n,I}$ représente le mineur principal de G_n obtenu en supprimant de G_n les lignes et les colonnes dont les indices sont hors de I.

À ces relations, qui proviennent de la nature géométrique de X, on peut ajouter les contraintes arithmétiques résultant des inégalités évidentes

$$\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q),$$

pour tout $i \geq 2$. Il s'ensuit que, pour tout $i \geq 2$, on a

$$x_i \leq \frac{x_1}{q^{\frac{i-1}{2}}} + \frac{q^{i-1} - 1}{2gq^{\frac{i-2}{2}}}.$$

En posant

$$h_i^{q,g}(x_1, x_i) = x_i - \frac{x_1}{\sqrt{q}^{i-1}} - \frac{\sqrt{q}}{2g} \left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}} \right),$$

on obtient que le n-uplet $(x_1, \ldots, x_n)$ appartient à l'ensemble

$$\mathcal{H}_n^{q,g} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | h_i^{q,g}(x_1, x_i) \leq 0, \text{ pour tout } 2 \leq i \leq n\}. \tag{4.7}$$

Nous adoptons ici la convention que $\mathcal{H}_1^{q,g} = \mathbb{R}$.

1. La *matrice de Gram* G d'un ensemble de vecteurs $v_1, \ldots, v_n$ dans un espace préhilbertien $(E, \langle \cdot, \cdot \rangle)$ est la matrice hermitienne des produits scalaires, dont les entrées sont données par $(G)_{ij} = \langle v_i, v_j \rangle$.

Remarque 4.4.2. On note que l'on a $h_i^{q,g}(x_1, x_i) = 0$ si et seulement si $\sharp X(\mathbb{F}_q) = \sharp X(\mathbb{F}_{q^i})$.

En définitive on obtient que, si X est une courbe lisse définie sur $\mathbb{F}_q$ de genre $g > 0$, alors son n-uplet associé $(x_1, \ldots, x_n)$ appartient à l'ensemble $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$, où $\mathcal{C}_n, \mathcal{W}_n, \mathcal{H}_n^{q,g}$ sont respectivement définis par (4.5), (4.6) and (4.7).

Pour $n = 1, 2, 3, \ldots$, on trouve des sous-ensembles compacts de $\mathbb{R}^n$ auxquels le n-uplet $(x_1, \ldots, x_n)$ appartient. Nous pouvons donc déterminer une borne inférieure pour $\sharp X(\mathbb{F}_{q^i})$ sur la base d'une borne supérieure pour x_i et, inversement, une borne supérieure pour $\sharp X(\mathbb{F}_{q^i})$ à partir d'une borne inférieure pour x_i.

En incrémentant la dimension n, l'ensemble $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$ fournit une borne inférieure de plus en plus fine pour x_1 (et donc une borne supérieure de plus en plus fine pour $\sharp X(\mathbb{F}_q)$) si g est assez grand devant q.

En effet, pour $n = 1$, on retrouve la borne de Weil (voir (2.6)), qui peut donc être vue comme *une borne de Weil au premier ordre* :

$$\sharp X(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Pour $n = 2$, on retrouve la borne de Ihara (voir (2.9)), qui peut donc être appelée *borne de Weil au second ordre* : si

$$g \geq g_2 := \frac{\sqrt{q}(\sqrt{q} - 1)}{2},$$

alors

$$\sharp X(\mathbb{F}_q) \leq q + 1 + \frac{1}{2}\left(\sqrt{(8q+1)g^2 + 4q(q-1)g} - g\right).$$

Enfin, pour $n = 3$, on trouve une *borne de Weil au troisième ordre* lorsque

$$g \geq g_3 := \frac{\sqrt{q}(q-1)}{\sqrt{2}},$$

comme énoncé dans le théorème [20, Th. 18]. Cependant, la borne donnée par Hallouin et Perret dans ce dernier théorème n'est pas correcte, car pour certaines valeurs de q et $g \geq g_3$ la borne de Weil au troisième ordre n'est pas meilleure que celle au deuxième ordre, ce qui ne se peut. Après correction, nous trouvons finalement que si $g \geq g_3$, alors

$$\sharp X(\mathbb{F}_q) \leq q + 1 + \frac{1}{1 + \frac{2}{\sqrt{q}}}\left(\sqrt{a(q) + \frac{b(q)}{g} + \frac{c(q)}{g^2}} - 1 - \frac{1}{q} - \frac{1}{g}d(q)\right) g\sqrt{q},$$

où

$$\begin{cases} a(q) = 5 + \frac{8}{\sqrt{q}} + \frac{2}{q} + \frac{1}{q^2} \\ b(q) = \frac{(q^2-1)(3\sqrt{q}-1)(\sqrt{q}+1)}{q\sqrt{q}} \\ c(q) = \frac{(q-1)^2(-4q\sqrt{q}-4\sqrt{q}+q^2-2q+1)}{4q} \\ d(q) = \frac{(q-1)(q-2\sqrt{q}-1)}{2\sqrt{q}}. \end{cases}$$

De façon analogue, nous souhaitons trouver des bornes inférieures de plus en plus fines pour x_2 (dépendant éventuellement de x_1), dans le but de fournir des nouvelles bornes supérieures

pour $\sharp X(\mathbb{F}_{q^2})$. De chacune de ces bornes, nous déduirons une nouvelle borne supérieure pour le nombre de points de degré 2 d'une courbe lisse, en rendant l'équivalence du théorème 4.3.1 plus explicite.

4.4.2 Bornes supérieures

Soit X une courbe lisse définie sur $\mathbb{F}_q$ de genre g. On rappelle que, si $B_2(X)$ désigne le nombre de points de degré 2 de X, on a

$$B_2(X) = \frac{\sharp X(\mathbb{F}_{q^2}) - \sharp X(\mathbb{F}_q)}{2}.$$

Nous allons établir des bornes supérieures pour le nombre $B_2(X)$, obtenues en considérant l'ensemble $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$ à différents *ordres*, c'est-à-dire, pour différentes valeurs de la dimension n (en l'occurrence $n = 1, 2, 3$). En particulier, si X est optimale, cela nous permettra d'obtenir des bornes supérieures pour la quantité $B_2(\mathcal{X}_q(g))$, qui, l'on rappelle, représente comme le nombre maximum de points de degré 2 d'une courbe lisse optimale de genre g définie sur $\mathbb{F}_q$.

