École Polytechnique fédérale de Lausanne
Section de Mathématiques

Projet de semester, Master I

Répartition de Frobenius et application aux courbes elliptiques

Auteur : Corentin Perret-Gentil

Supervisé par Nahid Walji

Chaire de Théorie analytique des nombres
Prof. Philippe Michel

Printemps 2013

Résumé

Ce document est le résultat d'un projet de semestre de master, dont le but était d'étudier des questions de répartition d'images de représentations galoisiennes, puis les applications de ceci aux courbes elliptiques, pour essayer notamment de comprendre les formulations de la conjecture de Sato-Tate.

Afin de travailler dans un cadre général, nous adoptons l'approche de Serre sur la répartition de suites, indexées par des idéaux premiers de corps de nombres, dans les classes de conjugaison de groupes compacts. Celle-ci permettra en effet de comprendre dans le même contexte le théorème des idéaux premiers, le théorème de densité de Chebotarev et les répartition du nombre de points rationnels des réductions modulo p d'une courbe elliptique dans les cas CM et non-CM.

Le travail se sépare en deux parties : dans la première, nous étudions la théorie de la ramification, l'équirépartition dans les groupes compacts et les questions de densités d'ensembles d'idéaux premiers, puis les fonctions L associées à l'approche de Serre et leur relation avec des énoncés d'équirépartition.

Dans la seconde, nous commençons par étudier le degré d'isogénies à l'aide de la généralisation de la théorie de la ramification aux anneaux de Dedekind, puis on applique cette notion pour étudier les groupes de torsion, définir le module de Tate, les représentations ℓ-adiques et étudier les courbes elliptiques sur les corps finis. Après avoir donné les propriétés fondamentales de la réduction modulo un idéal premier d'une courbe elliptique définie sur un corps de nombres, on passe à l'étude de la répartition du nombres de points rationnels des réductions d'une courbe fixée, en reformulant le problème dans le contexte de la première partie. Pour cela, on se ramène par théorie de Galois à des corps de nombres, dont on combine les Frobenius.

Comme premier exemple de ce lien entre les deux parties, nous utilisons un théorème de Serre pour appliquer le théorème de Chebotarev au calcul de densités d'ensembles de premiers vérifiant des relations polynomiales pour le nombre de points rationnels de réductions. Ensuite, nous illustrons la preuve de l'équirépartition des θ_p dans le cas CM (dans le contexte de la première partie et en utilisant un théorème de Hecke sur la répartition d'entiers de corps quadratiques dans des secteurs). Finalement, nous réinterprétons la conjecture de Sato-Tate dans le contexte de la première partie, ce qui permet d'en donner plusieurs reformulation et de comprendre la provenance de la mesure impliquée.

Table des matières

Introduction

Pour toute paire d'entiers a, m premiers entre eux, le théorème de la progression arithmétique de Dirichlet indique que

$$|\{p \leq x \text{ premier } : p \equiv a \pmod{m}\}| = \frac{1}{\varphi(m)} \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

quand $x \to +\infty$. En d'autres termes, les images des premiers ne divisant pas m sont équiréparties dans $(\mathbb{Z}/m)^\times$. Rappelons que la démonstration de ce résultat se base sur la non-annulation en 1 de fonctions L attachées à des caractères de Dirichlet.

En interprétant $(\mathbb{Z}/m)^\times$ comme le groupe de Galois du corps cyclotomique $\mathbb{Q}(\zeta_m)$ ($\zeta_m \in \mathbb{C}$ une racine primitive $m^{\text{ème}}$ de l'unité), le théorème de la progression arithmétique peut alors être vu comme un énoncé de répartition dans $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ de la suite $(\sigma_p : \zeta \mapsto \zeta_m^p)_p$ indexée par les premiers ne divisant pas m. Dans ce point de vue, les caractères de Dirichlet modulo m deviennent des caractères du groupe de Galois.

A partir de cette observation, il est possible de généraliser grandement le théorème : les corps cyclotomiques sont remplacés par des corps de nombres galoisiens et la suite d'automorphismes par les *Frobenius* associés aux premiers ne se ramifiant pas dans l'extension. En généralisant les fonctions L de Dirichlet et leurs propriétés, on obtient alors le *théorème de densité de Chebotarev*, parfait équivalent du théorème de Dirichlet dans ce contexte.

De manière encore plus générale, on peut s'intéresser à des questions de répartition de suites indexées par des idéaux premiers de corps de nombres dans les classes de conjugaison de *groupes compacts* (en particulier des groupes de Galois, finis ou non). Là encore, il est possible de définir des fonctions L reliées à des représentations et l'équirépartition de suites est caractérisée par des propriétés de prolongement et de non-annulation de ces fonctions.

En plus de donner un contexte plus global au théorème de Dirichlet et de le généraliser, cette approche peut par exemple s'appliquer à l'étude d'énoncés statistiques sur les réductions de courbes elliptiques : si E est une courbe elliptique définie sur $\mathbb{Q}$ (ou plus généralement sur un corps de nombres), on peut s'intéresser aux propriétés de ses réductions modulo les premiers de bonne réduction. En d'autres termes, on procède à une analyse locale de la courbe.

En particulier, on peut s'intéresser à la répartition du nombre de points rationnels des éléments "locaux" de la courbe. A partir de *représentations ℓ-adiques*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

associées à la courbe, on voit que ce problème revient en fait à étudier la répartition de *Frobenius* dans les classes de conjugaison de groupes compacts comme des groupes de Galois, $\mathbb{R}/\mathbb{Z}$ ou $\mathrm{SU}_2(\mathbb{C})$. Certaines questions deviennent alors plus claires dans ce contextes. Par exemple, la *conjecture de Sato-Tate* se transforme en un énoncé d'équirépartition dans les classes de conjugaison de $\mathrm{SU}_2(\mathbb{C})$, alors qu'elle contient à la base une distribution difficile à interpréter.

Grâce aux généralisations du théorème de Dirichlet, ces questions se reformulent de manière naturelle en termes de prolongement et non-annulation de fonctions L, où elles sont également plus tangibles.

Dans ce qui suit, nous présenterons les questions de répartition de *Frobenius* dans les classes de conjugaison de groupes compacts et les relations avec des fonctions L, puis nous appliquerons ceci à des questions sur les courbes elliptiques comme esquissé ci-dessus. La théorie de la ramification développée dans le premier chapitre sera également utilisée pour étudier des propriétés des courbes elliptiques.

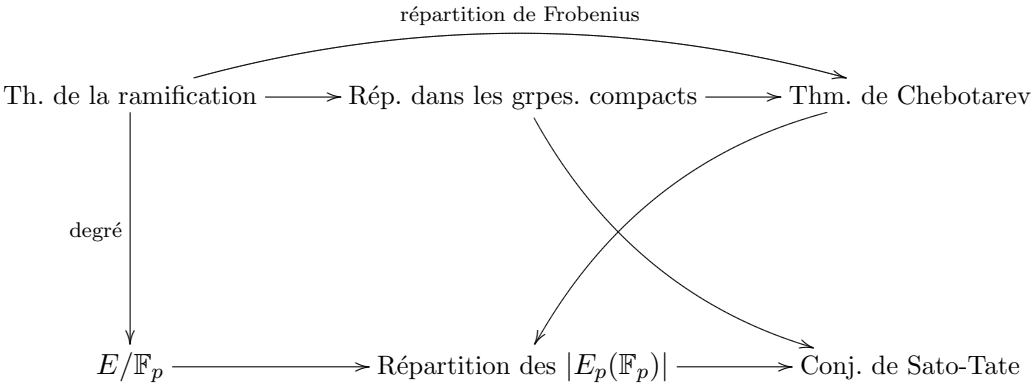


FIGURE 0.1: Les deux parties du document et leurs liens.

Références détaillées

Une bibliographie complète est présente à la fin de ce document. Une liste détaillées des références principales pour chaque chapitre est la suivante :

- *Chapitre 1 :* ce chapitre se base principalement sur les chapitres V et VI de [Sam71] et sur la section I.9 de [Neu99]. La généralisation aux anneaux Dedekind est tirée de [Lor96].
- *Chapitre 2 :* [Var07] pour les questions sur les groupes compacts et [Ser02] pour les questions d'équirépartition.
- *Chapitre 3 :* ce chapitre se base principalement sur [Ser02], dont on fournit les preuves laissées en exercices. La discussion sur les fonctions L d'Artin a également ses sources dans le chapitre VII de [Neu99].
- *Chapitre 4 :* les références principales sont les chapitre 7-8 de [Ser02] et le chapitre XV de [Lan94]. Dans [Ser02], la démonstration du théorème de Chebotarev est d'abord présentée, puis généralisée au contexte plus général. Nous procédons de manière inverse, en complétant les preuves du cas général à partir de celle du théorème de Chebotarev. Ensuite, on en déduit ce dernier de deux manières, ainsi que le théorème des idéaux premiers.
- *Chapitre 5 :* [Sil86], [Har77] et [Ful89]. La discussion sur la relation entre théorie de la ramification et degré se base sur [Lor96].
- *Chapitre 6 :* [Sil86], [Was08] et plusieurs de leurs exercices (notamment pour les résultats concernant les courbes supersingulières).
- *Chapitre 7 :* [Sil86, VII.2-3, VIII.1] et [Hus04, Chap. 5.1-5, 15.1], dont on simplifie la présentation pour pouvoir parler de réduction modulo un idéal premier d'un corps de nombres sans parler de corps locaux puis globaux.
- *Chapitre 8 :* ce chapitre est principalement composé d'exercices visant à détailler ou expliciter les éléments présentés au bas de la page 76 de [Ser02] et dans le cours d'introduction de [RM09]. La section sur les théorèmes de Deuring se base sur [Lan87] et [Cox89, Chapitre 14].
- *Annexe A :* cette annexe se base sur [Sil86], [Mil06], [Hus04] et [Was08], dont on tente d'extraire un ensemble aussi indépendant que possible des résultats et concepts nécessaires dans le travail et pour le calcul du degré des $\mathbb{Z}$-multiplications et du morphisme de Frobenius.

Calculs numériques

Les calculs non-triviaux présents dans certains exemples ou figures ont été obtenus à l'aide du logiciel open-source SAGE, disponible à l'adresse `sagemath.org`.

Merci à Nahid Walji pour avoir supervisé ce projet de semestre.

Première partie

Répartition de Frobenius

Chapitre 1

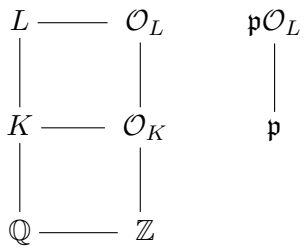
Théorie de la ramification et extensions galoisiennes de corps de nombres

Dans ce chapitre préliminaire, nous étudions les décompositions d'idéaux premiers dans des extensions de corps de nombres, puis le cas particulier d'extensions galoisiennes qui sera celui étudié par la suite. Finalement, nous expliquons comment ces résultats se généralisent pour des extensions de corps de fractions d'anneaux de Dedekind, situation qui sera également utilisée plus tard.

Comme donner les démonstrations de tous les résultats en jeu prendrait trop de place et qu'il ne s'agit pas du but principal de ce projet, nous renvoyons à [Sam71] pour la plupart d'entre elles. A la place, nous donnons des exemples détaillés, dont une détermination des Frobenius des corps quadratiques et cyclotomiques, menant en particulier à une démonstration de la loi de réciprocité quadratiques.

1. Décomposition d'idéaux premiers dans des extensions

Considérons une extension de degré fini L/K d'un corps de nombre K. Par suite, L est aussi un corps de nombre et on dénote par $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) l'anneau des entiers de K (resp. L).



Un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ ne reste pas forcément premier quand on le regarde comme idéal de $\mathcal{O}_L$ à travers l'application $\mathfrak{p} \mapsto \mathfrak{p}\mathcal{O}_L$. Plus précisément, comme $\mathcal{O}_L$ est un anneau de Dedekind, il va s'écrire de façon unique (à ordre près) comme

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}^{e_i},$$

où $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ sont des idéaux premiers distincts de $\mathcal{O}_L$ et $e_1, \ldots, e_r \geq 1$ des entiers. On appelle e_i l'**indice de ramification** de $\mathfrak{P}_i$.

Exemple 1.1. Par exemple, on peut considérer le cas $K = \mathbb{Q}$ et étudier la décomposition des idéaux premiers $p\mathbb{Z}$ (p un premier) dans l'anneau des entiers d'un corps de nombres L. Dans $L = \mathbb{Q}(i)$, on a par exemple

$$\begin{aligned} 3\mathcal{O}_L & \quad \text{également idéal premier de } \mathcal{O}_L, \\ 5\mathcal{O}_L = (2+i)(2-i) & \quad \text{produit de deux idéaux premiers,} \end{aligned}$$

comme on le verra plus tard.

On a une caractérisation simple des idéaux premiers divisant $\mathfrak{p}\mathcal{O}_L$:

Proposition 1.2. *Les idéaux premiers divisant $\mathfrak{p}\mathcal{O}_L$ sont les idéaux premiers $\mathfrak{P}$ de $\mathcal{O}_L$ tels que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.*

Démonstration. Voir [Sam71, V.2, proposition 1]. □

De ce fait, les $\mathfrak{P}_i$ sont appelés idéaux **au-dessus de $\mathfrak{p}$**.

Remarquons que l'on a alors pour tout i une injection canonique $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}_i$ pour tout $i = 1, \ldots, r$. Puisque l'on considère des anneaux de Dedekind, tout idéal premier est maximal, donc ces deux anneaux sont en fait des *corps*. Il s'agit même de corps *finis* (de cardinalité la norme des idéaux premiers respectifs). En particulier, on peut faire la définition suivante :

Définition 1.3. La dimension de $\mathcal{O}_L/\mathfrak{P}_i$ sur $\mathcal{O}_K/\mathfrak{p}$ est appelée **degré résiduel** de $\mathfrak{P}_i$, que l'on note f_i.

Similairement, on a une injection $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ et $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ est un $\mathcal{O}_K/\mathfrak{p}$–espace vectoriel de dimension finie, puisque $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini.

Théorème 1.4. *On a la relation*

$$\sum_{i=1}^{r} e_i f_i = [\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}] = [L : K].$$

Démonstration. Voir [Sam71, V.2, théorème 1]. □

Définition 1.5. On dit qu'un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est **ramifié** dans $\mathcal{O}_L$ si l'un des indices de ramification est strictement supérieur à 1.

Il existe une caractérisation élémentaire des idéaux qui se ramifient en fonction du discriminant de l'extension :

Proposition 1.6. *Un idéal premier de $\mathcal{O}_K$ est ramifié dans $\mathcal{O}_L$ si et seulement s'il contient le discriminant relatif $D_{L/K}$.*

Démonstration. Voir [Sam71, V.3, théorème 1]. □

Corollaire 1.7. *Il n'existe qu'un nombre fini d'idéaux premiers de $\mathcal{O}_K$ qui sont ramifiés dans $\mathcal{O}_L$.*

1.1. Exemples

Exemple 1.8 (Corps cyclotomiques). Soit q un premier et $\zeta_q \in \mathbb{C}$ une racine primitive $q^{\text{ème}}$ de l'unité. Considérons le cas $K = \mathbb{Q}$ et L le corps cyclotomique $\mathbb{Q}(\zeta_q)$. On sait que le discriminant de L est (l'idéal engendré par)

$$d_L = (-1)^{\frac{q(q-1)}{2}} p^{q-2}.$$

De manière naturelle, on dit qu'un nombre premier p est ramifié si l'idéal $p\mathbb{Z}$ l'est. Par la proposition 1.6, le seul nombre premier qui est ramifié dans L est p.

Exemple 1.9 (Corps quadratiques). Soit d un entier sans facteur carré. Considérons le cas $K = \mathbb{Q}$ et L le corps quadratique $\mathbb{Q}(\sqrt{d})$. Le discriminant de L est (l'idéal engendré par)

$$d_L = \begin{cases} 4d & \text{si } d \equiv 2,3 \pmod 4 \\ d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Par la proposition 1.6, les seuls nombres premiers ramifiés dans L sont les diviseurs premiers de d, auxquels on adjoint 2 si $d \equiv 2,3 \pmod 4$. Plus précisément, soit p un premier, et considérons la décomposition $p\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}^{e_i}$ de $p\mathbb{Z}$ dans $\mathcal{O}_L$, pour $\mathfrak{P}_i$ des idéaux premiers de $\mathcal{O}_L$ et $e_i \geq 1$ des entiers. Par la proposition 1.4, on a $\sum_{i=1}^{r} e_i f_i = 2$ avec f_i le degré résiduel de $\mathfrak{P}_i$. Par conséquent, les trois possibilités suivantes peuvent avoir lieu :

a) $r = 1$ et $(e_1, f_1) = (1, 2)$, c'est-à-dire que $p\mathcal{O}_L = \mathfrak{P}_1$. En d'autres termes, p *reste premier* (ou est *inerte*) dans $\mathcal{O}_L$.
b) $r = 1$ et $(e_1, f_1) = (2, 1)$, c'est-à-dire que $p\mathcal{O}_L = \mathfrak{P}_1^2$. Dans ce cas, p est *ramifié*.
c) $r = 2$ et $e_1 = e_2 = f_1 = f_2 = 1$, c'est-à-dire que $p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$ avec $\mathfrak{P}_1 \neq \mathfrak{P}_2$ On dit que p se *sépare*.

Il est possible de déterminer plus explicitement quand chacune de ces situations survient en étudiant l'anneau $R := \mathcal{O}_L/p\mathcal{O}_L$. Par le théorème chinois,

$$R \cong \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i},$$

donc R peut prendre les formes suivantes :

a) Si p reste premier, R est un corps.
b) Si p se ramifie, R a des éléments nilpotents.
c) Si p se sépare, R est le produit de deux corps.

Comme un corps n'a pas d'éléments nilpotent et que le produit de deux corps n'est pas un corps, mais n'a pas d'éléments nilpotent, ces implications sont des équivalences. Or, on connaît explicitement l'anneau des entiers $\mathcal{O}_L$,

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \pmod 4, \end{cases}$$

donc on peut déterminer explicitement R. Supposons que p soit impair. Dans ce cas,

$$\frac{1+\sqrt{d}}{2} \equiv (1+p)\frac{1+\sqrt{d}}{2} = \frac{1+p}{2}(1+\sqrt{d}) \text{ dans } \mathcal{O}_L/p\mathcal{O}_L,$$

donc $R = \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$ dans tous les cas. Comme $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[X]/(X^2-d)$, on peut réécrire ce quotient comme

$$\begin{aligned} R &\cong \left(\mathbb{Z}[X]/(X^2-d)\right)/(p) \\ &\cong \mathbb{Z}[X]/(p, X^2-d) \\ &\cong \mathbb{F}_p[X]/(X^2-d). \end{aligned}$$

Le polynôme $X^2 - d \in \mathbb{F}_p[X]$ peut être :

a) irréductible, quand $\left(\frac{d}{p}\right) = -1$.
b) produit de deux termes linéaires distincts, quand $\left(\frac{d}{p}\right) = -1$.
c) égal à X^2, quand $\left(\frac{d}{p}\right) = 0$.

L'anneau R est alors respectivement a) un corps b) un produit de deux corps (théorème chinois) c) un anneau possédant un élément nilpotent. Ainsi, en combinant les deux approches, on conclut que si p est impair,

$$p \begin{cases} \text{reste premier} & \text{si } \left(\frac{d}{p}\right) = -1 \\ \text{se ramifie} & \text{si } \left(\frac{d}{p}\right) = 0 \\ \text{se sépare} & \text{si } \left(\frac{d}{p}\right) = 1. \end{cases}$$

Le cas $p = 2$ se traite de manière similaire, mais en distinguant les cas $d \equiv 2,3 \pmod 4$ et $d \equiv 1 \pmod 4$. On trouve alors que 2 reste premier quand $d \equiv 5 \pmod 8$, se ramifie quand $d \equiv 2,3 \pmod 4$ et se sépare quand $d \equiv 1 \pmod 8$.

Exemple 1.10 (Le corps quadratique $\mathbb{Q}(i)$). Par l'exemple précédent et les propriétés du symbole de Legendre, un nombre premier impair p

$$\begin{cases} \text{reste premier dans } \mathbb{Q}(i) & \text{si } p \equiv 3 \pmod 4 \\ \text{se sépare dans } \mathbb{Q}(i) & \text{si } p \equiv 1 \pmod 4 \end{cases}$$

et aucun nombre premier impair ne se ramifie. De plus, 2 se ramifie.

Ainsi, si $p \equiv 1 \pmod 4$, il existe deux idéaux premiers $\mathfrak{P}_1, \mathfrak{P}_2$ de $\mathbb{Z}[i]$ (l'anneau des entiers de $\mathbb{Q}(i)$) tels que $p\mathbb{Z}[i] = \mathfrak{P}_1\mathfrak{P}_2$. En prenant les normes, on obtient que

$$p^2 = N(\mathfrak{P}_1)N(\mathfrak{P}_2),$$

d'où $N(\mathfrak{P}_1) = N(\mathfrak{P}_2) = p$. Or, $\mathbb{Z}[i]$ est euclidien, donc principal. Il existe par conséquent $x = a + bi \in \mathbb{Z}[i]$ tel que $a^2 + b^2 = N(x) = p$. On a retrouve donc le *théorème des deux carrés de Fermat.*

2. Cas des extensions galoisiennes

Considérons à nouveau une extension de degré fini L d'un corps de nombres K. Nous allons maintenant traiter le cas où cette extension est galoisienne. La séparabilité (resp. l'algébraicité) étant automatiques en caractéristique 0 (resp. pour une extension finie d'un corps de nombre), il suffit de supposer que L/K est une extension normale.

$$\begin{array}{c} L \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Sous ces hypothèses, considérons le groupe de Galois $G = \mathrm{Gal}(L/K)$. Notons que G préserve $\mathcal{O}_L$. En effet, si $x \in \mathcal{O}_L$, alors il existe $P \in \mathbb{Z}[X]$ tel que $P(x) = 0$. Or, si $\sigma \in G$, alors $0 = \sigma(P(x)) = P(\sigma(x))$ puisque $\sigma(K) = K$. Par conséquent, $\sigma(x) \in \mathcal{O}_L$.

Exemples

Exemple 1.11 (Corps quadratiques). Si $K = \mathbb{Q}$ et L est un corps quadratique, rappelons que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2$, le seul $\mathbb{Q}$-automorphisme non-trivial étant la conjugaison $x + y\sqrt{d} \mapsto x - y\sqrt{d}$.

Exemple 1.12 (Corps cyclotomiques). Soit $n \geq 1$ un entier et ζ_n une racine primitive $n^{\text{ème}}$ de l'unité. On considère comme dans l'exemple 1.8 le corps cyclotomique $L = \mathbb{Q}(\zeta_n)$ de $K = \mathbb{Q}$. Rappelons que cette extension a degré $\varphi(n)$ et que $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, un isomorphisme étant donné par $\sigma \in \mathrm{Gal}(L/K) \mapsto [j] \in (\mathbb{Z}/n\mathbb{Z})^\times$, où j est un entier tel que $\sigma(\zeta) = \zeta^j$. Notons que σ envoie ζ sur l'une des racines de $X^n - 1$, c'est-à-dire bien sur ζ^j pour un $0 \leq j < n$.

2.1. Groupes de Galois et décomposition de premiers

Revenons aux questions du chapitre précédent en considérant un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ et sa décomposition

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

en idéaux premiers $\mathfrak{P}_i$ dans $\mathcal{O}_L$.

Soit σ un élément de $\mathrm{Gal}(L/K)$. Comme ce dernier préserve $\mathcal{O}_L$, l'image $\sigma(\mathfrak{P}_i)$ est un idéal de $\mathcal{O}_L$ pour tout $i = 1, \ldots, r$. Or $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$ (Proposition 1.2), donc

$$\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P}_i) \cap \sigma(\mathcal{O}_K) = \sigma(\mathfrak{P}_I) \cap \mathcal{O}_K.$$

Par conséquent, $\sigma(\mathfrak{P}_i)$ est l'un des $\mathfrak{P}_j$. En d'autres termes, *le groupe de Galois de L/K agit sur les idéaux au-dessus de $\mathfrak{p}$.*

Définition 1.13. Le stabilisateur d'un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ sous l'action de $\mathrm{Gal}(L/K)$ est appelé **groupe de décomposition** $D_{\mathfrak{P}}$ de l'idéal.

Définition 1.14. Un idéal de $\mathcal{O}_L$ et son image par un élément du groupe de Galois sont dits **conjugués**.

Par la théorie élémentaire des actions de groupes, on a alors une bijection entre $\mathrm{Gal}(L/K)/D_{\mathfrak{P}}$ et l'ensemble des idéaux au-dessus de $\mathfrak{p}$ conjugués à $\mathfrak{P}$.

Le résultat suivant montre que l'action de $\mathrm{Gal}(L/K)$ sur les idéaux au-dessus de $\mathfrak{p}$ est en fait transitive :

Proposition 1.15. *Tous les idéaux au-dessus de $\mathfrak{p}$ sont conjugués.*

Démonstration. Voir [Sam71, VI.2, proposition 1]. □

Corollaire 1.16. *Tous les idéaux au-dessus de $\mathfrak{p}$ ont le même indice de ramification e et le même degré résiduel f. De plus, on a $[L : K] = efr$, où r est le nombre d'idéaux premiers divisant $\mathfrak{p}\mathcal{O}_L$.*

Démonstration. Voir [Sam71, VI.2, proposition 1]. □

Puisque tous les idéaux au-dessus de $\mathfrak{p}$ sont conjugués, ils ont tous exactement r conjugués. Par conséquent, $|\operatorname{Gal}(L/K)/D_{\mathfrak{P}}| = r$, donc $|D_{\mathfrak{P}}| = n/r = ef$.

2.2. Sous-groupe d'inertie

Au début du chapitre, nous avons considéré l'extension $\mathcal{O}_L/\mathfrak{P}$ de $\mathcal{O}_K/\mathfrak{p}$, qui est une extension de *corps finis* (donc galoisienne). Intéressons-nous maintenant au groupe de Galois $H = \operatorname{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$ de celle-ci.

Notons que si $\sigma \in D_{\mathfrak{P}}$, alors σ induit un morphisme $\overline{\sigma} \in H$ de manière naturelle par

$$\overline{\sigma}([x]_{\mathfrak{P}}) = [\sigma(x)]_{\mathfrak{P}}.$$

De là, on voit qu'il existe un homomorphisme de groupes

$$\begin{aligned} \Phi : D_{\mathfrak{P}} &\to H \\ \sigma &\mapsto \overline{\sigma}. \end{aligned}$$

Définition 1.17. Le noyau de Φ s'appelle **sous-groupe d'inertie** $I_{\mathfrak{P}}$ pour $\mathfrak{P}$.

Proposition 1.18. *Les points suivants sont vérifiés :*

a) L'extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ est galoisienne.

b) L'homomorphisme Φ est surjectif, donc on a un isomorphisme

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong H.$$

c) Le sous-groupe d'inertie pour $\mathfrak{P}$ a taille e, l'indice de ramification de $\mathfrak{P}$.

Démonstration. Voir [Sam71, VI.2, proposition 2 et son corollaire]. □

Ainsi, les sous-groupes d'inerties "mesurent" la ramification de $\mathfrak{p}$ dans $\mathcal{O}_L$.

2.3. Automorphisme de Frobenius

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ qui ne soit pas ramifié dans $\mathcal{O}_L$. Par la proposition 1.18, le sous-groupe d'inertie de $\mathfrak{P}$ est trivial et on a un isomorphisme naturel $D_{\mathfrak{P}} \cong H$.

Or, H est le groupe de Galois d'une extension de corps finis. En particulier, il est cyclique, engendré par l'automorphisme de Frobenius

$$\begin{aligned} \sigma : \mathcal{O}_L/\mathfrak{P} &\to \mathcal{O}_L/\mathfrak{P} \\ x &\mapsto x^{N(\mathfrak{p})}, \end{aligned}$$

du fait que $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. Par conséquent, D *est cyclique.*

Définition 1.19. Le générateur de $D_{\mathfrak{P}}$ induit par σ est également appelé **automorphisme de Frobenius** en $\mathfrak{P}$ de L/K. On note cet automorphisme $(\mathfrak{P}, L/K)$

Le résultat suivant montre que pour tout ce qui précède, la dépendance avec le choix d'un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ est uniquement à conjugaison près :

Proposition 1.20. *Soit $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$ et $\sigma \in G$. Alors*

1. $D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ *et* $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$,
2. $(\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$.

