université de BORDEAUX

université de BORDEAUX

THÈSE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX

ECOLE DOCTORALE MATHÉMATIQUES ET

INFORMATIQUE

MATHÉMATIQUES PURES

Par **Jean GASNIER**

Arithmétique et algorithmique des courbes algébriques et applications aux codes correcteurs et à la cryptographie

Sous la direction de : **Jean-Marc COUVEIGNES**

Soutenue le 10 juillet 2025, devant le jury présidé par : **Alain COUVREUR**

et composé de :

M. Alain COUVREUR	Directeur de Recherche INRIA	INRIA Saclay	Rapporteur
M. Pierrick GAUDRY	Directeur de Recherche CNRS	LORIA	Rapporteur
M. David KOHEL	Professeur des universités	Aix-Marseille Université	Examinateur
Mme Elisa LORENZO-GARCÍA	Maîtresse assistante	Université de Neuchâtel	Examinatrice
M. Jean-Marc COUVEIGNES	Professeur des universités	Université de Bordeaux	Directeur

Arithmétique et algorithmique des courbes algébriques et applications aux codes correcteurs et à la cryptographie

Résumé : L'arithmétique et l'algorithmique élémentaires des courbes algébriques est au cœur de contributions majeures à la théorie des codes correcteurs d'erreurs et à la cryptologie. Ce travail de thèse mobilise des notions plus avancées, provenant de la théorie du corps de classes, de la théorie de Riemann–Roch équivariante, et de la géométrie arithmétique des jacobiennes, pour établir un cadre général adapté à ces constructions et en améliorer l'efficacité.

On étudie notamment les propriétés de codes linéaires munis d'une structure de module sur l'algèbre d'un groupe fini G. On étudie plus spécifiquement les codes munis d'une structure de sous-module libre d'un module libre, et leur dualité. En particulier, on montre que ces codes peuvent être représentés par des matrices de contrôle à coefficients dans l'algèbre du groupe G. Dans le cas où G est commutatif, la transformée de Fourier rapide confère de bonnes propriétés algorithmiques à ces codes correcteurs. On montre aussi comment construire ces codes à l'aide de revêtements abéliens non ramifiés de courbes projectives lisses, et l'on donne les premiers exemples de codes correcteurs excellents encodables en temps quasi-linéaire et décodables en temps quasi-quadratique.

Une autre application concerne la construction de familles de courbes elliptiques à couplages, exploitées dans certains protocoles cryptographiques. La théorie de la multiplication complexe permet de réduire le problème géométrique sous-jacent à un problème d'arithmétique cyclotomique. On déduit de l'étude de ce problème une méthode unifiée de construction de familles de courbes elliptiques à couplages.
Mots-clés : Codes correcteurs, Cryptographie, Courbes algébriques, Géométrie Arithmétique, Théorie du corps de classes, Corps finis

---

Arithmetics and algorithmics of algebraic curves and applications to coding theory and cryptography

Abstract: The elementary arithmetics and algorithmics of algebraic curves is at the heart of major contributions to coding theory and cryptology. This PhD thesis draws on more advanced concepts, from class field theory, equivariant Riemann-Roch theory and the arithmetic geometry of jacobian varieties, to establish a general framework adapted to these constructions and improve their efficiency.

In particular, we study the properties of linear codes endowed with a module structure over the algebra of a finite group G. We study more specifically the codes endowed with a structure of free submodule of a free module, and their duality. Specifically, we show that these codes can be described by parity check matrices whose coefficients belong to the algebra of the group G. When G is commutative, the fast Fourier transform provides nice algorithmic properties to these error-correcting codes. We also show how to build these codes, using unramified abelian coverings of smooth projective curves, and we give the first examples of excellent codes encodable in quasi-linear time and decodable in quasi-quadratic time.

Another application involves the generation of families of pairing-friendly elliptic curves, used in some cryptographic protocols. The complex multiplication theory allows to reduce the underlying geometric problem to a problem of cyclotomic arithmetics. We deduce from the study of this problem an unified method of generation of families of pairing-friendly elliptic curves.
Keywords: Coding theory, Cryptography, Algebraic curves, Arithmetic Geometry, Class field theory, Finite fields

---

Unité de recherche
UMR 5251, Université de Bordeaux, Bordeaux INP, CNRS, INRIA, 33400 Talence, France.

Table des matières

Remerciements

Je veux adresser mes premiers remerciements à mon directeur, Jean-Marc Couveignes, pour son aide et ses précieux conseils tout au long de ces trois ans de thèse. Tu as été un directeur exceptionnel, et j'ai grandement apprécié travailler avec toi. Il est difficile d'écrire ici tout ce que tu m'as apporté, alors, sobrement, merci pour tout.

Je tiens également à remercier Pierrick Gaudry, Alain Couvreur, David Kohel et Elisa Lorenzo-García d'avoir accepté de faire partie de mon jury de thèse, et en particulier Pierrick et Alain pour avoir accepté de relire ce document en tant que rapporteurs.

Je remercie également tous les membres de l'équipe CANARI, et plus généralement tous les collègues bordelais que j'ai cotoyés. Ces trois ans ont été très interessants et agréables, et l'ambiance dans l'équipe CANARI et l'équipe de théorie des nombres y a grandement participé. En particulier, merci Damien, Aurel, Alice, Bill, Henri, Andreas, Razvan, Elena, Léo, Maxime, Wessel et Sabrina d'avoir répondu à mes interrogations.

Je remercie également Aurore Guillevic, avec qui j'ai écrit mon premier article, et qui m'a appris beaucoup de bonnes pratiques pour la rédaction d'articles, l'utilisation de Sagemath, et aussi des aspects moins scientifiques du travail de recherche.

Je remercie mes camarades du bureau 319, Fabrice, Nicolas, Pierrick et Wouter, pour tous les bons moments partagés durant ces trois ans. Merci également à Agathe, Guilhem, Fabrice, Afonso, Rayane et tous les doctorants et stagiaires de l'IMB avec qui j'ai bien ri.

À ma famille : je vous aime. Merci pour tout.

Notations

Notations générales

On note :

$[a..b]$	pour des entiers $a \leqslant b$, l'ensemble des entiers entre a et b.
ν_p	pour un premier p, la valuation p-adique.
$\mathbb{N}$	ensemble des entiers naturels.
$\mathbb{F}_p$	pour p un premier, le corps fini à p éléments.
$\mathbb{P}^1$	la droite projective.
$\mathbb{H}$	le demi-plan complexe supérieur.
$\mathrm{Re}(z)$	pour z un complexe, la partie réelle de z.
$O(f(n))$	l'ensemble des fonctions g t.q. il existe $B \in \mathbb{R}$ telle que $g(n) \underset{n\to\infty}{\leqslant} Bf(n)$.
$\lfloor . \rfloor$	la partie entière.
$\lceil . \rfloor$	l'arrondi au plus proche entier.
I_n	pour $n > 0$ un entier, la matrice identité de taille n.
M^t	pour M une matrice, la transposée de M.

Courbes algébriques

Ici :

— K désigne un corps fini.

— L désigne une extension algébrique de K.

— X désigne une courbe projective lisse absolument intègre sur K.

— Y désigne une courbe projective lisse absolument intègre sur K, munie d'un revêtement $\tau : Y \longrightarrow X$.

On note :

X_L	la courbe sur L canoniquement associée à X.
$L(X)$	le corps de fonction de X_L.
$X(L)$	les places de degré 1 de $L(X)$, i.e. les points L-rationnels de X_L.
$\mathrm{Irr}(X)$	l'ensemble des places de $K(X)$.
$\mathrm{Irr}^d(X)$	pour $d > 0$ un entier, l'ensemble des places de degré d.
ν_P	pour P une place de $K(X)$, la valuation de $K(X)$ associée à P.
$\mathcal{O}_P$	pour P une place de $K(X)$, l'anneau de valuation de ν_P.

K_P	pour P une place de $K(X)$, le corps résiduel en P.
$\mathrm{Div}(X)$	le groupe des diviseurs de X.
$\mathrm{supp}\, D$	pour $D \in \mathrm{Div}(X)$, l'ensemble des places P t.q. $\nu_P(D) \neq 0$.
$\deg D$	pour $D \in \mathrm{Div}(X)$, le degré de D.
(f)	pour $f \in K(X)$, le diviseur de f.
$f(P)$	pour $P \in X(K)$ et $f \in K(X)$ régulière en P, l'évaluation de f en P.
$\mathrm{Princ}(X)$	le sous-groupe des diviseurs principaux de X.
$\mathrm{Eff}(X)$	l'ensemble des diviseurs effectifs de X.
$\mathcal{O}_X$	le faisceau des fonctions régulières sur X.
$\mathcal{O}_X(D)$	pour $D \in \mathrm{Div}(X)$, le faisceau de fonctions sur X associé à D.
Γ_X	le foncteur des sections globales sur X.
$\Omega(X/K)$	l'espace des différentielles de X (relativement à K).
df	pour $f \in K(X)$, la différentielle associée à f.
$\mathrm{div}\, \omega$	pour $\omega \in \Omega(X/K)$, le diviseur de ω.
$\mathrm{Res}_P(\omega)$	pour $p \in X(K)$ et $\omega \in \Omega(X/K)$ t.q. $\nu_P(\omega) \geqslant -1$, le résidu de ω en P.
$\Omega_{X/K}(D)$	pour $D \in \mathrm{Div}(X)$, le faisceau de différentielles associé à D.
$D \sim D'$	pour $D, D' \in \mathrm{Div}(X)$, désigne que D et D' sont équivalents.
$\mathrm{Pic}(X)$	le groupe de Picard de X.
$\mathrm{Pic}^d(X)$	pour $d \in \mathbb{Z}$, le sous-ensemble des classes de $\mathrm{Pic}(X)$ de degré d.
$\mathcal{J}_X$	la jacobienne de X.
$\mathcal{J}_X(K)$	les points K-rationnels de la jacobienne de X.
$\mathcal{J}_X[n]$	pour $n \in \mathbb{Z}$, la n-torsion de la jacobienne.
$\mathcal{J}_X[n](K)$	pour $n \in \mathbb{Z}$, la n-torsion K-rationnelle de $\mathcal{J}_X$.
$D(Q/P)$	pour $P \in \mathrm{Irr}(X)$ et $Q \in \mathrm{Irr}(Y)$ au-dessus de P, le groupe de décomposition de Q.
$I(Q/P)$	pour $P \in \mathrm{Irr}(X)$ et $Q \in \mathrm{Irr}(Y)$ au-dessus de P, le groupe d'inertie de Q.

Corps de nombres

Ici :

— $\mathcal{K}$ désigne un corps de nombres.

— $\mathcal{L}$ désigne une extension finie de $\mathcal{K}$.

On note :

$\mathbb{Z}_\mathcal{K}$	l'anneau des entiers de $\mathcal{K}$.
$\nu_\mathfrak{p}$	pour $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_\mathcal{K}$, la valuation $\mathfrak{p}$-adique.
$\mathcal{K}_\mathfrak{p}$	pour $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_\mathcal{K}$, le corps résiduel en $\mathfrak{p}$.
$D(\mathfrak{P}/\mathfrak{p})$	pour $\mathfrak{p}$ et $\mathfrak{P}$ des idéaux premiers de $\mathcal{K}$ et $\mathcal{L}$, le groupe de décomposition de $\mathfrak{P}$.
$I(\mathfrak{P}/\mathfrak{p})$	pour $\mathfrak{p}$ et $\mathfrak{P}$ des idéaux premiers de $\mathcal{K}$ et $\mathcal{L}$, le groupe d'inertie de $\mathfrak{P}$.
$I(\mathcal{K})$	le groupe des idéaux fractionnaires non nuls de $\mathbb{Z}_\mathcal{K}$.
$P(\mathcal{K})$	le groupe des idéaux fractionnaires principaux de $\mathbb{Z}_\mathcal{K}$.
$\mathrm{Cl}(\mathcal{K})$	le groupe de classes de $\mathcal{K}$.
$\mathrm{cl}(\mathcal{K})$	le nombre de classes de $\mathcal{K}$.

$\mathrm{Hil}(\mathcal{K})$ le corps de classes de Hilbert de $\mathcal{K}$.

Chapitre 1

Introduction

Depuis le début des années 80, les contributions provenant de la géométrie algébrique à la cryptographie et aux codes correcteurs d'erreurs se sont largement développées. D'une part, Goppa a défini des codes correcteurs en étudiant le morphisme d'évaluation des fonctions d'un espace linéaire associé à un diviseur d'une courbe algébrique. Ces codes généralisent les célèbres codes de Reed-Solomon, et possèdent d'excellentes propriétés. D'autre part, suite à l'attaque du Problème du Logarithme Discret (abrégé en DLP d'après l'anglais) sur les corps finis par des algorithmes basés sur le *calcul d'indice* (*index calculus* en anglais), la communauté des cryptographes a commencé à concevoir et étudier des protocoles dont la sécurité repose sur le DLP sur des courbes elliptiques. Plus tard, dans les années 2000, une branche de cette théorie étudie les protocoles utilisant des couplages. Ces protocoles nécessitent des courbes elliptiques particulières, dites *à couplages*, et un pan de la littérature sur ce sujet développe des méthodes de construction de ces courbes. Dans cette thèse, on étudie une nouvelle construction de codes de Goppa disposant d'une structure additionnelle, ainsi qu'une méthode générale de construction de familles de courbes à couplages. Ces contributions relèvent de l'arithmétique et de la géométrie algorithmiques, et mobilisent notamment la théorie du corps de classes des corps de nombres et de fonctions.

Codes de Goppa

Soit K un corps fini à q éléments, et soit n un entier. Un code linéaire de longueur n est un sous-espace vectoriel d'un K-espace vectoriel de dimension n muni d'une distance, par exemple K^n muni de la distance de Hamming

$$d : K^n \times K^n \longrightarrow \mathbb{N}$$

qui à toute paire de vecteurs de K^n associe le nombre de coordonnées non nulles de leur différence. On appelle mots du code les éléments de ce sous-espace vectoriel.

Un problème classique consiste à déterminer, étant donné un élément de l'espace vectoriel ambiant, le mot le plus proche (ou un des mots les plus proches, s'il y en a plusieurs). Il est commun de se restreindre à résoudre ce problème uniquement pour les éléments à distance

au plus t d'un mot du code, où t est un entier positif. Soit d la distance minimale entre deux mots du code. Si $t < d/2$, tout élément de K^n compte au plus un mot du code à distance inférieure à t. Dans ce cas, la résolution du problème consiste à donner, s'il existe, l'unique mot du code dans la sphère de rayon t centrée en l'élément considéré. On appelle ce problème le *problème du décodage*.

À dimension fixée, la distance minimale détermine la capacité de correction t maximale du code. La borne de Singleton majore la distance minimale d pour une longueur n et une dimension k données :

$$k + d \leqslant n + 1.$$

On appelle MDS les codes qui atteignent cette borne. Peu de codes MDS sont connus, et les plus connus sont les codes de Reed–Solomon. Ces codes sont définis comme les vecteurs de K^n (muni de la distance de Hamming) dont les composantes sont les évaluations d'un polynôme de degré au plus $k-1$ en n éléments distincts de K fixés. Un défaut des codes de Reed–Solomon est leur longueur, limitée à q par définition.

Les codes géométriques de Goppa, aussi appelés codes AG, sont une généralisation des codes de Reed–Solomon. Soit X une courbe projective lisse absolument intègre sur K de genre g. Soient $P_1, \ldots, P_n$ des points deux à deux distincts de X, et soit D un diviseur sur X disjoint de $P = P_1 + \cdots + P_n$. Le sous-espace vectoriel de K^n (muni de la distance de Hamming) composé des vecteurs dont les composantes sont les valeurs d'une fonction de l'espace linéaire associé à D en les $(P_i)_{i\in[1..n]}$ est appelé code géométrique de Goppa associé à D et P.

Les codes de Goppa ne sont pas des codes MDS en général, mais leurs longueur n, dimension k et distance minimale d vérifient la relation

$$k + d \geqslant n + 1 - g,$$

car une fonction rationnelle ne peut pas s'annuler en plus de points que son degré. Les travaux de Ihara, et Tsfasman, Vladut et Zink ont démontré que sous certaines conditions sur K (e.g. l'ordre de K est un carré), il existe des courbes avec un nombre de points n suffisamment important pour que le défaut lié à leur genre g ne soit pas préjudiciable.

Contributions aux codes de Goppa

Dans les années 90, on a cherché des algorithmes de décodage pour les codes de Goppa généralisant les algorithmes de décodage des codes de Reed–Solomon. Il a été démontré qu'il est possible de décoder ces codes pour $t < d/2$ en $O(n^3)$ opérations dans K. Il faut savoir que décoder un code linéaire quelconque est un problème NP-difficile, et que les meilleurs algorithmes probabilistes connus décodant des codes linéaires aléatoires ont une complexité exponentielle en le poids de l'erreur. Ainsi la structure provenant de la géométrie algébrique des codes de Goppa les rend également performants du point de vue algorithmique. De plus, comme tout les codes linéaires, il est possible d'encoder, c'est-à-dire de calculer un élément du code à partir de ses coordonnées dans une base, en $O(n^2)$ opérations dans K.

Cependant, du point de vue applicatif, les codes de Goppa sont toujours considérés comme trop inefficaces, comparés par exemple aux codes de Reed-Solomon. Un des objectifs de la recherche sur ces codes est donc de trouver des algorithmes d'encodage et de décodage plus efficaces.

Dans ce document, on définit une sous-famille de codes de Goppa, dont on montre que les performances algorithmiques sont améliorées. Ces codes sont définis sur des courbes Y disposant d'un revêtement abélien non-ramifié au-dessus d'une autre courbe X :

$$\tau : Y \longrightarrow X.$$

Soit G le groupe de Galois de τ. Soit D un diviseur sur X et E son tiré en arrière sur Y. Soient $P_1, \ldots, P_n$ des points K-rationnels sur X totalement décomposés dans Y, et soit Q l'ensemble des points dans les fibres au-dessus de $P_1, \ldots, P_n$. Le diviseur E est stable par l'action de G, donc G agit sur les fonctions de $L(E)$. De plus, G agit sur les fibres de τ et donc agit sur Q. Enfin, l'évaluation des fonctions de $L(E)$ en Q est compatible avec l'action de G. On peut alors voir le code de Goppa associé à Q et E comme un $K[G]$-module. De plus, sous des hypothèses habituelles, on peut montrer que c'est un $K[G]$-module libre, ce qui signifie que l'action de G est très pertinente pour décrire le code.

En utilisant cette structure de $K[G]$-module, on peut définir des matrices génératrices de ces codes de Goppa dont les coefficients sont des éléments de $K[G]$. Il est possible d'utiliser la transformée de Fourier rapide (FFT) pour calculer rapidement les multiplications dans $K[G]$. Lorsque l'ordre de G est très important relativement à n, la complexité des algorithmes d'encodage et de décodage est diminuée. Plus précisément, on peut montrer que dans ce cas favorable, ces codes sont encodables en temps quasi-linéaire en leur longueur, et décodables en temps quasi-quadratique.

Il est également possible de démontrer que, sous certaines conditions sur K plus contraignantes que pour les codes de Goppa classiques, ces codes sont asymptotiquement excellents. Plus précisément, il est possible de trouver une famille de courbes, sur lesquelles agissent des groupes de Galois d'ordre suffisamment important pour que les algorithmes d'encodage et de décodage aient des complexités quasi-linéaire et quasi-quadratique, et disposant de suffisamment de points K-rationnels pour dépasser la borne de Gilbert–Varshamov.

Cette construction est la première construction de codes de Goppa ayant à la fois de bonnes propriétés asymptotiques et un algorithme de codage quasi-linéaire. À titre de comparaison, dans [NW19], les auteurs construisent une famille de codes de Goppa asymptotiquement bonne, et dont l'encodage a une complexité sous-quadratique en la longueur du code. Dans [BRS21], les auteurs montrent que les codes de Goppa provenant de courbes C_{ab} peuvent être encodés en temps quasi-linéaire. Cependant, comme pour les codes de Reed–Solomon, ces codes ont une longueur bornée $n \leqslant q^2$, et ne peuvent pas être considérés comme asymptotiquement bons.

Ce travail a donné lieu à l'article «Explicit Riemann-Roch spaces in the Hilbert class field », accepté pour publication dans les actes de la conférence AGC2T 2023.

Cryptographie basée sur les couplages

Soit K un corps fini, et soit E/K une courbe elliptique. La courbe E est naturellement isomorphe à sa jacobienne, et dispose donc d'une structure de groupe algébrique. Les points K-rationnels de E, notés $E(K)$ forment un groupe abélien fini ayant au plus 2 facteurs invariants. Soit G un sous-groupe cyclique de $E(K)$. On peut utiliser G pour instancier des protocoles cryptographiques dont la sécurité repose sur le DLP, comme par exemple l'échange de clé Diffie-Hellman. Le principal avantage de l'utilisation des courbes elliptiques pour instancier les protocoles basés sur le DLP réside dans le fait qu'en dehors de certains cas particuliers, aucun algorithme connu n'est plus efficace que les méthodes génériques (celles se basant exclusivement sur des opérations de groupe) pour résoudre le logarithme discret dans le groupe G.

Soit n_E le nombre de points K-rationnels de E, et r le plus grand facteur premier de l'ordre de G. On sait qu'en utilisant l'algorithme de Pohlig–Hellman et l'algorithme Baby-Step Giant-Step, il est possible de calculer un logarithme discret en $O(\sqrt{r})$ opérations dans G. Ainsi, pour maximiser la sécurité des protocoles cryptographiques sur G, il est préférable de choisir pour E une courbe elliptique telle que n_E ait un important facteur premier r, et de prendre G le sous-groupe d'ordre r de $E(K)$ (unique car $r > \sqrt{n_E}$). On demande également que r soit premier à la caractéristique de K.

Il est possible de définir des couplages sur les courbes elliptiques, c'est-à-dire des morphismes de groupes bilinéaires prenant en entrée deux points de la courbe et leur associant un élément non nul dans une extension finie de K. Par exemple, le couplage de Weil

$$e_r : E[r] \times E[r] \longrightarrow \mu_r$$

prend en entrée des points de r-torsion de la courbe, et renvoie une racine r-ième de l'unité. Depuis le début des années 2000, plusieurs articles utilisent les couplages pour définir de nouveaux protocoles de sécurité, comme par exemple l'échange de clés triparti de Joux [Jou00]. Pour que ces algorithmes soient efficaces, il faut que le degré k de l'extension K_r de K définie par les racines r-ièmes de l'unité soit le plus petit possible. Il est cependant extrêmement rare que k soit significativement plus petit que r (en général $\log\ k \approx \log\ r$). On appelle *courbes à couplages* les courbes dont le *degré de plongement* k est suffisamment petit pour que le couplage soit calculable en pratique. On considère communément qu'il faut avoir $k \leqslant 54$ pour qu'une courbe soit à couplages.

D'autre part, Menezes, Okamoto et Vanstone ont démontré qu'en utilisant les couplages, il était possible de réduire le DLP dans G (i.e. sur la courbe elliptique) au DLP dans K_r^*. Or le DLP dans K_r^* est résolu en temps sous-exponentiel par les algorithmes basés sur le calcul d'indices. Pour garantir un niveau de sécurité suffisant, il faut que k soit suffisamment grand pour que calculer un logarithme discret dans K_r^* requière au moins autant d'opérations que de calculer un logarithme discret dans G.

Ces injonctions contradictoires entre sécurité et efficacité ont conduit à développer des méthodes pour produire des courbes à couplages avec des paramètres prédéfinis (k par exemple), pour pouvoir par la suite optimiser le choix de ces paramètres, et déterminer des

courbes pour lesquelles les protocoles à base de couplages sont à la fois sécurisés et les plus efficaces.

Contribution à la génération de courbes à couplages

Soit $k > 1$ un entier fixé. Le problème de la génération de courbes à couplages est de trouver K un corps fini d'ordre q et E/K une courbe elliptique avec un sous-groupe de points K-rationnels d'ordre r premier différent de la caractéristique de K, tel que le degré de l'extension K_r/K soit k. On demande également pour garantir la difficulté du DLP que $r > 2^{2s}$, où s est un entier désignant le niveau de sécurité souhaité, et pour des raisons algorithmiques que $\log\ q < 2 \log\ r$. Dans cette thèse, on ne considérera que des courbes ordinaires. On note t la trace de la courbe E, alors $\mathrm{pgcd}(t, q) = 1$.

La manière habituelle de procéder consiste à trouver des entiers q, t et r remplissant les conditions nécessaires à l'existence d'une telle courbe. Par exemple, si q est une puissance de premier, si $\mathrm{pgcd}(t, q) = 1$ et si $|t| \leqslant 2\sqrt{q}$, on sait qu'il existe une courbe elliptique de trace t sur un corps à q éléments. En ajoutant des conditions supplémentaires concernant r et k, on obtient un ensemble de conditions nécessaires et suffisantes à l'existence d'une solution au problème considéré. De plus, si q est premier, la méthode de la multiplication complexe d'Atkin et Morain [AM93] permet d'obtenir le j-invariant de la courbe solution lorsque le discriminant de la courbe n'est pas trop grand.

Dans de nombreux cas, on cherche en réalité des familles de courbes à couplages dont le degré de plongement est k. En général, on cherche une famille $(E_i)_{i\in\mathbb{N}}$ paramétrée par des polynômes à coefficients rationnels Q, R et T, c'est-à-dire telle qu'il existe des entiers $(x_i)_{i\in\mathbb{N}}$ tels que pour tout $i \in \mathbb{N}$, la courbe E_i est définie sur un corps fini à $Q(x_i)$ éléments, à trace $T(x_i)$, et dispose d'un sous-groupe de points rationnels d'ordre $R(x_i)$, par rapport auquel son degré de plongement est k. Naturellement, pour que cela soit possible, les polynômes Q, R et T doivent satisfaire des conditions arithmétiques, similaires aux conditions posées précédemment sur les entiers q, r et t. Pour trouver des familles de courbes à couplages on cherche à trouver des triplets de polynômes satisfaisant ces conditions.

Pour contrôler la qualité d'une telle famille, on se base généralement sur la valeur ρ

$$\rho = \frac{\deg Q}{\deg R}.$$

Plus ρ est proche de 1, plus l'arithmétique des courbes de la famille sera efficace.

Dans ce document, on présente une méthode pour produire de tels polynômes. Cette méthode reprend l'approche de Kachisa, Schaeffer et Scott [KSS08], qui remarquent que le polynôme R peut être vu comme le polynôme minimal d'un élément d'un corps de nombres bien choisi. Ils utilisent une recherche exhaustive sur ces nombres algébriques pour produire des familles de courbes paramétrées. La nouvelle méthode généralise et précise cette approche en identifiant des nombres algébriques produisant des familles dont la valeur ρ est majorée.

Pour sélectionner et exploiter ces polynômes, il faut résoudre un problème algorithmique : étant donné un polynôme à coefficients entiers P, p un nombre premier et $n > 1$ un entier positif, résoudre pour une variable $x \in \mathbb{Z}$

$$P(x) \equiv 0 \bmod p^n.$$

Le lemme de Hensel permet de résoudre ce genre d'équations quand P a des racines simples modulo p, en relevant les solutions modulo p en solutions modulo p^n. De manière surprenante, il est difficile de trouver dans la littérature une résolution de ce problème dans le cas où P a une racine multiple modulo p. On détaille donc un algorithme résolvant ce problème dans le cas général.

On montre que la nouvelle méthode permet de produire des familles de meilleure qualité pour le cas $k = 22$ (et $k = 46$), et produit des alternatives aux familles déjà connues pour plusieurs valeurs de k. D'autre part, notre approche permet d'uniformiser plusieurs résultats précédents parmi les plus performants, et de mieux les comprendre. Par exemple, il est expliqué pourquoi tant de familles produites par des méthodes différentes ont des valeurs-ρ suivant une formule unifiée. Ce travail a donné lieu à l'article «An Algebraic Point of View on the Generation of Pairing-Friendly Curves », co-écrit avec Aurore Guillevic, publié dans le journal SIAGA [GG25].

Organisation de la thèse

Dans le **chapitre** 2, on définit les notions et notations relatives aux courbes algébriques et corps de fonctions que nous allons utiliser dans le reste de la thèse. On discute également de la représentation algorithmique de ces objets. Plus précisément, on dresse une liste de conditions qui doivent être satisfaites pour qu'une représentation algorithmique soit jugée satisfaisante. Enfin, on montre qu'en faisant ces hypothèses algorithmiques, il est possible de tirer au sort uniformément dans le sous-groupe rationnel de la jacobienne, de calculer sa structure en tant que groupe abélien et de calculer le couplage de Weil.

Dans le **chapitre** 3, on rappelle quelques résultats de la théorie du corps de classes, pour les corps de nombres et pour les corps de fonctions. On présente également quelques aspects effectifs de cette théorie pour les corps de nombres quadratiques imaginaires, et l'application de la théorie pour les corps de fonctions à la construction de courbes ayant beaucoup de points rationnels. En particulier, on présente de nouvelles courbes ayant des nombres records de points.

Dans le **chapitre** 4, après de rapides rappels sur les codes linéaires et les codes de Goppa, on présente une nouvelle construction de codes géométriques avec une structure de $K[G]$-module. On étudie l'arithmétique de $K[G]$, pour G un groupe abélien, et en particulier un algorithme utilisant la FFT pour calculer rapidement des produits dans $K[G]$, dont on donne la complexité. Ensuite, on étudie des codes linéaires ayant une structure de $K[G]$-module libre, pour G un groupe fini non nécessairement abélien. Ces codes sont des cas particuliers de quasi-G codes. En particulier, on présente quelques résultats de dualité dans ce contexte. On montre que ces codes peuvent être décrits par de l'algèbre linéaire

sur $K[G]$, similairement aux codes linéaires. Enfin, on montre que certains codes de Goppa construits à partir d'un revêtement galoisien de groupe de Galois G

$$\tau : Y \longrightarrow X$$

possèdent une structure de $K[G]$-module. Dans le cas où G est abélien et où le revêtement τ est non-ramifié, on donne des conditions suffisantes sur les diviseurs de Y pour que les espaces linéaires (de fonctions et de différentielles) associés soient des $K[G]$-modules libres. On étudie l'encodage, le décodage, et les propriétés asymptotiques de ces codes.

Dans le **chapitre** 5, on rappelle quelques principes de la cryptographie basée sur le logarithme discret dans les courbes elliptiques, et on présente rapidement la cryprographie à base de couplages. On détaille des méthodes classiques de génération de courbes à couplages, et de familles de courbes à couplages. En particulier, on détaille la méthode de Kachisa–Schaefer–Scott. Ensuite, on présente la nouvelle méthode de génération de familles de courbes, implémentée en Sagemath [The22] dans [Gas23]. On explique son fonctionnement, puis on présente les résultats produits. En particulier, on présente la nouvelle famille de courbes obtenue pour le degré de plongement $k = 22$. Enfin, on présente un algorithme général résolvant les équations de la forme

$$P(x) \equiv 0 \bmod p^n$$

pour P un polynôme à coefficients entiers, p un nombre premier, $n > 1$ un entier et x une variable à valeurs entières. On explique son utilité pour la recherche exhaustive de polynômes paramétrant des familles de courbes à couplages.

Le **chapitre** 6 contient l'annexe de cette thèse. On y présente des tables de résultats et des preuves de certaines propositions utilisées dans ce document, qui ne sont pas au cœur du sujet d'étude de la thèse.

Chapitre 2

Corps de fonctions et jacobiennes

Les courbes projectives lisses et leurs jacobiennes sont les objets fondamentaux qui nous intéressent dans ce document. En particulier, nous nous intéressons à leurs aspects algorithmiques. Dans ce chapitre, nous présentons dans la section 2.1 un cahier des charges de la représentation algorithmique des corps de fonctions de courbes et d'autres objets associés, consistant en une liste d'opérations qu'il doit être possible d'effectuer en un temps raisonnable pour répondre à nos besoins dans les prochains chapitres. Dans la section 2.2, nous examinons la représentation algorithmique de la jacobienne et présentons des algorithmes utilisant les opérations élémentaires que nous allons définir, lesquels seront utiles pour les applications abordées dans les chapitres suivants.

On commence par fixer quelques définitions. Soit K un corps parfait. On appelle variété affine sur K tout schéma affine associé à une K-algèbre de type fini. On appelle variété algébrique sur K tout schéma sur K (géométriquement) réduit disposant d'un recouvrement fini par des sous-variétés affines sur K. On appelle courbe algébrique sur K toute variété sur K géométriquement irréductible de dimension 1. En particulier, dans cette thèse, toute courbe algébrique sur K est géométriquement intègre.

Bien que plusieurs notions développées dans ce chapitre soient bien définies pour n'importe quel corps parfait K, nous serons principalement intéréssés par le cas des corps finis. Pour cette raison, il convient de préciser nos hypothèses concernant la représentation algorithmique des corps finis. Nous demandons essentiellement deux choses : des garanties sur la taille de la représentation des éléments et sur la complexité des opérations arithmétiques dans le corps, et la possibilité d'évaluer efficacement les morphismes entre corps finis. La deuxième contrainte a un intérêt dans notre contexte géométrique car il arrive régulièrement que la résolution de certains problèmes algorithmiques requière l'extension du corps de base ou d'appliquer le morphisme de Frobenius.

Supposons momentanément que K soit un corps fini à $q = p^m$ éléments. Si $m = 1$, alors il existe un modèle canonique de K sous la forme $\mathbb{Z}/p\mathbb{Z}$, i.e. les entiers modulo p. Si $m > 1$, il n'y a pas de modèle canonique du corps à q éléments ni de morphisme canonique entre les différents modèles. On trouvera dans [LdS13] et [Lü23] des propositions de modèles standards cohérents pour les corps finis et leurs morphismes. Nous n'irons pas si loin dans la normalisation. On représentera les éléments de K par leurs $\mathbb{F}_p$-coordonnées dans une base

fixée. Dans ce modèle, on fait les hypothèses minimales sur la complexité : l'addition de deux éléments s'effectue en $O(\log\ q)$ opérations élémentaires ; la multiplication est réalisée au prix de $O(m^2)$ additions et multiplications dans $\mathbb{F}_p$; un morphisme entre deux corps finis est décrit par sa matrice dans les bases choisies. Il est également possible de tirer uniformément au sort un élément du corps.

2.1 Représentation algorithmique des corps de fonctions

Nous supposons que le lecteur est familier avec certains concepts de géométrie algébrique. Pour une présentation des corps de fonctions, le lecteur peut se référer au premier chapitre de [Sti08]. Le lecteur peut se référer au premier chapitre de [Har77] pour une introduction plus générale à la géométrie algébrique.

Soit K un corps parfait. Il existe une équivalence de catégories entre la catégorie des courbes projectives lisses sur K (avec les morphismes dominants), et la catégorie des corps de fonctions de degré de transcendance 1 sur K dans lesquels K est algébriquement clos (avec les morphismes de K-algèbre) [Liu02, Section 7, Proposition 3.13]. Cela signifie que la plupart des problèmes géométriques concernant les courbes projectives lisses sur K peuvent être traités en étudiant ces corps de fonctions.

2.1.1 Anneaux de valuation et places

Par souci de concision, nous adopterons la définition suivante :

Définition 1. Soit K un corps parfait. Soit $K(x)$ le corps des fractions rationnelles en une indéterminée sur K. Un **corps de fonctions** sur K est une extension de degré fini de $K(x)$ dans laquelle K est algébriquement clos.

Soit X une courbe projective lisse sur K, alors $K(X)$ le corps des fonctions rationnelles sur X est un corps de fonctions sur K. En particulier, le corps de fonctions de $\mathbb{P}^1$ est isomorphe au corps des fractions rationnelles en une indéterminée $K(x)$. Réciproquement, tout corps de fonctions sur K est isomorphe au corps des fonctions rationnelles sur X, une courbe projective lisse sur K. Cette courbe X est unique à isomorphisme près. On s'autorisera donc à écrire $K(X)$ pour désigner un corps de fonctions sur K.

Définition 2. Soit $K(X)$ un corps de fonctions sur K. Soit

$$\nu : K(X) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

On dit que ν est une **valuation discrète** de $K(X)$ si :

- $\nu(f) = \infty$ si et seulement si $f = 0$.
- $\nu(fg) = \nu(f) + \nu(g)$ pour tous $f, g \in K(X)$.
- $\nu(f + g) \geqslant \min(\nu(f), \nu(g))$ pour tous $f, g \in K(X)$.
- Il existe $t \in K(X)$ tel que $\nu(t) = 1$.

— $\nu(f) = 0$ pour toute constante $f \in K$.

Définition 3. Soit $K(X)$ un corps de fonctions sur K, et ν une valuation discrète sur $K(X)$.

— On appelle appelle **place** associée à ν l'ensemble $P = \{f \in K(X) \mid \nu(f) > 0\}$.

— On appelle **anneau de valuation** de ν l'anneau $\mathcal{O}_P = \{f \in K(X) \mid \nu(f) \geqslant 0\}$. La place P est l'unique idéal maximal de $\mathcal{O}_P$.

— On appelle **uniformisante** en P un élément $t \in P$ tel que $\nu(t) = 1$.

On appelle place de $K(X)$ toute place associée à une valuation discrète sur $K(X)$. Si P est une place de $K(X)$, on notera ν_P la valuation discrète à laquelle P est associée. On note $\mathrm{Irr}(X)$ l'ensemble des places de $K(X)$.

La notion de place correspond à la notion de point fermé de X. Soit $\mathcal{O}_X$ le faisceau des fonctions régulières sur X, alors $\mathcal{O}_P$ est l'ensemble des germes en P du faisceau $\mathcal{O}_X$. Soit Γ_X le foncteur des sections globales sur X. Le quotient

$$K_P := \mathcal{O}_P/P = \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$$

est le **corps résiduel** en P. Le **degré** de P, noté $\deg P$, est le degré de K_P sur K. On note $\mathrm{Irr}^d(X)$ l'ensemble des places de degré d de $K(X)$. On note

$$X(K) := \mathrm{Irr}^1(X)$$

l'ensemble des places de degré 1 de X (ou de manière équivalente l'ensemble des points fermés K-rationnels de X).

Soit L une extension algébrique de K, on associe naturellement à X une courbe projective lisse sur L, notée X_L. On notera $L(X)$ le corps de fonctions (sur L) de X_L. On a l'égalité suivante :

$$L(X) = L \otimes_K K(X).$$

On notera

$$X(L) := \mathrm{Irr}^1(X_L)$$

l'ensemble des places de degré 1 de $L(X)$ (ou de manière équivalente l'ensemble des points fermés de X_L).

Supposons que K est un corps fini à $q = p^m$ éléments. Du point de vue algorithmique, nous aurons besoin de représenter les fonctions dans $K(X)$ et les places de $K(X)$ d'une manière nous permettant de réaliser les tâches suivantes :

1. Étant donnés $\alpha \in K$ et $f \in K(X)$, calculer αf.
2. Étant données f_1 et f_2 deux fonctions de $K(X)$, calculer $f_1 + f_2$, $f_1 f_2$ et f_1/f_2 si $f_2 \neq 0$.
3. Étant donné un entier $d > 0$, calculer $\mathrm{Irr}^d(X)$.
4. Étant donné P une place de $K(X)$, calculer son degré.

5. Étant donnée une place P de $K(X)$, choisir une uniformisante en P.
6. Étant données une place P de $K(X)$ et une fonction $f \in K(X)$, calculer la multiplicité $\nu_P(f)$ du zéro de f en P.
7. Étant données une place P de $K(X)$ et une fonction $f \in \mathcal{O}_P$, évaluer f en P.
8. Étant données L une extension finie de K et $f \in K(X)$, calculer l'image de f dans $L(X)$.
9. Étant données L une extension finie de K et P une place de $K(X)$, donner l'ensemble des places de $L(X)$ au-dessus de P.
10. Étant données L une extension finie de K et Q une place de $L(X)$, donner la place P de $K(X)$ au-dessous de Q.
11. Étant données L une extension finie de K, Q une place de $L(X)$ et $f \in L(X)$ une fonction, calculer la place $F_K(Q)$ et la fonction $F_K(f)$ où $F_K : L(X) \longrightarrow L(X)$ est l'endomorphisme de Frobenius relatif sur K.

En particulier, l'exigence 5, l'exigence 6 et l'exigence 7 permettent le calcul du développement en série de Laurent de f en P.

2.1.2 Diviseurs

Soit K un corps parfait. Soit X une courbe projective lisse sur K et $K(X)$ son corps de fonctions.

Définition 4. On définit le **groupe de diviseurs** de X, noté $\mathrm{Div}(X)$, le groupe abélien libre engendré par les places de $K(X)$.

Définition 5. Soit ν_P une valuation discrète de $K(X)$, et $D = \sum_Q n_Q Q$ un diviseur de X. On définit

$$\nu_P(D) = n_P.$$

On appelle

$$\operatorname{supp} D = \{Q \in \mathrm{Irr}(X) \mid \nu_Q(D) \neq 0\}$$

le support de D.

Définition 6. Soit $D = \sum_P n_P P$ un diviseur de X, on appelle **degré** de D l'entier

$$\deg D = \sum_P n_P \deg P.$$

Définition 7. Soit $f \in K(X)^*$, on définit le diviseur de f comme

$$(f) \ = \ \sum_P \nu_P(f) P.$$

Rappellons qu'il existe un nombre fini de places P telles que $\nu_P(f) \neq 0$. Un diviseur est dit **principal** si c'est le diviseur d'une fonction rationnel. On note $\mathrm{Princ}(X)$ le sous-groupe des diviseurs principaux de X.

Définition 8. Soit $D = \sum_P n_P P$ un diviseur de X. On dit que D est **effectif** si n_P est positif pour toute place P, et on note $D \geqslant 0$. On note $\mathrm{Eff}(X)$ l'ensemble des diviseurs effectifs de X.

Remarque 1. Soit $f \in K(X)^*$. Il existe deux diviseurs effectifs $D_f^+, D_f^- \in \mathrm{Eff}$ de supports disjoints tels que

$$(f) = D_f^+ - D_f^-.$$

On dit que le **degré** de f est $\deg(D_f^+)$.

Définition 9. Soit D un diviseur de X, on appelle espace de **Riemann–Roch** associé à D, ou simplement espace linéaire (de fonctions) associé à D, l'espace vectoriel $\Gamma_X(\mathcal{O}_X(D))$ constitué de la fonction nulle et des fonctions rationnelles sur X vérifiant

$$(f) + D \geqslant 0.$$

Supposons que K est un corps fini. On utilisera la représentation algorithmique naturelle pour les diviseurs, i.e. la représentation comme collection finie de paires (n_P, P) où P est une place de $K(X)$ et n_P est la multiplicité associée. En particulier, étant donné un diviseur, on peut donner son support, et ses valuations en chaque place de $K(X)$. On peut également déterminer si deux diviseurs sont égaux.

Nous attendons également d'être capable d'effectuer les opérations suivantes :

1. Calculer le diviseur d'une fonction non nulle.
2. Étant donné D un diviseur de X, calculer la dimension k de $\Gamma_X(\mathcal{O}_X(D))$ et des fonctions $f_1, \ldots, f_k \in K(X)$ formant une base de $\Gamma_X(\mathcal{O}_X(D))$.

D'après le théorème de Riemann–Roch, il est possible de calculer le genre g de X en calculant la dimension d'un espace de Riemann–Roch de degré suffisamment grand.

2.1.3 Différentielles

Soit K un corps parfait. Soit X une courbe projective lisse sur K. Dans ce paragraphe, nous définissons l'espace des différentielles de X relativement à K. Nous utiliserons la définition de Kähler, qui est équivalente à la définition de Weil [Sti08, Section 4.3].

Définition 10. Soit E un $K(X)$-espace vectoriel, une **K-dérivation** de X dans E est une application K-linéaire

$$\delta : K(X) \longrightarrow E$$

telle que :

$$\forall f, g \in K(X),\ \delta(fg) = f\delta(g) + g\delta(f).$$

On note $\mathrm{Der}_K(K(X), E)$ l'espace des K-dérivations de $K(X)$ dans E.

Définition 11. Il existe une K-dérivation $d : K(X) \longrightarrow \Omega(X/K)$ vérifiant la propriété universelle suivante : pour tout $K(X)$-espace vectoriel E,

$$\begin{array}{ccc} \mathrm{Hom}_{K(X)}(\Omega(X/K), E) & \longrightarrow & \mathrm{Der}_K(K(X), E) \\ u & \longmapsto & u \circ d \end{array}$$

est un isomorphisme de $K(X)$-espaces vectoriels.

L'espace $\Omega(X/K)$ est appelé **l'espace des différentielles** de X (relativement à K), il est unique à unique isomorphisme près. C'est un $K(X)$-espace vectoriel de dimension 1.

Définition 12. Soit $\omega \in \Omega(X/K)\backslash\{0\}$, soit P une place de $K(X)$ et soit t une uniformisante en P. Soit $f \in K(X)$ l'unique fonction telle que $\omega = f dt$. On définit

$$\nu_P(\omega) = \nu_P(f).$$

On définit le diviseur de la différentielle ω comme

$$\mathrm{div}\,\omega = \sum_P \nu_P(\omega) P.$$

Soit D un diviseur de X, on appelle espace des différentielles de X (relativement à K) associé à D l'espace $\Gamma_X(\Omega_{X/K}(D))$ constitué de la différentielle nulle et des différentielles ω vérifiant

$$\mathrm{div}\,\omega \geqslant D.$$

On notera $\Gamma_X(\Omega_{X/K})$ l'espace des différentielles holomorphes de X (dont le diviseur est effectif).

Supposons que K est un corps fini, nous demandons une représentation algorithmique des différentielles de $\Omega(X/K)$ nous permettant d'effectuer les opérations suivantes :

1. Étant donnée $\omega \in \Omega(X/K)$ non nulle, calculer le diviseur de ω.
2. Étant donnée une fonction $f \in K(X)$, calculer la différentielle df.
3. Étant donné un diviseur D de X, calculer une base de $\Gamma_X(\Omega_{X/K}(D))$.
4. Étant données une fonction $f \in K(X)$ et une différentielle $\omega \in \Omega(X/K)$, calculer la différentielle $f\omega$.
5. Étant données deux différentielles $\omega_1, \omega_2 \in \Omega(X/K)$, calculer la fonction $f = \omega_1/\omega_2$ et la différentielle $\omega_1 + \omega_2$.

En particulier, les conditions 2 et 5 nous permettent de calculer le développement en série de Laurent d'une différentielle ω en une place P et en particulier son résidu en P.

2.1.4 Groupe de Picard

Soit K un corps parfait. Soit X une courbe projective lisse sur K.

Définition 13. On dit que deux diviseurs D et D' de X sont **équivalents** et on note

$$D \sim D'$$

si $D - D'$ est principal.

Définition 14. On définit le **groupe de Picard** de X comme

$$\mathrm{Pic}(X) = \mathrm{Div}(X)/\,\mathrm{Princ}(X).$$

Pour tout $d \in \mathbb{Z}$, on note $\mathrm{Pic}^d(X)$ le sous-ensemble de $\mathrm{Pic}(X)$ constitué des classes de degré d. L'ensemble $\mathrm{Pic}^0(X)$ est un sous-groupe de $\mathrm{Pic}(X)$.

Supposons que K est un corps fini. La représentation algorithmique des classes de $\mathrm{Pic}(X)$ doit permettre de calculer les opérations de groupe :

1. Étant donné D un diviseur de X, calculer la classe c de D dans $\mathrm{Pic}(X)$.
2. Étant donnée c une classe dans $\mathrm{Pic}(X)$, donner un diviseur D dans la classe c.
3. Étant données c et c' deux classes dans $\mathrm{Pic}(X)$, déterminer si $c = c'$.
4. Étant données c et c' deux classes dans $\mathrm{Pic}(X)$, calculer $c + c'$.
5. Étant donnée c une classe dans $\mathrm{Pic}(X)$, calculer $-c$.

Remarque 2. Il est parfois utile d'avoir des représentants univoques des éléments du groupe de Picard (voir par exemple la sous-section 2.2.3). En effet, un élément du groupe de Picard peut avoir plusieurs représentants différents (algorithmiquement parlant). Un représentant univoque de $c \in \mathrm{Pic}(X)$ est un représentant particulier dans l'ensemble des représentants de c qui peut être calculé à partir de n'importe quel représentant de c. Avec nos hypothèses sur la représentation algorithmique du groupe de Picard, il est toujours possible de construire de tels représentants. Si la courbe X possède un point K-rationnel P, il est possible d'en construire un de la manière suivante.

Soit $c \in \mathrm{Pic}(X)$. Quitte à soustraire (ou ajouter) P suffisamment de fois, on peut supposer que $c \in \mathrm{Pic}^0(X)$. Soit g le genre de X, et soit D un diviseur de la classe c. D'après le théorème de Riemann–Roch, l'espace $\Gamma_X(\mathcal{O}_X(D + gP))$ est non-nul. On peut montrer qu'il existe une unique fonction non-nulle f (à une constante de K près) de $\Gamma_X(\mathcal{O}_X(D+gP))$ dont la valuation en P est maximale. Alors $D + (f)$ est un représentant univoque de c.

2.1.5 Fonction zêta

Dans ce paragraphe, on se restreint au cas où K est un corps fini à $q = p^m$ éléments. Soit X une courbe projective lisse sur K, soit $r \geqslant 1$ et L une extension de K de degré r. Notons

$$N_r = \#X(L).$$

Définition 15. Soit α_n le nombre de diviseurs effectifs de X (sur K) de degré n. On appelle

$$Z_X = \exp\left(\sum_{r\geqslant 1} \frac{N_r}{r} x^r\right) = \sum_{n\geqslant 0} \alpha_n x^n \in \mathbb{Z}[[x]]$$

la **fonction zêta** de X. On appelle

$$L_X = (1-x)(1-qx)Z_X \in \mathbb{Z}[x]$$

le **polynôme-L** de X.

On rappelle que le polynôme-L de X est un polynôme à coefficients entiers de degré $2g$ où g est le genre de X. Ses coefficients $\ell_0, \ldots, \ell_{2g}$ vérifient, pour tout $i \leqslant g$,

$$\ell_{2g-i} = q^{g-i}\ell_i.$$

Enfin, il est connu que $\ell_0 = 1$. On peut donc représenter algorithmiquement L_X par les g coefficients $\ell_1, \ldots, \ell_g$. Il est possible de déterminer les coefficients du polynôme-L de X à partir des valeurs N_r pour $1 \leqslant r \leqslant g$ [Sti08, Section 5.1].

Le calcul du polynôme-L du corps de fonctions X est un problème compliqué, et les algorithmes actuels pour le calculer ne sont pas efficaces dans toutes les situations. La première catégorie, généralisant les algorithmes de Schoof [Sch85] et Pila [Pil90], sont polynomiaux en $\log q = m \log p$ quand le genre g est petit, mais leurs complexités dépendent exponentiellement du genre. La seconde catégorie, les algorithmes généralisant les algorithmes de Satoh [Sat00] et Kedlaya [Ked01], ont des complexités polynomiales en m, p et g et sont efficaces en petite caractéristique.

2.2 Algorithmique des jacobiennes

Dans cette section, on présente des algorithmes utilisant les opérations élémentaires de la section 2.1 qui nous serviront dans les prochains chapitres.

Soit K un corps fini à $q = p^m$ éléments. Soit $\bar{K}$ une clôture algébrique de K. Soit X un courbe projective lisse sur K de genre g.

La jacobienne $\mathcal{J}_X$ de X est une variété abélienne de dimension g. On peut montrer que pour toute extension finie L de K,

$$\mathcal{J}_X(L) \simeq \mathrm{Pic}^0(X_L), \tag{2.2.1}$$

où X_L désigne la courbe projective lisse sur L naturellement associée à la courbe X. De plus, l'isomorphisme de l'équation (2.2.1) est fonctoriel relativement à L. Ainsi, on utilisera la représentation algorithmique de $\mathrm{Pic}^0(X_L)$ pour représenter $\mathcal{J}_X(L)$.

Supposons qu'il existe $P \in X(K)$. On peut alors définir

$$j_P : X \longrightarrow \mathcal{J}_X$$

l'application de Jacobi associée à P. C'est une immersion fermée de X dans sa jacobienne, induite par l'application

$$\begin{array}{ccc} \mathrm{Div}(X) & \longrightarrow & \mathrm{Pic}^0(X) \\ \sum_Q n_Q Q & \longmapsto & \sum_Q n_Q (Q - \deg(Q)P) \end{array}.$$

2.2.1 Couplage de Weil

Définition 16. On utilise les notations du début de la section 2.2. Soit n un entier non divisible par p. Supposons que la n-torsion de la jacobienne $\mathcal{J}_X$ est K-rationnelle, et que K contient les racines n-ièmes de l'unité (en réalité, le couplage de Weil permet de démontrer que cette deuxième hypothèse est redondante). Soient deux classes K-rationnelles de n-torsion de la jacobienne $(a, b) \in \mathcal{J}_X[n](K) \times \mathcal{J}_X[n](K)$. Soit D_a un diviseur représentant a et D_b un diviseur représentant b disjoint de D_a. Soient f_a une fonction de $K(X)$ de diviseur nD_a et f_b une fonction de diviseur nD_b. On pose :

$$e_n(a, b) = \frac{f_b(D_a)}{f_a(D_b)}.$$

Il est entendu ici que l'on note pour $f \in K(X)$ et $D \in \mathrm{Div}(X)$ un diviseur disjoint du support de f :

$$f(D) = \prod_{P \in \mathrm{Irr}(X)} \left(\mathrm{Norm}_K^{K_P} f(P)\right)^{\nu_P(D)} = \prod_{P \in \mathrm{Irr}(X)} \prod_{\substack{Q \in \mathrm{Irr}(X/\bar{K}) \\ Q|P}} f(Q)^{\nu_P(D)} \tag{2.2.2}$$

Notons que f_a et f_b dépendent du choix de D_a et D_b, mais pas $e_n(a, b)$. De même, f_a et f_b sont définies à une constante près, mais d'après l'équation (2.2.2), puisque D_a et D_b sont de degré 0, les valeurs $f(D_a)$ et $f(D_b)$ ne dépendent pas de cette constante. Enfin d'après la loi de réciprocité de Weil, on a

$$\left(\frac{f_b(D_a)}{f_a(D_b)}\right)^n = \frac{f_b(nD_a)}{f_a(nD_b)} = 1.$$

Cela définit le couplage de Weil

$$e_n : \mathcal{J}_X[n](K) \times \mathcal{J}_X[n](K) \longrightarrow \mu_n(K)$$

où $\mu_n(K)$ est le groupe des racines n-ièmes de l'unité de K.