Le premier ordre

D'après les bornes de Weil qui découlent de (2.5), on a

$$\sharp X(\mathbb{F}_{q^2}) \leq q^2 + 1 + 2gq,$$

et

$$\sharp X(\mathbb{F}_q) \geq q + 1 - 2g\sqrt{q}.$$

Une borne supérieure évidente pour $B_2(X)$ est donc :

$$B_2(X) \leq \frac{q^2 - q}{2} + g(q + \sqrt{q}). \tag{4.8}$$

Posons

$$M'(q, g) := \frac{q^2 - q}{2} + g(q + \sqrt{q}).$$

Nous pouvons considérer $M'(q, g)$ comme une borne supérieure au *premier ordre* pour $B_2(\mathcal{X}_q(g))$, puisque la borne (4.8) est une conséquence immédiate des bornes de Weil.

En utilisant la quantité $M'(q, g)$, nous indiquons dans le tableau 4.1 des bornes supérieures au premier ordre pour $B_2(\mathcal{X}_q(g))$, à des valeurs fixées du couple (q, g) :

q \ g	2	3	4	5	6
2	7	11	14	18	21
3	12	17	21	26	31
2^2	18	24	30	36	42

TABLE 4.1 – Bornes supérieures au premier ordre pour $B_2(\mathcal{X}_q(g))$, données par $M'(q,g)$.

Malheureusement, la borne (4.8) est plutôt mauvaise. Nous allons donc l'améliorer.

Soit $g > 0$. D'après les formules (4.4), on a

$$\sharp X(\mathbb{F}_q) = q + 1 - 2g\sqrt{q}x_1 \qquad \text{et} \qquad \sharp X(\mathbb{F}_{q^2}) = q^2 + 1 - 2gqx_2.$$

Ainsi, la quantité $B_2(X)$ peut être vue comme une fonction de x_1 et x_2 dans le domaine $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$:

$$B_2(X) = g\sqrt{q}(x_1 - \sqrt{q}x_2) + \frac{q^2 - q}{2}. \tag{4.9}$$

Nous remarquons que toute borne inférieure pour x_2 entraîne une borne supérieure (éventuellement dépendante de x_1) pour $B_2(X)$.

Nous allons donc étudier l'ensemble $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$ pour $n = 2$ (deuxième ordre) et $n = 3$ (troisième ordre).

Le deuxième ordre

Pour $n = 2$, l'ensemble $\mathcal{C}_2 \cap \mathcal{W}_2 \cap \mathcal{H}_2^{q,g}$ est constitué des couples $(x_1, x_2) \in \mathbb{R}^2$ qui satisfont le système d'inéquations suivant :

$$\begin{cases} 2x_1^2 - 1 \leq x_2 \leq 1 \\ x_2 \leq \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}. \end{cases} \tag{4.10}$$

Géométriquement, l'ensemble des solutions du système (4.10) correspond à la région du plan $\langle x_1, x_2 \rangle$ bornée par la parabole

$$P : x_2 = 2x_1^2 - 1$$

et les droites

$$L_2^{q,g} : x_2 = \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g} \qquad \text{et} \qquad x_2 = 1.$$

Plus précisément, selon que $g < g_2$, $g = g_2$ ou $g > g_2$, avec

$$g_2 = \frac{\sqrt{q}(\sqrt{q} - 1)}{2},$$

on se trouve dans l'une des configurations suivantes :

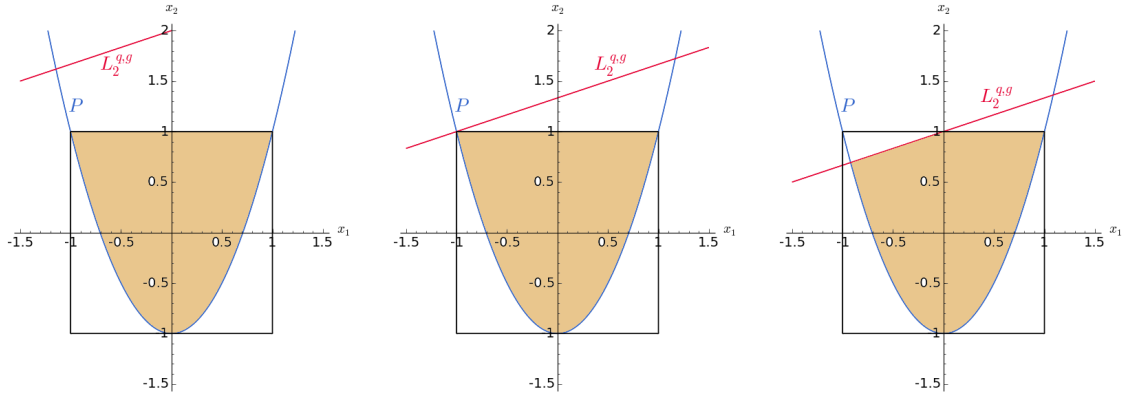


FIGURE 4.1 – La région $\mathcal{C}_2 \cap \mathcal{W}_2 \cap \mathcal{H}_2^{q,g}$, respectivement pour $g < g_2$, $g = g_2$ et $g > g_2$.

La première inégalité du système (4.10)

$$x_2 \geq 2x_1^2 - 1, \tag{4.11}$$

donne la borne supérieure :

$$B_2(X) \leq g\sqrt{q}(x_1 - \sqrt{q}(2x_1^2 - 1)) + \frac{q^2 - q}{2}. \tag{4.12}$$

En utilisant les formules (4.4) pour x_1, on obtient la borne supérieure suivante pour $B_2(X)$ (en fonction de q, g et $\sharp X(\mathbb{F}_q)$), ce qui est une reformulation de [20, Prop. 14] :

Proposition 4.4.3. *Soit X une courbe lisse de genre $g > 0$ définie sur $\mathbb{F}_q$. On a :*

$$B_2(X) \leq \frac{q^2 + 1 + 2gq - \frac{1}{g}\left(\sharp X(\mathbb{F}_q) - (q+1)\right)^2 - \sharp X(\mathbb{F}_q)}{2}.$$

Supposons maintenant que X est une courbe lisse optimale de genre $g > 0$, c'est-à-dire que X a $N_q(g)$ points rationnels. D'après la proposition 4.4.3, si l'on pose

$$M''(q,g) := \frac{q^2 + 1 + 2gq - \frac{1}{g}\left(N_q(g) - (q+1)\right)^2 - N_q(g)}{2},$$

alors on obtient :

$$B_2(\mathcal{X}_q(g)) \leq M''(q,g).$$

La quantité $M''(q,g)$ peut donc être vue comme une borne supérieure au deuxième ordre pour $B_2(\mathcal{X}_q(g))$.