Démonstration. Voir [Sam71, VI.3]. □

Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on parlera donc du *Frobenius $\sigma_{\mathfrak{p}}$ associé à $\mathfrak{p}$*, défini dans $\mathrm{Gal}(L/K)$ à conjugaison près. Dans le cas d'une extension abélienne, les Frobenius sont alors directement définis dans le groupe de Galois de l'extension et on notera $\sigma_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$. La similitude avec la notation pour le symbole de Legendre sera explicitée dans un exemple ci-après.

Les Frobenius se comportent bien par rapport aux extensions, comme le montre la proposition suivante :

Proposition 1.21. *Soit $L/M/K$ une tour de corps de nombres avec L/K galoisienne. Si $\mathfrak{p}$ est un idéal de K qui ne se ramifie pas dans L, alors*

a) L'idéal $\mathfrak{p}$ ne se ramifie pas dans M ;
b) Si $\mathfrak{P}$ un idéal au-dessus de $\mathfrak{p}$ dans L, alors $\mathfrak{P} \cap M$ est un idéal au-dessus de $\mathfrak{p}$ dans M ;
c) Si M/K est galoisienne, la restriction du Frobenius $(\mathfrak{P}, L/K) : L \to L$ à M est égale à $(\mathfrak{P} \cap M, M/K)$.

Démonstration. Voir [Sam71, VI.3, proposition 1]. □

Exemples

Exemple 1.22 (Corps quadratiques). Considérons comme précédemment le cas d'une extension quadratique $L = \mathbb{Q}(\sqrt{d})$ de $K = \mathbb{Q}$, pour d un entier sans facteur carré.

Soit $p > 2$ un nombre premier qui ne se ramifie pas, c'est-à-dire que p ne divise pas d selon l'exemple 1.9. Pour $\mathfrak{P} \subset \mathcal{O}_L$ au-dessus de p, le sous-groupe de décomposition $D_{\mathfrak{P}}$ est donc soit le groupe trivial, soit isomorphe à $\mathbb{Z}/2$. Si f est le degré résiduel, nous avons que $|D_{\mathfrak{P}}| = f \cdot 1 = f$, donc

a) Si p se sépare, alors $D_{\mathfrak{P}} \cong \mathbb{Z}/2$;

b) Si p reste premier, alors $D_{\mathfrak{P}}$ est le sous-groupe trivial.

En d'autres termes, selon l'exemple 1.9, le Frobenius $\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right)$ est égal à $\left(\frac{d}{p}\right) \in \{-1, 1\}$ respectivement, en identifiant les éléments du groupe de Galois avec cet ensemble. Ceci explique la similitude des notations entre Frobenius et symbole de Legendre.

Exemple 1.23 (Corps cyclotomiques). Comme dans l'exemple 1.8, soit q un nombre premier et ζ une racine primitive $q^{\text{ème}}$ de l'unité dans $\mathbb{C}$. On considère l'extension galoisienne $L = \mathbb{Q}(\zeta_q)$ de $K = \mathbb{Q}$. Rappelons que

$$\mathrm{Gal}(L/K) \cong (\mathbb{Z}/q)^\times$$

(exemple 1.12), qui contient le sous-groupe $(\mathbb{Z}/q)^{\times 2}$ d'indice 2. Par le théorème fondamental de la théorie de Galois, il existe un corps intermédiaire $\mathbb{Q} \subset M \subset \mathbb{Q}(\zeta)$ tel que $[M : \mathbb{Q}] = 2$.

$$\begin{array}{ccc} \mathbb{Q}(\zeta) & & \{1\} \\ | & & | \\ M & & (\mathbb{Z}/q)^{\times 2} \\ {\scriptstyle 2}\,| & & |\,{\scriptstyle \text{ind. } 2} \\ \mathbb{Q} & & (\mathbb{Z}/q)^\times \end{array}$$

On peut supposer que $M = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans facteur carré. Par l'exemple 1.9, les diviseurs premiers de d se ramifient dans M, donc se ramifient dans $\mathbb{Q}(\zeta)$. Comme les seuls premiers qui se ramifient dans $\mathbb{Q}(\zeta)$ sont les diviseurs de q, on obtient que $d = \pm q$. De plus, comme on suppose q impair, le premier 2 ne se ramifie pas dans $\mathbb{Q}(\zeta)$, donc le discriminant de $\mathbb{Q}(\sqrt{d})$ ne peut pas être un multiple de 4. Comme

$$d_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 4d & \text{si } d \equiv 2, 3 \pmod 4 \\ d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

(exemple 1.9), on trouve finalement que

$$d = \begin{cases} q & \text{si } q \equiv 1 \pmod 4 \\ -q & \text{si } q \equiv 3 \pmod 4 \end{cases} = (-1)^{\frac{q-1}{2}} q.$$

Soit p un nombre premier différent de q, non-ramifié dans $\mathbb{Q}(\zeta)$. Comme les extensions sont abéliennes, on peut considérer le Frobenius $\sigma_p = \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p}\right)$, dont la restriction à $\mathbb{Q}(\sqrt{d})$ est égale au Frobenius $\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right)$ par la proposition 1.21. Cette restriction peut être calculée de deux manières :

1. Par l'exemple 1.22, $\sigma_p\big|_{\mathbb{Q}(\sqrt{d})} = \left(\frac{d}{p}\right)$.
2. Par définition de σ_p, on a que $\sigma_p(\zeta) = \zeta^p$. Dans $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$, le Frobenius σ_p est identifié à $[p]_q$. Sa restriction à $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est donc triviale si et seulement si p est un carré modulo q. Par conséquent, $\sigma_p\big|_{\mathbb{Q}(\sqrt{d})} = \left(\frac{p}{q}\right)$.

Ainsi, on trouve que

$$\left(\frac{p}{q}\right) = \left(\frac{d}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right),$$

c'est-à-dire la loi de réciprocité quadratique !

3. Généralisation aux anneaux de Dedekind

En fait, la théorie présentée ci-dessus se généralise dans le cas d'extensions finies de corps de fractions d'anneaux de Dedekind. Plus précisément, soit A un anneau de Dedekind avec corps de fractions K. Soit L une extension finie de K et B la clôture intégrale de A dans L. Supposons que B soit un A-module finiment généré, donc en particulier un anneau de Dedekind avec corps de fractions L. Pour tout idéal premier (ou maximal) $\mathfrak{p}$ de A, il existe des idéaux premiers $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ de B (uniques à permutation près) et $e_1, \ldots, e_n \geq 1$ tels que

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}.$$

$$\begin{array}{ccc} L & \text{——} & B \\ | & & | \\ K & \text{——} & A \end{array} \qquad \begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{p} \end{array}$$

Notons que si A est l'anneau des entiers d'un corps de nombres, on retrouve précisément la situation du début du chapitre. Par analogie, on appelle les $\mathfrak{P}_i$ les *idéaux au-dessus de* $\mathfrak{p}$, les e_i les *indices de ramification* et les $f_i = [B/\mathfrak{P} : A/\mathfrak{p}]$ les *degrés résiduels*.

On dit que $\mathfrak{p}$ *se ramifie* dans B si $e_i > 1$ pour un certain i *ou* si l'extension $(B/\mathfrak{P}_i)/(A/\mathfrak{p})$ n'est pas séparable pour un certain i. Notons que dans le cas des anneaux d'entiers de corps de nombres, cette extension est une extension de corps finis, donc toujours séparable. Ainsi, les deux définitions coïncident.

On a alors les résultats suivants, analogues au cas des corps de nombres :

Proposition 1.24. $[L : K] = \sum_{i=1}^{r} e_i f_i$.

Proposition 1.25. *Un idéal premier* $\mathfrak{p}$ *de* A *se ramifie dans* B *si et seulement si* $\mathfrak{p} \mid \Delta_{B/A}$*, où le* discriminant $\Delta_{B/A}$ *est l'idéal de* A *généré par les éléments* $disc(b_1, \ldots, b_n)$ *pour toute base* $(b_1, \ldots, b_n)$ *de* L/K *contenue dans* B*. En particulier, si* $\Delta_{B/A} \neq 0$*, il n'y a qu'un nombre fini d'idéaux premiers de* A *se ramifiant dans* B*.*

Nous utiliserons cette généralisation pour étudier le degré d'un morphisme de courbes au chapitre suivant. Pour les preuves de ces résultats, voir [Lor96, Ch. III et Ch. IV].

Chapitre 2

Densité d'ensembles d'idéaux et équirépartition dans les groupes compacts

Soit L/K une extension galoisienne de corps de nombres. Dans le chapitre précédent, nous avons vu l'existence d'une application

$$\text{Frob} : \{\mathfrak{p} \text{ premier ne se ramifiant pas dans } L\} \to \text{Gal}(L/K)/\text{conjugaison},$$

associant à un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ ne se ramifiant pas dans L le Frobenius $\sigma_\mathfrak{p} \in \text{Gal}(L/K)$ défini à conjugaison près.

$$\begin{array}{ccc} L & \text{——} & \mathcal{O}_L \\ | & & | \\ K & \text{——} & \mathcal{O}_K \end{array} \qquad \begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{p} \end{array} \qquad \sigma_\mathfrak{p} \in \text{Gal}(L/K)/\text{conjugaison}$$

Nous avons déjà vu l'intérêt d'étudier ces endomorphismes, en redémontrant par exemple la loi de réciprocité quadratique. En fait, l'étude de la *répartition* de l'image de l'application Frob dans les classes de conjugaison de $\text{Gal}(L/\mathbb{Q})$ amène également des questions très intéressantes, comme l'illustre l'exemple suivant :

Exemple 2.1. Soit q un nombre premier et ζ une racine primitive $q^{\text{ème}}$ de l'unité dans $\mathbb{C}$. Tout nombre premier p différent de q ne se ramifie pas dans le corps cyclotomique $\mathbb{Q}(\zeta)$, donc on peut lui associer un Frobenius, défini dans $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$ (à priori à conjugaison près, mais ce groupe est abélien). Nous avons vu que celui-ci est associé à la classe de p dans $(\mathbb{Z}/q)^\times$. Ainsi, étudier la répartition des σ_p dans $(\mathbb{Z}/q)^\times$ équivaut à étudier la répartition des premiers différent de q dans $(\mathbb{Z}/q)^\times$. Or, c'est exactement ce que l'on souhaite faire dans le célèbre *théorème de la progression arithmétique* de Dirichlet qui énonce que pour tout entier a premier à q,

$$|\{p \leq x \text{ premier } : p \equiv a \pmod q\}| = \frac{1}{\varphi(q)} \frac{x}{\log x} + o\left(\frac{x}{\log x}\right),$$

donc en particulier qu'il existe une infinités de premiers p tels que $p \equiv a \pmod q$ (ou plus généralement pour q composé et a premier à q par application du théorème chinois).

Le **théorème de densité de Chebotarev**, dont l'étude est l'une des finalités de cette première partie, généralise le théorème de la progression arithmétique à la question suivante :

Question 2.2. *Étant donnée une extension galoisienne finie de corps de nombres L/K, quelle est la* répartition *(sens à préciser plus tard) de l'image de Frob dans les classes de conjugaison de* $\mathrm{Gal}(L/K)$ *?*

Avant d'étudier cela plus en détails, nous nous nous attachons à définir formellement ce que l'on entend par *répartition* dans la question 2.2. En fait, dans ce document, nous allons parler de répartition dans les contextes suivants :

— *Répartition/densité* des Frobenius $\mathrm{Frob}(\mathfrak{p})$ dans les classes de conjugaison de $\mathrm{Gal}(L/K)$, afin de répondre à la question 2.2.

— *Répartition* d'une suite (x_p) dans les classes de conjugaison de $\mathbb{R}/\mathbb{Z}$ et $\mathrm{SU}_2(\mathbb{C})$ dans la deuxième partie.

— *Répartition* d'une variable aléatoire $(\theta_p) \subset [0, \pi]$ dans la deuxième partie.

Par conséquent, nous commencerons par parler de répartition dans les classes de conjugaison d'un groupe compact (couvrant les deux premiers cas), avant de parler de densités d'ensembles d'idéaux pour traiter le second.

1. Equirépartition dans les groupes compacts

Dans cette section, nous considérons un groupe compact de Hausdorff noté G.

Exemple 2.3. Dans ce travail, les groupes compacts que nous allons considérer sont les groupes finis (avec la topologie discrète), $\mathbb{R}/\mathbb{Z} \cong S^1$ et $\mathrm{SU}_2(\mathbb{C}) \cong S^3$.

En premier lieu, nous faisons quelques rappels au sujet de la mesure de Haar et des représentations des groupes compacts. Pour les preuves des résultats de cette section et plus de détails, voir par exemple [Var07].

1.1. Mesure de Haar

Rappelons que G, en tant que groupe compact de Hausdorff, possède une unique *mesure de Haar normalisée*, c'est-à-dire une mesure μ sur la σ-algèbre borélienne $\mathcal{F}$ générée par ses sous-ensembles compacts, qui soit :

1. Invariante à gauche : $\mu(gA) = \mu(A)$ pour tout $A \in \mathcal{F}$
2. Finie sur tous les sous-ensembles compacts ;
3. Extérieurement régulière pour les éléments A de $\mathcal{F}$:

$$\mu(A) = \inf\{\mu(U) : A \subset U \in \mathcal{F} \text{ ouvert}\};$$

4. Extérieurement régulière pour les éléments A de $\mathcal{F}$ qui sont ouvertes :
$$\mu(A) = \sup\{\mu(K) : K \subset A,\ K \text{ compact}\};$$
5. Normalisée : $\mu(G) = 1$.

Remarque 2.4. En fait, une telle mesure, hormis le cinquième point, existe sur tout groupe *localement compact* de Hausdorff, et est unique à constante près. Par le deuxième point, on peut la supposer normalisée si G est compact.

Exemple 2.5. Si G est un groupe fini, alors $\mu(X) = |X|/|G|$ pour tout $X \subset G$. Dans le dernier chapitre, nous déterminerons explicitement la mesure de Haar sur $\mathrm{SU}_2(\mathbb{C})$. En tant que groupe localement compact de Hausdorff, la mesure de Haar sur $\mathbb{R}^\times$ est $dx/|x|$ (à constante près), i.e. $\mu(X) = \int_X \frac{1}{|x|}dx$ si $X \subset \mathbb{R}^\times$ est borélien. Similairement, la mesure de Haar sur $\mathrm{GL}_n(\mathbb{R})$ est $dX/|\det(X)|$, où dX est la mesure de Lebesgue sur $\mathbb{R}^{n^2}$.

Rappelons la propriété suivante qui sera utile par la suite :

Lemme 2.6. *Tout ouvert de G ayant mesure nulle est vide.*

Pour une fonction $f : G \to \mathbb{C}$ mesurable par rapport à $\mathcal{F}$, on définit l'intégrale de Lebesgue
$$\int_G f d\mu.$$
Notons que puisque μ est G-invariante à gauche, on a que $\int_G f(gx)d\mu(x) = \int_G f(x)d\mu(x)$ pour tout $g \in G$.

1.2. Représentations et caractères

Définition 2.7. Une **représentation** de G est un homomorphisme continu $\rho : G \to \mathrm{GL}(V)$, pour V un espace vectoriel complexe de dimension finie. Comme dans le cas fini, on munit V d'une structure de G-module et on définit la somme directe, l'irréducibilité de représentations ou encore l'équivalence entre deux représentations.

En utilisant la mesure de Haar, on peut toujours supposer que V est un espace de Hilbert tel que $\rho(g)$ soit unitaire pour tout $g \in G$ (on dit dans ce cas que ρ est **unitaire**). En effet, il suffit de définir le produit scalaire $\langle -, - \rangle : V \times V \to \mathbb{C}$ par
$$\langle v, w \rangle = \int_G \langle \rho(x)(v), \rho(x)(w) \rangle_{\text{eucl.}} d\mu,$$
pour μ la mesure de Haar de G et utiliser la G-invariance de l'intégrale. Il s'agit en fait d'une manière de généraliser le théorème de Maschke. En effet, supposons que W soit un sous-G-module de V (par rapport à ρ). Le

complément orthogonal $W^\perp$ de W par rapport au produit scalaire ci-dessus est alors également un G-sous-module de V par unitarité des $\rho(g)$ ($g \in G$). Ainsi, on a le résultat suivant :

Proposition 2.8. *Toute représentation de G est une somme directe (finie) de représentations irréductibles.*

De la même manière que dans le cas d'un groupe fini, on montre que toute représentation irréductible d'un groupe compact *abélien* est de dimension 1.

Définition 2.9. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. Le **caractère** associé est la composition

$$\chi_\rho = \mathrm{tr} \circ \rho : G \to \mathbb{C},$$

pour $\mathrm{tr} : \mathrm{GL}(V) \to \mathbb{C}$ l'homomorphisme trace. En particulier, il s'agit d'un homomorphisme continu.

Comme vu ci-dessus, on peut supposer que ρ est unitaire. Par conséquent, les valeurs propres de $\rho(x)$ ont valeur absolue 1 pour tout $x \in G$ d'où $|\chi_p(x)| \leq \dim V$ pour tout $x \in G$.

De la même manière que dans le cas des groupes finis, on munit l'espace vectoriel des fonctions intégrables $f : G \to \mathbb{C}$ d'un produit scalaire donné par

$$(f, g) = \int_G f\overline{g}\, d\mu$$

et on définit $L^2(G) = \{f : G \to \mathbb{C} \text{ intégrable } : (f, f) < \infty\}$. Similairement au cas fini, on a alors :

Proposition 2.10. *L'ensemble des caractères irréductibles de G est une base orthonormée du sous-espace de $L^2(G)$ constitué des fonctions centrales.*

En particulier, on trouve également qu'un caractère χ est irréductible si et seulement si $(\chi, \chi) = 1$.

Le dernier résultat qui nous sera utile est le suivant :

Proposition 2.11. *Le sous-espace engendré par les caractères irréductibles est dense (par rapport à la norme uniforme) dans l'espace des fonctions continues centrales $f : G \to \mathbb{C}$.*

Exemple 2.12. Les caractères du groupe compact $G = \mathbb{R}/\mathbb{Z} \cong S^1$ sont les $\chi_m : G \to \mathbb{C}^\times$ définis par $\chi_m(x) = e^{2i\pi xm}$, pour $m \in \mathbb{Z}$. En effet, comme G est abélien, toute représentation est de dimension 1, donc les caractères sont les homomorphismes de groupes continus $\chi : G \to \mathbb{C}^\times$. Par le même raisonnement d'unitarité que ci-dessus, un tel χ vérifie $|\chi(x)| = 1$ pour tout

$x \in G$. Par conséquent, on peut voir χ comme un homomorphisme continu de S^1 dans lui-même. Or, il est bien connu que ceux-ci sont sous précisément les applications sous la forme ci-dessus.

1.3. Équirépartition dans les classes de conjugaison

Nous pouvons maintenant définir et étudier le concept d'équirépartition qui nous intéressera.

Définition 2.13. Soit G un groupe compact et X l'ensemble de ses classes de conjugaison. Une suite $(x_n) \subset X$ est dite **équirépartie** si

$$\lim_{n\to\infty} \frac{1}{N} \sum_{n\leq N} f(x_n) = \int_X f d\mu$$

pour toute fonction continue $f : X \to \mathbb{R}$, où μ est la mesure induite sur X par la mesure de Haar sur G.

Proposition 2.14. *Dans les notations de la définition 2.13, si (x_n) est équirépartie, alors pour tout $C \subset X$ tel que $\mu(\partial C) = 0$, alors*

$$\lim_{N\to\infty} \frac{|\{n \leq N : x_n \in C\}|}{N} = \mu(C).$$

Démonstration. Considérons l'indicatrice $1_C : X \to \mathbb{R}$ de C. L'ensemble de ses points de discontinuité est ∂C, que l'on suppose par hypothèse de mesure nulle. Soit $\varepsilon > 0$. Par [Bou04, Lemme IV.5.5], il existe une fonction continue $f : X \to \mathbb{R}$ et une fonction continue bornée positive $g : X \to \mathbb{R}$ telles que $||1_C - f||_\infty \leq g$ et $\int_X g d\mu \leq \varepsilon$. La dernière condition implique que $g \leq \varepsilon$ presque partout. Par continuité, l'ensemble des $x \in X$ où $g(x) > \varepsilon$ est ouvert, donc le lemme 2.6 implique que celui-ci est vide, i.e. $g \leq \varepsilon$. Par conséquent, la différence $|\frac{1}{N}\sum_{n\leq N} 1_C(x_n) - \mu(C)|$ est bornée par

$$\left|\frac{1}{N}\sum_{n\leq N}(1_C(x_n) - f(x_n))\right| + \left|\frac{1}{N}\sum_{n\leq N} f(x_n) - \int_X f d\mu\right| + \left|\int_x (f - 1_C) d\mu\right| \leq 3\varepsilon$$

pour N assez grand. □

Exemple 2.15. Pour le groupe compact $G = \mathbb{R}/\mathbb{Z} \cong S^1$, nous avons $X \cong G$ (en tant qu'ensembles) et si l'image dans G d'une suite $(x_n) \subset \mathbb{R}$ est équirépartie, on dit que (x_n) est *équirépartie mod* 1. Remarquons qu'une suite $(x_n) \subset [0, 1) \hookrightarrow G$ est équirépartie si et seulement si

$$\lim_{N\to\infty} \frac{|\{n \leq N : x_n \in (\alpha, \beta)\}|}{N} = \beta - \alpha \tag{2.1}$$

pour tous $0 \leq \alpha < \beta \leq 1$. En effet, notons que par l'isomorphisme de groupes topologiques $\mathbb{R}/\mathbb{Z} \cong S^1$, l'image de l'intervalle (α, β) dans G correspond à un arc de cercle, dont la mesure de Haar sur S^1 est l'aire normalisée $\beta - \alpha$. Si la suite (x_n) est équirépartie au sens de la définition 2.13, il suffit d'appliquer la proposition 2.14 à (α, β). Réciproquement, supposons que (x_n) satisfasse (2.1) et soit $f : G \to \mathbb{R}$ une fonction continue. Soit $\varepsilon > 0$. Puisque f est à support compact, il existe des intervalles $I_1, \ldots, I_m \subset [0,1]$ et $c_1, \ldots, c_m \in \mathbb{R}$ tels que $||f - \sum_{i=1}^m c_i \chi_{I_i}||_\infty < \varepsilon$. Par hypothèse, on a alors pour $N = N(m, \varepsilon)$ assez grand que

$$\left| \frac{1}{N} \sum_{n \leq N} \sum_{i=1}^m c_i \chi_{I_i}(x_n) - \sum_{i=1}^m c_i |I_i| \right| \leq \sum_{i=1}^m c_i \left| \frac{1}{N} |\{n \leq N : x_n \in I_i\}| - |I_i| \right| \leq \varepsilon.$$

Par conséquent, la différence $|\frac{1}{N} \sum_{n \leq N} f(x_n) - \int_X f d\mu|$ est bornée par

$$\left| \frac{1}{N} \sum_{n \leq N} (f(x_n) - \sum_{i=1}^m c_i \chi_{I_i}(x_n)) \right| + \varepsilon + \left| \int_X (\sum_{i=1}^m c_i \chi_{I_i} - f) d\mu \right| \leq 2\varepsilon$$

et on obtient le résultat en passant à la limite.

A la place des indicatrices d'intervalles, nous aurions pu utiliser dans l'exemple précédent tout sous-espace dense (pour la norme uniforme) dans l'espace des fonctions continues à support compact. Par conséquent, on obtient exactement de la même manière le résultat suivant, en utilisant la proposition 2.11 :

Proposition 2.16 (Critère d'équirépartition de Weyl pour les groupes compacts)**.** *Soit G un groupe compact et X l'ensemble de ses classes de conjugaison. Alors une suite $(x_n) \subset X$ est équirépartie si et seulement si*

$$\sum_{n \leq N} \chi(x_n) = o(N)$$

quand $N \to \infty$ pour tout caractère irréductible $\chi \neq 1$ de G.

Exemple 2.17. Par l'exemple 2.12, une suite $(x_n) \subset \mathbb{R}/\mathbb{Z}$ est équirépartie si et seulement si

$$\sum_{n \leq N} e^{2i\pi m x_n} = o(N)$$

pour tout $m \in \mathbb{Z}$ non-nul. Il s'agit du critère d'équirépartition de Weyl sous sa forme classique. Pour le démontrer, sans utiliser la théorie des représentation des groupes compacts, on utilise le théorème de Stone-Weierstrass pour approximer les indicatrices d'intervalles de l'exemple 2.15 par des polynômes trigonométriques. C'est en fait ce même théorème que l'on utilise pour démontrer la proposition 2.11.

2. Densité et répartition d'ensembles d'idéaux premiers

Comme annoncé, nous étudions maintenant les questions de densité, afin de munir l'ensemble des idéaux premiers d'un corps de nombres d'une structure de (semi-)espace de probabilités.

2.1. Densité d'ensembles d'idéaux premiers

Pour cette section, fixons un corps de nombres K. Pour $x \geq 1$, soit $\pi_K(x) := |\{\mathfrak{p} \subset \mathcal{O}_K \text{ premier } : N(\mathfrak{p}) \leq x\}|$. Notons que $\pi_{\mathbb{Q}}(x) = \pi(x)$.

Définition 2.18. Un ensemble $\mathcal{P}$ d'idéaux premiers de $\mathcal{O}_K$ a **densité naturelle** λ si

$$\lim_{x \to +\infty} \frac{|\{\mathfrak{p} \in \mathcal{P} : N(p) \leq x\}|}{\pi_K(x)} = \lambda.$$

Exemple 2.19. Soit m un entier et a un entier premier à m. Alors l'ensemble des premiers p tels que $p \equiv a \pmod m$ a densité naturelle $1/\varphi(m)$ par le théorème de la progression arithmétique. En effet, ce dernier indique que

$$|\{p \leq x \text{ premier } : p \equiv a \pmod m\}| = \frac{1}{\varphi(m)} \frac{x}{\log x} + o\left(\frac{x}{\log x}\right),$$

ce qui implique l'affirmation par le théorème des nombres premiers. En d'autres termes, les premiers mod m sont équirépartis dans $(\mathbb{Z}/m)^\times$.

Proposition 2.20. *Si un ensemble d'idéaux premiers a une densité naturelle qui soit non-nulle, alors il est infini.*

Démonstration. Nous verrons plus tard (Théorème 4.4) que $\pi_K(x) \sim \frac{x}{\log x} \to +\infty$ quand $x \to +\infty$, d'où le résultat. □

Remarque 2.21. On peut aussi définir une notion de *densité analytique* (ou *densité de Dirichlet*) de $\mathcal{P}$ par la limite

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \subset \mathcal{O}_K} N(\mathfrak{p})^{-s}}$$

si elle existe, de telle sorte qu'un ensemble ayant une densité naturelle possède alors la même densité analytique (mais le contraire est en général faux). On remarquera plus loin que les hypothèses de certains résultats donnant une densité naturelle peuvent être affaiblies si l'on souhaite uniquement une information sur la densité analytique.

2.2. Répartition d'ensembles d'idéaux premiers

Soit K un corps de nombres. Dans la deuxième partie de ce travail, on souhaitera parler de répartition de variables aléatoire $X(\mathfrak{p}) \in \mathbb{R}$ avec $\mathfrak{p}$ un idéal premier de K. Afin de faire cela formellement, nous définissions un (semi-) espace de probabilités sur l'ensemble $\mathbb{P}$ des idéaux premiers de K, à l'aide des idées de la section précédente.