Cette définition du couplage de Weil demande d'avoir des représentants D_a et D_b disjoints. Dans le cas où D_a et D_b ne sont pas disjoints, il est possible de trouver un diviseur équivalent à D_b disjoint de D_a. Soit D_0 un diviseur de degré $2g$ disjoint de D_a (sur les corps finis, il existe toujours un tel diviseur). Alors, d'après le théorème de Riemann–Roch, $\Gamma_X(\mathcal{O}_X(D_0 + D_b))$ est un K-espace vectoriel de dimension $g + 1$ car

$$\deg(D_0 + D_b) = 2g \geqslant 2g - 1.$$

Soit $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$, le diviseur $(f) + D_0 + D_b$ est effectif. Ainsi, si $(f) + D_0 + D_b$ et D_a ne sont pas disjoints, il existe $P \in \mathrm{supp}\, D_a$ telle que $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b - P))$. Pour toute place $P \in \mathrm{supp}\, D_a$, le sous-espace $\Gamma_X(\mathcal{O}_X(D_0 + D_b - P))$ a dimension au plus g et est donc contenu dans un hyperplan de $\Gamma_X(\mathcal{O}_X(D_0 + D_b))$. Ainsi, les fonctions

$f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$ telles que $(f) + D_0 + D_b$ n'est pas disjoint de D_a appartiennent a une union d'au plus $\#\operatorname{supp} D_a$ d'hyperplans. Si $\#\operatorname{supp} D_a < q$, on peut utiliser l'algorithme de [ECdJ+11, Lemmes 13.1.8] pour calculer une fonction $f \in \Gamma_X(\mathcal{O}_X(D_0 + D_b))$, telle que

$$(f) + D_0 + D_b \text{ est disjoint de } D_a.$$

Alors $(f) + D_b$ est un diviseur équivalent à D_b disjoint de D_a.

Si $\#\operatorname{supp} D_a \geqslant q$, l'idée est d'étendre le corps de base et d'appliquer une technique similaire. Le lecteur peut se référer à [ECdJ+11, Lemmes 13.1.9].

Soient D_a^+ et D_a^- deux diviseurs effectifs disjoints tels que $D_a = D_a^+ - D_a^-$, alors le degré de la fonction f_a est $n \deg D_a^+$. Il est donc attendu que la complexité du calcul du couplage de Weil dépende polynomialement de n et $\deg D_a^+$. Cependant, l'algorithme de Miller (voir [MOV93, Annexe] ou [ECdJ+11, Section 13.3]) permet d'évaluer le couplage de Weil avec une complexité polynomiale en $\log n$ et $\deg D_a^+$.

2.2.2 Tirage au sort dans le groupe de Picard

On utilise les notations du début de la section 2.2. On chercher à choisir uniformément un élément de degré 0 du groupe de Picard de X. Il est possible d'accomplir ceci en utilisant la méthode décrite dans [Bru13, Sections 3.2-6]. Il est important de noter que cette méthode requiert de connaître le polynôme-L de X.

Tirage d'une place

Soit $d > 0$ un entier. On commence par chercher à tirer au sort une place de degré d uniformément dans $\mathrm{Irr}^d(X)$. Une procédure est détaillée dans l'algorithme 2.2.1.

Algorithme 2.2.1 : Tirer au sort une place de degré d

Entrées : $K(X)$ un corps de fonctions sur K, $d > 0$ un entier tel que $\mathrm{Irr}^d(X)$ soit non vide

Output : $P \in \mathrm{Irr}^d(X)$ choisi uniformément

1. Soit D_0 un diviseur effectif vérifiant $\deg D_0 - d \geqslant 2g$.
2. Choisir uniformément $f \in \Gamma_X(\mathcal{O}_X(D_0))$. Soit $D = (f)$ son diviseur.
3. Calculer $\#\mathrm{Irr}^d(D)$ le nombre de places de degré d présentes dans D (comptées avec multiplicité).
4. Avec probabilité $\#\mathrm{Irr}^d(D) / \lfloor \deg D_0/d \rfloor$, renvoyer une place $P \in \mathrm{Irr}^d(D)$ choisie uniformément.
5. Reprendre à l'étape 1.

L'algorithme 2.2.1 repose sur deux points clés. Premièrement, il est simple de tirer au sort un élément d'un espace de Riemann–Roch uniformément, car ce sont des espaces vectoriels de dimension finie. Deuxièmement, le renvoi du résultat avec probabilité $\#\mathrm{Irr}^d(D) / \lfloor \deg D_0/d \rfloor$ permet que la probabilité de renvoyer P ne dépende pas de D.

Remarque 3. Dans la suite, il sera nécessaire de tirer au sort des sommes formelles de places de degré commun d, ou de manière équivalente des ensembles avec répétition (non ordonnés). Tirer au sort une telle somme selon la loi uniforme est un peu plus compliqué que de tirer des places les unes à la suite des autres avec l'algorithme 2.2.1, car les sommes avec répétitions n'occureraient pas avec la même probabilité que les sommes sans répétitions. On utilisera un résultat de [Bru13, Algorithme 3.4] : il existe un algorithme générique qui, étant donné un ensemble E de cardinal fini connu, un entier ℓ, et un algorithme de tirage au sort uniforme dans E (d'un seul élément), renvoi un ensemble avec répétition de cardinal ℓ d'éléments de E, tiré au sort uniformément.

Il est nécessaire de s'assurer que l'entier d donné en entrée de l'algorithme satisfait bien la condition $\mathrm{Irr}^d(X) \neq \emptyset$, sinon l'algorithme ne termine pas. Il est possible de calculer la valeur de $\#\mathrm{Irr}^d(X)$ en utilisant L_X le polynôme-L de de X [Bru13, Section 3].

Tirage d'un diviseur effectif

Le tirage au sort uniforme d'un diviseur effectif de degré d se fait en deux temps : d'abord, on tire au sort uniformément le nombre de places de chaque degré (inférieur à d) qui apparaissent dans la somme, puis on tire au sort les places en utilisant l'algorithme 2.2.1.

Soit r et d deux entiers strictement positifs. On appelle un type de décomposition r-lisse de degré d une suite d'entiers $(\ell_1, \ell_2, \ldots)$ tel que $\sum_{i=1}^{r} \ell_i i = d$ et tel que pour tout $i > r$, l'entier ℓ_i est nul. En particulier, à tout diviseur effectif D de degré d, on peut associer un type de décomposition d-lisse de degré d, où ℓ_i est le nombre de places de degré i apparaissant dans D (comptées avec multiplicité). On dit que D est *r-lisse* si son type de décomposition l'est, i.e. si D est supporté par des places de degré au plus r. On note

$$\mathrm{Eff}^d_{\leqslant r}(X) = \{D \in \mathrm{Eff}(X) \mid \deg D = d \text{ et } D \text{ est } r\text{-lisse}\}$$

l'ensemble des diviseurs effectifs r-lisses de degré d de X, et pour tout entier ℓ on note

$$\mathrm{Eff}^{\ell r}_{=r}(X) = \{D \in \mathrm{Eff}(X) \mid D \text{ est composé de } \ell \text{ places de degré } r\}$$

l'ensemble des diviseurs effectifs de degré ℓr composés uniquement de places de degré r. Il est possible de calculer récursivement les valeurs $\#\,\mathrm{Eff}^d_{\leqslant r}(X)$ pour tout d et r à partir du nombre de places de chaque degré inférieur à r [Bru13, Section 3.3].

La loi uniforme sur les diviseurs r-lisses de degré d induit une loi de probabilité sur les types de décomposition. Si $r \geqslant 2$, on peut exprimer la loi marginale associée à la r-ième coordonnée par :

$$\mathbb{P}(\ell_r = \ell) = \frac{\#\,\mathrm{Eff}^{\ell r}_{=r}(X) \cdot \#\,\mathrm{Eff}^{d-\ell r}_{\leqslant r-1}(X)}{\#\,\mathrm{Eff}^{d}_{\leqslant r}(X)},\ 0 \leqslant \ell \leqslant \lfloor d/r \rfloor \tag{2.2.3}$$

On obtient alors l'algorithme récursif 2.2.2, qui utilise le fait que tout diviseur r-lisse de degré d est la somme d'un diviseur $(r-1)$-lisse de degré $d - \ell r$ et de ℓ places de degré r, pour un certain entier ℓ.

On rassemble les algorithmes précédents pour obtenir l'algorithme 2.2.3 tirant au sort un diviseur effectif de degré fixé choisi uniformément.

Algorithme 2.2.2 : Tirer au sort un type de décomposition r-lisse de degré d
Entrées : (d, r) deux entiers positifs
Output : $(\ell_1, \ldots, \ell_r, 0, \ldots)$ un type de décomposition r-lisse de degré d choisi uniformément

1 Si $r = 1$, renvoyer $(d, 0, \ldots)$.
2 Sinon, tirer au sort ℓ_r selon la loi de probabilité 2.2.3.
3 Appeler l'algorithme récursivement avec les paramètres $(d - \ell_r r, r - 1)$ pour obtenir un type de décomposition $(\ell_1, \ldots, \ell_{r-1}, 0, \ldots)$.
4 Renvoyer $(\ell_1, \ldots, \ell_r, 0, \ldots)$.

Algorithme 2.2.3 : Tirer au sort un diviseur effectif de degré d
Entrées : $d > 0$ un entier, $K(X)$ un corps de fonctions
Output : D un diviseur effectif de degré d choisi uniformément

1 Tirer au sort un type de décomposition $(\ell_1, \ldots, \ell_d, 0, \ldots)$, d-lisse de degré d avec l'algorithme 2.2.2.
2 Pour $i = 1, \ldots, d$, tirer au sort ℓ_i places de degré i comme précisé dans la remarque 3.
3 Renvoyer la somme des places.

Tirage d'une classe

Pour choisir uniformément une classe de $\mathrm{Pic}^0(X)$, on peut utiliser l'algorithme 2.2.3 de tirage au sort de diviseur effectif de degré prescrit. Il suffit de connaître une application surjective de $\mathrm{Eff}^d(X)$ dans $\mathrm{Pic}^0(X)$ dont les fibres ont le même cardinal, pour un certain degré d.

Soit D_0 un diviseur effectif de degré $d_0 \geqslant 2g - 1$. Alors l'application

$$D \in \mathrm{Eff}^{d_0}(X) \longmapsto [D - D_0] \in \mathrm{Pic}^0(X)$$

est surjective, et ses fibres ont le même cardinal. En effet, soit $c \in \mathrm{Pic}^0(X)$ une classe de degré 0. Soit $\tilde{D}$ un diviseur dans la classe c. Alors $\tilde{D} + D_0$ est de degré $d_0 \geqslant 2g - 1$, donc $\Gamma_X(\mathcal{O}_X(\tilde{D} + D_0))$ est de dimension $d_0 - g + 1$ et pour toute fonction $f \in \Gamma_X(\mathcal{O}_X(\tilde{D} + D_0))$ non nulle,

$$D := (f) + \tilde{D} + D_0 \geqslant 0 \text{ et } D - D_0 \sim \tilde{D}$$

De plus, la fibre au-dessus de c est en bijection avec l'ensemble des droites vectorielles de $\Gamma_X(\mathcal{O}_X(\tilde{D} + D_0))$, dont le cardinal est indépendant de c. On récapitule ces remarques dans l'algorithme 2.2.4.

2.2.3 Structure de la jacobienne

On utilise les notations du début de la section 2.2. Rappelons que K est un corps fini. Soit $P_\infty \in X(K)$. On verra dans la suite que la théorie du corps de classes démontre

Algorithme 2.2.4 : Tirer au sort dans le groupe de Picard
Entrées : $K(X)$ un corps de fonctions
Output : c une classe de $\mathrm{Pic}^0(X)$ tirée uniformément
1 Choisir un diviseur effectif D_0 de degré $d_0 \geqslant 2g-1$
2 Tirer au sort un diviseur effectif D de degré d_0 avec l'algorithme 2.2.3.
3 Renvoyer la classe de $D - D_0$

une correspondance entre les classes d'isomorphismes de revêtements abéliens sur K, non ramifiés, totalement scindés au-dessus de P_∞ de X et les sous-groupes de $\mathcal{J}_X(K)$. Nous souhaitons donc être en mesure de déterminer les sous-groupes de $\mathcal{J}_X(K) \simeq \mathrm{Pic}^0(X)$, et pour cela présentons des techniques pour calculer la structure de groupe abélien de $\mathrm{Pic}^0(X)$.

Le calcul de la structure de groupe demande d'être capable de calculer un ensemble de générateurs de $\mathrm{Pic}^0(X)$. Soit ℓ un entier premier, et $k > 0$ un entier positif. Il est connu que $\mathcal{J}_X[\ell^k](\bar{K})$ est un groupe abélien fini ayant au plus $2g$ facteurs invariants. On en déduit que $\mathcal{J}_X[\ell^k](K)$ est également un groupe abélien fini ayant au plus $2g$ facteurs invariants. Cela implique que $\mathcal{J}_X(K)$ a au plus $2g$ facteurs invariants également. Supposons que L_X est connu, on peut tirer au sort uniformément $2g+2+n$ classes dans $\mathrm{Pic}^0(X)$ avec l'algorithme 2.2.4 pour obtenir une famille génératrice avec probabilité supérieure à $1 - 1/2^n$ (voir la section 6.2 de l'annexe).

Généralisons le problème au calcul de la structure d'un groupe abélien G quelconque. On présente rapidement l'algorithme de Buchmann–Schmidt [BS05]. Étant donné n éléments engendrant un groupe abélien G, cet algorithme calcule des éléments $\gamma_1, \ldots, \gamma_r \in G$ d'ordres $d_1 | \cdots | d_r$ engendrant G, en calculant une base B du réseaux des relations des n générateurs de G, sous forme normale de Smith. La diagonale de B est $(d_1, \ldots, d_r, 1, \ldots, 1)$, et

$$G = \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_r \rangle \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

L'algorithme de Buchmann–Schmidt est une extension de l'algorithme de calcul du logarithme discret de Shanks (voir [Coh93, Section 5.4.1]), également appelé algorithme Baby-Step Giant-Step, et nécessite de réaliser $O(n\sqrt{|G|})$ opérations de groupes dans G et $O(n\sqrt{G}\log(G))$ comparaisons d'éléments de G, et de stocker $O(\sqrt{|G|})$ éléments de G.

Remarque 4. Il faut noter que pour limiter ainsi le nombre de comparaisons, il est nécessaire d'être capable d'ordonner les éléments de G. Si on dispose de représentants univoques d'éléments de G, on peut facilement les ordonner (par exemple par ordre lexicographique).

Chapitre 3

Théorie effective du corps de classes

L'objet de la théorie du corps de classes (globale) est la caractérisation des extensions abéliennes des corps de nombres et des corps de fonctions (sur les corps finis). Ces deux types de corps partagent de nombreuses caractéristiques, et par conséquent les résultats de la théorie du corps de classes peuvent être exprimés de manière semblable dans les deux situations. Plusieurs versions de cette théorie ont été rédigées, utilisant des objets différents pour en exprimer et en démontrer les résultats. On utilisera la version employant le langage des idéaux pour l'étude des corps de nombres, car celle-ci est la plus simple à adapter d'un point de vue algorithmique. Pour les corps de fonctions, on reprendra les présentations de Rosen [Ros87] et de Serre [Ser84].

Dans ce chapitre, on commence par présenter rapidement la théorie du corps de classes pour les corps de nombres dans la section 3.1. On présente quelques applications et méthodes algorithmiques issues de cette théorie dans la section 3.2. Dans la section 3.3, on présente la théorie du corps de classes pour les corps de fonctions de deux points de vue, et on discute rapidement le lien entre ces deux présentations. Enfin, on présente une application de la théorie du corps de classes à la construction de courbes algébriques ayant beaucoup de points rationnels dans la section 3.4. En particulier, on présente de nouvelles courbes ayant des nombres records de points rationnels. Les notions et méthodes présentées dans ce chapitre seront utilisées dans les chapitres 4 et 5.

3.1 Théorie du corps de classes pour les corps de nombres

L'objectif de cette section est de présenter les principaux objets de la théorie du corps de classes des corps de nombres et d'en récapituler certains résultats. Pour une exposition plus détaillée de la théorie, le lecteur peut se référer aux ouvrages suivants [AT09, Jan96, Neu86, Lan94]. Cette section est inspirée de [Coh00, Chapitre 3].

Le but de la théorie du corps de classes est de décrire les extensions abéliennes d'un corps de nombres $\mathcal{K}$ (ou de manière plus générale d'un corps global) en utilisant l'arithmétique de $\mathcal{K}$. Le point de départ de la théorie est le travail de Hilbert et Furtwängler sur les extensions abéliennes non ramifiées. Soit $\mathcal{K}$ un corps de nombres, l'ensemble des classes

d'isomorphismes des extensions abéliennes non ramifiées de $\mathcal{K}$ a un maximum, au sens qu'il existe une extension abélienne non ramifiée de $\mathcal{K}$ notée $\mathrm{Hil}(\mathcal{K})$ telle que toute extension abélienne non ramifiée $\mathcal{L}$ de $\mathcal{K}$ est isomorphe à une sous-extension de $\mathrm{Hil}(\mathcal{K})$. On appelle $\mathrm{Hil}(\mathcal{K})$ le corps de classes de Hilbert de $\mathcal{K}$. Le degré de l'extension $[\mathrm{Hil}(\mathcal{K}) : \mathcal{K}] = \mathrm{cl}(\mathcal{K})$ est le nombre de classes de $\mathcal{K}$ et le groupe de Galois $\mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K})$ est canoniquement isomorphe au groupe de classes $\mathrm{Cl}(\mathcal{K})$ de $\mathcal{K}$. Ainsi, la théorie de Galois permet d'identifier les sous-groupes de $\mathrm{Cl}(\mathcal{K})$ et les classes d'isomorphismes d'extensions abéliennes non ramifiées de $\mathcal{K}$. Enfin, le corps de classes de Hilbert possède une deuxième propriété importante : soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_{\mathcal{K}}$, et soit f l'ordre de $\mathfrak{p}$ dans le groupe de classes de $\mathcal{K}$. Alors f est également le degré d'inertie de $\mathfrak{p}$ dans l'extension $\mathrm{Hil}(\mathcal{K})/\mathcal{K}$.

On va voir dans la suite qu'il est possible de généraliser les notions de groupe de classes et corps de classes pour paramétrer les extensions abéliennes (ramifiées ou non). Soit $\mathcal{L}$ une extension abélienne de $\mathcal{K}$. La première étape consiste à définir des objets permettant de décrire la ramification de $\mathcal{L}$.

Définition 17.

1. Un module $\mathfrak{m}$ est une paire $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ où $\mathfrak{m}_0$ est un idéal de $\mathbb{Z}_{\mathcal{K}}$ et $\mathfrak{m}_\infty$ est un ensemble de plongements réels de $\mathcal{K}$ dans $\mathbb{C}$.
2. Si $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ et $\mathfrak{n} = (\mathfrak{n}_0, \mathfrak{n}_\infty)$ sont deux modules, on dit que $\mathfrak{n}$ divise $\mathfrak{m}$ si $\mathfrak{n}_0 \mid \mathfrak{m}_0$ et $\mathfrak{n}_\infty \subset \mathfrak{m}_\infty$. On note alors $\mathfrak{n} \mid \mathfrak{m}$.
3. Si $\mathfrak{a}$ est un idéal fractionnaire non nul de $\mathbb{Z}_{\mathcal{K}}$, on dit que $\mathfrak{a}$ est premier à $\mathfrak{m}$ si $\mathfrak{a}$ est premier avec $\mathfrak{m}_0$, c'est-à-dire il existe deux idéaux $\mathfrak{b}$ et $\mathfrak{c}$ premiers à $\mathfrak{m}_0$ tels que $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$.
4. On dit que $\alpha \in \mathcal{K}^*$ est premier à $\mathfrak{m}$ si $\alpha\mathbb{Z}_{\mathcal{K}}$ l'est.
5. Soit $\alpha \in \mathcal{K}^*$, on dit que
$$\alpha = 1 \bmod {}^*\mathfrak{m}$$
si pour tout idéal premier $\mathfrak{p}$ divisant $\mathfrak{m}_0$, $\nu_{\mathfrak{p}}(\alpha - 1) \geqslant \nu_{\mathfrak{p}}(\mathfrak{m}_0)$ et pour tout $\sigma \in \mathfrak{m}_\infty$, $\sigma(\alpha) > 0$.
6. Soient $\alpha, \beta \in \mathcal{K}^*$, on dit que $\alpha = \beta \bmod {}^*\mathfrak{m}$ si α et β sont premiers à $\mathfrak{m}$ et $\alpha/\beta = 1 \bmod {}^*\mathfrak{m}$.

L'objet nous permettant de quantifier la ramification de $\mathcal{L}$ qui nous sera utile dans la suite est un module appelé le conducteur de $\mathcal{L}$ sur $\mathcal{K}$. Pour pouvoir le définir, on rappelle la notion de norme locale. Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_{\mathcal{K}}$, on note $\mathcal{K}_{\mathfrak{p}}$ le complété de $\mathcal{K}$ en la place $\mathfrak{p}$. Soit $\mathfrak{P}$ un idéal premier de $\mathbb{Z}_{\mathcal{L}}$ au-dessus de $\mathfrak{p}$. On dit que $\alpha \in \mathcal{K}_{\mathfrak{p}}^*$ est une norme locale modulo $\mathfrak{p}$ si $\nu_{\mathfrak{p}}(\alpha) \geqslant 0$ et s'il existe $\beta \in (\mathcal{L}_{\mathfrak{P}})^*$ tel que $\alpha = \mathrm{Norm}_{\mathcal{K}_{\mathfrak{p}}}^{\mathcal{L}_{\mathfrak{P}}}(\beta)$.

On pose $k_{\mathfrak{p}}$ le plus petit entier positif ou nul tel que tous les éléments $\alpha \in \mathcal{K}^*$ premier à $\mathfrak{p}$ vérifiant $\alpha = 1 \bmod {}^*\mathfrak{p}^{k_{\mathfrak{p}}}$ sont des normes locales modulo $\mathfrak{p}$. Il est possible de démontrer que $k_{\mathfrak{p}}$ existe, et que $k_{\mathfrak{p}} = 0$ si et seulement si $\mathfrak{p}$ est non ramifié dans $\mathcal{L}/\mathcal{K}$ [Coh00, Sect 3.4.1].

Définition 18. On reprend les notations définies dans le paragraphe précédent. Soit

$$\mathfrak{c}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{k_\mathfrak{p}}$$

un idéal de $\mathbb{Z}_\mathcal{K}$ (le produit a un nombre fini de facteurs non triviaux). Soit $\mathfrak{c}_\infty$ l'ensemble (fini) des plongements réels de $\mathcal{K}$ dans $\mathbb{C}$ associés aux places réelles de $\mathcal{K}$ qui se ramifient dans $\mathcal{L}/\mathcal{K}$. Alors on définit le **conducteur** de $\mathcal{L}/\mathcal{K}$ comme le module

$$\mathfrak{c}_{\mathcal{L}/\mathcal{K}} = (\mathfrak{c}_0, \mathfrak{c}_\infty).$$

Remarque 5. Le conducteur $\mathfrak{c}_{\mathcal{L}/\mathcal{K}}$ est composé de toutes les places ramifiées dans $\mathcal{L}/\mathcal{K}$, et uniquement de ces places.

Si $\mathcal{L}_1$ et $\mathcal{L}_2$ sont deux extensions abéliennes de $\mathcal{K}$, telles que $\mathcal{L}_1$ est isomorphe à une sous-extension de $\mathcal{L}_2$, alors $\mathfrak{c}_{\mathcal{L}_1/\mathcal{K}} \mid \mathfrak{c}_{\mathcal{L}_2/\mathcal{K}}$. Cela motive la définition suivante :

Définition 19. Soit $\mathcal{K}$ un corps de nombres, et soit $\mathcal{L}$ une extension abélienne de $\mathcal{K}$. On dit qu'un module $\mathfrak{m}$ est approprié pour l'extension $\mathcal{L}/\mathcal{K}$ si $\mathfrak{c}_{\mathcal{L}/\mathcal{K}}$ divise $\mathfrak{m}$.

Ensuite, on définit la notion qui va généraliser le groupe de classes.

Définition 20. Avec les notations précédentes,

1. On définit
$$(\mathbb{Z}_\mathcal{K}/\mathfrak{m})^\times = (\mathbb{Z}_\mathcal{K}/\mathfrak{m}_0)^\times \times \mathbb{F}_2^{\mathfrak{m}_\infty}.$$
2. On note $I_\mathfrak{m}(\mathcal{K})$ le groupe des idéaux fractionnaires non nuls de $\mathbb{Z}_\mathcal{K}$ premiers au module $\mathfrak{m}$.
3. On note $P_\mathfrak{m}(\mathcal{K})$ le groupe des idéaux fractionnaires principaux de $\mathbb{Z}_\mathcal{K}$ engendrés par un élément $\alpha \in \mathcal{K}^*$ tel que $\alpha = 1 \bmod {}^*\mathfrak{m}$.
4. Le groupe $P_\mathfrak{m}(\mathcal{K})$ est un sous-groupe de $I_\mathfrak{m}(\mathcal{K})$. On définit le groupe de classes de rayons (modulo $\mathfrak{m}$) de $\mathcal{K}$ comme le quotient
$$\mathrm{Cl}_\mathfrak{m}(\mathcal{K}) = I_\mathfrak{m}(\mathcal{K})/P_\mathfrak{m}(\mathcal{K}).$$

Remarque 6. Le groupe $(\mathbb{Z}_\mathcal{K}/\mathfrak{m})^\times$ ne va pas intervenir dans la suite de la présentation, mais il doit être défini car il intervient dans l'algorithme de calcul des groupes de classes de rayons $\mathrm{Cl}_\mathfrak{m}(\mathcal{K})$ (voir la section 3.2 et [Coh00]).

Exemple 1. Soit $\mathbf{1} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ le module tel que :

— $\mathfrak{m}_0 = \mathbb{Z}_\mathcal{K}$.

— $\mathfrak{m}_\infty = \emptyset$.

Alors on voit que $I_\mathfrak{m}(\mathcal{K})$ est le groupe des idéaux fractionnaires non nulles de $\mathbb{Z}_\mathcal{K}$, que $P_\mathfrak{m}(\mathcal{K})$ est le groupe des idéaux principaux dans $I_\mathfrak{m}(\mathcal{K})$, et que $\mathrm{Cl}_\mathfrak{m}(\mathcal{K}) = \mathrm{Cl}(\mathcal{K})$.

On voit également que pour toute extension $\mathcal{L}'$ abélienne non ramifiée de $\mathcal{K}$, le conducteur de $\mathcal{L}'/\mathcal{K}$ est $\mathbf{1}$. Le corps de classes est donc l'extension maximale de $\mathcal{K}$ dont le conducteur est $\mathbf{1}$.

Cet exemple permet de voir que les définitions généralisent bien les notions connues pour le corps de classes de Hilbert. Il indique également comment se généralise le corps de classes de Hilbert (voir théorème 3).

Soit $\mathfrak{p}$ un premier de $\mathbb{Z}_\mathcal{K}$ et $\mathfrak{P}$ un premier de $\mathbb{Z}_\mathcal{L}$ au-dessus de $\mathfrak{p}$. On note

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathbf{Gal}(\mathcal{L}/\mathcal{K}) \mid \mathfrak{P}^\sigma = \mathfrak{P}\}$$

le groupe de décomposition de $\mathfrak{P}$. On a alors un morphisme de groupe canonique, surjectif de $D(\mathfrak{P}/\mathfrak{p})$ dans le groupe de Galois $\mathbf{Gal}(\mathcal{L}_\mathfrak{P}/\mathcal{K}_\mathfrak{p})$, dont le noyau est le groupe d'inertie $I(\mathfrak{P}/\mathfrak{p})$ de $\mathfrak{P}$.

Le groupe de Galois $\mathbf{Gal}(\mathcal{L}_\mathfrak{P}/\mathcal{K}_\mathfrak{p})$ est cyclique, engendré par le morphisme de Frobenius :

$$\alpha \longmapsto \alpha^{\mathrm{Norm}_\mathbb{Q}^\mathcal{K}(\mathfrak{p})}.$$

Si $\mathfrak{p}$ est non ramifié, alors $I(\mathfrak{P}/\mathfrak{p})$ est trivial, et le morphisme

$$D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \mathbf{Gal}(\mathcal{L}_\mathfrak{P}/\mathcal{K}_\mathfrak{p})$$

est un isomorphisme. Il existe alors un unique élément $\mathfrak{s}_\mathfrak{P} \in D(\mathfrak{P}/\mathfrak{p})$ qui est envoyé sur le morphisme de Frobenius. De plus, puisque $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ est abélien, $D(\mathfrak{P}/\mathfrak{p})$ ne dépend pas du choix de $\mathfrak{P}$, donc on peut définir $\mathfrak{s}_\mathfrak{p} = \mathfrak{s}_\mathfrak{P}$.

Soit $\mathfrak{m}$ un module approprié pour l'extension $\mathcal{L}/\mathcal{K}$. En particulier, tous les premiers de $\mathcal{K}$ qui se ramifient dans $\mathcal{L}$ divisent $\mathfrak{m}$. On peut donc définir une application de $I_\mathfrak{m}(\mathcal{K})$ dans $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ en utilisant l'application du paragraphe précédent.

Définition 21. Soit $\mathfrak{a} = \prod \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} \in I_\mathfrak{m}(\mathcal{K})$. On définit :

$$(\mathfrak{a}, \mathcal{L}/\mathcal{K}) = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{s}_\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}.$$

On appelle $(\cdot, \mathcal{L}/\mathcal{K})$ l'application d'Artin, ou le symbole d'Artin.

Il est désormais possible d'énoncer les théorèmes principaux de la théorie du corps de classes.

Théorème 1 (Réciprocité d'Artin [Coh00, Théorèmes 3.4.3 et 3.4.5])**.** *Soit $\mathcal{K}$ un corps de nombres, $\mathcal{L}$ une extension abélienne de $\mathcal{K}$ et $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ un module approprié à l'extension $\mathcal{L}/\mathcal{K}$. Alors :*

1. *L'application d'Artin est un morphisme de groupe surjectif de $I_\mathfrak{m}(\mathcal{K})$ dans $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$.*
2. *Le noyau de l'application d'Artin $A_\mathfrak{m}(\mathcal{L}/\mathcal{K})$ contient $P_\mathfrak{m}(\mathcal{K})$. Plus précisément,*

$$A_\mathfrak{m}(\mathcal{L}/\mathcal{K}) = P_\mathfrak{m}(\mathcal{K})\,\mathrm{Norm}_\mathcal{K}^\mathcal{L}(I_{\mathfrak{m}_0\mathbb{Z}_\mathcal{L}}(\mathcal{L}))$$

où $\mathfrak{m}_0\mathbb{Z}_\mathcal{L}$ désigne l'idéal de $\mathbb{Z}_\mathcal{L}$ engendré par les éléments de $\mathfrak{m}_0$. On appelle ce groupe le groupe de normes (ou le groupe de Takagi).

L'application d'Artin induit un isomorphisme explicite entre $\mathbf{Gal}(\mathcal{L}/\mathcal{K})$ et un quotient du groupe de classes de rayons $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{K})$. Pour décrire complètement l'extension $\mathcal{L}/\mathcal{K}$ en fonction de l'arithmétique de $\mathcal{K}$, il faut être capable de décrire $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$ sans faire intervenir $\mathcal{L}$.

Théorème 2 ([Coh00, Théorème 3.4.4])**.** *Soit $\mathcal{K}$ un corps de nombres, $\mathcal{L}$ une extension abélienne de $\mathcal{K}$ et $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ un module approprié à l'extension $\mathcal{L}/\mathcal{K}$.*

1. *Soit $\mathfrak{p}$ un premier de $\mathbb{Z}_{\mathcal{K}}$ dans $I_{\mathfrak{m}}(\mathcal{K})$, et $\mathfrak{P}$ un premier de $\mathbb{Z}_{\mathcal{L}}$ au-dessus de $\mathfrak{p}$. Soit f l'ordre de $\mathfrak{p}$ modulo $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$, alors f est le degré d'inertie de $\mathfrak{P}$. Puisqu'il ne dépend pas du choix de $\mathfrak{P}$, on s'autorise à l'appeler degré d'inertie de $\mathfrak{p}$.*
2. *Réciproquement, $A_{\mathfrak{m}}(\mathcal{L}/\mathcal{K})$ est engendré par les idéaux $\mathfrak{p}^f$ (où $\mathfrak{p}$ est un premier dans $I_{\mathfrak{m}}(\mathcal{K})$ et f est son degré d'inertie) et $P_{\mathfrak{m}}(\mathcal{K})$. Il est même possible de se restreindre aux premiers de $I_{\mathfrak{m}}(\mathcal{K})$ de degré d'inertie $f = 1$ (toujours avec les idéaux de $P_{\mathfrak{m}}(\mathcal{K})$).*

Enfin, le dernier théorème stipule l'existence d'une extension abélienne maximale associée à chaque module.

Théorème 3 (Théorème d'existence de Takagi [Coh00, Théorème 3.5.1])**.** *Soit $\mathcal{K}$ un corps de nombres et soit $\mathfrak{m}$ un module de $\mathcal{K}$. Il existe un maximum des classes d'isomorphismes d'extensions abéliennes de conducteur divisant $\mathfrak{m}$. On l'appelle le corps de classes de rayons (modulo $\mathfrak{m}$) de $\mathcal{K}$, et on le note $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$.*

Le groupe de Galois de l'extension $\mathbf{Gal}(\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})/\mathcal{K})$ est isomorphe au groupe de classes de rayons $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{K})$ (isomorphisme induit par l'application d'Artin).

Remarque 7. De manière équivalente, on peut caractériser le corps de classes de rayons $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$ comme étant l'extension abélienne de $\mathcal{K}$ unique à isomorphisme près telle que les premiers de $\mathcal{K}$ totalement scindés dans $\mathrm{Ray}_{\mathfrak{m}}(\mathcal{K})$ sont exactement les premiers de $P_{\mathfrak{m}}(\mathcal{K})$.

3.2 Multiplication complexe des courbes elliptiques

Dans cette section, nous détaillons des aspects effectifs de la théorie du corps de classes des corps de nombres quadratique imaginaire, dans le cas non ramifié. Le calcul du groupe de classes et du corps de classes de Hilbert, dans ce contexte spécifique, peuvent être traités en utilisant la théorie de la multiplication complexe des courbes elliptiques. Dans la sous-section 3.2.1, on donne rapidement les quelques résultats de la théorie de la multiplication complexe dont nous avons besoin. Dans la sous-section 3.2.2, on présente un algorithme pour calculer le polynôme de classes de Hilbert associé à un corps quadratique imaginaire. Enfin, dans la sous-section 3.2.3, on présente l'algorithme de Atkin et Morain, dit *de la multiplication complexe*, permettant, étant donné deux entiers q et t satisfaisant les conditions ad hoc, de calculer une courbe elliptique ordinaire définie sur un corps fini à q éléments, et de trace t.

3.2.1 Action du groupe de classes sur les courbes elliptiques à multiplication complexe

Avant de présenter les algorithmes, on rappelle quelques théorèmes de la théorie de la multiplication complexe. Pour plus d'informations sur ce sujet, le lecteur peut consulter les livres [Sil94, Chapitre II] et [Coh93, Section 7.2].

Définition 22. Soit $E/\mathbb{C}$ une courbe elliptique, soit $\mathcal{K}$ un corps quadratique imaginaire et soit $\mathcal{O}$ un ordre de $\mathcal{K}$.

- On dit que E a multiplication complexe par $\mathcal{O}$ si $\mathrm{End}(E) \simeq \mathcal{O}$.
- On dit que E est à multiplication complexe si $\mathrm{End}(E) \not\simeq \mathbb{Z}$, auquel cas E est nécessairement à multiplication complexe par un ordre dans un corps quadratique imaginaire.
- On note $\mathrm{Ell}(\mathcal{O})$ l'ensemble des classes d'isomorphismes de courbes elliptiques sur $\mathbb{C}$ ayant multiplication complexe par $\mathcal{O}$. On note $[E]$ la classe de E dans $\mathrm{Ell}(\mathcal{O})$.

Définition 23. Soit $\tau \in \mathbb{H}$ (où $\mathbb{H}$ désigne le demi-plan complexe supérieur), on définit les formes et fonctions modulaires suivantes :

1. (Séries d'Eisenstein) pour tout $k \geqslant 2$ entier,
$$G_{2k}(\tau) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^{2k}}.$$
2. $g_2(\tau) = 60G_4(\tau)$ et $g_3(\tau) = 140G_6(\tau)$.
3. (Discriminant modulaire) $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$.
4. (j-invariant modulaire)
$$j(\tau) = 1728\frac{g_2(\tau)}{\Delta(\tau)}.$$

Définition 24. Soit $E/\mathbb{C}$ une courbe elliptique et $\tau \in \mathbb{H}$ tel que $E \simeq \mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$. On définit le j-invariant de E :
$$j(E) = j(\tau).$$
Une propriété du j-invariant modulaire est que $j(E)$ ne dépend pas du choix de τ.

Théorème 4 ([Coh93, Théorème 7.2.13])**.** *Soit $\mathcal{K}$ un corps quadratique imaginaire. Soit $E/\mathbb{C}$ une courbe elliptique, et $\tau \in \mathbb{H}$ tel que $E \simeq \mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$. Alors E a multiplication complexe par un ordre de $\mathcal{K}$ si et seulement si $\tau \in \mathcal{K}$. De plus, si $\tau \in \mathcal{K}$, alors $j(\tau)$ est un entier algébrique.*

Théorème 5 ([Sil94, Chapitre II, Théorème 4.3])**.** *Soit $\mathcal{K}$ un corps quadratique imaginaire, et soit $E/\mathbb{C}$ une courbe elliptique à multiplication complexe par $\mathbb{Z}_\mathcal{K}$. Alors :*

1. $\mathrm{Hil}(\mathcal{K}) \simeq \mathcal{K}(j(E))$.

2. $[\mathrm{Hil}(\mathcal{K}) : \mathcal{K}] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$.
3. $\mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K}) \simeq \mathrm{Cl}(\mathcal{K})$ *agit librement sur l'ensemble* $\mathrm{Ell}(\mathbb{Z}_\mathcal{K})$ *et :*

$$\forall \sigma \in \mathbf{Gal}(\mathrm{Hil}(\mathcal{K})/\mathcal{K}), j(\sigma * [E]) = \sigma(j(E)).$$

Définition 25. Soient $\mathcal{K}$ un corps quadratique imaginaire et D le discriminant de son anneau d'entiers. On définit le polynôme de classes de Hilbert (pour le discriminant D) :

$$H_D = \prod_{[E] \in \mathrm{Ell}(\mathbb{Z}_\mathcal{K})} (x - j([E])) \in \mathbb{Z}[x].$$

3.2.2 Calcul du polynôme de classes de Hilbert

Soit $\mathcal{K}$ un corps quadratique imaginaire et D le discriminant de $\mathbb{Z}_\mathcal{K}$. Pour calculer le polynôme de classes de Hilbert de $\mathcal{K}$, on veut être capable de réaliser deux opérations :

— déterminer $\tau_1, \ldots, \tau_{|\mathrm{Cl}(\mathcal{K})|} \in \mathbb{H}$ tels que les $(\mathbb{C}/\mathbb{Z} + \tau_k\mathbb{Z})$ forment une famille de représentants de $\mathrm{Ell}(\mathbb{Z}_\mathcal{K})$.

— étant donné $\tau \in \mathbb{H}$ et une précision n, calculer $j(\tau)$ avec précision n.

Si on est capable de réaliser ces deux tâches, il est possible de calculer les coefficients de H_D à une précision choisie. On peut alors utiliser le fait que H_D a des coefficients entiers pour retrouver les valeurs exactes de ses coefficients.

Puisque $\mathcal{K}$ est quadratique imaginaire, il est connu depuis les travaux de Gauss [Gau01] qu'il existe un isomorphisme de groupes entre $\mathrm{Cl}(\mathcal{K})$ et le groupe des formes quadratiques binaires définies positives réduites. Cet isomorphisme offre la possibilité d'énumérer rapidement les éléments du groupe de classes. On va présenter quelques propriétés des formes quadratiques binaires. Pour une présentation plus générale, le lecteur peut se référer par exemple à [BV07].

Définition 26.

— Une forme quadratique binaire est une fonction de la forme $f(x, y) = ax^2 + bxy + cy^2$ à coefficients a, b, c non tous nuls. Par soucis de concision, on écrit $f = (a, b, c)$ et on appelle f une forme.

— On dit que la forme (a, b, c) est primitive si $\mathrm{pgcd}(a, b, c) = 1$.

— On dit que deux formes f et g sont équivalentes s'il existe une matrice

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

de $\mathrm{SL}_2(\mathbb{Z})$ telle que

$$g(x, y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

On note alors $g = fU$.

— Soit $f = (a, b, c)$ une forme, on définit le discriminant $\mathrm{disc}(f) = b^2 - 4ac$ de f. Soit D un entier, on note

$$\mathrm{Quad}(D) = \{(a, b, c) \mid b^2 - 4ac = D\}.$$

Proposition 6. D'après [Coh93, Section 5.2] :

— Soient f et g deux formes équivalentes, alors $\mathrm{disc}(f) = \mathrm{disc}(g)$.

— Tout entier $D \neq 1$ congru à 0 ou 1 modulo 4 est le discriminant d'une forme.

— Posons $U = -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Pour toute forme f, on a $fU = f$.

— Soit D un discriminant, $\mathrm{PSL}_2(\mathbb{Z})$ agit sur $\mathrm{Quad}(D)$.

Définition 27. Soit $f = (a, b, c)$ une forme.

— On dit que f est définie positive si $\mathrm{disc}(f) < 0$ et $a > 0$.

— On dit que f est réduite si elle est définie positive, $|b| \leqslant a \leqslant c$ et si $b \leqslant 0$ lorsque a et $|b|$ ou a et c sont égaux.

— Soit $D < 0$ un discriminant. On note $\mathrm{Quad}_{\mathrm{red}}(D)$ l'ensemble des formes réduites de discriminant D.

Proposition 7. D'après [Coh93, Théorème 5.2.8, Proposition 5.3.3, Lemme 5.3.4] :

1. Soit f une forme définie positive et g une forme équivalente à f. Alors g est définie positive.
2. Soit f une forme définie positive, alors il existe une forme g réduite équivalente à f.
3. Soit $f = (a, b, c)$ une forme réduite de discriminant D, alors $a \leqslant \sqrt{|D|/3}$.
4. Soient f et g deux formes réduites et équivalentes, alors $f = g$.

Ces propriétés sont cruciales pour l'intérêt algorithmique des formes quadratiques. En effet, la forme réduite de la propriété 2 peut être calculée explicitement en utilisant l'algorithme de Gauss [Coh93, Algorithme 5.4.2]. De plus, la propriété 3 permet de concevoir un algorithme d'énumération de $\mathrm{Quad}_{\mathrm{red}}(D)$. Ainsi, l'ensemble $\mathrm{Quad}_{\mathrm{red}}(D)$ est un ensemble de représentants uniques des classes d'équivalence de $\mathrm{Quad}(D)$ modulo l'action de $\mathrm{PSL}_2(\mathbb{Z})$, qui peuvent être calculés explicitement. Dans le cadre de l'application à la théorie du corps de classes des corps quadratiques imaginaires, D est le discriminant de l'anneau d'entiers du corps quadratique imaginaire $\mathcal{K}$. On peut définir une loi de groupe sur $\mathrm{Quad}_{\mathrm{red}}(D)$ et expliciter un isomorphisme de groupe entre $\mathrm{Quad}_{\mathrm{red}}(D)$ et $\mathrm{Cl}(\mathcal{K})$ [Coh93, Section 5.2]. Ici, nous n'avons seulement besoin d'une version affaiblie de ce théorème (voir théorème 8).

Définition 28. Soit $f = (a, b, c)$ une forme réduite, et $D = \mathrm{disc}(f)$. Soit $i \in \mathbb{H}$ tel que $i^2 = -1$. On définit

$$\tau_f = \frac{-b + i\sqrt{-D}}{2a} \in \mathbb{H}.$$

Théorème 8 ([Coh93, Théorème 5.2.8 et Proposition 5.3.3])**.** *Soit $\mathcal{K}$ un corps quadratique imaginaire et D le discriminant de $\mathbb{Z}_{\mathcal{K}}$. L'application*

$$\begin{array}{ccc} \mathrm{Quad}_{red}(D) & \longrightarrow & \mathrm{Ell}(\mathbb{Z}_{\mathcal{K}}) \\ f & \longmapsto & [\mathbb{C}/\mathbb{Z}+\tau_f\mathbb{Z}] \end{array}$$

est une bijection.

Ce théorème répond à la première problématique, à savoir calculer une famille de représentants de $\mathrm{Ell}(\mathbb{Z}_{\mathcal{K}})$. La deuxième étape est de calculer $j(\tau)$ pour $\tau \in \mathbb{H}$. L'idée principale est d'utiliser la 1-périodicité de la fonction j pour calculer sa décomposition en série de Fourier [Sil94, Section I.7].

Théorème 9 ([Sil94, Chapitre I, Proposition 7.4])**.** *Il existe une suite d'entiers $(c_n)_{n\geqslant 0}$ tels que pour tout $\tau \in \mathbb{H}$,*

$$j(\tau) = \frac{1}{q} + \sum_{n\geqslant 0} c_n q^n$$

où $q = e^{2i\pi\tau}$.

Cette formule n'est pas utilisée en pratique car les coefficients (c_n) croissent rapidement. On utilisera plutôt la formule du théorème 11 comme dans [Coh93, Section 7.6.1] et [AM93] :

Théorème 10 ([Sil94, Chapitre I, Théorème 8.1] et [Coh93, Section 7.6.1])**.** *Soit $\tau \in \mathbb{H}$ et $q = e^{2i\pi\tau}$. On a*

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n\geqslant 1} (1-q^n)^{24} = (2\pi)^{12} q \left(1 + \sum_{n\geqslant 1} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2}\right)\right)^{24}.$$

La série intervenant dans la décomposition est bien plus pratique car les termes sont de petite taille, et les exposants croissent quadratiquement en n. Pour utiliser cette décomposition, il faut relier le j-invariant modulaire et le discriminant modulaire :

Théorème 11 ([Coh93, Section 7.6.1])**.** *Soit $\tau \in \mathbb{H}$ et $q = e^{2i\pi\tau}$. On a*

$$j(\tau) = \frac{(256 f(\tau)+1)^3}{f(\tau)} \text{ où } f(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}.$$

Remarque 8. Il faut remarquer que

$$\Delta(2\tau) = (2\pi)^{12} q^2 \left(1 + \sum_{n\geqslant 1} (-1)^n \left(q^{n(3n-1)} + q^{n(3n+1)}\right)\right)^{24}.$$

L'article [AM93, Section 7] relie la précision désirée et le nombre de termes nécessaires à calculer dans la série du théorème 10 :

Théorème 12 ([AM93, Section 7]). *Soit N un entier, et soit $q \in \mathbb{C}$, $|q| < 1$. Alors*

$$\left| \sum_{n \leqslant N+1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2}) \right| \leqslant 6|q|^{3N^2/2}.$$

Les théorèmes 11 et 12 répondent à la deuxième problématique. On peut donner l'algorithme complet du calcul du polynôme de classes de Hilbert (algorithme 3.2.1). L'algorithme 3.2.1 repose sur l'algorithme 3.2.2 pour calculer la précision nécessaire dans le calcul du j-invariant. Le fonctionnement de l'algorithme 3.2.2 est détaillée dans [Coh93, Section 7.6.2].

Algorithme 3.2.1 : Calcul du polynôme de classes de Hilbert [Coh93, Algorithme 7.6.1]

Entrées : D le discriminant de l'anneau d'entiers d'un corps quadratique imaginaire.

Output : H_D le polynôme de classes de Hilbert

Soit $k = \text{CalculPrécision}(D)$.
Soit $P = 1$, $b = D \bmod 2$, $B = \lfloor \sqrt{-D/3} \rfloor$.
tant que $b \leqslant B$ **faire**
  Soit $t = (b^2 - D)/4$ et $a = b$.
  tant que $a^2 \leqslant t$ **faire**
    si $a \mid t$ **alors**
      Soit $j = j((-b + i\sqrt{-D})/(2a))$ (calculé avec k bits significatifs)
      si $a = b$ *ou* $a^2 = t$ *ou* $b = 0$ **alors**
        $P \leftarrow (x - j)P$
      sinon
        $P \leftarrow (x^2 - 2\,\mathrm{Re}(j)x + |j|^2)P$
    $a \leftarrow a + 1$
  $b \leftarrow b + 2$
Arrondir les coefficients de P et le renvoyer

Exemple 2. Soit $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$, un corps quadratique imaginaire, son anneau d'entiers a discriminant $D = -20$. On pose $B = \lfloor \sqrt{20/3} \rfloor = 2$. On commence l'énumération des formes quadratiques réduites de discriminant D.

- Pour $b = 0$, on définit $t = (b^2 - D)/4 = 5$.
  - Pour $a = 0$, on a $a \nmid t$.
  - Pour $a = 1$, on a $a \mid t$, donc on obtient la forme $(1, 0, 5)$.
  - Pour $a = 2$, on a $a \nmid t$.
- Pour $b = 2$, on définit $t = (b^2 - D)/4 = 6$.
  - Pour $a = 2$, on a $a \mid t$, donc on obtient la forme $(2, 2, 3)$.

Algorithme 3.2.2 : CalculPrécision(D)

Entrées : D le discriminant de l'anneau d'entiers d'un corps quadratique imaginaire.

Soit $S = 0$, $b = D \bmod 2$, $B = \lfloor \sqrt{-D/3} \rfloor$.
tant que $b \leqslant B$ **faire**
  Soit $t = (b^2 - D)/4$ et $a = b$.
  tant que $a^2 \leqslant t$ **faire**
    si $a \mid t$ **alors**
      si $a = b$ *ou* $a^2 = t$ *ou* $b = 0$ **alors**
        $S \leftarrow S + \frac{1}{a}$
      sinon
        $S \leftarrow S + \frac{2}{a}$
    $a \leftarrow a + 1$
  $b \leftarrow b + 2$
Renvoyer $\lceil \frac{\pi\sqrt{-D}S}{\ln(10)} \rceil + 10$.

On déduit de l'énumération la précision $k = 20$. On calcule les valeurs des j-invariants.

```
sage: tau = I*sqrt(D)/2; elliptic_j(tau,prec=66) #10^20 vaut environ 2^66
1.2645389094751405 09e6
sage: tau = (-2+I*sqrt(D))/4; elliptic_j(tau,prec=66)
-538.9094751405093202
```

On calcule une valeur approchée du polynôme de Hilbert : $P = x^2 - 1264000.00000000x - 681472000.000000$. On en déduit que

$$H_{-20} = x^2 - 1264000x - 681472000.$$

3.2.3 Génération de courbes elliptiques de trace prescrite sur les corps premiers

Dans cette section, on présente une application de la théorie du corps de classes à la génération de courbes elliptiques d'ordre prescrit sur les corps finis. Le problème considéré est le suivant : soit N un entier positif, et $p \geqslant 5$ un entier premier tel que $|N - p - 1| \leqslant 2\sqrt{p}$ et $N \neq p + 1$, on cherche à construire une courbe elliptique E sur le corps K à p éléments, de trace $t = N - p - 1$. Il est possible de trouver une telle courbe en calculant les racines modulo p du polynôme de classes de Hilbert associé à un discriminant bien choisi.

Pour tout N vérifiant les conditions ci-dessus, il existe :

— D un entier négatif congru à t^2 modulo 4 tel que $8 \nmid D$ et pour tout premier $l > 2$ divisant D, on a $l^2 \nmid D$.

— un entier y tel que $t^2 - 4p = Dy^2$.

En particulier, D est le discriminant de l'anneau d'entiers du corps quadratique imaginaire $\mathcal{K} = \mathbb{Q}(\sqrt{D})$. On sait que t et p sont premiers entre eux, donc $p \nmid Dy^2$ et $D \equiv (t/y)^2 \bmod p$ est un carré modulo p. Donc l'idéal principal $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ est scindé dans $\mathcal{K}$. On sait que, à conjugaison près, $\mathfrak{p} = (\pi)$ où $\pi = \frac{t+\sqrt{D}y}{2} \in \mathbb{Z}_\mathcal{K}$ (π est entier car t^2 et D ont la même congruence modulo 4). L'idéal $\mathfrak{p}$ est principal, donc il est totalement scindé dans $\mathrm{Hil}(\mathcal{K})$. Soit $\mathfrak{P}$ un premier de $\mathrm{Hil}(\mathcal{K})$ au-dessus de $\mathfrak{p}$, alors $\mathrm{Hil}(\mathcal{K})_\mathfrak{P} = \mathbb{F}_p$.