Ainsi, nous obtenons la proposition suivante, en conséquence du théorème 4.3.1 :

Proposition 4.4.4. *Soit $g > 0$. Si $\pi > g + M''(q,g)$, alors il n'existe pas de courbe δ-optimale*

définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π, ou, autrement dit,

$$N_q(g,\pi) < N_q(g) + \pi - g.$$

Nous reportons dans le tableau 4.2 des bornes supérieures pour $B_2(\mathcal{X}_q(g))$, à valeurs fixées du couple (q,g), données par la quantité $M''(q,g)$. Pour le calcul de $M''(q,g)$ nous avons utilisé les données sur $N_q(g)$ disponibles sur le site web `www.manypoints.org` [48].

q \ g	2	3	4	5	6
2	1	2	3	4	5
3	3	3	3	5	7
2^2	5	0	4	5	3

TABLE 4.2 – Bornes supérieures au deuxième ordre pour $B_2(\mathcal{X}_q(g))$ données par $M''(q,g)$.

Le troisième ordre

En dimension $n = 3$, de nouvelles contraintes pour x_1, x_2 et x_3 apparaissent, en plus de celles du système (4.10). En effet, l'ensemble $\mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g}$ est donné par les triplets $(x_1,x_2,x_3) \in \mathbb{R}^3$ qui satisfont le système d'inéquations suivant :

$$\begin{cases} 2x_1^2 - 1 \leq x_2 \leq 1 \\ -1 + \frac{(x_1+x_2)^2}{1+x_1} \leq x_3 \leq 1 - \frac{(x_1-x_2)^2}{1-x_1} \\ 1 + 2x_1x_2x_3 - x_3^2 - x_1^2 - x_2^2 \geq 0 \\ x_2 \leq \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g} \\ x_3 \leq \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}}. \end{cases}$$

Considérons la projection de $\mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g}$ sur le plan $\langle x_1, x_2 \rangle$, c'est-à-dire l'ensemble

$$\{(x_1,x_2) \in \mathbb{R}^2 : (x_1,x_2,x_3) \in \mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g}\}.$$

On montre facilement que ce dernier est constitué par les couples $(x_1,x_2) \in \mathbb{R}^2$ qui vérifient :

$$\begin{cases} 2x_1^2 - 1 \leq x_2 \leq 1 \\ -1 + \frac{(x_1+x_2)^2}{1+x_1} \leq \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}} \\ x_2 \leq \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}. \end{cases} \tag{4.13}$$

En effet, la projection sur le plan $\langle x_1, x_2 \rangle$ du sous-ensemble de $\mathcal{C}_3$ défini par

$$1 + 2x_1x_2x_3 - x_3^2 - x_1^2 - x_2^2 \geq 0$$

est égale à $\mathcal{C}_2$, puisque pour tout $(x_1, x_2) \in \mathcal{C}_2$ on a :

$$x_3 \in \left[x_1x_2 - \sqrt{(x_2^2-1)(x_1^2-1)}, x_1x_2 + \sqrt{(x_2^2-1)(x_1^2-1)}\right] \subseteq [-1,1].$$

L'équation correspondant à la deuxième inégalité du système (4.13) :

$$x_2^2 + 2x_1x_2 - \left(\frac{1}{q} - 1\right)x_1^2 - \left(\frac{1}{q} + 1 + \frac{q^2-1}{2g\sqrt{q}}\right)x_1 - 1 - \frac{q^2-1}{2g\sqrt{q}} = 0 \tag{4.14}$$

décrit, dans le plan $\langle x_1, x_2\rangle$, une hyperbole $H^{q,g}$ passant par le point $(-1,1)$. Pour

$$g \geq g_3 = \frac{\sqrt{q}(q-1)}{\sqrt{2}},$$

l'hyperbole $H^{q,g}$ coupe la parabole en au moins trois points. Ainsi, la région du plan $\langle x_1, x_2\rangle$ correspondant au système (4.13) peut se trouver dans l'une des deux configurations suivantes :

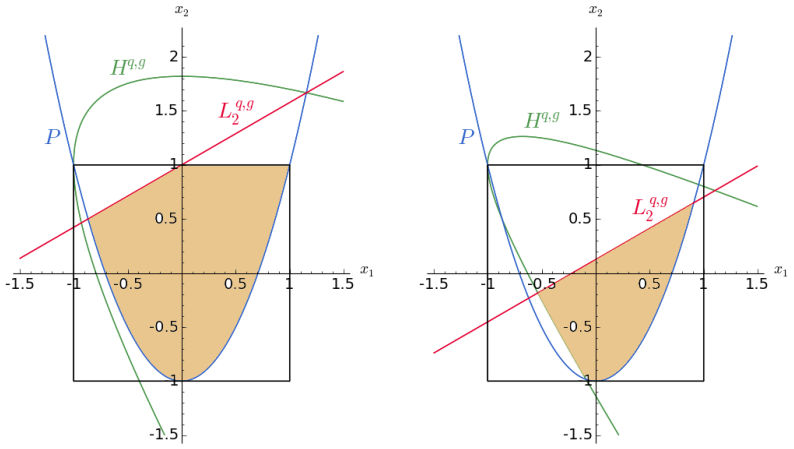


FIGURE 4.2 – La projection de $\mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g}$ sur le plan $< x_1, x_2 >$, pour $g < g_3$ et $g > g_3$.