Pour tout sous-ensemble E de $\mathbb{P}$, on peut considérer la limite

$$\lim_{n\to\infty} \frac{|\{\mathfrak{p} \in \mathcal{P} : N(\mathfrak{p}) \leq n, \mathfrak{p} \in E\}|}{\pi_K(n)},$$

qui définit la densité naturelle $\mu(E)$ de E si elle existe. Notons $\mathcal{F}$ le sous-ensemble de $\mathbb{P}$ constitué des ensembles admettant une densité naturelle. La fonction $\mu : \mathcal{F} \to [0,1]$ définit alors une mesure de probabilité sur l'espace $(\mathbb{P}, \mathcal{F})$, à l'exception de l'additivité dénombrable infinie.

Rappelons que la **fonction de répartition** d'une variable aléatoire $\{X_\mathfrak{p}\}_\mathfrak{p}$ est la fonction $F : \mathbb{R} \to \mathbb{R}$ définie par $F(x) = \mu(X_\mathfrak{p} \leq x)$. Etudier la répartition de $\{X_\mathfrak{p}\}_\mathfrak{p}$ signifie alors précisément étudier sa fonction de répartition.

Nous dirons qu'une variable aléatoire $\{X_\mathfrak{p}\}_\mathfrak{p}$ est **discrète** si elle ne prend qu'un nombre fini de valeurs et **continue** si elle admet une **fonction de densité**, c'est-à-dire une fonction continue $f : \mathbb{R} \to \mathbb{R}$ telle que

$$F(\beta) - F(\alpha) = \mu\left(X_\mathfrak{p} \in [\alpha, \beta]\right) = \int_\alpha^\beta f(x)dx$$

pour tout intervalle $[\alpha, \beta] \subset \mathbb{R}$. Si la fonction de répartition de $\{X_\mathfrak{p}\}_\mathfrak{p}$ ne possède qu'un nombre fini de discontinuités, alors il est facile de voir qu'elle s'écrit comme combinaison convexe d'une fonction de répartition d'une variable aléatoire continue et d'une variable aléatoire discrète.

Exemple 2.22. Une variable aléatoire $\{X_\mathfrak{p}\}_\mathfrak{p}$ est continue avec fonction de répartition $f = \frac{1}{b-a} 1_{[a,b]}$ si

$$\lim_{n\to\infty} \frac{|\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq n,\ X_\mathfrak{p} \in [\alpha, \beta]\}|}{\pi_K(n)} = \frac{1}{b-a} \left|[\alpha, \beta] \cap [a, b]\right|,$$

pour tout intervalle $[\alpha, \beta] \subset \mathbb{R}$, c'est-à-dire précisément que $X_\mathfrak{p}$ est *équirépartie* dans $[a, b]$, selon l'exemple 2.15.

Finalement, le résultat suivant donne un parallèle à la définition 2.13 :

Proposition 2.23. *Une variable aléatoire $(X_\mathfrak{p})_\mathfrak{p}$ admet comme fonction de densité $f \in C(\mathbb{R})$ si et seulement si*

$$\lim_{N\to\infty} \frac{1}{\pi_K(N)} \sum_{p \leq N} g(X_\mathfrak{p}) = \int_\mathbb{R} g(x) f(x) dx$$

pour toute fonction continue à support compact $g : \mathbb{R} \to \mathbb{R}$.

Démonstration. On procède comme dans l'exemple 2.15, en approximant uniformément g par des indicatrices d'intervalles et réciproquement en approximant uniformément l'indicatrice d'un intervalle par une fonction continue. □

Chapitre 3

Fonctions L associées à des représentations de groupes compacts

La preuve du théorème de la progression arithmétique et celle du théorème des nombres premiers se basent sur l'étude de fonctions L associées à des caractères de Dirichlet, en particulier sur leur prolongement méromorphe et leur non-annulation sur la droite $\mathrm{Re}(s) = 1$. Dans ce chapitre, nous introduisons une généralisation de ces fonctions associées à des représentations de groupes de Galois d'extensions de corps de nombres. Dans le chapitre suivant, nous verrons comment elles s'utilisent pour caractériser des énoncés d'équirépartition, démontrer le théorème de Chebotarev (généralisant le théorème de Dirichlet) ainsi que la généralisation du théorème des nombres premiers à des corps de nombres.

1. Motivation

A tout caractère de Dirichlet [1] $\chi : (\mathbb{Z}/q)^\times \to \mathbb{C}^\times$ (q un premier), rappelons que l'on associe la fonction L de Dirichlet

$$L_q(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p \neq q} \frac{1}{1 - \chi(p)p^{-s}},$$

qui admet un prolongement holomorphe sur $\mathrm{Re}(s) > 0$ si $\chi \neq 1$. Notons que si ζ est une racine $q^{\text{ème}}$ de l'unité, alors

$$(\mathbb{Z}/q)^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}),$$

donc χ *peut être vu comme un caractère du groupes de Galois de* $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Si un premier p est distinct de q, il n'est pas ramifié et on peut alors considérer le Frobenius associé $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$ (bien défini puisque ce groupe est abélien). Dans le chapitre précédent, nous avons montré que σ_p correspond à la classe de p dans $(\mathbb{Z}/q)^\times$. Par conséquent, en identifiant les deux groupes, on peut aussi écrire

$$L_q(\chi, s) = \prod_{p \neq q} \frac{1}{1 - \chi(\sigma_p)p^{-s}},$$

écriture que l'on va pouvoir généraliser à d'autres corps de nombres galoisiens.

1. Implicitement prolongé en une fonction arithmétique q-périodique $\chi : \mathbb{Z} \to \mathbb{C}$ par $\chi(m) = \chi([m]_q)$ si $(m, q) = 1$ et $\chi(m) = 0$ sinon.

2. Théorie générale

Afin de généraliser les fonctions L de Dirichlet au travers de l'observation de la section précédente, considérons :

— Un groupe compact G avec une représentation $\rho : G \to \mathrm{GL}(V)$ pour V un espace vectoriel complexe de dimension finie, comme traité au chapitre précédent. Soit X l'ensemble des classes de conjugaison de G.

— Un corps de nombres K et $\mathcal{P}$ un ensemble d'idéaux premiers de K ayant densité 1 (la plupart du temps l'ensemble des idéaux premiers de K sauf un nombre fini).

— Une application $\sigma : \mathcal{P} \to X$, pour laquelle nous noterons $\sigma_{\mathfrak{p}}$ à la place de $\sigma(\mathfrak{p})$.

Pour $\mathfrak{p} \in \mathcal{P}$, soit le polynôme $f_{\mathfrak{p}}(X) = \det(\mathrm{id} - \rho(\sigma_{\mathfrak{p}})X, V)$, bien défini puisque $\rho(\sigma_{\mathfrak{p}})$ est défini à conjugaison près.

Définition 3.1. On définit alors la **fonction L_c associée à ρ** par

$$L_c(s, \rho) = \prod_{\mathfrak{p} \in \mathcal{P}} f_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}.$$

Comme une représentation est déterminée à équivalence près par son caractère et que $f_{\mathfrak{p}}$ ne dépend pas de la classe d'équivalence de ρ, on notera aussi $L_c(s, \chi)$ à la place de $L_c(s, \rho)$ si χ est la représentation de G associée à ρ.

Remarque 3.2. Rappelons (voir [Ahl79, Théorème 2.2.6]) qu'un produit infini $\prod_{n=1}^{\infty}(1+a_n)$ avec $(a_n) \in \mathbb{C} - \{-1\}$ converge (resp. converge uniformément) si et seulement s'il en est de même pour la série $\sum_{n\geq 1} a_n$. De plus, la convergence est absolue (i.e. $\prod_{n=1}^{\infty}(1+|a_n|)$ converge) si et seulement si $\sum_{n\geq 1} a_n$ converge absolument, et dans ce cas, le produit ne dépend pas de l'ordre des facteurs. En écrivant un produit infini sur un ensemble dénombrable (sans choix explicite d'ordre), on requerra donc toujours la convergence uniforme.

Remarque 3.3. La notation L_c n'est pas standard. Elle nous permettra simplement d'éviter des conflits de notation entre fonctions L avec des facteurs de ramification/mauvaise réduction (à définir plus tard) et celles sans ceux-ci.

Remarque 3.4. Pour $\mathfrak{p} \in \mathcal{P}$, soient $\varepsilon_1(\mathfrak{p}), \ldots, \varepsilon_n(\mathfrak{p}) \in \mathbb{C}$ les valeurs propres de $\rho(\sigma_{\mathfrak{p}})$ (défini à conjugaison près), avec $n = \dim \rho$. Observons qu'alors

$$L_c(s, \rho) = \prod_{\mathfrak{p} \in \mathcal{P}} \prod_{i=1}^{n} (1 - \varepsilon_i(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}. \tag{3.1}$$

Cette remarque illustre comment ces fonctions généralisent notamment les fonctions L de Dirichlet :

Exemple 3.5. Dans la section précédente, nous avons considéré le cas $K = \mathbb{Q}(\zeta)$ pour ζ une racine primitive $q^{\text{ème}}$ de l'unité, $\mathcal{P}$ les premiers distinct de q, $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ (compact car fini) avec un caractère de Dirichlet χ et σ_p le Frobenius associé à tout premier $p \neq q$. La fonction $L_c(s, \chi)$ est alors la fonction L de Dirichlet associée à χ.

La section suivante sera dédiée à étudier le cas $G = \mathrm{Gal}(L/K)$ pour L/K une extension galoisienne finie de corps de nombres et σ l'application associant premier non-ramifié son Frobenius. Avant cela, nous donnons quelques propriétés générales.

2.1. Quelques propriétés générales

Proposition 3.6. *La fonction $L_c(s, \chi)$ introduite dans la définition 3.1 est holomorphe dans le domaine $E = \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ et ne s'y annule pas.*

Démonstration. Considérons l'écriture (3.1) obtenue dans la remarque 3.4. Par la remarque 3.2, il suffit de montrer que la série

$$f(s) := \sum_{\mathfrak{p} \in \mathcal{P}} \sum_{i=1}^{n} \frac{|\varepsilon_i(\mathfrak{p})|}{|N(\mathfrak{p})^s|} = n \sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{N(\mathfrak{p})^{\mathrm{Re}(s)}}$$

converge absolument uniformément sur tous les compacts de E, où l'égalité ci-dessus découle du fait que $\rho(\sigma_{\mathfrak{p}})$ est unitaire pour tout $\mathfrak{p} \in \mathcal{P}$, d'où $|\varepsilon_i(\mathfrak{p})| = 1$ pour $1 \leq i \leq n$. En utilisant la théorie de la ramification, on se ramène alors au cas de la fonction zêta de Riemann : commençons par décomposer la somme définissant f comme

$$f(s) = n \sum_{p} \sum_{\substack{\mathfrak{p} | (p) \\ \mathfrak{p} \in \mathcal{P}}} \frac{1}{N(\mathfrak{p})^{\mathrm{Re}(s)}}.$$

Pour un premier p, soit $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ la décomposition p en produit d'idéaux premiers dans $\mathcal{O}_K$. Par la proposition 1.4, on a $[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$. Par conséquent, $r \leq [K : \mathbb{Q}]$. De plus, notons que

$$N(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| = |\mathbb{F}_p|^{[\mathcal{O}/\mathfrak{p} : \mathbb{F}_p]} = p^{[\mathcal{O}/\mathfrak{p} : \mathbb{F}_p]} \geq p$$

Ainsi,

$$f(s) \leq n[K : \mathbb{Q}] \sum_{p} \frac{1}{p^{\mathrm{Re}(s)}} \ll \zeta(\mathrm{Re}(s)) < \infty \text{ si } s \in E$$

et les mêmes estimations montrent que la convergence est uniforme dans tout compact de E, en utilisant la propriété analogue de la fonction zêta. Ainsi, $L_c(s, \chi)$ est holomorphe dans E et ne s'y annule pas par définition. □

Proposition 3.7. *Pour* $\mathrm{Re}(s) > 1$, *la dérivée logarithmique* $\mathcal{L}(L(s,\chi))$ *de* $L_c(s,\chi)$ *est donnée par*

$$\frac{L_c'(s,\chi)}{L_c(s,\chi)} = -\sum_{\mathfrak{p},m\geq 1} \frac{\log(N(\mathfrak{p}))\chi(\sigma_{\mathfrak{p}}^m)}{N(\mathfrak{p})^{ms}}.$$

Démonstration. Pour $s > 1$, on trouve en utilisant l'écriture de la remarque 3.4 que

$$\begin{aligned}
\mathcal{L}(L(s,\chi)) &= \mathcal{L}\left(\prod_{\mathfrak{p}\in\mathcal{P}}\prod_{i=1}^{n}\frac{1}{1-\varepsilon_i(\mathfrak{p})N(\mathfrak{p})^{-s}}\right)\\
&= \sum_{\mathfrak{p}\in\mathcal{P}}\sum_{i=1}^{n}\mathcal{L}\left(\frac{1}{1-\varepsilon_i(\mathfrak{p})N(\mathfrak{p})^{-s}}\right)\\
&= -\sum_{\mathfrak{p}\in\mathcal{P}}\sum_{i=1}^{n}\frac{d}{ds}\left(\varepsilon_i(\mathfrak{p})N(\mathfrak{p})^{-s}\right)\frac{1}{1-\varepsilon_i(\mathfrak{p})N(\mathfrak{p})^{-s}}\\
&= -\sum_{\mathfrak{p}\in\mathcal{P}}\sum_{i=1}^{n}\sum_{m\geq 1}\varepsilon_i(\mathfrak{p})\log N(\mathfrak{p})N(\mathfrak{p})^{-ms}.
\end{aligned}$$

Or, $\sum_{i=1}^{n}\varepsilon_i(\mathfrak{p})^m = \chi(\sigma_{\mathfrak{p}}^m)$, donc il vient finalement que

$$\mathcal{L}(L(s,\chi)) = -\sum_{\mathfrak{p}\in\mathcal{P}}\sum_{m\geq 1}\log(N(\mathfrak{p}))\chi(\sigma_{\mathfrak{p}}^m)N(\mathfrak{p})^{-ms}.$$

□

3. Fonctions L d'Artin

Les *fonctions L d'Artin* généralisent les fonctions L de Dirichlet en considérant des *représentations/caractères d'extensions galoisiennes de corps de nombres* et la théorie de la section précédente.

Soit L/K une extension galoisienne finie de corps de nombres et une représentation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$$

pour V un espace vectoriel complexe de dimension finie. Soit $\mathcal{P}$ l'ensemble des idéaux premiers de K ne se ramifiant pas dans L et considérons l'application $\sigma : \mathcal{P} \to \mathrm{Gal}(L/K)$ associant à un idéal $\mathfrak{p} \in \mathcal{P}$ son Frobenius $\sigma_{\mathfrak{p}}$. Alors on a la fonction L associée

$$L_c(s,\rho) = \prod_{\mathfrak{p}\in\mathcal{P}} f_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1} \tag{3.2}$$

convergeant pour $\mathrm{Re}(s) > 1$.

Afin de pouvoir obtenir une équation fonctionnelle, on ajoute également des facteurs aux idéaux premiers de K se ramifiant dans L :

Si $\mathfrak{p}$ est un idéal premier de K qui peut être ramifié, et $\mathfrak{P}$ un idéal au-dessus de $\mathfrak{p}$, il existe $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$ dont l'image par l'isomorphisme $D_{\mathfrak{P}}/I_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ est l'automorphisme de Frobenius du groupe de Galois de l'extension de corps finis $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$. Dans ce cas, $\sigma_{\mathfrak{P}}$ agit sur $V^{I_{\mathfrak{P}}} \subset V$ (en voyant V comme $\mathrm{Gal}(L/K)$-module à travers ρ) et on peut considérer le polynôme minimal

$$\det(\mathrm{id} - X\rho(\sigma_{\mathfrak{P}}), V^{I_{\mathfrak{P}}}),$$

qui ne dépend à nouveau pas de l'idéal $\mathfrak{P}$ choisi au-dessus de $\mathfrak{p}$. Par conséquent, on peut encore noter ce polynôme minimal $f_{\mathfrak{p}}(X)$, qui coïncide avec la définition précédente si $\mathfrak{p}$ ne se ramifie pas (i.e. $I_{\mathfrak{P}} = \{\mathrm{id}\}$).

La **fonction L d'Artin** associée à ρ, notée $L(s, \rho)$, est alors définie comme en (3.2), mais en prenant pour $\mathcal{P}$ tous les idéaux premiers de K. Bien sûr, cela ne va pas changer la convergence puisqu'il n'existe qu'un nombre fini d'idéaux premiers de K se ramifiant dans L.

Exemple 3.8. Si $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$ pour ζ une racine $q^{\text{ème}}$ de l'unité et $\chi : (\mathbb{Z}/q)^\times \to \mathbb{C}^\times$ un caractère de Dirichlet mod q, nous avons vu dans l'exemple 3.5 que la fonction $L_c(s, \chi)$ est égale à la fonction L de Dirichlet associée à χ. La fonction L d'Artin $L(s, \chi)$ associée à χ vu comme caractère de $\mathrm{Gal}(L/K)$ est égale à $L_c(s, \chi)$ à l'exception d'un facteur supplémentaire pour l'unique premier de mauvaise réduction q. En déterminant celui-ci et en utilisant l'exemple 3.5, on voit que

$$L(s, \chi) = \begin{cases} L_q(s, \chi) & \text{si } \chi \neq 1 \\ (1 - q^{-s})L_q(s, \chi) & \text{si } \chi = 1. \end{cases}$$

En effet, rappelons que $\mathcal{O}_L = \mathbb{Z}[\zeta_q]$ et comme dans l'exemple 1.9, on a

$$\mathcal{O}_L/q\mathcal{O}_L \cong \mathbb{F}_q[X]/(\Phi_q(X)),$$

où $\Phi_q(X) = 1 + X + \cdots + X^{q-1}$ est le $q^{\text{ème}}$ polynôme cyclotomique. Notons que dans $\mathbb{F}_q[X]$, on a $X^q - 1 = (X - 1)^q$, donc $\Phi_q(X) = (X - 1)^{q-1} \in \mathbb{F}_q[X]$. Ainsi, $q\mathcal{O}_L = \mathfrak{P}^{q-1}$ pour $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$. Il vient de la proposition 1.16 que $D_{\mathfrak{P}} = I_{\mathfrak{P}} = \mathrm{Gal}(L/K)$. Par conséquent, $\mathbb{C}^{I_{\mathfrak{P}}} = 0$ si $\chi \neq 1$ et $\mathbb{C}^{I_{\mathfrak{P}}} = \mathbb{C}$ sinon. Ainsi, $f_{\mathfrak{P}}(X) = 1$ (respectivement $f_{\mathfrak{P}}(X) = 1 - X$), d'où l'affirmation.

Exemple 3.9. Si $K = \mathbb{Q}$ et χ est le caractère trivial de $\mathrm{Gal}(L/\mathbb{Q})$, on trouve que $L(s, \chi) = \zeta_L(s)$, la **fonction zêta de Dedekind** du corps de nombres L, généralisant la fonction zêta de Riemann. On a en effet

$$L(s, \chi) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}$$

et on montre de la même manière que pour la fonction zêta de Riemann que cette fonction coïncide avec $\zeta_K(s) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$ pour $\mathrm{Re}(s) > 1$. Rappelons

que la fonction zêta de Riemann possède un prolongement analytique à $\mathbb{C}-\{1\}$ avec un pôle simple en $s=1$ et satisfait une équation fonctionnelle. Ce résultat se généralise très bien aux fonctions zêta de Dedekind : la fonction ζ_L admet un prolongement analytique à $\mathbb{C}-\{1\}$ avec un pôle simple en $s=1$ et satisfait une équation fonctionnelle (voir [Neu99, VII.5]).

3.1. Propriétés

La proposition suivante donne des propriétés fondamentale des fonctions L d'Artin, à propos de leur comportement remarquable vis-à-vis des opérations sur les caractères.

Proposition 3.10. *Soit L/K une extension galoisienne finie de corps de nombres et χ, χ' des caractères de* $\mathrm{Gal}(L/K)$*. Alors*

1. $L(s, \chi+\chi') = L(s,\chi)L(s,\chi')$;
2. *(Restriction) Si L'/K est une extension galoisienne finie de corps de nombres telle que $L \subset L'$, notons χ^* le caractère de* $\mathrm{Gal}(L'/K)$ *induit par la restriction* $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$*. Alors*
$$L(s,\chi^*) = L(s,\chi);$$
3. *(Induction) Si M est un corps intermédiaire $K \subset M \subset L$ et ψ un caractère de* $\mathrm{Gal}(L/M)$*, soit ψ_* le caractère induit sur* $\mathrm{Gal}(L/K)$ *à travers l'inclusion* $\mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K)$*. Alors*
$$L(s,\psi) = L(s,\psi_*).$$

Démonstration.

1. Soient (V,ρ) et (V',ρ') les représentations associées à χ, respectivement χ'. Le caractère $\chi+\chi'$ est alors le caractère associé à la représentation $(V\oplus V', \rho\oplus\rho')$. Pour tout idéal premier $\mathfrak{p}$ de K, on a alors $f_{\mathfrak{p}}^{\rho\oplus\rho'}(X) = f_{\mathfrak{p}}^{\rho}(X) f_{\mathfrak{p}}^{\rho'}(X)$, d'où le résultat.
2. Soit (V,ρ) la représentation associée à χ. Il suffit de voir que pour tout idéal premier $\mathfrak{p}$ de K, on a
$$f_{\mathfrak{p}}^{\chi}(X) = f_{\mathfrak{p}}^{\chi^*}(X),$$
où le premier polynôme fait intervenir $\rho(\sigma_{\mathfrak{P}})$ pour un idéal premier $\mathfrak{P}$ de L quelconque au-dessus de $\mathfrak{p}$, tandis que le second fait intervenir $\rho(\sigma_{\mathfrak{P}'})$ pour un idéal premier $\mathfrak{P}'$ de L' quelconque au-dessus de $\mathfrak{p}$. Soit $\mathfrak{P}'$ un idéal premier de L' au-dessus de $\mathfrak{p}$. Alors $\mathfrak{P} := \mathfrak{P}' \cap \mathcal{O}_L$ est un idéal premier de L au-dessus de $\mathfrak{p}$. On a alors le diagramme commutatif exact ci-dessus. Par conséquent, $(V^{I_{\mathfrak{P}'}}, \rho(\sigma_{\mathfrak{P}'})) = (V^{I_{\mathfrak{P}}}, \rho(\sigma_{\mathfrak{P}}))$, d'où $f_{\mathfrak{p}}^{\chi}(X) = f_{\mathfrak{p}}^{\chi^*}(X)$ comme souhaité.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I_{\mathfrak{P}'} & \longrightarrow & D_{\mathfrak{P}'} & \longrightarrow & \mathrm{Gal}((\mathcal{O}_{L'}/\mathfrak{P}')/(\mathcal{O}_K/\mathfrak{p})) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_{\mathfrak{P}} & \longrightarrow & D_{\mathfrak{P}} & \longrightarrow & \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & & 1 & & 1 & & 1 & &
\end{array}$$

3. Cette partie de la proposition est plus technique est assez longue, voir [Neu99, VII.10].

□

Comme conséquence de cette proposition, on obtient la factorisation suivante des fonctions zêta de Dedekind en fonction des fonctions L d'Artin :

Corollaire 3.11. *Soit L/K une extension galoisienne finie de corps de nombres. Alors*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} L(s,\chi)^{\chi(1)},$$

où χ varie parmi les caractères irréductible non-triviaux de $\mathrm{Gal}(L/K)$.

Démonstration. Le caractère 1_* de $G = \mathrm{Gal}(L/K)$ induit à partir de l'unique caractère du sous-groupe trivial est égal à $\sum_{\chi \in \hat{G}} \chi(1)\chi$ puisque pour tout caractère φ de G, on a

$$\langle \varphi^*, 1 \rangle = \varphi(1) = \langle \varphi, \sum_{\chi \in \hat{G}} \chi(1)\chi \rangle.$$

Par la proposition 3.10, on trouve alors directement l'identité voulue. □

Remarque 3.12. Notons qu'avec le prolongement analytique des fonctions zêta de Dedekind, ce résultat implique la non-annulation en $s = 1$ des fonctions L associées à des caractères de Dirichlet mod p non-triviaux. En effet, en considérant $K = \mathbb{Q}$, $L = \mathbb{Q}(e^{2i\pi/p})$ on a $\zeta_K(s) = \prod_{\mathfrak{p}|(q)}(1-N(\mathfrak{p})^{-s})^{-1}\zeta(s)\prod_{\chi\neq 1} L(\chi,s)$. Comme ζ_K et ζ ont toutes deux un pôle simple en $s = 1$ et que le premier produit est holomorphe, il vient que $L(\chi, 1) \neq 0$ pour tout $\chi \neq 1$.

3.2. Prolongement analytique

De la même manière que les fonctions zêta de Dedekind et les fonctions L de Dirichlet (pour des caractères non-triviaux) qu'elles généralisent, les fonctions L d'Artin possèdent un prolongement méromorphe à $\mathbb{C}$:

Théorème 3.13 (Brauer)**.** *Soit L/K une extension galoisienne finie de corps de nombres et χ un caractère de* $\mathrm{Gal}(L/K)$*. Alors $L(s,\chi)$ admet un prolongement méromorphe à $\mathbb{C}$ d'ordre ≤ 1.*

Par la proposition 3.10, il suffit en fait de faire la démonstration dans le cas d'une représentation de dimension 1. En effet, rappelons que par le théorème de Brauer sur les caractères des groupes finis, tout caractère χ de $\mathrm{Gal}(L/K)$ peut s'écrire comme $\chi = \sum_{i=1}^{n} n_i(\chi_i)_i$ pour des entiers $n_i \in \mathbb{Z}$, où les χ_i sont des caractères de dimension 1 de sous-groupes de H. Par la proposition 3.10, on a donc $L(s,\chi) = \prod_{i=1}^{n} L(s,\chi_i)^{n_i}$.

Le théorème suivant résume la situation du cas abélien :

Théorème 3.14 (Hecke)**.** *Si χ est une représentation de dimension* 1 *de* $\mathrm{Gal}(L/K)$*, alors $L(s,\chi)$ admet un prolongement méromorphe sur $\mathbb{C}$ d'ordre au plus* 1*. Plus précisément, ce prolongement est analytique sur $\mathbb{C}$ si $\chi \neq 1$ et a des pôles simple en $s = 1, 0$ si $\chi = 1$.*

Par la discussion ci-dessus, le théorème de Hecke 3.14 entraîne le théorème de Brauer 3.13.

Remarque 3.15. La fameuse *conjecture d'Artin* prétend que si l'on suppose que χ est irréductible et non-trivial dans le théorème 3.13, alors $L(s,\chi)$ est analytique sur tout $\mathbb{C}$. Par le théorème 3.14, la conjecture d'Artin est vraie dans le cas d'extensions abéliennes puisque toute représentation irréductible est de dimension 1.

3.3. Ordre et non-annulation

Étant donnée une extension galoisienne finie L/K de corps de nombres et χ un caractère de $G = \mathrm{Gal}(L/K)$, le théorème de Brauer 3.13 indique que $L(s,\chi)$ est (prolongée en) une fonction méromorphe sur $\mathbb{C}$ d'ordre ≤ 1. On a alors le théorème suivant, généralisant parfaitement le cas des fonctions L de Dirichlet :

Théorème 3.16. *Soit χ un caractère irréductible de G. Alors $L(s,\chi)$ est holomorphe pour* $\mathrm{Re}(s) \geq 1$ *et ne s'annule pas pour* $\mathrm{Re}(s) = 1$*, à l'exception du cas $\chi = 1$ où $L(s,\chi) = \zeta_K(s)$ a un pôle simple en $s = 1$.*

Chapitre 4

Répartition de Frobenius et théorème de densité de Chebotarev

Dans ce chapitre, nous allons voir le lien entre les fonctions L définies dans le chapitre précédent et l'équirépartition de suites dans les classes de conjugaison de groupes compacts. En particulier, nous allons en déduire le théorème des idéaux premiers et le théorème de densité de Chebotarev, en utilisant les résultats de non-annulation des fonctions L d'Artin. La théorie générale présentée dans ce chapitre sera aussi notamment utilisée dans le dernier chapitre pour comprendre la conjecture de Sato-Tate.