L'algorithme 3.2.3 calcule une courbe de trace t définie sur $\mathbb{F}_p$. L'idée de l'algorithme est qu'il existe une courbe E_0 définie sur $\mathrm{Hil}(\mathcal{K})$ qui a multiplication complexe par $\mathbb{Z}_\mathcal{K}$, et dont la réduction modulo $\mathfrak{P}$ est une courbe elliptique E définie sur $\mathbb{F}_p$ telle que

$$\mathbb{Z}_\mathcal{K} \simeq \mathrm{End}(E_0) \simeq \mathrm{End}(E),$$

et telle que $\pi \in \mathbb{Z}_\mathcal{K}$ est envoyé sur le morphisme de Frobenius dans $\mathrm{End}(E)$ (pour des détails sur la réduction des courbes elliptiques en caractéristique p, le lecteur peut consulter [Lan87]). On en déduit donc que le polynôme minimal du Frobenius sur E est $x^2 - tx + p$ et que t est la trace de E. On sait que $j(E_0)$ est une racine de H_D. On peut donc trouver directement le j-invariant de E en cherchant parmi les racines de H_D modulo p.

Algorithme 3.2.3 : Génération de courbes elliptiques

Entrées : $p \geqslant 5$ un premier, $t \in [-2\sqrt{p}, 2\sqrt{p}] \setminus \{0\}$ entier.

Output : E une courbe elliptique sur le corps à p éléments de trace t.

```
1 Déterminer K un corps quadratique imaginaire et D le discriminant de son anneau
    d'entiers tel que t^2 − 4p = 0 mod D et (t^2 − 4p)/D est un carré.
2 Soit y un entier tel que t^2 − 4p = Dy^2.
3 Déterminer l'expression de H_D, le polynôme de classes de Hilbert associé à D.
4 Soit K un corps fini à p éléments. Calculer R l'ensemble des racines de H_D dans K.
5 pour j ∈ R faire
6 |   Soit E une courbe sur K de j-invariant j.
7 |   pour E' une tordue de E faire
8 |   |   si E' a trace t alors
9 |   |   |   Renvoyer E'.
```

Exemple 3. Soit $p = 34873130969$ et $t = 372876$. On peut vérifier que p est premier, et donc p et t sont premiers entre eux. On calcule

$$t^2 - 4p = -456012500 = -20 \times 4775^2 \tag{3.2.1}$$

Soit $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$ et $\mathbb{Z}_\mathcal{K}$ l'anneau d'entiers de $\mathcal{K}$. Le discriminant de l'ordre $\mathbb{Z}_\mathcal{K}$ est -20. Soit $\mathbb{F}_p$ un corps fini à p éléments, l'équation (3.2.1) garantit qu'il existe une courbe elliptique E sur $\mathbb{F}_p$, à multiplication complexe par $\mathbb{Z}_\mathcal{K}$. Dans ce cas son j-invariant est une racine du polynôme de classes de Hilbert

$$H_{-20} = x^2 - 1264000x - 681472000 \equiv (x - 23162900482)(x - 11711494487) \bmod p$$

dans $\mathbb{F}_p$. Posons $j = 23162900482$, alors la courbe

$$\tilde{E} : y^2 = x^3 + 3j(1728 - j)x - 2j(1728 - j)^2 = x^3 + 22026048806x + 14488057806$$

a j-invariant j et trace $-372876 = -t$. Soit

$$E : y^2 = x^3 + 302722578x + 19597229242$$

une tordue quadratique de $\tilde{E}$, alors la trace de E est $t = 372876$. On trouve une courbe avec la trace désirée, donc on ne considère pas le j-invariant $j = 11711494487$.

3.3 Théorie du corps de classes pour les corps de fonctions

Les corps de fonctions (sur les corps finis) sont des corps semblables aux corps de nombres, du point de vue de l'arithmétique. Leurs ordres maximaux sont des anneaux de Dedekind et on peut dans les deux cas définir les notions de places (les premiers des ordres maximaux), valuations associées et un groupe de classes. L'unicité de la décomposition d'un idéal en produit d'idéaux premiers dans les ordres maximaux permet d'étudier le comportement des places dans des extensions, et de distinguer trois cas : la décomposition, l'inertie et la ramification. Au vu de ces similitudes, il n'est pas surprenant que les corps de fonctions disposent d'une théorie du corps de classes, dont les résultats sont très proches de ceux de la théorie du corps de classes pour les corps de nombres. Il est même possible de définir une théorie du corps de classes pour les corps globaux (i.e. une théorie commune aux corps de nombres et aux corps de fonctions définis sur des corps finis), comme par exemple dans [AT09].

Cependant, bien que semblable, l'arithmétique des corps de fonctions est différente de celle des corps de nombres sur plusieurs points. Par exemple, les corps de fonctions disposent d'une infinité d'ordres maximaux, contrairement aux corps de nombres qui n'en ont qu'un seul. Un autre exemple : soit $\mathcal{K}$ un corps de nombres, alors son extension abélienne non ramifiée maximale $\mathrm{Hil}(\mathcal{K})$ est une extension finie, tandis que pour $K(X)$ un corps de fonction défini sur un corps fini K, et pour $\bar{K}$ une clôture algébrique de K, on voit que $\bar{K} \otimes_K K(X)$ est une extension abélienne non ramifiée de degré infini de $K(X)$. Enfin, les corps de fonctions ont une caractéristique positive, ce qui rend l'étude de la ramification plus complexe que pour les corps de nombres. Ainsi plusieurs expositions de la théorie du corps de classes ont été rédigées pour le cas spécifique des corps de fonctions.

Dans cette thèse, on ne présentera que le cas non ramifié de la théorie du corps de classes sur les corps de fonctions. Le cas ramifié est étudié par Serre dans [Ser84] en utilisant des jacobiennes généralisées [Ros54]. On commence par présenter une exposition géométrique à la Serre [Ser84] dans la section 3.3.1. C'est le point de vue qui nous intéresse le plus, puisqu'il servira dans le chapitre 4 pour définir des codes de Goppa structurés. On présente également l'exposition de Rosen [Ros87], qui montre très explicitement l'analogie avec les corps de nombres dans la section 3.3.2. Enfin, on discute rapidement des liens entre les deux points de vue dans la section 3.3.3.

3.3.1 Approche géométrique

Soit K un corps fini à $q = p^m$ éléments, $\bar{K}$ une clôture algébrique de K, et X une courbe projective lisse sur K. La théorie du corps de classes (pour les extensions non ramifiées) des corps de fonctions se formule géométriquement en utilisant les revêtements définis et abéliens sur K (non ramifiés) de X et la jacobienne $\mathcal{J}_X$.

En effet, soit

$$\tau : Y \longrightarrow X$$

un revêtement abélien sur K de groupe de Galois G, il définit une extension $K(Y)/K(X)$ abélienne de $K(X)$. Cette section résume une partie des résultats de [Lan56a, Lan56b] et [Ser84] sur le lien entre les isogénies de la jacobienne et les revêments abéliens non ramifiés de la courbe.

Dans la suite, on notera F_V l'endomorphisme de Frobenius (associé à K) sur une K-variété V. Toute K-variété V définit naturellement une variété sur $\bar{K}$ que nous identifierons à V.

Définition 29.

— Soit $\theta : \mathbb{G} \longrightarrow \mathbb{G}'$ un morphisme de groupes algébriques commutatifs connexes sur $\bar{K}$. On dit que θ est une isogénie si θ est surjectif et que son noyau est fini.

— On dit que θ est séparable si son degré est égal à l'ordre de son noyau.

— Si $\mathbb{G}$ et $\mathbb{G}'$ sont des K-variétés, on dit que θ est définie sur K si

$$F_{\mathbb{G}'} \circ \theta = \theta \circ F_{\mathbb{G}}.$$

Définition 30. Soit V une $\bar{K}$-variété, $\mathbb{G}$ et $\mathbb{G}'$ deux groupes algébriques commutatifs connexes sur $\bar{K}$. Soit $f : V \longrightarrow \mathbb{G}'$ une application régulière et $\theta : \mathbb{G} \longrightarrow \mathbb{G}'$ une isogénie séparable. On définit $V \times_{\mathbb{G}'} \mathbb{G}$ le produit fibré de V et $\mathbb{G}$ sur $\mathbb{G}'$ comme la sous-variété de $V \times \mathbb{G}$ dont les point $\bar{K}$-rationnels sont

$$V \times_{\mathbb{G}'} \mathbb{G}(\bar{K}) = \{(x, g) \in V \times \mathbb{G} \mid f(x) = \theta(g)\}.$$

Le produit fibré $V \times_{\mathbb{G}'} \mathbb{G}$ est muni de projections π_V et π_G qui font commuter le diagramme suivant :

$$\begin{array}{ccc} V \times_{\mathbb{G}'} \mathbb{G} & \xrightarrow{\pi_{\mathbb{G}}} & \mathbb{G} \\ \Big\downarrow{\scriptstyle \pi_V} & & \Big\downarrow{\scriptstyle \theta} \\ V & \xrightarrow[f]{} & \mathbb{G}' \end{array}$$

On dit que π_V est le tiré en arrière de θ par f, et on note $\pi_V = f^{-1}(\theta)$.

On remarque que l'isogénie θ est un revêtement abélien non ramifié de $\mathbb{G}'$ de groupe de Galois G composé des translations par les éléments de $\ker\theta$. Alors π_V est un revêtement abélien de groupe de Galois G, non ramifié de V.

Lemme 13. Avec les notations de la définition 30, si V, $\mathbb{G}$ et $\mathbb{G}'$ sont des K-variétés, et si f et θ sont définies sur K, alors $V \times_{\mathbb{G}'} \mathbb{G}$ est une K-variété et π_V est défini sur K.

Démonstration. Notons $W = V \times_{\mathbb{G}'} \mathbb{G}$. Soit $(x, g) \in W$. On veut vérifier que W est stable par

$$F_{V\times\mathbb{G}} : (y, h) \longmapsto (F_V(y), F_{\mathbb{G}}(h)).$$

Pour cela on calcule

$$f(F_V(x)) = F_{\mathbb{G}'}(f(x)) = F_{\mathbb{G}'}(\theta(g)) = \theta(F_{\mathbb{G}}(g)),$$

donc W est stable par $F_{V\times\mathbb{G}}$ et est bien une K-variété.

De plus, $\pi_V(F_W((x, g))) = F_V(x) = F_V(\pi_V((x, g)))$, donc π_V est définie sur K. □

Revenons à l'étude de la courbe X. La jacobienne $\mathcal{J}_X$ de X est un groupe algébrique commutatif connexe défini sur K. De plus, soit P un point K-rationnel de X, l'application de Jacobi j_P associée à P est une application régulière de X dans $\mathcal{J}_X$ définie sur K. Soit

$$\theta : \mathbb{G} \longrightarrow \mathcal{J}_X$$

une isogénie séparable, notons

$$Y = X \times_{\mathcal{J}_X} \mathbb{G}.$$

Alors Y est une courbe projective lisse intègre (sur $\bar{K}$), et $\pi_X : Y \longrightarrow X$ est un revêtement abélien non ramifié de X. De plus, on peut démontrer que

- Y est une K-variété et π_X est défini sur K si et seulement si θ est défini sur K.
- le revêtement π_X est galoisien sur K si et seulement si, de plus, l'action de $F_{\mathbb{G}}$ sur $\ker\theta$ est triviale. Dans ce cas, le revêtement est abélien de groupe de Galois isomorphe à $\ker\theta$.
- le revêtement π_X est totalement décomposé au-dessus de P si et seulement si, de même, l'action de $F_{\mathbb{G}}$ sur $\ker\theta$ est triviale.

Théorème 14 ([Ser84, Chapitre I, Corollaire du Théorème 4 et Théorème 5])**.** *Soit K un corps fini et X une courbe projective lisse sur K. Soit P un point K-rationnel de X.*

Il existe une courbe Y_{max} projective lisse sur K et un revêtement

$$\tau_{max} : Y_{max} \longrightarrow X$$

abélien sur K non ramifié totalement décomposé au-dessus de P et maximal dans le sens suivant : pour tout revêtement

$$\tau_Y : Y \longrightarrow X$$

satisfaisant ces propriétés, il existe un revêtement abélien non ramifié

$$\tau_{Y_{max}/Y} : Y_{max} \longrightarrow Y$$

tel que

$$\tau = \tau_Y \circ \tau_{Y_{max}/Y}.$$

Le revêtement τ_{max} est obtenu en tirant en arrière l'isogénie

$$\varphi = F_{\mathcal{J}_X} - \mathrm{Id},$$

par l'application de Jacobi j_P.

Le théorème 14 induit une correspondance entre les classes d'isomorphismes de revêtements définis et abéliens sur K, non ramifiés et totalement décomposés au-dessus de P de X et les sous-groupes de $\mathcal{J}_X(K)$. En effet, soit H un sous-groupe de $\mathcal{J}_X(K)$, il existe une isogénie séparable dont le noyau est H. On note cette isogénie

$$\pi_H : \mathcal{J}_X \longrightarrow \mathcal{J}_X/H.$$

Il existe alors

$$\theta : \mathcal{J}_X/H \longrightarrow \mathcal{J}_X$$

une isogénie telle que

$$\theta \circ \pi_H = F_{\mathcal{J}_X} - \mathrm{Id}\,.$$

Le revêtement

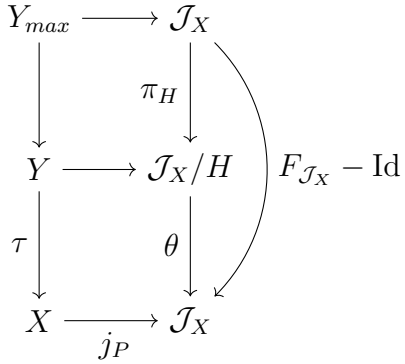
$$\tau = j_P^{-1}(\theta) \tag{3.3.1}$$

est un revêtement de X abélien sur K, non ramifié, totalement décomposé au-dessus de P, de groupe de Galois $\mathcal{J}_X(K)/H$.

Proposition 15. Avec les notations du théorème 14, soit Q un point K-rationnel de X, et soit H un sous-groupe de $\mathcal{J}_X(K)$. Soit $\tau : Y \longrightarrow X$ le revêtement abélien sur K, non ramifié, totalement décomposé au-dessus de P, associé à H, défini dans l'équation (3.3.1).

Alors τ est totalement décomposé au-dessus de Q si et seulement si la classe de $Q - P$ dans $\mathcal{J}_X(K)$ appartient à H.

Démonstration. Il faut vérifier que la fibre de τ au-dessus de Q est composée de points K-rationnels. Nous sommes dans la situation suivante :



Notons c la classe de $Q - P$ dans $\mathcal{J}_X(K)$. On doit vérifier que les points de Y au-dessus de Q sont fixés par le morphisme de Frobenius sur Y si et seulement si $c \in H$. Soit $(Q, a + H)$ un point de Y au-dessus de Q. On a

$$F_Y((Q, a + H)) = (F_X(Q), F_{J_X/H}(a + H)) = (Q, F_{\mathcal{J}_X}(a) + H)$$

où $\theta(a+H) = j_P(Q) = c$. Donc $(Q, a+H)$ est fixé par F_Y si et seulement si $F_{J_X}(a)-a \in H$. Mais

$$F_{J_X}(a) - (a) = \theta(a + H) = c,$$

donc $F_{J_X}(a) - a \in H$ si et seulement si $c \in H$. □

3.3.2 Approche algébrique

Dans cette section, on résume la présentation de [Ros87] de la théorie du corps de classes (cas non-ramifié), et sa définition d'un corps de classes de Hilbert pour les corps de fonctions. Soit K un corps fini à $q = p^m$ éléments, et X une courbe projective lisse sur K. Soit $K(X)_{sep}$ une clôture séparable de $K(X)$. Soit $\bar{K}$ la clôture algébrique de K dans $K(X)_{sep}$.

Il existe une extension abélienne non ramifiée de $K(X)$ maximum dans $K(X)_{sep}$, mais cette extension est de degré infini (même relativement à $\bar{K}(X)$). Pour définir un corps de classes de Hilbert dont le degré d'extension est fini, il faut rajouter une condition qui, entre autres, limite l'extension du corps des constantes. Soit S_∞ un ensemble fini non vide de places de $K(X)$ de degrés quelconques. Soit $\mathcal{O}_{X\setminus S_\infty}$ l'anneau des fonctions ayant leurs pôles en S_∞. C'est un anneau de Dedekind (voir [Ros87, Section 1]) dont le groupe de classes $\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty})$ est fini. On peut faire une analogie entre le triplet $K(X), \mathcal{O}_{X\setminus S_\infty}, S_\infty$ et un corps de nombres, son anneau d'entiers, et ses places à l'infini.

Proposition 16. Il existe une extension abélienne non ramifiée maximum de $K(X)$ dans $K(X)_{sep}$ dans laquelle les places de S_∞ sont totalement décomposées. On l'appelle corps de classes de Hilbert de $K(X)$ par rapport à S_∞, et on la note $\mathrm{Hil}_{S_\infty}(X)$.

Démonstration. Les propriétés d'être abélienne, d'être non ramifiée, et d'être totalement décomposée au-dessus de S_∞ sont conservées par compositum. □

Proposition 17. Soit

$$\delta = \mathrm{pgcd}_{P \in S_\infty} \deg P.$$

Soit $L = \bar{K} \cap \mathrm{Hil}_{S_\infty}(X)$ le corps des constantes de $\mathrm{Hil}_{S_\infty}(X)$. Alors L est l'extension de K de degré δ dans $\bar{K}$.

Démonstration. Soit $P \in S_\infty$ et soit Q une place au-dessus de P. Soit K_Q le corps résiduel en Q. Puisque P est totalement décomposée dans $\mathrm{Hil}_{S_\infty}(X)$, on sait que K_Q est égal à K_P le corps résiduel en P. Or L est un sous-corps de K_Q, donc de K_P. Donc le degré de l'extension L/K divise $\deg P$. C'est le cas quelle que soit $P \in S_\infty$, donc

$$[L : K] \mid \delta.$$

Soit L' l'extension de K de degré δ dans $\bar{K}$. Alors le compositum $L'\operatorname{Hil}_{S_\infty}(X)$ est une extension de Galois de $K(X)$ dont le groupe de Galois est un sous-groupe de

$$\mathbf{Gal}(L'(X)/K(X)) \times \mathbf{Gal}(\operatorname{Hil}_{S_\infty}(X)/K(X)) = \mathbf{Gal}(L'/K) \times \mathbf{Gal}(\operatorname{Hil}_{S_\infty}(X)/K(X)).$$

C'est donc une extension abélienne de $K(X)$. De plus, d'après [Sti08, Théorème 3.6.3], $L'\operatorname{Hil}_{S_\infty}(X)$ est non ramifiée, et toutes les places de S_∞ sont totalement décomposées dans $L'\operatorname{Hil}_{S_\infty}(X)$, car δ divise le degré de toutes les places de S_∞. Par maximalité de $\operatorname{Hil}_{S_\infty}(X)$, on en déduit

$$L'\operatorname{Hil}_{S_\infty}(X) = \operatorname{Hil}_{S_\infty}(X) \text{ et } L' = L.$$

□

Proposition 18. Soit N le sous-groupe de $\operatorname{Div}(X)$ engendré par les places de S_∞. Alors il existe un isomorphisme de groupe

$$I(\mathcal{O}_{X\setminus S_\infty}) \simeq \operatorname{Div}(X)/N$$

où $I(\mathcal{O}_{X\setminus S_\infty})$ est le groupe des idéaux fractionnaires de $\mathcal{O}_{X\setminus S_\infty}$.

Démonstration. D'après [Sti08, Proposition 3.2.9], les idéaux premiers de $\mathcal{O}_{X\setminus S_\infty}$ sont en bijection avec les places de $K(X)$ qui ne sont pas dans S_∞. Puisque $\operatorname{Div}(X)$ est le groupe abélien libre engendré par les places de $K(X)$, et que $I(\mathcal{O}_{X\setminus S_\infty})$ est isomorphe au groupe abélien libre engendré par les idéaux premiers de $\mathcal{O}_{X\setminus S_\infty}$, on en déduit le résultat. □

On peut définir l'application d'Artin de l'extension $\operatorname{Hil}_{S_\infty}(X)/K(X)$ comme dans la définition 21. Soit P une place de $K(X)$ et Q une place de $\operatorname{Hil}_{S_\infty}(X)$ au-dessus de P. On note $D(Q/P)$ le groupe de décomposition de Q et $I(Q/P)$ son groupe d'inertie. Puisque $\operatorname{Hil}_{S_\infty}(X)/K(X)$ est une extension non ramifiée, $I(Q/P)$ est trivial. Notons K_P et K_Q les corps résiduels en P et Q respectivement, on a alors un isomorphisme canonique

$$D(Q/P) \longrightarrow \mathbf{Gal}(K_Q/K_P).$$

Soit $\mathfrak{s}_Q \in D(Q/P)$ l'élément associé au morphisme de Frobenius via cet isomorphisme. Puisqu'il ne dépend pas du choix de Q (l'extension est abélienne), on le note $\mathfrak{s}_P$. On définit

$$(.,\operatorname{Hil}_{S_\infty}(X)/K(X)) : \begin{array}{ccc} \operatorname{Div}(X) & \longrightarrow & \mathbf{Gal}(\operatorname{Hil}_{S_\infty}(X)/K(X)) \\ \sum_P n_P P & \longmapsto & \prod \mathfrak{s}_P^{n_P} \end{array}$$

l'application d'Artin.

On peut remarquer que l'application d'Artin est triviale sur S_∞ par définition de $\operatorname{Hil}_{S_\infty}(X)$. Alors $(.,\operatorname{Hil}_{S_\infty}(X)/K(X))$ induit un morphisme

$$I(\mathcal{O}_{X\setminus S_\infty}) \longrightarrow \mathbf{Gal}(\operatorname{Hil}_{S_\infty}(X)/K(X)).$$

Théorème 19 ([Ros87, Théorème 1.3])**.** *L'application d'Artin* $(.,\operatorname{Hil}_{S_\infty}(X)/K(X))$ *est surjective et induit un isomorphisme*

$$\operatorname{Cl}(\mathcal{O}_{X\setminus S_\infty}) \xrightarrow{\sim} \mathbf{Gal}\left(\operatorname{Hil}_{S_\infty}(X)/K(X)\right).$$

Ce théorème démontre que cette définition du corps de classes de Hilbert de $K(X)$ permet d'obtenir une situation très semblable au cas des corps de nombres. Pour compléter cette exposition, il faut exprimer $\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty})$ en fonction de $\mathrm{Pic}(X)$ et de S_∞ et donner son nombre de classes.

Théorème 20 ([Ros87, Théorème 1.3 et Lemmes 1.1-2])**.**

— *Soit N le sous-groupe de $\mathrm{Pic}(X)$ engendré par les classes des places de S_∞. Alors*

$$\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \simeq \mathrm{Pic}(X)/N.$$

— *Soit H le sous-groupe de $\mathrm{Pic}^0(X)$ engendré par les places de S_∞ (i.e. les classes des combinaisons linéaires de S_∞ de degré 0). Alors*

$$|\mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty})| = \delta |\mathrm{Pic}^0(X)|/|H|$$

où $\delta = \mathrm{pgcd}_{P\in S_\infty} \deg P$.

Corollaire 20.1. *$[\mathrm{Hil}_{S_\infty}(X) : K(X)]$ est fini.*

Corollaire 20.2. *Le noyau de l'application d'Artin est le sous-groupe de $\mathrm{Div}(X)$ engendré par les diviseurs principaux et les places de S_∞.*

Corollaire 20.3. *Supposons que $S_\infty = \{P\}$ où P est une place de $K(X)$ de degré 1. Alors*

$$\mathbf{Gal}(\mathrm{Hil}_{S_\infty}(X)/K(X)) \simeq \mathrm{Pic}^0(X) = \mathcal{J}_X(K).$$

En particulier, à tout sous-groupe H de $\mathrm{Pic}^0(X)$, on associe une unique extension abélienne non ramifiée de $K(X)$ dans $K(X)_{sep}$ de groupe de Galois naturellement isomorphe à $\mathrm{Pic}^0(X)/H$ (et réciproquement).

Corollaire 20.4. *Supposons que $S_\infty = \{P\}$ où P est une place de $K(X)$ de degré 1. Soit $K(X) \subset K(Y) \subset \mathrm{Hil}_{S_\infty}(X)$ l'extension associée au sous-groupe H de $\mathrm{Pic}^0(X)$. Soit Q une place de $K(X)$, alors Q est totalement décomposée dans $K(Y)$ si et seulement si*

$$Q - \deg(Q)P \in H.$$

Preuve du théorème 20. La première affirmation est une conséquence directe de la proposition 18. On démontre la deuxième affirmation.

On sait qu'il existe une suite exacte de groupes additifs

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathbb{Z} \longrightarrow 0$$

d'après un théorème de Schmidt [Sch31]. On a similairement

$$0 \to \mathrm{Pic}^0(X)/(\mathrm{Pic}^0(X) \cap N) \to \mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \to \mathrm{Pic}(X)/(N + \mathrm{Pic}^0(X)) \to 0$$

Or

$$(\mathrm{Pic}^0(X) \cap N) = H,$$

et

$$\mathrm{Pic}(X)/\mathrm{Pic}^0(X) \simeq \mathbb{Z},$$

et

$$(N + \mathrm{Pic}^0(X))/\mathrm{Pic}^0(X) \simeq \delta\mathbb{Z}.$$

On en déduit

$$0 \longrightarrow \mathrm{Pic}^0(X)/H \longrightarrow \mathrm{Cl}(\mathcal{O}_{X\setminus S_\infty}) \longrightarrow \mathbb{Z}/\delta\mathbb{Z} \longrightarrow 0.$$

□

3.3.3 Liens entre les approches

On voit qu'une partie des résultats du théorème 14 et de la proposition 15 sont retrouvés dans les corollaires 20.3 et 20.4. Dans cette section, on étudie les relations entre le point de vue algébrique et le point de vue géométrique.

Soit K un corps fini à $q = p^m$ éléments, et X une courbe projective lisse sur K. Soit $K(X)_{sep}$ une clôture séparable de $K(X)$. Soit $\bar{K}$ la clôture algébrique de K dans $K(X)_{sep}$. Soit S_∞ un ensemble fini non vide de places de $K(X)$ tels que

$$\delta := \mathrm{pgcd}_{P\in S_\infty} \deg P = 1.$$

Soit $\mathcal{O}_{X\setminus S_\infty}$ l'anneau des fonctions ayant leurs pôles en S_∞.

Puisque le degré de l'extension $\mathrm{Hil}_{S_\infty}(X)/K(X)$ est fini, le corps $\mathrm{Hil}_{S_\infty}(X)$ est aussi un corps de fonction (sur K car $\delta = 1$). Ainsi, il existe une courbe Y projective lisse sur K telle que $K(Y) = \mathrm{Hil}_{S_\infty}(X)$. Il est naturel de se demander quelles sont les relations géométriques entre X et Y.

Premier cas : S_∞ contient une place de degré 1

Il s'agit du cas le plus simple et le plus direct. Soit P un point K-rationnel de X correspondant à une place de degré 1 de S_∞. L'extension $K(Y)/K(X)$ est abélienne non-ramifiée, ce qui signifie qu'il existe

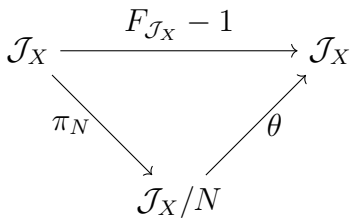
$$\tau : Y \longrightarrow X$$

un revêtement non-ramifié abélien sur K. De plus, puisque $P \in S_\infty$, on sait que τ est totalement décomposé au-dessus de P.

Soit N le sous-groupe de $\mathcal{J}_X(K)$ engendré par les classes de $Q - \deg(Q)P$ pour $Q \in S_\infty$. On sait que

$$\mathbf{Gal}(K(Y)/K(X)) \simeq \mathcal{J}_X(K)/N$$

d'après les théorèmes 19 et 20. Soit θ l'isogénie séparable faisant commuter le diagramme suivant :



où π_N est l'isogénie quotient. Alors τ est isomorphe au tiré en arrière de θ par j_P l'application de Jacobi associée à P d'après le théorème 14.

Cas général

Le cas général demande d'être un peu plus prudent, car il peut ne pas y avoir de places de degré 1 dans S_∞. Cependant, puisque $\delta = 1$, on sait qu'il existe $D \in \mathrm{div}(X)$ un diviseur engendré par les places de S_∞ de degré 1. Soit N le sous-groupe de $\mathcal{J}_X(K)$ engendré par les classes de $Q - \deg(Q)D$ pour $Q \in S_\infty$. Alors d'après les théorèmes 19 et 20,

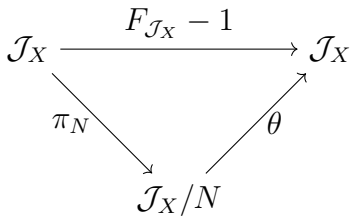
$$\mathbf{Gal}(K(Y)/K(X)) \simeq \mathcal{J}_X(K)/N.$$

Il existe

$$\tau : Y \longrightarrow X$$

un revêtement abélien sur K non ramifié totalement décomposé au-dessus des points associés aux places de S_∞.

Soit j_D l'application de Jacobi associée au diviseur D (qui à tout point fermé P de X associe la classe de $P - \deg(P)D$ dans $\mathcal{J}_X$). C'est une application régulière et définie sur K (car D est de degré 1). Soit θ l'isogénie séparable faisant commuter le diagramme suivant :



Alors τ est isomorphe au tiré en arrière de θ par j_D.

3.4 Construction de courbes algébriques avec beaucoup de points rationnels

Les courbes (lisses projectives) définies sur les corps fini disposant de nombreux points rationnels sont très interessantes. En effet, étant donné un corps fini K, il est possible de montrer que, lorsque le genre grandit, la borne de Weil devient grossière, et n'est plus suffisante pour estimer correctement le nombre maximal de points rationnels qu'une courbe

peut posséder. Or, dans le cadre de la conception de codes de Goppa (voir section 4.2), il est important de connaître des courbes X sur K disposant du plus grand nombre de points K-rationnels possible par rapport à leur genre. La base de données manYPoints [vdGHLR09] recense, en fonction de l'ordre du corps q et du genre g, les courbes connues ayant le plus grand nombre de points. Elle recense également les meilleures majorations connues du nombre maximum de points qu'une courbe peut posséder.

Soit $q = p^m$ l'ordre de K, on définit la constante d'Ihara

$$A(q) = \limsup_{X/K} \frac{N(X)}{g_X}$$

où $N(X)$ et g_X désignent respectivement le nombre de points K-rationnels et le genre de X. La constante d'Ihara est une donnée qui décrit avec précision le nombre maximal de points qu'une courbe sur K peut posséder asymptotiquement. Elle est très utile pour décrire la qualité des codes de Goppa sur K (en tant que famille de codes).

La théorie du corps de classes permet de construire des exemples de courbes avec beaucoup de points. Dans la sous-section 3.4.1, on explique comment construire des courbes avec beaucoup de points comme extension abélienne d'une autre courbe, et on donne un exemple issu de [Ser20, Section 7.3]. On présente également de nouvelles courbes possédant des nombres records de points sur les corps à 4, 9, 16 et 25 éléments. Dans la sous-section 3.4.2, on explique qu'il est possible de minorer la constante d'Ihara en construisant des tours d'extensions abéliennes non-ramifiées de courbes (d'après [Ser20, Section 5.9]).

3.4.1 Exemples de constructions

Dans cette sous-section, on explique comment construire des courbes algébriques possédant beaucoup de points comme revêtements abéliens non-ramifiés au-dessus d'une autre courbe. En particulier, on présente de nouvelles courbes ayant un nombre de points record relativment à leur genre sur les corps finis à 4, 9, 16 et 25 éléments. Cette méthode est généralisable au cas abélien ramifié (voir [Ser20, Section 7.3]).

Soit X une courbe projective lisse sur un corps fini K. On suppose que X possède un point K-rationnel P. Soit H un sous-groupe de $\mathcal{J}_X(K)$. D'après le théorème 14, il existe une courbe projective lisse Y_H et un revêtement abélien non-ramifié

$$\tau_H : Y_H \longrightarrow X$$

de groupe de Galois isomorphe à $\mathcal{J}_X(K)/H$ et totalement décomposé au-dessus de P. De plus, d'après la proposition 15, les points K-rationnels de Y_H sont dans les fibres (totalement décomposées) au-dessus des points Q de X de degré 1, tels que

$$j_P(Q) \in H.$$

Soit n le nombre de points K-rationnels de X dont l'image par j_P appartient à H. Soit

$$d = \frac{|\mathcal{J}_X(K)|}{|H|},$$

et soit g_X le genre de X et g_{Y_H} le genre de Y_H. Alors

— la courbe Y_H a nd points K-rationnels.

— d'après la formule de Riemann–Hurwitz, puisque τ_H est non-ramifié,

$$g_{Y_H} = d(g_X - 1) + 1.$$

L'exemple suivant est issu de [Ser20, Section 7.3].

Exemple 4. Soit X la courbe projective lisse de genre $g_X = 2$ définie sur $\mathbb{F}_2$ par

$$X : y^2 + y = \frac{x^2 + x}{x^3 + x + 1}.$$

La courbe X compte 6 points $\mathbb{F}_2$-rationnels, et on peut montrer qu'il existe un ismorphisme de groupe abélien

$$\mathcal{J}_X(\mathbb{F}_2) \simeq \mathbb{Z}/19\mathbb{Z}.$$

Soit P un point $\mathbb{F}_2$-rationnel de X, et soit

$$\tau : Y \longrightarrow X$$

un revêtement abélien non-ramifié totalement décomposé au-dessus de P de groupe de Galois isomorphe à $\mathcal{J}_X(\mathbb{F}_2)$ (associé au sous-groupe $H = \{0\}$). Alors P est le seul point $\mathbb{F}_2$-rationnel de X totalement décomposé dans Y, et Y est une courbe de genre $g_Y = 20$ avec 19 points $\mathbb{F}_2$-rationnels.

Il est possible de montrer qu'une courbe de genre 20 sur $\mathbb{F}_2$ possède au plus 21 points [Ser20, Section 7.1]. La question de savoir s'il existe une courbe de genre 20 sur $\mathbb{F}_2$ ayant au moins 20 points n'est toujours pas résolue [vdGHLR09].

Le nombre de sous-groupes de $\mathcal{J}_X(K)$ peut croître exponentiellement en le genre et polynomialement en q, le nombre d'éléments de K. Ainsi, il devient vite difficile d'énumérer ces sous-groupes pour produire des courbes records. On présente une astuce utilisée dans [GX22, NX98, Que89, vdG09] consistant à étudier un sous-groupe spécifique. Supposons qu'il existe κ un sous-corps de K d'indice 2, et que la courbe X est définie sur κ, i.e. qu'il existe une courbe projective lisse X_κ sur κ telle que

$$X = (X_\kappa)_K .$$

Dans ce contexte, une astuce consiste à choisir pour P un point κ-rationnel de X, i.e. stable sous l'action de $\mathbf{Gal}(K/\kappa)$ sur X, et à poser

$$H = \mathcal{J}_{X_\kappa}(\kappa)$$

le sous-groupe des points κ-rationnels de $\mathcal{J}_X(K)$. Alors, $\tau_H : Y_H \longrightarrow X$ est un revêtement abélien non-ramifié de groupe de Galois

$$G = \mathcal{J}_X(K)/\mathcal{J}_X(\kappa)$$

et les points de X totalement décomposés dans Y_H sont exactement les points κ-rationnels de X.

En particulier, si le polynôme-L de X_κ est connu, on peut calculer :

— le polynôme-L de X.

— l'ordre de $\mathcal{J}_X(\kappa)$ et l'ordre de $\mathcal{J}_X(K)$.

— la trace de X_κ, ou de manière équivalente le nombre de points κ-rationnels de X.

On peut alors déterminer l'ordre de G, le genre g_{Y_H} de Y_H et le nombre de points K-rationnels de Y_H.

On va désormais utiliser cette astuce pour produire de nouvelles courbes records. La base de données LMFDB [LMF25] recense, entre autres, des polynômes-L de courbes algébriques sur les corps finis à 2, 3, 4 et 5 éléments (entre autres). En énumérant parmi ces données, on peut produire de nouvelles courbes avec un nombre record de points sur les corps finis à 4, 9, 16 et 25 éléments. On présente ces records dans les tables 3.1, 3.2, 3.3 et 3.4.

Étiquette LMFDB de X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_4)$	Précédent record ([vdGHLR09])
4.2.d_i_o_x	11	34	66	65
5.2.e_m_ba_bv_cu	12	49	84	81

TABLE 3.1 – Nouvelles courbes ayant un nombre de points record sur un corps à 4 éléments

Étiquette LMFDB de X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_9)$	Précédent record ([vdGHLR09])
4.3.i_bi_ds_hn	9	28	108	105
4.3.h_ba_co_ez	11	34	121	114
4.3.h_bb_ct_fk	12	37	132	126

TABLE 3.2 – Nouvelles courbes ayant un nombre de points record sur un corps à 9 éléments

Étiquette LMFDB de X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_{16})$	Précédent record ([vdGHLR09])
3.4.g_v_bx	19	39	209	194
3.4.f_p_bg	23	47	230	$\emptyset$

TABLE 3.3 – Nouvelles courbes ayant un nombre de points record sur un corps à 16 éléments

3.4.2 Tours de courbes

Soit K un corps fini à $q = p^m$ éléments. On souhaite minorer la constante d'Ihara

$$A(q) = \limsup_{X/K} \frac{N(X)}{g_X}$$

Étiquette LMFDB de X	$\lvert G\rvert$	g_{Y_H}	$\#Y_H(\mathbb{F}_{25})$	Précédent record ([vdGHLR09])
3.5.k_bv_fc	16	33	256	226
3.5.j_bn_ec	20	41	300	260
3.5.j_bo_eh	21	43	315	276
3.5.i_bf_dc	24	49	336	315

TABLE 3.4 – Nouvelles courbes ayant un nombre de points record sur un corps à 25 éléments

où $N(X)$ désigne le nombre de points K-rationnels sur X et g_X désigne le genre de X. Pour cela, il faut définir une suite de courbes $(X_i)_{i\in\mathbb{N}}$ projectives lisses sur K telle que $N(X_i)/g_{X_i}$ converge vers une constante non-nulle.

Il est possible d'utiliser la théorie du corps de classes pour définir de telles suites de courbes [Ser20, Section 5.9]. Soit X une courbe projective lisse sur K, soit S un ensemble fini non-vide de points K-rationnels de X et soit ℓ un premier (potentiellement égal à la caractéristique p). On définit

- $(X_0, S_0) = (X, S)$;
- pour tout $i \in \mathbb{N}$, le revêtement $\tau_i : X_{i+1} \longrightarrow X_i$ est le revêtement abélien, non-ramifié, d'ordre une puissance de ℓ, totalement décomposé au-dessus des points de S_i, maximal ;
- pour tout $i \in \mathbb{N}$, l'ensemble S_{i+1} est l'ensemble des points dans les fibres au-dessus des points de S_i.

Ainsi, en composant les τ_i, on obtient une suite de revêtements galoisiens non-ramifiés totalement décomposés au-dessus de S. Notons que nous pouvons affirmer que ces revêtements sont galoisiens grâce à la maximalité des τ_i. On appelle la suite $(X_i)_{i\in\mathbb{N}}$ la (S,ℓ)-*tour de corps de classes* de X.

Soit G_i le groupe de Galois du revêtement $X_i \longrightarrow X$ pour tout $i \in \mathbb{N}$, alors G_i est un groupe fini d'ordre une puissance de ℓ. De plus, pour tout $i \in \mathbb{N}$, le groupe G_i est un quotient de G_{i+1}. On définit

$$G = \varprojlim G_i.$$

Le groupe G est un pro-ℓ-groupe. Posons r le nombre minimal de générateurs de G (comme pro-ℓ-groupe). Notons que $r \geqslant 1$ si et seulement si $\mathcal{J}_X(K)$ a un sous-groupe d'ordre ℓ.

Théorème 21 ([Ser20, Théorème 5.9.4])**.** *On utilise les notations du début de la sous-section 3.4.2. Supposons que $r \geqslant 1$ et que*

$$\#S \leqslant \frac{r^2}{4} - r + \begin{cases} 1 \text{ si } \ell \text{ divise } q-1, \\ 0 \text{ sinon.} \end{cases}$$

Alors la (S,ℓ)-tour de corps de classes de X est infinie, i.e. la suite $(X_i)_{i\in\mathbb{N}}$ n'est pas stationnaire.

Le théorème suivant utilise une tour de corps de classes infinie de X pour minorer la constante d'Ihara.

Théorème 22 ([Ser20, Théorème 5.9.5])**.** *On utilise les notations du début de la sous-section 3.4.2. Supposons que la (S, ℓ)-tour de corps de classes de X est infinie. Alors*

$$A(q) \geqslant \frac{\#S}{g_X - 1}.$$

Démonstration. Définissons d_i l'ordre de G_i pour tout $i \in \mathbb{N}$. D'après la formule de Riemann–Hurwitz, on a

$$g_{X_i} = d_i(g_X - 1) + 1.$$

De plus, puisque les points de S sont totalement décomposés dans X_i, donc $N(X_i)$, le nombre de points K-rationnels de X_i, vérifie

$$N(X_i) \geqslant \#S \cdot d_i.$$

En particulier, $(N(X_i)_{i\in\mathbb{N}})$ diverge car $(d_i)_{i\in\mathbb{N}}$ diverge. On a

$$\frac{N(X_i)}{g_{X_i}} \geqslant \frac{\#S \cdot d_i}{d_i(g_X - 1) + 1}$$

et en prenant la limite en $i \to +\infty$

$$A(q) \geqslant \limsup_{i\in\mathbb{N}} \frac{N(X_i)}{g_{X_i}} \geqslant \frac{\#S}{g_X - 1}.$$

□

Corollaire 22.1 ([Ser20, Corollaire 5.9.7])**.** *Soit $q = p^m$ une puissance de premier avec $m > 0$. Alors*

$$A(q) > 0.$$

Chapitre 4

Codes correcteurs

L'objectif de ce chapitre est de présenter une famille de codes de Goppa disposant d'une structure additionnelle. Cette structure a un intérêt algorithmique, permettant de réduire l'espace nécessaire pour stocker les matrices génératrices et de contrôle des codes, et permettant dans certains cas de réduire la complexité de l'encodage et du décodage.

Dans la section 4.1, on rappelle rapidement les notions basiques de la théorie des codes correcteurs linéaires. Ensuite, dans la section 4.2, on présente la définition des codes géométriques de Goppa, également appelés codes AG, et quelques-unes de leurs propriétés. Dans la section 4.3, on rappelle la définition d'une algèbre de groupe, et on présente la transformation de Fourier d'une algèbre de groupe abélien fini. On détaille la complexité du calcul de la transformée de Fourier sur les corps finis, et on montre que les algèbres de groupe abélien fini sur les corps finis disposent d'une multiplication rapide.

Ensuite, dans la section 4.4, étant donnés G un groupe fini et K un corps fini, on étudie des codes linéaires définis par les sous-modules à gauche (et à droite) libres de $K[G]^E$, pour E un ensemble fini. En particulier, on définit la notion de code dual dans ce contexte particulier, et on montre que ces codes possèdent des matrices génératrices (et des matrices de contrôle) à coefficients dans $K[G]$. Enfin, dans la section 4.5, on définit une nouvelle famille de codes géométriques, provenant de revêtements abéliens non-ramifiés de groupe de Galois G. Sous certaines hypothèses usuelles, ces codes sont des sous-$K[G]$-modules libres de $K[G]^E$, pour E un ensemble fini. On étudie les spécificités de cette nouvelle famille de codes.

4.1 Codes linéaires

On commence par introduire les notions basiques de la théorie des codes correcteurs. Le lecteur peut se référer à [Sti08] ou n'importe quel livre sur le sujet des codes correcteurs pour plus de détails sur ce qui suit. Dans cette section, K désigne un corps fini à $q = p^m$ éléments.

4.1.1 Définitions générales

Un *code correcteur* C de *longueur* n et *dimension* k sur K est un sous-espace vectoriel de K^E de dimension k, où E est un ensemble de cardinal n. On dit également que C est un $[n,k]$-code sur K. Soit $c \in C$, on dit que c est un mot du code C. On utilisera parfois la notation $\operatorname{len} C$ pour désigner la longueur de C et $\dim C$ pour désigner sa dimension. Dans le cas où $E = [1..n]$ l'ensemble des entiers de 1 à n, on notera $K^E = K^n$.

Définition 31. Soit $a = (a_i)_{i \in E} \in K^E$, on définit

$$\operatorname{wt}(a) = \#\{i \in E | a_i \neq 0\}$$

le poids de a. On définit la *distance de Hamming* d sur K^E

$$\forall a, b \in K^E, d(a,b) = \operatorname{wt}(b-a).$$

La distance de Hamming est bien une distance sur K^E.

Définition 32. Soit C un $[n,k]$-code sur K avec $k > 0$. On définit

$$d(C) = \min_{\substack{a,b \in C \\ a \neq b}} d(a,b) = \min_{\substack{c \in C \\ c \neq 0}} \operatorname{wt}(c)$$

la *distance minimale* de C. On définit également

$$\rho(C) = \frac{k}{n} \text{ et } \delta(C) = \frac{d(C)}{n}$$

le *rendement* et la *distance relative* de C. Dans le cas où $d \in \mathbb{N}$ est la distance minimale de C, on dira que C est un $[n,k,d]$-code sur K. On appelle la *capacité de correction* de C l'entier $t(C) = \lfloor \frac{d-1}{2} \rfloor$.

La distance minimale, la dimension et la longueur sont reliées de la manière suivante :

Théorème 23 (Borne de Singleton)**.** *Soit C un $[n,k,d]$-code sur K, alors*

$$d + k \leqslant n + 1.$$

Si l'inégalité précédente est une égalité, on dit que C est MDS (pour Maximum Distance Separable en anglais).

Soit F un ensemble de cardinal k, on note $\mathcal{M}_{F,E}(K)$ le K-espace vectoriel des matrices indexées par $F \times E$. Dans le cas où $F = [1..k]$, on notera $\mathcal{M}_{k,E}(K)$ à la place de $\mathcal{M}_{F,E}(K)$. Dans le cas où $E = [1..n]$, on notera $\mathcal{M}_{F,n}(K)$ à la place de $\mathcal{M}_{F,E}(K)$.

Pour représenter une matrice de $\mathcal{M}_{F,E}(K)$ sous forme de tableau de coefficients, il faut fixer un ordre sur les éléments de F et E. Par convention, si E ou F sont des ensembles d'entiers, on choisira systématiquement l'ordre naturel sur les entiers.

Soit G un ensemble fini. On rappelle la définition du produit matriciel

$$\begin{array}{ccc} \mathcal{M}_{F,E}(K) \times \mathcal{M}_{E,G}(K) & \longrightarrow & \mathcal{M}_{F,G}(K) \\ ((m_{i,j})_{(i,j)\in F\times E}, (m'_{i,j})_{(i,j)\in E\times G}) & \longmapsto & (\sum_{e\in E} m_{i,e}m'_{e,j})_{(i,j)\in F\times G} \end{array}$$

Soit $C \subset K^E$ un $[n,k]$-code correcteur sur K. Il existe une matrice $\mathcal{E} \in \mathcal{M}_{F,E}(K)$ telle que

$$C = \{a\mathcal{E}; a \in K^F\}.$$

On dit que $\mathcal{E}$ est une *matrice génératrice* de C. Soit G un ensemble de cardinal $n-k$, il existe une matrice $\mathcal{C} \in \mathcal{M}_{E,G}(K)$ telle que

$$C = \{a \in K^E \mid a\mathcal{C} = 0\}.$$

On dit que $\mathcal{C}$ est une *matrice de contrôle* de C. On a

$$\mathcal{E}\mathcal{C} = 0.$$

L'espace vectoriel K^E est naturellement muni d'une forme bilinéaire symétrique non-dégénérée :

$$\langle ., . \rangle : a, b \in K^E \mapsto \sum_{i\in E} a_i b_i. \tag{4.1.1}$$

On définit alors le *code dual* $C^\perp$ de C par

$$C^\perp = \{a \in K^E \mid \forall c \in C, \langle a, c\rangle = 0\}.$$

Si C est un $[n,k]$-code alors $C^\perp$ est un $[n, n-k]$-code. Les matrices génératrices de $C^\perp$ sont les transposées des matrices de contrôle de C et inversement.

4.1.2 Familles de codes linéaires

Soit $(C_i)_{i\in\mathbb{N}}$ une famille de codes dont les longueurs divergent. On note

$$\delta_{lim} = \liminf \delta(C_i) \text{ et } \rho_{lim} = \liminf \rho(C_i).$$

Alors la borne de Singleton impose

$$\delta_{lim} + \rho_{lim} \leqslant 1.$$

Un des objectifs de la théorie des codes est de construire des codes s'approchant le plus possible de cette borne. Un résultat classique est le suivant :

Théorème 24 (Borne de Gilbert–Varshamov)**.** *Soit $\delta_{lim} \in]0, 1-q^{-1}[$, il existe $(C_i)_{i\in\mathbb{N}}$ une famille de codes linéaires sur K dont les longueurs divergent telle que* $\liminf \delta(C_i) = \delta_{lim}$ *et*

$$\rho_{lim} = \liminf \rho(C_i) = 1 - H_q(\delta_{lim}),$$

où

$$H_q : x \longmapsto x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x).$$

Remarque 9. Cette borne est atteinte par les familles de codes aléatoires (dont les longueurs divergent).

On peut naturellement demander s'il existe des familles de codes dont les paramètres sont meilleurs que ceux du théorème de Gilbert-Varshamov. Plus précisément, soit $\delta_{lim} \in]0, 1 - q^{-1}[$, existe-t-il une famille de codes linéaires $(C_i)_{i\in\mathbb{N}}$ sur K dont les longueurs divergent et telle que

$$\liminf \delta(C_i) = \delta_{lim} \text{ et } \liminf \rho(C_i) > 1 - H_q(\delta_{lim}) \ ?$$

Cette question motive les définitions suivantes (voir [Lac86]).

Définition 33. Soit $(C_i)_{i\in\mathbb{N}}$ une famille de codes linéaires sur K dont les longueurs divergent. On dit que $(C_i)_{i\in\mathbb{N}}$ est une famille de *bons code* si

$$\liminf \delta(C_i) > 0 \text{ et } \liminf \rho(C_i) > 0.$$

Définition 34. Soit $(C_i)_{i\in\mathbb{N}}$ une famille de bons codes linéaires sur K. Soit $\delta_{lim} = \liminf \delta(C_i)$. Supposons que $\delta_{lim} \in]0, 1 - q^{-1}[$. On dit que $(C_i)_{i\in\mathbb{N}}$ est une famille de *codes excellents* si

$$\liminf \rho(C_i) > 1 - H_q(\delta_{lim}).$$

4.1.3 Le problème du décodage

Pour finir cette section, on présente le *problème du décodage* de codes correcteurs linéaires. Soit $C \subset K^E$ un $[n, k, d]$-code correcteur sur K. Soit c un mot du code C et $e \in K^E$. Soit $t > 0$ un entier, on suppose que

$$\mathrm{wt}(e) \leqslant t \leqslant t(C) = \lfloor (d-1)/2 \rfloor.$$

Enfin, soit

$$r = c + e.$$

Le problème du décodage (de C) est le suivant : étant donné C, r et t, déterminer c, l'unique mot du code C à distance au plus t de r.

Le problème du décodage est un problème NP-difficile [BMvT78]. Cependant, lorsque le problème du décodage est restreint à certaines familles de codes, il est possible de le résoudre en temps polynomial en la longueur du code. En particulier, on verra dans la section 4.2.3 que c'est le cas des codes de Goppa.

4.2 Codes géométriques de Goppa

Les codes géométriques de Goppa, aussi appelés codes AG, sont une famille spécifique de codes linéaires introduits par Goppa au début des années 80 [Gop83] pour généraliser les codes de Reed–Solomon [RS60]. Les codes géométriques de Goppa ont de bonnes propriétés

asymptotiques, et dépassent la borne de Gilbert-Varshamov lorsque q le cardinal du corps de base est suffisamment grand. Le lecteur peut se référer à [Sti08] pour une étude détaillée des codes AG.

On commence par présenter les codes de Reed–Solomon. Soit K un corps fini à $q = p^m$ éléments. Soient k et n deux entiers tels que $0 < k \leqslant n \leqslant q$. Soient $P_1, \ldots, P_n \in K$ des éléments distincts. On définit

$$P = \{P_i; 1 \leqslant i \leqslant n\}.$$

Notons $K[x]_{\leqslant k-1}$ l'ensemble des polynôme sur K de degrés inférieurs à $k-1$. C'est évidemment un K-espace vectoriel de dimension k. Soit l'application K-linéaire d'évaluation en P

$$\mathrm{ev}_P : f \in K[x]_{\leqslant k-1} \longmapsto (f(P_i))_{P_i \in P} \in K^P.$$

Cette application est injective puisqu'un polynôme $f \in K[x]_{\leqslant k-1}$ non nul a au plus $k-1 < n$ racines. En utilisant l'isomorphisme canonique de K-espaces vectoriels

$$\begin{array}{rccc} \varphi : & K^k & \longrightarrow & K[x]_{\leqslant k-1} \\ & (f_i)_{0 \leqslant i \leqslant k-1} & \longmapsto & \sum_{i=0}^{k-1} f_i x^i \end{array}$$

on peut définir un $[n,k]$-code de Reed–Solomon (ou code RS) avec la matrice génératrice $\mathcal{E}$ correspondant à l'application linéaire $\mathrm{ev}_P \circ \varphi$ dans les bases canoniques de K^k et K^P :

$$\mathcal{E} = \begin{pmatrix} 1 & 1 & & 1 \\ P_1 & P_2 & \cdots & P_n \\ P_1^2 & P_2^2 & & P_n^2 \\ \vdots & \vdots & & \vdots \\ P_1^{k-1} & P_2^{k-1} & & P_n^{k-1} \end{pmatrix} \in \mathcal{M}_{k,P}(K).$$

On définit donc

$$\mathrm{RS}(k,P) = \mathrm{Im}\ \mathcal{E} = \{(f(P_i))_{P_i \in P}; f \in K[x]_{\leqslant k-1}\}.$$

Proposition 25. $\mathrm{RS}(k,P)$ est un $[n,k]$-code MDS. Autrement dit,

$$d(\mathrm{RS}(k,P)) = n - k + 1.$$

Les codes RS sont intéressants puisqu'ils atteignent la borne de Singleton. De plus, ils ont de bonnes propriétés algorithmiques. Leur défaut réside principalement dans leur longueur. En effet, les codes de Reed–Solomon ne peuvent pas avoir une longueur supérieure à q ce qui en fait des codes relativement courts. L'idée de Goppa en introduisant les codes géométriques était de généraliser les codes de Reed–Solomon dans une situation où davantage de points d'évaluation sont disponibles.