On remarque que, lorsque $g \geq g_3$, nous avons une meilleure borne inférieure pour x_2 en fonction de x_1 (par rapport à la borne (4.11)), donnée par la plus petite solution de l'équation quadratique en x_2 (4.14) :

$$x_2 \geq -x_1 - \sqrt{\frac{1}{q}x_1^2 + \left(\frac{1}{q} + 1 + \frac{q^2-1}{2g\sqrt{q}}\right)x_1 + 1 + \frac{q^2-1}{2g\sqrt{q}}}.$$

Ainsi, de (4.9), on obtient une nouvelle borne supérieure pour $B_2(X)$, en fonction de q, g et x_1 :

$$B_2(X) \leq g\sqrt{q}(1+\sqrt{q})x_1 + gq\sqrt{\frac{1}{q}x_1^2 + \left(\frac{1}{q} + 1 + \frac{q^2-1}{2g\sqrt{q}}\right)x_1 + 1 + \frac{q^2-1}{2g\sqrt{q}}} + \frac{q^2-q}{2}. \tag{4.15}$$

En injectant l'expression (4.4) de x_1 dans (4.15), on trouve une nouvelle borne supérieure pour $B_2(X)$ en fonction de q, g et $\sharp X(\mathbb{F}_q)$:

Proposition 4.4.5. *Soit X une courbe lisse de genre $g \geq \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ définie sur $\mathbb{F}_q$. On a :*

$$B_2(X) \leq \sqrt{1/4\left(\sharp X(\mathbb{F}_q)\right)^2 + \alpha(q,g)\sharp X(\mathbb{F}_q) + \beta(q,g)} - \frac{(1+\sqrt{q})}{2}\sharp X(\mathbb{F}_q) + \frac{q^2+1+\sqrt{q}(q+1)}{2}, \tag{4.16}$$

où

$$\begin{cases} \alpha(q,g) = -\frac{1}{4}((2q\sqrt{q}+2\sqrt{q})g + q^3 + q + 2) \\ \beta(q,g) = \frac{1}{4}(4q^2g^2 + 2\sqrt{q}(q^3+q^2+q+1)g + q^4 + q^3 + q + 1). \end{cases}$$

Comme précédemment, si l'on pose

$$M'''(q,g) := \sqrt{1/4\left(N_q(g)\right)^2 + \alpha(q,g)N_q(g) + \beta(q,g)} - \frac{(1+\sqrt{q})}{2}N_q(g) + \frac{q^2+1+\sqrt{q}(q+1)}{2}, \tag{4.17}$$

où $\alpha(q,g)$ et $\beta(q,g)$ sont définis comme dans la proposition 4.4.5, on trouve

$$B_2(\mathcal{X}_q(g)) \leq M'''(q,g).$$

D'après le théorème 4.3.1, nous obtenons la proposition suivante :

Proposition 4.4.6. *Soit $g \geq \frac{\sqrt{q}(q-1)}{\sqrt{2}}$. Si $\pi > g + M'''_q(g)$, alors il n'existe pas de courbe δ-optimale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π, ou, autrement dit,*

$$N_q(g,\pi) < N_q(g) + \pi - g.$$

Dans le tableau 4.3, en utilisant la quantité $M'''(q,g)$, nous reportons des bornes supérieures pour $B_2(\mathcal{X}_q(g))$ au troisième ordre. Certaines cases du tableau sont évidemment vides, puisque $M'''(q,g)$ est défini seulement lorsque $g \geq \frac{\sqrt{q}(q-1)}{\sqrt{2}}$.

q \ g	2	3	4	5	6
2	0	0	1	1	1
3		2	1	2	3
2^2				4	1

TABLE 4.3 – Bornes supérieures au troisième ordre pour $B_2(\mathcal{X}_q(g))$, données par $M'''(q,g)$.

D'après les propositions 4.4.3 et 4.4.5, il est possible de synthétiser les tableaux 4.2 et 4.3 dans le suivant :

q \ g	2	3	4	5	6
2	0	0	1	1	1
3	3	2	1	2	3
2^2	5	0	4	4	1

TABLE 4.4 – Bornes supérieures pour $B_2(\mathcal{X}_q(g))$.

4.4.3 Bornes inférieures

De la même manière, nous pouvons utiliser l'approche euclidienne d'Hallouin-Perret pour déterminer des bornes inférieures pour $B_2(X)$.

En premier lieu, d'après les bornes de Weil qui découlent de (2.5), nous avons

$$\sharp X(\mathbb{F}_{q^2}) \geq q^2 + 1 - 2gq \qquad \text{et} \qquad \sharp X(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q},$$

et donc

$$B_2(X) \geq \frac{q^2 - q}{2} - g(q + \sqrt{q}). \tag{4.18}$$

Il est simple de montrer que la quantité à droite dans (4.18) est strictement positive si et seulement si $g < g_2 = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$.

Ainsi, nous pouvons considérer l'inégalité (4.18) comme une borne inférieure au premier ordre pour $B_2(X)$, puisqu'elle est une conséquence immédiate des bornes de Weil.

Géométriquement, il est également clair que nous n'obtiendrions pas de meilleures bornes inférieures pour $B_2(X)$ en passant au deuxième ou au troisième ordre. En effet, en observant les graphes des figures 4.1 et 4.2, nous remarquons qu'une borne supérieure plus fine pour x_2 peut seulement être donnée par la droite $L_2^{q,g}$. Or, nous avons vu dans la remarque 4.4.2 que, si le couple (x_1, x_2) est sur la droite $L_2^{q,g}$, alors $\sharp X(\mathbb{F}_q) = \sharp X(\mathbb{F}_{q^2})$, ce qui entraîne $B_2(X) = 0$.

Pour $g < g_2$, l'inégalité (4.18) donne les bornes inférieures suivantes pour $B_2(\mathcal{X}_q(g))$:

q \ g	2	3	4	5
7	2			
2^3	7			
3^2	12			
11	27	13		
13	45	29	12	
2^4	80	60	40	20

TABLE 4.5 – Bornes inférieures pour $B_2(\mathcal{X}_q(g))$.

Ainsi, d'après le théorème 4.3.1 et l'inégalité (4.18), on obtient la proposition suivante :

Proposition 4.4.7. *Soit $g < \frac{\sqrt{q}(\sqrt{q}-1)}{2}$. Si $g \leq \pi \leq g + \frac{q^2-q}{2} - g(q+\sqrt{q})$, alors il existe une courbe δ-optimale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π.*

4.5 Quelques valeurs exactes de $N_q(g,\pi)$

Nous utilisons ci-dessous les bornes obtenues pour $B_2(\mathcal{X}_q(g))$ dans la section précédente (voir les tableaux 4.4 et 4.5) pour déterminer quelques valeurs exactes de $N_q(g,\pi)$. Nous complétons la proposition suivante avec les résultats sur $N_q(g,\pi)$ déjà obtenus dans la section 4.3.