1. Sommes d'images de Frobenius et fonctions L

Comme dans le chapitre précédent, considérons

- Un groupe compact G et X l'ensemble de ses classes de conjugaison.
- Un corps de nombres K et $\mathcal{P}$ un ensemble d'idéaux premiers de K ayant densité 1.
- Une application $\sigma : \mathcal{P} \to X$.

Le but de cette section est de démontrer le théorème suivant, reliant une propriété de prolongement/non-annulation de la fonction L_c associée à un caractère de G avec une propriété analytique de sommes d'images de σ par des caractères de G :

Théorème 4.1. *Soit χ un caractère irréductible de G tel que $L_c(s, \chi)$ se prolonge analytiquement sur $\mathrm{Re}(s) \geq 1$ sans s'y annuler, hormis possiblement un ordre $\alpha \in \mathbb{Z}$ en $s = 1$. Alors*

$$\sum_{\mathfrak{p} : N(\mathfrak{p}) \leq x} \chi(\sigma_{\mathfrak{p}}) = \alpha \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Ce résultat sera utilisé pour donner un critère d'équirépartition à la fin de ce chapitre.

1.1. Théorème taubérien de Wiener-Ikehara

La preuve du théorème 4.1 se base sur l'application du (puissant) théorème suivant :

Théorème 4.2. *Soient $f(s), g(s)$ des séries de Dirichlet de termes $a_n \in \mathbb{C}$, respectivement $b_n \in \mathbb{R}$, telles que :*

- *$b_n \geq 0$ et $|a_n| \leq C$ pour tout $n \geq 0$;*
- *$f(s)$ est holomorphe sur $\mathrm{Re}(s) \geq 1$, hormis possiblement un pôle d'ordre 1 et de résidu α en $s = 1$;*
- *$g(s)$ est holomorphe sur $\mathrm{Re}(s) \geq 1$, à l'exception d'un pôle simple en $s = 1$.*

Alors $\sum_{n<x} a_n = \alpha x + o(x)$ quand $x \to +\infty$.

Démonstration. Voir [Lan94, XV.2-3]. □

1.2. Un lemme : asymptotique de séries logarithmiques

Pour démontrer le théorème 4.1, nous allons utiliser l'application suivante du procédé sommatoire d'Abel :

Lemme 4.3. *Soit $(b_n) \subset \mathbb{R}$ une suite telle que $\sum_{n\leq x} b_n = \alpha x + o(x)$ quand $x \to \infty$ pour un certain $\alpha \in \mathbb{R}$. Alors*

$$\sum_{2\leq n\leq x} \frac{b_n}{\log n} = \alpha \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

Démonstration. Pour $x > 1$, notons $B_x = \sum_{n\leq x} b_n$. Par le procédé sommatoire d'Abel, nous trouvons que

$$\begin{aligned}\sum_{2\leq n\leq x} \frac{b_n}{\log n} &= \sum_{2\leq n\leq x} B_n \left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) + (B_x - B_1)\frac{1}{\log x} \\ &= \sum_{2\leq n\leq x} B_n \frac{\log((n+1)/n)}{\log(n+1)\log n} + \alpha\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).\end{aligned}$$

Comme $n\log((n+1)/n) = O(1)$, on trouve que le premier terme de la somme ci-dessus est $o\left(\sum_{2\leq n\leq x} \frac{1}{\log(n)^2}\right) = o\left(\frac{x}{\ln x}\right)$ par comparaison avec l'intégrale $\mathrm{Li}(x) = \int_2^x \frac{1}{\log x} dx = o\left(\frac{x}{\log x}\right)$, d'où le résultat. □

1.3. Preuve du théorème

Nous pouvons maintenant prouver le théorème 4.1.

Preuve du théorème 4.1. Écrivons $L_c(s,\chi) = (s-1)^{-\alpha} f(s)$ avec f holomorphe ne s'annulant pas dans un voisinage de 1. Au voisinage de $s = 1$, considérons

la dérivée logarithmique

$$\begin{aligned} f(s) := -\frac{L_c'(s,\rho)}{L_c(s,\rho)} &= \frac{\alpha}{s-1} - \frac{f'}{f} = \sum_{\mathfrak{p},m\geq 1} \frac{\log(N(\mathfrak{p}))\chi(\sigma_\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} \\ &= \sum_{\mathfrak{p}} \frac{\log(N(\mathfrak{p}))\chi(\sigma_\mathfrak{p})}{N(\mathfrak{p})^{ms}} + \sum_{\mathfrak{p},m\geq 2} \frac{\log(N(\mathfrak{p}))\chi(\sigma_\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}}, \end{aligned}$$

où la troisième égalité provient de la proposition 3.7. Rappelons que si χ est de dimension N, alors $|\chi(\sigma_\mathfrak{p})| \leq N$. Comme dans la preuve de la proposition 3.6, on peut alors borner le dernier terme par

$$\sum_{\mathfrak{p},m\geq 2} \frac{\log N(\mathfrak{p})\chi(\sigma_\mathfrak{p}^m)}{N(\mathfrak{p})^{ms}} \ll \sum_{n\geq 1} \frac{\log n}{n^{2s}} \quad (\mathrm{Re}(s) \geq 1),$$

donc on en déduit que $h(s) = \sum_\mathfrak{p} \frac{\log N(\mathfrak{p})\chi(\sigma_\mathfrak{p})}{N(\mathfrak{p})^s}$ est holomorphe pour $\mathrm{Re}(s) \geq 1$, sauf au plus un pôle simple de résidu α en $s = 1$.

Nous pouvons également appliquer ceci à la fonction zêta de Dedekind de K (voir exemple 3.9) : par le théorème 3.16, $\zeta_K(s)$ est holomorphe sur $\mathrm{Re}(s) \geq 1$ et ne s'annule pas pour $\mathrm{Re}(s) = 1$, à l'exception d'un pôle simple en $s = 1$. Par conséquent, la fonction

$$g(s) := -N\frac{\zeta_K'(s)}{\zeta_K(s)} = \sum_{\mathfrak{p},m} \frac{\log(N(\mathfrak{p}))}{N(\mathfrak{p})^{ms}}$$

est en particulier holomorphe sur $\mathrm{Re}(s) \geq 1$, à l'exception d'un pôle simple en $s = 1$.

Bien sûr, on peut voir h et g comme des séries de Dirichlet en sommant sur la norme des idéaux. Ces fonctions vérifient alors les hypothèse du théorème taubérien 4.2, donc il vient que

$$\sum_{n\leq x} \sum_{\substack{\mathfrak{p} \\ N(\mathfrak{p})=n}} \log n\chi(\sigma_\mathfrak{p}) = \alpha x + o(x).$$

Par le lemme 4.3, ceci implique que $\sum_{\mathfrak{p}:N(\mathfrak{p})\leq x} \chi(\sigma_\mathfrak{p}) = \alpha\frac{x}{\log x} + o(\frac{x}{\log x})$. □

2. Le théorème des idéaux premiers

Nous remarquons en passant que le théorème 4.1 associé aux propriétés de la fonction zêta de Dedekind donne la généralisation suivante du théorème des nombres premiers :

Théorème 4.4 (des idéaux premiers)**.** *Pour tout corps de nombres K, on a*

$$\pi_K(x) \sim \frac{x}{\log x}.$$

Démonstration. Dans les notations du théorème 4.1, on considère $G = \mathrm{Gal}(K/\mathbb{Q})$, $\mathcal{P}$ l'ensemble des idéaux premiers et σ une application quelconque. Pour χ égal au caractère trivial, $L(s,\chi) = \zeta_K(s)$ qui satisfait les hypothèse du théorème 4.1 avec $\alpha = 1$ (voir exemple 3.9). Par conséquent, $\pi_K(x) = \sum_{\mathfrak{p}:N(\mathfrak{p})\leq x} \chi(\sigma_\mathfrak{p}) = \frac{x}{\log x} + o(\frac{x}{\log x})$. □

Ainsi, les fonctions zêta de Dedekind et leur non-annulation sur la droite $\mathrm{Re}(s) = 1$ ont permis de généraliser parfaitement la fonction zêta de Riemann pour généraliser le théorème des nombres premiers ! Nous verrons à la fin de ce chapitre comment le théorème de la progression arithmétique se généralise lui aussi.

3. Relation entre équirépartition et fonctions L

Le théorème principal de ce chapitre est alors le critère d'équirépartition suivant :

Théorème 4.5. *Considérons la situation du théorème 4.1. Supposons que pour tout caractère irréductible $\chi \neq 1$ de G, la fonction $L_c(s,\chi)$ se prolonge analytiquement sans s'annuler sur $\mathrm{Re}(s) \geq 1$, à part possiblement un pôle en $s = 1$. Alors $(\sigma\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ est équirépartie dans X si et seulement si $L(s,\chi)$ est holomorphe et non-nulle en $s = 1$ pour tout caractère irréductible $\chi \neq 1$ de G.*

Preuve du théorème 4.5. Par le critère d'équirépartition de Weyl (proposition 2.16), la suite $(x_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ est équirépartie dans X si et seulement si

$$\sum_{\mathfrak{p}:N(\mathfrak{p})\leq x} \chi(x_\mathfrak{p}) = o(\pi_K(x)),$$

pour tout caractère irréductible χ de G, en utilisant que $\mathcal{P}$ a densité 1 dans l'ensemble des idéaux premiers de K. Par le théorème des idéaux premiers 4.4, ceci est équivalent à

$$\sum_{\mathfrak{p}:N(\mathfrak{p})\leq x} \chi(\sigma_\mathfrak{p}) = o\left(\frac{x}{\log x}\right),$$

pour tout caractère irréductible χ de G. Or, par le théorème 4.1,

$$\sum_{\mathfrak{p}:N(\mathfrak{p})\leq x} \chi(\sigma_\mathfrak{p}) = \alpha(\chi)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right) \tag{4.1}$$

pour tout caractère irréductible χ de G, où $\alpha(\chi) \in \mathbb{Z}$ est l'ordre de $L_c(s,\chi)$ en $s = 1$ si $\chi \neq 1$ et $\alpha(1) = 1$ par définition (le théorème des idéaux premiers donne l'équation (4.1) pour ce cas). En combinant les relations ci-dessus, on obtient alors l'équivalence souhaitée. □

Remarque 4.6. Sous les hypothèses du théorème 4.5, on peut en fait montrer que si $L(s,\chi)$ est holomorphe en $s=1$ pour tout caractère $\chi \neq 1$ de G, alors $L(s,\chi) \neq 0$ pour $\mathrm{Re}(s)=1$ et tout tel caractère χ. Une preuve de ce résultat se trouve dans [Ser02, Chapitre 8]. Elle généralise l'astuce trigonométrique utilisée dans le théorème d'Hadamard-de la Vallée Poussin.

4. Le théorème de densité de Chebotarev

Nous pouvons finalement énoncer et démontrer le théorème de Chebotarev.

Théorème 4.7 (de densité de Chebotarev)**.** *Soit L/K une extension galoisienne finie de corps de nombres avec groupe de Galois $G = \mathrm{Gal}(L/K)$. Soit $\mathcal{P}$ l'ensemble des idéaux premiers de K ne se ramifiant pas dans L. Alors la suite des Frobenius $(\sigma_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ est équirépartie dans les classes de conjugaison du groupe compact G.*

Démonstration. Appliquons le théorème 4.5 avec $G = \mathrm{Gal}(L/K)$, $\mathcal{P}$ l'ensemble des idéaux premiers de K ne se ramifiant pas dans L et $\sigma : \mathcal{P} \to X$ envoyant $\mathfrak{p} \in \mathcal{P}$ sur son Frobenius $\sigma_\mathfrak{p} \in X$. Les fonctions $L(s,\chi)$ associées aux caractères irréductibles non-triviaux χ de G sont des fonctions L d'Artin (à un nombre fini de facteurs de ramification près), qui se prolongent analytiquement sur $\mathrm{Re}(s) \geq 1$ sans s'y annuler, par le théorème 3.16. Par conséquent, le théorème 4.5 implique que le résultat. □

Corollaire 4.8. *Sous les hypothèses du théorème 4.7, soit C une classe de conjugaison de G. Alors l'ensemble d'idéaux premiers $P_C = \{\mathfrak{p} \subset \mathcal{O}_K : \sigma_\mathfrak{p} \in C\}$ a densité naturelle $|C|/|G|$. Plus précisément, quand $x \to +\infty$,*

$$|\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq x, \sigma_\mathfrak{p} \in C\}| = \frac{|C|}{|G|}\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Démonstration. La mesure de Haar normalisée μ sur G est simplement donnée par $\mu(E) = |E|/|G|$ pour tout $E \subset G$. Soit ν l'image de μ sur X. Pour toute classe de conjugaison $C \in X$, on a alors $\nu(\{C\}) = \mu(C) = |C|/|G|$. La proposition 2.14 donne alors les deux affirmations. □

Remarque 4.9. Une autre manière de montrer ceci, sans passer par le critère d'équirépartition, est la suivante : soit $\delta_C : G \to \mathbb{C}$ l'indicatrice de C. Comme il s'agit d'une fonction centrale, il existe des caractères irréductibles distincts $\chi_0, \ldots, \chi_r$ (χ_0 le caractère trivial) et $c_0, \ldots, c_r \in \mathbb{C}$ tels que $\delta_C = \sum_{i=0}^{r} c_i\chi_i$. En utilisant l'équation (4.1), on trouve alors que $|\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq x, \sigma_\mathfrak{p} \in C\}| = c_0\frac{x}{\log x} + \left(\frac{x}{\log x}\right)$. Or, $c_0 = \langle \delta_C, \chi_0\rangle = |C|/|G|$, d'où le résultat.

Remarque 4.10. Il est possible de prouver facilement que P_C a densité *analytique* en supposant uniquement sur $L(s,\chi)$ est holomorphe et non-nulle en $s=1$. On montre alors les approximations

$$\sum_{\mathfrak{p}\subset\mathcal{O}_K}\frac{\chi(\sigma_\mathfrak{p})}{N(\mathfrak{p})^s}=O(1),\ \sum_{\mathfrak{p}\subset\mathcal{O}_K}\frac{1}{N(\mathfrak{p})^s}=\log\frac{1}{s-1}+O(1).$$

quand $s\to 1^+$, pour χ un caractère non-trivial de $\mathrm{Gal}(L/K)$, analogues à celles pour les fonctions L de Dirichlet. Il suffit alors de décomposer l'indicatrice $\delta_C : G\to\mathbb{C}$ de C en combinaison linéaire de caractères irréductibles et d'utiliser ces estimations pour conclure. Montrer la non-annulation et l'holomorphie en $s=1$ est également assez facile en utilisant les propriétés des fonctions L d'Artin par rapport aux opérations sur les caractères (Proposition 3.10). Pour cela, voir [Ser02, Chapitre 6].

Exemple 4.11. Comme application du théorème de Chebotarev, on retrouve comme annoncé le *théorème de la progression arithmétique de Dirichlet*, et on voit que le théorème de Chebotarev généralise très similairement celui-ci (comparer les deux expressions asymptotiques) :

Théorème 4.12 (Dirichlet)**.** *Soit q un nombre premier et a un entier premier à q. Alors il existe une infinité de premiers p tels que $p\equiv a \pmod q$. Plus précisément,*

$$|\{p\leq x \text{ premier } : p\equiv a \pmod q\}|=\frac{1}{\varphi(q)}\frac{x}{\log x}+o\left(\frac{x}{\log x}\right).$$

Démonstration. Soit ζ une racine $q^{\text{ème}}$ de l'unité et $L=\mathbb{Q}(\zeta)$. Comme on l'a rappelé plus tôt, $G=\mathrm{Gal}(L/\mathbb{Q})\cong(\mathbb{Z}/q)^\times$ et le Frobenius associé à un nombre premier $p\neq q$ est associé à la classe de p mod q. Par le théorème de densité de Chebotarev, on a le résultat puisque G est abélien, donc toutes ses classes de conjugaison ont taille 1. □

Exemple 4.13. Dans le deuxième partie de ce travail, nous verrons comment le théorème de Chebotarev peut s'appliquer pour déterminer la densité d'ensembles de premiers vérifiant toute une classes d'hypothèses relatives à des courbes elliptiques.

Deuxième partie

Application aux courbes elliptiques

Chapitre 5

Degré d'isogénies et conséquences

Dans ce chapitre, nous étudions principalement la notion de *degré* d'isogénies de courbes elliptiques, à l'aide de la généralisation aux anneaux de Dedekind de la théorie de la ramification présentée dans la première partie.

Ce concept sera fondamental pour toute la suite, notamment afin d'étudier le nombre de points rationnels des courbes elliptiques sur les corps finis. Parallèlement, on étudie les propriétés du morphisme de Frobenius, qui sera également essentiel pour ceci.

Dans ce chapitre, utilise notamment le degré pour :

— Étudier les noyaux d'isogénies non-constantes, en particulier leur cardinalité.

— Déterminer les groupes de torsion d'une courbe elliptique.

— Définir le module de Tate et les représentations ℓ-adiques.

L'annexe A contient des rappels et des compléments sur les courbes elliptiques pour fixer les notations et servir de référence. Les propriétés (degré, séparabilité) des endomorphismes de multiplication et des Frobenius y sont étudiés.

1. Morphisme de Frobenius

Soit K un corps de caractéristique p. Si q est une puissance de p, on a l'homomorphisme de Frobenius $\varphi_q \in \mathrm{End}(\overline{K})$ défini par $\varphi_q(x) = x^q$, qui induit un morphisme d'anneaux de fonctions $\tilde{\varphi}_q \in \mathrm{End}(\overline{K}[X])$ défini sur K.

Définition 5.1. Si $C \subset \mathbb{P}^n$ est une courbe projective définie sur K associée à l'idéal homogène $I \subset K[X_0, \ldots, X_n]$, on définit la courbe projective $C^{(q)}$ comme la courbe associée à l'idéal homogène engendré par $\tilde{\varphi}_q(f)$, pour tout $f \in I$. On définit alors le morphisme $\hat{\varphi}_q : C \to C^{(q)}$ défini sur K par

$$\hat{\varphi}_q([x_0, \ldots, x_n]) = [\varphi_q(x_0), \ldots, \varphi_q(x_n)],$$

appelé **q-morphisme de Frobenius**.

Notons que cette application est bien définie puisque pour tout $f \in I$, on a $\tilde{\varphi}_q(f)(X_0^q, \ldots, X_n^q) = (f(X_0, \ldots, X_n))^q \in \tilde{\varphi}_q(I(C))$.

Rappelons que si K est fini et $q = |K|$, alors les points fixes de φ_q sont exactement les éléments de K. Par conséquent, dans ce cas :

— Si C est définie sur K, la courbe $C^{(q)}$ est égale à la courbe C.

— Dans ce cas, les points fixes de $\hat{\varphi}_q$ sont exactement les points de $C(K)$.

Exemple 5.2. Soit E une courbe elliptique définie sur un corps K de caractéristique $p > 0$, avec une équation de Weierstrass fixée. Si q est une puissance de p, on peut considérer selon la définition 5.1 le q-endomorphisme de Frobenius

$$\hat{\varphi}_q : E \to E^{(q)}.$$

Comme $\hat{\varphi}_q(\infty) = [0, 1^q, 0] = \infty$, il s'agit d'une isogénie. Remarquons que

— $E^{(q)}$ est aussi une courbe elliptique sous la forme de Weierstrass, dont les coefficients sont les images des coefficients de E par le q-Frobenius $\varphi_q : K \to K$. En particulier,

$$\Delta(E^{(q)}) = \varphi_q(\Delta(E)) = \Delta(E)^q,$$

donc $E^{(q)}$ n'est pas singulière si et seulement si E ne l'est pas.

— Si E est définie sur $\mathbb{F}_q \subset K$, alors $E^{(q)} = E$, donc $\hat{\varphi}_q \in \mathrm{End}(E)$.

Par la discussion du paragraphe précédent, les points fixes de φ sont précisément les points rationnels de E. Grâce à cette propriété, les morphismes de Frobenius seront fondamentaux pour étudier les points rationnels des courbes elliptiques.

2. Degré d'un morphisme de courbes

Intuitivement, un morphisme de courbes projectives planes est de *degré* $n \geq 1$ si la préimage de tout point possède au plus n éléments. On verra par exemple qu'un morphisme de degré 1 est un isomorphisme (l'injectivité étant le principal point, en raison du théorème A.2). La taille exacte des fibres sera mesurée exactement, en général, par le *degré de séparabilité*.

Soient V_1 et V_2 des variétés projectives définies sur K. Un morphisme non-constant $f : V_1 \to V_2$ défini sur K induit un morphisme des corps de fonctions $f^* : K(V_2) \to K(V_1)$ par

$$f^*\phi = \phi \circ f$$

pour tout $\phi \in K(V_2)$ (vu comme une fonction). Notons que ce morphisme est bien défini, car f est non-constante, donc surjective par le théorème A.2 : ainsi, si $(\phi \circ f)\,|_{V_1} = 0$, il vient que que $\phi\,|_{V_2} = 0$.

On obtient alors une extension de corps

$$K(V_1)/f^*(K(V_2)).$$

Dans le cas des courbes projectives, cette extension a la propriété particulière d'être *finie* dès que f n'est pas constante :

Proposition 5.3. *Si $f : C_1 \to C_2$ est une application rationnelle non-constante entre des courbes projectives, alors l'extension $K(C_1)/f^*(K(C_2))$ a degré fini.*

Esquisse de la démonstration. On commence par montrer que si $K/L(x)$, $M/L(y)$ sont deux extensions finies de corps de fonctions avec $K \subset M$, alors M/K est une extension finie (voir [Lor96, VII.4.4] et [Lor96, VII.4.9]). Supposons que $C_1 = V(F)$ avec F irréductible. On note alors que $K(C_1) \cong K(X)[Y]/(F)$, où $F \in K(X)[Y]$ reste irréductible par le lemme de Gauss. Ainsi, $K(C_1)$ et $F^*(K(C_2))$ sont des extensions finies de corps de fonctions, donc on peut conclure par le résultat préliminaire. □

On peut alors faire la définition suivante :

Définition 5.4. Soit $f : C_1 \to C_2$ une application rationnelle de courbes projectives. Le **degré** de f est le degré de l'extension

$$K(C_1)/f^*(K(C_2)),$$

noté $\deg f$. Si f est constante, on pose par convention $\deg f = 0$.

Définition 5.5. Soit $f : C_1 \to C_2$ une application rationnelle de courbes projectives. Le **degré de séparabilité** de f est le degré de séparabilité de l'extension $K(C_1)/f^*(K(C_2))$, noté $\deg_s f$. On dit que f est **séparable** s'il en est de même pour l'extension précédente.

Notons que le degré se comporte de façon multiplicative avec la composition.

Proposition 5.6. *Soient $f : C_1 \to C_2$ et $g : C_2 \to C_3$ des morphismes non-constants. Alors* $\deg(g \circ f) = \deg f \cdot \deg g$ *et* $\deg_s(g \circ f) = \deg_s f \cdot \deg_s g$

Démonstration. Considérons la tour d'extensions de la figure 5.1. Comme f^*

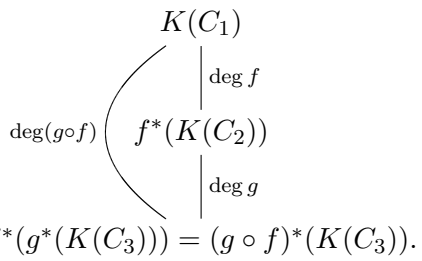


FIGURE 5.1: Degré d'une composition de morphismes.

est un homomorphisme de corps non-nul, c'est une injection. Par conséquent,

$$[f^*(K(C_2)) : f^*(g^*(K(C_3)))] = [K(C_2) : g^*(K(C_3))] = \deg g,$$

de même pour les degrés de séparabilité. □

La proposition suivante donne une première idée du lien du degré d'une application avec la taille de ses fibres.

Proposition 5.7. *Si une application rationnelle $f : C_1 \to C_2$ entre deux courbes projectives lisses a degré* 1*, alors c'est un isomorphisme.*

Démonstration. Par hypothèse, on a $K(C_1) = f^*(K(C_2))$. Comme f^* est injective, il s'agit alors d'un isomorphisme de corps $K(C_2) \xrightarrow{\cong} K(C_1)$. Par conséquent, il existe une application rationnelle $g : C_2 \to C_1$ inverse de f. Puisque C_2 est lisse, g est un morphisme par le théorème A.1, donc f est un isomorphisme. □

Avant de donner des résultats plus précis, on donne plusieurs exemples de calcul du degré de morphismes de courbes.

2.1. Exemples

Exemple 5.8. Pour tout $n \geq 1$, on a une application rationnelle $f : \mathbb{P}^1 \to \mathbb{P}^1$ définie sur K donnée par

$$[x, y] \mapsto [x^n, y^n].$$

Nous avons $K(\mathbb{P}^1) \cong K(\mathbb{A}^1) \cong K(X)$ et ces mêmes isomorphismes induisent des isomorphismes $f^*(K(\mathbb{P}^1)) \cong g^*(K(\mathbb{A}^1)) \cong K(X^n)$ pour $g : \mathbb{A}^1 \to \mathbb{A}^1$ défini par $g(x) = x^n$. Il s'agit donc de considérer l'extension $K(X)/K(X^n)$. Le polynôme

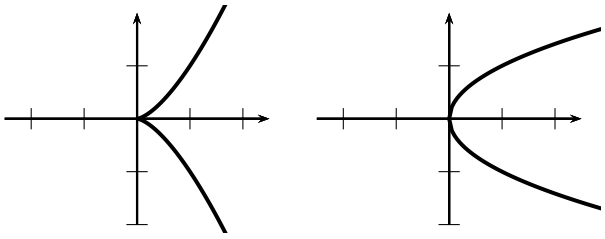
$$T^n - X^n \in K(X^n)[T]$$

annule $X \in K(X) = K(X^n)(X)$ et est irréductible par le critère d'Eisenstein. Par conséquent, $\deg f = [K(X) : K(X^n)] = n$. Clairement, tout $P \in \mathbb{P}^1$ possède au plus n préimages par f.

Exemple 5.9. Soient les courbes $C_1 : y^2 = x^3$ et $C_2 : y^2 = x$ définies sur $\mathbb{R}$ dans $\mathbb{P}^2$. On considère l'application rationnelle $f : C_1 \to C_2$ définie par

$$[x, y, z] \mapsto [x^2, yz, xz].$$

Le morphisme de corps de fonctions correspondant est $f^* : K(C_2) \to K(C_1)$. Notons que $K(C_2) \cong K(Y)$ et $K(C_1)$ est isomorphe au corps de fractions L

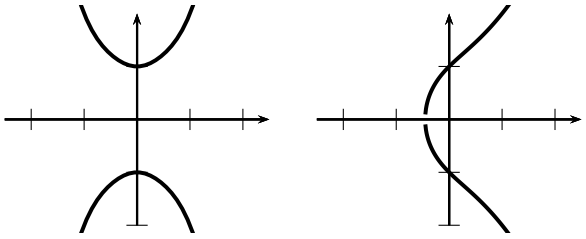


(a) $y^2 = x^3$. (b) $y^2 = x$.

de $K[X,Y]/(Y^2 - X^3)$. A travers ces isomorphismes, f^* correspond à l'application $\hat{f} : K(Y) \to L$ donnée par $Y \mapsto Y/X$. Comme $Y/X \in \hat{f}(K(Y))$, nous avons également $Y^2/X^2 = X^3/X^2 = X \in \hat{f}(K(Y))$, d'où $\hat{f}(K(Y)) = L$. Par conséquent, f a degré 1.

Exemple 5.10. Soient les courbes $C_1 : y^2 = x^6+2x^2+1$ et $C_2 : y^2 = x^3+2x+1$ définies sur $\mathbb{R}$ dans $\mathbb{P}^2$. On considère l'application rationnelle $f : C_1 \to C_2$ définie par

$$[x, y, z] \mapsto [x^2, yz, z^2].$$



(a) $y^2 = x^6 + 2x^2 + 1$. (b) $y^2 = x^3 + 2x + 1$.