4.2.1 Définition

Soit K un corps fini à $q = p^m$ éléments. Soit X une courbe projective lisse géométriquement intègre sur K et $K(X)$ son corps de fonctions. Soit g le genre de X. Soient $P_1, \ldots, P_n \in X(K)$ des points K-rationnels de X distincts deux à deux, et

$$P = \sum_{i=1}^{n} P_i \in \mathrm{Div}(X).$$

Soit $D \in \mathrm{Div}(X)$ un diviseur de degré positif tel que $\mathrm{supp}\, D \cap \mathrm{supp}\, P = \emptyset$. On note

$$\mathcal{L}(D) := \Gamma_X(\mathcal{O}_X(D))$$

l'espace de Riemann–Roch associé à D, et $\ell(D)$ sa dimension en tant que K-espace vectoriel. On note également

$$\mathbf{R}_P := \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$$

l'algèbre résiduelle en P. On notera K^P à la place de $K^{\mathrm{supp}\, P}$. On note

$$\mathrm{ev}_{D,P} : \mathcal{L}(D) \longrightarrow \mathbf{R}_P$$

l'application d'évaluation des fonctions de l'espace de Riemann–Roch $\mathcal{L}(D)$ en P. Dans ce cas précis, il existe un isomorphisme canonique de K-espaces vectoriels

$$\mathbf{R}_P \simeq \bigoplus_{i=1}^{n} K_{P_i}$$

entre l'algèbre résiduelle en P et la somme directe des corps résiduels en les places P_i. Puisque les places P_i sont K-rationnelles, ces corps résiduels sont naturellement isomorphes à K. On peut alors définir le code géométrique de Goppa associé à D et P :

$$\mathrm{Gop}(P, D) = \{(f(P_i))_{P_i \in P} \in K^P ; f \in \mathcal{L}(D)\} \simeq \mathrm{Im}\ \mathrm{ev}_{D,P}.$$

L'application $\mathrm{ev}_{D,P}$ n'est en général pas injective. Son noyau est $\mathcal{L}(D-P)$. On en déduit la propriété suivante :

Proposition 26. Avec les notations précédentes,

$$\dim(\mathrm{Gop}(P, D)) = \ell(D) - \ell(D - P).$$

En particulier, si $2g - 1 \leqslant \deg D \leqslant n - 1$, le théorème de Riemann–Roch impose que

$$\dim(\mathrm{Gop}(P, D)) = \deg D - g + 1.$$

Soit $k = \dim(\mathrm{Gop}(P, D))$. Si $k > 0$, on peut donner une estimation de la distance minimale de $\mathrm{Gop}(P, D)$:

Proposition 27. Avec les notations précédentes, si $k > 0$

$$d(\mathrm{Gop}(P, D)) \geqslant n - \deg D.$$

En particulier, si $2g - 1 \leqslant \deg D \leqslant n - 1$,

$$d(\mathrm{Gop}(P, D)) \geqslant n - k - g + 1.$$

En effet, soit $f \in \mathcal{L}(D)$, telle que f s'annule en $\deg D + 1$ places de P. Soit P' le diviseur de degré $\deg D + 1$ composé des places P_i où f s'annule, alors $f \in \mathcal{L}(D - P')$ car $\operatorname{supp} D \cap \operatorname{supp} P' = \emptyset$. Or $\deg(D - P') = -1$, ainsi f est nécessairement nulle.

On note

$$d^*(P, D) = n - \deg D \tag{4.2.1}$$

la *distance prescrite* du code $\mathrm{Gop}(P, D)$. La proposition 27 montre que les codes AG sont proches d'être MDS. Dans le cas particulier $g = 0$, ils le sont même systématiquement (par exemple les codes de Reed–Solomon). On notera

$$t^*(P, D) = \left\lfloor \frac{d^*(P, D) - 1}{2} \right\rfloor \tag{4.2.2}$$

la *capacité de correction prescrite* de $\mathrm{Gop}(P, D)$.

Dans le cas où $\deg D \leqslant n - 1$, l'application $\mathrm{ev}_{D,P}$ est injective, et on peut définir une matrice génératrice $\mathcal{E}_{D,P}$ du code $\mathrm{Gop}(P, D)$. Elle n'est pas canonique puisqu'il n'existe en général pas de base canonique de $\mathcal{L}(D)$. Soit $f_1, \ldots, f_k$ une base de $\mathcal{L}(D)$, on définit

$$\mathcal{E}_{D,P} = \begin{pmatrix} f_1(P_1) & f_1(P_2) & & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & & f_2(P_n) \\ f_3(P_1) & f_3(P_2) & \cdots & f_3(P_n) \\ \vdots & \vdots & & \vdots \\ f_k(P_1) & f_k(P_2) & & f_k(P_n) \end{pmatrix} \in \mathcal{M}_{k,P}(K).$$

Les codes duaux des codes AG sont également de nature géométrique. En effet le K-espace vectoriel $\mathbf{R}_P$ est en dualité avec le K-espace vectoriel

$$\Omega_P := \Gamma_X(\Omega_{X/K}(-P)/\Omega_{X/K})$$

via la forme K-bilinéaire

$$\begin{array}{rccc} \langle ., . \rangle_X : & \mathbf{R}_P \times \Omega_P & \longrightarrow & K \\ & (f, \omega) & \longmapsto & \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega) \end{array} \tag{4.2.3}$$

où $\mathrm{Res}_{P_i}(f\omega)$ désigne le résidu en P_i de $f\omega$.

Remarque 10. Les notations de l'équation (4.2.3) sont légèrement abusives, donc on précise notre propos. Le faisceau $\mathcal{O}_X/\mathcal{O}_X(-P)$ a un nombre fini de fibres non-nulles, les fibres en les places $(P_i)_{i \in [1..n]}$ de P. De plus, pour $i \in [1..n]$, la fibre de $\mathcal{O}_X/\mathcal{O}_X(-P)$ en P_i est

$$\mathcal{O}_{P_i}/P_i = K_{P_i}.$$

On sait alors qu'un élément f de $\mathbf{R}_P = \Gamma_X(\mathcal{O}_X/\mathcal{O}_X(-P))$ est exactement la donnée de ses germes

$$f_i \in \mathcal{O}_{P_i}/P_i$$

pour tout $i \in [1..n]$. Soit $\tilde{f}_i \in \mathcal{O}_{P_i}$ telle que

$$\tilde{f}_i \bmod P_i = f_i.$$

Similairement, étant donné $\omega \in \Omega_P$, on peut déterminer $(\tilde{\omega_i})_{i\in[1..n]}$ des différentielles de $\Omega(X/K)$ telles que

$$\nu_{P_i}(\tilde{\omega_i}) \geqslant -1$$

décrivant le germe de ω en les $(P_i)_{i\in[1..n]}$. Alors on peut vérifier que pour tout $i \in [1..n]$, le résidu $\mathrm{Res}_{P_i}(\tilde{f}_i\tilde{\omega_i})$ ne dépend que de f et ω. On note donc $\mathrm{Res}_{P_i}(f\omega)$ pour le désigner.

Puisque les $(P_i)_{i\in[1..n]}$ sont K-rationnels, on sait que les corps résiduels $(K_{P_i})_{i\in[1..n]}$ sont naturellement isomorphes à K. Ainsi, l'application bilinéaire de l'équation (4.2.3) correspond à la forme bilinéaire canonique $\langle ., . \rangle$ sur K^P via les isomorphismes naturels

$$\begin{array}{ccc} \mathbf{R}_P & \longrightarrow & K^P \\ f & \longmapsto & (f(P_i))_{P_i\in P} \end{array}$$

et

$$\begin{array}{ccc} \Omega_P & \longrightarrow & K^P \\ \omega & \longmapsto & (\mathrm{Res}_{P_i}(\omega))_{P_i\in P} \end{array}.$$

L'équation (4.2.3) motive la définition de codes à partir d'espaces de différentielles. Pour tout diviseur D' de X, on note

$$\Omega(D') := \Gamma_X(\Omega_{X/K}(D'))$$

et $\iota(D')$ sa dimension en tant que K-espace vectoriel (ou de manière équivalente l'indice de spécialité de D'). Puisque D et P sont disjoints, on a une application

$$\mathrm{res}_{D,P} : \Omega(D - P) \longrightarrow \Omega_P \tag{4.2.4}$$

L'image de $\mathrm{res}_{D,P}$ dans Ω_P est l'orthogonal de l'image de $\mathrm{ev}_{D,P}$ pour la forme $\langle ., . \rangle_X$.

On peut définir

$$\begin{aligned} \mathrm{Gop}_\Omega(P, D) &= \{(\mathrm{Res}_{P_i}(\omega))_{P_i\in P} \in K^P ; \omega \in \Omega(D - P)\} \\ &\simeq \mathrm{Im}\ \mathrm{res}_{D,P} \end{aligned}$$

Proposition 28. Avec les notations précédentes,

$$\mathrm{Gop}_\Omega(P, D) = \mathrm{Gop}(P, D)^\perp.$$

En particulier, si $2g-1 \leqslant \deg D \leqslant n-1$ alors l'application $\mathrm{res}_{D,P}$ est injective et

$$\begin{aligned}\dim \mathrm{Gop}_\Omega(P,D) = \dim \Omega(D-P) &= \iota(D-P)\\ &= n - \deg D + g - 1\\ &= n-k.\end{aligned}$$

Étant donné une base $(\omega_1, \ldots, \omega_{n-k})$ de $\Omega(D-P)$, on a une matrice génératrice de $\mathrm{Gop}_\Omega(P,D)$:

$$\mathcal{C}_{D,P} = \begin{pmatrix} \mathrm{Res}_{P_1}(\omega_1) & \mathrm{Res}_{P_2}(\omega_1) & & \mathrm{Res}_{P_n}(\omega_1)\\ \mathrm{Res}_{P_1}(\omega_2) & \mathrm{Res}_{P_2}(\omega_2) & & \mathrm{Res}_{P_n}(\omega_2)\\ \mathrm{Res}_{P_1}(\omega_3) & \mathrm{Res}_{P_2}(\omega_3) & \cdots & \mathrm{Res}_{P_n}(\omega_3)\\ \vdots & \vdots & & \vdots\\ \mathrm{Res}_{P_1}(\omega_{n-k}) & \mathrm{Res}_{P_2}(\omega_{n-k}) & & \mathrm{Res}_{P_n}(\omega_{n-k}) \end{pmatrix} \in \mathcal{M}_{n-k,P}(K).$$

En particulier ${\mathcal{C}_{D,P}}^t$ est une matrice de contrôle de $\mathrm{Gop}(P,D)$ (où $.^t$ désigne la transposition de matrice).

Remarque 11. Il est possible de généraliser les définitions de cette section au cas où

$$\mathrm{supp}\, D \cap \mathrm{supp}\, P \neq \emptyset.$$

En effet les applications de passage au quotient

$$\mathcal{L}(D) \longrightarrow \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P))$$

et

$$\Omega(D-P) \longrightarrow \Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D))$$

offrent des alternatives à $\mathrm{ev}_{D,P}$ et $\mathrm{res}_{D,P}$ dans ce contexte. En revanche, il n'y a plus d'isomorphismes naturels entre $\Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P))$ ou $\Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D))$ et K^P.

Ce problème est résolu sans difficulté. Il suffit de trouver deux isomorphismes,

$$\varphi\colon \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P)) \longrightarrow K^P$$

et

$$\psi\colon \Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D)) \longrightarrow K^P,$$

de manière à ce que, pour toutes

$$f \in \Gamma_X(\mathcal{O}_X(D)/\mathcal{O}_X(D-P)) \text{ et } \omega \in \Gamma_X(\Omega_{X/K}(D-P)/\Omega_{X/K}(D)),$$

on ait

$$\langle \varphi(f), \psi(\omega)\rangle = \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega),$$

où $\langle .,. \rangle$ désigne la forme K-bilinéaire naturelle sur K^P définie dans l'équation (4.1.1). Il est aisé de construire de tels isomorphismes, en utilisant des uniformisantes en les places $P_i \in \mathrm{supp}\, P \cap \mathrm{supp}\, D$.

4.2.2 Propriétés asymptotiques

Soit K un corps fini à $q = p^m$ éléments. Pour trouver une famille de codes AG intéressante, on cherche des courbes $(X_i)_{i\in\mathbb{N}}$ projectives lisses géométriquement intègres sur K ayant un grand nombre de places rationnelles relativement à leurs genres. La quantité qui nous intéresse ici est donc

$$A(q) = \limsup \frac{\#X(K)}{g_X}$$

où g_X désigne le genre de X. Nous avons discuté dans la section 3.4 de la grossièreté de la borne de Weil lorsque le genre diverge vers l'infini. Le théorème 29 en est une illustration.

Théorème 29 (Borne de Drinfeld–Vladut [VD83])**.** *Avec les notations précédentes,*

$$A(q) \leqslant \sqrt{q} - 1.$$

Cette inégalité est vraie pour toute puissance de premier $q = p^m$. Dans le cas où m est pair, i.e. q est un carré, les constructions de [Iha81] et [TVZ82] démontrent que $A(q) = \sqrt{q} - 1$.

On utilise ce résultat pour définir une famille de codes AG. Soit $(X_i)_{i\in\mathbb{N}}$ une famille de courbes projectives lisses géométriquement intègres, de genres g_{X_i} croissants, telle que

$$\lim \#X_i(K)/g_{X_i} = \sqrt{q} - 1.$$

Pour tout $i \in \mathbb{N}$, soit $n_i = \#X_i(K)$ et soient $P_{i,1}, \ldots, P_{i,n_i}$ des points K-rationnels de X_i et

$$P_i = P_{i,1} + \cdots + P_{i,n_i}.$$

Soit D_i un diviseur de X_i tel que $2g_{X_i} - 1 \leqslant \deg D_i \leqslant n_i - 1$. Soit

$$C_i = \mathrm{Gop}(D_i, P_i).$$

Alors

$$\rho(C_i) = \frac{\deg D_i - g_{X_i} + 1}{n_i} \text{ et } \delta(C_i) \geqslant \frac{n_i - \deg D_i}{n_i},$$

et donc

$$\rho(C_i) \geqslant \frac{n_i - g_{X_i} + 1}{n_i} - \delta(C_i).$$

Dans le cas où $\deg D_i/g_{X_i}$ converge, en posant $\delta_{lim} = \lim \delta(C_i)$ et $\rho_{lim} = \lim \rho(C_i)$, on obtient

$$\rho_{lim} \geqslant 1 - \frac{1}{\sqrt{q} - 1} - \delta_{lim}. \tag{4.2.5}$$

On voit que cette famille de codes approche fortement la borne de Singleton lorsque q est grand. En réalité, pour $q \geqslant 49$ fixé, la minoration (4.2.5) est parfois meilleure que la borne de Gilbert-Varshamov.

Théorème 30 (Tsfasman–Vladut–Zink bound[TVZ82]). *Avec les notations précédentes, si q est un carré et $q \geqslant 49$, il existe $0 < \delta_1 \leqslant \delta_2 < 1 - \frac{1}{q}$ tels que pour tout $x \in [\delta_1, \delta_2]$,*

$$1 - \frac{1}{\sqrt{q} - 1} - x \geqslant 1 - H_q(x).$$

Ces résultats démontrent qu'il existe des familles excellentes de codes AG. Plus précisément, il existe une famille de codes AG excellente sur K si q est un carré et $q \geqslant 49$.

4.2.3 Décodage des codes géométriques

Au début des années 90, un nombre important de contributions visant à généraliser les algorithmes de décodages des codes de Reed–Solomon aux codes AG furent proposées. Le premier algorithme développé fut l'algorithme dit basique, généralisant les algorithmes de Arimoto [Ari61] et Peterson [Pet60], d'abord par Justesen, Larsen, Elbrønd Jensen, Havemose et Høholdt [Hav89, JLJ+89] dans le cas des courbes planes, puis par Skorobogatov et Vladut dans le cas général [SV90]. Sugiyama, Kasahara, Hirasawa et Namekawa [SKHN75] ont développé un algorithme reposant sur une équation clé et l'algorithme d'Euclide, généralisé ensuite par Porter [Por88]. Ces algorithmes ont le défaut de ne pas décoder les codes AG jusqu'à leur capacité de correction prescrite. L'algorithme de Ehrhard [Ehr93] améliore l'algorithme basique et permet de décoder jusqu'à la capacité de correction prescrite. Une autre approche, due à Feng et Rao [FR93] et Duursma [Duu93], utilise le décodage par syndromes, et permet également le décodage des codes AG jusqu'à leur capacité de correction prescrite. Pour plus de détails sur ces algorithmes, le lecteur peut se référer aux excellents états de l'art de Høholdt et Pellikaan [HP95] et de Beelen et Høholdt [BH08].

On présente ici l'*algorithme basique*, pour résoudre le problème du décodage (voir sous-section 4.1.3). Soit K un corps fini à $q = p^m$ éléments. Soit X une courbe projective lisse géométriquement intègre sur K. Soient $P_1, \ldots, P_n$ des points K-rationnels de X distincts et $P = \sum_{i=1}^{n} P_i$. Soit g le genre de X et $D \in \operatorname{Div} X$ un diviseur tel que

$$\operatorname{supp} D \cap \operatorname{supp} P = \emptyset \text{ et } 2g - 1 \leqslant \deg D \leqslant n - 1.$$

On donne un algorithme de décodage pour $\operatorname{Gop}(P, D)$.

Soit $c \in \operatorname{Gop}(P, D)$ et $e \in K^P$ telle que $\operatorname{wt}(e) \leqslant t^*(P, D)$ (la capacité de correction prescrite définie dans l'équation (4.2.2)). Soit $r = c + e$, on cherche à retrouver le mot du code c à partir de la donnée r. En utilisant l'isomorphisme naturel entre K^P et $\mathbf{R}_P$, on obtient $f_r, f_c, f_e \in \mathbf{R}_P$, telles que

$$f_r = f_c + f_e \in \mathbf{R}_P, \ \ f_c \in \operatorname{Im} \operatorname{ev}_{D,P} \text{ et } \#\operatorname{supp} f_e \leqslant t^*(P, D).$$

On note $P_{\text{err}} = \operatorname{supp} f_e$, le diviseur somme des P_i sur lesquelles f_e ne s'annule pas, et $t = \deg P_{\text{err}}$. L'objectif est de trouver une fonction h qui s'annule sur P_{err}. Cette fonction nous aidera à localiser les positions des erreurs.

Soit F un diviseur tel que

$$\deg F \geqslant g + t \text{ et } \operatorname{supp} F \cap \operatorname{supp} P = \emptyset. \tag{4.2.6}$$

Alors $\mathcal{L}(F - P_{\text{err}}) \neq \{0\}$ d'après le théorème de Riemann–Roch, car $\deg(F - P_{\text{err}}) \geqslant g$. Il existe donc au moins une fonction dans $\mathcal{L}(F)$ qui s'annule sur P_{err}. Il reste à donner un moyen de déterminer une telle fonction.

Soit $h \in \mathcal{L}(F)$ une fonction quelconque. Il est clair que h induit des applications K-linéaires

$$\begin{array}{rccc} m_{D,h} : & \mathcal{L}(D) & \longrightarrow & \mathcal{L}(D+F) \\ & s & \longmapsto & hs \end{array}$$

et

$$\begin{array}{rccc} m_{P,h} : & \mathbf{R}_P & \longrightarrow & \mathbf{R}_P \\ & s & \longmapsto & \mathrm{ev}_{F,P}(h)s \end{array}$$

faisant commuter le diagramme suivant :

$$\begin{array}{ccc} \mathcal{L}(D) & \xrightarrow{\mathrm{ev}_{D,P}} & \mathbf{R}_P \\ \Big\downarrow{\scriptstyle m_{D,h}} & & \Big\downarrow{\scriptstyle m_{P,h}} \\ \mathcal{L}(D+F) & \xrightarrow[\mathrm{ev}_{D+F,P}]{} & \mathbf{R}_P \end{array}$$

Si $h \in \mathcal{L}(F - P_{\text{err}})$, alors $hf_e = 0$ et $hf_r = hf_c \in \operatorname{Im} \mathrm{ev}_{D+F,P}$. On veut s'assurer que la réciproque est vraie, i.e. que si $hf_r \in \operatorname{Im} \mathrm{ev}_{D+F,P}$ alors $h \in \mathcal{L}(F - P_{\text{err}})$. Pour cela, il va falloir faire une deuxième hypothèse sur F (et sur t).

Supposons que $h \in \mathcal{L}(F)$ est telle que $hf_r \in \operatorname{Im} \mathrm{ev}_{D+F,P}$. De manière équivalente, $hf_e \in \operatorname{Im} \mathrm{ev}_{D+F,P}$, donc il existe une fonction $a \in \mathcal{L}(D+F)$ telle que

$$\mathrm{ev}_{D+F,P}(a) = \mathrm{ev}_{F,P}(h)f_e.$$

En particulier, a s'annule sur $P - P_{\text{err}}$ (comme f_e), donc $a \in \mathcal{L}(D + F - P + P_{\text{err}})$. Puisqu'on veut démontrer $a = 0$, il suffit que

$$\mathcal{L}(D + F - P + P_{\text{err}}) = \{0\}.$$

Une condition suffisante sur F est alors

$$\deg F \leqslant n - 1 - \deg D - t. \tag{4.2.7}$$

Ainsi, si

$$g + t \leqslant \deg F \leqslant n - 1 - \deg D - t,$$

alors on peut déterminer $\mathcal{L}(F - P_{\text{err}})$ en calculant

$$\{h \in \mathcal{L}(F) \mid hf_r \in \operatorname{Im} \mathrm{ev}_{D+F,P}\}.$$

On définit la matrice diagonale $\mathcal{D}_r$ de la multiplication par f_r dans $\mathbf{R}_P$. Le calcul de $\mathcal{L}(F - P_{\text{err}})$ revient alors au calcul du noyau à gauche de

$$\mathcal{E}_{F,P} \times \mathcal{D}_r \times {\mathcal{C}_{D+F,P}}^t \in \mathcal{M}_{\ell(F),(n-\ell(D+F))}(K)$$

où $\mathcal{E}_{F,P}$ est une matrice génératrice de $\mathrm{Gop}(F, P)$ et $\mathcal{C}_{D+F,P}$ est une matrice génératrice de $\mathrm{Gop}_\Omega(D + F, P)$.

Soit maintenant $h \in \mathcal{L}(F - P_{\text{err}})$. On note P_h le diviseur somme des P_i où h s'annule, alors $P_{\text{err}} \leqslant P_h$. En particulier, la restriction de f_r à $\mathbf{R}_{P-P_h}$ est dans l'image de l'application $\mathrm{ev}_{D,P-P_h}$, et est égale à la restriction de f_c. Pour pouvoir retrouver f_c, il faut que $\mathrm{ev}_{D,P-P_h}$ soit injective. Il est suffisant de supposer que

$$\deg D \leqslant \deg(P - P_h) - 1.$$

Or $\deg(P - P_h) \geqslant n - \deg F$, donc il est suffisant que

$$\deg F \leqslant n - \deg D - 1. \tag{4.2.8}$$

Cette condition est plus faible que la condition (4.2.7).

Les conditions des équations (4.2.6) et (4.2.7) sur le degré de F impliquent que

$$0 \leqslant n - 1 - \deg D - g - 2t,$$

ou de manière équivalente

$$t \leqslant \frac{d^*(P, D) - 1 - g}{2}.$$

En particulier, on ne peut en général pas décoder jusqu'à la capacité de correction prescrite $t^*(P, D)$. Par contre, cet algorithme est essentiellement un calcul matriciel (une fois que certains précalculs sont effectués) dont les complexités temporelle et spatiale sont polynomiales. En particulier, la complexité temporelle de l'algorithme de décodage est au plus celle de la multiplication dans $\mathcal{M}_n(K)$ [BCG+17, Théorème 8.5].

4.3 Tranformée de Fourier discrète

L'objectif de cette section est d'estimer le coût de la multiplication dans $K[G]$ pour K un corps et G un groupe abélien fini. Pour cela, on doit étudier de manière plus générale la transformation de Fourier dans $A[G]$ pour toute K-algèbre commutative A.

4.3.1 Définitions et propriétés

Soit K un corps. Soit A une K-algèbre commutative et G un groupe fini. On note $A[G]$ l'anneau qui, muni de son addition forme le A-module libre engendré par G

$$\left\{ \sum_{\sigma \in G} \alpha_\sigma \sigma ; \alpha := (\alpha_\sigma)_{\sigma \in G} \in A^G \right\},$$

et muni du produit de convolution

$$\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right)=\sum_{g,h\in G}\alpha_g\beta_h gh=\sum_{\sigma\in G}\left(\sum_{\tau\in G}\alpha_\tau\beta_{\tau^{-1}\sigma}\right)\sigma.$$

On appelle $A[G]$ l'algèbre de groupe de G sur A. Notons que $A[G]$ n'est en général pas une K-algèbre commutative, mais l'est si G est abélien.

On remarque que G s'injecte de manière canonique dans $A[G]^\times$. En particulier,

$$1_G = 1_{A[G]}.$$

De plus, A s'injecte canoniquement dans $A[G]$ via l'application $a \mapsto a1_G$.

Soit G' un groupe fini et $\chi : G \longrightarrow G'$ un morphisme de groupe, alors χ se prolonge par A-linéarité en un morphisme de A-algèbre

$$\begin{array}{rccc}\tilde{\chi}: & A[G] & \longrightarrow & A[G'] \\ & \sum_{\sigma\in G}\alpha_\sigma\sigma & \longmapsto & \sum_{\sigma\in G}\alpha_\sigma\chi(\sigma)\end{array}$$

et on désignera $\tilde{\chi}$ par χ, de manière légèrement abusive. En particulier, si $G' = A^\times$, alors χ induit un morphisme d'évaluation

$$\mathrm{ev}_\chi : A[G] \longrightarrow A$$

en voyant la somme formelle dans $A[A^\times]$ comme une somme dans A.

Similairement, soit B une K-algèbre commutative et $\varphi : A \longrightarrow B$ un morphisme de K-algèbres, alors il existe un unique morphisme de K-algèbre

$$\begin{array}{rccc}\tilde{\varphi}: & A[G] & \longrightarrow & B[G] \\ & \sum_{\sigma\in G}\alpha_\sigma\sigma & \longmapsto & \sum_{\sigma\in G}\varphi(\alpha_\sigma)\sigma\end{array}$$

prolongeant φ. On désignera $\tilde{\varphi}$ par φ, de manière légèrement abusive.

En tant que A-module, $A[G]$ est canoniquement isomorphe à A^G via l'isomorphisme de A-modules

$$\begin{array}{rccc}\mathsf{T}: & A^G & \longrightarrow & A[G] \\ & \alpha & \longmapsto & \sum_{\sigma\in G}\alpha(\sigma)\sigma\end{array}$$

Soit K un corps fini à $q = p^m$ éléments, A une K-algèbre commutative de dimension finie et G un groupe fini. On représente algorithmiquement les éléments de $A[G]$ de la manière naturelle, c'est-à-dire comme ensemble de paires $(\alpha_\sigma, \sigma)_{\sigma\in G}$.

4.3.2 Transformation de Fourier

Soient K un corps, A une K-algèbre commutative et G un groupe abélien fini. Soit

$$\mathfrak{o} = |G|$$

l'ordre du groupe G et $\mathfrak{e}$ son exposant. On suppose que K contient une racine primitive $\mathfrak{e}$-ième de l'unité, ce qui implique que $\mathfrak{e}$ et $\mathfrak{o}$ sont non nuls dans K. Soit

$$\hat{G} = \mathrm{Hom}(G, K^\times)$$

le groupe dual de G. En particulier, $\hat{G}$ est un groupe donc on peut définir comme précédemment l'algèbre $A[\hat{G}]$ et l'isomorphisme de A-modules libres $\hat{\mathsf{T}} : A^{\hat{G}} \longrightarrow A[\hat{G}]$.

On définit les morphismes de A-algèbres

$$\begin{array}{rccc} \mathrm{FT}_G : & A[G] & \longrightarrow & A^{\hat{G}} \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \left(\chi \mapsto \sum_{\sigma\in G} \alpha_\sigma \chi(\sigma)\right) \end{array}$$

et

$$\begin{array}{rccc} \mathrm{FT}_{\hat{G}} : & A[\hat{G}] & \longrightarrow & A^{G} \\ & \sum_{\chi\in \hat{G}} \alpha_\chi \chi & \longmapsto & \left(\sigma \mapsto \sum_{\chi\in \hat{G}} \alpha_\chi \chi(\sigma)\right) \end{array}$$

où A^G et $A^{\hat{G}}$ sont classiquement munis de la multiplication terme à terme. On appelle ces applications les transformations de Fourier de G et $\hat{G}$. On va voir que ces applications sont proches d'être des inverses l'une de l'autre.

Proposition 31. En reprenant les notations ci-dessus, soit

$$\iota : A[G] \longrightarrow A[G]$$

le prolongement de l'inversion dans G par linéarité, alors

$$\mathsf{T} \circ \mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G = \mathfrak{o}\iota.$$

En particulier, FT_G et $\mathrm{FT}_{\hat{G}}$ sont des isomorphismes d'algèbres.

Démonstration. Par A-linéarité, il suffit de démontrer que l'image de σ est $\mathfrak{o}\sigma^{-1}$ pour tout $\sigma \in G$. Soit $\sigma \in G$. Alors

$$\hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \sum_{\chi\in\hat{G}} \chi(\sigma)\chi,$$

et donc

$$\mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \left(\sigma' \mapsto \sum_{\chi\in\hat{G}} \chi(\sigma)\chi(\sigma')\right).$$

Soit $\sigma' \in G$, alors

$$\sum_{\chi\in\hat{G}} \chi(\sigma)\chi(\sigma') = \sum_{\chi\in\hat{G}} \chi(\sigma\sigma').$$

Soit $\mathfrak{o}_{\sigma\sigma'}$ l'ordre de $\sigma\sigma'$, et soit $\zeta_{\mathfrak{o}_{\sigma\sigma'}}$ une racine primitive $\mathfrak{o}_{\sigma\sigma'}$-ième de l'unité dans K (qui existe car K contient les racines $\mathfrak{e}$-ièmes de l'unité). On a

$$\sum_{\chi\in\hat{G}} \chi(\sigma\sigma') = \frac{\mathfrak{o}}{\mathfrak{o}_{\sigma\sigma'}} \sum_{i=1}^{\mathfrak{o}_{\sigma\sigma'}} \zeta_{\mathfrak{o}_{\sigma\sigma'}}^i \in K.$$

Cette somme vaut 0 si $\zeta_{\mathfrak{o}_{\sigma\sigma'}} \neq 1$, i.e. si $\sigma' \neq \sigma^{-1}$. On en déduit que

$$\mathsf{T} \circ \mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}} \circ \mathrm{FT}_G(\sigma) = \mathfrak{o}\sigma^{-1}.$$

□

Remarque 12. Il existe une définition alternative (mais équivalente) de la transformée de Fourier. Soit $\alpha \in K^G$, on définit la transformée de Fourier de α

$$\begin{array}{rccc} \hat{\alpha} : & \hat{G} & \longrightarrow & K \\ & \chi & \longmapsto & \frac{1}{\mathfrak{o}} \sum_{\sigma \in G} \alpha(\sigma)\chi(\sigma)^{-1} \end{array}$$

de manière à pouvoir décomposer α dans la base formée des caractères de G :

$$\alpha = \sum_{\chi \in \hat{G}} \hat{\alpha}(\chi)\chi.$$

Cette définition revient à composer FT_G avec $\frac{1}{\mathfrak{o}}\iota \circ \mathsf{T}$.

D'un point de vue algorithmique, l'application FT_G est très utile car la complexité temporelle de la multiplication dans $A^{\hat{G}}$ est linéaire. Elle peut être utilisée pour majorer la complexité temporelle de la multiplication dans $A[G]$. En utilisant cette méthode, la complexité temporelle de la multiplication dans $A[G]$ est essentiellement la complexité de l'évaluation de FT_G. Notons que le cas d'application que nous visons est celui où K est un corps fini, mais que les théorèmes 32 et 33 sont vrais pour n'importe quel corps disposant des racines de l'unité appropriées.

Cas particulier : groupes cycliques

On suppose dans ce paragraphe uniquement que G est cyclique. Soit ζ une racine $\mathfrak{o}$-ième de l'unité dans K et σ un générateur de G. Soit $\chi \in \hat{G}$ tel que $\chi(\sigma) = \zeta$. On peut alors poser les isomorphismes de K-algèbres suivants :

$$\begin{array}{ccc} A[G] & \longrightarrow & A[x]/(x^{\mathfrak{o}} - 1) \\ \sum_{i=0}^{\mathfrak{o}-1} \alpha_i \sigma^i & \longmapsto & \sum_{i=0}^{\mathfrak{o}-1} \alpha_i x^i \end{array}$$

et

$$\begin{array}{ccc} A^{\hat{G}} & \longmapsto & A^{\mathfrak{o}} \\ (\chi^i \mapsto \alpha_i) & \longmapsto & (\alpha_i)_{0 \leqslant i \leqslant \mathfrak{o}-1} \end{array}$$

La transformation de Fourier devient via ces isomorphismes d'algèbres :

$$\begin{array}{rccc} \mathrm{FT}_{\sigma,\zeta} : & A[x]/(x^{\mathfrak{o}} - 1) & \longmapsto & A^{\mathfrak{o}} \\ & f & \longmapsto & (f(\zeta^i))_{0 \leqslant i \leqslant \mathfrak{o}-1} \end{array}$$

Réaliser la transformation de Fourier d'un élément $f \in A[x]/(x^{\mathfrak{o}} - 1)$ consiste donc à effectuer une évaluation multipoints de f en $(1, \zeta, \ldots, \zeta^{\mathfrak{o}-1})$. Cette évaluation est calculable rapidement si K contient une racine primitive t-ième de l'unité pour t une puissance de 2 supérieure strictement à $3(\mathfrak{o} - 1)$, grâce à une idée de [RSR69, Blu70].

Théorème 32. *Soient K un corps, A une K-algèbre commutative et G un groupe cyclique fini d'ordre $\mathfrak{o} \geqslant 2$. On suppose que K contient une racine primitive $\mathfrak{o}$-ième de l'unité ζ et une racine primitive t-ième de l'unité pour t une puissance de 2 supérieure strictement à $3(\mathfrak{o}-1)$. Soit $\sigma \in G$ un générateur de G. Soit*

$$f = \sum_{i=0}^{\mathfrak{o}-1} f_i x^i \in A[x]/(x^{\mathfrak{o}} - 1).$$

Alors $\mathrm{FT}_{\sigma,\zeta}(f)$ peut être calculé avec $O(\mathfrak{o} \log \mathfrak{o})$ additions dans A, multiplications scalaires dans A (par un élément de K) et multiplications dans K. Plus précisément, il existe une constante $\mathcal{Q}$ absolue telle que $\mathrm{FT}_{\sigma,\zeta}(f)$ peut être calculée avec $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ de ces opérations.

Démonstration. On démontre que le calcul de $\mathrm{FT}_{\sigma,\zeta}(f)$ se réduit en temps linéaire à la multiplication d'un polynôme de $K[x]$ avec un polynôme de $A[x]$, en suivant la preuve de [BCG+17, Proposition 5.10]. On peut alors conclure en adaptant les arguments de [BCG+17, Théorème 2.8, Algorithme 2.3].

Pour tout $0 \leqslant i \leqslant 2\mathfrak{o}-2$, on pose

$$c_i = i(i-1)/2 \text{ et } \beta_i = \zeta^{c_i}.$$

Puisque $\zeta^{\mathfrak{o}} = 1$, il est suffisant de calculer les $\mathfrak{o}$ puissances de ζ ($\mathfrak{o}$ multiplications dans K) et d'utiliser $\beta_i = \zeta^{c_i \bmod \mathfrak{o}}$. On observe que pour tout $0 \leqslant i, j \leqslant \mathfrak{o}-1$

$$c_{i+j} = c_i + c_j + ij \text{ et } \beta_{i+j} = \beta_i \beta_j \zeta^{ij}.$$

On pose pour tout $0 \leqslant i \leqslant \mathfrak{o}-1$

$$h_i = \beta_i^{-1} f_i = \zeta^{-c_i \bmod \mathfrak{o}} f_i.$$

Ces coefficients peuvent être calculés en $\mathfrak{o}$ multiplications scalaires dans A, car $\zeta \in K$. On a alors pour tout $0 \leqslant i \leqslant \mathfrak{o}-1$

$$f(\zeta^i) = \sum_{j=0}^{\mathfrak{o}-1} \zeta^{ij} f_j = \beta_i^{-1} \sum_{j=0}^{\mathfrak{o}-1} \beta_{i+j} h_j.$$

L'astuce consiste à remarquer que $\sum_{j=0}^{\mathfrak{o}-1} \beta_{i+j} h_j$ est le $(\mathfrak{o}-1+i)$-ième coefficient d'un polynôme. On pose

$$h(x) = \sum_{i=0}^{\mathfrak{o}-1} h_{\mathfrak{o}-1-i} x^i \in A[x] \text{ et } b(x) = \sum_{i=0}^{2\mathfrak{o}-2} \beta_i x^i \in K[x] \tag{4.3.1}$$

et

$$r(x) = b(x)h(x) := \sum_{i=0}^{3\mathfrak{o}-3} r_i x^i \in A[x].$$

Alors pour tout $0 \leqslant i \leqslant \mathfrak{o}-1$

$$r_{\mathfrak{o}-1+i} = \sum_{j=0}^{\mathfrak{o}-1} \beta_{i+j} h_j \text{ et } f(\zeta^i) = \beta_i^{-1} r_{\mathfrak{o}-1+i}.$$

Ainsi, on a bien réduit le calcul de $\mathrm{FT}_{\sigma,\zeta}(f)$ au calcul de $r(x) = b(x)h(x)$. □

Groupe abélien quelconque

On va démontrer que le théorème 32 s'étend à tout groupe abélien fini.

Théorème 33. *Soit K un corps, A une K-algèbre commutative et G un groupe abélien fini. Soit $\mathfrak{o} \geqslant 2$ l'ordre de G et $\mathfrak{e}$ son exposant. Soit t une puissance de 2 strictement supérieure à $3(\mathfrak{e}-1)$, on suppose que K contient des racines primitives $\mathfrak{e}$-ième et t-ième de l'unité. On suppose qu'on dispose d'une décomposition explicite de G en produits de groupes cycliques*

$$G = C_1 \times \cdots \times C_I$$

d'ordres respectifs $2 \leqslant \mathfrak{o}_1 \mid \cdots \mid \mathfrak{o}_I = \mathfrak{e}$. Alors il existe un algorithme récursif évaluant

$$\mathrm{FT}_G : A[G] \longrightarrow A^{\hat{G}}$$

en $O(\mathfrak{o} \sum_{i=0}^{I} \log \mathfrak{o}_i) = O(\mathfrak{o} \log \mathfrak{o})$ additions dans A, multiplications scalaires dans A et multiplications dans K. Plus précisément, il existe une constante absolue $\mathcal{Q}$ telle que FT_G peut être évaluée avec $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ de ces opérations. La profondeur de l'arbre de récursion est un $O(I)$.

Remarque 13. En particulier, si $A = K$, alors la transformation de Fourier sur $K[G]$ nécessite $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ additions et multiplications dans K.

Démonstration. Il suffit de montrer que le théorème est vrai pour une constante absolue $\mathcal{Q}$ supérieure à celle du théorème 32. On raisonne par récurrence sur I. Le cas $I = 1$ découle simplement du théorème 32. Supposons que $I \geqslant 2$, et que le théorème est vrai pour tout groupe ayant $I-1$ facteurs invariants. On peut remarquer que $\mathrm{FT}_{C_1 \times \cdots \times C_{I-1}}$ s'étend en un isomorphisme de A-algèbres

$$A[G] = A[C_1] \ldots [C_{I-1}][C_I] \overset{\mathrm{FT}_{C_1 \times \cdots \times C_{I-1}}}{\longrightarrow} A^{\hat{C_1} \times \cdots \times \hat{C_{I-1}}}[C_I] =: A'[C_I].$$

Calculer cet isomorphisme requiert le calcul de $\mathfrak{o}_I$ transformations de Fourier $\mathrm{FT}_{C_1 \times \cdots \times C_{I-1}}$. Par hypothèse de récurrence, il existe une constante $\mathcal{Q}$ telle que calculer l'extension de $\mathrm{FT}_{C_1 \times \cdots \times C_{I-1}}$ à $A[G]$ nécessite $\mathfrak{o}_I \mathcal{Q} \frac{\mathfrak{o}}{\mathfrak{o}_I} \log(\frac{\mathfrak{o}}{\mathfrak{o}_I}) = \mathcal{Q}\mathfrak{o} \log(\frac{\mathfrak{o}}{\mathfrak{o}_I})$ opérations. Il reste alors à calculer

$$\mathrm{FT}_{C_I} : A'[C_I] \longrightarrow A'^{\hat{C_I}} = A^{\hat{C_1} \times \cdots \times \hat{C_I}} = A^{\hat{G}}$$

La somme et la multiplication scalaire dans A' peuvent être calculées avec $\frac{\mathfrak{o}}{\mathfrak{o}_I}$ sommes et multiplications scalaires dans A. D'après le théorème 32, l'évaluation de FT_{C_I} nécessite $\mathcal{Q}\mathfrak{o}_I \log \mathfrak{o}_I$ additions et multiplications scalaires dans A', soit $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}_I$ additions et multiplications scalaires dans A. Ainsi, il est possible de calculer FT_G en $\mathcal{Q}\mathfrak{o} \log(\frac{\mathfrak{o}}{\mathfrak{o}_I}) + \mathcal{Q}\mathfrak{o} \log \mathfrak{o}_I = \mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ opérations. Par récurrence, on déduit le théorème 33. □

Remarque 14. On peut donner une formulation itérative de l'algorithme du théorème 33. Pour cela, définissons

$$A_0 = A \text{ et } \forall 1 \leqslant i \leqslant I, A_i = A^{\hat{C_1} \times \cdots \times \hat{C_i}}$$

ainsi que $\forall 0 \leqslant i \leqslant I-1$,

$$\mathrm{FT}_i : (A_i[C_{i+2}] \dots [C_I])\,[C_{i+1}] \longrightarrow (A_i[C_{i+2}] \dots [C_I])^{\hat{C}_{i+1}}\,.$$

En remarquant que $\forall 0 \leqslant i \leqslant I-1$,

$$A_i[C_{i+1}] \dots [C_I] = (A_i[C_{i+2}] \dots [C_I])\,[C_{i+1}]$$

et

$$(A_i[C_{i+2}] \dots [C_I])^{\hat{C}_{i+1}} = A_{i+1}[C_{i+2}] \dots [C_I],$$

on déduit que

$$\mathrm{FT}_G = \mathrm{FT}_{I-1} \circ \dots \circ \mathrm{FT}_0\,.$$

Calculer FT_i nécessite au plus $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}_{i+1}$ additions et multiplications dans A et multiplications dans K.

4.3.3 Multiplication dans l'algèbre d'un groupe abélien fini

Soit K un corps fini à $q = p^m$ éléments et G un groupe abélien fini (non trivial). On note $\mathfrak{o}$ l'ordre de G et $\mathfrak{e}$ son exposant. Soit t une puissance de 2 strictement supérieure à $3(\mathfrak{e}-1)$. Il est clair d'après le théorème 33 que si K contient des racines primitives $\mathfrak{e}$-ième et t-ième de l'unité, il est possible d'utiliser la transformée de Fourier FT_G pour multiplier dans $K[G]$. Notons que le théorème 33 requiert qu'une décomposition explicite de G en facteurs cycliques soit connue. Cela ne pose pas problème dans la proposition 34 et le théorème 36 car une telle décomposition existe toujours, et peut être précalculée.

Proposition 34. Soit K un corps fini et G un groupe abélien fini d'ordre $\mathfrak{o} \geqslant 2$ et d'exposant $\mathfrak{e}$. Soit t une puissance de 2 strictement supérieure à $3(\mathfrak{e}-1)$. Supposons que K contient des racines primitives $\mathfrak{e}$-ième et t-ième de l'unité, alors la multiplication dans $K[G]$ nécessite $O(\mathfrak{o} \log \mathfrak{o})$ opérations dans K. Plus précisément, il existe une constante absolue $\mathcal{Q}$ telle que la multiplication dans $K[G]$ peut être calculée avec $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ additions et multiplications dans K.

Démonstration. Soient $a, b \in K[G]$. Soit $\mathcal{Q}$ la constante absolue du théorème 33. On calcule

$$\mathrm{FT}_G(ab) = \mathrm{FT}_G(a)\,\mathrm{FT}_G(b)$$

en effectuant au plus $2\mathcal{Q}\mathfrak{o} \log \mathfrak{o} + \mathfrak{o}$ opérations dans K (car la multiplication dans K^G s'effectue composante par composante). D'après la proposition 31, on peut calculer

$$\mathfrak{o}\iota(ab) = \mathsf{T} \circ \mathrm{FT}_{\hat{G}} \circ \hat{\mathsf{T}}(\mathrm{FT}_G(ab))$$

en au plus $\mathcal{Q}\mathfrak{o} \log \mathfrak{o}$ opérations dans K supplémentaires. Puisque K contient les racines primitives $\mathfrak{e}$-ièmes de l'unité, alors $\mathfrak{o}$ a un inverse $\mathfrak{o}^{-1}$ dans K. On peut donc calculer $\iota(ab) = \mathfrak{o}^{-1}\mathfrak{o}\iota(ab)$ avec une multiplication dans K supplémentaire. Enfin, ι est une involution qui fait permuter les coordonnées des éléments de $K[G]$, donc on peut retrouver ab en $O(\mathfrak{o})$ opérations dans K supplémentaires. □

On s'intéresse maintenant au cas où K ne contient pas les racines de l'unité nécessaires. Commençons par le cas particulier où $m = 1$, i.e. $K = \mathbb{Z}/p\mathbb{Z}$. Dans le pire cas, $\text{pgcd}(p, \mathfrak{o}) \neq 1$ et il est impossible de trouver une K-algèbre contenant des racines $\mathfrak{e}$-ième de l'unité.

L'astuce que nous allons employer est de réduire le calcul du produit dans $K[G]$ au calcul du produit dans $K'[G]$ où $K' = \mathbb{Z}/p'\mathbb{Z}$ est un corps fini de caractéristique $p' > p$ via des applications non-algébriques. On commence par donner des contraintes sur le choix de p'.

On définit

$$\text{lift}_p : K \longrightarrow \mathbb{Z}$$

la section (ensembliste) de la réduction modulo p à image dans $[0, p[$. L'application lift_p s'étend en une application non-algébrique

$$\begin{array}{rccc} \text{lift}_p : & K[G] & \longrightarrow & \mathbb{Z}[G] \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma\in G} \text{lift}_p(\alpha_\sigma)\sigma \end{array}.$$

On définit similairement pour $p' > p$

$$\text{lift}_{p'} : K'[G] \longrightarrow \mathbb{Z}[G].$$

On peut également définir des applications

$$\uparrow\!: \begin{array}{ccc} K & \longrightarrow & K' \\ \alpha & \longmapsto & \text{lift}_p(\alpha) \bmod p' \end{array} \quad \text{et} \quad \downarrow\!: \begin{array}{ccc} K' & \longrightarrow & K \\ \alpha' & \longmapsto & \text{lift}_{p'}(\alpha') \bmod p \end{array}.$$

En particulier, pour tout $\alpha \in K$,

$$\downarrow (\uparrow (\alpha)) = \alpha.$$

Les applications $\uparrow$ et $\downarrow$ s'étendent également en des applications

$$\uparrow\!: K[G] \longrightarrow K'[G] \text{ et } \downarrow\!: K'[G] \longrightarrow K[G].$$

On souhaite que les applications $\uparrow$ et $\downarrow$ vérifient

$$\forall a, b \in K[G], \downarrow (\uparrow (a) \cdot \uparrow (b)) = ab.$$

Soient

$$a = \sum_{\sigma\in G} \alpha_\sigma \sigma \in K[G] \text{ et } b = \sum_{\sigma\in G} \beta_\sigma \sigma \in K[G]$$

et soient

$$A = \text{lift}_p(a) \in \mathbb{Z}[G] \text{ et } B = \text{lift}_p(b) \in \mathbb{Z}[G].$$

Les coefficients de $AB \in \mathbb{Z}[G]$ sont des entiers dans $[0, \mathfrak{o}(p-1)^2]$, et $ab = AB \bmod p$. Alors

$$AB = \text{lift}_{p'}(\uparrow (a) \uparrow (b)) \Longrightarrow \downarrow (\uparrow (a) \cdot \uparrow (b)) = ab. \tag{4.3.2}$$

Le terme de gauche de l'équation (4.3.2) est vérifié pour tout $a, b \in K[G]$ si et seuleument si

$$p' > \mathfrak{o}(p-1)^2. \tag{4.3.3}$$

On souhaite également que $K' = \mathbb{Z}/p'\mathbb{Z}$ contiennent des racines primitives $\mathfrak{e}$-ième et t-ième de l'unité. Il est équivalent de demander

$$p' \equiv 1 \bmod \operatorname{ppcm}(\mathfrak{e}, t). \tag{4.3.4}$$

On choisit p' comme le plus petit premier satisfaisant les conditions (4.3.3) et (4.3.4). La question qu'il convient de se poser désormais concerne la taille de p'. Soit p'' le plus petit premier satisfaisant

$$p'' \equiv 1 \bmod (\mathfrak{o}(p-1)^2 t),$$

alors il est clair que p'' satisfait les conditions (4.3.3) et (4.3.4), donc $p' \leqslant p''$. D'après les résultats de Heath-Brown [HB92] sur la constante dans le théorème de Linnik sur les premiers dans les suites arithmétiques, il existe une constante $\mathcal{Q}$ telle que

$$p' \leqslant p'' \leqslant \mathcal{Q}(\mathfrak{o}(p-1))^{11}. \tag{4.3.5}$$

Autrement dit,

$$\log p' = O(\log(\mathfrak{o}) + \log(p)).$$

Remarque 15. Cette borne supérieure n'est clairement pas optimale. Tout d'abord, un résultat de Xylouris [Xyl11] raffine légèrement l'exposant dans l'inéquation (4.3.5). De plus, un résultat de Bach–Sorenson [BS96] démontre que, en supposant GRH, il existe $\mathcal{Q}$ telle que

$$p'' \leqslant \mathcal{Q}\left(\varphi(\mathfrak{o}^2(p-1)^2)\log(\mathfrak{o}(p-1))\right)^2$$

où φ désigne l'indicatrice d'Euler. Ensuite, on utilise l'inégalité $t \leqslant 6\mathfrak{o}$ qui est assez mauvaise lorsque le groupe G se décompose en un grand nombre de cycles. Enfin, il semble que, sur de nombreux exemples, l'inégalité $p' \leqslant p''$ est assez large également. Cependant, cette borne est suffisante pour arriver au résultat souhaité.

La proposition 34 et l'équation (4.3.5) nous permettent d'affirmer la proposition suivante :

Proposition 35. Il existe une constante absolue $\mathcal{Q}$ telle que l'énoncé suivant soit vrai. Soit K le corps fini à p éléments. Soit G un groupe abélien fini d'ordre $\mathfrak{o} \geqslant 2$ et d'exposant $\mathfrak{e}$. Soit t une puissance de 2 supérieure strictement à $3(\mathfrak{e}-1)$. Il existe un premier $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$ qui satisfait les conditions (4.3.3) et (4.3.4). Alors, la multiplication dans $K[G]$ peut être calculée en $\mathcal{Q}\mathfrak{o}\log\mathfrak{o}$ opérations. On entend par opération une addition ou une multiplication dans $K' = \mathbb{Z}/p'\mathbb{Z}$, ou une évaluation de $\uparrow$ ou de $\downarrow$.