Proposition 4.5.1. *Soit q une puissance d'un nombre premier p. Soient g et π des entiers positifs tels que $g \leq \pi$. On a :*

1. $N_q(0,\pi) = q+1+\pi$ *si et seulement si* $0 \leq \pi \leq \frac{q^2-q}{2}$.
2. *Si p ne divise pas $[2\sqrt{q}]$, q est un carré, ou $q = p$, alors*
   $N_q(1,\pi) = q + [2\sqrt{q}] + \pi$ *si et seulement si* $1 \leq \pi \leq 1 + \frac{q^2+q-[2\sqrt{q}]([2\sqrt{q}]+1)}{2}$.
   Sinon,
   $N_q(1,\pi) = q + [2\sqrt{q}] + \pi - 1$ *si et seulement si* $1 \leq \pi \leq 1 + \frac{q^2+q+[2\sqrt{q}](1-[2\sqrt{q}])}{2}$.
3. *Si $g < \frac{\sqrt{q}(\sqrt{q}-1)}{2}$ et $g \leq \pi \leq \frac{q^2-q}{2} - g(q+\sqrt{q}-1)$, alors $N_q(g,\pi) = N_q(g) + \pi - g$.*
4. $N_2(2,3) = 6$.
5. $N_2(3,4) = 7$.
6. $N_{2^2}(4,5) = 14$.

Démonstration. Les points 1 et 2 sont les corollaires 4.3.2 et 4.3.4. Le point 3 est donné par la proposition 4.4.7.

Montrons, ensuite, le point 4. On remarque que, d'après la proposition 3.2.4, $N_2(2,3) \geq N_2(2) = 6$ et, d'après le tableau 4.4, $B_2(\mathcal{X}_2(2)) = 0$. Ainsi on obtient, par la proposition 4.4.6, que $N_2(2,3) < N_2(2)+1 = 7$. Les points 5 et 6 se démontrent de la même manière que le point 4. □

4.6 Courbes maximales

Soit X une courbe définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π. On rappelle que X est une *courbe maximale* si elle atteint la borne d'Aubry-Perret, à savoir

$$\sharp X(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}] + \pi - g.$$

Les courbes maximales constituent une sous-classe des courbes δ-optimales. Ainsi elles héritent de toutes les propriétés listées dans la théorème 4.2.1.

Considérons d'abord le résultat suivant, qui donne, entres autres, la forme de la fonction zêta d'une courbe maximale.

Proposition 4.6.1. *Si X est une courbe maximale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π. Alors on a :*

$$\pi \leq g + \frac{q^2 + (2g-1)q - g[2\sqrt{q}]([2\sqrt{q}]+1)}{2}$$

et

$$Z_X(T) = \frac{(qT^2 + [2\sqrt{q}]T + 1)^g (1+T)^{\pi - g}}{(1-T)(1-qT)}.$$

Démonstration. D'après le théorème 4.2.1, la courbe X a une normalisée maximale $\tilde{X}$, et

$$\pi \leq g + B_2(\tilde{X}).$$

Or, toute courbe lisse maximale de genre g a le même nombre de points de degré 2. En effet, si $\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g$ sont les racines inverses du numérateur de la fonction zêta $Z_{\tilde{X}}(T)$ de $\tilde{X}$, on a vu, dans la proposition 2.1.18, que $\omega_i + \overline{\omega}_i = -[2\sqrt{q}]$. Comme dans la preuve du corollaire 4.3.4, on peut donc calculer le nombre de points de degré 2 de $\tilde{X}$:

$$B_2(\tilde{X}) = \frac{q^2 + (2g-1)q - g[2\sqrt{q}]([2\sqrt{q}]+1)}{2},$$

ce qui donne l'inégalité concernant g, π et q voulue.

La forme de la fonction zêta de X est immédiate d'après le théorème 4.2.1 et la proposition 2.1.18. □

4.6.1 Le spectre des genres de courbes maximales

La proposition 4.6.1 confirme que, pour π assez grand devant g, il n'existe pas de courbe maximale de genre géométrique g et genre arithmétique π.

Ainsi, par analogie avec le cas lisse, nous pouvons considérer la problématique de déterminer le *spectre des genres* de courbes maximales définies sur $\mathbb{F}_q$, c'est à dire l'ensemble des couples (g, π) pour lesquels il existe une courbe maximale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π :

$$\begin{aligned}\Gamma_q := \{&(g,\pi) \in \mathbb{N} \times \mathbb{N} : \text{il existe une courbe maximale définie sur } \mathbb{F}_q \\ &\text{de genre géométrique } g \text{ et genre arithmétique } \pi\}.\end{aligned}$$

On supposera, par la suite, que q est un carré. La proposition suivante est une conséquence simple des théorèmes 4.2.1 et 4.3.1, et de la proposition 4.6.1.

Proposition 4.6.2. *Soit q un carré. Il existe une courbe maximale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π si et seulement si $N_q(g) = q + 1 + 2g\sqrt{q}$ et*

$$g \leq \pi \leq (-q - \sqrt{q} + 1)g + \frac{q^2 - q}{2}. \tag{4.19}$$

Remarque 4.6.3. La quantité de droite dans l'inégalité (4.19) est linéairement décroissante par rapport à g. Ainsi, elle atteint sa valeur maximale pour $g = 0$ (cela signifie aussi que le nombre de points de degré 2 d'une courbe lisse maximale est une fonction décroissante du genre). On obtient de cette façon une borne pour le genre arithmétique π en fonction de la cardinalité du corps fini :

$$\pi \leq \frac{q(q-1)}{2}. \tag{4.20}$$

D'un point de vue géométrique, nous avons donc montré que l'ensemble Γ_q est contenu (voir la figure 4.3) dans le triangle (OAB) du plan $\langle g, \pi \rangle$ délimité par les droites

$$\mathcal{D}_1 : g = 0, \qquad \mathcal{D}_2 : \pi = (-q - \sqrt{q} + 1)g + \frac{q^2 - q}{2} \qquad \text{et} \qquad \mathcal{D}_3 : g = \pi.$$

Le point d'intersection des droites $\mathcal{D}_2$ et $\mathcal{D}_3$ est le point

$$B\left(\frac{\sqrt{q}(\sqrt{q}-1)}{2}, \frac{\sqrt{q}(\sqrt{q}-1)}{2}\right).$$

Cela signifie que toute courbe maximale définie sur $\mathbb{F}_q$ de genre geometrique $g = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$ est nécessairement lisse, et donc isomorphe à la courbe Hermitienne (voir la section 2.1.4).