Soit $f^* : K(C_2) \to K(C_1)$ le morphisme des corps de fonctions correspondant. Si $(C_1)_*$ et $(C_2)_*$ sont les courbes affines obtenues à partir de C_1 et C_2, nous avons que $K(C_i) \cong K((C_i)_*)$ pour $i = 1, 2$ et f^* correspond à l'application $\hat{f} : K((C_2)_*) \to K((C_1)_*)$ donnée par $X \mapsto X^2$ et $Y \mapsto Y$. Si l'on pose $L = \hat{f}(K(C_2))$, on remarque que $K(C_1) = L(X)$. Or, $X \in K(C_1)$ annule le polynôme $g(T) = T^2 - X^2 \in L[T]$. Clairement, g n'a pas de zéro dans L, donc il est irréductible. Par conséquent, $\deg f = [L(X) : L] = 2$.

Exemple 5.11 (Morphisme de Frobenius et multiplications). On montrera plus tard que le degré d'un q-morphisme de Frobenius est égal à q et que le degré de la multiplication par $n \in \mathbb{Z}$ dans une courbe elliptique est n^2.

2.2. Ramification et propriétés du degré

Nous étudions maintenant les propriétés du degré, notamment sa relation avec les fibres d'un morphisme, à l'aide de la théorie de la ramification développée dans la première partie. La clé est le résultat suivant :

Proposition 5.12. *Soit $f : C_1 \to C_2$ un morphisme non-constant de courbes projectives planes lisses définies sur K, donnant donc lieu à une inclusion de corps de fonctions $f^* : K(C_2) \hookrightarrow K(C_1)$. Pour $Q \in C_2$, soit C_Q la clôture intégrale de $f^*(\mathcal{O}_Q(C_2))$ dans $K(C_1)$. Alors C est un anneau de Dedekind.*

$$\begin{array}{ccc} K(C_1) & & C_Q \\ {\scriptstyle f^*}\big| & & \big|{\scriptstyle f^*} \\ K(C_2) & & \mathcal{O}_Q(C_2) \end{array}$$

Esquisse de la preuve. Il s'agit de montrer que C_Q est noetherien, intégralement clos dans $K(C_1)$ et que tous ses idéaux premiers sont maximaux. Par construction, C_Q est intégralement clos et comme C_Q est la clôture intégrale d'un anneau de Dedekind dans une extension finie, tous ses idéaux premiers sont maximaux. Il suffit donc de montrer que C_Q est noetherien. Pour cela, on montre que C_Q est un $\mathcal{O}_Q(C_2)$-module finiment généré. Il s'agit d'une partie plus technique, qui peut se trouver dans [Lor96, VII.5.5]. □

Dans les notations de la proposition 5.12, considérons maintenant l'idéal maximal (donc premier) $\mathfrak{m}_Q$ de $\mathcal{O}_Q(C_2)$. Dans C_Q, il se décompose comme

$$f^*(\mathfrak{m}_Q)C = \mathfrak{M}_1^{e_1} \dots \mathfrak{M}_n^{e_n}$$

pour des idéaux premiers $\mathfrak{M}_1, \dots, \mathfrak{M}_n$ de C_Q (qui sont aussi maximaux puisque C_Q est un anneau de Dedekind). Par la géométrie algébrique, ces idéaux correspondent à des points $P_1, \dots, P_n$ de C_1. Montrons que $\{P_1, \dots, P_n\} = f^{-1}(Q)$. Par la proposition 1.2 et [Ful89, ex. 2.21], nous avons que, pour $1 \leq i \leq n$,

$$f^*(\mathfrak{m}_{f(P_i)}) \subset \mathfrak{M}_i \cap f^*(\mathcal{O}_Q(C_2)) = f^*(\mathfrak{m}_Q).$$

Puisque f^* est une injection, on en déduit que $\mathfrak{m}_{f(P_i)} \subset \mathfrak{m}_Q$, donc $f(P_i) = Q$ par maximalité.

En appliquant la théorie de la ramification du premier chapitre, on obtient alors l'information suivantes sur les fibres de f, en posant $e_{P_i} := e_i$:

Théorème 5.13. *Pour tout $Q \in C_2$, on a l'équation*

$$\sum_{P \in f^{-1}(Q)} e_P = \deg f,$$

De plus, pour tous les $Q \in C_2$ sauf au plus un nombre fini, on a $|f^{-1}(Q)| = \deg_s(f)$.

Démonstration. Comme $C/\mathfrak{M}_i$ et $\mathcal{O}_Q(C_2)/\mathfrak{m}_Q$ sont isomorphes à K, tous les degrés résiduels sont égaux à 1, donc la première partie de l'assertion découle immédiatement de la proposition 1.24. Pour la seconde assertion, il s'agit d'étudier quels points de C_2 sont tels que $\mathfrak{m}_Q(C_2) \subset \mathcal{O}_Q(C_2)$ se ramifient dans C_Q. Par la proposition 1.25, il faut pour cela étudier le discriminant $\Delta_{C/\mathcal{O}_Q(C_2)}$. Pour cette partie que nous n'aurions pas la place de faire en détails ici, nous renvoyons à [Lor96, Chapitre VII]. □

Corollaire 5.14. *Soit $f : C_1 \to C_2$ un morphisme non-constante entre des courbes lisses et $Q \in C_2$. Alors $f^{-1}(Q)$ a au plus* $\deg f$ *éléments.*

Démonstration. Par le théorème 5.13, on a que

$$\deg f = \sum_{P \in f^{-1}(Q)} e_P \geq \sum_{P \in f^{-1}(Q)} 1 = |f^{-1}(Q)|.$$

□

3. Degré et isogénies

Dans le reste de ce chapitre, nous étudions et utilisons les propriétés du degré d'isogénies entre des courbes elliptiques, afin d'obtenir un grand nombre de résultats fondamentaux pour la suite.

Des rappels sur les isogénies sont présents dans l'annexe A. Pour cette section, soient (E, O) et (E', O') deux courbes elliptiques

3.1. Noyau d'isogénies

En premier lieu, il est possible de donner une version plus forte de la proposition 5.13 pour la taille des fibres d'une isogénie.

Proposition 5.15. *Si $f : E \to E'$ est une isogénie non-constante, alors* $\ker f$ *est un groupe fini d'ordre* $\deg_s \phi$.

Démonstration. Par le théorème 5.13, on sait que pour tout $Q \in E'$ sauf au plus un nombre fini, on a $|f^{-1}(Q)| = \deg_s(f)$. L'idée est d'utiliser le fait que l'on travaille avec des groupes et un homomorphisme pour se ramener si besoin par translation à l'un des points où cette relation est vérifiée. Comme E' est infini, choisissons en effet $Q \in E'$ tel que $|f^{-1}(Q)| = \deg_s(f)$. Comme f est

surjective, il existe $R \in E$ tel que $f(R) = Q$. Considérons $g \in \mathrm{Aut}(E)$ défini par $g(P) = P + R$. On a alors

$$|\ker f| = |(f \circ g)^{-1}(Q)| = |g^{-1}(f^{-1}(Q))| = |f^{-1}(Q)| = n.$$

□

Isogénies duales, degré et séparabilité de la multiplication et des morphismes de Frobenius Dans l'annexe A, on détermine le degré des multiplications et des morphismes de Frobenius, ainsi que des résultats sur leur séparabilité. Pour cela, on utilise en particulier la relation entre degré et *isogénie duale*.

3.2. L'application degré

Nous remarquons maintenant que l'application degré sur le groupe des isogénies entre deux courbes elliptiques a la propriété très particulière d'être une forme quadratique.

Proposition 5.16. *L'application*

$$\deg : (\mathrm{Hom}(E, E'), +) \to \mathbb{Z}$$

est une forme quadratique définie-positive, c'est-à-dire que

1. $\deg f = \deg(-f)$ *pour tout* $f \in \mathrm{Hom}(E, E')$.
2. *L'application* $b : \mathrm{Hom}(E, E') \times \mathrm{Hom}(E, E') \to \mathbb{Z}$ *définie par*

$$b(f, g) = \deg(f + g) - \deg f - \deg g$$

   est bilinéaire.
3. $\deg f \geq 0$ *pour tout* $f \in \mathrm{Hom}(E, E')$ *avec égalité si et seulement si* $f \equiv O'$.

Démonstration. Soient $f, g \in \mathrm{Hom}(E, E')$. Par les propositions 5.6 et A.18,

$$\deg(-f) = \deg([-1] \circ f) = \deg[-1] \deg f = \deg f.$$

Par définition, $\deg f \geq 0$ avec égalité si et seulement si $f = \infty$. Pour montrer la bilinéarité de b, on utilise les isogénies duales et l'injectivité de l'homomorphisme $\mathbb{Z} \to \mathrm{Hom}(E, E)$, $m \mapsto [m]$ (corollaire A.17). Par le théorème A.12 et la proposition A.13,

$$\begin{aligned} [b(f, g)] &= \widehat{f + g} \circ (f + g) - \widehat{f} \circ f - \widehat{g} \circ g \\ &= \hat{f} \circ g + \hat{g} \circ f. \end{aligned}$$

Comme $\widehat{\cdot}$ est linéaire, on obtient que pour tous $f_1, f_2 \in \mathrm{Hom}(E, E)$,

$$[b(f_1 + f_2, g)] = [b(f_1, g) + b(f_2, g)],$$

d'où $b(f_1 + f_2, g) = b(f_1, g) + b(f_2, g)$ par injectivité. □

Remarque 5.17. Notons que la définition d'une forme quadratique définie positive $d : (A, +) \to \mathbb{Z}$ sur un groupe abélien $(A, +)$ implique que $d(nx) = n^2 d(x)$ pour tous $x \in A, n \in \mathbb{Z}$. Par le premier point de la définition, il suffit de montrer le résultat pour $n \geq 0$. Ce dernier est clair pour $n = 0, 1$ par le troisième point de la définition. En utilisant que

$$b(nx, -x) = d((n-1)x) - d(nx) - d(x)$$

par définition et

$$b(nx, -x) = -n(d(2x) - d(x) - d(x)) = 2nd(x) - nd(2x)$$

par bilinéarité, on obtient que

$$d(nx) = d((n-1)x) - d(x) + nd(2x) - 2nd(x),$$

ce qui implique le résultat pour $n = 2$ puis pour $n > 2$ par récurrence.

4. Points d'ordre fini

Comme premier exemple de l'utilisation du degré d'un morphisme, nous déterminons les groupes de torsion d'une courbe elliptique, information qui sera très utile pour la suite.

Définition 5.18. Soit (E, O) une courbe elliptique et $m \geq 1$ un entier. Le m**-sous-groupe de torsion** de E est

$$E[m] = \{P \in E : [m]P = O\}.$$

Théorème 5.19. *Soit E une courbe elliptique définie sur K et $m \geq 1$ un entier. Alors $|E[m]| \leq m^2$ et si $\mathrm{car}\, K = 0$ ou si $\mathrm{car}\, K > 0$ ne divise pas m, alors*

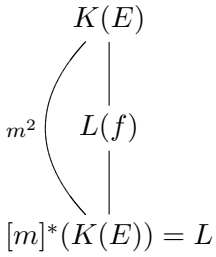
$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

Démonstration. Remarquons que $E[m] = \ker[m]$. Par le théorème 5.15 sur les tailles de noyaux d'isogénies,

$$|E[m]| = \deg_s[m] \mid \deg[m] = m^2,$$

d'où la première partie du théorème. Posons $L = [m]^*(K(E))$ et distinguons deux cas :

— Si $\operatorname{car} K = 0$, alors l'extension $K(E)/L$ est séparable, donc $\deg_s[m] = \deg[m]$.
— Si que $\operatorname{car} K = p > 0$ ne divisant pas m, soit $f \in K(E)$ quelconque. Comme $[L(f) : L] \mid [K(E) : L] = m^2$, il vient que $p \nmid [L(f) : L]$. Par conséquent, $\min_L(f)$ est un polynôme séparable, donc $L(f)/L$ est



séparable. Ainsi, il en est de même pour $K(E)/L$ et $\deg_s[m] = \deg[m]$.

Dans ces deux cas, on trouve que

$$|E[m]| = \deg[m] = m^2. \tag{5.1}$$

Par le théorème de structure des groupes abéliens finis,

$$E[m] \cong \mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_r \tag{5.2}$$

avec $a_1 \mid \cdots \mid a_r$ des entiers tels que $a_1 \dots a_r = m^2$. Notons que comme $mE[m] = O$, il vient que $a_i \mid m$ pour tout i. Le nombre d'éléments de $E[a_1] \subset E[m]$ est égal à a_1^2 par (5.1). D'autre part, il est égal à a_1^r par (5.2). Par conséquent, $r = 2$. Comme $a_1 a_2 = m^2$, on doit avoir $a_1 \geq m$ ou $a_2 \geq m$. Comme $a_1, a_2 \mid m$, on a $a_1, a_2 \leq m$, donc tous les cas on obtient $a_1 = a_2 = m$ et $E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$. □

Remarque 5.20. Plus généralement, on peut aussi montrer que si $\operatorname{car} K = p > 0$ et $m = p^r m'$ avec $(m, m') = 1$, alors $E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m'$ ou $E[m] \cong \mathbb{Z}/m' \times \mathbb{Z}/m'$. Pour cela, voir par exemple [Sil86, III.6.4].

La définition suivante sera utile dans la suite, où l'on en verra une reformulation plus explicite et des exemples.

Définition 5.21. Une courbe elliptique E définie sur un corps K de caractéristique p est dite **supersingulière** si $E[p] = \{O\}$.

5. Le module de Tate et représentations ℓ-adiques

Dans cette section, on définit le module de Tate et les représentations ℓ-adiques associées à une courbe elliptique, qui seront utilisés dans le dernier chapitre pour relier les deux parties du travail.

Dans la section précédente, nous avons vu que si (E, O) est une courbe elliptique sur un corps de caractéristique 0 ou si $\operatorname{car} K > 0$ ne divise pas m, alors

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

Ainsi, en fixant une base, on a un isomorphisme d'anneaux $\operatorname{End}(E[m]) \cong \operatorname{Mat}_2(\mathbb{Z}/m)$.

Notons que puisque la multiplication par m est une isogénie, nous avons une action de $\operatorname{Gal}(\overline{K}/K)$ sur $E[m] = \ker[m]$. Par conséquent, ceci induit une représentation

$$\operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}_2(\mathbb{Z}/m).$$

Il est possible de "combiner" toutes ces représentations par le biais d'une construction similaire aux entiers p-adiques, ce que nous allons voir dans le paragraphe suivant.

5.1. Le module de Tate

Pour ℓ un premier, rappelons que l'on définit les entiers ℓ-adiques par la limite inverse $\mathbb{Z}_\ell = \varprojlim_{n\geq 1} \mathbb{Z}/\ell^n$ par rapport aux homomorphismes naturels $f_n : \mathbb{Z}/\ell^{n+1} \to \mathbb{Z}/\ell^n$. Dans le cas des groupes de torsion d'une courbe elliptique, on fait la définition similaire suivante :

Définition 5.22. Soit E une courbe elliptique sur un corps K de caractéristique $p \geq 0$ et ℓ un premier distinct de p. Le **module de Tate ℓ-adique associé à** E est la limite inverse

$$T_\ell(E) = \varprojlim_{n\geq 1} E[\ell^n]$$

par rapport aux homomorphismes $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$.

Notons que $T_\ell(E)$ est bien un $\mathbb{Z}_\ell$-module, dont l'action (bien-définie) de $\mathbb{Z}_\ell$ est donnée par

$$(\overline{x_n})_{n\in\mathbb{N}}(P_n)_{n\in\mathbb{N}} = (x_n P_n)_{n\in\mathbb{N}}$$

pour $(\overline{x_n})_{n\in\mathbb{N}} \in \mathbb{Z}_\ell$ et $(P_n)_{n\in\mathbb{N}} \in T_\ell(E)$.

A partir de la structure de chacun des $E[\ell^n]$, on obtient le résultat suivant sur la structure du module de Tate :

Proposition 5.23. *Soit E une courbe elliptique définie sur un corps de caractéristique $p \geq 0$ et $\ell \neq p$ un nombre premier. Alors*

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

en tant que $\mathbb{Z}_\ell$-modules.

Démonstration. Par le théorème 5.19, $T_\ell(E) = \varprojlim_{n\geq 1} E[\ell^n] \cong \varprojlim_{n\geq 1}(\mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n) \cong \left(\varprojlim_{n\geq 1} \mathbb{Z}/\ell^n\right) \times \left(\varprojlim_{n\geq 1} \mathbb{Z}/\ell^n\right) = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. □

5.2. Représentations ℓ-adiques

Sous les mêmes notations que dans le paragraphe précédent, notons que $G = \mathrm{Gal}(\overline{K}/K)$ agit sur $T_\ell(E)$, de la manière suivante :

$$\sigma((P_n)_{n\in\mathbb{N}}) = (\sigma(P_n))_{n\in\mathbb{N}}$$

pour tout $\sigma \in G$ et $(P_n)_{n\in\mathbb{N}} \in T_\ell(E)$. Cette action est bien définie par la remarque A.7, la multiplication par $[\ell]$ étant définie sur K.

On obtient par conséquent une représentation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell),$$

appelée **représentation ℓ-adique** de $\mathrm{Gal}(\overline{K}/K)$ associée à E.

5.3. Isogénies et module de Tate

Soient E_1, E_2 des courbes elliptiques définies sur un corps K de caractéristique $p \geq 0$ et $f : E_1 \to E_2$ une isogénie. Pour un premier ℓ différent de p et $n \geq 1$, on peut considérer l'application induite

$$\hat{f} : E_1[\ell^n] \to E_2[\ell^n].$$

Cette application induit à son tour un morphisme de $\mathbb{Z}_\ell$-modules

$$f_\ell : T_\ell(E_1) \to T_\ell(E_2)$$

de la façon suivante : si $(P_n)_{n\in\mathbb{N}} \in T_\ell(E_1)$, alors $f_\ell((P_n)_{n\in\mathbb{N}}) = (\hat{f}(P_n))_{n\in\mathbb{N}} \in T_\ell(E_2)$. Par conséquent, on a une application

$$\cdot_\ell : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2)).$$

En fait, il s'agit d'une injection :

Proposition 5.24 ([Sil86, exercice 3.14])**.** *L'application $\cdot_\ell$ est injective.*

Démonstration. Soit $f \in \mathrm{Hom}(E_1, E_2)$ une isogénie telle que $f_\ell = 0$. Il vient alors que $E[\ell^m] \subset \ker f$ pour tout $m \geq 1$. En effet, soit $m \geq 1$ et $P \in E[\ell^m]$. Comme l'isogénie $[\ell]$ est non-constante (proposition A.16), elle est surjective. Il existe donc $(P_n)_{n\in\mathbb{N}} \in T_\ell(E_1)$ avec $P_m = P$, obtenu en posant $P_i = [\ell^{m-i}](P)$ pour $1 \leq i \leq m$ et en définissant $P_{m+1}, \ldots$ récursivement à l'aide de la

surjectivité de $[\ell]$. Par hypothèse, $0 = f_\ell((P_n)_{n\in\mathbb{N}}) = (f(P_n))_{n\in\mathbb{N}}$, donc $f(P) = 0$. Ainsi, on a

$$\bigcup_{n\geq 1} E[\ell^n] \subset \ker f.$$

Par la proposition 5.1, $|E[\ell^n]| = \ell^{2n}$, donc l'ensemble de droite est infini. Ceci force f à être constante (donc $f = 0$), puisque dans le cas contraire $\ker f$ serait un groupe fini (proposition 5.15). □

Si E est une courbe elliptique définie sur un corps de caractéristique $p \geq 0$ avec $\ell \neq p$, la proposition 5.23 montre que le module de Tate $T_\ell(E)$ associé est un $\mathbb{Z}_\ell$-module libre de rang 2. Par conséquent, $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \mathrm{Mat}_2(\mathbb{Z}_\ell)$ et on a des applications

$$\begin{aligned} \det : \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) &\to \mathbb{Z}_\ell \\ \mathrm{tr} : \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) &\to \mathbb{Z}_\ell \end{aligned}$$

qui induisent à travers $\cdot_\ell$ des applications

$$\begin{aligned} \det : \mathrm{End}(E) &\to \mathbb{Z}_\ell \\ \mathrm{tr} : \mathrm{End}(E) &\to \mathbb{Z}_\ell. \end{aligned}$$

En utilisant le *couplage de Weil* (voir [Sil86, III.8]), on montre la relation suivante entre degré d'une isogénie et son déterminant ainsi que sa trace. En particulier, on remarque qu'il n'y a en fait pas de dépendance par rapport à ℓ et que $\det, \mathrm{tr}$ ont image dans $\mathbb{Z} \subset \mathbb{Z}_\ell$!

Proposition 5.25. *Soit $f \in \mathrm{End}(E)$ une isogénie. Alors*

$$\det f = \deg f \ \textit{et}\ \mathrm{tr}\, f = 1 + \deg f - \deg(\mathrm{id} - f),$$

sous l'inclusion usuelle $\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell$.

Démonstration. Voir [Sil86, III.8.6]. □

Exemple 5.26. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ et $\varphi \in \mathrm{End}(E)$ le Frobenius. Par les propositions 5.25 et A.21, on trouve que

$$\det \varphi = \deg \varphi_\ell = q.$$

La trace de φ_ℓ sera calculée explicitement dans le chapitre suivant, où nous verrons son lien le nombre de points rationnels de E.

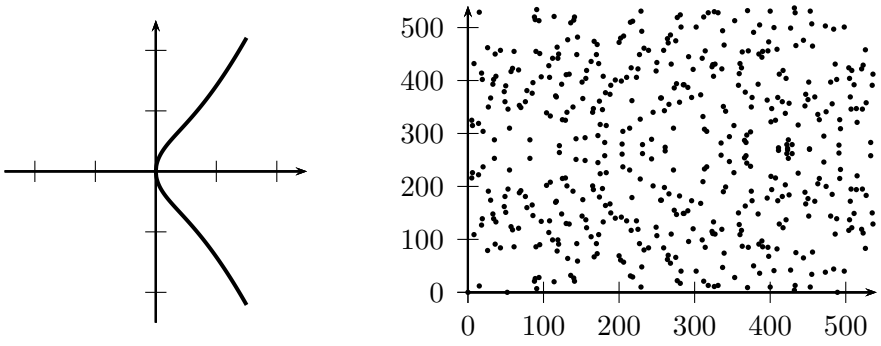
Chapitre 6

Courbes elliptiques sur les corps finis

Dans ce chapitre, nous nous intéressons aux courbes elliptiques définies sur un corps fini. Dans tout ce qui suit, on considérera un corps fini $\mathbb{F}_q$, pour q une puissance d'un premier.

Les questions les plus naturelles sont celles concernant la *structure* et la *cardinalité* du groupe des points rationnels, qui est dans ce cas un groupe abélien fini.

Exemple 6.1. Par exemple, on peut considérer la courbe elliptique $E : y^2 = x^3 + x$ sur $\mathbb{F}_{541}$. Elle possède 500 points rationnels. Dans la figure 6.1, on représente $E(\mathbb{F}_{541})$ par la bijection $\mathbb{F}_{541} \cong \{0, \ldots, 540\}$.



(a) sur $\mathbb{R}$. (b) sur F_{541}.

Figure 6.1: La courbe $y^2 = x^3 + x$ dans $\mathbb{R}$ et $\mathbb{F}_{541}$.

1. Nombre de points rationnels

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Avant de s'intéresser à la structure de $E(\mathbb{F}_q)$, nous étudions sa cardinalité.

1.1. Formule explicite

Premièrement, notons qu'il est facile de donner une formule explicite pour $|E(\mathbb{F}_q)|$ en fonction du symbole de Legendre, en caractéristique impaire [1].

En effet, supposons alors E soit sous la forme de Weierstrass $y^2 = x^3 + ax^2 + bx + c$. Pour tout $x \in \mathbb{F}_q$:

- Soit $x^3 + ax^2 + bx + c$ est un carré non-nul dans $\mathbb{F}_q$ et on a alors deux points rationnels de première coordonnée x ;
- Soit $x^3 + ax^2 + bx + c = 0$ dans $\mathbb{F}_q$ et on a alors un point rationnel de première coordonnée x ;
- Soit $x^3 + ax^2 + bx + c$ n'est pas un carré dans $\mathbb{F}_q$ et aucun point rationnel n'a x comme première coordonnée.

Supposons que $q = p^r$. Pour $n \geq 1$, définissions la généralisation suivante du symbole de Legendre :

$$\left(\frac{n}{\mathbb{F}_q}\right) = \begin{cases} 1 & \text{si } n \in \mathbb{F}_q^{\times 2} \\ 0 & \text{si } q \mid n \\ -1 & \text{sinon.} \end{cases}$$

Par conséquent, pour tout $x \in \mathbb{F}_q$, on a dans tous les cas $1 + \left(\frac{x^3+ax^2+bx+c}{\mathbb{F}_q}\right)$ points rationnels avec x comme première coordonnée. En comptant l'unique point à l'infini, on obtient :

Proposition 6.2. $|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax^2 + bx + c}{\mathbb{F}_q}\right)$.

Rappelons que si $p > 2$, alors $\left(\frac{n}{p^e}\right) = \left(\frac{n}{p}\right)$. En stockant une liste des résidus quadratiques du corps, on obtient donc un calcul en $O(q)$, contrairement à un calcul en $O(q^2)$ par force brute.

Exemple 6.3. Pour la courbe elliptique $y^2 = x^3 + x$ sur $\mathbb{F}_5$, on a

$$|E(\mathbb{F}_5)| = 6 + \left(\frac{0}{5}\right) + \left(\frac{2}{5}\right) + \left(\frac{0}{5}\right) + \left(\frac{0}{5}\right) + \left(\frac{3}{5}\right) = 4.$$

Par contre, il est difficile de travailler au niveau théorique directement sur cette expression pour estimer $|E(\mathbb{F}_q)|$. Néanmoins, on peut l'utiliser pour avoir une idée heuristique sur l'ordre de grandeur de $|E(\mathbb{F}_q)|$:

1. En caractéristique 2, on ne peut pas supposer que E aie une équation de la forme $y^2 = f(x)$.

En effet, $\mathbb{F}_q^\times$ est composé précisément à moitié de carrés. Par conséquent, si les valeurs $x^3 + ax^2 + bx + c$ sont réparties "uniformément" dans $\mathbb{F}_q$, on peut s'attendre à ce que la somme soit proche de 0 et donc que $|E(\mathbb{F}_q)|$ soit proche de $q+1$. Nous allons voir dans la section suivante que cette approximation est effectivement assez bonne, comme le suggère la table 6.1.

q	$\lvert E_1(\mathbb{F}_q)\rvert$	$\frac{\lvert\lvert E_1(\mathbb{F}_q)\rvert-(q+1)\rvert}{\lvert E_1(\mathbb{F}_q)\rvert}$	q	$\lvert E_2(\mathbb{F}_q)\rvert$	$\frac{\lvert\lvert E_2(\mathbb{F}_q)\rvert-(q+1)\rvert}{\lvert E_2(\mathbb{F}_q)\rvert}$
31	32	0.0 %	31	-	-
37	36	6.0 %	37	48	21.0 %
41	32	31.0 %	41	35	20.0 %
43	44	0.0 %	43	34	29.0 %
47	48	0.0 %	47	60	20.0 %
53	68	21.0 %	53	58	7.0 %
59	60	0.0 %	59	63	5.0 %
61	52	19.0 %	61	50	24.0 %
67	68	0.0 %	67	56	21.0 %
71	72	0.0 %	71	59	22.0 %
73	80	8.0 %	73	72	3.0 %
79	80	0.0 %	79	86	7.0 %
83	84	0.0 %	83	90	7.0 %
89	80	13.0 %	89	100	10.0 %
97	80	23.0 %	97	97	1.0 %

TABLE 6.1: Ordre de $E(\mathbb{F}_q)$ pour $31 \leq q \leq 100$ et les courbes $E_1 : y^2 = x^3 + x$, $E_2 : y^2 = x^3 + x + 1$, quand celles-ci peuvent être vues comme des courbes elliptiques sur $\mathbb{F}_q$.