Il reste à traiter le cas où $m > 1$, i.e. K n'est pas un corps premier. Nos hypothèses sur la représentation algorithmique des corps finis dans le chapitre 2 permettent de voir K comme un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimension m, et d'identifier les éléments de K à leurs coordonnées dans une $\mathbb{Z}/p\mathbb{Z}$-base de K. On peut donc utiliser l'algorithme de multiplications dans les corps finis de Chudnovsky–Chudnovsky [CC88], qui permet de généraliser l'approche précédente. Les travaux de Chudnovsky–Chudnovsky [CC88], Shparlinski–Tsfasman–Vladut [STV92], Shokrollahi [Sho92], Ballet–Rolland [BR04], Chaumine [Cha08], Randriambololona [Ran12] et d'autres, démontrent qu'il existe une constante

absolue $\mathcal{Q}$, un entier $r \leqslant \mathcal{Q}m$, des formes $\mathbb{Z}/p\mathbb{Z}$-linéaires $\phi_1, \dots, \phi_r$ et $\psi_1, \dots, \psi_r$ sur K, et $w_1, \dots, w_r \in K$ tels que

$$\forall x, y \in K,\ xy = \sum_{i=1}^{r} \phi_i(x)\psi_i(y)w_i.$$

Pour $1 \leqslant i \leqslant r$, on peut étendre les formes linéaires aux algèbres de groupes

$$\begin{array}{rccc} \tilde{\phi}_i : & K[G] & \longrightarrow & \mathbb{Z}/p\mathbb{Z}[G] \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma\in G} \phi_i(\alpha_\sigma)\sigma \end{array}$$

$$\begin{array}{rccc} \tilde{\psi}_i : & K[G] & \longrightarrow & \mathbb{Z}/p\mathbb{Z}[G] \\ & \sum_{\sigma\in G} \alpha_\sigma \sigma & \longmapsto & \sum_{\sigma\in G} \psi_i(\alpha_\sigma)\sigma \end{array}$$

et remarquer que

$$\forall a, b \in K[G],\ ab = \sum_{i=1}^{r} w_i \tilde{\phi}_i(a)\tilde{\psi}_i(b)$$

de sorte que la part bilinéaire de multiplication dans $K[G]$ se réduit à r multiplications dans $\mathbb{Z}/p\mathbb{Z}[G]$. On déduit de cette formule et de la proposition 35 le théorème 36 :

Théorème 36. *Il existe une constante absolue $\mathcal{Q}$ telle que l'énoncé suivant est vrai. Soit K un corps fini à p^m éléments. Soit G un groupe abélien fini d'ordre $\mathfrak{o} \geqslant 2$. Il existe un premier $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$ qui satisfait les conditions (4.3.3) et (4.3.4). Alors une multiplication dans $K[G]$ peut être calculée en $\mathcal{Q}(m\mathfrak{o}\log\mathfrak{o} + m^2\mathfrak{o})$ opérations. On entend par opération une addition ou une multiplication dans $\mathbb{Z}/p\mathbb{Z}$ ou dans $\mathbb{Z}/p'\mathbb{Z}$, ou une évaluation de $\uparrow$ ou de $\downarrow$.*

4.4 Codes sur des algèbres de groupes finis

Dans la section 4.3, nous nous sommes principalement intéressés aux algèbres de groupes abéliens finis. Dans la section 4.5 également, nous nous intéresserons principalement au cas abélien. Par contre, le contenu de cette section vaut pour les groupes abéliens et non-abéliens de la même manière. Nous ne ferons donc pas d'hypothèse sur la commutativité des groupes finis considérés.

Pour toute cette section, on fixe G un groupe fini d'ordre $\mathfrak{o}$ et K un corps fini à $q = p^m$ éléments.

4.4.1 Quelques formes bilinéaires

On commence par fixer des notations pour les formes K-bilinéaires et $K[G]$-bilinéaires que nous allons utiliser par la suite. Soit R un anneau (unitaire, associatif) et E un ensemble fini. On note

$$\begin{array}{rccc} \langle ., . \rangle : & R^E \times R^E & \longrightarrow & R \\ & (a_i)_{i\in E}, (b_i)_{i\in E} & \longmapsto & \sum_{i\in E} a_i b_i \end{array} \tag{4.4.1}$$

la forme R-bilinéaire canonique sur R^E. Cette notation est légèrement ambiguë, car elle ne précise pas l'anneau de définition R. On fera en sorte de lever l'ambiguité dans la suite, si nécessaire.

En particulier, cela définit la forme $K[G]$-bilinéaire canonique sur $K[G]^E$

$$\langle .,. \rangle : K[G]^E \times K[G]^E \longrightarrow K[G].$$

On définit également la forme K-bilinéaire

$$\begin{array}{rccc} \langle .,. \rangle_K : & K[G]^E \times K[G]^E & \longrightarrow & K \\ & a, b & \longmapsto & 1_G^*(\langle a, b \rangle) \end{array} \tag{4.4.2}$$

qui est la composante de $\langle .,. \rangle$ associée au neutre de G. De manière générale, pour tout $\sigma \in G$, on notera $\sigma^* : K[G] \longrightarrow K$ l'application donnant la composante associée à σ des éléments de $K[G]$.

Le $K[G]$-module libre $K[G]^E$ dispose naturellement de deux actions de G (à gauche et à droite) :

$$\forall \sigma \in G, \forall a = (a_i)_{i \in E} \in K[G]^E,\ \sigma \cdot a = (\sigma a_i)_{i \in E} \text{ et } a \cdot \sigma = (a_i \sigma)_{i \in E}. \tag{4.4.3}$$

La forme $\langle .,. \rangle_K$ est compatible avec l'action de G sur $K[G]^E$ dans le sens suivant.

Proposition 37. On utilise les notations du début de la section 4.4 et de la sous-section 4.4.1. Soit $\sigma \in G$, soient $a, b \in K[G]^E$, alors

$$\langle a \cdot \sigma, b \rangle_K = \langle a, \sigma \cdot b \rangle_K.$$

Démonstration. On pose $a = (a_i)_{i \in E} \in K[G]^E$ et $b = (b_i)_{i \in E} \in K[G]^E$. Alors

$$\begin{aligned} \langle a \cdot \sigma, b \rangle_K &= 1_G^* \left(\sum_{i \in E} (a_i \sigma) b_i \right) \\ &= 1_G^* \left(\sum_{i \in E} a_i (\sigma b_i) \right) \\ &= \langle a, \sigma \cdot b \rangle_K. \end{aligned}$$

□

Proposition 38. On utilise les notations du début de la section 4.4 et de la sous-section 4.4.1. Soient $a, b \in K[G]^E$. Alors

$$\langle a, b \rangle = \sum_{\sigma \in G} \langle a, b \cdot \sigma^{-1} \rangle_K \sigma.$$

Démonstration. Soit $\sigma \in G$. On a

$$\begin{aligned} \sigma^*(\langle a, b \rangle) &= 1_G^*(\langle a, b \rangle \sigma^{-1}) \\ &= 1_G^*(\langle a, b\sigma^{-1} \rangle) \\ &= \langle a, b\sigma^{-1} \rangle_K. \end{aligned}$$

□

Remarque 16. De manière plus générale, étant donné M un $K[G]$-module à gauche, N un $K[G]$-module à droite et une application $K[G]$-bilinéaire

$$< .,. >: M \times N \longrightarrow K[G],$$

on peut lui associer une application K-bilinéaire

$$< .,. >_K : b, a \in N \times M \longmapsto 1_G^*(< a, b >)$$

compatible avec l'action de G sur M et N, et réciproquement. Dans la définition (4.4.2), on peut se permettre de ne pas renverser l'ordre des paramètres car $\langle ., . \rangle_K$ est symétrique (voir la proposition 40).

Définissons l'isomorphisme de K-espaces vectoriels

$$\begin{array}{rccc} \varphi : & K[G]^E & \longrightarrow & K^{E\times G} \\ & (\sum_{\sigma\in G} a_{i,\sigma}\sigma)_{i\in E} & \longmapsto & (a_{i,\sigma})_{(i,\sigma)\in E\times G} \end{array} \tag{4.4.4}$$

et l'isomorphisme de K-espaces vectoriels

$$\begin{array}{rccc} \iota : & K[G]^E & \longrightarrow & K[G]^E \\ & (\sum_{\sigma\in G} \alpha_{i,\sigma}\sigma)_{i\in E} & \longmapsto & (\sum_{\sigma\in G} \alpha_{i,\sigma^{-1}}\sigma)_{i\in E} \end{array} . \tag{4.4.5}$$

Remarquons que l'application ι revient à appliquer l'involution $\sigma \longmapsto \sigma^{-1}$ coordonnée par coordonnée. On notera également ι cette involution.

On peut expliciter une relation entre les formes K-bilinéaires

$$\langle ., . \rangle_K : K[G]^E \times K[G]^E \longrightarrow K$$

et

$$\langle ., . \rangle : K^{E\times G} \times K^{E\times G} \longrightarrow K$$

en utilisant les isomorphismes φ et ι.

Proposition 39. On utilise les notations du début de la section 4.4 et de la section 4.4.1. Soient $a, b \in K[G]^E$ alors

$$\langle a, b \rangle_K = \langle \varphi \circ \iota(a), \varphi(b) \rangle.$$

Démonstration. On pose $a = (a_i)_{i\in E} \in K[G]^E$ et $b = (b_i)_{i\in E} \in K[G]^E$. Pour $i \in E$, on note

$$a_i = \sum_{\sigma\in G} a_{i,\sigma}\sigma \text{ et } b_i = \sum_{\sigma\in G} b_{i,\sigma}\sigma$$

Alors

$$\begin{aligned}
\langle a, b\rangle_K &= 1_G^*\left(\sum_{i\in E} a_i b_i\right)\\
&= \sum_{i\in E} 1_G^*(a_i b_i)\\
&= \sum_{i\in E} 1_G^*\left(\sum_{\sigma\in G}\left(\sum_{\tau\in G} a_{i,\tau} b_{i,\tau^{-1}\sigma}\right)\sigma\right)\\
&= \sum_{i\in E}\sum_{\tau\in G} a_{i,\tau} b_{i,\tau^{-1}}\\
&= \sum_{i\in E}\sum_{\tau\in G} a_{i,\tau^{-1}} b_{i,\tau}\\
&= \langle \varphi\circ\iota(a), \varphi(b)\rangle.
\end{aligned}$$

□

Cette preuve démontre également la proposition suivante :

Proposition 40. On utilise les notations du début de la section 4.4 et de la section 4.4.1. Soient $a, b \in K[G]^E$. Alors

$$\langle a, b\rangle_K = \langle b, a\rangle_K$$

4.4.2 Sous-modules et codes

On reprend les notations du début de la section 4.4, des formes linéaires (4.4.1) et (4.4.2), et des isomorphismes (4.4.4) et (4.4.5). Dans cette sous-section, on montre comment définir des codes correcteurs à partir de sous-$K[G]$-modules libres de $K[G]$-modules libres de rang fini.

Définition 35. Soit $n \geqslant 0$ un entier et E un ensemble de cardinal n. Soit M un sous-$K[G]$-module à gauche (resp. à droite) libre de $K[G]^E$. On définit une structure de code correcteur sur M en définissant, pour tout $a \in M$,

$$\mathrm{wt}(a) = \mathrm{wt}(\varphi(a)) \text{ (resp. } \mathrm{wt}(\varphi\circ\iota(a))).$$

Alors la longueur de M est

$$\mathrm{len}\, M = \#(E\times G) = n\mathfrak{o}.$$

On appelle n la G-longueur de M sur K. Soit k le rang de M en tant que $K[G]$-module libre, la dimension de M en tant que K-espace vectoriel est

$$\dim M = k\mathfrak{o}.$$

Remarque 17. Si G est abélien, les codes définis dans la définition 35 sont des exemples particuliers de codes quasi-abéliens [Was77]. Si G n'est pas abélien, ce sont des exemples de codes quasi-groupes, ou quasi-G-codes [DGTT18, BW23].

4.4.3 Orthogonal et code dual

On reprend les notations du début de la section 4.4, des formes linéaires (4.4.1) et (4.4.2), et des isomorphismes (4.4.4) et (4.4.5).

Soit E un ensemble fini de cardinal n. Soit M un sous-$K[G]$-module à gauche de $K[G]^E$. On définit

$$M^\perp = \{a \in K[G]^E \mid \langle M, a\rangle = 0\} \tag{4.4.6}$$

l'orthogonal de M. La $K[G]$-bilinéarité de $\langle .,.\rangle$ permet de démontrer que $M^\perp$ est un sous-$K[G]$-module à droite de $K[G]^E$. Similairement, si M est un sous-$K[G]$-module à droite de $K[G]^E$, on définit

$$M^\perp = \{a \in K[G]^E \mid \langle a, M\rangle = 0\} \tag{4.4.7}$$

l'orthogonal de M. C'est un sous-$K[G]$-module à gauche de $K[G]^E$.

Notons que le placement de M dans les équations (4.4.6) et (4.4.7) n'est pas anodin. En effet, si G n'est pas abélien, $\langle .,.\rangle$ n'est pas symétrique. Par exemple, si E est un singleton, $\langle .,.\rangle$ désigne le produit dans $K[G]$. Soient $\sigma, \tau \in G$ deux éléments qui ne commutent pas, alors

$$\langle \sigma, \tau\rangle \neq \langle \tau, \sigma\rangle.$$

Proposition 41. On utilise les notations du début de la sous-section 4.4.3. Soit M un sous-$K[G]$-module à gauche de $K[G]^E$. Alors

$$M^\perp = \{a \in K[G]^E \mid \langle a, M\rangle_K = 0\}$$

Similairement, soit M un sous-$K[G]$-module à droite de $K[G]^E$. Alors

$$M^\perp = \{a \in K[G]^E \mid \langle M, a\rangle_K = 0\}$$

Démonstration. On prouve la proposition pour M un sous-$K[G]$-module à gauche de $K[G]^E$. Soit $a \in M^\perp$, et $b \in M$ alors

$$\begin{aligned}\langle a, b\rangle_K &= \langle b, a\rangle_K \\ &= 1_G^*(\langle b, a\rangle) \\ &= 1_G^*(0) = 0.\end{aligned}$$

Donc

$$M^\perp \subset \{a \in K[G]^E \mid \langle a, M\rangle_K = 0\}.$$

Réciproquement, soit $a \in K[G]^E$ tel que $\langle a, M\rangle_K = 0$, et soit $b \in M$. Soit $\sigma \in G$. D'après les proposition 37 et 38, on a

$$\begin{aligned}\sigma^*(\langle b, a\rangle) &= \langle b, a\sigma^{-1}\rangle_K \\ &= \langle a\sigma^{-1}, b\rangle_K \\ &= \langle a, \sigma^{-1}b\rangle_K \\ &= 0\end{aligned}$$

car $\sigma^{-1}b \in M$ puisque M est un module à gauche. Ainsi, on a montré que $\langle b, a\rangle = 0$, donc

$$\{a \in K[G]^E \mid \langle a, M\rangle_K = 0\} \subset M^\perp.$$

□

Remarque 18. Dans la continuité de la remarque 16, la proposition 41 peut être généralisée à toute application $K[G]$-bilinéaire.

Soit M un sous-$K[G]$-module libre (à gauche ou à droite) de $K[G]^E$ de rang k. D'après le théorème 79 prouvé en annexe, $M^\perp$ est également un sous-$K[G]$-module libre (à droite ou à gauche) de $K[G]^E$ de rang $n-k$. De plus, le code associé à $M^\perp$ est le code dual du code associé à M, d'après la proposition 39.

4.4.4 Matrices génératrices et matrices de contrôle

On reprend les notations du début de la section 4.4, des formes linéaires (4.4.1) et (4.4.2), des isomorphismes (4.4.4) et (4.4.5) et de l'orthogonal (4.4.6) et (4.4.7).

Soit E un ensemble de cardinal n. On va définir des matrices génératrices et des matrices de contrôle à coefficients dans $K[G]$ pour les codes associés à des sous-$K[G]$-modules libres de $K[G]^E$.

Définition 36. Avec les notations du début de la sous-section 4.4.4. Soit M un sous-$K[G]$-module à gauche libre de $K[G]^E$ de rang k. Soit F un ensemble de cardinal k, on dit que $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ est une G-matrice génératrice de M si

$$M = \{a\mathcal{E}; a \in K[G]^F\}.$$

Soit H un ensemble de cardinal $n-k$, on dit que $\mathcal{C} \in \mathcal{M}_{E,H}(K[G])$ est une G-matrice de contrôle de M si

$$M = \{a \in K[G]^E \mid a\mathcal{C} = 0\}.$$

Soit M un sous-$K[G]$-module à droite libre de $K[G]^E$ de rang k. On dit similairement que $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ est une G-matrice génératrice de M si

$$M = \{\mathcal{E}a; a \in K[G]^F\}.$$

On dit que $\mathcal{C} \in \mathcal{M}_{H,E}(K[G])$ est une G-matrice de contrôle de M si

$$M = \{b \in K[G]^E \mid \mathcal{C}b = 0\}.$$

Remarque 19. Il est correct de définir les G-matrices génératrices et les G-matrices de contrôle de cette façon car les modules sont supposés libres. Dans ce cas, leur orthogonal est libre également (voir le théorème 79).

Remarque 20. Les conventions de la définition 36 ne sont pas arbitraires. Soit M un sous-$K[G]$-module libre de $K[G]^E$ de rang k. Il existe donc $a_1, \dots, a_k \in K[G]^E$ une $K[G]$-base de M et en particulier

$$M = K[G] \cdot a_1 \oplus K[G] \cdot a_2 \oplus \cdots \oplus K[G] \cdot a_k.$$

Si G n'est pas abélien, M n'est en général pas stable par multiplication à droite. Ainsi, la matrice dont les colonnes sont les coordonnées des $(a_i)_{i\in[1..k]}$ ne peut pas être considérée comme une matrice génératrice de M. Les générateurs de M doivent être vus comme des lignes.

Soit $a \in K[G]$, alors la multiplication à droite par a induit un endomorphisme linéaire de K^G via l'isomorphisme φ, défini dans l'équation 4.4.4. On peut alors identifier a et une matrice de $\mathcal{M}_G(K)$.

Soit M un sous-$K[G]$-module à gauche libre de $K[G]^E$ de rang k. Soit F un ensemble de cardinal k. Soit $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ une G-matrice génératrice de M. On cherche à définir une matrice associée à $\mathcal{E}$ engendrant $\varphi(M)$. On peut obtenir une telle matrice en remplaçant dans $\mathcal{E}$ les coefficients dans $K[G]$ par les matrices de $\mathcal{M}_G(K)$ correspondant aux multiplications à droite par ces éléments. On obtient alors une matrice dans $\mathcal{M}_{F,E}(\mathcal{M}_G(K))$, à laquelle on associe naturellement une matrice $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$, l'unique matrice vérifiant

$$\forall a \in K[G]^F, \varphi^{-1}(\varphi(a)\mathcal{E}_K) = a\mathcal{E}.$$

Soit M un sous-$K[G]$-module à droite libre de $K[G]^E$ de rang k. Soit $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ une G-matrice génératrice de M. Dans ce cas, on cherche à définir une matrice $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ engendrant $\varphi \circ \iota(M)$. On peut la définir à partir d'une équation similaire.

Définition 37. Soit M un sous-$K[G]$-module à gauche libre de $K[G]^E$ de rang k. Soit $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ une G-matrice génératrice de M. On note $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ la matrice telle que

$$\forall a \in K[G]^F, \varphi(a)\mathcal{E}_K = \varphi(a\mathcal{E}).$$

Soit M un sous-$K[G]$-module à droite libre de $K[G]^E$ de rang k. Soit $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ une G-matrice génératrice de M. On note $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ la matrice telle que

$$\forall a \in K[G]^F, (\varphi \circ \iota)(a)\mathcal{E}_K = (\varphi \circ \iota)(\mathcal{E}a).$$

Remarque 21. Il peut paraître surprenant d'associer une matrice $\mathcal{E}_K \in \mathcal{M}_{F\times G,E\times G}(K)$ à une matrice $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$. En réalité, dans ce cas, il s'agit simplement d'une convention d'écriture car la multiplication dans K est commutative. Notre choix est justifié par les conventions usuelles sur la notation des matrices génératrices de codes linéaires et par la proposition 44, qui montre que la matrice associée à la G-matrice génératrice du dual de M est génératrice du code dual de $\varphi(M)$, où M est un sous-module à gauche libre de $K[G]^E$. Pour changer la convention, il faut utiliser l'équation

$$\forall a \in K[G]^F, \mathcal{E}_K(\varphi \circ \iota)(a) = (\varphi \circ \iota)(\mathcal{E}a).$$

Exemple 5. Soit $K = \mathbb{F}_2$ et $G = \{1, \tau, \tau^2\}$ un groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$ où $\tau^3 = 1$. Soit M le sous-module à gauche libre de $\mathbb{F}_2[G]^2$ de rang 1 engendré par $(1, \tau)$;

$$M = \mathbb{F}_2[G] \cdot (1, \tau).$$

L'orthogonal de M et un sous-module à droite libre de rang 1 de $\mathbb{F}_2[G]^2$; on en déduit

$$M^\perp = (-\tau, 1) \cdot \mathbb{F}_2[G] = (\tau, 1) \cdot \mathbb{F}_2[G].$$

Une G-matrice génératrice de M (module à gauche) est

$$\mathcal{E} = \begin{pmatrix} 1 & \tau \end{pmatrix}$$

et une G-matrice génératrice de $M^\perp$ (module à droite) est

$$\mathcal{C} = \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Cette dernière est également une G-matrice de contrôle de M.

On va calculer les matrices $\mathcal{E}_{\mathbb{F}_2}$ et $\mathcal{C}_{\mathbb{F}_2}$ associées à $\mathcal{E}$ et $\mathcal{C}$, et vérifier qu'elles engendrent $\varphi(M)$ et $\varphi \circ \iota(M^\perp)$ respectivement. Soit

$$\alpha = a + b\tau + c\tau^2 \in \mathbb{F}_2[G],$$

on identifie α au vecteur $\begin{pmatrix} a & b & c \end{pmatrix}$ via l'application φ (et l'identification $K^G \simeq K^3$). On a

$$\alpha\tau = c + a\tau + b\tau^2.$$

On en déduit que la matrice associée à la multiplication à droite par τ dans la base canonique de K^G est

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

en identifiant K^G et K^3. Ainsi la matrice génératrice de $\varphi(M)$ associée à $\mathcal{E}$ est

$$\mathcal{E}_{\mathbb{F}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

et c'est bien une matrice génératrice de $\varphi(M)$.

Puisque $M^\perp$ est un module à droite, le code linéaire qui lui est associé est $\varphi \circ \iota(M^\perp)$. Or

$$\iota(M^\perp) = \mathbb{F}_2[G] \cdot \iota((\tau, 1)) = \mathbb{F}_2[G] \cdot (\tau^2, 1) = M. \tag{4.4.8}$$

Donc $\varphi \circ \iota(M^\perp) = \varphi(M)$.

Calculons la matrice génératrice de $\varphi \circ \iota(M^\perp)$ associée à $\mathcal{C}$. Soit

$$\alpha = a + b\tau + c\tau^2 \in \mathbb{F}_2[G],$$

on identifie α au vecteur $\begin{pmatrix} a & c & b \end{pmatrix}$ via l'application $\varphi \circ \iota$ (et l'identification $K^G \simeq K^3$). On a

$$\mathcal{C}\alpha = \begin{pmatrix} \tau\alpha \\ \alpha \end{pmatrix} = \begin{pmatrix} c + a\tau + b\tau^2 \\ a + b\tau + c\tau^2 \end{pmatrix}$$

qu'on identifie au vecteur $\begin{pmatrix} c & b & a & a & c & b \end{pmatrix}$ via l'application $\varphi \circ \iota$. On en déduit

$$\mathcal{C}_{\mathbb{F}_2} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

qui engendre bien $\varphi \circ \iota(M^\perp) = \varphi(M)$. On peut également remarquer que cette matrice correspond au résultat du calcul (4.4.8) car

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

est la matrice de la multiplication (à droite) par τ^2.

Notons enfin qu'on a

$$\mathcal{E}_{\mathbb{F}_2}\mathcal{C}_{F_2}^t = 0.$$

Remarque 22. L'exemple autorise à dire que M est autodual si $M = \iota(M^\perp)$.

Proposition 42. Soit E un ensemble fini de cardinal n. Soit M un sous-$K[G]$-module à gauche libre (resp. à droite) de $K[G]^E$ de rang k. Soit $\mathcal{E}$ une G-matrice génératrice de M, alors $\mathcal{E}_K$ est une matrice génératrice de $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Démonstration. On le démontre pour les codes à droite. Soit F un ensemble de cardinal k. On suppose que $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$. Soit $c \in K^{E\times G}$, on a

$$\begin{aligned} c \in \varphi \circ \iota(M) &\Leftrightarrow \exists a \in K[G]^F, c = \varphi \circ \iota(\mathcal{E}a) \\ &\Leftrightarrow \exists a \in K[G]^F, c = \varphi \circ \iota(a)\mathcal{E}_K \\ &\Leftrightarrow \exists a \in K^{F\times G}, c = a\mathcal{E}_K. \end{aligned}$$

Donc $\mathcal{E}_K$ est génératrice de $\varphi \circ \iota(M)$. □

On se permettra de dire abusivement que $\mathcal{E}_K$ est une matrice génératrice de M.

Proposition 43. Soit E un ensemble fini de cardinal n. Soit $M \subset K[G]^E$ un sous-$K[G]$-module à gauche libre (resp. à droite) de $K[G]^E$ de rang k. Soit F un ensemble de cardinal k et soit $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ (resp. $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$) une G-matrice génératrice de M. Le module $\iota(M)$ est un code à droite (resp. à gauche).

Posons

$$\mathcal{E}' := \iota(\mathcal{E})^t,$$

où ι est appliquée à chaque coefficient. Alors $\mathcal{E}'$ est une G-matrice génératrice de $\iota(M)$, et

$$\mathcal{E}_K = \mathcal{E}'_K.$$

Démonstration. On démontre la proposition pour les codes à gauche. On rappelle que ι est une involution. Soit $a \in K[G]^F$, on a

$$\iota(\iota(a)\mathcal{E}) = \iota(\mathcal{E})^t a,$$

En effet, soit $(b_i)_{i\in F}$ une colonne de $\mathcal{E}$, posons $a = (a_i)_{i\in F}$, alors

$$\iota(\sum_{i\in F} \iota(a_i)b_i) = \sum_{i\in F} \iota(b_i)\iota(\iota(a_i)) = \sum_{i\in F} \iota(b_i)a_i,$$

car $\iota : K[G] \longrightarrow K[G]$ est un anti-isomorphisme de K-algèbres sur $K[G]$. On en déduit

$$(\varphi \circ \iota)(a)\mathcal{E}_K = \varphi(\iota(a)\mathcal{E}) = \varphi \circ \iota(\iota(\mathcal{E})^t a) = (\varphi \circ \iota)(\mathcal{E}' a).$$

□

On peut démontrer que la matrice génératrice associée à une G-matrice génératrice de $M^\perp$ engendre le dual de $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Proposition 44. Soit E un ensemble fini de cardinal n. Soit $M \subset K[G]^E$ un sous-$K[G]$-module à gauche libre (resp. à droite) de $K[G]^E$. Soit $\mathcal{C}$ une G-matrice génératrice de $M^\perp$. Alors $\mathcal{C}$ est une G-matrice de contrôle de M et ${\mathcal{C}_K}^t$ est une matrice de contrôle de $\varphi(M)$ (resp. $\varphi \circ \iota(M)$).

Démonstration. On rédige la preuve pour les sous-$K[G]$-modules à gauche. Soient k et n le rang et la G-longueur de M. Soit H un ensemble de cardinal $n-k$, soit $\mathcal{C} \in \mathcal{M}_{E,H}(K[G])$ une G-matrice génératrice de $M^\perp$, et soit $(c_j)_{j\in H}$ la $K[G]$-base de $M^\perp$ constituée des colonnes de $\mathcal{C}$. Pour tout $j \in H$, on pose

$$c_j = (c_{i,j})_{i\in E}.$$

Soit $a = (a_i)_{i\in E} \in K[G]^E$. Alors

$$\begin{aligned} a\mathcal{C} = 0 &\Leftrightarrow \forall j \in H, \sum_{i\in E} a_i c_{i,j} = 0 \\ &\Leftrightarrow \forall j \in H, \langle a, c_j \rangle = 0 \\ &\Leftrightarrow a \in (M^\perp)^\perp = M. \end{aligned}$$

Donc $\mathcal{C}$ est une G-matrice de contrôle de M.

De plus, $\mathcal{C}_K$ est une matrice génératrice de $\varphi \circ \iota(M^\perp)$. Donc d'après la proposition 39, la matrice ${\mathcal{C}_K}^t$ est une matrice de contrôle de $\varphi(M)$. □

On montre un dernier résultat de compatibilité entre les opérations matricielles sur $K[G]$ et sur K.

Proposition 45. Soit E un ensemble de cardinal n. Soit M un sous-$K[G]$-module à droite libre de $K[G]^E$ de rang k. Soit $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ une G-matrice génératrice de M. Soit $a \in K[G]^E$, on a

$$\varphi(a\mathcal{E}) = \mathcal{E}_K \varphi(a).$$

Soit M un sous-$K[G]$-module à gauche libre de $K[G]^E$ de rang k. Soit F un ensemble de cardinal k et soit $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ une G-matrice génératrice de M. Soit $a \in K[G]^E$, on a

$$(\varphi \circ \iota)(\mathcal{E}a) = \mathcal{E}_K(\varphi \circ \iota)(a).$$

Démonstration. On montre le résultat pour les sous-modules à gauche. Pour tout $b \in K^{E\times G}$ alors

$$\begin{aligned}
\langle b, \varphi \circ \iota(\mathcal{E}a)\rangle &= \langle \varphi^{-1}(b), \mathcal{E}a\rangle_K, \text{ d'après la proposition 39,}\\
&= 1_G^*(\langle \varphi^{-1}(b), \mathcal{E}a\rangle), \text{ par définition de } \langle .,.\rangle_K,\\
&= 1_G^*(\langle \varphi^{-1}(b)\mathcal{E}, a\rangle), \text{ par associativité du produit matriciel,}\\
&= \langle \varphi^{-1}(b)\mathcal{E}, a\rangle_K, \text{ par définition de } \langle .,.\rangle_K,\\
&= \langle b\mathcal{E}_K, \varphi \circ \iota(a)\rangle, \text{ d'après la proposition 39,}\\
&= \langle b, \mathcal{E}_K\varphi \circ \iota(a)\rangle, \text{par associativité du produit matriciel.}
\end{aligned}$$

□

On termine cette section en définissant des G-matrices d'interpolation, des pseudo-inverses de la G-matrice génératrice.

Proposition 46. Soit M un sous-$K[G]$-module à gauche libre de $K[G]^E$, et soit $\mathcal{E} \in \mathcal{M}_{F,E}(K[G])$ une G-matrice génératrice de M. Il existe une matrice $\mathcal{I} \in \mathcal{M}_{E,F}(K[G])$ telle que

$$\mathcal{E}\mathcal{I} = \mathrm{Id}_F\,.$$

On dit que $\mathcal{I}$ est une matrice d'interpolation de M associée à $\mathcal{E}$.

Soit M un sous-$K[G]$-module à droite libre de $K[G]^E$, et soit $\mathcal{E} \in \mathcal{M}_{E,F}(K[G])$ une G-matrice génératrice de M. Il existe une matrice $\mathcal{I} \in \mathcal{M}_{F,E}(K[G])$ telle que

$$\mathcal{I}\mathcal{E} = \mathrm{Id}_F\,.$$

On dit que $\mathcal{I}$ est une matrice d'interpolation de M associée à $\mathcal{E}$.

Démonstration. On rédige la preuve pour les codes à gauche. Soit $(m_i)_{i\in F}$ la $K[G]$-base de M associée à la matrice $\mathcal{E}$. Soit $(e_i)_{i\in E}$ la base canonique de $K[G]^E$. D'après la proposition 77, il existe un sous-module à gauche N de $K[G]^E$ tel que $K[G]^E = M \oplus N$. Alors π la projection sur M parallèlement à N est un morphisme de $K[G]$-module à gauche, et $\mathcal{I}$ est la matrice de π dans les bases $(e_i)_{i\in E}$ et $(m_i)_{i\in F}$. □

4.5 Codes géométriques sur des algèbres de groupes finis

Soit K un corps fini à $q = p^m$ éléments. Dans cette section, on étudie la structure de $K[G]$-modules de certains espaces linéaires des revêtements abéliens non-ramifiés de groupe de Galois G d'une courbe X projective lisse sur K. Lorsque G est abélien, sous certaines hypothèses, ces espaces sont des $K[G]$-modules libres. On peut alors définir des codes de Goppa structurés. On montre qu'il existe alors des algorithmes d'encodage et de décodage de ces codes exploitant la structure de $K[G]$-module. Dans certains cas, ces algorithmes sont significativement plus rapides que les algorithmes d'encodage et de décodage classiques des codes de Goppa. Enfin, on définit des familles de codes de Goppa structurés, asymptotiquement bonnes et parfois excellentes, et dont les codes sont encodables en temps quasi-linéaire en leur longueur, et décodables en temps quasi-quadratique. Dans la sous-section 4.5.4, on donne un exemple de code géométrique structuré, et on détaille le calcul d'une matrice génératrice.

4.5.1 Construction

Cette sous-section est décomposée en plusieurs étapes. D'abord, on montre comment le groupe de Galois d'un revêtement galoisien

$$\tau : Y \longrightarrow X$$

agit sur $K(Y)$ et sur $\Omega(Y/K)$. Cela induit une action sur les algèbres résiduelles en les diviseurs effectifs invariants sous l'action de G et leurs espaces duaux (pour l'application bilinéaire $\langle ., . \rangle_Y$ définie dans l'équation (4.2.3)). On étudie leur structure en tant que $K[G]$-modules lorsque τ est non-ramifié. On montre de plus que l'application $\langle ., . \rangle_Y$ est compatible avec l'action de G, au sens de la proposition 37. Ainsi, on montre que lorsque τ est non-ramifié, les codes de Goppa définis par des diviseurs de Y invariants sous l'action de G sont des $K[G]$-modules. Enfin, on donne des conditions suffisantes pour que ces codes soient des $K[G]$-modules libres lorsque τ est un revêtement abélien non-ramifié.

Actions du groupe de Galois

Dans ce paragraphe, nous n'avons pas besoin de supposer que K est un corps fini. Soit K un corps parfait. Soient X et Y deux courbes projectives lisses sur K. Soit

$$\tau : Y \longrightarrow X$$

un revêtement galoisien sur K de groupe de Galois G. On peut définir une action à droite de G sur $K(Y)$ par

$$\forall f \in K(Y), \forall \sigma \in G,\ f \cdot \sigma = f \circ \sigma. \tag{4.5.1}$$

Définition 38. Soit $\sigma \in \mathrm{Aut}(Y)$. On rappelle que $\Omega(Y/K)$ est un $K(Y)$-espace vectoriel de dimension 1. Soit dt un générateur de $\Omega(Y/K)$. Soit $\omega \in \Omega(Y/K)$ une différentielle, il existe $f \in K(Y)$ telle que $\omega = fdt$. On définit le tiré en arrière de ω par σ comme

$$\sigma^*\omega = (f \circ \sigma)d(t \circ \sigma).$$

Remarque 23. La définition du tiré en arrière ne dépend pas du choix de dt. Soit dt_2 un générateur de $\Omega(Y/K)$ en tant que $K(Y)$-espace vectoriel, il existe $g \in K(Y)$ tel que $\omega = gdt_2$. On a

$$\frac{dt_2}{dt} = \frac{f}{g}.$$

Puisque $x \mapsto x \circ \sigma$ est un morphisme de K-algèbres, on a

$$\frac{d(t_2 \circ \sigma)}{d(t \circ \sigma)} = \frac{dt_2}{dt} \circ \sigma.$$

Alors

$$\begin{aligned}
\sigma^*\omega &= (f \circ \sigma)d(t \circ \sigma) \\
&= (f \circ \sigma)\frac{d(t \circ \sigma)}{d(t_2 \circ \sigma)}d(t_2 \circ \sigma) \\
&= (f \circ \sigma)(\frac{dt}{dt_2} \circ \sigma)d(t_2 \circ \sigma) \\
&= (g \circ \sigma)d(t_2 \circ \sigma)
\end{aligned}$$

On peut ainsi définir une action de G à droite sur $\Omega(Y/K)$ par

$$\forall \omega \in \Omega(Y/K), \forall \sigma \in G,\ \omega \cdot \sigma = \sigma^*\omega$$

à laquelle on associe canoniquement à une action à gauche

$$\forall \omega \in \Omega(Y/K), \forall \sigma \in G,\ \sigma \cdot \omega = (\sigma^{-1})^*\omega. \tag{4.5.2}$$

On a la relation de compatibilité suivante :

$$\forall \omega \in \Omega(Y/K), \forall f \in K(Y), \forall \sigma \in G,\ \sigma \cdot (f\omega) = (f \cdot \sigma^{-1})(\sigma \cdot \omega). \tag{4.5.3}$$

Extensions d'algèbres résiduelles

Soit K un corps parfait. Soient X et Y deux courbes projectives lisses sur K. Soit

$$\tau : Y \longrightarrow X$$

un revêtement galoisien sur K de groupe de Galois G. On suppose désormais que τ est non-ramifié.

On veut montrer que les algèbres résiduelles en les diviseurs effectifs de Y invariants sous l'action de G sont des $K[G]$-modules libres. On commence par le cas de la fibre d'une unique place de degré 1.

Soit P une place de $K(X)$ de degré 1 totalement décomposée dans $K(Y)$. Soit Q_1 une place de $K(Y)$ au dessus de P. En particulier, $\deg Q_1 = 1$. On note

$$\forall \sigma \in G,\ Q_\sigma := \sigma(Q_1) \text{ et } Q = \sum_{\sigma \in G} Q_\sigma.$$

Le diviseur Q est la fibre de τ au-dessus de P. Notons

$$\tau^* : \mathrm{Div}(X) \longrightarrow \mathrm{Div}(Y)$$

le morphisme de groupes abéliens induit par τ, qui a une place associe la fibre de τ au-dessus de cette place. Par définition, $Q = \tau^*(P)$.

On a des isomorphismes de K-algèbres canoniques

$$\forall \sigma \in G, K_{Q_\sigma} \simeq K$$

et

$$\mathbf{R}_Q = \Gamma_Y(\mathcal{O}_Y/\mathcal{O}_Y(-Q)) \simeq \bigoplus_{\sigma \in G} K_{Q_\sigma} \simeq K^G.$$

Le groupe G agit sur $\mathbf{R}_Q$ à droite par composition. Soit $\sigma, \sigma' \in G$, soit $f \in K_{Q_\sigma}$, alors

$$f \circ \sigma' \in K_{Q_{\sigma'^{-1}\sigma}}.$$

Pour tout $f \in \mathbf{R}_Q$, on notera $f = (f_\sigma)_{\sigma \in G}$ où $f_\sigma \in K_{Q_\sigma}$.

$$\forall (f_\sigma)_{\sigma \in G} \in \mathbf{R}_Q, \forall \sigma' \in G,\ (f_\sigma)_{\sigma \in G} \cdot \sigma' = (f_{\sigma'\sigma} \cdot \sigma')_{\sigma \in G}. \tag{4.5.4}$$

Cette action confère à $\mathbf{R}_Q$ une structure de $K[G]$-module à droite libre de rang 1.

Considérons maintenant le cas d'une unique place de degré quelconque. Soit $P \in \mathrm{Irr}(X)$ une place de X et soit $Q = \tau^*(P)$. Soit Q_1 une place de Y au-dessus de P. Soit $D(Q_1/P)$ le groupe de décomposition de Q_1, les places au-dessus de P sont paramétrées par les classes à gauche de $G/D(Q_1/P)$. On définit pour tout $\sigma \in G/D(Q_1/P)$,

$$Q_\sigma = \sigma(Q_1)$$

et on a

$$D(Q_\sigma/P) = \sigma D(Q_1/P)\sigma^{-1}$$

En particulier

$$Q = \sum_{\sigma \in G/D(Q_1/P)} Q_\sigma.$$

On a donc un isomorphisme naturel

$$\mathbf{R}_Q \simeq \bigoplus_{\sigma \in G/D(Q_1/P)} K_{Q_\sigma}.$$

Soit $\sigma \in D(Q_1/P)$ et soit $f \in K_{Q_\sigma}$, alors, puisque τ est non-ramifié, $D(Q_\sigma/P)$ est isomorphe au groupe de Galois de l'extension K_{Q_σ}/K_P. De plus, pour toute σ' classe à droite de $D(Q_\sigma/P)$
G, on a

$$f \circ \sigma' \in K_{Q_{\sigma'^{-1}\sigma}}.$$

On peut donc définir une action à droite sur $\mathbf{R}_Q$ de manière similaire à l'équation (4.5.4). Soit θ un élément normal de l'extension K_{Q_1}/K_P, alors l'orbite de θ pour l'action de G forme une base de $\mathbf{R}_Q$ comme K_P-espace vectoriel. En effet, puisque θ est normal dans K_{Q_1}/K_P,

$$\theta \cdot D(Q_1/P) \text{ est une base de } K_{Q_1}.$$

Soit $\sigma \in G$ représentant la classe à droite $D(Q_1/P)\sigma$, alors $\theta \cdot \sigma$ est normal dans l'extension $K_{Q_{\sigma^{-1}}}/K_P$ et

$$\theta \cdot D(Q_1/P) \cdot \sigma = \theta \cdot \sigma \cdot D(Q_{\sigma^{-1}}/P) \text{ est une base de } K_{Q_{\sigma^{-1}}}.$$

Donc $\theta \cdot G$ est une base de $\mathbf{R}_Q$ en tant que K_P-espace vectoriel. Donc $\mathbf{R}_Q$ est un $K[G]$-module à droite libre de rang $\deg P$.

Considérons maintenant le cas d'une place présente avec multiplicité positive. Soit $n > 0$ un entier, soit $P \in \mathrm{Irr}(X)$. Soit $Q = \tau^*(P)$. Soit t une uniformisante en P, alors $t \circ \tau$ est une uniformisante en toute les places au-dessus de P, qu'on notera t par la suite. Notons

$$\mathbf{R}_{nQ} := \Gamma_Y(\mathcal{O}_Y/\mathcal{O}_Y(-nQ)),$$

alors t induit un isomorphisme de K-espaces vectoriels

$$\mathbf{R}_{nQ} \simeq \mathbf{R}_Q[x]/(x^n) \tag{4.5.5}$$

via $t \longmapsto x$. Le groupe G agit à droite sur $\mathbf{R}_Q[x]/(x^n)$ via l'action sur les coefficients. Ainsi, puisque $t \circ \sigma = t$ pour tout $\sigma \in G$, l'ismorphisme (4.5.5) est un isomorphisme de $K[G]$-modules à droites. Enfin, on a

$$\mathbf{R}_Q[x]/(x^n) \simeq \mathbf{R}_Q^n.$$

Donc $\mathbf{R}_{nQ}$ est un $K[G]$-module à droite libre de rang $n \deg P$.

On en déduit la proposition suivante :

Proposition 47. Soient X et Y deux courbes projectives lisses sur K un corps parfait. Soit

$$\tau : Y \longrightarrow X$$

un revêtement galoisien non-ramifié de groupe de Galois G. Soit $P \in \mathrm{Div}(X)$ un diviseur effectif et soit $Q = \tau^*(P)$. Alors $\mathbf{R}_Q$ est un $K[G]$-module à droite libre de rang $\deg P$.

Dualité

Soit K un corps parfait. Soient X et Y deux courbes projectives lisses sur K. Soit

$$\tau : Y \longrightarrow X$$

un revêtement galoisien non-ramifié sur K de groupe de Galois G. Soient $P_1, \ldots, P_n \in X(K)$ des points K-rationnels distincts de X totalement décomposés dans Y. Soit

$$P = P_1 + \cdots + P_n \text{ et } Q = \tau^*(P).$$

Soit $i \in [1..n]$, et soit $Q_{i,1}$ un point K-rationnel de Y au-dessus de P_i. Soit $\sigma \in G$, on pose

$$Q_{i,\sigma} = \sigma(Q_{i,1}).$$

On a

$$Q = \sum_{i=1}^{n} \sum_{\sigma \in G} Q_{i,\sigma}.$$

Le dual de $\mathbf{R}_Q$ en tant que K-espace vectoriel est

$$\Omega_Q = \Gamma_Y(\Omega_{Y/K}(-Q)/\Omega_{Y/K}) \simeq \bigoplus_{i=1}^{n} \bigoplus_{\sigma \in G} \Gamma_Y(\Omega_{Y/K}(-Q_{i,\sigma})/\Omega_{Y/K})$$

via la forme K-bilinéaire

$$\begin{array}{rccc} \langle ., . \rangle_Y : & \mathbf{R}_Q \times \Omega_Q & \longrightarrow & K \\ & (f, \omega) & \longmapsto & \sum_{i=1}^{n} \sum_{\sigma \in G} \mathrm{Res}_{Q_{i,\sigma}}(f\omega) \end{array}$$

Tout d'abord, on remarque que l'action de G à gauche sur $\Omega(Y/K)$ induit une action à gauche sur Ω_Q par permutation des germes. Soit $\omega = (\omega_{i,\sigma})_{i,\sigma \in [1..n] \times G} \in \Omega_Q$. Soit $\sigma' \in G$, pour tous $1 \leqslant i \leqslant n$ et pour tout $\sigma \in G$ on a

$$(\sigma' \cdot \omega)_{i,\sigma} = (\sigma'^{-1})^* \omega_{i,\sigma'^{-1}\sigma}. \tag{4.5.6}$$

Cette action définit une structure de $K[G]$-module à gauche libre de rang n sur Ω_Q. De plus, les équations (4.5.3) et (4.5.4) et (4.5.6) montrent que la forme K-bilinéaire $\langle ., . \rangle_Y$ vérifie la relation de compatibilité de la proposition 37 :

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \forall \sigma \in G, \ \langle f \cdot \sigma, \omega \rangle_Y = \langle f, \sigma \cdot \omega \rangle.$$

On peut donc définir une application $K[G]$-bilinéaire en suivant la proposition 38 :

$$\begin{array}{rccc} \langle ., . \rangle_G : & \Omega_Q \times \mathbf{R}_Q & \longrightarrow & K[G] \\ & (\omega, f) & \longmapsto & \sum_{\sigma \in G} \langle f \cdot \sigma^{-1}, \omega \rangle_Y \sigma \end{array}.$$

L'application $\langle ., . \rangle_G$ permet d'identifier Ω_Q au dual de $\mathbf{R}_Q$ en tant que $K[G]$-module.

Morphismes et codes

On reprend les notations du début du paragraphe 4.5.1. On suppose que K est un corps fini à $q = p^m$ éléments. Soit $E \in \mathrm{Div}(Y)$ un diviseur G-invariant disjoint de Q, il existe $D \in \mathrm{Div}(X)$ tel que

$$\tau^*(D) = E$$

car le revêtement τ est non-ramifié. Soit

$$\mathcal{L}(E) := \Gamma_Y(\mathcal{O}_Y(E))$$

l'espace de Riemann–Roch associé à E. L'action de G à droite sur $K(Y)$ définie dans l'équation (4.5.1) induit une structure de $K[G]$-module à droite sur $\mathcal{L}(E)$. En effet, soit $f \in K(Y)$, on a pour tout $\sigma \in G$

$$(f \cdot \sigma) = \sigma^{-1} \cdot (f). \tag{4.5.7}$$

Les équations (4.5.1) et (4.5.4) indiquent que le morphisme canonique d'évaluation introduit dans la section 4.2

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E) \longrightarrow \mathbf{R}_Q$$

est un morphisme de $K[G]$-modules à droite.

De même, soit

$$\Omega(E - Q) = \Gamma_Y(\Omega_{Y/K}(E - Q)).$$

L'action de G à gauche sur $\Omega(Y/K)$ définie dans l'équation (4.5.2) induit une structure de $K[G]$-module à gauche sur $\Omega(E - Q)$. En effet, soit $\omega \in \Omega(Y/K)$, alors pour tout $\sigma \in G$,

$$\mathrm{div}(\sigma \cdot \omega) = \sigma \cdot \mathrm{div}\, \omega. \tag{4.5.8}$$

Les équations (4.5.2) et (4.5.6) indiquent que le morphisme canonique

$$\mathrm{res}_{E,Q} : \Omega(E - Q) \longrightarrow \Omega_Q$$

est un morphisme de $K[G]$-module à gauche.

Soit g_Y le genre de Y. Supposons que

$$2g_Y - 2 < \deg E < \deg Q,$$

de sorte que $\mathrm{ev}_{E,Q}$ et $\mathrm{res}_{E,Q}$ soient injectifs. On voit alors $\mathcal{L}(E)$ comme un sous-module à droite de $\mathbf{R}_Q$ et $\Omega(E - Q)$ comme un sous-module à gauche de Ω_Q. On a vu que Ω_Q est isomorphe au dual de $\mathbf{R}_Q$ via l'application $\langle ., . \rangle_G$. L'orthogonal de $\mathcal{L}(E)$ pour l'application $\langle ., . \rangle_G$ est l'orthogonal de $\mathcal{L}(E)$ pour la forme $\langle ., . \rangle_Y$, i.e. l'espace de différentielles $\Omega(E - Q)$.

Nous désignerons $K[G]^{\mathrm{supp}\, P}$ par $K[G]^P$. Définissons des morphismes de $K[G]$-modules à droite et à gauche respectivement

$$\begin{array}{rccc} \psi : & \mathbf{R}_Q & \longrightarrow & K[G]^P \\ & f & \longmapsto & (\sum_{\sigma \in G} f(Q_{i,\sigma^{-1}})\sigma)_{P_i \in P} \end{array},$$

et

$$\chi : \begin{array}{ccc} \Omega_Q & \longrightarrow & K[G]^P \\ \omega & \longmapsto & (\sum_{\sigma\in G} \mathrm{Res}_{Q_{i,\sigma}}(\omega)\sigma)_{P_i\in P} \end{array}.$$

On a

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \langle \omega, f\rangle_G = \langle \chi(\omega), \psi(f)\rangle$$

où $\langle ., .\rangle$ est la forme $K[G]$-bilinéaire définie en (4.4.1), et donc

$$\forall f \in \mathbf{R}_Q, \forall \omega \in \Omega_Q, \langle f, \omega\rangle_Y = \langle \psi(f), \chi(\omega)\rangle_K.$$

On définit

$$\mathrm{Gop}^G(Q, E) = \psi(\mathcal{L}(E))$$

et

$$\mathrm{Gop}^G_\Omega(Q, E) = \chi(\Omega(E - Q)).$$

Si $\mathcal{L}(E)$ (ou de manière équivalent $\Omega(E-Q)$) est un $K[G]$-module libre, alors $\mathrm{Gop}^G(Q, E)$ et $\mathrm{Gop}^G_\Omega(Q, E)$ le sont aussi, et on peut appliquer les résultats de la section 4.4. Dans le paragraphe 4.5.1, on donne des conditions suffisantes sur E pour que $\mathcal{L}(E)$ soit libre lorsque G est abélien.

Remarque 24. Les isomorphismes ψ et χ ne sont pas canoniques car ils dépendent du choix des $(Q_{i,1})_{i\in n}$. Cela a peu d'incidence sur les codes $\mathrm{Gop}^G(Q, E)$ et $\mathrm{Gop}^G_\Omega(Q, E)$ car changer le choix de $Q_{i,1}$ revient à multiplier la i-ème composante des éléments de $\mathrm{Gop}^G(Q, E)$ et $\mathrm{Gop}^G_\Omega(Q, E)$ par un élément de G, ce qui ne change pas le poids des mots du code.

Remarque 25. Dans le cas où E et Q ne sont pas disjoints, on peut malgré tout définir des $K[G]$-codes $\mathrm{Gop}^G(Q, E)$ et $\mathrm{Gop}^G_\Omega(Q, E)$ en procédant comme dans la remarque 11 avec une précaution : les uniformisantes choisies doivent être permutées par l'action de G à droite. Une solution simple est de prendre des uniformisantes en les $(P_i)_{1\leqslant i\leqslant n}$ et d'utiliser les uniformisantes induites sur les fibres.

Liberté de modules de fonctions

On se restreint au cas abélien. Soit K un corps fini à $q = p^m$ éléments. Soient X et Y deux courbes projectives lisses sur K. Soit

$$\tau : Y \longrightarrow X$$

un revêtement abélien non-ramifié sur K de groupe de Galois G. Soit g_X le genre de X, g_Y le genre de Y, et $\mathfrak{o}$ l'ordre de G. La formule de Riemann–Hurwitz montre que

$$g_Y - 1 = \mathfrak{o}(g_X - 1).$$

Dans ce contexte, il est possible de démontrer que sous certaines conditions peu contraignantes, $\mathcal{L}(E)$ est un $K[G]$-module libre. La stratégie principale consistera à montrer que $\mathcal{L}(E)$ est isomorphe à une algèbre résiduelle en un diviseur effectif G-invariant de Y. On commence par démontrer une proposition qui repose sur la semisimplicité de $K[G]$ lorsque p ne divise pas $\mathfrak{o}$.

Proposition 48. On utilise les notations du début du paragraphe 4.5.1. Supposons que p ne divise pas $\mathfrak{o}$. Soit $D \in \mathrm{Div}(X)$ un diviseur de degré $\deg D \geqslant g_X$. Soit $E = \tau^*(D)$, alors $\mathcal{L}(E)$ contient un $K[G]$-module à droite libre de rang $\deg D - g_X + 1$.