En outre, la borne (4.20) est atteinte. En effet, la courbe de Fukasawa, Homma et Kim, décrite dans la section 4.1.1, est un exemple de courbe maximale définie sur $\mathbb{F}_q$ de genre arithmétique $\pi = \frac{q(q-1)}{2}$.

En utilisant les inégalités (2.12), les propositions 4.5.1 et 4.6.2, et la remarque 4.6.3, nous pouvons énoncer le théorème suivant.

Théorème 4.6.4. *Soit q un carré et X une courbe maximale définie sur $\mathbb{F}_q$ de genre géométrique g et genre arithmétique π. On pose*

$$g' := \frac{\sqrt{q}(\sqrt{q}-1)}{2}, \quad g'' := \left[\frac{(\sqrt{q}-1)^2}{4}\right] \quad \textit{et} \quad g''' := \left[\frac{q - \sqrt{q} + 4}{6}\right].$$

Soit

$$\begin{aligned}\Gamma_q := \{&(g,\pi) \in \mathbb{N} \times \mathbb{N} : \textit{il existe une courbe maximale définie sur } \mathbb{F}_q \\ &\textit{de genre géométrique } g \textit{ et genre arithmétique } \pi\}.\end{aligned}$$

On a :

1. $0 \leq g \leq g'$, $g \leq \pi \leq \frac{q(q-1)}{2}$ *et* $\pi \leq (-q - \sqrt{q} + 1)g + \frac{q^2-q}{2}$. *Autrement dit, Γ_q est contenu dans l'ensemble des points à coordonnées entières à l'intérieur du triangle (OAB) de la figure 4.3.*

2. *Le point $B = (g', g')$ appartient à Γ_q et*

$$\left\{(0,\pi), \ \textit{avec } 0 \leq \pi \leq \frac{q^2-q}{2}\right\} \subseteq \Gamma_q.$$

3. *Si $g \neq g'$, alors $g \leq g''$ et*

$$\left\{(g'',\pi), \ \textit{avec } g'' \leq \pi \leq (-q - \sqrt{q} + 1)g'' + \frac{q^2-q}{2}\right\} \subseteq \Gamma_q.$$

4. Si $g \neq g'$ et $g \neq g''$, alors $g \leq g'''$ et

$$\left\{(g''', \pi)\,,\ \textit{avec } g''' \leq \pi \leq (-q - \sqrt{q} + 1)g''' + \frac{q^2 - q}{2}\right\} \subseteq \Gamma_q.$$

Le théorème 4.6.4 est illustré à l'aide de la figure 4.3 (dans laquelle on a choisi un rapport d'échelle entre les axes de 0.025 pour des raisons de lisibilité).

Remarque 4.6.5. Si X est une courbe maximale définie sur $\mathbb{F}_q$ de genre géométrique g', g'' ou g''', alors sa courbe normalisée $\tilde{X}$ est une courbe lisse maximale définie sur $\mathbb{F}_q$ de genre respectivement g', g'' ou g''', et donc $\mathbb{F}_q$-isomorphe à une des courbes rappelées dans la sous-section 2.1.4.

4.7 Un théorème sur les revêtements de courbes singulières

Nous terminons par quelques considérations sur les revêtements de courbes singulières.

Commençons par rappeler le résultat suivant dû à Serre.

Théorème 4.7.1. [30, Prop. 6] *Soient X et Y deux courbes lisses définies sur $\mathbb{F}_q$. Supposons qu'il existe un morphisme non constant $f : Y \to X$ défini sur $\mathbb{F}_q$. Alors, si $P_X(T)$ et $P_Y(T)$ désignent les numérateurs des fonctions zêta de X et Y respectivement, alors le polynôme $P_X(T)$ divise $P_Y(T)$. En particulier, si Y est maximale, il en va de même pour X.*

Ce résultat est par exemple utilisé dans [15] et [16] pour déterminer des exemples de courbes maximales, non isomorphes, de même genre et même groupe d'automorphismes.

Nous prouvons ici que le résultat subsiste sans l'hypothèse de lissité sur les courbes, en supposant que le morphisme est plat. Il faut remarquer que la divisibilité des numérateurs des fonctions zêta dans un revêtement plat, démontrée par Aubry et Perret pour des courbes non nécessairement lisses dans [7], et pour des variétés non nécessairement lisses dans [8], ne donne pas le résultat.

Théorème 4.7.2. *Soit $f : Y \to X$ un morphisme plat fini entre deux courbes définies sur $\mathbb{F}_q$. Si Y est maximale alors X est maximale.*

Démonstration. Soient g_X et π_X (respectivement g_Y et π_Y) le genre géométrique et le genre arithmétique de X (respectivement de Y). Puisque Y est maximale, on a

$$\sharp Y(\mathbb{F}_q) = q + 1 + g_Y[2\sqrt{q}] + \pi_Y - g_Y.$$

D'après [5, Remarque 4.1] nous savons que

$$|\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq (\pi_Y - g_Y) - (\pi_X - g_X) + (g_Y - g_X)[2\sqrt{q}].$$

Ainsi nous obtenons :

$$\sharp X(\mathbb{F}_q) \geq \sharp Y(\mathbb{F}_q) - (\pi_Y - g_Y) + (\pi_X - g_X) - (g_Y - g_X)[2\sqrt{q}] = q + 1 + g_X[2\sqrt{q}] + \pi_X - g_X.$$