1.2. Endomorphisme de Frobenius et borne de Hasse

Rappelons qu'étant donnée une courbe elliptique E sur un corps fini $\mathbb{F}_q$, on peut considérer le q-endomorphisme de Frobenius

$$\begin{array}{rcl} \varphi_q : E & \to & E \\ [x, y, z] & \mapsto & [x^q, y^q, z^q]. \end{array}$$

Cet endomorphisme a la propriété suivante particulièrement intéressante pour l'étude des points rationnels : ses points fixes sont exactement les éléments de $E(\mathbb{F}_q)$ (voir exemple 5.2). Ainsi, $P \in E(\mathbb{F}_q)$ si et seulement si $\varphi_q(P) = P$, c'est-à-dire $P \in \ker \psi$ où $\psi = \mathrm{id} - \varphi_q \in \mathrm{End}(E)$. Par conséquent,

$$E(\mathbb{F}_q) = \ker \psi.$$

Or, le degré séparable d'un morphisme permet justement de calculer la cardinalité de ses fibres. Puisque ψ est séparable (proposition A.23), on a

$$|E(\mathbb{F}_q)| = |\ker \psi| = \deg \psi.$$

Rappelons que par la proposition 5.16 l'application $\deg : \mathrm{End}(E) \to \mathbb{Z}$ est une forme quadratique définie-positive sur le groupe abélien $(\mathrm{End}(E), +)$. Pour de telles applications, on a la généralisation suivante de l'inégalité de Cauchy-Schwartz :

Lemme 6.4. *Soit $(A, +)$ un groupe abélien et $f : (A, +) \to \mathbb{Z}$ une forme quadratique définie positive sur A. Alors pour tous $x, y \in A$, on a*

$$|b(x, y)| \leq 2\sqrt{f(x)f(y)},$$

où $b : A \times A \to \mathbb{Z}$ est l'application bilinéaire associée à f.

Démonstration. Soient $x, y \in A$. Pour $m, n \in \mathbb{Z}$, on a par positivité $f(mx - ny) \geq 0$. Or,

$$f(mx-ny) = f(mx)+f(-ny)+b(mx,-ny) = m^2 f(x)+n^2 f(y)-mnb(x,y).$$

En posant $m = b(x, y)$ et $n = 2f(x)$, on obtient que $f(x)(4f(x)f(y) - b(x, y)^2) \geq 0$, ce qui donne le résultat étant donné que $f(x) \geq 0$. □

En appliquant ce lemme à l'endomorphisme de Frobenius, on obtient la *borne de Hasse*[2], qui montre que l'approximation esquissée dans la section précédente est en général assez bonne.

Proposition 6.5 (Borne de Hasse)**.** *Si E est une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, alors $|E(\mathbb{F}_q)| = q + 1 + O(\sqrt{q})$.*

Démonstration. Soit b l'application bilinéaire associée à la forme quadratique $\deg : \mathrm{End}(E) \to \mathbb{Z}$. En appliquant le lemme 6.4 à $b(\mathrm{id}, -\psi)$, on obtient que

$$|\deg \psi - \deg \mathrm{id} - \deg \varphi_q| \leq 2\sqrt{\deg \mathrm{id} \deg \varphi_q}.$$

Or, par la proposition A.21, $\deg(\varphi_q) = q$. Puisque $\deg \psi = |E(\mathbb{F}_q)|$ et $\deg(\mathrm{id}) = 1$, on obtient la borne $||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$. □

En d'autres termes, si l'on s'intéresse à la différence

$$a_q := q + 1 - |E(\mathbb{F}_q)|,$$

la borne de Hasse indique que $|a_q| \leq 2\sqrt{q}$.

Remarque 6.6. Il existe une généralisation de ce résultat à des courbes de genre supérieur à 1 (Théorème de Hasse-Weil). Des cas particuliers de la borne de Hasse avaient été obtenus par Gauss (voir [ST10, pp. 110-111]).

2. Conjecturée par Artin dans sa thèse en 1924 et démontrée par Hasse en 1933.

1.3. Le morphisme de Frobenius dans le module de Tate

Rappelons que grâce au module de Tate, nous avons défini des applications $\det, \mathrm{tr} : \mathrm{End}(E) \to \mathbb{Z}$ reliées au degré. On remarque que dans la démonstration de la borne de Hasse, nous avons en fait déterminé le déterminant et la trace du morphisme de Frobenius φ_q :

Proposition 6.7. *Pour une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$, on a*

$$\det \varphi_q = q, \ \mathrm{tr}\, \varphi_q = a_q.$$

De plus, pour tout premier ℓ distinct de p, le polynôme caractéristique de φ_q vue dans $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \mathrm{Mat}_2(\mathbb{Z}_\ell)$ est est $X^2 - a_q X + q$.

Démonstration. Par la proposition 5.25,

$$\begin{aligned} \mathrm{tr}\, \varphi &= 1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi) = 1 + q - |E(\mathbb{F}_q)| = a_q, \\ \det \varphi &= \deg \varphi = q, \end{aligned}$$

d'où l'assertion sur le polynôme minimal. □

Cette interprétation sera utilisées dans le dernier chapitre pour relier les deux parties du travail, mais aussi dans la section suivante.

1.4. Nombre de points dans une extension

Supposons que l'on aie déterminé le nombre de points rationnels d'une courbe elliptique E définie sur $\mathbb{F}_q$ (q une puissance d'un premier p). Le résultat suivant permet en particulier de calculer algébriquement le nombre de points rationnels dans toute extension finie de $\mathbb{F}_q$. En particulier, si la courbe est définie sur $\mathbb{F}_p$, on peut déterminer son nombre de points rationnels sur tout corps de caractéristique p à partir de $|E(\mathbb{F}_p)|$.

Proposition 6.8. *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Pour tout $n \geq 1$, on a*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - x_1^n - x_2^n,$$

où $x_1, x_2 \in \mathbb{C}$ sont les racines du polynôme $X^2 - a_q X + q \in \mathbb{Z}[X]$.

Démonstration. Soit $n \geq 1$ un entier. Si φ_q est le q-endomorphisme de Frobenius, alors le q^n-endomorphisme de Frobenius est φ_q^n. Par la section précédente,

$$|E(\mathbb{F}_{q^n})| = \deg(\mathrm{id} - \varphi_q^n).$$

Le degré de l'isogénie $\mathrm{id} - \varphi_q^n$ peut se calculer en passant dans le module de Tate, à l'aide de la proposition 5.25. En effet, on a

$$\deg(\mathrm{id} - \varphi_q^n) = \deg(\varphi_q^n) + 1 - \mathrm{tr}((\varphi_q^n)_\ell) = q^n + 1 - \mathrm{tr}((\varphi_q)_\ell^n).$$

Pour calculer la trace de φ_ℓ^n, remarquons que comme $X^2 - a_q X + q$ est le polynôme caractéristique de φ_ℓ (proposition 6.7), il existe une base dans laquelle la matrice de φ_ℓ est

$$\begin{pmatrix} x_1 & * \\ 0 & x_2 \end{pmatrix}.$$

Par conséquent, $\mathrm{tr}(\varphi_\ell^n) = x_1^n + x_2^n$, d'où le résultat. □

Exemple 6.9. Dans l'exemple 6.3, on a trouvé que le nombre de points rationnels de $E : y^2 = x^3 + x$ sur $\mathbb{F}_5$ est 4. Utilisons la proposition 6.8 pour déterminer $|E(\mathbb{F}_{25})|$. Par définition, $a_5 = 6 - 4 = 2$. Les racines du polynôme $x^2 - 2x + 5$ sont $1 \pm 2i$. Comme $(1 + 2i)^2 + (1 - 2i)^2 = -6$, il vient que $|E(\mathbb{F}_{25})| = 25 + 1 + 6 = 32$.

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. On peut s'intéresser à la façon dont évolue l'estimation de $|E(\mathbb{F}_{q^n})|$ par $q^n + 1$ (borne de Hasse) quand $n \geq 1$ croît. En d'autres termes, on s'intéresse à la valeur de $b_n := q^n + 1 - |E(\mathbb{F}_{q^n})|$ pour $n \geq 1$ (noter que $b_1 = a_q$). Le résultat précédent donne une relation de récurrence pour ces valeurs, qui simplifie aussi les calculs comme ceux de l'exemple 6.9.

Proposition 6.10 ([Sil86, ex. 5.13])**.** *Sous les notations précédentes, on a* $b_{n+2} = b_1 b_{n+1} - q b_n$ *pour* $n \geq 0$*, en posant* $b_0 = 2$.

Démonstration. Soient $x_1, x_2 \in \mathbb{C}$ les racines du polynôme $X^2 - a_q X + q$. Par la proposition 6.8, nous avons que $b_n = x_1^n + x_2^n$ pour $n \geq 0$. Par conséquent,

$$\begin{aligned} b_{n+2} = x_1^2 x_1^n + x_2^2 x_2^n &= (a_q x_1 - q) x_1^n + (a_q x_1 - q) x_2^n \\ &= a_q (x_1^{n+1} + x_2^{n+1}) - q(x_1^n + x_2^n) = a_1 b_{n+1} - q b_n. \end{aligned}$$

□

Exemple 6.11. Dans le cas de l'exemple 6.9, on trouve que $b_2 = b_1^2 - 5 \cdot 2 = (6 - 4)^2 - 10 = -6$, donc on retrouve que $|E(\mathbb{F}_{25})| = 32$, sans faire de calculs dans $\mathbb{C}$.

2. Structure du groupe des points rationnels

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Le groupe $E(\mathbb{F}_q)$ est alors un groupe abélien fini. A l'aide du théorème de structure des groupes abéliens finis et des informations que nous avons sur les groupes de torsion, on peut donner une forme plus précise pour $E(\mathbb{F}_q)$.

Proposition 6.12. *Le groupe* $E(\mathbb{F}_q)$ *est isomorphe à* $\mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ *pour* $n_1, n_2 \geq 1$ *des entiers tels que* $n_1 \mid n_2$.

Démonstration. Par le théorème de structure des groupes abéliens finis,

$$E(\mathbb{F}_q) \cong \mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_r$$

avec $a_i \geq 1$ des entiers tels que $a_i \mid a_{i+1}$. Par le théorème 5.19, $|E[a_1]| \leq a_1^2$. Or, selon l'isomorphisme ci-dessus, $|E[a_1]| = a_1^r$. Par conséquent, $r \leq 2$ et le résultat suit. □

Exemple 6.13. Dans l'exemple 6.3, on a montré que le nombre de points rationnels de $E : y^2 = x^3 + x$ sur $\mathbb{F}_5$ est 4. Par conséquent, $E(\mathbb{F}_4) \cong \mathbb{Z}/4$ ou $\mathbb{Z}/2 \times \mathbb{Z}/2$. Comme

$$(0,0), (2,0) \in E(\mathbb{F}_5)$$

sont deux points d'ordre 2, il vient que $E(\mathbb{F}_5) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Exemple 6.14. En utilisant une des méthodes du paragraphe précédent, on trouve que le nombre de points rationnels de la courbe elliptique $E : y^2 = x^3 + 3x + 2$ sur $\mathbb{F}_7$ est égal à 9. Par conséquent, $E(\mathbb{F}_7) \cong \mathbb{Z}/9$ ou $\mathbb{Z}/3 \times \mathbb{Z}/3$. Comme le point $(0,3) \in E(\mathbb{F}_7)$ a ordre 9, on obtient que $E(\mathbb{F}_7) \cong \mathbb{Z}/9$.

3. Courbes supersingulières

Rappelons qu'une courbe elliptique E définie sur un corps fini de caractéristique p est supersingulière si $E[p] = O$ (voir la définition 5.21), où $E[p]$ représente les points d'ordre p dans $E(\overline{\mathbb{F}}_q)$ (et pas seulement dans $E(\mathbb{F}_q)$).

En utilisant les résultats développés dans ce chapitre, on peut donner de nouvelles caractérisations de la supersingularité. En particulier, on voit que pour $p \geq 5$, les courbes supersingulières sont précisément celles pour lesquelles l'estimation $E(\mathbb{F}_q) \approx q + 1$, validée par la borne de Hasse, est atteinte.

Proposition 6.15 ([Sil86, exercice 5.10])**.** *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. Alors les assertions suivantes sont équivalentes :*

1. *E est supersingulière ;*
2. *$a_q \equiv 0 \pmod{p}$;*
3. *$E(\mathbb{F}_q) \equiv 1 \pmod{p}$.*

Démonstration. Par définition, $a_q = q + 1 - |E(\mathbb{F}_q)|$, donc il est clair que les deux derniers énoncés sont équivalents. Pour les autres, nous allons utiliser les trois faits suivants :

1. $\overline{\mathbb{F}}_q = \cup_{n \geq 1} \mathbb{F}_{p^n}$;
2. Si un premier p divise l'ordre d'un groupe fini G, alors G a un élément d'ordre p (découle des théorèmes de Sylow ou du théorème de structure si G est abélien) ;

3. Par la proposition 6.10, $b_n = q^n + 1 - |E(\mathbb{F}_{q^n})|$ satisfait la relation de récurrence $b_{n+2} = b_1 b_{n+1} - q b_n$ $(n \geq 0)$.

La courbe E est supersingulière si et seulement si $E(\overline{\mathbb{F}}_q)$ n'a aucun point d'ordre p. Par le premier point, c'est le cas si et seulement si $E(\mathbb{F}_{p^n})$ n'a aucun point d'ordre p pour tout $n \geq 1$.

Supposons que $a_q \not\equiv 0 \pmod{p}$, ce qui implique que $a_q^{p-1} \equiv 1 \pmod{p}$. Par le troisième point, on a alors

$$\begin{aligned} b_1 &= a_q \\ b_2 &\equiv b_1^2 \pmod{p} \\ b_n &\equiv b_1 b_{n-1} \pmod{p} \ (n > 2), \end{aligned}$$

d'où $b_n \equiv a_q^n \pmod{p}$ pour tout $n \geq 1$. En particulier, $|E(\mathbb{F}_{p^{p-1}})| = p^{p-1} + 1 - b_{p-1} \equiv 0 \pmod{p}$. Par le point 2, $E(\mathbb{F}_{p^{p-1}})$ possède un élément d'ordre p. Ainsi, E n'est pas supersingulière.

Réciproquement, supposons que $a_p \equiv 0 \pmod{p}$. Par le point 3, on trouve que $b_n \equiv 0 \pmod{p}$ pour tout $n > 1$, i.e. $|E(\mathbb{F}_{p^n})| \equiv 1 \pmod{p}$ pour tout $n > 1$. Par conséquent, $E(\mathbb{F}_{p^n})$ n'a pas d'élément d'ordre p pour tout $n > 1$, c'est-à-dire que E est supersingulière. □

Exemple 6.16. La courbe elliptique $E : y^2 = x^3 + x^2 + 2x$ sur $\mathbb{F}_5$ est supersingulière. En effet, $|E(\mathbb{F}_5)| = 6 \equiv 1 \pmod{5}$.

Corollaire 6.17. *Soit E une courbe elliptique définie sur $\mathbb{F}_p$ avec $p \geq 5$ un premier. Alors les assertions suivantes sont équivalentes :*

1. *E est supersingulière.*
2. *$a_p = 0$.*
3. *$E(\mathbb{F}_p) = p + 1$.*

Démonstration. Par la proposition, il suffit de montrer que $a_p \equiv 0 \pmod{p}$ si et seulement si $a_p = 0$. Si $a_p \equiv 0 \pmod{p}$, soit $k \in \mathbb{Z}$ tel que $a_q = kp$. Par la borne de Hasse, $|a_p| \leq 2\sqrt{p}$. Or $2\sqrt{p} < p$ $(p \geq 5)$, donc $k = 0$ et $a_q = 0$, ce qui termine la démonstration. □

Remarque 6.18. Le corollaire 6.17 n'est pas valable si $p < 5$ puisque la courbe elliptique $E : y^2 = x^3 + 2x + 2$ sur $\mathbb{F}_3$ est supersingulière, bien que l'on ait $a_p = 3 \neq 0$.

A partir de ces résultats, on termine par donner une forme plus précise pour la structure du groupe des points rationnels d'une courbe supersingulière.

Proposition 6.19 ([Sil86, exercice 5.6])**.** *Soit E une courbe elliptique supersingulière définie sur le corps fini $\mathbb{F}_p$ avec $p \geq 5$ un premier. Alors*

$$E(\mathbb{F}_p) \equiv \begin{cases} \mathbb{Z}/2 \times \mathbb{Z}/2n & ou \\ \mathbb{Z}/n \end{cases}$$

pour un certain $n \geq 1$. Si $p \equiv 1 \pmod 4$, c'est le deuxième cas qui est vérifié.

Démonstration. Par la proposition 5.19, il existe $m, n \geq 1$ tels que

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m \times \mathbb{Z}/mn. \tag{6.1}$$

On commence par montrer que l'on peut supposer $p \nmid m$. En effet, si $p|m$, alors $p^2 \mid |E(\mathbb{F}_p)|$, d'où $|E(\mathbb{F}_p)| = p^2$ puisque $E(\mathbb{F}_p) \subset \mathbb{A}^2(\mathbb{F}_p) \cup \{\infty\}$, qui a cardinalité $p^2 + 1$. Par la borne de Hasse,

$$2\sqrt{p} \geq |a_p| = |p^2 - p - 1| = p^2 - p - 1 \geq 2p \text{ si } p > 3,$$

ce qui est impossible si $p \geq 5$. Par conséquent, on peut supposer que $p \nmid m$.

Selon l'équation 6.1, $E(\mathbb{F}_p)$ contient m^2 points d'ordre divisant m. Or $|E[m]| \leq m^2$ (théorème 5.19), donc $E[m] \subset E(\mathbb{F}_p)$. Par le corollaire 8.1.1 de [Sil86] (résultant des propriétés du *couplage de Weil*), ceci implique que $\mu_m \subset \mathbb{F}_p$, pour μ_m le groupe des racines $m^{\text{èmes}}$ de l'unité dans $\mathbb{C}$. Par le théorème de Lagrange, $m|p-1$, donc $p \equiv 1 \pmod m$.

Si E est supersingulière, le corollaire 6.17 implique que $mn^2 = |E(\mathbb{F}_p)| = p+1$. Par conséquent, $2 \equiv p + 1 \equiv 0 \pmod m$ si $m > 1$. Ainsi, $m = 1$ ou $m = 2$. Si $m = 2$, alors $E(\mathbb{F}_p) = 4n = p + 1$, donc $p \equiv 3 \pmod 4$. □

Exemple 6.20. La courbe $E : y^2 = x^3+x^2+10x+11$ sur $\mathbb{F}_{17}$ est supersingulière puisque $|E(\mathbb{F}_{17})| = 18 = 17+1$. Par la proposition 6.19, on trouve directement que $E(\mathbb{F}_{17}) \cong \mathbb{Z}/18$.

Exemple 6.21. La courbe $E : y^2 = x^3 + 2x^2 + 4x$ sur $\mathbb{F}_7$ est supersingulière puisque $|E(\mathbb{F}_7)| = 8 = 7 + 1$. Par la proposition 6.19, on a donc $E(\mathbb{F}_7) \cong \mathbb{Z}/8$ ou $\mathbb{Z}/2 \times \mathbb{Z}/4$. Notons que les deux points $(0, 0), (4, 0) \in E(\mathbb{F}_7)$ ont ordre 2, donc $E(\mathbb{F}_7) \cong \mathbb{Z}/2 \times \mathbb{Z}/4$ puisque $\mathbb{Z}/8$ n'a qu'un élément d'ordre 2.

Chapitre 7

Réduction modulo un premier

Dans ce chapitre, nous formalisons l'idée esquissée dans l'introduction d'étude "locale" d'une courbe elliptique définie sur un corps de nombres, et en étudions quelques propriétés.

1. Réduction modulo $\mathfrak{p}$

Soit K un corps de nombres et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Si $R = (\mathcal{O}_K)_\mathfrak{p}$ est la localisation de $\mathcal{O}_K$ en $\mathfrak{p}$, alors on a l'homomorphisme de réduction modulo $\mathfrak{p}$: $\pi_\mathfrak{p} : R \to \mathcal{O}_K/\mathfrak{p}$. Comme $\mathfrak{p}$ est aussi maximal, $k = \mathcal{O}_K/\mathfrak{p}$ est un corps et on peut définir une application

$$\pi_\mathfrak{p} : \mathbb{P}^n(K) \to \mathbb{P}^n(k)$$

de la manière suivante : rappelons que toute localisation à un idéal premier d'un anneau de Dedekind est un anneau de valuation discrète, donc principal et factoriel. Si $P \in \mathbb{P}^n(K)$, alors il existe par conséquent $x_0, \dots, x_n \in R$ premiers entre eux tels que $P = [x_0, \dots, x_n]$ par l'inclusion $R \subset K$. On pose alors $\pi_\mathfrak{p}(P) = [\pi_\mathfrak{p}(x_0), \dots, \pi_\mathfrak{p}(x_n)] \in \mathbb{P}^n(k)$. Ceci est bien défini puisque :

- Si $(\pi_\mathfrak{p}(x_0), \dots, \pi_\mathfrak{p}(x_n)) = 0 \in \mathbb{A}^{n+1}(k)$, alors $x_1, \dots, x_n \in \mathfrak{p}R$, l'idéal maximal de R. Puisque celui-ci est principal, cela implique que $x_1, \dots, x_n$ ne sont pas premiers entre eux.
- Par définition de $\mathbb{P}^n(K)$, l'élément $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}(R)$ est unique à multiplication par une unité de R près.

Exemple 7.1. Pour p un premier, l'application $\pi_p : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Z}/p)$ est simplement donnée par $P \mapsto [\overline{x}, \overline{y}, \overline{z}]$, où $(x, y, z) \in \mathbb{Z}^3$ est un choix de coordonnées pour P tel que x, y, z soient premiers entre eux. La définition générale est plus compliquée du fait que $\mathcal{O}_K$ n'est en général par lui-même factoriel.

Soit E une courbe elliptique définie sur un corps de nombres K, sous une forme de Weierstrass fixée

$$E : y^2 = x^3 + ax + b.$$

En appliquant au besoin un changement de variable du type $y = y/c^3$, $x = x/c^2$ pour un $c \in \mathcal{O}_K$, on peut supposer sans perte de généralité que $a, b \in \mathcal{O}_K$.

Pour tout idéal premier $\mathfrak{p}$ de K, on peut alors considérer la courbe $E_\mathfrak{p}$ définie sur le corps fini $k = \mathcal{O}_K/\mathfrak{p}$, obtenue en réduisant les coefficients de E mod $\mathfrak{p}$:

$$E_\mathfrak{p} : y^2 = x^3 + \pi_\mathfrak{p}(a)x + \pi_\mathfrak{p}(b),$$

On appelle $E_\mathfrak{p}$ la **réduction de** E **modulo** $\mathfrak{p}$. En d'autres termes, $E = \pi_\mathfrak{p}(E_\mathfrak{p})$

Exemple 7.2. Au début du chapitre 6, nous avons illustré la réduction modulo 541 de la courbe $y^2 = x^3 + x$ définie sur $\mathbb{Q}$. Plus généralement, il est clair que toute courbe elliptique sur un corps fini $\mathbb{F}_p$ est la réduction modulo un premier d'une courbe définie sur $\mathbb{Q}$.

Proposition 7.3. *La projection $\pi_\mathfrak{p}$ se (co)restreint en un homomorphisme de groupes abéliens $\pi_\mathfrak{p} : E(K) \to E_\mathfrak{p}(k)$.*

Démonstration. Clair en considérant les formules explicites. Une preuve "géométrique" peut également être trouvée dans [Hus04, p. 109]. □

2. Bonnes et mauvaises réductions

Notons que la réduction modulo un premier d'une courbe elliptique définie sur un corps de nombres n'est *pas forcément une courbe elliptique*, comme le montre l'exemple suivant :

Exemple 7.4. La réduction de la courbe elliptique $E : y^2 = x^3 + x + 2$ modulo 2 est la courbe $E_2 : y^2 = x^3 + x$, définie sur $\mathbb{F}_2$. Son discriminant est $-4 \equiv 0 \pmod 2$, donc il ne s'agit pas d'une courbe elliptique. Similairement, E_7 a discriminant $-112 \equiv 0 \pmod 7$, donc n'est également pas une courbe elliptique.

Définition 7.5. Soit E une courbe elliptique définie sur un corps de nombres K et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On dit que E a **bonne réduction** mod $\mathfrak{p}$ si $E_\mathfrak{p}$ est une courbe elliptique. Dans le cas contraire, on dit que E a **mauvaise réduction** mod $\mathfrak{p}$.

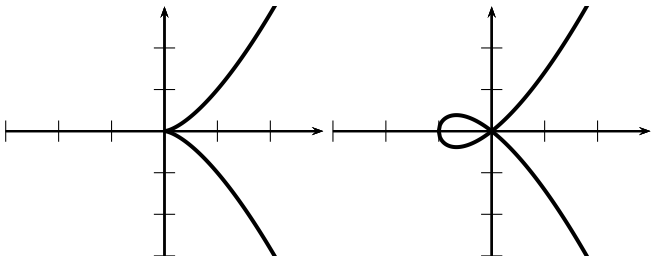
Proposition 7.6. *Soit E une courbe elliptique définie sur un corps de nombres K. Il n'existe qu'un nombre fini de premiers $\mathfrak{p}$ tels que E a mauvaise réduction mod $\mathfrak{p}$.*

Démonstration. La courbe elliptique E a mauvaise réduction mod $\mathfrak{p}$ si et seulement si

$$0 = \Delta(E_\mathfrak{p}) = \pi_\mathfrak{p}(\Delta(E)) \in \mathcal{O}_K/\mathfrak{p},$$

où $\pi_p : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ est la projection. Par conséquent, la courbe E a mauvaise réduction précisément aux idéaux premiers divisant $\Delta(E)\mathcal{O}_K$, qui sont en nombre fini. □

Exemple 7.7. La courbe $E : y^2 = x^3 + x + 2$ définit une courbe elliptique sur $\mathbb{Q}$ de discriminant $\Delta(E) = -112 = -2^4 \cdot 7$. Par conséquent, E a mauvaise réduction mod 2 et mod 7. En effet, les courbes $E_2 : y^2 = x^3 + x$ et $E_7 : y^2 = x^3 + x + 2$ sur $\mathbb{F}_2$, respectivement $\mathbb{F}_7$, sont singulières puisqu'elles ont discriminant nul.



(a) $y^2 = x^3$. (b) $y^2 = x^3 + x^2$.

FIGURE 7.1: Deux cubiques singulières dans le plan affine, l'origine étant un point de rebroussement, respectivement un noeud.

Remarque 7.8. Parmi les mauvaises réduction, on distingue encore entre l'existence d'un noeud ou d'un point de rebroussement (rappelons qu'une courbe cubique singulière a au plus un point singulier, [Sil86, III.1.4]). Dans le premier cas, on parle de **réduction multiplicative**, dans le second de **réduction additive**. Nous n'utiliserons néanmoins pas cette distinction dans la suite.