Démonstration. La K-algèbre $K[G]$ est semisimple d'après le théorème de Maschke [Lan02, Chapitre XVIII,Théorème 1.2]. Ainsi tout $K[G]$-module est semisimple [Lan02, Chapitre XVII, Proposition 4.1], i.e. se décompose comme somme directe de sous-modules simples. Soit $\mathcal{S}$ l'ensemble des $K[G]$-modules simples (considérés à isomorphisme près), $\mathcal{S}$ est fini puisque $K[G]$ est noethérien (et semisimple). Alors

$$\mathcal{L}(E) \simeq \bigoplus_{S \in \mathcal{S}} (\mathcal{L}(E) : S) S$$

où $(\mathcal{L}(E) : S)$ désigne la multiplicité de Jordan-Hölder de S dans $\mathcal{L}(E)$ (voir définition 51). Soit $\bar{K}$ une clôture algébrique de K. Soit $\hat{G} = \mathrm{Hom}(G, \bar{K}^*)$ le groupe dual de G. Alors tout $\bar{K}[G]$-module simple est un $\bar{K}$-espace vectoriel de dimension 1 associé à un unique caractère $\chi \in \hat{G}$ [Lan02, Chapitre XVIII,Théorème 3.1]. On note S_χ le $\bar{K}[G]$-module simple associé à $\chi \in \hat{G}$. En remarquant que, puisque la représentation régulière est somme de toutes les représentations irréductibles,

$$\bar{K}[G] = \bigoplus_{\chi \in \hat{G}} S_\chi = \bigoplus_{S \in \mathcal{S}} S \otimes_K \bar{K}$$

on déduit que pour tout $\chi \in \hat{G}$, il existe un unique $S \in \mathcal{S}$ tel que

$$(S \otimes_K \bar{K} : S_\chi) \neq 0$$

(auquel cas $(S \otimes_K \bar{K} : S_\chi) = 1$). On a

$$\mathcal{L}(E) \otimes_K \bar{K} \simeq \bigoplus_{S \in \mathcal{S}} (\mathcal{L}(E) : S) S \otimes_K \bar{K}.$$

Soit

$$\mu = \min_{\chi \in \hat{G}} \{(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi)\}.$$

Pour tout $\chi \in \hat{G}$, il existe $S \in \mathcal{S}$ tel que

$$(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi) = (\mathcal{L}(E) : S).$$

Donc

$$\mu = \min_{S \in \mathcal{S}} \{(\mathcal{L}(E) : S)\}.$$

Il est alors clair que $\mathcal{L}(E)$ contient un sous $K[G]$-module libre de rang μ. On montre que $\mu \geqslant \deg D - g_X + 1$.

Soit $\chi \in \hat{G}$. Puisque $\bar{K}(Y)$ est un $\bar{K}[G]$-module, il contient un espace propre associé à χ. Cet espace propre est non nul (voir Théorème 51 à suivre). Soit $r \in \bar{K}(Y)$ un vecteur

propre associé à χ. Cela implique que le diviseur (r) de r est G-invariant, donc il existe $R \in \mathrm{Div}(X_{\bar{K}})$ tel que $\tau^*(R) = (r)$. Soit $(\mathcal{L}(E) \otimes_K \bar{K})_\chi$ l'espace propre de $\mathcal{L}(E) \otimes_K \bar{K}$ associé à χ. Soit $f \in (\mathcal{L}(E) \otimes_K \bar{K})_\chi$, alors f/r est invariant sous l'action de G. On peut donc voir f/r comme une fonction sur $X_{\bar{K}}$. On a alors un isomorphisme de $\bar{K}$-espaces vectoriels entre $(\mathcal{L}(E) \otimes_K \bar{K})_\chi$ et $\Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D+R))$:

$$\begin{array}{ccc} (\mathcal{L}(E) \otimes_K \bar{K})_\chi & \longrightarrow & \Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D+R)) \\ f & \longmapsto & f/r \end{array}.$$

Donc d'après le théorème de Riemann–Roch,

$$\dim_{\bar{K}}((\mathcal{L}(E) \otimes_K \bar{K})_\chi) = \dim_{\bar{K}}(\Gamma_{X_{\bar{K}}}(\mathcal{O}_{\bar{K}}(D+R))) \geqslant \deg D - g_X + 1.$$

En particulier, puisque $(\mathcal{L}(E) \otimes_K \bar{K} : S_\chi) = \dim_{\bar{K}}((\mathcal{L}(E) \otimes_K \bar{K})_\chi)$, on a

$$\mu \geqslant \deg D - g_X + 1.$$

□

On démontre également une proposition permettant d'étendre les résultats de cette section sur les espaces linéaires de fonctions à des espaces linéaires de différentielles.

Proposition 49. Soit $D \in \mathrm{Div}(X)$ un diviseur, et soit C_X un diviseur canonique de X. Soit $E = \tau^*(D)$ et $C_Y = \tau^*(C_X)$, alors $\Omega(E)$ est $K[G]$-module à gauche libre si et seulement si $\mathcal{L}(C_Y - E)$ est un $K[G]$-module à droite libre.

De plus, $\Omega(E)$ contient un sous-module libre de rang $k \geqslant 0$ si et seulement si $\mathcal{L}(C_Y - E)$ contient un sous-module libre de rang k.

Démonstration. Soit $\omega_0 \in \Omega(X/K)$ une différentielle régulière de diviseur C_X, alors $\tau^*(\omega_0)$ le tiré en arrière de ω_0 par τ est une différentielle homogène sur Y de diviseur C_Y. L'application

$$\begin{array}{ccc} \Omega(E) & \longrightarrow & \mathcal{L}(C_Y - E) \\ \omega & \longmapsto & \omega/\tau^*(\omega_0) \end{array}$$

est un isomorphisme de K-espaces vectoriels compatible avec l'action de G au sens suivant :

$$\forall \sigma \in G, \forall \omega \in \Omega(E), \frac{\sigma \cdot \omega}{\tau^*(\omega_0)} = \frac{\sigma \cdot \omega}{\sigma \cdot \tau^*(\omega_0)} = \frac{\omega}{\tau^*(\omega_0)} \cdot \sigma^{-1}.$$

Puisque $\sigma \longrightarrow \sigma^{-1}$ définit un anti-isomorphisme de $K[G]$, on en déduit le résultat. □

Soit $f \in K(X)$ une fonction non nulle, alors on a une égalité de diviseurs

$$\tau^*((f)) = (f \circ \tau).$$

Ainsi, τ^* induit un morphisme de groupes de $\mathrm{Pic}(X)$ dans $\mathrm{Pic}(Y)$.

Le lemme suivant permet de produire des diviseurs de Y non spéciaux de degré $g_Y - 1$ et invariants sous l'action de G.

Lemme 50. [CE23, Section 14] On utilise les notations du début du paragraphe 4.5.1. Soit $\bar{K}$ une clôture algébrique de K. Posons

$$\mathfrak{o} = \mathfrak{o}_p \times \mathfrak{o}_{p'}$$

où $\mathfrak{o}_p$ est la plus grande puissance de p divisant $\mathfrak{o}$. Soit $c \in \mathrm{Pic}^{g_X-1}(X_{\bar{K}})$, et soit $\tau^*(c) \in \mathrm{Pic}^{g_Y-1}(Y_{\bar{K}})$ son tiré en arrière par τ. Alors $\tau^*(c)$ est spéciale si et seulement si c est somme d'une classe spéciale et d'une classe dans l'intersection des noyaux de τ^* et de la multiplication par $\mathfrak{o}_{p'}$.

Démonstration. Soit D un diviseur représentant la classe c. Soit $E = \tau^*(D)$, c'est un diviseur de la classe $\tau^*(c)$. Notons

$$\mathcal{L}(E)_{\bar{K}} := \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)).$$

Supposons que $\tau^*(c)$ est spéciale, alors $\mathcal{L}(E)_{\bar{K}}$ est un $\bar{K}[G]$-module non nul (car sa dimension est non-nulle par hypothèse). Rappellons que G est un sous-groupe des automorphismes de $\bar{K}$-espace vectoriel de $\mathcal{L}(E)_{\bar{K}}$. Puisque G est fini et commutatif, et que $\bar{K}$ est algébriquement clos, il existe $f \in \mathcal{L}(E)_{\bar{K}}$ un vecteur propre commun aux éléments de G. Donc il existe un diviseur effectif $J \in \mathrm{Div}(Y_{\bar{K}})$ tel que

$$(f) = J - E.$$

Puisque f est un vecteur propre de l'action de G, son diviseur (f) est stable par l'action de G, donc J l'est également. Donc il existe $I \in \mathrm{Div}(X_{\bar{K}})$ un diviseur effectif tel que

$$\tau^*(I - D) = J - E = (f).$$

Soit c' la classe de $D - I$, on en déduit $\tau^*(c') = 0$. Soit c'' la classe de I, alors c'' est spéciale car I est effectif, donc

$$\dim_{\bar{K}} \mathcal{L}(I)_{\bar{K}} > 0.$$

On a $c = c' + c''$. Il reste à démontrer que $\mathfrak{o}_{p'}c' = 0$. D'abord, remarquons que $f^{\mathfrak{o}_{p'}}$ est stable par G. Soit $\sigma \in G$. Puisque $\bar{K}$ est de caractéristique p, toute racine $\mathfrak{o}$-ième de l'unité est une racine $\mathfrak{o}_{p'}$-ième de l'unité. Il existe donc une racine $\mathfrak{o}_{p'}$-ième de l'unité ζ telle que

$$f^{\mathfrak{o}_{p'}} \cdot \sigma = (f \cdot \sigma)^{\mathfrak{o}_{p'}} = (\zeta f)^{\mathfrak{o}_{p'}} = f^{\mathfrak{o}_{p'}}.$$

La fonction $f^{\mathfrak{o}_{p'}}$ est G-invariante, donc il existe $g \in \bar{K}(X)$ tel que $f^{\mathfrak{o}_{p'}} = g \circ \tau$. On a $\mathfrak{o}_{p'}(D - I) = -(g)$, donc $\mathfrak{o}_{p'}c' = 0$.

La réciproque est directe. □

Théorème 51. *On utilise les notations du début du paragraphe 4.5.1. Soit $E \in \mathrm{Div}(Y)$ un diviseur invariant sous l'action de G. Supposons que*

$$\deg E > 2g_Y - 2.$$

Alors $\mathcal{L}(E)$ est un $K[G]$-module libre.

Démonstration. La preuve est triviale si $g_X = 0$ car dans ce cas G est trivial. On suppose $g_X \geqslant 1$. Soit $D \in \mathrm{Div}(X)$ un diviseur tel que $\tau^*(D) = E$ (qui existe car τ est non ramifié). Alors $\deg D > 2g_X - 2$. Soit $\bar{K}$ un clôture algébrique de K. D'après le théorème de Noether-Deuring [CR62, Théorème 29.7], il suffit de démontrer que

$$\mathcal{L}(E)_{\bar{K}} := \mathcal{L}(E) \otimes_K \bar{K} \simeq \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E))$$

est un $\bar{K}[G]$-module libre.

Soit

$$k = \deg D - g_X + 1$$

la dimension de $\mathcal{L}(D)$ (d'après le théorème de Riemann–Roch). $\mathrm{Pic}^{g_X-1}(X_{\bar{K}})$ est une variété sur $\bar{K}$ de même dimension que la jacobienne $\mathcal{J}_{X_{\bar{K}}}$, donc de dimension g_X. Pour toute classe $c \in \mathrm{Pic}^{g_X-1}(X_{\bar{K}})$, il existe

$$P_1, \ldots, P_k \in X(\bar{K})$$

tels que le diviseur $D - P_1 - \cdots - P_k$ est dans la classe c (car $k \geqslant g_X$). D'autre part, l'ensemble des classes spéciales de degré $g_X - 1$ est une sous-variété de $\mathrm{Pic}^{g_X-1}(X_{\bar{K}})$ de dimension $g_X - 1$. De plus, le noyau $\ker(\tau^*)$ du morphisme de groupe τ^* est fini (car il est inclus dans le noyau de la multiplication par $\mathfrak{o}$). Ainsi, par dimension et puisque $\bar{K}$ est algébriquement clos, il existe des places $P_1, \ldots, P_k \in X(\bar{K})$ tels que la classe de $D - P_1 - \cdots - P_k$ n'est pas somme d'une classe spéciale et d'une classe de $\ker(\tau^*)$.

Soit $P = P_1 + \cdots + P_k$ et $Q = \tau^*(P)$. D'après le lemme 50, le diviseur $E - Q$ est un diviseur de degré $g_Y - 1$ non spécial. Alors le morphisme d'évaluation

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E)_{\bar{K}} \longrightarrow \Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)/\mathcal{O}_{Y_{\bar{K}}}(E - Q))$$

est un isomorphisme de $\bar{K}[G]$-modules. Puisque $\Gamma_{Y_{\bar{K}}}(\mathcal{O}_{Y_{\bar{K}}}(E)/\mathcal{O}_{Y_{\bar{K}}}(E - Q))$ est isomorphe à $\mathbf{R}_Q \otimes_K \bar{K}$ en tant que $\bar{K}[G]$-module, alors, d'après la proposition 47, le $\bar{K}[G]$-module $\mathcal{L}(E)_{\bar{K}}$ est libre. □

Proposition 52. On utilise les notations du début du paragraphe 4.5.1. Supposons que K est un corps fini à au moins quatre éléments, que $g_X \geqslant 2$ et que $\mathfrak{o}$ est une puissance de p. Soit $d \geqslant g_X$ un entier tel qu'il existe un diviseur effectif de X de degré $d - g_X + 1$. Alors il existe $E \in \mathrm{Div}(Y)$ un diviseur invariant sous l'action de G de degré $d\mathfrak{o}$ tel que $\mathcal{L}(E)$ est un $K[G]$-module libre de rang $d - g_X + 1$.

Démonstration. Soit $P \in \mathrm{Div}(X)$ un diviseur effectif de degré $d - g_X + 1$. D'après un théorème de Ballet et Le Brigand [BLB06, Théorème 11], il existe un diviseur I de X non spécial de degré $g_X - 1$. Soit $D = I + P$. Soient $E = \tau^*(D)$, $J = \tau^*(I)$ et $Q = \tau^*(P)$. Le lemme 50 permet d'affirmer que J est un diviseur non spécial (notons que $\mathfrak{o}_{p'} = 1$). Ainsi le morphisme d'évaluation

$$\mathrm{ev}_{E,Q} : \mathcal{L}(E) \longrightarrow \Gamma_Y(\mathcal{O}_Y(E)/\mathcal{O}_Y(E - Q)) \simeq \mathbf{R}_Q$$

est un isomorphisme de $K[G]$-modules. Alors la proposition 47 démontre que $\mathcal{L}(E)$ est libre. □

4.5.2 Encodage et décodage dans le cas abélien

Dans cette sous-section, on étudie les coûts de l'encodage et du décodage des codes construits avec des revêtements abéliens non-ramifiés.

Soient K un corps fini à $q = p^m$ éléments. Soient X et Y deux courbes projectives lisses sur K et

$$\tau : Y \longrightarrow X$$

un revêtement abélien non-ramifié de groupe de Galois G. Soit $\mathfrak{o}$ l'ordre de G, g_X le genre de X et g_Y le genre de Y. D'après la formule de Riemann–Hurwitz, on a

$$g_Y - 1 = \mathfrak{o}(g_X - 1).$$

Soient $P_1, \ldots, P_n$ des points K-rationnels de X totalement décomposés dans Y, soit

$$P = \sum_{i=1}^{n} P_i$$

et soit

$$Q = \tau^*(P).$$

Soit D un diviseur disjoint de P de X tel que

$$2g_X - 1 \leqslant \deg D \leqslant n - 1.$$

Soit

$$E = \tau^*(D).$$

Soit

$$k = \deg D - g_X + 1.$$

D'après le théorème 51, les $K[G]$-modules $\mathrm{Gop}^G(Q, E)$ et $\mathrm{Gop}^G_\Omega(Q, E)$ sont des sous-modules libres de $K[G]^P$ de rangs respectifs k et $n - k$. Notons

$$N = \mathfrak{o}n.$$

Alors, d'après la définition 35, $\mathrm{Gop}^G(Q, E)$ définit un code linéaire sur K de longueur N et de dimension $\mathfrak{o}k$. Sa distance prescrite est

$$d^*(Q, E) = N - \deg E = N - \mathfrak{o}k - g_Y + 1.$$

Soient φ et ι les isomorphismes K-linéaires définis dans les équations (4.4.4) et (4.4.5). On peut vérifier que

$$\varphi \circ \iota(\mathrm{Gop}^G(Q, E)) = \mathrm{Gop}(Q, E) \text{ et } \varphi(\mathrm{Gop}^G_\Omega(Q, E)) = \mathrm{Gop}_\Omega(Q, E).$$

D'après les résultats de la section 4.4.4, il existe

$$\mathcal{E} \in \mathcal{M}_{P,k}(K[G])$$

une G-matrice génératrice de $\mathrm{Gop}^G(Q,E)$, à laquelle on associe une matrice génératrice de $\mathrm{Gop}(Q,E)$

$$\mathcal{E}_K \in \mathcal{M}_{k\times G,P\times G}(K),$$

et il existe

$$\mathcal{C} \in \mathcal{M}_{(n-k),P}(K[G])$$

une G-matrice de contrôle de $\mathrm{Gop}^G(Q,E)$ (ou de manière équivalente, une G-matrice génératrice de $\mathrm{Gop}^G_\Omega(Q,E)$), à laquelle on associe une matrice génératrice de $\mathrm{Gop}_\Omega(Q,E)$

$$\mathcal{C}_K \in \mathcal{M}_{(n-k)\times G,P\times G}(K).$$

Encodage

On utilise les notations définies au début de la section 4.5.2. On cherche à encoder un élément $a \in K^{k\times G}$ en un élément de $\mathrm{Gop}(Q,E)$. Cela revient à calculer

$$a\mathcal{E}_K = \varphi\circ\iota\left(\mathcal{E}(\varphi\circ\iota)^{-1}(a)\right). \tag{4.5.9}$$

Dans le pire cas, les applications $\varphi\circ\iota$ et $(\varphi\circ\iota)^{-1}$ peuvent être évaluées en respectivement $n\mathfrak{o}$ et $k\mathfrak{o}$ opérations. Ainsi le coût de l'encodage de a se réduit au coût du calcul de

$$\mathcal{E}(\varphi\circ\iota)^{-1}(a).$$

Cette opération nécessite de calculer kn multiplications dans $K[G]$. D'après le théorème 36, il existe une constante absolue $\mathcal{Q}$ telle qu'une multiplication dans $K[G]$ requiert au plus

$$\mathcal{Q}(m\mathfrak{o}\log\mathfrak{o} + m^2\mathfrak{o})$$

opérations dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p'\mathbb{Z}$, où p' est un premier et $p' \leqslant \mathcal{Q}(\mathfrak{o}p)^{11}$. Alors il existe une constante absolue $\mathcal{Q}'$ telle que le calcul (4.5.9) peut être effectué avec

$$\mathcal{Q}'\cdot kn\cdot\mathfrak{o}\log\mathfrak{o}\cdot m^2\cdot(\log\mathfrak{o}+\log p)^2$$

opérations élémentaires.

Dans la construction de la section 4.5.3, il existe une constante absolue $\alpha > 0$ telle que $\alpha\sqrt[4]{q}\log\mathfrak{o} \geqslant k\log p$ et $\alpha\log\mathfrak{o} \geqslant \log p$. Alors

$$\begin{aligned}
\mathcal{Q}'\cdot nk\cdot\mathfrak{o}\log\mathfrak{o}\cdot m^2\cdot(\log\mathfrak{o}+\log p)^2 &\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot\log\mathfrak{o}\cdot(k\log\mathfrak{o}+\alpha\sqrt[4]{q}\log\mathfrak{o})\cdot(\log\mathfrak{o}+\log p)\\
&\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot\log\mathfrak{o}\cdot(\alpha\sqrt[4]{q}(\log\mathfrak{o})^2+\alpha\sqrt[4]{q}\log\mathfrak{o})\cdot(\log\mathfrak{o}+\alpha\log\mathfrak{o})\\
&\leqslant \mathcal{Q}'\cdot m^2\cdot N\cdot(\log\mathfrak{o})\cdot\alpha\sqrt[4]{q}\cdot((\log\mathfrak{o})^2+\log\mathfrak{o})\cdot(1+\alpha)\cdot\log\mathfrak{o}\\
&\leqslant \mathcal{Q}''\cdot m^2\cdot\sqrt[4]{q}\cdot N\cdot(\log\mathfrak{o})^4\\
&\leqslant \mathcal{Q}''\cdot m^2\cdot\sqrt[4]{q}\cdot N(\log N)^4
\end{aligned}$$

où $\mathcal{Q}''$ est une constante absolue. Si on considère que $q = p^m$ est fixé, alors l'encodage est quasi-linéaire en la longueur N du code.

Décodage

On utilise les notations définies au début de la section 4.5.2. Soient $f_r, f_c, f_e \in \mathbf{R}_Q$ tels que

$$f_r = f_c + f_e,\ \ f_c \in \operatorname{Im} \operatorname{ev}_{E,Q} \text{ et } \#\operatorname{supp} f_e \leqslant t^*(Q,E).$$

On note

$$Q_{\mathrm{err}} = \operatorname{supp} f_e \text{ et } t = \deg Q_{\mathrm{err}}.$$

On sait d'après la section 4.2.3 qu'étant donné f_r, il est possible de calculer f_c en $O(N^3)$ opérations dans K si

$$t \leqslant \frac{d^*(Q,E) - g_Y - 1}{2}.$$

Supposons que

$$t \leqslant \mathfrak{o}\lfloor \frac{d^*(P,D) + g_X - 1}{2} \rfloor - g_Y. \tag{4.5.10}$$

Soit $F \in \operatorname{Div}(Y)$ un diviseur de degré

$$\deg F = \mathfrak{o}\lfloor \frac{d^*(P,D) + g_X - 1}{2} \rfloor = \mathfrak{o}\lfloor \frac{n-k}{2} \rfloor$$

disjoint de Q et invariant sous l'action de G (notons que $\mathfrak{o}$ divise $\deg F$). On a alors

$$g_Y + t \leqslant \deg F \leqslant N - 1 - \deg E - t.$$

On va supposer que le $K[G]$-module à droite $\mathcal{L}(F)$ contient un sous-$K[G]$-module libre de rang $(\deg F/\mathfrak{o}) - g_X + 1$. Notons que si

$$\lfloor \frac{n-k}{2} \rfloor > 2(g_X - 1) \tag{4.5.11}$$

ou

$$\mathfrak{o} \text{ est premier à } p \tag{4.5.12}$$

ou

$$\mathfrak{o} \text{ est une puissance de } p \text{ et } q \geqslant 4 \text{ et } g_X \geqslant 2, \tag{4.5.13}$$

alors, par le théorème 51 ou la proposition 48 ou la proposition 52, $\mathcal{L}(F)$ contient bien un sous-$K[G]$-module libre de rang $(\deg F/\mathfrak{o}) - g_X + 1$. Pour simplifier les notations, quitte à restreindre $\mathcal{L}(F)$, on supposera que $\mathcal{L}(F)$ est un $K[G]$-module libre de rang $(\deg F/\mathfrak{o}) - g_X + 1$.

Puisque $g_Y + t \leqslant \deg F \leqslant N - 1 - \deg E - t$, on sait que, comme dans la section 4.2.3, les applications $\operatorname{ev}_{F,Q}$ et $\operatorname{ev}_{E+F,Q}$ sont injectives, et que $h \in \mathcal{L}(F)$ s'annule en Q_{err} si et seulement si $\operatorname{ev}_{F,Q}(h) f_r \in \operatorname{Im} \operatorname{ev}_{E+F,Q}$. Sous nos hypothèses, $\operatorname{ev}_{F,Q}$ et $\operatorname{ev}_{E+F,Q}$ sont des morphismes de $K[G]$-modules à droites injectifs. Notons

$$\mathcal{E}_F \in \mathcal{M}_{P,(\ell(F)/\mathfrak{o})}(K[G])$$

une G-matrice génératrice de $\mathcal{L}(F)$ et

$$\mathcal{E}_{F,K} \in \mathcal{M}_{(\ell(F)/\mathfrak{o})\times G, P\times G}(K)$$

la matrice associée, et

$$\mathcal{C}_{E+F} \in \mathcal{M}_{(n-\ell(E+F)/\mathfrak{o}),P}(K[G])$$

une matrice de contrôle de $\mathcal{L}(E+F)$, ainsi que

$$\mathcal{C}_{E+F,K} \in \mathcal{M}_{(n-\ell(E+F)/\mathfrak{o})\times G, P\times G}(K)$$

la matrice associée. Enfin, soit

$$\mathcal{D}_r \in \mathcal{M}_n(K)$$

la matrice diagonale correspondant à la multiplication par f_r (coordonnée par coordonnée).

Ici, la matrice $\mathcal{D}_r$ n'est en général pas associée à une matrice à coefficients dans $K[G]$, donc $\ker(\mathcal{E}_{F,K} \times \mathcal{D}_r \times {\mathcal{C}_{E+F,K}}^t)$ n'est en général pas un $K[G]$-module. Trouver un élément du noyau (à gauche) de ce produit de matrices ne se réduit pas à un problème d'algèbre linéaire sur $K[G]$. On va chercher à utiliser le théorème 53. On doit montrer qu'il est possible d'évaluer rapidement (à gauche) les matrices $\mathcal{E}_{F,K}$, $\mathcal{D}_r$ et ${\mathcal{C}_{E+F,K}}^t$.

D'après le paragraphe précédent, en utilisant l'arithmétique rapide de $K[G]$, il est possible d'évaluer la matrice $\mathcal{E}_{F,K}$ avec une constante absolue fois

$$n \cdot (\lfloor (n-k)/2 \rfloor) \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

opérations élémentaires. Ensuite, la matrice $\mathcal{D}_r$ est diagonale, donc il est possible de l'évaluer en réalisant $N = \mathfrak{o}n$ multiplications dans K. Enfin, d'après la proposition 45, le coût de la multiplication par $\mathcal{C}^t_{E+F,K}$ est le coût de la multiplication par $\mathcal{C}_{E+F}$. Ainsi, il est possible d'évaluer ${\mathcal{C}_K}^t$ avec une constante absolue fois

$$n^2 \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

opérations élémentaires. Ainsi, il existe une constante absolue $\mathcal{Q}$ telle qu'il est possible d'évaluer $\mathcal{E}_{F,K} \times \mathcal{D}_r \times {\mathcal{C}_{E+F,K}}^t$ avec

$$n^2 \cdot m^2 \cdot \mathfrak{o} \log \mathfrak{o} \cdot (\log \mathfrak{o} + \log p)^2$$

opérations élémentaires.

On va maintenant utiliser un algorithme probabiliste issu de [Wie86, KS91].

Théorème 53 (Wiedemann, Kaltofen, Saunders)**.** *Les notations de ce théorème sont indépendantes. Il existe un algorithme probabiliste (Las Vegas) prenant en entrée une matrice A de dimensions $\ell \times n$ à coefficients dans un corps K et un vecteur b de K^ℓ, et renvoyant une solution x uniformément distribuée de $Ax = b$ avec une probabilité supérieure à $1/2$, au prix de $\mathcal{Q}m \log m$ évaluations de A (en boîte noire) et $\mathcal{Q}(m \log m)^2$ opérations dans K (addition, multiplication, tirage au sort, inversion), où $\mathcal{Q}$ est une constante absolue et $m = \max(\ell, n)$.*

Corollaire 53.1. *On utilise les notations du début de la sous-section 4.5.2. On suppose que les équations (4.5.10) et (4.5.11) sont vérifiées. Il existe un algorithme probabiliste (Las Vegas) prenant en entrée $f_r \in \mathbf{R}_Q$ et les matrices $\mathcal{E}_{F,K}$, $\mathcal{E}_F$, $\mathcal{C}_{E+F,K}$ et $\mathcal{C}_{E+F}$ et renvoyant f_c avec une probabilité supérieure à $1/2$, au prix de*

$$\mathcal{Q} \cdot n^2 \cdot N^2 (\log N)^2 \cdot m^2 \cdot (\log p + \log \mathfrak{o})^2$$

opérations élémentaires, où $\mathcal{Q}$ est une constante absolue.

Remarque 26. On a expliqué comment trouver la localisation des erreurs en trouvant une solution à

$$x\mathcal{E}_{F,K} \times \mathcal{D}_r \times \mathcal{C}_{E+F,K}^t = 0.$$

Si la localisation des erreurs Q_{err} n'est pas un diviseur G-invariant, $\mathbf{R}_{Q-Q_{\text{err}}}$ n'est pas un $K[G]$-module. L'équation

$$\text{ev}_{E,Q-Q_{\text{err}}}(x) = f_c$$

n'est donc pas $K[G]$-linéaire. Ce n'est pas une difficulté car on peut utiliser la même astuce : l'application $\text{ev}_{E,Q-Q_{\text{err}}}$ peut être évaluée rapidement en restreignant l'application $\text{ev}_{E,Q}$. En appliquant le théorème 53, on montre qu'on peut résoudre cette équation en

$$\mathcal{Q}' \cdot n \cdot N^2 (\log N)^2 \cdot m^2 \cdot (\log p + \log \mathfrak{o})^2$$

opérations élémentaires, pour $\mathcal{Q}'$ une constante absolue.

Dans la construction de la section 4.5.3, il existe une constante absolue $\alpha > 0$ telle que

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant k \log p$$

et

$$\alpha \log \mathfrak{o} \geqslant \log p$$

et

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant n.$$

Alors il existe une constante absolue $\mathcal{Q}''$ telle que l'algorithme de décodage peut être réalisé avec

$$\mathcal{Q}'' \cdot m^2 \cdot \sqrt[4]{q} \cdot N^2 (\log N)^5$$

opérations élémentaires. En particulier, si on considère que $q = p^m$ est fixé, alors le décodage est quasi-quadratique en la longueur N du code.

4.5.3 Familles de codes géométriques structurés

Dans ce paragraphe, on construit une famille de codes de Goppa associés à des diviseurs invariants sous l'action de groupes de Galois asymptotiquement bonne (i.e. les liminf des rendements et des distances relatives sont non nulles), et dont les algorithmes d'encodage et de décodage ont des complexités temporelles quasi-linéaires et quasi-quadratiques respectivement.

La construction de cette famille repose sur l'existence d'une famille de revêtements abéliens non ramifiés

$$\tau_i : Y_i \longrightarrow X_i$$

de courbes projectives lisses sur un corps fini K à q éléments, dont le degré $\deg \tau_i$ croît exponentiellement en le genre g_{X_i} de X_i, et dont le nombre de points K-rationnels de X_i totalement décomposés dans Y_i croît linéairement en le genre de X_i. D'après la section 3.3, en particulier le théorème 14, tout revêtement abélien non ramifié de X_i totalement décomposé au-dessus d'un point $P_\infty \in X_i(K)$ est le tiré en arrière d'un facteur de l'isogénie

$$\Phi = F_{\mathcal{J}_{X_i}} - 1.$$

Plus précisément, à tout sous-groupe H de $\mathcal{J}_{X_i}(K)$, on peut associer

$$\tau_{i,H} : Y_{i,H} \longrightarrow X_i$$

un revêtement abélien non-ramifié totalement décomposé au-dessus de P_∞ de groupe de Galois $\mathcal{J}_{X_i}(K)/H$. Soit P un point K-rationnel de X_i, alors d'après la proposition 15, le point P est totalement décomposé dans $Y_{i,H}$ si et seulement si $P - P_\infty \in H$.

Le succès de la construction dépend essentiellement de la capacité à trouver des sous-groupes de $\mathcal{J}_{X_i}(K)$ adaptés à nos besoins, pour des courbes X_i ayant un grand nombre de points rationnels. Un grand nombre de travaux traitent de problèmes similaires. Par exemple, si q est un carré, on peut trouver dans [Iha81], [TVZ82] et [GS95] des familles de courbes sur K pour lesquels le ratio

$$\#X_i(K)/g_{X_i}$$

converge vers $\sqrt{q} - 1$. On peut également trouver dans [Ser20] des techniques géométriques pour construire des courbes disposant de beaucoup de points, intéressantes pour notre problème. Nous utiliserons une autre technique, utilisée dans [GX22, NX98, Que89, vdG09], qui requiert que K contienne un sous-corps strict κ, que les courbes X_i soient définies sur κ et possèdent un point κ-rationnel.

On explicite maintenant notre construction. Soit $m > 0$ un entier. Soit κ un corps fini à p^{2m} éléments et K une extension de κ de degré 2, donc un corps fini à $q = p^{4m}$ éléments. Puisque p^{2m} est un carré, il existe une famille $(X_i)_{i\in\mathbb{N}}$ de courbes projectives lisses sur κ de genres $(g_{X_i})_{i\in\mathbb{N}}$, telle que

$$\lim_{i\to\infty} \#X_i(\kappa)/g_{X_i} = p^m - 1.$$

Pour simplifier les notations, on négligera dans la suite de préciser l'indice $i \in \mathbb{N}$. Soit

$$n = \#X(\kappa) > 0.$$

Soient $P_1, \ldots, P_n$ les points κ-rationnels de X. On identifie naturellement à X une courbe X_K lisse projective sur K, et les $(P_j)_{j\in[1..n]}$ aux n points de X_K stables sous l'action de $\mathbf{Gal}(K/\kappa)$ sur X_K. Notons

$$P = \sum_{j=1}^{n} P_j.$$

Soit

$$H = \mathcal{J}_X(\kappa)$$

le groupe des points κ-rationnels de $\mathcal{J}_X(K)$, i.e. les points de $\mathcal{J}_X(K)$ stables sous l'action de $\mathbf{Gal}(K/\kappa)$. Soit $\tilde{Y}$ une courbe projective lisse sur K telle qu'il existe

$$\tilde{\tau} : \tilde{Y} \longrightarrow X$$

un revêtement abélien non ramifié totalement décomposé au-dessus de P_1 de groupe de Galois

$$\tilde{G} = \mathcal{J}_X(K)/H.$$

On a d'après l'hypothèse de Riemann (démontré pour les corps de fonctions par Weil [Wei48])

$$\tilde{\mathfrak{o}} := |\tilde{G}| \geqslant (p^{2m} - 1)^{2g_X}/(p^m + 1)^{2g_X} = (p^m - 1)^{2g_X}.$$

On veut un groupe de Galois dont l'ordre est soit une puissance de p, soit premier à p, pour pouvoir appliquer les propositions 48 et 52. Notons

$$\tilde{G} = \tilde{G}_p \times \tilde{G}_{p'}$$

où $\tilde{G}_p$ est un sous-groupe maximal de $\tilde{G}$ d'ordre $\tilde{\mathfrak{o}}_p$ une puissance de p et $\tilde{G}_{p'}$ est un supplémentaire de $\tilde{G}_p$, d'ordre $\tilde{\mathfrak{o}}_{p'} = \tilde{\mathfrak{o}}/\tilde{\mathfrak{o}}_p$ premier à p. Soit $\tilde{H}$ le plus petit de ces deux sous-groupes. Alors il existe Y une courbe projective lisse sur K et

$$\tau : Y \longrightarrow X$$

un revêtement abélien non ramifié totalement décomposé au-dessus de P_1 de groupe de Galois

$$G = \tilde{G}/\tilde{H}.$$

L'ordre de G, noté $\mathfrak{o}$, est soit une puissance de p, soit premier à p, et

$$\mathfrak{o} \geqslant \sqrt{\tilde{\mathfrak{o}}} \geqslant (p^m - 1)^{g_X}.$$

Tous les points κ-rationnels de X sont totalement décomposés dans Y (car totalement décomposés dans $\tilde{Y}$). Soit

$$Q = \tau^*(P),$$

c'est un diviseur sur Y de degré

$$\deg Q = n\mathfrak{o} = N.$$

On suppose que

$$p^m > 3,$$

alors, d'une part, $\mathfrak{o} \geqslant (p^m - 1)^{g_X}$ croît exponentiellement par rapport à g_X et, d'autre part, on a

$$(p^m - 1)g_X > 2g_X - 1.$$

Ainsi, on a asymptotiquement

$$n > 2g_X - 1.$$

Soit

$$\delta_{lim} \in]0, 1 - \frac{2}{p^m - 1}[$$

et soit

$$\rho_{lim} = 1 - \delta_{lim} - \frac{1}{p^m - 1} \in]\frac{1}{p^m - 1}, 1 - \frac{1}{p^m - 1}[.$$

Soit $D \in \mathrm{Div}(X)$ un diviseur disjoint de P, tel que

$$\deg D = \lceil \rho_{lim} n + g_X - 1 \rfloor.$$

Alors asymptotiquement on a

$$2g_X - 2 < \deg D < (p^m - 1)g_X \approx n.$$

Soit

$$E = \tau^*(D)$$

et

$$k = \deg D - g_X + 1.$$

Alors $\mathcal{L}(E)$ est un $K[G]$-module libre de rang k. On a

$$|\rho(\mathrm{Gop}(Q, E)) - \rho_{lim}| \leqslant \frac{1}{2n} \text{ et } |\delta^*(Q, E) - \delta_{lim}| \leqslant \frac{1}{2n}$$

où $\delta^*(Q, E) := d^*(Q, E)/N$ désigne la distance prescrite relative de $\mathrm{Gop}(Q, E)$.

Soit $\varepsilon > 0$, on veut qu'il soit possible de décoder $\lfloor \varepsilon n \mathfrak{o} \rfloor$ erreurs pour le code $\mathrm{Gop}(E, Q)$. D'après l'équation (4.5.10), il est possible de décoder au plus

$$\mathfrak{o} \lfloor \frac{d^*(P, D) + g_X - 1}{2} \rfloor - g_Y \approx \frac{d^*(Q, E) - g_Y - 1}{2}$$

erreurs. On doit donc avoir

$$0 < \varepsilon \leqslant \frac{1}{2} \left(\frac{d^*(Q, E)}{n\mathfrak{o}} - \frac{g_Y + 1}{n\mathfrak{o}} \right) \approx \frac{1}{2} \left(\delta^*(D, P) - \frac{1}{p^m - 1} \right).$$

Il faudra donc imposer

$$\delta_{lim} > \frac{1}{p^m - 1}$$

ce qui induit

$$\frac{1}{p^m - 1} < 1 - \frac{2}{p^m - 1}$$

ou de manière équivalente

$$p^m > 4.$$

On rappelle que

$$\log \mathfrak{o} \geqslant g_X \log(p^m - 1),$$

donc, puisque $n \approx (\sqrt[4]{q} - 1)g_X$, il existe une constante absolue

$$\alpha > 0$$

(en particulier, indépendante de l'indice $i \in \mathbb{N}$) telle que

$$\alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant k \log p \text{ et } \alpha \sqrt[4]{q} \log \mathfrak{o} \geqslant n \text{ et } \alpha \log \mathfrak{o} \geqslant \log p. \tag{4.5.14}$$

Notons également que l'une des conditions (4.5.12) ou (4.5.13) est respectée par construction. Donc, d'après les résultats de la section 4.5.2, on déduit le théorème 54.

Théorème 54. *Soit p un entier premier et $m > 0$ un entier tel que*

$$p^m \geqslant 4.$$

Soit K un corps fini à p^{4m} éléments. Soit

$$\delta_{lim} \in]0, 1 - \frac{2}{p^m - 1}[.$$

Alors il existe une famille de code correcteurs munis d'une structure de module d'une K-algèbre de groupe

- *dont les longueurs tendent vers l'infini.*
- *dont les distances prescrites relatives convergent vers $\delta_{lim} > 0$.*
- *dont les rendements convergent vers $1 - \delta_{lim} - \frac{1}{p^m - 1} > 0$.*
- *encodables en temps quasi-linéaire en leur longueur.*

Si de plus,

$$p^m \geqslant 5 \text{ et } \delta_{lim} > \frac{1}{p^m - 1},$$

alors il existe une famille de code correcteurs munis d'une structure de module d'une K-algèbre de groupe vérifiant les points précédents, et dont on peut décoder un rendement d'erreurs de

$$\frac{1}{2}\left(\delta_{lim} - \frac{1}{p^m - 1}\right)$$

en temps quasi-quadratique en leur longueur.

Remarque 27. Ces codes peuvent être excellents si q est assez grand. Pour le vérifier, on fait un calcul similaire à celui de Lachaud [Lac86, Section 4.7]. On rappelle qu'une famille de codes sur le corps K est excellente si δ_{lim} et ρ_{lim}, les liminf des distances relatives et des rendements de la famille, vérifient

$$\rho_{lim} > 1 - H_q(\delta_{lim}).$$

Avec nos formules on obtient :

$$\exists x \in [0,1], 1 - \frac{1}{p^m - 1} - x > 1 - H_q(x) \Leftrightarrow \frac{1}{p^m - 1} < \log_q \left(\frac{2q-1}{q} \right)$$
$$\Leftrightarrow q \geqslant 19^4.$$

Si on sélectionne pour le calcul non pas δ_{lim}, mais la distance relative effectivement décodable avec l'algorithme basique $\delta_{lim} - \frac{1}{p^m - 1}$, on a des codes excellents si

$$\exists x \in [0,1], 1 - \frac{2}{p^m - 1} - x > 1 - H_q(x) \Leftrightarrow \frac{2}{p^m - 1} < \log_q \left(\frac{2q-1}{q} \right)$$
$$\Leftrightarrow q \geqslant 47^4.$$

4.5.4 Un exemple de code géométrique structuré

Dans cette sous-section, on calcule un exemple de code géométrique structuré. Soit κ un corps à 4 éléments et K une extension de κ de degré 2, possédant donc 16 éléments. Soit $a \in K$ un élément tel que

$$a^4 + a + 1 = 0.$$

Soit

$$X : y^2 + y = x^5 + x^4 + x^3$$

une courbe hyperelliptique (donc projective lisse) sur K de genre $g_X = 2$. Notons que X est définie sur κ. Notons L_κ et L_K les polynômes-L de X_κ et X respectivement. On a

$$L_\kappa = 16z^4 + 16z^3 + 12z^2 + 4z + 1 \text{ et } L_K = 256z^4 + 128z^3 + 48z^2 + 8z + 1.$$

On en déduit que

— X possède 9 points κ-rationnels et 25 points K-rationnels.

— $|\mathcal{J}_X(K)| = 441 = 49 \cdot 9$ et $|\mathcal{J}_X(\kappa)| = 49$.

Notre premier objectif est de déterminer un revêtement de X sur K, abélien, non ramifié, de groupe de Galois isomorphe à $\mathcal{J}_X(K)/\mathcal{J}_X(\kappa)$, totalement décomposé au-dessus des points κ-rationnels de X.

Soit P_∞ l'unique point à l'infini de X. C'est un point κ-rationnel de X. On note $P_1, \ldots, P_8$ les autres points κ-rationnels de X dont les coordonnées affines sont :

$$\begin{array}{rcc|rcc} P_1 & = & (0,0) & P_2 & = & (0,1) \\ P_3 & = & (a^2+a,0) & P_4 & = & (a^2+a,1) \\ P_5 & = & (a^2+a+1,0) & P_6 & = & (a^2+a+1,1) \\ P_7 & = & (1,a^2+a) & P_8 & = & (1,a^2+a+1). \end{array}$$

Enfin soient P_9 et P_{10} des points K-rationnels de X dont les coordonnées affines sont :

$$P_9 = (a^3, a^3) \text{ et } P_{10} = (a^3 + 1, a + 1).$$

Soient c_1 et c_2 les classes des diviseurs $3P_\infty + P_{10} - 4P_9$ et $P_\infty - P_9$ dans $\mathcal{J}_X(K)$. On peut montrer que c_1 et c_2 engendrent $\mathcal{J}_X(K)$, ou plus précisément

$$\mathcal{J}_X(K) = (\mathbb{Z}/21\mathbb{Z})c_1 \times (\mathbb{Z}/21\mathbb{Z})c_2.$$

Ainsi

$$\mathcal{J}_X(K)/\mathcal{J}_X(\kappa) \simeq (\mathbb{Z}/3\mathbb{Z})^2 .$$

En particulier, ce groupe est d'exposant 3. Or K possède une racine primitive cubique de l'unité

$$\zeta_3 = a^2 + a.$$

D'après la théorie de Kummer, toute extension abélienne de $K(X)$ de degré 9 et d'exposant 3 est isomorphe à une extension de la forme $K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$, où $R_1, R_2 \in K(X)^*$ ne sont pas des cubes. D'après [Sti08, Proposition 3.7.3], l'extension associée à R_1 et R_2 est non-ramifiée si et seulement s'il existe deux diviseurs Γ_1 et Γ_2 tels que

$$(R_1) = 3\Gamma_1 \text{ et } (R_2) = 3\Gamma_2. \tag{4.5.15}$$

Enfin, l'extension est purement géométrique (i.e. le corps des constantes de l'extension est K) si et seulement si les classes de Γ_1 et Γ_2 dans $\mathcal{J}_X(K)$ sont d'ordre 3.

Réciproquement, soient

$$\Gamma_1 = P_{11} + P_{12} - 2P_\infty \text{ et } \Gamma_2 = P_9 + P_{13} - 2P_\infty$$

où les coordonées affines de P_{11}, P_{12} et P_{13} sont

$$P_{11} = (a^3 + a, a^3 + a + 1) \ ; \ P_{12} = (a^3 + a^2, a^3 + a^2) \ ; \ P_{13} = (a^3 + a^2 + a + 1, a^3 + a^2 + a).$$

On a

$$\Gamma_1 \sim 7 * c_1 \text{ et } \Gamma_2 \sim 7 * c_2$$

donc les classes de Γ_1 et Γ_2 sont d'ordre de 3 et engendrent la 3-torsion de $\mathcal{J}_X(K)$. Soient $R_1, R_2 \in K(X)^*$ des fonctions satisfaisant la condition (4.5.15), et telles que

$$R_1(P_1) = R_2(P_1) = 1.$$

Alors $K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$ est une extension abélienne, non-ramifiée, purement géométrique de $K(X)$, de groupe de Galois d'ordre 9 et d'exposant 3. On note

$$K(Y) := K(X)[z_1, z_2]/\langle z_1^3 - R_1, z_2^3 - R_2\rangle$$

et on note Y une courbe projective lisse sur K dont $K(Y)$ est le corps de fonctions. Alors il existe un revêtement abélien non-ramifié

$$\tau : Y \longrightarrow X$$

de groupe de Galois G isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$.

Il reste à démontrer que τ est totalement décomposé au-dessus des points κ-rationnels de X. Pour cela, d'après le théorème 14 et la proposition 15, il suffit de montrer que τ est totalement décomposé au-dessus de P_1. Soient $r_1, r_2 \in K(Y)$ tels que

$$r_1^3 = R_1 \text{ et } r_2^3 = R_2.$$

Soit Q un point K-rationnel de Y dans la fibre de τ au-dessus de P_1. On sait que, comme K-algèbre, le corps résiduel K_Q est engendré par $r_1(Q)$ et $r_2(Q)$. Or, par construction,

$$r_1(Q)^3 = R_1(Q) = R_1(P_1) = 1 \text{ et similairement } r_2(Q)^3 = 1.$$

Puisque K contient les racines cubiques de l'unité, on déduit que $K_Q \simeq K$, et donc P_1 est totalement décomposé dans Y.

Notre second objectif est de calculer une G-matrice d'encodage d'un code géométrique sur Y. Soient

$$D = 3P_9 \text{ et } P = P_\infty + \sum_{i=1}^{8} P_i$$

et soient

$$E = \tau^*(D) \text{ et } Q = \tau^*(P).$$

Notons que les points de P sont κ-rationnels, donc complètement décomposés dans Y. Soit

$$k = \deg D - g_X + 1 = 2.$$

Rappelons que r_1 et r_2 sont des fonctions de $K(Y)^*$ telles que

$$r_1^3 = R_1 \text{ et } r_2^3 = R_2.$$

En particulier, on a

$$(r_1) = \tau^*(\Gamma_1) \text{ et } (r_2) = \tau^*(\Gamma_2).$$

On fixe une famille génératrice de G. Soit σ_1 et σ_2 des éléments de G tels que

$$\begin{array}{cc} r_1 \cdot \sigma_1 = \zeta_3 r_1 & r_1 \cdot \sigma_2 = r_1 \\ r_2 \cdot \sigma_1 = r_2 & r_2 \cdot \sigma_2 = \zeta_3 r_2 \end{array}$$

alors σ_1 et σ_2 engendrent G. On fixe également une famille génératrice de

$$\hat{G} = \mathrm{Hom}(G, K^*).$$

Soient χ_1 et χ_2 deux caractères de $\hat{G}$ tels que

$$\begin{array}{cc} \chi_1(\sigma_1) = \zeta_3 & \chi_1(\sigma_2) = 1 \\ \chi_2(\sigma_1) = 1 & \chi_2(\sigma_2) = \zeta_3. \end{array}$$

D'après la formule de Riemann-Hurwitz, le genre de Y est

$$g_Y = 9(g_X - 1) + 1 = 10.$$

On a

$$\deg E = 9 \deg D = 27 > 18 = 2g_Y - 2,$$

donc d'après le théorème 51, l'espace $\mathcal{L}(E)$ est un $K[G]$-module libre de rang $k = 2$. Rappelons que l'ordre de G est premier à 16, le nombre d'éléments de K. De plus, puisque K contient les racines cubiques de l'unité, $\mathcal{L}(E)$ se décompose de la manière suivante :

$$\mathcal{L}(E) = \bigoplus_{0 \leqslant i,j \leqslant 2} \mathcal{L}(E)_{\chi_1^i \chi_2^j}$$

où pour tous $0 \leqslant i, j \leqslant 2$, le K-espace vectoriel $\mathcal{L}(E)_{\chi_1^i \chi_2^j}$ est le sous-$K[G]$-module simple de $\mathcal{L}(E)$ associé au caractère $\chi_1^i \chi_2^j$, i.e. l'ensemble des fonctions $f \in \mathcal{L}(E)$ telles que

$$\forall \alpha, \beta \in [0..2], f \cdot (\sigma_1^\alpha \sigma_2^\beta) = \zeta_3^{(\alpha i + \beta j)} f.$$

En l'occurence, ce sont des K-espaces vectoriels de dimension $k = 2$.

Soient $i, j \in [0..2]$, et soit $f \in \mathcal{L}(E)_{\chi_1^i \chi_2^j}$. Pour tous $\alpha, \beta \in [0..2]$, on a

$$\frac{f}{r_1^i r_2^j} \cdot (\sigma_1^\alpha \sigma_2^\beta) = \frac{\zeta_3^{(\alpha i + \beta j)} f}{\zeta_3^{(\alpha i + \beta j)} r_1^i r_2^j} = \frac{f}{r_1^i r_2^j}.$$

Autrement dit, $f/(r_1^i r_2^j) \in K(X)$ et plus précisément

$$f/(r_1^i r_2^j) \in \mathcal{L}(D + i\Gamma_1 + j\Gamma_2).$$

Pour tous $i, j \in [0..2]$, on fixe $(f_{(1,i,j)}, f_{(2,i,j)})$, une K-base de $\mathcal{L}(D + i\Gamma_1 + j\Gamma_2)$. Soient

$$f_1 = \sum_{1 \leqslant i,j \leqslant 3} f_{(1,i,j)} r_1^i r_2^j \text{ et } f_2 = \sum_{0 \leqslant i,j \leqslant 2} f_{(2,i,j)} r_1^i r_2^j,$$

alors (f_1, f_2) est une $K[G]$-base de $\mathcal{L}(E)$.

Pour calculer une G-matrice génératrice de $\mathrm{Gop}^G(Q, E)$, il faut être capable d'évaluer f_1 et f_2 sur la fibre au-dessus de P. On explique comment évaluer f_1 sur la fibre au-dessus de P_1. Rappellons que

$$R_1(P_1) = R_2(P_1) = 1,$$

donc les valeurs de r_1 et r_2 sur la fibre au-dessus de P_1 sont des racines cubiques de l'unité. Soit $Q_{1,1}$ le point de Y au-dessus de P_1 tel que

$$r_1(Q_{1,1}) = r_2(Q_{1,1}) = \zeta_3.$$

Pour tout $\sigma \in G$, on définit

$$Q_{1,\sigma} = \sigma(Q_{1,1}).$$

Alors pour tous $\alpha, \beta \in [0..2]$,

$$\begin{aligned} f_1(Q_{i,\sigma_1^\alpha \sigma_2^\beta}) &= \sum_{0 \leqslant i,j \leqslant 2} \zeta_3^{(\alpha i + \beta j)} f_{(1,i,j)}(P_1) r_1(Q_{1,1})^i r_2(Q1,1)^j \\ &= \sum_{0 \leqslant i,j \leqslant 2} \zeta_3^{((\alpha+1)i + (\beta+1)j)} f_{(1,i,j)}(P_1) \end{aligned}$$

Notons que ces calculs ne nécessitent que de calculer une racine primitive cubique de l'unité ζ_3, les fonctions $(f_{(1,i,j)})_{i,j \in [0..2]}$, et des racines cubiques de $R_1(P_1)$ et $R_2(P_1)$.

Pour terminer, on calcule la matrice $\mathcal{E} \in \mathcal{M}_{P,2}(K[G])$, dont la composante de coordonnées $(P_i, j)_{P_i \in P, j \in [1..2]}$ est

$$\mathcal{E}_{P_i,j} = \sum_{0 \leqslant \alpha,\beta \leqslant 2} f_j(Q_{j,\sigma_1^{-\alpha}\sigma_2^{-\beta}}) \sigma_1^\alpha \sigma_2^\beta.$$

Pour la composante de coordonnées $(P_1, 1)$, on trouve

$$\begin{array}{rccccc} \mathcal{E}_{P_1,1} = & (a^3+a^2+a+1) & + & a^2\sigma_1 & + & (a^3+1)\sigma_1^2 \\ + & (a+1)\sigma_2 & + & (a^3+a+1)\sigma_1\sigma_2 & & \\ + & (a^3+a)\sigma_2^2 & + & (a^2+1)\sigma_1\sigma_2^2 & + & (a^3+1)\sigma_1^2\sigma_2^2. \end{array}$$

Chapitre 5

Courbes elliptiques à couplages

Les courbes elliptiques sont aujourd'hui un outil incontournable de la cryptographie à clé publique. En particulier, les cryptosystèmes dont la sécurité repose sur la difficulté du calcul de logarithmes discrets sont utilisés dans de nombreuses situations. Depuis le début des années 2000, de nouveaux protocoles utilisant des couplages de courbes elliptiques ont été développés. Ces protocoles nécessitent des courbes spécifiques, dites *à couplages*, pour fonctionner de manière satisfaisante. La génération de courbes à couplages est donc un enjeu important pour discuter de l'efficacité et de la sureté de ces protocoles.