On en conclut que X est aussi maximale. □

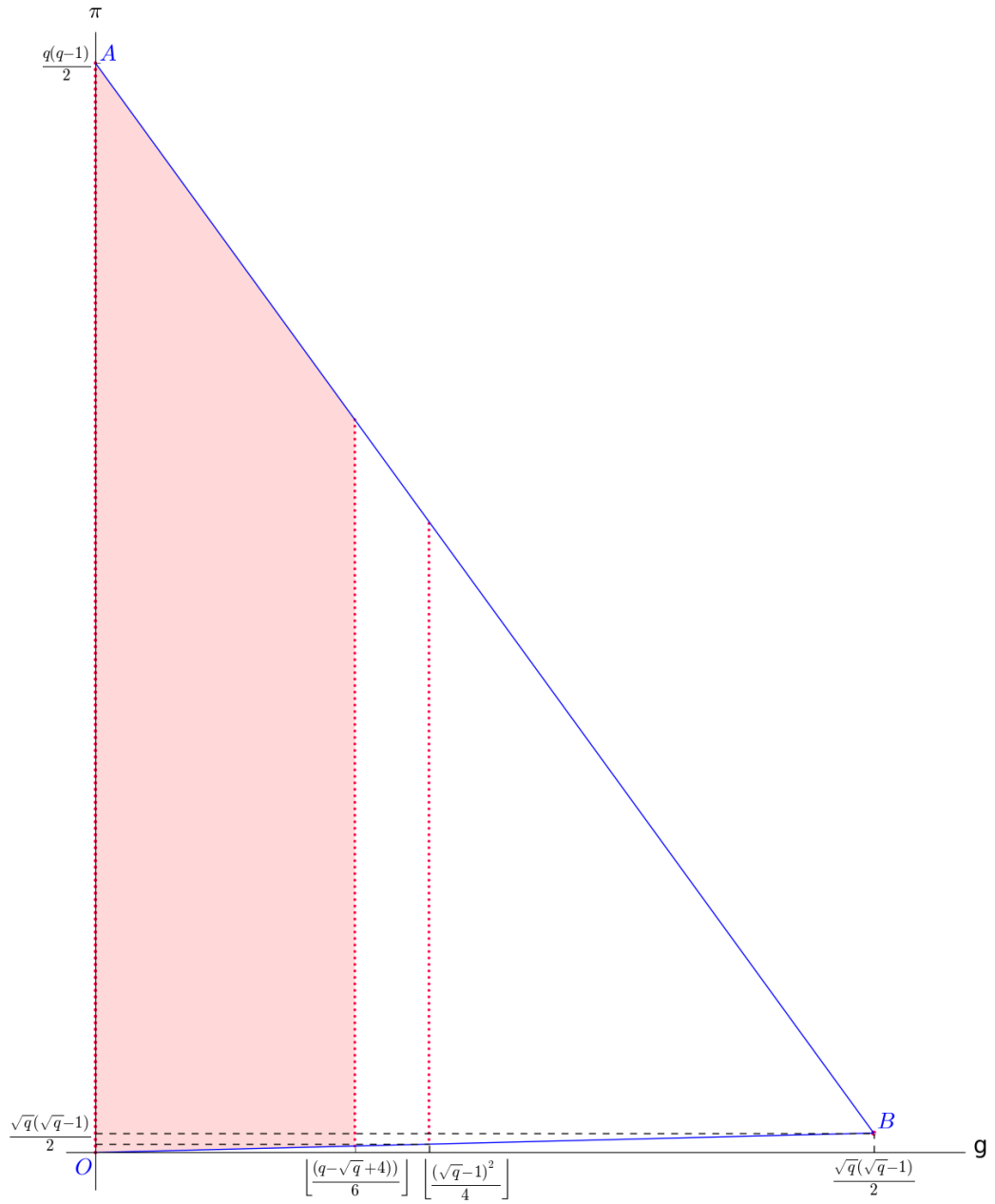


FIGURE 4.3 – L'ensemble Γ_q est contenu dans l'ensemble des points à coordonnées entières à l'intérieur ou sur le bord du triangle (OAB). Les points correspondent aux couples (g, π) que nous avons déjà montrés être dans Γ_q. Le reste de l'ensemble Γ_q doit être contenu dans le trapézoïde coloré.

Bibliographie

[1] M. Abdón and F. Torres. On $\mathbf{F}_{q^2}$-maximal curves of genus $\frac{1}{6}(q-3)q$. *Beiträge Algebra Geom.*, 46(1) :241–260, 2005.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[3] Y. Aubry and A. Iezzi. On the maximum number of rational points on singular curves over finite fields. *Mosc. Math. J.*, 15(4) :615–627, 2015.

[4] Y. Aubry and A. Iezzi. Optimal and maximal singular curves. À paraître dans *Contemporary Mathematics (AMS), arXiv:1510.01853v1*, 2016.

[5] Y. Aubry and M. Perret. Coverings of singular curves over finite fields. *Manuscripta Math.*, 88(4) :467–478, 1995.

[6] Y. Aubry and M. Perret. A Weil theorem for singular curves. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 1–7. de Gruyter, Berlin, 1996.

[7] Y. Aubry and M. Perret. Divisibility of zeta functions of curves in a covering. *Arch. Math. (Basel)*, 82(3) :205–213, 2004.

[8] Y. Aubry and M. Perret. On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields. *Finite Fields Appl.*, 10(3) :412–431, 2004.

[9] Y. Aubry and F. Rodier. Differentially 4-uniform functions. In *Arithmetic, geometry, cryptography and coding theory 2009*, volume 521 of *Contemp. Math.*, pages 1–8. Amer. Math. Soc., Providence, RI, 2010.

[10] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14(1) :197–272, 1941.

[11] B. Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82 :631–648, 1960.

[12] R. Fuhrmann, A. Garcia, and F. Torres. On maximal curves. *J. Number Theory*, 67(1) :29–51, 1997.

[13] R. Fuhrmann and F. Torres. The genus of curves over finite fields with many rational points. *Manuscripta Math.*, 89(1) :103–106, 1996.

[14] S. Fukasawa, M. Homma, and S. J. Kim. Rational curves with many rational points over a finite field. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 37–48. Amer. Math. Soc., Providence, RI, 2012.

[15] M. Giulietti, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. Curves covered by the Hermitian curve. *Finite Fields Appl.*, 12(4) :539–564, 2006.

[16] M. Giulietti, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. A family of curves covered by the Hermitian curve. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 63–78. Soc. Math. France, Paris, 2010.

[17] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6) :1289–1290, 1981.

[18] V. D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988. Translated from the Russian by N. G. Shartse.

[19] A. Grothendieck. Formule de Lefschetz et rationalité des fonctions L. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris, 1995.

[20] E. Hallouin and M. Perret. From Hodge index theorem to the number of points of curves over finite fields. *arXiv:1409.2357v1*, 2014.