Remarque 7.9 (Equation minimale). Pour une courbe elliptique E définie sur un corps de nombres K, il existe une infinité d'équations pour E (i.e. de polynômes générant la même courbe). Or, le choix d'une équation influe le nombre de bonnes et de mauvaises réductions. Par exemple, la courbe elliptique $E : y^2 = x^3 + 64$ a discriminant $\Delta(E) = -110592 = -2^{12}3^3$, donc elle a mauvaise réduction mod 2 et 3. Néanmoins, le changement de variable $x' = 4x$ et $y' = 8y$ donne l'équation

$$E : y^2 = x^3 + 1$$

et le discriminant de E sous cette forme est $-27 = -3^3$ dont E n'a plus que mauvaise réduction mod 3. Par conséquent, on souhaiterait travailler une équation sous la forme de Weierstrass avec coefficients entiers pour E minimisant le nombre de premiers où E a mauvaise réduction, c'est-à-dire qui minimise

$$|\{\mathfrak{p} : \Delta(E) \equiv 0 \pmod{\mathfrak{p}}\}|.$$

En d'autres termes, on souhaite minimiser le nombre d'idéaux premiers de K divisant $\Delta(E)$ sous la condition que les coefficients de l'équation soient entiers. Comme ce discriminant est alors entier, une telle équation minimisante existe. Pour le cas rationnel, il est facile de déterminer une telle équation explicitement, en utilisant la détermination des changements de variable d'une courbe elliptique donnée par [Sil86, III.3.1b]. Quand l'anneau des entiers n'est pas factoriel, la situation est un peu plus compliquée (voir [Hus04, Ch. 15] ou [Sil86, VIII.8])

3. Réduction des endomorphismes

Soit E une courbe elliptique définit sur un corps de nombres et $f \in \mathrm{End}(E)$. Pour tout idéal premier $\mathfrak{p}$ de bonne réduction, on obtient une isogénie $f_\mathfrak{p} \in \mathrm{End}(E_\mathfrak{p})$ en réduisant modulo $\mathfrak{p}$ les polynômes définissant f.

Proposition 7.10. *L'application $\pi_\mathfrak{p} : \mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p})$ donnée par $f \mapsto f_\mathfrak{p}$ est un homomorphisme d'anneaux.*

Démonstration. Clair, en considérant les formules explicites. □

Proposition 7.11. *L'homomorphisme $\pi_\mathfrak{p} : \mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p})$ préserve les isogénies duales, i.e. $\widehat{(f_p)} = (\hat{f})_p$ pour tout $f \in \mathrm{End}(E)$.*

Démonstration. Soit $f \in \mathrm{End}(E)$. Par définition de la réduction modulo $\mathfrak{p}$, on a $\pi_\mathfrak{p} \circ \hat{f} = (\hat{f})_p \circ \pi_\mathfrak{p}$. On remarque alors que le diagramme de la figure 7.2 commute, i.e. $\pi_\mathfrak{p} \circ \hat{f} = \widehat{(f_p)} \circ \pi_\mathfrak{p}$. Par conséquent, $\widehat{(f_p)} \circ \pi_\mathfrak{p} = (\hat{f})_p \circ \pi_\mathfrak{p}$. Comme $\pi_\mathfrak{p}$ est surjective, on obtient la conclusion. □

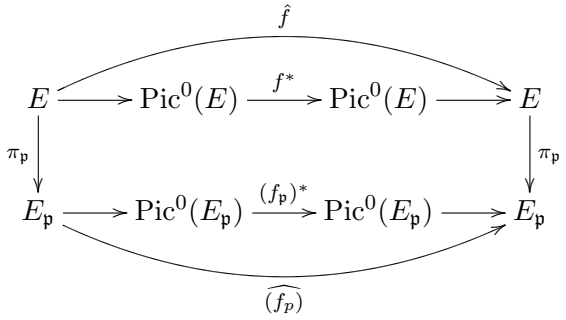


FIGURE 7.2: Réduction des isogénies duales.

Corollaire 7.12. *L'homomorphisme $\pi_\mathfrak{p} : \mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p})$ préserve les degrés, i.e. $\deg f = \deg f_\mathfrak{p}$ pour tout $f \in \mathrm{End}(E)$.*

Démonstration. Soit $f \in \mathrm{End}(E)$. Par les propositions 7.11 et 7.10, ainsi que les propriétés des isogénies duales (proposition A.13), on a

$$[\deg f_\mathfrak{p}] = f_\mathfrak{p} \circ \widehat{(f_\mathfrak{p})} = f_\mathfrak{p} \circ (\hat{f})_\mathfrak{p} = (f \circ \hat{f})_\mathfrak{p} = [\deg f]_\mathfrak{p} = [\deg f].$$

Par les propriétés de la multiplication (voir proposition A.17), on obtient alors que $\deg f_\mathfrak{p} = \deg f$. □

4. Noyau de la réduction mod $\mathfrak{p}$

Soit E une courbe elliptique sur un corps de nombres K, $\mathfrak{p}$ un idéal premier de K tel que E aie bonne réduction mod $\mathfrak{p}$ et $k = \mathcal{O}_K/\mathfrak{p}$. Dans cette section, nous nous intéressons au noyau de la réduction mod $\mathfrak{p}$

$$\pi_\mathfrak{p} : E(K) \to E_\mathfrak{p}(k),$$

ce qui sera utile dans le chapitre suivant.

Proposition 7.13. *Le sous-groupe* $\ker \pi_\mathfrak{p}$ *n'a pas de point d'ordre fini* m *pour tout entier* m *ne divisant pas* $\mathrm{car}(k)$.

Dans [Sil86], ce résultat est démontré en montrant que ce noyau est isomorphe au *groupe formel* associé à la courbe et en démontrant l'affirmation pour celui-ci. Une démonstration plus directe est donnée dans [Hus04, Ch. 5.5], mais dans les deux cas il serait trop long d'en rendre compte ici.

Corollaire 7.14. *Pour tout* $m \geq 1$ *ne divisant pas* $\mathrm{car}(k)$*, la projection*

$$E(K)[m] \to E_\mathfrak{p}(k)$$

est injective.

Démonstration. Pour tout $m \geq 1$, la projection $\pi_\mathfrak{p}$ se restreint à $(\pi_\mathfrak{p})_m : E(K)[m] \to E_\mathfrak{p}(k)$. Comme $\ker \pi_\mathfrak{p}$ ne possède pas de points d'ordre fini, il suit que $(\pi_\mathfrak{p})_m$ est injective. □

Exemple 7.15. Ces résultats peuvent être utiles pour obtenir des informations à propos du groupe de torsion (voire le groupe des points rationnels) d'une courbe elliptique, en la réduisant modulo plusieurs idéaux premiers. Par exemple, considérons la courbe $E : y^2 = x^3 + 3$, de discriminant $-243 = -3^5$. En utilisant une des méthodes données dans le chapitre précédent, on trouve que

$$|E_5(\mathbb{F}_5)| = 6,\ |E_{13}(\mathbb{F}_{13})| = 13.$$

Par la proposition 7.14, pour tout m ne divisant ni 5 ni 13, le groupe de m-torsion $E(\mathbb{Q})[m]$ est trivial. En effet, il est alors isomorphe à un sous-groupe de $E_5(\mathbb{F}_5)$ (resp. de $E_{13}(\mathbb{F}_{13})$) et $(6, 13) = 1$. De plus, $E(\mathbb{Q})[13]$ (dont tous les éléments ont ordre 1 ou 13) est isomorphe à un sous-groupe de $E_5(\mathbb{F}_5)$ (dont tous les éléments ont ordre divisant 6), d'où $E(\mathbb{Q})[13]$ est trivial. On montre de même que $E(\mathbb{Q})[5]$ est trivial. Ainsi, E n'a pas de point d'ordre fini !

Chapitre 8

Répartition des a_p et la conjecture de Sato-Tate

Dans ce chapitre, nous relions les deux parties du travail, en étudiant les questions de répartition à propos de courbes elliptiques esquissées dans l'introduction, en exploitant les notions développées dans la première partie.

Soit E une courbe elliptique définie sur $\mathbb{Q}$, avec une équation minimale $f \in \mathbb{Z}[X, Y]$. Pour tout premier p de bonne réduction (c'est-à-dire tout premier sauf un nombre fini), on peut s'intéresser à la courbe elliptique E_p sur $\mathbb{F}_p$, obtenue par réduction de E mod p (voir le chapitre précédent). Rappelons la question générale soulevée dans l'introduction :

Question 8.1. *Comment est-ce que les propriétés des courbes E_p varient quand p varie parmi les premiers de bonne réduction ? Par exemple, comment est-ce que le nombre de points rationnels de E_p varie avec p ou quelle est la répartition/densité des premiers p tels que E_p soit supersingulière ?*

Dans ce chapitre, nous allons nous intéresser plus particulièrement à la seconde partie de cette question. De manière équivalente, il s'agit d'étudier les valeurs a_p, représentant la différence entre $|E(\mathbb{F}_p)|$ et la valeur "moyenne" $p + 1$.

La borne de Hasse indiquant que $|a_p| \leq 2\sqrt{p}$ pour tout p de bonne réduction, on peut aussi normaliser de la manière suivante : pour tout p de bonne réduction, il existe $0 \leq \theta_p \leq \pi$ tel que

$$\cos \theta_p = \frac{a_p}{2\sqrt{p}}.$$

Notons que par la proposition 6.17, un premier $p \geq 5$ de bonne réduction pour E est supersingulier si et seulement si $\theta_p = \pi/2$. La seconde partie de la question 8.1 devient alors

Question 8.2. *Quelle est la répartition (au sens de la section 2.2 du chapitre 2) de la variable aléatoire $\{\theta_p\}_p$ dans $[0, \pi]$ quand p varie parmi les premiers de bonne réduction ? Quelle est la répartition/densité des premiers p tels que $\theta_p = \pi/2$?*

1. Prélude : multiplication complexe

Nous verrons dans les sections qui suivent que les réponses à la question 8.1 varient suivant que la courbe ait ou non des "symétries supplémentaires".

Plus précisément, on dit qu'une courbe elliptique E définie sur $\mathbb{C}$ a **multiplication complexe** (CM) si elle contient plus d'endomorphismes que les $\mathbb{Z}$-multiplications, c'est-à-dire si

$$\mathrm{End}(E) \supsetneq \{[m] : E \to E : m \in \mathbb{Z}\}.$$

Exemple 8.3. La courbe elliptique $y^2 = x^3 + x$ a multiplication complexe. En effet, un endomorphisme f est donné par $(x, y) \mapsto (-x, iy)$. Ce morphisme n'est pas un des morphismes de multiplication, puisque ceux-ci sont définis sur $\mathbb{Q}$ (la courbe l'étant), alors que f ne l'est pas. De même, la courbe $y^2 = x^3 + 1$ a multiplication complexe : si $\zeta \in \mathbb{C}$ est une racine $3^{\text{ème}}$ de l'unité, alors $(x, y) \mapsto (\zeta x, y)$ est un endomorphisme de la courbe qui n'est pas un endomorphisme de multiplication pour la même raison que précédemment.

Exemple 8.4. En revanche, la courbe $y^2 = x^3 + x + 1$ n'a pas multiplication complexe, ce qui est toutefois difficile à montrer. Nous verrons une illustration graphique de ce fait plus loin.

En fait, il est possible de connaître explicitement à quels anneaux l'anneau d'endomorphismes d'une courbe elliptique peut être isomorphe :

Proposition 8.5. *Soit E une courbe elliptique définie sur un corps de caractéristique* 0. *Alors* $\mathrm{End}(E)$ *est isomorphe à $\mathbb{Z}$ ou à un ordre d'un corps quadratique imaginaire.*

Démonstration. Voir par exemple [Was08, Th. 10.2] ou [Sil86, III.9]. En particulier, on note que l'anti-involution $\hat{\cdot} : \mathrm{End}(E) \to \mathrm{End}(E)$ (isogénie duale) correspond à la conjugaison dans $\mathbb{C}$ et que tout entier rationnel $m \in \mathbb{Z} \subset \mathbb{C}$ correspond à la multiplication $[m] \in \mathrm{End}(E)$. Par conséquent, le degré d'une isogénie correspond à la norme (de l'extension $\mathbb{C}/\mathbb{R}$). En effet, si $f \in \mathrm{End}(E)$, alors $[\deg f] = f \circ \hat{f}$ par le théorème A.12. □

Remarque 8.6. Dans le cas d'une courbe elliptique sur un corps quelconque, ce résultat reste vrai si l'on rajoute le cas d'ordres d'algèbres de quaternions, voir [Sil86, III.9.4].

2. Réinterprétation du problème

En premier lieu, nous réinterprétons la question 8.2 dans le contexte de la première partie du travail. Plus précisément, on montre un lien entre les morphismes de Frobenius associés aux réductions de la courbe et des morphismes de Frobenius reliés à des corps de nombres associés à la courbe.

Comme plus haut, considérons une courbe elliptique E définie sur $\mathbb{Q}$. Rappelons que pour tout premier ℓ, nous avons la représentation galoisienne ℓ-adique

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

qui va permettre d'obtenir le lien cherché.

Pour la suite, fixons un premier ℓ quelconque, donc on discutera la dépendance plus tard.

2.1. Réduction à des corps de nombres

Considérons en premier lieu pour tout $m \geq 1$ la représentation

$$\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell^m)$$

induite par projection. Comme $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\ker\rho_m \cong \mathrm{im}\,\rho \leq \mathrm{GL}_2(\mathbb{Z}/\ell^m)$, le sous-groupe $\ker\rho_m$ est d'indice fini dans $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Par théorie de Galois infinie, $\ker\rho_m$ correspond à un sous-corps

$$\mathbb{Q} \subset K_m = \overline{\mathbb{Q}}^{\ker\rho_m} \subset \overline{\mathbb{Q}}$$

d'indice fini dans $\mathbb{Q}$. De plus,

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\ker\rho_m \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K_m) \cong \mathrm{Gal}(K_m/\mathbb{Q})$$

au travers du morphisme $(\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}) \mapsto (\sigma_{|K_m} : K_m \to \sigma(K_m) = K_m)$.

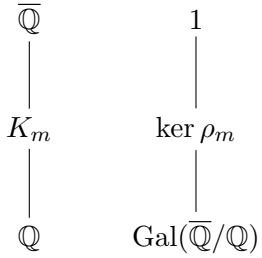


FIGURE 8.1: Illustration de la correspondance de Galois utilisée.

Ainsi, on s'est donc réduit à des représentations injectives

$$\overline{\rho}_m : \mathrm{Gal}(K_m/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell^m)$$

avec K_m un corps de nombres relié à la courbe elliptique E. Notons que comme $K_m = \overline{\mathbb{Q}}^{\ker\rho_m}$, on a $E[\ell^m] \subset K_m$, ce qui va être utile plus tard.

2.2. Ramification

Puisque K_m est un corps de nombres, on peut examiner la ramification d'un premier p dans K_m. Il se trouve que celle-ci dépend de la courbe d'une manière très naturelle.

Proposition 8.7. *Si p ne divise pas $\Delta(E)$ et $p \neq \ell$, alors p n'est pas ramifié dans K_m pour tout $m \geq 1$.*

En d'autres termes, il suffit que E ait bonne réduction mod $p \neq \ell$ afin que p ne se ramifie pas dans K_m.

Démonstration. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_{K_m}$ au-dessus de p. Rappelons que si $D_{\mathfrak{P}}$ est le groupe de décomposition de $\mathfrak{P}$, l'homomorphisme

$$f : D_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_{K_m}/\mathfrak{P})/\mathbb{F}_p)$$

est surjectif, de noyau est égal au sous-groupe d'inertie $I_{\mathfrak{P}}$, dont la cardinalité est égale à l'exposant de $\mathfrak{P}$ dans la décomposition de p dans $\mathcal{O}_{K_m}$. Par conséquent, il suffit de montrer que f est injectif pour tout $\mathfrak{P}$ au-dessus de p pour montrer que p n'est pas ramifié dans K.

Supposons que $\sigma \in \ker f$. Cela signifie que pour tout $P \in \mathcal{O}_{K_m}$, on a $[\sigma(P)]_{\mathfrak{P}} = [P]_{\mathfrak{P}}$, c'est-à-dire que $\sigma(x) - x \in \mathfrak{P}$ pour tout $x \in \mathcal{O}_{K_m}$. Pour montrer que $\sigma = \mathrm{id}$, il suffit de montrer que $\overline{\rho}_m(\sigma) = 0$, du fait que $\overline{\rho}_m$ est injective. On a

$$\begin{aligned} \overline{\rho}_m(\sigma) : E[\ell^m] &\to E[\ell^m] \\ P &\mapsto \hat{\sigma}(P), \end{aligned}$$

où $\hat{\sigma}$ est un prolongement de σ à $\overline{\mathbb{Q}}$. Plus haut, nous avons remarqué que $E[\ell^m] \subset K$. Du fait que K_m soit le corps de fractions de $\mathcal{O}_{K_m}$, il suffit donc de montrer que $\overline{\rho}_m(\sigma)(E(\mathcal{O}_{K_m})[\ell^m]) = 0$. Soit $P \in E(\mathcal{O}_{K_m})[\ell^m]$. Par l'observation ci-dessus, on a

$$\overline{\rho}(\sigma)(P) = P + Q$$

avec $Q \in \mathbb{A}^2(\mathfrak{P}) \cap E(\mathcal{O}_K)$. Par conséquent, il suffit de montrer que $Q = O$.

Comme E a bonne réduction mod p, on peut considérer la réduction E_p. Par le corollaire 7.14, puisque $p \neq \ell$, l'application

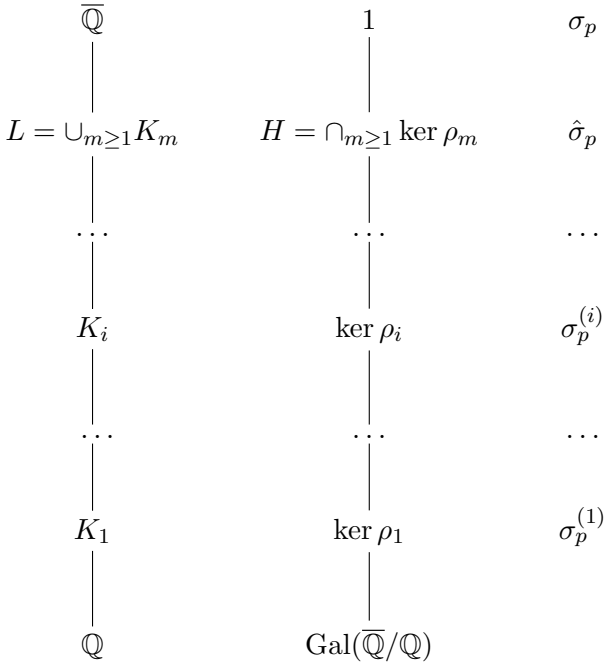
$$E(\mathcal{O}_K)[\ell^m] \to E_{\mathfrak{P}}(\mathbb{F}_p)$$

est injective. Or, comme $\mathfrak{P} \cap \mathbb{Z} = (p)$, l'image de Q y est égale à O, d'où le résultat. □

2.3. Les Frobenius reliés aux K_m

Par la proposition 8.7, tout premier $p \neq \ell$ de bonne réduction pour E ne se ramifie dans aucun des K_m pour $m \geq 1$. On peut donc considérer pour tout $m \geq 1$ le Frobenius $\sigma_p^{(m)} \in \mathrm{Gal}(K_m/\mathbb{Q})$ correspondant à p dans K_m, défini à conjugaison près.

Par définition, $K_m = \overline{\mathbb{Q}}^{\ker \rho_m}$. Comme $\ker \rho_{m+1} \leq \ker \rho_m$ pour $m \geq 1$, on a que $K_m \subset K_{m+1}$ pour tout $m \geq 1$. Par conséquent, l'union $L = \cup_{m \geq 1} K_m$ est un sous-corps de $\overline{\mathbb{Q}}$, qui correspond au sous-groupe $H = \cap_{m \geq 1} \ker \rho_m$.



Remarquons que par définition, on a $\sigma_p^{(m+1)}|_{K_m} = \sigma_p^{(m)} \in \mathrm{Gal}(K_m/\mathbb{Q})$ pour tout $m \geq 1$ (à conjugaison près). Par conséquent, on peut définir à conjugaison près $\hat{\sigma}_p \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\hat{\sigma}_p|_{K_m} = \sigma_p^{(m)}$ pour tout $m \geq 1$.

Soit $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H$ l'image de $\hat{\sigma}_p$ par l'isomorphisme

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/L) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H.$$

Par définition de H, il fait alors sens d'évaluer $\rho(\sigma_p) \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ et on a que $\overline{\rho}_m(\sigma_p|_{K_m}) = \overline{\rho}_m(\sigma_p^{(m)})$ pour tout $m \geq 1$.

2.4. Les deux Frobenius

Pour tout premier $p \neq \ell$ de bonne réduction pour E, nous avons maintenant deux *Frobenius*, l'un obtenu à travers la représentation galoisienne ℓ-adique, l'autre intrinsèque à la courbe :

1. Dans la section précédente, nous avons obtenu un élément
$$\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H$$
pour lequel on peut évaluer $\rho(\sigma_p) \in \mathrm{GL}_2(\mathbb{Z}_\ell)$.
2. De plus, nous avons aussi l'application de Frobenius $\varphi_p : E_p \to E_p$ sur la réduction de E modulo p et son image par rapport au module de Tate
$$(\varphi_p)_\ell \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E_p)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

En fait, il se trouve que ces deux *Frobenius* sont égaux dans $\mathrm{GL}_2(\mathbb{Z}_\ell)$:

Proposition 8.8. *Sous les hypothèses précédentes,*
$$\rho(\sigma_p) = (\varphi_p)_\ell \in \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Démonstration. Il s'agit de comparer l'action de σ_p sur $E_p[\ell^m]$ pour tout $m \geq 1$ avec celle de φ_p. Soit $m \geq 1$ et $P = [x, y, z] \in E[\ell^m]$. D'une part, on a
$$\varphi_p(P) = [x^p, y^p, z^p] =: P^p.$$
D'autre part, on a $E_p[\ell^m] \subset K_m$ (voir les sections précédentes), donc on peut supposer comme dans la preuve de la proposition 8.7 que $P \in \mathcal{O}_{K_m}$. Soit $\mathfrak{P}$ un idéal au-dessus de p dans $\mathcal{O}_{K_m}$. On a alors par définition $[\sigma_p(x)]_\mathfrak{P} = [x^p]_\mathfrak{P}$. Comme dans la preuve de la proposition 8.7, on voit que
$$\sigma_p(P) = P^p \in E_p[\ell^m],$$
ce qui permet de conclure. □

Corollaire 8.9. $\det \rho(\sigma) = p$ *et* $\mathrm{tr}\, \rho(\sigma) = a_p$ *dans* $\mathbb{Z}_\ell$.

Démonstration. Découle immédiatement de la proposition 6.7, décrivant le déterminant et la trace du morphisme de Frobenius φ_p dans le module de Tate. □

Par conséquent, étudier la répartition des a_p modulo ℓ revient à s'intéresser à *la répartition des (traces) des images des Frobenius par* $\overline{\rho}$, ce qui est précisément ce qui a été étudié au chapitre 4.

Remarque 8.10. Comme dans la proposition 6.7, on remarque qu'il n'y a en fait pas de dépendance par rapport à ℓ si l'on s'intéresse uniquement à la trace et au déterminant de $\rho(\sigma_p)$, ce qui sera notre cas.

Notons que si l'on est uniquement intéressés à des relations modulo ℓ, on peut considérer le Frobenius $\sigma_p^{(1)} \in \mathrm{Gal}(K_1/\mathbb{Q})$ (défini à conjugaison près), qui vérifie

$$\det\left(\overline{\rho}_1(\sigma_p^{(1)})\right) \equiv p \pmod{\ell} \text{ et } \mathrm{tr}\left(\overline{\rho}_1(\sigma_p^{(1)})\right) \equiv a_p \pmod{\ell}, \tag{8.1}$$

où la trace et le déterminant sont définis à travers l'isomorphisme $\mathrm{End}(E[\ell]) \cong \mathrm{Mat}_2(\mathbb{Z}/\ell)$.

3. Densités : application du théorème de Chebotarev

Comme première application du lien explicité dans la section précédente, nous examinons la densité d'ensembles de premiers faisant intervenir les a_p polynomialement : pour tout polynôme non-nul $f \in \mathbb{Q}[X,Y]$, on définit l'ensemble de premiers

$$\mathcal{P}_f = \{p \text{ de bonne réduction } : f(p, a_p) = 0\}.$$

Sous cette forme, on peut poser de nombreuses questions, par exemple :

- Pour $f(X,Y) = Y$, l'ensemble $\mathcal{P}_f$ représente les premiers de bonne réduction p tels que E_p est supersingulière.
- Si $f(X,Y) = Y - 1$, alors $\mathcal{P}_f$ représente les premiers de bonne réduction p tels que $|E_p(\mathbb{F}_p)| = p$, c'est-à-dire quand $E_p(\mathbb{F}_p)$ est un groupe cyclique d'ordre p.

En appliquant le théorème de densité de Chebotarev, nous allons montrer le résultat suivant :

Théorème 8.11. *Si E n'a pas multiplication complexe, alors pour tout polynôme non-nul $f \in \mathbb{Q}[X,Y]$, l'ensemble $\mathcal{P}_f$ a densité naturelle nulle.*

En fait, le théorème 8.11 se base sur un résultat important de Serre donnant précisément l'image de $\bar{\rho}_1$ dans le cas où la courbe n'a pas multiplication complexe :

Théorème 8.12 (Serre)**.** *Si E n'a pas multiplication complexe, alors il existe ℓ assez grand tel que $\bar{\rho}_1$ soit surjective, c'est-à-dire que* $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$.

Ce théorème se trouve dans l'article [Ser72] et sa démonstration serait hors de portée de ce travail. Néanmoins, nous allons montrer comment en découle le théorème 8.11 à partir du théorème de densité de Chebotarev.

Pour cela, on se ramène au fait que le Corollaire 8.9 (plus précisément l'équation (8.1)) donne des informations modulo un premier. Pour $f \in \mathbb{Q}[X, Y]$ et un premier ℓ, on considère l'ensemble $\mathcal{P}_{f,\ell} = \{p \text{ de bonne réduction } : f(p, a_p) = 0 \pmod{\ell}\}$ et on montre premièrement le résultat suivant :

Théorème 8.13. *Si E a multiplication complexe, alors pour tout premier ℓ, l'ensemble $P_{f,\ell}$ admet une densité λ_ℓ et $\lim_{\ell\to\infty} \lambda_\ell = 0$.*

Démonstration. Par l'équation (8.1),

$$\mathcal{P}_{f,\ell} = \{p \neq \ell \text{ de bonne réd. } : f(\det(\overline{\rho}_1(\sigma_p)), \operatorname{tr}(\overline{\rho}_1(\sigma_p))) = 0 \pmod{\ell}\}.$$

En posant $E = \{M \in \mathrm{GL}_2(\mathbb{F}_\ell) : f(\det(M), \operatorname{tr}(M)) = 0\}$, on a la vision alternative $\mathcal{P}_{f,\ell} = \{p : \sigma_p \in E\}$. Comme $M \mapsto f(\det(M), \operatorname{tr}(M))$ est une fonction centrale, E est contenu dans une unique classe de conjugaison C_ℓ de $\mathrm{GL}_2(\mathbb{F}_\ell)$, donc la densité $\lim_{n\to\infty} \frac{|\{p\in\mathcal{P}_{f,\ell} : p\leq n\}|}{\pi(n)}$ est bornée par

$$\lim_{n\to\infty} \frac{|\{p \leq n \text{ de bonne réd. } : p \neq \ell,\ \sigma_p \in C_\ell\}|}{\pi(n)} = \frac{|C_\ell|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|},$$

où l'égalité pour ℓ assez grand découle du théorème de densité de Chebotarev et le théorème 8.12. Rappelons que $\mathrm{GL}_2(\mathbb{F}_\ell)$ a cardinalité $(\ell^2 - 1)(\ell^2 - \ell)$ et qu'il possède $\ell^2 - 1$ classes de conjugaison de tailles 1, $\ell^2 - 1$ (représentant parabolique), $\ell^2 + \ell$ (représentant hyperbolique) ou $\ell^2 - \ell$ (représentant elliptique). Par conséquent, $\lambda_\ell \ll \ell^2/\ell^4 \to 0$ quand $\ell \to \infty$. □

Démonstration du théorème 8.11. Pour tout premier ℓ, on a $\mathcal{P} \subset \mathcal{P}_\ell$, donc le résultat est clair par le théorème précédent. □

4. Distribution des θ_p : observations numériques

Après avoir répondu à une partie de la question 8.2, intéressons-nous maintenant au problème de la répartition des θ_p pour une courbe elliptique E définie sur $\mathbb{Q}$ et p un premier de bonne réduction. Rappelons que nous avons formalisé les questions de répartition de variables aléatoires $(X_p) \subset \mathbb{R}$ (p un premier) à la fin du chapitre 2.