Dans ce chapitre, après une introduction rapide à la cryptographie à base de couplages, on présente les méthodes classiques de génération de courbes à couplages. Dans un second temps, on présente une nouvelle méthode pour produire des familles de courbes, ainsi que des familles produites par cette méthode. Enfin, on étudie un des problèmes algorithmiques intervenant dans l'utilisation de la méthode.

5.1 Cryptographie à base de couplages

Dans cette section, on présente rapidement le principe et les enjeux de sécurité de la cryptographie à base de couplages.

5.1.1 Rappels de cryptographie basée sur le DLP dans les courbes elliptiques

On commence par quelques rappels sur les courbes elliptiques. Soit K un corps fini à $q = p^m$ éléments, où $p \geqslant 5$. Notons $\bar{K}$ une clôture algébrique de K. Une courbe elliptique E peut-être définie sur K par un polynôme sous forme de Weierstrass courte :

$$E/K : y^2z = x^3 + Axz^2 + Bz^3,$$

où $A, B \in K$ vérifient $4A^3 + 27B^2 \neq 0$. On notera P_∞ le point à l'infini de la courbe E, dont les coordonnées projectives sont $[0 : 1 : 0]$. Dans le cas des courbes elliptiques, l'application

de Jacobi $P \mapsto P - P_\infty$ est un isomorphisme entre E et $\mathcal{J}_E$, qui induit une structure de groupe algébrique sur E. On note $E(K)$ le groupe des points K-rationnels de la courbe.

Pour tout entier r, on notera $E[r]$ la r-torsion de la courbe E. On notera alors $E[r](K)$ le groupe des points de r-torsion rationnels de E et $E[r](\bar{K})$ le groupe des points de r-torsion de E définis sur $\bar{K}$.

Le polynôme-L de la courbe elliptique E est de la forme

$$L_{E/K} = qX^2 - tX + 1$$

avec t un entier appelé trace de E. La courbe E étant isomorphe à sa jacobienne, on sait que

$$|E(K)| = L_{E/K}(1) = q + 1 - t.$$

La borne de Hasse-Weil garantit que $|t| \leqslant 2\sqrt{q}$. La courbe E est ordinaire si $\text{pgcd}(t, p) = 1$, sinon elle est supersingulière.

Si E est une courbe elliptique ordinaire, alors $\text{End}(E)$ est un anneau isomorphe à un ordre $\mathcal{O}$ dans un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-D})$ (où D est un entier positif non divisible par un carré). L'endomorphisme de Frobenius engendre un anneau isomorphe à un sous-ordre de $\mathcal{O}$, dont le discriminant est le même, à un facteur carré près, que celui de $\mathcal{O}$ ou de celui du corps $\mathbb{Q}(\sqrt{-D})$. Le discriminant du sous-ordre engendré par le Frobenius est égal au discriminant du polynôme caractéristique du Frobenius $X^2 - tX + q$:

$$\text{disc}(X^2 - tX + q) = t^2 - 4q.$$

Donc D est le diviseur maximal sans facteur carré de $4q - t^2$, et il existe un entier y tel que :

$$-Dy^2 = t^2 - 4q$$

Remarque 28. Le terme discriminant peut référer à plusieurs valeurs différentes : le discriminant de la courbe $-16(4A^3 + 27B^2)$, le discriminant de son anneau d'endomorphismes, le discriminant du Frobenius, ou le discriminant de l'ordre maximal de $\mathbb{Q}(\sqrt{-D})$. De plus, dans la littérature sur la génération de courbes à couplages, D est souvent appelé discriminant également. Dans ce chapitre, sauf mention contraire, on désignera par discriminant le discriminant de l'anneau d'endomorphismes, et par discriminant cryptographique l'entier positif sans facteur carré D.

Pour les applications cryptographiques, on se place dans le cas où $|E(K)| = rh$, où r est un entier premier, différent de p la caractéristique de K, et $h \ll r$, de sorte que

$$\log(q) \approx \log\left(|E(K)|\right) \approx \log(r).$$

Dans ce cas, il est clair que la r-torsion rationnelle de la courbe E est cyclique. Il est considéré que le calcul d'un logarithme discret dans $E[r](K)$ nécessite $O(\sqrt{r})$ opérations dans $E(K)$. Alors, pour garantir s **bits de sécurité** (ce qui définit le **niveau de sécurité** s) aux schémas cryptographiques reposant sur la difficulté du calcul du logarithme discret, il faut que $\log(r) \geqslant 2s$. Ainsi, le calcul du logarithme discret requiert d'effectuer au moins $\sqrt{r} \geqslant 2^s$ opérations sur la courbe.

5.1.2 Couplages

En toute généralité, un couplage est un morphisme de groupe entre un produit de groupes (notés additivement) $\mathbb{G}_1 \times \mathbb{G}_2$ et un groupe (noté multiplicativement) $\mathbb{G}_T$

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

vérifiant deux conditions :

— *(Non-dégénérescence)*

$$\forall P \in \mathbb{G}_1 \setminus \{0\}, \exists Q \in \mathbb{G}_2, e(P,Q) \neq 1,$$

et

$$\forall Q \in \mathbb{G}_2 \setminus \{0\}, \exists P \in \mathbb{G}_1, e(P,Q) \neq 1.$$

— *(Bilinéarité)* $\forall P_1, P_2 \in \mathbb{G}_1, \forall Q_1, Q_2 \in \mathbb{G}_2, \forall n_1, n_2 \in \mathbb{Z}$,

$$e(n_1P_1 + n_2P_2, Q_1) = e(P_1, Q_1)^{n_1} e(P_2, Q_1)^{n_2},$$

et

$$e(P_1, n_1Q_1 + n_2Q_2) = e(P_1, Q_1)^{n_1} e(P_1, Q_2)^{n_2}.$$

Le couplage de Weil introduit dans la section 2.2.1 est un exemple de couplage. Reprenons les notations de la sous-section 5.1.1, E est une courbe elliptique sur K, et r est un premier distinct de la caractéristique p divisant $|E(K)|$. Dans ce cas, puisque E est isomorphe à sa jacobienne, on définit le couplage de Weil comme suit

$$e_r : E[r](\bar{K}) \times E[r](\bar{K}) \longrightarrow \mu_r(\bar{K})$$

en identifiant tout point P au diviseur $P - P_\infty$.

Soit k l'ordre de q modulo r, on appelle k le **degré de plongement**. Supposons que $k > 1$. Soit K_r une extension de degré k de K. Puisque r est premier à la caractéristique, qu'une partie de la r-torsion est rationnelle et $k > 1$, on sait que la r-torsion de E est K_r-rationnelle, et que K_r contient r racines r-ièmes de l'unité. Dans ce cas, le couplage de Weil est défini sur K_r.

Si $r^2 \nmid q^k - 1$, on peut également définir le **couplage de Tate** (réduit)[Ver10]

$$\mathfrak{e}_r : E[r](K_r) \times E(K_r)/rE(K_r) \longrightarrow \mu_r(K_r)$$

de manière similaire au couplage de Weil. Soit $P \in E[r](K_r)$, soit f_P la fonction de diviseur $rP - (rP) - (r-1)P_\infty$ normalisée en P_∞, i.e. étant donné une uniformisante u_∞ en P_∞, on a $u_\infty^{r-1} f_P(P_\infty) = 1$. Soit $Q \in E(K_r)/rE(K_r)$, alors

$$\mathfrak{e}_r(P,Q) = f_P(Q)^{(q-1)/r}.$$

Il existe un couplage dérivé du couplage de Tate, appelé **couplage Ate optimal**, dont l'évaluation requiert moins d'opérations que celle du couplage de Tate [Ver10].

Il est clair d'après ce qui précède que, pour que ces couplages puissent être calculés efficacement, il est nécessaire que le degré de plongement k soit de taille raisonnable (en pratique, il est commun de demander $k \leqslant 54$). Dans ce cas, on dira que E est une courbe à couplages. Cependant, les courbes à couplage sont extrêmement rares [BK98], et ne peuvent pas être trouvées par tirage au sort. Il existe néanmoins des méthodes pour en construire, et on en détaillera certaines dans la section 5.2.

En guise d'exemple, on sait que les courbes supersingulières ont de petits degrés de plongement ($k \leqslant 6$). Autrement dit, il n'y a pas d'obstacle au calcul de couplages sur une courbe supersingulière. Par contre, avoir un degré de plongement si petit nuit à la sécurité des protocoles reposant sur le logarithme discret, comme expliqué dans la sous-section 5.1.4. Ainsi, on s'intéressera plutôt à la construction de courbes à couplages ordinaires.

5.1.3 Un exemple de protocole

Les couplages peuvent être utilisés pour plusieurs applications cryptographiques. On présente ici un protocole d'échange de clé triparti proposé par Joux dans [Jou00].

Soit P un générateur de la r-torsion rationnelle de E. Le célèbre échange de clé de Diffie-Hellman fonctionne comme suit : deux protagonistes $\mathcal{A}$ et $\mathcal{B}$ s'accordent pour utiliser les paramètres publics E, r et P. Le protagoniste $\mathcal{A}$ tire au sort un paramètre secret $s_{\mathcal{A}} \in \mathbb{Z}/r\mathbb{Z}$ et calcule le point $s_{\mathcal{A}}P$ qui constitue sa clé publique. Le protagoniste $\mathcal{B}$ tire au sort $s_{\mathcal{B}} \in \mathbb{Z}/r\mathbb{Z}$ et calcule $s_{\mathcal{B}}P$. Les protagonistes s'envoient mutuellement leur clé publique et peuvent calculer la clé commune $s_{\mathcal{A}}s_{\mathcal{B}}P = s_{\mathcal{B}}s_{\mathcal{A}}P$.

Mais comment doivent procéder trois protagonistes $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ pour échanger une clé commune ? Une solution serait d'utiliser le protocole ci-dessus plusieurs fois pour calculer $s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}P$. Par exemple, $\mathcal{A}$ et $\mathcal{B}$ échangent leur clé $s_{\mathcal{A}}s_{\mathcal{B}}P$, et l'envoient à $\mathcal{C}$, qui peut alors calculer $s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}P$. Cette solution a plusieurs défauts, notamment de demander que $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ soient connectés simultanément.

La solution de Joux consiste à utiliser le pairing de Tate réduit $\mathfrak{e}_r$ pour calculer la clé commune. Alors :

— $\mathcal{A}$ calcule $\mathfrak{e}_r(s_{\mathcal{B}}P, s_{\mathcal{C}}P)^{s_{\mathcal{A}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.

— $\mathcal{B}$ calcule $\mathfrak{e}_r(s_{\mathcal{A}}P, s_{\mathcal{C}}P)^{s_{\mathcal{B}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.

— $\mathcal{C}$ calcule $\mathfrak{e}_r(s_{\mathcal{A}}P, s_{\mathcal{B}}P)^{s_{\mathcal{C}}} = \mathfrak{e}_r(P,P)^{s_{\mathcal{A}}s_{\mathcal{B}}s_{\mathcal{C}}}$.

Cette solution a l'intérêt de réduire le nombre de rondes nécessaires pour échanger les clés. Par exemple, si $\mathcal{C}$ veut envoyer un message commun à $\mathcal{A}$ et $\mathcal{B}$, en utilisant l'échange de clés de Joux, il n'a besoin que d'aller chercher leurs clés publiques, au lieu de devoir attendre que $\mathcal{A}$ et $\mathcal{B}$ envoient leur secret commun.

Les couplages peuvent également servir pour d'autres applications. Par exemple, dans [BLS01], Boneh, Lynn et Shacham proposent d'utiliser les couplages pour construire des signatures courtes. Une autre application très intéressante des couplages est le chiffrement basé sur l'identité introduit par Boneh et Franklin dans [BF03].

5.1.4 Sécurité des courbes à couplage

On reprend les notations introduites dans la sous-section 5.1.2.

Les courbes à couplages sont vulnérables à une attaque présentée dans [MOV93], dénommée attaque MOV. Le principe est d'utiliser un couplage pour réduire le problème du logarithme discret dans la r-torsion de la courbe E sur K au problème du logarithme discret dans K_r^*. Or la complexité de résolution du problème du logarithme discret dans K_r^* est sous-exponentielle en $k \log\ q$ [BGK15]. Pour les courbes à couplages, où le degré de plongement k est petit relativement à q (en pratique, on a toujours $k \leqslant \log\ q$ par exemple), il est possible que les logarithmes discrets soient plus simples à calculer dans K_r^* que dans $E(K)$.

Pour des considérations pratiques, cela signifie par exemple qu'il est contraignant d'utiliser les courbes dont les degrés de plongement sont les plus petits (les courbes supersingulières par exemple) car, pour préserver la difficulté du logarithme discret, il faut augmenter la taille des paramètres r et q.

5.2 Génération de courbes à couplages

Comme il a été mentionné dans le paragraphe 5.1.2, Les courbes à couplages nécessitent des méthodes de construction spécifiques. Dans cette section, on rappelle des méthodes classiques de génération de courbes et de familles de courbes à couplage. On s'intéressera uniquement aux techniques produisant des courbes ordinaires.

5.2.1 Courbes ordinaires et multiplication complexe

L'approche standard pour produire des courbes à couplages consiste à fixer le degré de plongement k souhaité comme paramètre de départ, puis en déduire des conditions sur les autres paramètres. Fixons alors $k > 1$ un entier. On cherche à produire des courbes à couplage de degré de plongement k ordinaires.

Soit E une courbe elliptique ordinaire définie sur un corps fini K à q éléments. Soit t la trace de E, alors $\text{pgcd}(t, q) = 1$. De plus, la borne de Hasse-Weil indique que

$$|t| \leqslant 2\sqrt{q}$$

ou de manière équivalente $4q - t^2 > 0$. D'après [Wat69], la réciproque est vraie : pour toute paire d'entiers (q, t) où q est une puissance de premier et t est premier à q tel que $4q - t^2 > 0$, il existe une courbe elliptique ordinaire E, définie sur un corps fini K à q éléments, de trace t.

Pour produire des courbes à couplages, on ajoute un entier r et des conditions sur r, q, t et k décrivant que E doit avoir un sous-groupe de points K-rationnels d'ordre r premier et de degré de plongement k.

Proposition 55 ([FST10])**.** Soit $k \geqslant 1$ un entier. Soient q, r, t des entiers tels que :

1. q est une puissance de premier.
2. r est premier, et $r \nmid kq$.
3. t et q sont premiers entre eux.
4. il existe un entier h tel que $q + 1 - t = rh$.
5. r divise $\Phi_k(t-1)$ où Φ_k désigne le k-ième polynôme cyclotomique.
6. $4q - t^2 > 0$.

Alors il existe une courbe elliptique ordinaire E définie sur un corps fini K à q éléments, de trace t, ayant un sous-groupe K-rationnel d'ordre r, de degré de plongement k.

Maintenant, il faut être capable de retrouver E explicitement. En supposant que q est premier, on peut utiliser la méthode de la multiplication complexe d'Atkin et Morain (voir la sous-section 3.2.3) pour calculer le j-invariant de E. Soit D le discriminant cryptographique de la courbe E (i.e. le plus petit entier D tel qu'il existe $y \in \mathbb{Z}$ tel que $4q - t^2 = Dy^2$). L'algorithme de la multiplication complexe demande de calculer (ou de connaître) le polynôme de classes de Hilbert du corps $\mathbb{Q}(\sqrt{-D})$. Cela n'est réalisable que si D est relativement petit. Pour cette raison, il est commun de fixer D comme paramètre de départ avec k.

Corollaire 55.1. Soit $k \geqslant 1$ un entier, et D un entier positif non divisible par un carré. Soient q, r, t des entiers tels que :

1. q est premier.
2. r est premier, et $r \nmid kq$.
3. t et q sont premiers entre eux.
4. il existe un entier h tel que $q + 1 - t = rh$.
5. r divise $\Phi_k(t-1)$ où Φ_k désigne le k-ième polynôme cyclotomique.
6. il existe un entier y tel que $4q - t^2 = Dy^2$.

Alors il existe une courbe elliptique ordinaire E définie sur un corps fini K à q éléments, de trace t, ayant un sous-groupe K-rationnel d'ordre r, de degré de plongement k. Le discriminant cryptographique de E est D.

La condition 6 est appelée **équation CM**. Elle est équivalente à

$$Dy^2 = 4hr - (t-2)^2 \tag{6'}$$

dans le sens qu'il est possible de remplacer la condition 6 par la condition 6' sans changer la proposition.

Enfin, il a déjà été mentionné que pour les applications cryptographiques, on souhaitait que

$$\log\ r \approx \log\ q.$$

Généralement, plus le rapport $\log\ q / \log\ r$ est proche de 1, plus la courbe est intéressante. On définit la valeur-ρ

$$\rho = \frac{\log\ q}{\log\ r}$$

qui sera le critère de qualité principal des courbes à couplages produites.

5.2.2 Méthode de Cocks–Pinch

On utilise les notations du corollaire 55.1. La méthode de Cocks–Pinch [FST10] est une méthode pour construire des courbes à couplage. L'idée de cette méthode est d'utiliser les relations arithmétiques entre q, t et y modulo r, pour pouvoir les calculer quand r est fixé.

La condition 5 implique que $t-1$ est une racine primitive k-ième de l'unité modulo r, et la condition 6' implique que $-D$ a une racine carrée modulo r. Ainsi, on obtient des contraintes supplémentaires sur r, à savoir :

— $k \mid r-1$,

— $\left(\frac{-D}{r}\right) = 1$.

On peut alors générer une courbe à couplage avec l'algorithme 5.2.1.

Algorithme 5.2.1 : Algorithme de Cocks–Pinch

Entrées : $k \geqslant 1$ un entier, D un entier positif non divisible par un carré

Output : q, r et t des entiers paramétrant une courbe à couplage

1 Soit r un entier premier tel que $k \mid r-1$ et $\left(\frac{-D}{r}\right) = 1$

2 Soit ζ_k une racine k-ième de l'unité modulo r

3 Calculer un entier $t \equiv \zeta_k + 1 \bmod r$

4 Calculer un entier $y \equiv (\zeta_k - 1)/\sqrt{-D} \bmod r$

5 Calculer $q = (t^2 + Dy^2)/4$

6 Si q est entier et premier, renvoyer q, r et t, sinon reprendre à 1. et changer r, ζ_k, t ou y.

On peut toujours choisir t et y dans $[-r, r]$, donc $q \leqslant \frac{D+1}{4} r^2$. Ainsi, de manière générale, la méthode de Cocks–Pinch génère des courbes à couplage dont la valeur-ρ est proche de 2, ce qui en fait d'assez mauvaises courbes comparées aux courbes utilisées en pratique, produites par d'autres méthodes. Cependant, cette méthode est très flexible, et permet d'avoir beaucoup de contrôle sur r, par exemple sur le poids de Hamming de sa décomposition binaire. De plus, la plupart des méthodes de génération utilisés pour les familles de courbes s'inspirent de la méthode de Cocks–Pinch, par exemple celle de Brezing–Weng (section 5.2.4).

5.2.3 Familles de courbes

Dans cette sous-section, on aborde le problème de construire des familles de courbes à couplage. La plupart des courbes à couplages utilisées en pratique ont été produites en tant qu'éléments de familles de courbe. Il est intéressant d'étudier les méthodes produisant des familles de courbes car dans de nombreux cas, elles produisent des courbes à couplages dont la valeur-ρ est meilleure que celles des courbes produites par les méthodes de construction de courbes seules, comme la méthode de Cocks–Pinch.

Pour construire des familles de courbes à couplage, on cherche des polynômes Q, R et T à coefficients rationnels tels qu'il existe des entiers $(x_i)_{i\in\mathbb{N}}$ tels que $Q(x_i)$, $R(x_i)$ et $T(x_i)$ satisfassent les conditions du corollaire 55.1 pour tout $i \in \mathbb{N}$.

En particulier, il faut que Q prenne une infinité de valeurs entières premières. Dans l'état actuel des connaissances, nous ne connaissons pas de condition nécessaire et suffisante sur Q (non-triviale) pour que ce soit le cas. On supposera que la conjecture de Bunyakovsky–Schinzel est vraie :

Conjecture 1 (Bunyakovsky–Schinzel)**.** *Soit Q un polynôme de $\mathbb{Q}[Z]$. Alors Q prend des valeurs premières en une infinité d'entiers si et seulement si :*

— *Q est non constant, irréductible et a un coefficient dominant positif.*

— *Q prend une valeur entière en un certain $z \in \mathbb{Z}$.*

— $\text{pgcd}(\{Q(z) \mid z, Q(z) \in \mathbb{Z}\}) = 1$.

On dira qu'un polynôme à coefficients rationnels représente les premiers s'il satisfait les conditions de la conjecture.

Définition 39. Soient $k \geqslant 1$ un entier et D un entier positif non divisible par un carré. Soient Q, R et T des polynômes de $\mathbb{Q}[X]$. On dit que Q, R et T paramétrisent une **famille potentielle** de courbes à couplages (de degré de plongement k et discriminant cryptographique D) si :

1. R est un polynôme non constant, irréductible, dont le coefficient dominant est positif.
2. Il existe un polynôme $H \in \mathbb{Q}[X]$ tel que $HR = Q + 1 - T$.
3. R divise $\Phi_k(T-1)$.
4. Il existe un polynôme $Y \in \mathbb{Q}[X]$ tel que $DY^2 = 4Q - T^2$.

On dit que Q, R et T paramétrisent une **famille** de courbes à couplages si de plus :

5. Q représente les premiers.
6. Q, R, T, Y, H prennent des valeurs entières en un entier commun $x \in \mathbb{Z}$.

On définit la **valeur-ρ** d'une famille de courbes :

$$\rho = \frac{\deg\ Q}{\deg\ R}$$

De cette manière, les valeurs-ρ des courbes de la famille $\frac{\log Q(x)}{\log R(x)}$ convergent vers la valeur-ρ de la famille.

Remarque 29. Dans la suite, on ne considérera que des familles paramétrées par des polynômes. Pour des soucis de concision, on identifiera parfois la famille et les polynômes la paramétrant.

5.2.4 Méthode de Brezing–Weng

Les polynômes paramétrant une famille doivent satisfaire des relations arithmétiques similaires à celles décrites dans le corollaire 55.1. Ainsi, la méthode de Cocks–Pinch se généralise bien à la production de familles de courbes. Brezing et Weng ont formalisé cette

généralisation [BW05]. On reformule leur algorithme avec un point de vue plus proche de l'approche de Kachisa–Schaefer–Scott.

Fixons $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Soit $\mathcal{C}_k$ le k-ième corps cyclotomique dans $\bar{\mathbb{Q}}$ et $\sqrt{-D}$ une racine carrée de $-D$ dans $\bar{\mathbb{Q}}$.

Lemme 56. Soit $\mathcal{K}$ un corps de nombres et θ un élément primitif de $\mathcal{K}$ (i.e. $\mathcal{K} = \mathbb{Q}(\theta)$). Soit ζ un élément de $\mathcal{K}$. Il existe un unique polynôme $T \in \mathbb{Q}[X]$ de degré minimal, tel que :

$$T(\theta) = \zeta \ .$$

On dira que T est le polynôme canonique envoyant θ sur ζ.

Démonstration. Soit R le polynôme minimal de θ. On a un isomorphisme canonique

$$\begin{array}{ccc} \mathbb{Q}[X]/\langle R\rangle & \longrightarrow & \mathcal{K} \\ P \bmod R & \longmapsto & P(\theta) \end{array}$$

Soit $P \in \mathbb{Q}[X]$ tel que $P(\theta) = \zeta$. Alors T est le reste de la division euclidienne de P par R. □

De manière similaire à la méthode de Cocks–Pinch, la méthode de Brezing–Weng (algorithme 5.2.2) consiste à produire des familles potentielles à partir d'un choix de polynôme R, jusqu'à obtenir une famille.

Algorithme 5.2.2 : Méthode de Brezing–Weng
Entrées : $k > 1$ un entier et D un entier positif non divisible par un carré
Output : Q, R, T, Y, H paramétrant une famille de courbes à couplage de discriminant cryptographique D et degré de plongement k

1 Fixer $\mathcal{K} \subset \bar{\mathbb{Q}}$ un corps de nombres contenant $\mathcal{C}_k$ et $\mathbb{Q}(\sqrt{-D})$.
2 Fixer $\theta \in \mathcal{K}$ un élément primitif (i.e. $\mathcal{K} = \mathbb{Q}(\theta)$).
3 Calculer $R \in \mathbb{Q}[X]$ le polynôme minimal de θ.
4 Fixer ζ_k une racine primitive k-ième de l'unité dans $\mathcal{K}$.
5 Déterminer $T \in \mathbb{Q}[X]$ le polynôme canonique envoyant θ sur $\zeta_k + 1$.
6 Déterminer $Y \in \mathbb{Q}[X]$ le polynôme canonique envoyant θ sur $\frac{\zeta_k - 1}{\sqrt{-D}}$.
7 Calculer $Q = (T^2 + DY^2)/4 \in \mathbb{Q}[X]$ et $H = (Q + 1 - T)/R \in \mathbb{Q}[X]$.
8 Si Q représente les premiers et s'il existe un entier z_0 et un rationnel $\lambda > 0$ tels que $Q(z_0)$, $\lambda R(z_0)$, $T(z_0)$, $Y(z_0)$ et $H(z_0)/\lambda$ soient des entiers, renvoyer $(Q, \lambda R, T, Y, H/\lambda)$, sinon reprendre à 1 et changer $\mathcal{K}$, θ ou ζ_k.

Puisque T et Y sont de degrés strictement inférieurs à R, on peut montrer que les familles produites par cette méthode vérifient

$$\rho \leqslant 2 - \frac{2}{\deg\ R}.$$

Généralement, l'égalité est atteinte. Il faut désormais exhiber des polynômes R (ou de manière équivalente des nombres algébriques θ) produisant des familles dont la valeur ρ est significativement plus petite que 2.

Une première technique consiste à remarquer que, lorsque $D = 1$ ou $D = 3$, le corps $\mathcal{C}_k(\sqrt{-D})$ est une extension cyclotomique de $\mathbb{Q}$. Si $D = 1$, resp. $D = 3$, posons $\ell = \mathrm{ppcm}(k, 4)$, resp. $\ell = \mathrm{ppcm}(k, 3)$, et posons $\theta = \zeta_\ell$ une racine primitive ℓ-ième de l'unité dans $\bar{\mathbb{Q}}$. Alors θ peut être utilisé dans la méthode Brezing–Weng. Les premiers à avoir utilisé des polynômes cyclotomiques pour générer des familles de courbes furent Barreto, Lynn et Scott [BLS03], et en parallèle Brezing et Weng [BW05]. Leurs travaux furent repris et étendus par Freeman, Scott et Teske [FST10]. Pour la plupart des degrés de plongement k, les meilleurs familles connues sont issues de ces contributions [FST10, Table 8.2]. Des exceptions notables sont les cas $18 \mid k$ et parfois $k \equiv 4 \bmod 6$.

Kachisa, Schaefer et Scott ont également travaillé dans le corps cyclotomique $\mathcal{C}_\ell$, mais ont procédé par recherche exhaustive sur les paramètres θ et ζ_k [KSS08], dans le but de produire des familles pour les cas problématiques, en particulier $18 \mid k$. Soit ζ_ℓ une racine ℓ-ième de l'unité dans $\mathcal{C}_\ell$. Soient B_1 et B_2 deux entiers positifs. On définit $\mathbf{KSS}(B_1, B_2)$ l'ensemble des éléments primitifs de $\mathcal{C}_\ell$ de la forme

$$P(\zeta_\ell) = \sum_{i=0}^{\varphi(\ell)-1} P_i \zeta_\ell^i,$$

où $P = \sum_{i=0}^{\varphi(\ell)-1} P_i X^i$ est un polynôme à coefficients rationnels tel que

- P a au plus B_1 coefficients non nuls.
- $\forall i \in [0, \varphi(\ell) - 1], \max(\mathrm{num}(|P_i|), \mathrm{denom}(|P_i|)) \leq B_2$, où φ désigne l'indicatrice d'Euler.

Les familles construites par Kachisa, Schaefer et Scott proviennent d'éléments primitifs de $\mathcal{C}_\ell$ dans $\mathbf{KSS}(2, 3)$.

À une poignée d'exceptions près, les familles obtenues par les deux méthodes précédentes sont les familles avec les plus petites valeurs-ρ connues [FST10, Table 8.2].

5.3 La nouvelle méthode

Dans cette section, on présente une amélioration et généralisation de la méthode de Kachisa, Schaefer et Scott. L'idée de cette construction réside dans l'identification d'une famille de nombres algébriques produisant des familles potentielles dont la valeur-ρ est majorée. On présente également de nouvelles familles de courbes produites avec cette nouvelle méthode. Une implémentation Sagemath [The22] de la méthode est disponible [Gas23]. Cette section contient mes apports personnels à l'article [GG25], co-écrit avec Aurore Guillevic.

5.3.1 Présentation de la méthode

Fixons $k > 1$ et D un entier positif non divisible par un carré. Soit $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$, soit $\mathcal{C}_k$ le k-ième corps cyclotomique dans $\bar{\mathbb{Q}}$, et soit $\sqrt{-D}$ une racine carrée de $-D$ dans $\bar{\mathbb{Q}}$. On définit les corps de nombres $\mathcal{F} = \mathbb{Q}(\sqrt{-D})$ et $\mathcal{K} = \mathcal{F}\mathcal{C}_k \subset \bar{\mathbb{Q}}$.

Soient θ un élément primitif de $\mathcal{K}$ (i.e. $\mathcal{K} = \mathbb{Q}(\theta)$) et ζ_k une racine primitive k-ième de l'unité. En appliquant les étapes 5 à 7 de l'algorithme 5.2.2 à θ et ζ_k, on obtient les polynômes Q, R et T d'une famille potentielle. On définit

$$\rho(\theta, \zeta_k) = \frac{\deg\ Q}{\deg\ R}$$

la valeur-ρ de cette famille potentielle.

Soit $\mathcal{S}$ un ensemble d'éléments primitifs de $\mathcal{K}$. On définit

$$\rho(\mathcal{S}, \zeta_k) = \max_{\theta \in \mathcal{S}} \rho(\theta, \zeta_k)\ .$$

Cette quantité désigne la pire valeur-ρ d'une famille potentielle provenant d'un élément de $\mathcal{S}$. En particulier, si cette valeur est petite, tous les éléments de $\mathcal{S}$ produisent des familles potentielles de petite valeur-ρ.

On peut voir $\mathcal{K}$ comme un $\mathcal{F}$-espace vectoriel. Soit $\mathcal{F}\zeta_k$ la $\mathcal{F}$-droite vectorielle dans $\mathcal{K}$ engendré par ζ_k.

$$\mathcal{F}\zeta_k = \{\alpha\zeta_k; \alpha \in \mathcal{F}\} = \{(a + b\sqrt{-D})\zeta_k; a, b \in \mathbb{Q}\}.$$

Soit $\theta \in \mathcal{F}\zeta_k$, supposons que θ est un élément primitif de $\mathcal{K}$ (sur $\mathbb{Q}$). Soit R le polynôme minimal de θ (sur $\mathbb{Q}$). On pose

$$\alpha = \theta/\zeta_k \in \mathcal{F}.$$

Soit e le plus petit diviseur entier de k tel que $\zeta_k^e \in \mathcal{F}$. Alors $\theta^e \in \mathcal{F}$. Supposons que θ^e est un élément primitif de $\mathcal{F}$.

Remarque 30. L'hypothèse que θ^e est primitif n'est pas très restrictive.

Puisque $\alpha, \sqrt{-D} \in \mathcal{F}$, il existe P_1, P_2 et P_3, trois polynômes à coefficients rationnels, de degré au plus 1 tels que :

$$\begin{aligned} P_1(\theta^e) &= 1/\alpha, \\ P_2(\theta^e) &= 1/(\alpha\sqrt{-D}), \\ P_3(\theta^e) &= 1/\sqrt{-D}. \end{aligned}$$

Alors on a

$$P_1(\theta^e)\theta + 1 = \theta/\alpha + 1 = \zeta_k + 1$$

et

$$P_2(\theta^e)\theta - P_3(\theta^e) = \zeta_k/\sqrt{-D} - 1/\sqrt{-D} = (\zeta_k - 1)/\sqrt{-D}\ .$$

Soit T le polynôme canonique envoyant θ sur $\zeta_k + 1$, et soit Y le polynôme canonique envoyant θ sur $(\zeta_k - 1)/\sqrt{-D}$. Alors T est le reste de la division euclidienne de $P_1(X^e)X + 1$ par R. Ainsi, on a

$$\deg T \leqslant \deg(P_1(X^e)X + 1) \leqslant e + 1 \ .$$

Similairement, on a $\deg Y \leqslant \deg(P_2(X^e)X - P_3(X^e)) \leqslant e + 1$. En conséquence

$$\max(\deg T, \deg Y) \leqslant e + 1 \ .$$

Soit $Q = (T^2 + DY^2)/4$, alors

$$\deg Q \leq 2e + 2 \ .$$

Ainsi, puisque $\deg R = [\mathcal{K} : \mathbb{Q}]$, on a

$$\rho(\theta, \zeta_k) \leqslant \frac{2e + 2}{[\mathcal{K} : \mathbb{Q}]} \ .$$

De plus, si $\frac{2e+2}{[\mathcal{K}:\mathbb{Q}]} < 2$, ou de manière équivalente si $e + 1 < \deg R$, on a

$$T = P_1(X^e)X + 1 \text{ and } Y = P_2(X^e)X - P_3(X^e).$$

Dès lors, puisque α et $\alpha\sqrt{-D}$ ne peuvent pas être rationnels simultanément, P_1 ou P_2 doit être de degré 1. Alors T ou Y doit être de degré $e + 1$. Ainsi, on obtient l'égalité

$$\rho(\theta, \zeta_k) = \frac{2e + 2}{[\mathcal{K} : \mathbb{Q}]} \ .$$

Théorème 57. *Avec les notations du début de la sous-section 5.3.1, soit*

$$\mathcal{S} = \{\theta \in \mathcal{F}\zeta_k \text{ primitif dans } \mathcal{K} \mid \theta^e \text{ est primitif dans } \mathcal{F}\}.$$

Alors si $\frac{2e+2}{[\mathcal{K}:\mathbb{Q}]} < 2$, *on a*

$$\rho(\mathcal{S}, \zeta_k) = \frac{2e + 2}{[\mathcal{K} : \mathbb{Q}]}.$$

Remarque 31. Cette construction est facilement généralisable au cas où $\mathcal{F}$ est une extension de $\mathbb{Q}(\sqrt{-D})$. Alors P_1,P_2,P_3 ont un degré d'au plus $[\mathcal{F} : \mathbb{Q}] - 1$ et la borne sur les valeurs-ρ devient :

$$\rho(\mathcal{S}, \zeta_k) \leqslant \frac{2e([\mathcal{F} : \mathbb{Q}] - 1) + 2}{[\mathcal{K} : \mathbb{Q}]}.$$

Cette généralisation ne produit pas de meilleurs résultats.

On donne des bornes plus explicites pour $\rho(\mathcal{S}, \zeta_k)$.

Théorème 58. *Avec les notations du Théorème 57, et où φ désigne l'indicatrice d'Euler, supposons que* $\frac{2e+2}{[\mathcal{K}:\mathbb{Q}]} < 2$. *Alors :*

1. *Supposons que k est un multiple de 6 et $D = 3$. Alors $e = k/6$ et*

$$\rho(\mathcal{S}, \zeta_k) = \frac{(k/3 + 2)}{\varphi(k)}.$$

2. *Supposons que k est un multiple de 4 et $D = 1$. Alors $e = k/4$ et*

$$\rho(\mathcal{S}, \zeta_k) = \frac{(k/2 + 2)}{\varphi(k)}.$$

3. *Supposons que k est un multiple de 3 et $D = 3$. Alors $e = k/3$ et*

$$\rho(\mathcal{S}, \zeta_k) = \frac{(2k/3 + 2)}{\varphi(k)}.$$

4. *Supposons que k est pair et $\sqrt{-D} \notin \mathcal{C}_k$. Alors $e = k/2$ et*

$$\rho(\mathcal{S}, \zeta_k) = \frac{(k/2 + 1)}{\varphi(k)}.$$

5. *Supposons que k est impair et $\sqrt{-D} \notin \mathcal{C}_k$. Alors $e = k$ et*

$$\rho(\mathcal{S}, \zeta_k) = \frac{(k + 1)}{\varphi(k)}.$$

Démonstration. On se contente de prouver le cas 4 en guise d'exemple. Supposons que k est pair et $\sqrt{-D} \notin \mathcal{C}_k$. Alors $[\mathcal{K} : \mathbb{Q}] = 2\varphi(k)$ puisque $\mathcal{K}$ est une extension quadratique de $\mathcal{C}_k$. Prouvons que $e = k/2$. Puisque $\sqrt{-D} \notin \mathcal{C}_k$, alors ζ_k^e n'est pas primitif dans $\mathcal{F}$ (sinon $\mathcal{F} \subset \mathcal{C}_k$), et $\mathcal{F}$ est quadratique, donc ζ_k^e est rationnel. Donc $\zeta_k^e \in \{1, -1\}$, car ζ_k^e est une racine de l'unité. Puisque k est pair, $e = k/2$ et $\zeta_k^e = -1$. Ainsi,

$$\rho(\mathcal{S}, \zeta_k) = \frac{2e + 2}{[\mathcal{K} : \mathbb{Q}]} = \frac{k + 2}{2\varphi(k)} = \frac{k/2 + 1}{\varphi(k)}.$$

□

Dans la suite, on appellera *méthode du sous-corps* la méthode de génération de familles de courbes via une recherche exhaustive sur les entiers algébriques dans $\mathcal{S}$. Notons que considérer des entiers algébriques uniquement n'est pas très restrictif, car il est possible d'obtenir le reste des familles potentielles en appliquant des changements de variables affines (sur $\mathbb{Q}$) aux polynômes obtenus.

Remarque 32. Notons que lorsque $D = 1$ ou $D = 3$, pour certaines valeurs de k, tout élément de l'ensemble $\mathcal{S}$ est un élément de $\mathbf{KSS}(2, B)$ pour un B suffisamment grand. Plus précisément, posons $\ell = \mathrm{ppcm}(k, 4)$ si $D = 1$ ou $\ell = \mathrm{ppcm}(k, 3)$ si $D = 3$. Soit ζ_ℓ une racine primitive ℓ-ième de l'unité de $\mathcal{C}_\ell$. Alors $\zeta_k := \zeta_\ell^{\ell/k}$ est une racine primitive k-ième de l'unité.

De plus, il existe $d \in \{3,4,6\}$ maximal tel que $\zeta_d := \zeta_\ell^{\ell/d} \in \mathcal{F}$ est une racine de l'unité irrationnelle de $\mathcal{F} = \mathbb{Q}(\sqrt{-D})$. Alors, pour tout $\theta \in \mathcal{S}$, il existe deux nombres rationnels a et b tels que

$$\theta = (a\zeta_d + b)\zeta_k = (a\zeta_\ell^{\ell/d} + b)\zeta_\ell^{\ell/k}.$$

Si $\ell/d + \ell/k < \varphi(\ell)$ alors $\theta \in \cup_{B>0} \mathbf{KSS}(2, B)$. En particulier, on peut démontrer que cette inégalité est vraie pour $k \in \{16, 18, 32, 36, 40\}$, les degrés de plongement des familles KSS. On peut remarquer que les éléments générant les familles KSS proviennent de $\mathcal{S}$. De cette façon, on peut voir la méthode du sous-corps comme une amélioration de la recherche exhaustive de Kachisa, Schaefer et Scott. Cela implique que, dans ce cas, il est possible de générer les familles produites par la méthode du sous-corps avec la méthode KSS, au prix d'une recherche exhaustive plus longue. Cependant, si $D \notin \{1,3\}$, la méthode du sous-corps est une stricte généralisation de la méthode KSS.

5.3.2 Les résultats

L'intérêt de la méthode du sous-corps dépend de la capacité à satisfaire ces conditions :

1. la méthode produit des familles potentielles de valeurs-ρ inférieures ou égales aux valeurs de référence de la première colonne de [FST10, Table 8.2].
2. la méthode produit des familles parmi les familles potentielles.
3. les familles produites par la méthode permettent de générer des courbes à couplages pour le niveau de sécurité désiré.

Pour la condition 3, il peut arriver que la famille permette seulement de générer des courbes à couplages dont les paramètres q et r sont trop grands comparés aux tailles requises pour garantir le niveau de sécurité souhaité. Cela peut se produire lorsque les dénominateurs des polynômes Q, R et T paramétrant la famille sont élevés.

Dans la suite, nous allons présenter de nouvelles familles de courbes, produites par la méthode du sous-corps, générant des courbes adaptées au niveau de sécurité de 192 bits. Ainsi, les trois conditions précédentes sont remplies.

Supposons que $k \notin \{2,3,4,6,12\}$, alors les familles potentielles produites par la méthode du sous-corps ont des valeurs-ρ au moins aussi petites que les valeurs de référence de [FST10, Table 8.2]. Les degrés de plongement pour lesquelles les valeurs-ρ sont améliorées sont compilés dans la table 5.1. Une valeur en gras signale une amélioration, tandis qu'une case verte indique qu'il est possible de trouver des familles parmi les familles potentielles produites par mon implémentation Sagemath de la méthode [Gas23].

On donne deux familles de degrés de plongement $k = 22$ et $k = 28$ dont les dénominateurs ne sont pas trop importants et dont les valeurs-ρ sont inférieures strictement aux valeurs de référence :

Exemple 6 (Famille GG22 [GG25]). Soit $k = 22$ et $D = 7$. Fixons une clôture algébrique de $\mathbb{Q}$ et $\sqrt{-7}$ une racine carrée de -7. Soit $\mathcal{F} = \mathbb{Q}(\sqrt{-7})$. Soit $\mathcal{K} = \mathcal{F}\mathcal{C}_{22}$. Soit ζ_{22} une racine primitive 22-ième de l'unité, et soit $\omega = \frac{1+\sqrt{-7}}{2}$. On a $\mathcal{K} = \mathbb{Q}(\omega, \zeta_{22})$.

k	$\rho, D=1$	$\rho, D=3$	$\rho, \sqrt{-D} \notin \mathcal{C}_k$	ρ, Méthode précédente
16	1.250	1.125	**1.125**	1.250, [FST10, 6.11]
22	**1.200**	**1.200**	**1.200**	1.300, [FST10, 6.3]
28	1.333	1.250	**1.250**	1.333, [FST10, 6.4]
40	1.375	1.3125	**1.3125**	1.375, [FST10, 6.15]
46	1.091	1.091	**1.091**	1.136, [FST10, 6.3]

TABLE 5.1 – Comparaison des valeurs-ρ des familles potentielles produites par la méthode du sous-corps avec les valeurs de référence [FST10].

Soit $\alpha = 1+\omega$ et $\theta = \alpha\zeta_{22}$. On a $\zeta_{22}^{11} \in \mathcal{F}$, et $\theta^{11} \notin \mathbb{Q}$. Donc, $\mathbb{Q}(\theta^{11}) = \mathcal{F}$, et $\theta \in \mathcal{S}$. Mon implémentation Sagemath de la méthode du sous-corps [Gas23] donne :

— $T = (X^{12} + 45X + 46)/46$

— $Y = (X^{12} - 4X^{11} - 47X - 134)/322$

— $R = (X^{20} - X^{19} - X^{18} + 3X^{17} - X^{16} - 5X^{15} + 7X^{14} + 3X^{13} - 17X^{12} + 11X^{11} + 23X^{10} + 22X^9 - 68X^8 + 24X^7 + 112X^6 - 160X^5 - 64X^4 + 384X^3 - 256X^2 - 512X + 1024)/23$

— $Q = (X^{24} - X^{23} + 2X^{22} + 67X^{13} + 94X^{12} + 134X^{11} + 2048X^2 + 5197X + 4096)/7406$

La famille générée par θ a une valeur-ρ de $6/5$. Cette valeur-ρ est inférieure à la valeur de référence de $13/10$ pour $k = 22$.

Exemple 7. Soit $k = 28$, $D = 11$, $\omega = (-1+\sqrt{-11})/2$, $\alpha = \omega$, $\theta = \alpha\zeta_{28}$. On obtient :

— $T = (X^{15} + 718X + 3237)/3237$

— $Y = (X^{15} + 6X^{14} + 7192X + 7545)/35607$

— $R = (X^{24} + 5X^{22} + 16X^{20} + 35X^{18} + 31X^{16} - 160X^{14} - 1079X^{12} - 1440X^{10} + 2511X^8 + 25515X^6 + 104976X^4 + 295245X^2 + 531441)/(3^{12} \cdot 13^2 \cdot 83^2)$

— $Q = (X^{30} + X^{29} + 3X^{28} + 2515X^{16} + 14384X^{15} + 7545X^{14} + 4782969X^2 + 13304911X + 14348907)/38419953$

La valeur-ρ de cette famille est $5/4$ et améliore le précédent record à $4/3$.

La famille GG22 de l'exemple 6 a un intérêt cryptographique pour des situations particulières et a été étudiée dans [AFG24, LZZ24] suite à la rédaction d'un article sur cette nouvelle méthode.

Un dernier intérêt de la nouvelle méthode réside dans sa capacité à générer de nombreuses familles alternatives aux familles connues et de qualité équivalente. Cela permet d'éviter les attaques spécifiques à une famille. Ainsi, dans [AFG24], les auteurs considèrent une courbe de degré de plongement $k = 20$ produite par la méthode du sous-corps au lieu de l'ancienne courbe de [FST10, Construction 6.4].

On donne en annexe la liste des familles alternatives produites par la méthode du sous-corps (sous-section 6.1.1). On donne également une liste d'entiers $x \in \mathbb{Z}$ permettant de

générer des courbes pour le niveau de sécurité 192-bits pour certaines des nouvelles familles (sous-section 6.1.2).

5.4 Algorithme pour trouver les racines d'un polynôme modulo une puissance de premier

Soient Q, R et T des polynômes à coefficients rationnels paramétrant une famille potentielle de courbes à couplages. On se pose la question de démontrer que Q, R et T paramétrisent une famille de courbes. Pour cela, on doit montrer que Q représente les premiers et que les polynômes ont des valeurs entières en un même $x \in \mathbb{Z}$ (notons que cela implique qu'il existe une infinité de tels entiers x).

Pour vérifier ces deux conditions, il suffit d'être capable de :

— calculer à quels entiers un polynôme à coefficients rationnels prend des valeurs entières.

— calculer le PGCD des valeurs entières d'un polynôme à coefficients rationnels.

Prenons pour l'exemple le polynôme Q. Soit Δ le dénominateur de Q, i.e. le plus petit entier positif tel que $\Delta Q \in \mathbb{Z}[X]$. Soit $x \in \mathbb{Z}$, alors

$$Q(x) \in \mathbb{Z} \Leftrightarrow \Delta Q(x) \equiv 0 \bmod \Delta.$$

On peut donc connaître les entiers auxquels Q prend des valeurs entières en calculant les racines de ΔQ modulo p^n, pour tout p^n apparaissant dans la décomposition de Δ en facteurs premiers, si celle-ci est connue.

Supposons que les entiers auxquels Q prend des valeurs entières sont connus. Soit α le PGCD de quelques valeurs entières de Q. Si $\alpha = 1$, alors le PGCD des valeurs entières de Q est 1. Sinon, pour tout premier p divisant α, on se demande si p divise les valeurs entières de Q. On a

$$\forall x \in \mathbb{Z} \text{ tel que } Q(x) \in \mathbb{Z}, Q(x) \equiv 0 \bmod p \Leftrightarrow \Delta Q(x) \equiv 0 \bmod p\Delta.$$

Il suffit donc de comparer l'ensemble des racines de ΔQ modulo Δ et modulo $p\Delta$.

Il reste à expliquer comment, étant donné $P \in \mathbb{Z}[X]$, p un entier premier, et $n > 0$ un entier, calculer l'ensemble des entiers x tels que

$$P(x) \equiv 0 \bmod p^n. \tag{5.4.1}$$

L'approche classique pour résoudre ce problème est de résoudre d'abord

$$P(x) \equiv 0 \bmod p$$

puis de relever les solutions modulo p^n. Le lemme de Hensel [Ser78] détaille comment relever les racines simples modulo p en une unique racine modulo p^n. Cependant, le relèvement des racines multiples est moins étudié. Dans cette section, on donne un algorithme général pour résoudre de telles équations. On commence par présenter une manière appropriée de

représenter l'ensemble des solutions entières de l'équation (5.4.1) dans la sous-section 5.4.1. Dans la sous-section 5.4.2, on présente une fonction μ utilisée dans l'algorithme final, et on explique comment la calculer. Enfin, l'algorithme final est présenté dans la sous-section 5.4.3.

Pour toute la section, on fixe un polynôme $P \in \mathbb{Z}[X]$, un premier p et un entier $n > 0$.

5.4.1 La représentation des solutions

Nous utiliserons des classes de congruences pour décrire l'ensemble des solutions entières de $P(x) \equiv 0 \bmod p^n$.

Définition 40. Soit a un entier et soit $j \geqslant 0$ un entier. On définit

$$D(a, j) = \{x \in \mathbb{Z} \mid x \equiv a \bmod p^j\}$$

la classe de p-congruence de a modulo p^j.

On rappelle la propriété élémentaire suivante :

Proposition 59. Soient a_1, a_2 deux entiers et soit j_1, j_2 deux entiers positifs tels que $j_1 \leqslant j_2$. Définissons $D(a_1, j_1)$ et $D(a_2, j_2)$ comme dans la définition 40. Supposons que

$$D(a_1, j_1) \cap D(a_2, j_2) \neq \emptyset.$$

Alors

$$D(a_2, j_2) \subset D(a_1, j_1).$$

Démonstration. Soit $x \in D(a_1, j_1) \cap D(a_2, j_2)$ un entier. Alors

$$x \equiv a_1 \bmod p^{j_1} \text{ and } x \equiv a_2 \bmod p^{j_2}.$$

Puisque $j_1 \leqslant j_2$, on a

$$x \equiv a_2 \bmod p^{j_1}.$$

Ainsi,

$$a_2 \equiv a_1 \bmod p^{j_1} \text{ and } D(a_2, j_2) \subset D(a_1, j_1).$$

□

Maintenant, fixons un ensemble p^n-périodique $S \subset \mathbb{Z}$.

Définition 41. Une représentation par classes de p-congruence de S est une collection de classes de p-congruence $(D(a_i, j_i))_{i \in I}$ telle que

$$S = \cup_{i \in I} D(a_i, j_i).$$

On dit que la représentation par classes de p-congruence est finie si I l'est.

Remarque 33. S possède toujours une représentation par classes de p-congruence finie, car S est p^n-périodique. Ainsi

$$S = \cup_{a \in S \cap [0, p^n - 1]} D(a, n).$$

On souhaite définir une représentation par classes de p-congruence canonique. Une première étape consiste à demander que les classes $(D(a_i, j_i))_{i \in I}$ soient disjointes, mais ce n'est pas suffisant. En effet, soit a un entier et $j \geqslant 0$ un entier positif. Alors

$$D(a, j) = \cup_{i=0}^{p-1} D(a + i \cdot p^j, j + 1)$$

et l'union du membre de droite est disjointe. C'est le seul autre obstacle à la définition d'une représentation canonique.

Définition 42. Soit C une classe de p-congruence dans S. On dit que C est maximale si elle est maximale pour l'inclusion parmi les classes de p-congruence dans S.

D'après la proposition 59, l'ensemble S est l'union disjointe de ses classes de p-congruence maximales. On appelle la représentation de S composée de ses classes de p-congruence maximales la **représentation réduite** de S.

5.4.2 La fonction μ

Rappellons que nous voulons calculer l'ensemble

$$S = \{x \in \mathbb{Z} \mid P(x) \equiv 0 \bmod p^n\}. \tag{5.4.2}$$

Puisque S est p^n-périodique, on demande en plus de calculer une représentation par classes de p-congruence réduite de S. Le contenu de cette sous-section permettra d'atteindre cet objectif dans la prochaine sous-section.

On définit

$$\mu(P) = \sup\{j \in \mathbb{Z}_{\geq 0} \mid \forall x \in \mathbb{Z}, P(x) \equiv 0 \bmod p^j\}\ . \tag{5.4.3}$$

Exemple 8. On donne deux exemples jouets pour $p = 2$:

— soit $P = X^2 + 3$. On remarque que $P(0) = 3 \not\equiv 0 \bmod 2$. Alors $\mu(P) = 0$.

— soit $P = X^2 - X$. Puisque pour tout entier x, soit x est pair soit $x - 1$ l'est, alors $P(x)$ est pair. On peut montrer que $\mu(P) = 1$.

On peut remarquer que $S = \mathbb{Z}$ si et seulement si $\mu(P) \geqslant n$. De manière générale, on peut utiliser la fonction μ pour tester si une classe de p-congruence est incluse dans S.

Proposition 60. Soit $n > 0$ un entier positif, soit $P \in \mathbb{Z}[X]$, et p un premier. Soit S et μ comme dans les équations (5.4.2) et (5.4.3). Soit a un entier et soit $j \geqslant 0$ un entier positif. On définit $D(a, j)$ comme dans la définition 40. Alors

$$\mu(P(a + p^j X)) \geq n \text{ si et seulement si } D(a, j) \subset S.$$

Démonstration.

$$\begin{aligned}\mu(P(a+p^jX)) \geq n &\Leftrightarrow \forall b \in \mathbb{Z}, P(a+p^jb) \equiv 0 \bmod p^n \\ &\Leftrightarrow \forall x \in D(a,j), P(x) \equiv 0 \bmod p^n \\ &\Leftrightarrow D(a,j) \subset S.\end{aligned}$$

□

Pour pouvoir vérifier si une classe de p-congruence est incluse dans S, il suffit de savoir évaluer μ. On donne une méthode pour évaluer μ dans le théorème suivant.