[21] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[22] H. Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *J. Reine Angew. Math.*, 172 :37–54, 1935.

[23] H. Hasse. Über die Riemannsche Vermutung in Funktionenkörpern. *Comptes Rendus du congrès international des mathématiciens, Oslo*, pages 189–206, 1936.

[24] D. Hilbert and A. Hurwitz. Über die diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, 14(1) :217–224, 1890.

[25] M. Hindry. La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini. In *Henri Cartan & André Weil, mathématiciens du XX$^{\text{e}}$ siècle*, pages 63–98. Ed. Éc. Polytech., Palaiseau, 2012.

[26] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. The number of points on an algebraic curve over a finite field. In *Surveys in combinatorics 2007*, volume 346 of *London Math. Soc. Lecture Note Ser.*, pages 175–200. Cambridge Univ. Press, Cambridge, 2007.

[27] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[28] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3) :721–724 (1982), 1981.

[29] G. Korchmáros and F. Torres. On the genus of a maximal curve. *Math. Ann.*, 323(3) :589–608, 2002.

[30] G. Lachaud. Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(16) :729–732, 1987.

[31] J. B. Little. Algebraic geometry codes from higher dimensional varieties. In *Advances in algebraic geometry codes*, volume 5 of *Ser. Coding Theory Cryptol.*, pages 257–293. World Sci. Publ., Hackensack, NJ, 2008.

[32] H. T. Muhly and O. Zariski. Hilbert's characteristic function and the arithmetic genus of an algebraic variety. *Trans. Amer. Math. Soc.*, 69 :78–88, 1950.

[33] M. Perret. Nombre maximum de points rationnels d'une courbe sur un corps fini. *Sém. Théor. Nombres Bordeaux (2)*, 3(2) :261–274, 1991.

[34] D. Perrin. *Géométrie algébrique*. Savoirs Actuels. [Current Scholarship]. InterEditions, Paris ; CNRS Éditions, Paris, 1995. Une introduction. [An introduction].

[35] C. Ritzenthaler. Optimal curves of genus 1, 2 and 3. In *Actes de la Conférence "Théorie des Nombres et Applications"*, Publ. Math. Besançon Algèbre Théorie Nr., pages 99–117. Presses Univ. Franche-Comté, Besançon, 2011.

[36] M. Rosenlicht. Equivalence relations on algebraic curves. *Ann. of Math. (2)*, 56 :169–191, 1952.

[37] H.-G. Rück and H. Stichtenoth. A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.*, 457 :185–188, 1994.

[38] J.-P. Serre. Faisceaux algébriques cohérents. *Ann. of Math. (2)*, 61 :197–278, 1955.

[39] J.-P. Serre. *Groupes algébriques et corps de classes*. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[40] J.-P. Serre. Nombres de points des courbes algébriques sur $\mathbf{F}_q$. In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.

[41] J.-P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9) :397–402, 1983.

[42] J.-P. Serre. *Rational points on curves over finite fields*. Springer-Verlag, New York-Heidelberg, 1985. Lectures given at Harvard University, Notes by F.Q. Gouvea.

[43] F. Severi. Fondamenti per la geometria sulle varietà algebriche. II. *Ann. Mat. Pura Appl. (4)*, 32 :1–81, 1951.

[44] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[45] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[46] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[47] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes : basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[48] G. van der Geer, E. W. Howe, K. E. Lauter, and C. Ritzenthaler. Tables of curves with many points. 2009. Retrieved 30/04/2016.

[49] J. Voight. Curves over finite fields with many points : an introduction. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 124–144. World Sci. Publ., Hackensack, NJ, 2005.

[50] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2 :521–560, 1969.

[51] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1) :281–315, 1929.

[52] A. Weil. *Variétés abéliennes et courbes algébriques.* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[53] O. Zariski. The concept of a simple point of an abstract algebraic variety. *Trans. Amer. Math. Soc.*, 62 :1–52, 1947.

[54] O. Zariski. Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi. *Ann. of Math. (2)*, 55 :552–592, 1952.

Résumé

On s'intéresse, dans cette thèse, à des questions concernant le nombre maximum de points rationnels d'une courbe singulière définie sur un corps fini, sujet qui, depuis Weil, a été amplement abordé dans le cas lisse. Cette étude se déroule en deux temps. Tout d'abord on présente une construction de courbes singulières de genres et corps de base donnés, possédant un grand nombre de points rationnels : cette construction, qui repose sur des notions et outils de géométrie algébrique et d'algèbre commutative, permet de construire, en partant d'une courbe lisse X, une courbe à singularités X', de telle sorte que X soit la normalisée de X', et que les singularités ajoutées soient rationnelles sur le corps de base et de degré de singularité prescrit. Ensuite, en utilisant une approche euclidienne, on prouve une nouvelle borne sur le nombre de points fermés de degré deux d'une courbe lisse définie sur un corps fini. La combinaison de ces résultats, à priori indépendants, permet notamment d'étudier le problème de savoir quand la borne d'Aubry-Perret, analogue de la borne de Weil dans le cas singulier, est atteinte. Cela nous amène de façon naturelle à l'étude des propriétés des courbes maximales et, lorsque la cardinalité du corps de base est un carré, à l'analyse du spectre des genres de ces dernières.

Mots-clés : courbe singulière, courbe maximale, corps fini, point rationnel, point de degré deux, fonction zêta.

Abstract

In this PhD thesis, we focus on some issues about the maximum number of rational points on a singular curve defined over a finite field. This topic has been extensively discussed in the smooth case since Weil's works. We have split our study into two stages. First, we provide a construction of singular curves of prescribed genera and base field and with many rational points: such a construction, based on some notions and tools from algebraic geometry and commutative algebra, yields a method for constructing, given a smooth curve X, another curve X' with singularities, such that X is the normalization of X', and the added singularities are rational on the base field and with the prescribed singularity degree. Then, using a Euclidian approach, we prove a new bound for the number of closed points of degree two on a smooth curve defined over a finite field. Combining these two a priori independent results, we can study the following question: when is the Aubry-Perret bound (the analogue of the Weil bound in the singular case) reached? This leads naturally to the study of the properties of maximal curves and, when the cardinality of the base field is a square, to the analysis of the spectrum of their genera.

Keywords : singular curve, maximal curve, finite field, rational point, point of degree two, zeta function.