Théorème 61. *Soit $P \in \mathbb{Z}[X]$ et p un premier. Soit μ la fonction définie dans l'équation (5.4.3). Soient $a_0, a_1, \ldots, a_{\deg P}$ des entiers tels que*

$$P = \sum_{i=0}^{\deg P} a_i \binom{X}{i}$$

où

$$\binom{X}{i} = \frac{X(X-1)\ldots(X-i+1)}{i!}.$$

Alors

$$\mu(P) = \min_{0 \leq i \leq \deg P} (\mathrm{val}_p(a_i)).$$

Démonstration. Un résultat connu dit que $(\binom{X}{i})_{i \in \mathbb{Z}}$ est une $\mathbb{Z}$-base du groupe abélien des polynômes à valeurs entières. Puisque P est à valeurs entières, il existe de tels $a_0, a_1, \ldots, a_{\deg P}$.

Soit $m = \min_{0 \leq i \leq \deg P} (\mathrm{val}_p(a_i))$. Il est clair que

$$\mu(P) \geq m.$$

Soit $0 \leq i_0 \leq \deg P$ le plus petit entier tel que

$$\mathrm{val}_p(a_{i_0}) = m.$$

Alors

$$\begin{aligned}P(i_0) &= \sum_{i=0}^{\deg P} a_i \binom{i_0}{i} \\ &= \sum_{i=0}^{i_0} a_i \binom{i_0}{i} \\ &\equiv a_{i_0} \binom{i_0}{i_0} \bmod p^{n+1} \text{ par minimalité de } i_0 \\ &\equiv a_{i_0} \bmod p^{m+1} \\ &\not\equiv 0 \bmod p^{m+1}.\end{aligned}$$

Ainsi,

$$\mu(P) \leq m.$$

□

5.4.3 L'algorithme

On donne un algorithme récursif pour calculer une représentation réduite de l'ensemble S des solutions entières de

$$P(x) \equiv 0 \bmod p^n.$$

L'idée de l'algorithme est en réalité assez directe. On calcule $\mu(P)$ pour vérifier si $\mu(P) \geqslant n$. Si la réponse est oui, on sait que $S = \mathbb{Z}$. Sinon, on cherche récursivement des solutions dans les classes de congruence modulo p en utilisant des changements de variables.

Avant de présenter l'algorithme 5.4.1, rappelons le lemme suivant.

Lemme 62. Soit $P \in \mathbb{Z}[X]$, soit p un premier et soit a un entier. Alors

$$P(a) \equiv 0 \bmod p$$

si et seulement si

$$p \mid P(a + pX), \text{ i.e. } \frac{P(a + pX)}{p} \in \mathbb{Z}[X].$$

Démonstration. Il existe $Q \in \mathbb{Z}[X]$ tel que

$$P(a + X) = P(a) + X \cdot Q(X).$$

Ainsi,

$$P(a + pX) = P(a) + pX \cdot Q(pX),$$

dont on déduit le lemme. □

L'algorithme 5.4.1 est donné ci-dessous. On peut facilement vérfier que l'algorithme termine car la variable n décroît strictement dans l'arbre de récursion, et est minorée par 0. La correction vient de la proposition 60 et de l'observation que si

$$P(a) \not\equiv 0 \bmod p$$

alors

$$\forall x \equiv a \bmod p, P(x) \not\equiv 0 \bmod p.$$

Remarque 34. J'ai présenté l'algorithme dans le but d'être le plus clair possible. Cet algorithme peut être amélioré de plusieurs façons. D'abord, plutôt que de tester si $P(a) \equiv 0 \bmod p$ pour tout a modulo p, il est préférable d'utiliser l'algorithme de Berlekamp pour calculer les racines de P modulo p. Ensuite, pour diminuer la profondeur de l'arbre de récursion, il faut diviser $P(a + pX)$ par la plus grande puissance de p possible. Enfin, il est préférable d'utiliser le lemme d'Hensel dès que cela est possible dans la récursion. L'algorithme est implémenté avec ces améliorations dans [Gas23].

Algorithme 5.4.1 : RootsModPrimePowers(P, p, n)

Entrées : $P \in \mathbb{Z}[X]$, p un premier, $n > 0$ un entier

si $\mu(P) \geqslant n$ **alors**
  Renvoyer $D(0, 0)$.
sinon
  $S \leftarrow \emptyset$
  pour $0 \leqslant a \leqslant p - 1$ **faire**
    si $P(a) \equiv 0 \bmod p$ **alors**
      $Q \leftarrow P(a + pX)/p$
      $\cup_{i \in I} D(a_i, j_i) \leftarrow$ RootsModPrimePowers$(Q, p, n - 1)$
      $S \leftarrow \cup_{i \in I} D(a + p \cdot a_i, j_i + 1) \cup S$
  Renvoyer S.

Chapitre 6

Annexe

6.1 Nouvelles courbes à couplages

Dans cette section, on liste quelques productions supplémentaires de la nouvelle méthode de génération de familles de courbes à couplages de la section 5.3.1. On donne dans la sous-section 6.1.1 les familles produites par cette nouvelle méthode, dont la valeur-ρ n'améliore pas les précédents records, mais qui ont un intérêt cryptographique pour les raisons données dans la section 5.3.2. On donne dans la sous-section 6.1.2 des entiers permettant de générer de nouvelles courbes à couplage pour le niveau de sécurité 192 bits avec nos nouvelles familles.

6.1.1 Familles alternatives

On donne quelques exemples de nouvelles familles de courbe à couplages.

Exemple 9 (GG20a). Soit $k = 20$, et $D = 1$. Soit $\theta = (1 - 2\sqrt{-1})\zeta_{20}$. Alors

- $T = (2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 - 44X - 190)/205$
- $R = (X^8 + 4X^7 + 11X^6 + 24X^5 + 41X^4 + 120X^3 + 275X^2 + 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} + 76X^7 + 176X^6 + 380X^5 + 3125X^2 + 12938X + 15625)/33620$

est une famille de courbes à couplages de degré de plongement $k = 20$ et discriminant cryptographique $D = 1$.

Exemple 10 (GG20b). Soit $k = 20$, soit $D = 1$, soit $\theta = (1 + 2\sqrt{-1})\zeta_{20}$. Alors

- $T = (-2X^6 + 117X + 205)/205$
- $Y = (X^6 - 5X^5 + 44X + 190)/205$
- $R = (X^8 - 4X^7 + 11X^6 - 24X^5 + 41X^4 - 120X^3 + 275X^2 - 500X + 625)/25625$
- $Q = (X^{12} - 2X^{11} + 5X^{10} - 76X^7 - 176X^6 - 380X^5 + 3125X^2 + 12938X + 15625)/33620$

est une famille de courbes à couplages de degré de plongement $k = 20$ et discriminant cryptographique $D = 1$.

Exemple 11 (GG28). Soit $k = 28$, soit $D = 1$, soit $\theta = (1 + 2\sqrt{-1})\zeta_{28}$. Alors

— $T = (-2X^8 - 527X + 145)/145$

— $Y = (X^8 - 5X^7 + 336X - 1390)/145$

— $R = (X^{12} + 4X^{11} + 11X^{10} + 24X^9 + 41X^8 + 44X^7 - 29X^6 + 220X^5 + 1025X^4 + 3000X^3 + 6875X^2 + 12500X + 15625)/29$

— $Q = (X^{16} - 2X^{15} + 5X^{14} + 556X^9 - 1344X^8 + 2780X^7 + 78125X^2 - 217382X + 390625)/16820$

est une famille de courbes à couplages de degré de plongement $k = 28$ et discriminant cryptographique $D = 1$.

6.1.2 Nouvelles courbes

On donne des entiers permettant de générer des courbes à couplages à partir de certaines nouvelles familles.

famille de courbes	générateur $x \in \mathbb{Z}$	$\log q$	$\log r$	ρ	$\log q^k$	sécu K_r^*
GG20a	$-(2^{49} + 2^{46} + 2^{41} + 2^{18} + 2^3 + 2^2 + 1)$	576	379	1.52	11520	196
GG20a	$2^{49} + 2^{46} + 2^{44} + 2^{40} + 2^{34} + 2^{27} + 2^{14} + 1$	576	380	1.52	11500	196
GG20b	$-2^{49} - 2^{45} - 2^{42} - 2^{36} + 2^{11} + 1$	575	379	1.52	11500	196
GG20b	$-2^{49} + 2^{46} - 2^{41} + 2^{35} + 2^{30} - 1$	575	379	1.52	11500	196
GG20b	$-2^{49} - 2^{47} + 2^{45} - 2^{27} - 2^{22} - 2^{18} - 1$	576	380	1.52	11520	196
GG22D7	$-2^{19} - 2^{17} - 2^{15} - 2^{13} - 2^7 + 1$	453	380	1.19	9966	220
GG22D7	$-2^{20} + 2^{18} + 2^{14} + 2^{12} + 2^{10} - 2^8 - 2^5 + 1$	457	382	1.20	10054	220
GG22D7	$-2^{20} + 2^{18} + 2^{13} - 2^{10} - 2^8 - 2^2 + 1$	457	383	1.19	10054	220

TABLE 6.1 – Paramètres de nouvelles courbes pour le niveau de sécurité 192-bits.

6.2 Générateurs aléatoires dans un groupe abélien

L'objectif de cette partie est de démontrer le corollaire 63.1 et le théorème 64. Ces théorèmes majorent la probabilité de ne pas engendrer un groupe abélien fini en tirant au sort uniformément un nombre donné d'éléments. On utilise ces théorèmes par exemple pour trouver un ensemble de générateurs de la jacobienne d'une courbe projective lisse sur un corps fini (voir section 2.2.3).

Soit G un groupe abélien fini.

Définition 43. On appelle **facteurs invariants** de G les entiers $d_1 | \dots | d_r$ tels que :

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

Nous allons étudier le nombre d'éléments qu'il est nécessaire de tirer au sort uniformément dans G pour le générer entièrement avec probabilité d'échec inférieure à $1/2^n$, pour n un entier. On peut commencer par observer que la probabilité que k éléments $g_1, \ldots, g_k$ soient contenus dans un sous-groupe maximal H de G est $1/[G : H]^k \leqslant 1/2^k$. Dès lors, la probabilité que k éléments n'engendrent pas G est majorée par $\#\{H \text{ sous-groupe maximal de } G\}/2^k$. Or tout sous-groupe maximal correspond à un unique caractère de G dont il est le noyau. Puisque le nombre de caractères de G est borné par $|G|$, on a :

$$\mathbb{P}(\langle g_1, \ldots, g_k\rangle \subsetneq G) \leqslant |G|/2^k$$

En particulier, pour que $\mathbb{P}(\langle g_1, \ldots, g_k\rangle \subsetneq G) \leqslant 1/2^n$, il suffit que $k \geqslant \lceil \log |G| \rceil + n$. Cette borne a de bonnes propriétés asymptotiques, car on voit que tirer un élément supplémentaire divise la probabilité d'échec par 2. Cependant, le terme $\lceil \log |G| \rceil$ la rend peu intéressante lorsque $n = o(\log |G|)$, car elle ne tient pas compte de la structure du groupe. Par exemple, si G est un ℓ-groupe cyclique, pour ℓ un premier, le nombre attendu d'éléments de G à tirer uniformément pour générer G est $\ell/(\ell - 1)$.

Génération aléatoire des ℓ-groupes

On commence par s'intéresser au cas des ℓ-groupes. Soit ℓ un premier. Soit G un ℓ-groupe abélien fini, et soit r le nombre de facteurs invariants de G. On sait qu'il faut au minimum r éléments de G pour le générer en entier. De plus, des éléments $g_1, \ldots, g_r$ de G engendrent G si et seulement si [Pom01] :

$$\forall 1 \leqslant i \leqslant r, g_i \neq 0 \bmod \ell G + \langle g_1, \ldots, g_{i-1}\rangle.$$

Ainsi, pour $1 \leqslant i \leqslant r$, soient $g_1, \ldots, g_{i-1}$ des éléments de G vérifiant la condition précédente, et soit g_i tiré uniformément dans G, alors

$$\mathbb{P}\left(g_i \neq 0 \bmod \ell G + \langle g_1, \ldots, g_{i-1}\rangle\right) = \frac{\ell^{r-i+1} - 1}{\ell^{r-i+1}} = 1 - \frac{1}{\ell^{r-i+1}}$$

car $G/(\ell G + \langle g_1, \ldots, g_{i-1}\rangle) \cong \mathbb{F}_\ell^{r-i+1}$.

On considère désormais une suite $X_1, X_2, \ldots$ de variables aléatoires indépendantes et identiquement distribuées selon la loi uniforme sur G. On définit

$$T_1 = \min\{j \in \mathbb{N} \mid X_j \neq 0 \bmod lG\}$$

et pour tout $2 \leqslant i \leqslant r$,

$$T_i = \min\{j \in \mathbb{N} \mid X_j \neq 0 \bmod \ell G + \langle X_{T_1}, \ldots, X_{T_{i-1}}\rangle\} - T_{i-1}$$

Donc, pour tout $1 \leqslant i \leqslant r$, la variable aléatoire T_i est un temps d'arrêt, qui désigne le premier succès d'une suite d'épreuves de Bernouilli indépendantes de probabilité de succès $p_i = 1 - \frac{1}{\ell^{r-i+1}}$. La variable T_i suit donc une loi géométrique de paramètre p_i :

$$T_i \sim \mathcal{G}\left(1 - \frac{1}{\ell^{r-i+1}}\right)$$

Soit $S = \sum_{i=1}^{r} T_i$, alors pour tout entier $n > 0$,

$$\mathbb{P}(\langle X_1, \ldots, X_n \rangle = G) = \mathbb{P}(S \leqslant n)$$

Nous souhaitons donc borner la probabilité $\mathbb{P}(S > n)$ pour tout entier n. Dans l'article [Pom01], une formule explicite de la probabilité $\mathbb{P}(S \leqslant n)$ est donnée. Cependant, la borne du théorème 63 permet de simplifier les calculs :

Théorème 63. *Soit ℓ un entier premier. Soient $(T_i)_{i\in\mathbb{N}}$ une suite de variables aléatoires mutuellement indépendantes telle que pour tout $i \in \mathbb{N}$,*

$$T_i \sim \mathcal{G}(1 - \frac{1}{\ell^i})$$

Pour tout $r \geqslant 1$, on définit la somme $S_r = \sum_{i=1}^{r} T_i$. Alors pour tout entier n,

$$\mathbb{P}(S_r > n) \leqslant \left(\sum_{i=0}^{r-1} \frac{1}{\ell^i} \right) \frac{1}{\ell^{n-r+1}}$$

Démonstration. On procède par récurrence sur r. Pour $r = 1$, alors $S_1 = T_1$ suit une loi géométrique de paramètre $1 - 1/\ell$, donc pour tout $n \geqslant 1$,

$$\mathbb{P}(S_1 > n) = \left(1 - (1 - \frac{1}{\ell})\right)^n = \frac{1}{\ell^n}$$

Si $n \leqslant 0$, alors $\mathbb{P}(S_1 > n) = 1 \leqslant \frac{1}{\ell^n}$. Donc le théorème est vrai pour $r = 1$.

Soit $r \geqslant 2$, on va supposer que le théorème est vrai au rang $r-1$. Alors pour tout $n \in \mathbb{Z}$,

$$\begin{aligned}
\mathbb{P}(S_r > n) &= \sum_{i=1}^{\infty} \mathbb{P}(T_r = i)\mathbb{P}(S_{r-1} > n-i) \\
&\leqslant \sum_{i=1}^{\infty} \frac{1}{\ell^{r(i-1)}} \left(1 - \frac{1}{\ell^r}\right) \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \frac{1}{\ell^{n-i-r+2}} \\
&\leqslant \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \left(1 - \frac{1}{\ell^r}\right) \sum_{i=1}^{\infty} \frac{1}{\ell^{n+i(r-1)-2(r-1)}} \\
&\leqslant \left(\sum_{j=0}^{r-2} \frac{1}{\ell^j}\right) \left(1 - \frac{1}{\ell^r}\right) \frac{1}{\ell^{n-2(r-1)}} \frac{1}{\ell^{r-1}-1} \\
&\leqslant \frac{\sum_{j=0}^{r-2} \ell^j}{\ell^{r-2}} \frac{\ell^r - 1}{\ell^r} \frac{1}{\ell^{r-1}-1} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \frac{\left(\sum_{j=0}^{r-2} \ell^j\right)}{\ell^{r-2}} \frac{(\ell-1)\left(\sum_{j=0}^{r-1} \ell^j\right)}{\ell^r} \frac{1}{(\ell-1)\left(\sum_{j=0}^{r-2} \ell^j\right)} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \frac{\left(\sum_{j=0}^{r-2} \ell^j\right)(\ell-1)\left(\sum_{j=0}^{r-1} \ell^j\right)}{\ell^{2(r-1)}(\ell-1)\left(\sum_{j=0}^{r-2} \ell^j\right)} \frac{1}{\ell^{n-2(r-1)}} \\
&\leqslant \left(\sum_{j=0}^{r-1} \frac{1}{\ell^j}\right) \frac{1}{\ell^{n-(r-1)}}
\end{aligned}$$

Par récurrence sur r, le théorème est démontré. □

Corollaire 63.1. *Soit G un ℓ-groupe abélien fini. Soit r son nombre de facteurs invariants. Soit $n \geqslant r$ un entier, et soient $g_1, \ldots, g_n$ des éléments de G tirés uniformément. Alors*

$$\mathbb{P}(\langle g_1, \ldots, g_n \rangle \subsetneq G) \leqslant \left(\sum_{i=0}^{r-1} \frac{1}{\ell^i}\right) \frac{1}{\ell^{n-r+1}} \leqslant \frac{1}{\ell^{n-r}(\ell-1)}$$

Cas général

Soit G un groupe abélien fini, soit r son nombre de facteurs invariants, soit ℓ un nombre premier, et soit h_ℓ le plus grand diviseur de $|G|$ premier avec ℓ, alors $h_\ell G$ est un ℓ-groupe dont le nombre de facteurs invariants est inférieur à r. De plus, la distribution uniforme sur G et la multiplication par h_ℓ induisent une distribution uniforme sur $h_\ell G$.

Soit $n \geqslant r$, et soient $g_1, \ldots, g_n$ des éléments de G tirés uniformément. Ils engendrent G si et seulement si pour tout ℓ premier,

$$\langle h_\ell g_1, \ldots, h_\ell g_n \rangle = h_\ell G.$$

De plus, les événements $(\{\langle h_\ell g_1, \dots, h_\ell g_n\rangle = h_\ell G\})_\ell$ sont indépendants. Donc

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &= 1 - \mathbb{P}(\langle g_1, \dots, g_n\rangle = G)\\ &= 1 - \prod_{\ell \text{ premier}} \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle = h_\ell G)\\ &= 1 - \prod_{\ell \text{ premier}} (1 - \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle \subsetneq h_\ell G))\end{aligned}$$

En utilisant les bornes obtenues précédemment on obtient le théorème suivant :

Théorème 64. *Soit G un groupe abélien fini. Soit r son nombre de facteurs invariants. Soit $n \geqslant r+2$ un entier, et soient $g_1, \dots, g_n$ des éléments de G tirés uniformément. Alors*

$$\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) \leqslant \frac{2}{3}\left(\frac{1}{2}\right)^{n-r-2}$$

Démonstration. On utilise le fait que les groupes $h_\ell G$ sont des ℓ-groupes avec moins de r facteurs invariants, et le corollaire 63.1.

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &= 1 - \prod_{\ell \text{ premier}} (1 - \mathbb{P}(\langle h_\ell g_1, \dots, h_\ell g_n\rangle \subsetneq h_\ell G))\\ &\leqslant 1 - \prod_{\ell \text{ premier}} \left(1 - \frac{1}{\ell^{n-r}(\ell-1)}\right)\end{aligned}$$

Or, puisque $n - r \geqslant 2$, pour tout ℓ premier $\frac{1}{\ell^{n-r}(\ell-1)} \in [0, 1/2]$ et

$$\ln(1 - \frac{1}{\ell^{n-r}(\ell-1)}) \geqslant -2\frac{1}{\ell^{n-r}(\ell-1)}$$

en utilisant l'inégalité

$$\forall x \in [-1/2, 0],\ 2x \leqslant \ln(1+x).$$

Ainsi

$$\begin{aligned}\mathbb{P}(\langle g_1, \dots, g_n\rangle \subsetneq G) &\leqslant 1 - e^{-2\sum_{\ell \text{ premier}} \frac{1}{\ell^{n-r}(\ell-1)}}\\ &\leqslant 2\sum_{\ell \text{ premier}} \frac{1}{\ell^{n-r}(\ell-1)}\end{aligned}$$

en utilisant l'inégalité de convexité

$$\forall x \in \mathbb{R}, 1 - e^x \leqslant -x.$$

Cette somme est convergente car $n - r \geqslant 2$.

Enfin,

$$\frac{1}{\ell^{n-r}(\ell-1)} = \frac{1}{\ell^{n-r-2}} \frac{1}{\ell^2(\ell-1)} \leqslant \frac{1}{2^{n-r-2}} \frac{1}{\ell^2(\ell-1)}.$$

Ainsi

$$\mathbb{P}(\langle g_1, \ldots, g_n \rangle \subsetneq G) \leqslant \frac{1}{2^{n-r-2}} \left(2 \sum_{\ell \text{ premier}} \frac{1}{\ell^2(\ell-1)} \right).$$

On conclut en calculant à l'aide d'un ordinateur que

$$2 \sum_{\ell \text{ premier}} \frac{1}{\ell^2(\ell-1)} \leqslant \frac{2}{3}.$$

□

6.3 Simplicité et liberté des $K[G]$-modules

L'objectif de cette section est de démontrer le théorème 79. Ce résultat est utilisé dans la section 4.4 pour justifier l'existence d'un code dual.

Modules, simplicité et théorème de Jordan-Hölder

On commence par rappeler quelques notions de théorie des modules avant de considérer le cas spécifique des $K[G]$-modules (i.e. des représentations linéaires de groupes). Cette sous-section reprend un cours de Pierre-Baumann [Bau08]. Soit A un anneau (unitaire).

Définition 44. Soit M un groupe abélien (noté additivement). On dit que M est un A-module à gauche s'il existe une action à gauche (notée multiplicativement) de A sur M telle que :

- $\forall m \in M, 1_A m = m$.
- $\forall a, b \in A, \forall m, n \in M, (a+b)(m+n) = am + bm + an + bn$.
- $\forall a, b \in A, \forall m \in M, (ab)m = a(bm)$.

Un sous-module N de M est un sous-groupe abélien de M stable par l'action de A. Le groupe quotient M/N est également un A-module :

$$\forall a \in A, \forall m \in M, a(m+N) = am + N.$$

Exemple 12. L'anneau A dispose naturellement d'une structure de A-module à gauche, en agissant sur lui-même par multiplication à gauche. On appelle ce module le A-module régulier à gauche, et on le note ${}_A A$.

Soit I un ensemble et soit $A^{(I)}$ l'ensemble des familles d'éléments de A indexées par I de support fini. Soit $i \in I$, on note e_i l'élément $A^{(I)}$ dont la composante d'indice i est 1_A et

dont les autres composantes sont nulles. Alors $(e_i)_{i\in I}$ forme une base de $A^{(I)}$. On appelle modules libres (à gauche) les modules (à gauche) disposant d'une base.

Enfin $\{0\}$ est un A-module appelé module zéro ou module nul. Il est parfois noté simplement 0.

Définition 45. Soient M, N deux A-modules à gauche. Soit $\varphi : M \longrightarrow N$ un morphisme de groupes. On dit que φ est un morphisme de A-modules à gauche si

$$\forall a \in A, \forall m \in M, \varphi(am) = a\varphi(m).$$

On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N. C'est sous-groupe abélien de $\mathrm{Hom}_{\mathbb{Z}}(M, N)$. L'image de φ est un sous-module de N, et le noyau de φ est un sous-module de M.

Les définitions précédentes se généralisent naturellement "à droite". Certaines propriétés des modules ne dépendent pas du côté où A agit. On se permettra de ne pas préciser "à gauche" ou "à droite" dans les énoncés lorsque ce n'est pas nécessaire.

Définition 46. Soit M un A-module à gauche. Alors $\mathrm{Hom}_A(M, {}_AA)$ le groupe des morphismes de A-modules à gauche de M vers ${}_AA$ est naturellement muni d'une structure de A-module à droite :

$$\forall f \in \mathrm{Hom}_A(M, {}_AA), \forall a \in A, \forall m \in M, (fa)(m) = f(m)a.$$

On l'appelle module dual de M, et on le notera parfois M^*.

Proposition 65. $({}_AA)^*$ est isomorphe à A_A, le A-module régulier à droite.

Démonstration. On donne l'isomorphisme explicitement :

$$\begin{array}{ccc} \mathrm{Hom}_A({}_AA, {}_AA) & \longrightarrow & A_A \\ f & \longmapsto & f(1) \end{array}.$$

□

Définition 47. Soit M un A-module. On dit que

- M est noethérien si toute suite croissante de sous-modules de M est stationnaire.
- M est artinien si toute suite décroissante de sous-modules de M est stationnaire.
- M est simple s'il a exactement deux sous-modules M et 0.

On voit que tout A-module simple est artinien et noethérien.

Proposition 66. Soit M un A-module à gauche simple. Alors il existe un idéal à gauche maximal $\mathfrak{m}$ de A tel que $M \simeq A/\mathfrak{m}$.

Démonstration. Soit $m \in M$ non nul. Alors $\mathfrak{m}$ est le noyau de l'application $a \in A \longmapsto am \in M$. Cette application est surjective car son image est un sous-module non nul de M. □

Proposition 67. Soit M un A-module noethérien (resp. artinien). Alors tout ensemble non-vide de sous-modules de M possède un élément maximal (resp. minimal) pour l'inclusion.

Démonstration. Supposons qu'il existe un ensemble $\mathcal{E}$ non-vide de sous-modules de M ne possédant pas d'élément maximal pour l'inclusion. Alors il est possible de trouver une suite $N_0 \subsetneq N_1 \subsetneq \dots$ de sous-modules de M dans $\mathcal{E}$. Donc M n'est pas noethérien. Un argument similaire démontre le cas artinien. □

Définition 48. Soit M un A-module. Une filtration croissante de M est une suite croissante $(M_n)_{n\in\mathbb{Z}}$ de sous-modules de M telle que :

— $\cup_{n\in\mathbb{Z}} M_n = M$.

— $\cap_{n\in\mathbb{Z}} M_n = 0$.

On appelle les A-modules M_{n+1}/M_n les quotients ou les facteurs de la filtration.

Soient $(M_n)_{n\in\mathbb{Z}}$ et $(N_n)_{n\in Z}$ deux filtrations croissantes de M. On dit que $(N_n)_{n\in Z}$ est un raffinement de $(M_n)_{n\in Z}$ s'il existe une injection croissante $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ telle que

$$\forall n \in \mathbb{Z}, M_n = N_{\varphi(n)}.$$

Une série de composition de M est une filtration dont tous les quotients sont simples. Deux séries de composition sont dites équivalentes si elles ont la même suite de quotients à permutation et isomorphisme près.

Lemme 68 (Schur)**.** Soit $\varphi : M \longrightarrow N$ un morphisme de A-modules simples. Alors φ est soit un isomorphisme, soit le morphisme nul.

Une preuve est disponible dans [Lan02, Chapitre 7, Proposition 1.1].

Théorème 69 (Jordan-Hölder)**.** *Soit M un A-module. Si M a des séries de composition, elles sont toutes équivalentes.*

Une preuve est disponible dans [CR62, Théorème 13.7].

Définition 49. On appelle les quotients d'une série de composition de M les quotients de Jordan-Hölder de M.

Proposition 70. Soit M un A-module artinien et noethérien. Alors M possède une série de composition.

Démonstration. Notons $\mathcal{E}$ l'ensemble des sous-modules de M admettant une série de composition. L'ensemble $\mathcal{E}$ est non vide car $0 \in \mathcal{E}$. Puisque M est noethérien, $\mathcal{E}$ contient un élément maximal N pour l'inclusion.

Supposons que $N \neq M$. Alors l'ensemble $\mathcal{F}$ des sous-modules de M contenant strictement N est non vide car $M \in \mathcal{F}$. Puisque M est artinien, $\mathcal{F}$ contient un élément minimal L pour l'inclusion. Donc N est un sous-module maximal de L, et donc L/N est simple. Donc L admet une série de composition, ce qui est absurde.

Donc $N = M$, et M admet une série de composition. □

Définition 50. Soit M un A-module. On dit que M est de type fini s'il existe un ensemble fini I et un morphisme surjectif de A-modules $\pi : A^{(I)} \longrightarrow M$, ou de manière équivalente s'il est engendré par un nombre fini d'éléments.

Lemme 71. Tout A-module noethérien est de type fini.

Démonstration. Soit M un A-module noethérien. On note $\mathcal{E}$ l'ensemble des sous-modules de M de type fini. Alors, puisque M est noethérien, $\mathcal{E}$ possède un élément maximal N pour l'inclusion. De plus, pour tout $x \in M$, $N + Ax$ est de type fini (car N l'est). Par maximalité de N, on a $N = N + Ax$ donc $x \in L$. Donc $N = M$. □

Définition 51. Soit M un A-module artinien et noethérien. Soit S un A-module simple. On note $\ell(M)$ le nombre de quotients dans une série de composition de M, autrement appelé longueur de M (fini, car M est de type fini). On note $(M : S)$ le nombre de quotients de Jordan-Hölder de M isomorphes à S. On dit que $(M : S)$ est la multiplicité de Jordan-Hölder de M par rapport à S.

Proposition 72. Soient L, M, N trois A-modules tels que

$$0 \to L \to M \to N \to 0.$$

Alors M est artinien et noethérien si et seulement si L et N sont artiniens et noethériens.

Démonstration. On peut supposer que $L \subset M$ et $N = M/L$. Supposons que L et M/L sont noethériens. Soit $(T_n)_{n\in\mathbb{N}}$ une suite de sous-modules de M croissante. Alors $(T_n \cap L)_{n\in\mathbb{N}}$ est une suite de sous-modules de L croissante et $((T_n + L)/L)_{n\in\mathbb{N}}$ est une suite de sous-modules de M/L croissante. Alors il existe $T_L \subset L$ et $T_{M/L} \subset M/L$ deux sous modules, et $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0$, $(T_n \cap L) = T_L$ et $((T_n + L)/L) = T_{M/L}$. Cela implique que pour tout $n \geqslant n_0$, le module T_n est constant. Donc M est noethérien. La réciproque ne pose pas de difficultés. La preuve est similaire pour les modules artiniens. □

Proposition 73. Soit M un A-module noethérien (resp. artinien). Alors pour tout entier $n \geqslant 0$, M^n est noethérien (resp. artinien).

Démonstration. En remarquant l'existence d'une suite exacte

$$0 \to M \to M^n \to M^{n-1} \to 0$$

on raisonne par récurrence en utilisant la proposition 72. □

Proposition 74. Soit L, M, N trois A-modules artiniens et noethériens tels que

$$0 \to L \to M \to N \to 0.$$

Alors

$$\ell(M) = \ell(L) + \ell(N)$$

et pour tout A-module simple S,

$$(M : S) = (L : S) + (N : S).$$

Démonstration. On peut supposer que $L \subset M$ et $N = M/L$. Soit $0 = L_0 \subset L_1 \subset \cdots \subset L_{\ell(L)} = L$ une série de composition de L et $0 = N_0 \subset N_1 \subset \cdots \subset N_{\ell(N)} = N$ une série de composition de N. Soit $\pi_L : M \longrightarrow N$ le morphisme quotient. Alors on a une filtration

$$0 = L_0 \subset L_1 \subset \cdots \subset L_{\ell(L)} = L = \pi_L^{-1}(N_0) \subset \pi_L^{-1}(N_1) \subset \cdots \subset \pi_L^{-1}(N_{\ell(N)}) = M.$$

Pour tout $0 \leqslant i \leqslant \ell(N) - 1$,

$$\pi_L^{-1}(N_{i+1})/\pi_L^{-1}(N_i) \simeq N_{i+1}/N_i$$

est un module simple, donc $L_0 \subset \cdots \subset \pi_L^{-1}(N_{\ell(N)})$ est une série de composition de M. On en déduit la proposition. □

Proposition 75. Il existe un ensemble contenant un représentant de toutes les classes d'isomorphisme de A-modules artiniens et noethériens.

Démonstration. Soit $\mathcal{M}$ une classe d'isomorphisme de A-modules artiniens et noethériens. Les modules dans la classe de M sont donc de type fini. Alors il existe un sous-module N de $A^{\mathbb{N}}$ et M un module de la classe d'isomorphisme $\mathcal{M}$ tel que $M = A^{\mathbb{N}}/N$.

Soit $\mathcal{E}$ l'ensemble des sous-modules de $A^{\mathbb{N}}$ (contenu dans l'ensemble des parties). Il est en bijection avec l'ensemble $\{A^{\mathbb{N}}/N; N \in \mathcal{E}\}$ qui contient bien (au moins) un représentant de toutes les classes d'isomorphisme de A-modules artiniens et noethériens. □

Définition 52. Soit $\mathcal{E}$ un ensemble de représentants des classes d'isomorphisme de A-modules artiniens et noethériens. Considérons $\mathbb{Z}^{(\mathcal{E})}$ le groupe abélien libre sur $\mathcal{E}$, et considérons $\mathrm{Gr}(A)$ le quotient de $\mathbb{Z}^{(\mathcal{E})}$ par le sous-groupe engendré par les éléments de la forme $M - L - N$ pour toute suite exacte

$$0 \to L \to M \to N \to 0$$

d'éléments L, M, N de $\mathcal{E}$. On appelle $\mathrm{Gr}(A)$ le groupe de Grothendieck des classes d'isomorphisme de A-modules artiniens et noethériens.

Remarque 35. $\mathrm{Gr}(A)$ ne dépend pas du choix de $\mathcal{E}$ et est uniquement caractérisé par A.

Définition 53. Soit L, M, N des A-modules.

— On dit que N est projectif s'il existe M un A-module libre et L un A-module tels que $M \simeq L \oplus N$.

— On dit que L est injectif si toute suite exacte courte

$$0 \to L \to M \to N \to 0$$

est scindée, i.e. $M \simeq L \oplus N$.

Définition 54. On définit $\mathrm{PGr}(A)$ le groupe de Grothendieck des classes d'isomorphisme de A-modules projectifs artiniens et noethériens (voir définition 52). Soit P un A-module projectif artinien et noethérien. On note $[P]$ l'image de P dans $\mathrm{PGr}(A)$.

Liberté de l'orthogonal

Soit K un corps (commutatif) et G un groupe fini.

Définition 55. On note ${}_GK[G]$ le $K[G]$-module régulier à gauche et $K[G]_G$ le $K[G]$-module régulier à droite.

Proposition 76. Les $K[G]$-modules réguliers (à droite et à gauche) sont artiniens et noethériens.

Démonstration. Tout $K[G]$-module est un K-espace vectoriel. De plus, $K[G]$ est un K-espace vectoriel de dimension finie. Soit une suite croissante $M_0 \subset M_1 \subset \dots$ de sous-modules de $K[G]$. Alors $\dim(M_0) \leqslant \dim(M_1) \leqslant \dots$ est une suite croissante d'entiers majorée par $\dim(K[G])$. Donc la suite des dimensions est stationnaire, et $(M_i)_{i\in\mathbb{N}}$ également. Donc les $K[G]$-modules réguliers sont noethériens. Un raisonnement similaire montre qu'ils sont artiniens. □

Corollaire 76.1. Tout $K[G]$-module de type fini est artinien et noethérien.

Démonstration. On le déduit des propositions 73 et 72. □

Proposition 77. Soit M un $K[G]$-module et N un sous-module libre de M. Alors il existe L un sous-module de M tel que $M = N \oplus L$.

Démonstration. Cette propriété est dûe au fait que l'algèbre $K[G]$ est une algèbre de Frobenius [CR62, Théorème 62.1], i.e.

$$\mathrm{Hom}_{K[G]}(K[G]_G, K[G]_G) \simeq \mathrm{Hom}_K(K[G]_G, K).$$

Alors tout $K[G]$-module projectif est également injectif [CR62, Théorème 62.3]. En particulier, N est libre donc projectif, et donc injectif. Ainsi, la suite exacte

$$0 \to N \to M \to M/N \to 0$$

est scindée, donc il existe un sous-module L de M tel que $L \simeq M/N$ et $M = N \oplus L$. □

Proposition 78. Soient P_1 et P_2 deux $K[G]$-modules projectifs artiniens et noethériens. Alors $P_1 \simeq P_2$ si et seulement si $[P_1] = [P_2]$ dans $\mathrm{PGr}(K[G])$.

Démonstration. La proposition est démontrée dans [Ser71, Chapitre 14, Corollaire 3]. □

Soit $n \geqslant 1$ un entier. On rappelle que $\langle ., . \rangle$ désigne la forme $K[G]$-bilinéaire sur $K[G]^n$ définie dans l'équation (4.4.1).

Théorème 79. *Soit M un sous-module libre de ${}_GK[G]^n$ (resp. $K[G]_G^n$). Alors $M^\perp$, l'orthogonal de M pour la forme $K[G]$-bilinéaire $\langle ., . \rangle$, est un sous-module libre de $K[G]_G^n$ (resp. ${}_GK[G]^n$).*

Démonstration. On démontre le cas où M est un $K[G]$-module à gauche. Soit k le rang de M comme $K[G]$-module libre. Donc $M \simeq {}_GK[G]^k$. D'après la proposition 77, il existe un sous-module N de ${}_GK[G]^n$ tel que

$$ {}_GK[G]^n = M \oplus N. \tag{6.3.1}$$

De plus, on a trivialement

$$ {}_GK[G]^n \simeq {}_GK[G]^k \oplus {}_GK[G]^{n-k}. \tag{6.3.2}$$

Les modules ${}_GK[G]^n$, ${}_GK[G]^k$, ${}_GK[G]^{n-k}$, M et N sont projectifs, artiniens et noethériens (car ils sont de type fini). On a

$$\begin{aligned}
[N] &= [{}_GK[G]^n] - [M] && \text{d'après l'équation (6.3.1)} \\
&= [{}_GK[G]^n] - [{}_GK[G]^k] && \text{car } M \simeq {}_GK[G]^k \\
&= [{}_GK[G]^{n-k}] && \text{d'après l'équation (6.3.2)}
\end{aligned}$$

D'après la proposition 78, le module $N \simeq {}_GK[G]^{n-k}$ est un $K[G]$-module à gauche libre. Ainsi, $\mathrm{Hom}_{K[G]}(N, {}_GK[G])$ est un $K[G]$-module à droite libre. En effet, on a

$$\begin{aligned}
\mathrm{Hom}_{K[G]}(N, {}_GK[G]) &\simeq \mathrm{Hom}_{K[G]}({}_GK[G]^{n-k}, {}_GK[G]) \\
&\simeq \mathrm{Hom}_{K[G]}({}_GK[G], {}_GK[G])^{n-k} \\
&\simeq (K[G]_G)^{n-k}
\end{aligned}$$

d'après la proposition 66.

On montre finalement que $M^\perp \simeq \mathrm{Hom}_{K[G]}(N, {}_GK[G])$. Soit

$$L = \{f \in \mathrm{Hom}_{K[G]}({}_GK[G]^n, {}_GK[G]) \mid f_{|M} = 0\},$$

alors $L \simeq \mathrm{Hom}_{K[G]}(N, {}_GK[G])$. Il reste à montrer que $M^\perp \simeq L$. Soit

$$\begin{array}{rccc} \phi : & M^\perp & \longrightarrow & L \\ & m & \longmapsto & \langle ., m \rangle \end{array},$$

est un morphisme de $K[G]$-module injectif. De plus, $M^\perp$ et L sont des K-espaces vectoriels de même dimension. En effet, L est un $K[G]$-module à droite libre de rang $(n-k)$, et donc sa dimension (sur K) est $|G|(n-k)$. Ensuite,d'après la proposition 41, le $K[G]$-module à droite $M^\perp$ est le dual de M pour la forme $\langle ., . \rangle_K$, et donc sa dimension est également $|G|(n-k)$. On en déduit que

$$M^\perp \simeq L \simeq \mathrm{Hom}_{K[G]}(N, {}_GK[G]).$$

□

Bibliographie

[AFG24] Diego F. Aranha, Georgios Fotiadis, and Aurore Guillevic. A short-list of pairing-friendly curves resistant to the special TNFS algorithm at the 192-bit security level. *IACR Communications in Cryptology*, 1(3), 2024.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comput.*, 61(203) :29–68, 1993.

[Ari61] S. Arimoto. Encoding and decoding of p-ary group codes and the correction system. *Information Processing in Japan*, 2 :320–325, 1961. (in Japanese).

[AT09] Emil Artin and John Tate. *Class field theory*. Providence, RI : AMS Chelsea Publishing, reprint of the 1990 2nd ed. edition, 2009.

[Bau08] Pierre Baumann. Introduction à la théorie des représentations. cours de M2 donné à l'Université Louis Pasteur, 2008. https://irma.math.unistra.fr/~baumann/coursM2-2008.pdf.

[BCG+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (auto-édit.), Palaiseau, September 2017. 686 pages. Imprimé par CreateSpace. Aussi disponible en version électronique.

[BF03] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. *SIAM J. of Computing*, 32(3) :586–615, 2003.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The Tower Number Field Sieve. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015*, volume 9453 of *Advances in cryptology-Asiacrypt 2015*, pages 31–58, Auckland, New Zealand, 2015. International Association of Cryptologic Research, Springer.

[BH08] Peter Beelen and Tom Høholdt. The decoding of algebraic geometry codes. In *Advances in algebraic geometry codes.*, pages 49–98. Hackensack, NJ : World Scientific, 2008.

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes - okamoto - vanstone algorithm. *J. Cryptology*, 11 :141–145, 1998.

[BLB06] S. Ballet and D. Le Brigand. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_2$. *J. Number Theory*, 116(2) :293–310, 2006.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.

[BLS03] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in communication networks. Third international conference, SCN 2002, Amalfi, Italy, September 11–13, 2002. Revised papers*, pages 257–267. Berlin : Springer, 2003.

[Blu70] L. Bluestein. A linear filtering approach to the computation of discrete fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18(4) :451–455, 1970.

[BMvT78] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory*, 24 :384–386, 1978.

[BR04] S. Ballet and R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *J. Algebra*, 272(1) :173–185, 2004.

[BRS21] Peter Beelen, Johan Rosenkilde, and Grigory Solomatov. Fast encoding of AG codes over C_{ab} curves. *IEEE Trans. Inf. Theory*, 67(3) :1641–1655, 2021.

[Bru13] Peter Bruin. Computing in Picard groups of projective curves over finite fields. *Math. Comput.*, 82(283) :1711–1756, 2013.

[BS96] Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comput.*, 65(216) :1717–1735, 1996.

[BS05] Johannes Buchmann and Arthur Schmidt. Computing the structure of a finite Abelian group. *Math. Comput.*, 74(252) :2017–2026, 2005.

[BV07] Johannes Buchmann and Ulrich Vollmer. *Binary quadratic forms. An algorithmic approach*, volume 20 of *Algorithms Comput. Math.* Berlin : Springer, 2007.

[BW05] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptography*, 37(1) :133–141, 2005.

[BW23] Martino Borello and Wolfgang Willems. On the algebraic structure of quasi-group codes. *J. Algebra Appl.*, 22(10) :16, 2023. Id/No 2350222.

[CC88] D. V. Chudnovsky and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *J. Complexity*, 4(4) :285–316, 1988.

[CE23] Jean-Marc Couveignes and Tony Ezome. The equivariant complexity of multiplication in finite field extensions. *J. Algebra*, 622 :694–720, 2023.

[Cha08] Jean Chaumine. Multiplication in small finite fields using elliptic curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 343–350. World Sci. Publ., Hackensack, NJ, 2008.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Grad. Texts Math.* Berlin : Springer-Verlag, 1993.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Grad. Texts Math.* New York, NY : Springer, 2000.

[CR62] Charles W. Curtis and Irving Reiner. Representation theory of finite groups and associative algebras. Pure and Applied Mathematics. 11. New York-London : Interscience Publishers, a division of John Wiley & Sons. xiv, 685 pp. (1962)., 1962.

[DGTT18] Steven T. Dougherty, Joseph Gildea, Rhian Taylor, and Alexander Tylyshchak. Group rings, G-codes and constructions of self-dual and formally self-dual codes. *Des. Codes Cryptography*, 86(9) :2115–2138, 2018.

[Duu93] I.M. Duursma. *Decoding codes from curves and cyclic codes*. PhD thesis, Eindhoven Univ. Techn., Sept. 1993.

[ECdJ+11] Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman. *Computational Aspects of Modular Forms and Galois Representations*. Princeton University Press, 2011. Edited by Bas Edixhoven and Jean-Marc Couveignes.

[Ehr93] Dirk Ehrhard. Achieving the designed error capacity in decoding algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 39(3) :743–751, 1993.

[FR93] Gui-Liang Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inf. Theory*, 39(1) :37–45, 1993.

[FST10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2) :224–280, 2010.

[Gas23] Jean Gasnier. Sagemath code for the subfield method. https://gitlab.inria.fr/jgasnier/subfield-method, 2023.

[Gau01] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. 1801.

[GG25] Jean Gasnier and Aurore Guillevic. An algebraic point of view on the generation of pairing-friendly curves. *SIAM Journal on Applied Algebra and Geometry*, 9(2) :456–480, 2025.

[Gop83] V. D. Goppa. Algebraico-geometric codes. *Math. USSR, Izv.*, 21 :75–91, 1983.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121(1) :211–222, 1995.

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2) :48, 2022. Id/No 10.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Hav89] A. Havemose. *Decoding algebraic geometric codes.* PhD thesis, Danmarks Tekniske Højskole, Aug. 1989.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. Lond. Math. Soc. (3)*, 64(2) :265–338, 1992.

[HP95] Tom Høholdt and Ruud Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 41(6) :1589–1614, 1995.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci., Univ. Tokyo, Sect. I A*, 28 :721–724, 1981.

[Jan96] Gerald J. Janusz. *Algebraic number fields.*, volume 7 of *Grad. Stud. Math.* Providence, RI : AMS, American Mathematical Society, 2nd ed. edition, 1996.

[JLJ+89] Jørn Justesen, Knud J. Larsen, H. Elbrønd Jensen, Allan Havemose, and Tom Høholdt. Construction and decoding of a class of algebraic geometry codes. *IEEE Trans. Inf. Theory*, 35(4) :811–821, 1989.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In Wieb Bosma, editor, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4) :323–338, 2001.

[KS91] Erich Kaltofen and B. David Saunders. On Wiedemann's method of solving sparse linear systems. In *Applied algebra, algebraic algorithms and error-correcting codes. 9th international symposium, AAECC '9, New Orleans, LA, USA, October 7–11, 1991. Proceedings*, pages 29–38. Berlin etc. : Springer-Verlag, 1991.

[KSS08] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer, 2008.

[Lac86] Gilles Lachaud. The geometric Goppa codes. Sémin. Bourbaki, 37e année, Vol. 1984/85, Exp. No. 641, Astérisque 133/134, 189-207 (1986)., 1986.

[Lan56a] Serge Lang. Sur les séries L d'une variété algébrique. *Bull. Soc. Math. Fr.*, 84 :385–407, 1956.

[Lan56b] Serge Lang. Unramified class field theory over function fields in several variables. *Ann. Math. (2)*, 64 :285–325, 1956.

[Lan87] Serge Lang. *Elliptic functions. Second edition*, volume 112 of *Grad. Texts Math.* Springer, Cham, 1987.

[Lan94] Serge Lang. *Algebraic number theory.*, volume 110 of *Grad. Texts Math.* New York : Springer-Verlag, 2nd ed. edition, 1994.

[Lan02] Serge Lang. *Algebra*. Springer New York, NY, 2002.

[LdS13] Hendrik Lenstra and Bart de Smit. Standard models of finite fields. In Gary L. Mullen and Daniel Panario, editors, *Handbook of Finite Fields*, Discrete mathematics and its applications, pages 345–363. CRC Press, 2013.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxf. Grad. Texts Math.* Oxford : Oxford University Press, 2002.

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2025. [Online ; accessed 20 February 2025].

[LZZ24] Jianming Lin, Chang-An Zhao, and Yuhao Zheng. Efficient implementation of super-optimal pairings on curves with small prime fields at the 192-bit security level. ePrint 2024/1195, 2024.

[Lü23] Frank Lübeck. Standard generators of finite fields and their cyclic subgroups. *Journal of Symbolic Computation*, 117 :51–67, 2023.

[MOV93] Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory*, 39(5) :1639–1646, 1993.

[Neu86] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren Math. Wiss.* Springer, Cham, 1986.

[NW19] Anand Kumar Narayanan and Matthew Weidner. Subquadratic time encodable codes beating the Gilbert-Varshamov bound. *IEEE Trans. Inf. Theory*, 65(10) :6010–6021, 2019.

[NX98] Harald Niederreiter and Chaoping Xing. A general method of constructing global function fields with many rational places. In *Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings*, pages 555–566. Berlin : Springer, 1998.

[Pet60] W. W. Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. IRE Trans. Inf. Theory IT-6, 459-470 (1960) ; translation in Kibern. Sb. 6, 25-54 (1963) ;, 1960.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comput.*, 55(192) :745–763, 1990.

[Pom01] Carl Pomerance. The expected number of random elements to generate a finite Abelian group. *Period. Math. Hung.*, 43(1-2) :191–198, 2001.

[Por88] S.C. Porter. *Decoding codes arising from Goppa's construction on algebraic curves*. PhD thesis, Yale univ., Dec. 1988.

[Que89] Heinz-Georg Quebbemann. Cyclotomic Goppa codes. *IEEE Trans. Inf. Theory*, 34(5) :1317–1320, 1989.

[Ran12] Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, 28(4) :489–517, 2012.

[Ros54] Maxwell Rosenlicht. Generalized jacobian varieties. *Ann. Math. (2)*, 59 :505–530, 1954.

[Ros87] Michael Rosen. The Hilbert class field in function fields. *Expo. Math.*, 5 :365–378, 1987.

[RS60] I. S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *J. Soc. Ind. Appl. Math.*, 8 :300–304, 1960.

[RSR69] Lawrence R. Rabiner, Ronald W. Schafer, and Charles M. Rader. The chirp z-transform algorithm and its application. *Bell System Tech. J.*, 48 :1249–1292, 1969.

[Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4) :247–270, 2000.

[Sch31] Friedrich Karl Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Z.*, 33 :1–32, 1931.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comput.*, 44 :483–494, 1985.

[Ser71] Jean-Pierre Serre. Représentations linéaires des groupes finis. 2e éd., refondue. (Linear representations of finite groups. 2nd ed., revised). Collection methodes. Paris : Hermann. 182 p. 32 F (1971)., 1971.

[Ser78] Jean-Pierre Serre. *A course in arithmetic. Translation of "Cours d'arithmetique". 2nd corr. print*, volume 7 of *Grad. Texts Math.* Springer, Cham, 1978.

[Ser84] Jean-Pierre Serre. Groupes algébriques et corps de classes. 2ième éd., rev. et corr. (Nouv. tirage). Actualités Scientifiques et Industrielles. 1264. Publications de l'Institut de Mathématique de l'Université de Nancago, VII. Paris : Hermann. 208 p. (1984)., 1984.

[Ser20] Jean-Pierre Serre. *Rational points on curves over finite fields.*, volume 18 of *Doc. Math. (SMF)*. Paris : Société Mathématique de France (SMF), 2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler. Edited by Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler and René Schoof.

[Sho92] Mohammad Amin Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6) :1193–1198, 1992.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Grad. Texts Math.* New York, NY : Springer-Verlag, 1994.

[SKHN75] Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A method for solving key equation for decoding Goppa codes. *Inf. Control*, 27 :87–99, 1975.

[Sti08] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Publishing Company, Incorporated, 2nd edition, 2008.

[STV92] Igor E. Shparlinski, Michael A. Tsfasman, and Serge G. Vladut. Curves with many points and multiplication in finite fields. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 145–169. Springer, Berlin, 1992.

[SV90] Alexei N. Skorobogatov and Sergei G. Vlăduţ. On the decoding of algebraic-geometric codes. *IEEE Trans. Inf. Theory*, 36(5) :1051–1060, 1990.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2022. `https://www.sagemath.org`.

[TVZ82] M. A. Tsfasman, S. G. Vlădut, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109 :21–28, 1982.

[VD83] S. G. Vladut and V. G. Drinfel'd. Number of points of an algebraic curve. *Funct. Anal. Appl.*, 17 :53–54, 1983.

[vdG09] Gerard van der Geer. Hunting for curves with many points. In *Coding and cryptology. Second international workshop, IWCC 2009, Zhangjiajie, China, June 1–5, 2009. Proceedings*, pages 82–96. Berlin : Springer, 2009.

[vdGHLR09] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler. Tables of curves with many points, 2009. Retrieved January 2025.

[Ver10] Frederik Vercauteren. Optimal pairings. *IEEE Trans. Inf. Theory*, 56(1) :455–461, 2010.

[Was77] Siri Krishan Wasan. Quasi abelian codes. *Publ. Inst. Math., Nouv. Sér.*, 21 :201–206, 1977.

[Wat69] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Éc. Norm. Supér. (4)*, 2 :521–560, 1969.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann, Paris, 1948.

[Wie86] Douglas H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory*, 32 :54–62, 1986.

[Xyl11] Triantafyllos Xylouris. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arith.*, 150(1) :65–91, 2011.