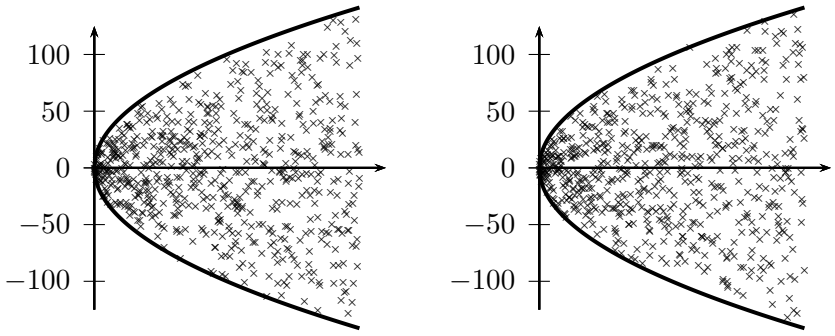
Les figures 8.3 et 8.2 illustrent graphiquement la répartition des valeurs a_p et des angles θ_p pour un échantillon de premiers, dans le cas de deux courbes CM et deux courbes non-CM. A partir de là, il est possible de faire plusieurs observations :

1. Dans le cas CM, les angles θ_p semblent se répartir selon une distribution avec fonction de distribution combinaison convexe
   a) de la fonction de répartition $F_{U(0,\pi)}$ d'une variable aléatoire uniforme sur $[0, \pi]$;

b) de la fonction de répartition $F_{\delta_{\pi/2}}$ d'une variable aléatoire discrète prenant comme seule valeur $\pi/2$.

En d'autres termes, il semble qu'hormis les premiers supersinguliers, la distribution des θ_p soit uniforme.

2. Dans le cas non-CM, les angles θ_p semblent suivre une fonction de densité proportionnelle à $\sin^2(x)$, tracée sur les histogrammes de la figure 8.3.



(a) $y^2 = x^3 + x + 1$. (b) $y^2 = x^3 + x$.

FIGURE 8.2: Graphe des fonctions a_p pour deux courbes elliptiques, avec $p < 5000$. En gras, la courbe $|y| = 2\sqrt{x}$ pour illustrer la borne de Hasse $|a_p| \leq 2\sqrt{p}$.

5. Le cas CM

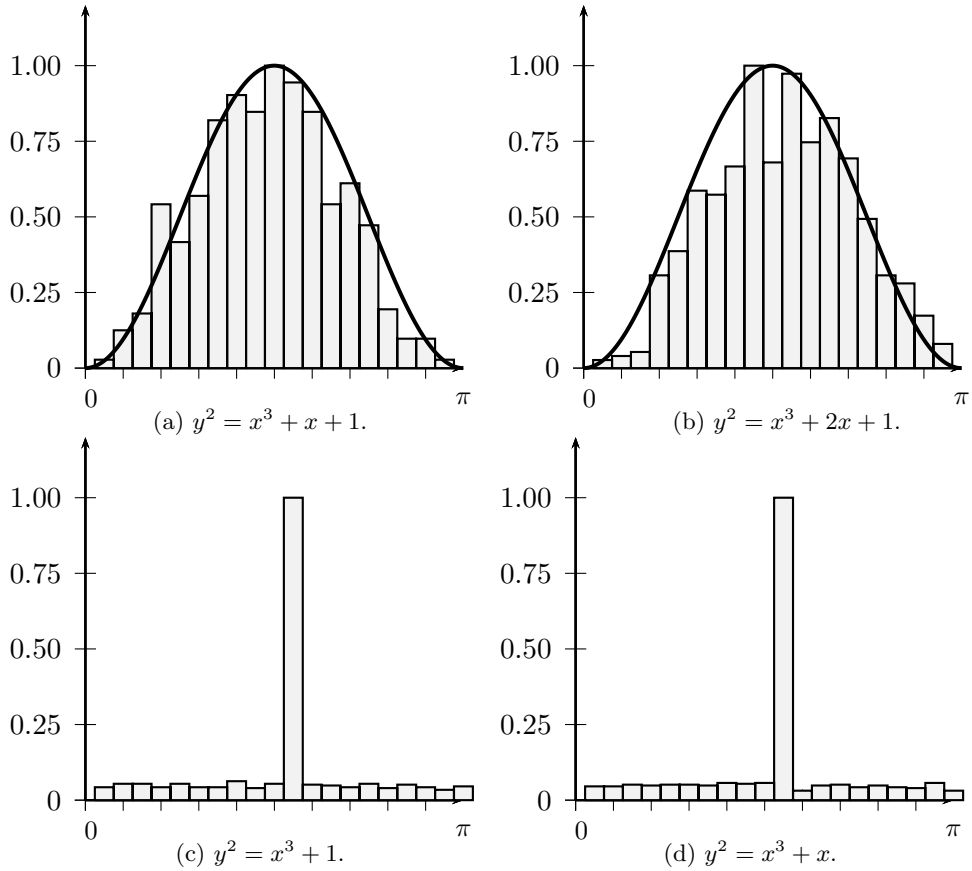
Dans le cas CM, nous montrons pourquoi la distribution observée dans la section précédente est vérifiée dans le cas général, à savoir :

Théorème 8.14. *Soit E une courbe elliptique définie sur $\mathbb{Q}$ avec multiplication complexe Alors la variable aléatoire θ_p (p premier de bonne réduction) possède comme fonction de répartition*

$$CF_{U(0.\pi)} + (1 - C)F_{\delta_{\pi/2}},$$

pour une certaine constante $C \in (0, 1)$, dans les notations de la section précédente.

Remarque 8.15. Dans ce chapitre, nous nous restreignons à des courbes elliptiques définies sur $\mathbb{Q}$. Néanmoins, on peut considérer les mêmes questions pour une courbe elliptique sur un corps de nombres K : à tout idéal premier $\mathfrak{p}$ de K est alors associé un angle $\theta_{\mathfrak{p}}$. De même, on construit une semi-mesure de probabilité sur l'ensemble des idéaux premiers de K et on définit les courbes avec multiplication complexe de manière similaire. Le théorème 8.14 se généralise alors, mais la composante discrète disparaît si le corps quadratique dans lequel se trouve $\mathrm{End}(E)$ est contenu dans K : la variable aléatoire $\theta_{\mathfrak{p}}$ est simplement équirépartie dans $[0, \pi]$. Il s'agit du cas traité dans [Kob82, p. 195] pour simplifier.



(a) $y^2 = x^3 + x + 1$. (b) $y^2 = x^3 + 2x + 1$.

(c) $y^2 = x^3 + 1$. (d) $y^2 = x^3 + x$.

FIGURE 8.3: Histogrammes des répartitions des angles θ_p pour plusieurs courbes elliptiques (CM et non-CM), avec $p < 5000$. Pour les deux premières, la courbe $y = 2/\pi \sin^2(x)$ est tracée.

Comme une partie de la théorie sous-jacente est trop vaste pour être présentée ici, nous renvoyons la preuve de certains résultats à des références, tout en essayant d'en illustrer la plus grande partie possible.

Dans les deux paragraphes qui suivent, nous tentons d'expliquer la distribution du théorème 8.14. Pour cela, on considère une courbe elliptique E définie sur $\mathbb{Q}$ avec multiplication complexe, c'est-à-dire $\mathrm{End}(E) \cong \mathcal{O}$, avec $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K. Soit $d < 0$ sans facteur carré tel que $K \cong \mathbb{Q}(\sqrt{d})$. Notons encore f le conducteur de $\mathcal{O}$, i.e. $\mathcal{O} \cong \mathbb{Z} + f\mathcal{O}_K$.

5.1. Composante discrète

D'une part, le résultat suivant de Deuring permet de décrire facilement quand la réduction de E mod p est supersingulière (rappelons que l'on suppose que E a multiplication complexe).

Proposition 8.16 (Deuring)**.** *Si $p > 2$ est un premier de bonne réduction ne divisant pas f, alors E_p est supersingulière si et seulement si p se ramifie ou reste premier dans K.*

Démonstration. Voir [Lan87, Théorème 12, p. 182]. □

Corollaire 8.17. *Si $p > 2$ est un premier de bonne réduction ne divisant pas f, alors*

$$E_p \text{ supersingulière } \Leftrightarrow \left(\frac{d}{p}\right) \in \{-1, 0\}.$$

Démonstration. Nous avons vu dans l'exemple 1.22 du chapitre 1 que p se sépare si et seulement si $\left(\frac{d}{p}\right) = 1$. □

5.2. Composante continue

Pour la composante continue, nous avons donc le résultat suivant de répartition uniforme :

Proposition 8.18. *Pour tout intervalle $[\alpha, \beta] \subset [0, \pi]$, on a que*

$$\mu\left(\theta_p \in [\alpha, \beta] \mid \theta_p \neq \pi/2\right) = \beta - \alpha.$$

Pour expliquer ceci, nous donnons deux approches :

1. La première se ramenant à un problème de répartition dans des secteurs d'éléments de norme un premier dans l'ordre d'un corps quadratique imaginaire. Cette approche permet de comprendre en partie le rôle du corps quadratique, mais ne permet seulement de démontrer que $\{\theta_p, -\theta_p\}$ est équirépartie dans $[-\pi, \pi]$, avec l'hypothèse que $d < -4$.
2. La seconde dans le contexte du chapitre 4, à travers des fonctions L. Elle s'appuie sur la relation avec des fonctions L de Hecke et leur propriété de prolongement, mais permet de démontrer la proposition 8.18 en admettant ceci.

La seconde approche sera développée plus en détails pour étudier le cas non-CM.

Première approche

Théorème 8.19 (Théorème de réduction de Deuring)**.** *Si $p \nmid f$ est un premier tel que E_p ne soit pas supersingulière, alors l'application de réduction des homomorphismes modulo p*

$$\begin{array}{ccc} \mathrm{End}(E) & \to & \mathrm{End}(E_p) \\ f & \mapsto & f_p \end{array}$$

est un isomorphisme d'anneaux, d'où $\mathrm{End}(E_p) \cong \mathcal{O}$.

Démonstration. Voir [Lan87, Théorème 12, p. 182]. Rappelons (proposition 7.11 et corollaire 7.12) que cet homomorphisme préserve les isogénies duales et les degrés. □

Corollaire 8.20. *Sous les notation du théorème 8.19, on a*

$$a_p = x + \overline{x} = 2\,\mathrm{Re}(x),$$

pour un certain $x \in \mathcal{O}$ *tel que* $N(x) = p$. *De plus, si* $d < -4$ *et* $y \in \mathcal{O}$ *vérifie* $N(y) = p$, *alors* $2\,\mathrm{Re}(y) = \pm a_p$.

Démonstration. Considérons la préimage $\varphi \in \mathrm{End}(E)$ du Frobenius $\varphi_p \in \mathrm{End}(E_p)$ par l'isomorphisme $\mathrm{End}(E) \to \mathrm{End}(E_p)$ donné par le théorème. Par le corollaire 7.12, on a

$$p = \deg \varphi_p = \deg \varphi = N(\varphi),$$

en identifiant $\mathrm{End}(E)$ avec $\mathcal{O}$. Par conséquent, $(\varphi), (\overline{\varphi})$ sont des idéaux premiers de $\mathcal{O}$ tels que $(p) = (\varphi)(\overline{\varphi})$. Or, par la section 6.1 du chapitre 6,

$$\begin{aligned} |E(\mathbb{F}_p)| &= \deg(\mathrm{id} - \varphi_p) = \deg(\mathrm{id} - \varphi) = N(1-\varphi) = (1-\varphi)(1-\overline{\varphi}) \\ &= 1 - (\varphi + \overline{\varphi}) + N(\varphi) = 1 - (\varphi + \overline{\varphi}) + p, \end{aligned}$$

d'où le résultat. Si $y \in \mathcal{O}$ vérifie $N(y) = p$, alors $2\,\mathrm{Re}(y) = u\varphi + \overline{u\varphi}$ avec $u \in \mathcal{O}^\times = \{\pm 1\}$ ($d < -4$), d'où la seconde affirmation. □

Nous en tirons alors le résultat suivant qui montre le lien avec des questions de répartition d'arguments d'éléments de $\mathcal{O}$:

Corollaire 8.21. *Sous les notation du théorème 8.19, on a*

$$\theta_p = \pm \arg(x)$$

pour tout $x \in \mathcal{O}$ *tel que* $N(x) = p$.

Démonstration. Le corollaire 8.20 montre donc que

$$\cos\theta_p = \frac{|a_p|}{2\sqrt{p}} = \frac{|\,\mathrm{Re}(x)|}{\sqrt{p}} = \cos(\arg(x))\frac{||x||}{\sqrt{N(x)}} = \cos(\arg(x))$$

puisque K est un corps quadratique *imaginaire*, ce qui implique que $\theta_p = \pm\arg(x)$. □

Rappelons que $\mathcal{O}$ est un $\mathbb{Z}$-module libre de rang 2, une $\mathbb{Z}$-base étant par exemple donnée par $\{1, \tau\} = \{1, f\frac{d+\sqrt{d}}{2}\}$. Nous obtenons que, pour $a, b \in \mathbb{Z}$,

$$N(a,b) := N(a+b\tau) = (a+b\tau)(a+b\bar{\tau}) = a^2 + df \cdot ab + f^2\frac{d^2-d}{4}b^2,$$

c'est-à-dire que la norme N peut être vue comme une forme quadratique binaire à coefficients entiers de discriminant $f^2 d$. Nous avons alors le théorème suivant :

Proposition 8.22 (Hecke)**.** *Soit $Q(x,y) = ax^2 + bxy + cy^2$ une forme quadratique définie positive à coefficients entiers, de discriminant $d < -4$ supposé fondamental. Pour $0 \leq \alpha < \beta \leq 2\pi$ et $N \geq 0$, soit $S(N, [\alpha, \beta])$ le nombre de $(x,y) \in \mathbb{Z}^2$ tels que $Q(x,y)$ soit un premier $\leq N$ et*

$$\alpha \leq \arg\left(ax + \frac{b+\sqrt{d}}{2}y\right) \leq \beta.$$

Alors $S(N, [\alpha, \beta]) \sim \frac{\beta-\alpha}{2\pi} S(N, [0, 2\pi])$.

Démonstration. Voir par exemple l'article [Kna69], où S. Knapowski donne une preuve en utilisant le critère d'équirépartition de Weyl la correspondance entre formes quadratiques binaires et idéaux d'ordres de corps quadratiques. □

Pour le cas plus haut, nous avons que pour tous $0 \leq \alpha < \beta \leq 2\pi$,

$$\begin{aligned} S(N, [\alpha, \beta]) &= |\{x \in \mathcal{O} : N(x) = p \leq N, \arg(x) \in [\alpha, \beta]\}| \\ &= \sum_{p \leq N} \sum_{x \in \mathcal{O} : N(x) = p} 1_{[\alpha,\beta]}(\arg(x)) \\ &= \sum_{p \leq N} \left(1_{[\alpha,\beta]}(\theta_p) + 1_{[\alpha,\beta]}(-\theta_p)\right), \end{aligned}$$

d'où la répartition uniforme des $\{\theta_p, -\theta_p\}$ (p premier de bonne réduction tel que E_p ne soit pas supersingulière) dans $[-\pi, \pi]$, par la proposition 8.22.

Seconde approche Plaçons-nous dans le cadre du chapitre 4 en posant $\mathcal{P}$ l'ensemble des premiers de bonne réduction pour E tels que E_p ne soit pas supersingulière et $\sigma : \mathcal{P} \to \mathbb{R}/\mathbb{Z}$ l'application envoyant $p \in \mathcal{P}$ sur $\tilde{\theta}_p = \theta_p/\pi \in [0,1]$. Par l'exemple 2.12, les représentations irréductibles de $\mathbb{R}/\mathbb{Z}$ sont les caractères $\chi_m : \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$ définis par $\chi_m(x) = e^{2i\pi m x}$, pour $m \in \mathbb{Z}$. Par la remarque 3.4, la fonction L associée à χ_m est

$$L_m(s) := L_c(s, \chi_m) = \prod_{\mathfrak{p} \in \mathcal{P}} \left(1 - \frac{\chi_m(\theta_p)}{p}\right)^{-1}.$$

Par l'exemple 2.15, l'équirépartition des $\tilde{\theta}_p$ ($p \in \mathcal{P}$) dans $\mathbb{R}/\mathbb{Z}$ est équivalente à l'équirépartition des θ_p dans $[0, \pi]$. Par le théorème central de la première partie (Théorème 4.5), ceci est vérifié si L_m se prolonge analytiquement sur $\mathrm{Re}(s) \geq 1$ sans s'y annuler.

En fait, on peut montrer que dans le cas CM, les fonctions L_m sont reliées avec des fonctions L de Hecke, qui admettent cette propriété, d'où la répartition uniforme de la proposition 8.18. Ceci peut se trouver par exemple dans [Sil94, II.9-10]. La théorie des fonctions L de Hecke est quant à elle par exemple développée dans [Neu99, VII].

5.3. Conclusion

Preuve du théorème 8.14. Par les paragraphes précédentes, nous avons donc, pour deux réels $\alpha < \beta$,

$$\begin{aligned}\mu(\theta_p \in [\alpha, \beta]) &= \mu\left(\theta_p \in [\alpha, \beta] \mid \theta_p = \frac{1}{2}\right)\mu\left(\theta_p = \frac{1}{2}\right) \\ &\quad + \mu\left(\theta_p \in [\alpha, \beta] \mid \theta_p \neq \frac{1}{2}\right)\mu\left(\theta_p \neq \frac{1}{2}\right) \\ &= C\delta_{[\alpha,\beta]}(1/2) + (1 - C)\frac{\beta - \alpha}{\pi},\end{aligned}$$

où $C = \mu(p : \left(\frac{d}{p}\right) \in \{-1, 0\})$. □

6. Le cas non-CM

Pour le cas non-CM, la distribution des θ_p est en fait encore un problème ouvert et la distribution que nous avons observé numériquement est la *conjecture de Sato-Tate* :

Conjecture 8.23 (Sato-Tate)**.** *Si E est une courbe elliptique définie sur $\mathbb{Q}$ n'ayant pas multiplication complexe, alors la variable aléatoire $\{\theta_p\}$ (p premier de bonne réduction) est distribuée selon la densité $2/\pi \sin^2\theta \; 1_{[0,\pi]}$.*

En fait, en utilisant le point de vue des Frobenius induits par les représentations ℓ-adique comme dans la section 8.2, on peut donner une interprétation très naturelle de la mesure $2/\pi \sin^2\theta d\theta$, ainsi qu'une autre vision du problème. C'est ce que nous ferons dans la section suivante.

6.1. Transfert de la question dans $\mathrm{SU}_2(\mathbb{C})$

Pour tout premier ℓ, nous avons la représentation ℓ-adique

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell) \subset \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

associée à E

Dans la section 8.2, nous avons montré l'existence d'un Frobenius $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tel que

$$\det(\rho(\sigma_p)) = p \in \mathbb{Z}_\ell \text{ et } \mathrm{tr}(\rho(\sigma_p)) = a_p \in \mathbb{Z}_\ell.$$

En fixant un représentant de la classe de conjugaison de σ_p, la matrice $\sigma_p \in \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ est conjuguée à une matrice de la forme

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$$

pour $a, b, c \in \overline{\mathbb{Q}}_\ell$. Par ce qui précède, $a + b = a_p$ et $ab = p$, donc on peut en fait voir cette matrice dans $\mathrm{GL}_2(\mathbb{C})$. Plus précisément, le polynôme minimal de $\rho(\sigma_p)$ est $X^2 - a_p X + p$, qui a discriminant $a_p^2 - 4p \leq 0$ par la borne de Hasse. Par conséquent, ses racines sont complexes conjuguées et de norme $\sqrt{p}$. Ainsi, on peut voir la (classe de conjugaison de) la matrice $\rho(\sigma_p)/\sqrt{p}$ comme une matrice dans $\mathrm{SU}_2(\mathbb{C})$! Ainsi, on a une application

$$\begin{array}{rcl} \psi : \{p \neq \ell \text{ premier de bonne réduction}\} & \to & \mathrm{SU}_2(\mathbb{C})/\text{conjugaison} \\ p & \mapsto & \rho(\sigma_p)/\sqrt{p} \end{array}$$

telle que $\mathrm{tr}(\psi(p))) = a_p/\sqrt{p}$. En d'autres termes, $\mathrm{tr}(\psi(p)) = 2\cos\theta_p$.

A l'aide du théorème spectral, on décrit facilement les classes de conjugaison de $\mathrm{SU}_2(\mathbb{C})$:

Proposition 8.24. *L'application*

$$\mathrm{tr} : \mathrm{SU}_2(\mathbb{C})/\textit{conjugaison} \to [-2, 2]$$

est une bijection.

Démonstration. Par le théorème spectral, tout élément de $\mathrm{SU}_2(\mathbb{C})$ est diagonalisable, c'est-à-dire est conjugué *dans* $\mathrm{SU}_2(\mathbb{C})$ à une matrice de la forme

$$M = \begin{pmatrix} a + bi & 0 \\ 0 & a - bi \end{pmatrix}$$

avec $a, b \in \mathbb{R}$ tels que $a^2 + b^2 = 1$. Notons que $\mathrm{tr}\, M = 2a$ et $|a| \leq 1$, d'où $\mathrm{tr}(\mathrm{SU}_2(\mathbb{C})) \subset [-2, 2]$. De plus, l'application tr est clairement surjective. Pour

finir, si $\operatorname{tr} M = \operatorname{tr} M'$ avec $M, M' \in \mathrm{SU}_2(\mathbb{C})$, il existe $a, b, b' \in \mathbb{R}$ tels que M (resp. M') soit $\mathrm{SU}_2(\mathbb{C})$-conjugué à

$$\begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix}, \text{ resp. à } \begin{pmatrix} a+b'i & 0 \\ 0 & a-b'i \end{pmatrix}.$$

Comme $a^2 + b^2 = a^2 + (b')^2 = 1$, on a $b = \pm b'$. Si $b = b'$, on conclut immédiatement que M est conjugué à M'. Si $b = -b'$, il suffit de remarquer qu'en conjugant la seconde matrice avec $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SU}_2(\mathbb{C})$ on obtient la première. □

Ainsi, étudier la répartition des θ_p revient à étudier la répartition des $\psi(p)$ ($p \neq \ell$ premier de bonne réduction) dans les classes de conjugaison de $\mathrm{SU}_2(\mathbb{C})$.

6.2. Reformulation de la conjecture

Comme annoncé, nous allons maintenant pouvoir reformuler la conjecture de Sato-Tate de manière naturelle comme un énoncé d'équirépartition.

En premier lieu, nous déterminons explicitement l'image de la mesure de Haar sur les classes de conjugaison de $\mathrm{SU}_2(\mathbb{C})$.

Proposition 8.25. *L'image sur* $[-2, 2]$ *de la mesure de Haar normalisée* $\hat{\mu}$ *sur* $\mathrm{SU}_2(\mathbb{C})$ *par rapport à l'application*

$$\operatorname{tr} : \mathrm{SU}_2(\mathbb{C}) \to [-2, 2]$$

est donné par $\frac{1}{2\pi}\sqrt{4 - x^2}dx$. *Par suite, pour toute fonction* $f \in C([-2, 2])$, *on a*

$$\int_{\mathrm{SU}_2(\mathbb{C})} (f \circ \operatorname{tr})\, d\hat{\mu} = \frac{1}{2\pi} \int_{-2}^{2} f(x)\sqrt{4 - x^2}dx.$$

Démonstration. Soit $\mathbb{H}$ le corps gauche des quaternions de Hamilton et notons $\mathbb{H}_1$ l'ensemble des quaternions unitaires. L'idée est d'utiliser l'isomorphisme de groupes topologiques $\mathrm{SU}_2(\mathbb{C}) \cong \mathbb{H}_1$ donné par

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \mapsto a + bi + cj + dk \in \mathbb{H}_1$$

ainsi que la bijection naturelle $\mathbb{H}_1 \cong S^3$.

Soit λ la mesure de Lebesgue sur $\mathbb{R}^4$, qui est invariante par isométries. La 3-sphère S^3 possède donc une mesure μ invariante par isométries donnée par

$$\mu(A) = \lambda(\{x\underline{a} : \underline{a} \in A, x \in [0, 1]\})$$

pour tout $A \subset S^3$ mesurable. Notons que sous la bijection $\mathbb{H} \cong \mathbb{R}^4$, le produit scalaire euclidien de $x, y \in \mathbb{H}$ vus dans $\mathbb{R}^4$ peut s'exprimer par

$$\langle x, y \rangle = \mathrm{Re}(x\overline{y}).$$

Pour $x \in \mathbb{H}_1$ et $y, z \in \mathbb{H}$ on a donc

$$\langle xy, xz \rangle = \mathrm{Re}(xy\overline{xz}) = \mathrm{Re}(xy\overline{z}\overline{x}) = \mathrm{Re}(x\overline{x}y\overline{z}) = \mathrm{Re}(|x|^2 y\overline{z}) = \mathrm{Re}(y\overline{z}) = \langle y, z \rangle.$$

Ainsi, la multiplication dans $\mathbb{H}_1$ agit par isométries. Il en suit que la mesure induite sur $\mathbb{H}_1$ par la bijection $\mathbb{H}_1 \cong S^3$ est bi-invariante.

Par l'isomorphisme $\mathrm{SU}_2(\mathbb{C}) \cong \mathbb{H}_1$, on obtient alors une mesure $\hat{\mu}$ bi-invariante sur $\mathrm{SU}_2(\mathbb{C})$. Calculons maintenant son pushforward $\mathrm{tr}_* \hat{\mu}$ par rapport à tr. Pour $A \subset [-2, 2]$ mesurable, on a

$$(\mathrm{tr}_* \hat{\mu})(A) = \hat{\mu}(\mathrm{tr}^{-1}(A)) = \mu(\{(a, b, c, d) \in S^3 : 2a \in A\}).$$

Pour effectuer l'intégrale sous-jacente, on passe en coordonnées hypersphériques

$$\begin{aligned} x_1 &= r\cos\varphi_1 \\ x_2 &= r\sin\varphi_1\cos\varphi_2 \\ x_1 &= r\sin\varphi_1\sin\varphi_2\cos\varphi_3 \\ x_1 &= r\sin\varphi_1\sin\varphi_2\sin\varphi_3 \end{aligned} \tag{8.2}$$

avec $\varphi_1, \varphi_2 \in [0, \pi]$, $\varphi_3 \in [0, 2\pi)$, $r \in [0, 1]$. Puisque $d\underline{x} = r^3 \sin^2\varphi_1 \sin\varphi_2 dr d\varphi_1 d\varphi_2 d\varphi_3$, on trouve que

$$\begin{aligned} (\mathrm{tr}_* \hat{\mu})(A) &= \int_0^1 dr \int_0^\pi d\varphi_1 \int_0^\pi d\varphi_2 \int_0^{2\pi} d\varphi_3 \; r^3 \sin^2\varphi_1 \sin\varphi_2 \, \chi_A(2\cos\varphi_1) \\ &= C \int_0^\pi \sin^2\varphi_1 \, \chi_A(2\cos\varphi_1) \; d\varphi_1 \\ &= C/2 \int_{-2}^2 \chi_A(x)\sqrt{4-x^2}\, dx = C/2 \int_{x\in A} \sqrt{4-x^2} dx \end{aligned}$$

où C désigne une constante ne dépendant pas de A. Pour trouver le pushforward de l'unique mesure de Haar normalisée sur $\mathrm{SU}_2(\mathbb{C})$, on calcule encore

$$\int_{-2}^2 \sqrt{4-x^2} dx = 4 \int_0^\pi \sin^2\varphi \, d\varphi = 2\pi.$$

Ainsi, la mesure cherchée sur $[-2, 2]$ est $\frac{1}{2\pi}\sqrt{4-x^2}dx$. □

Au changement de variable $x = 2\cos\theta$ près, il s'agit précisément de la mesure présente dans la conjecture de Sato-Tate ! A partir de là, nous pouvons donner la reformulation annoncée.

Proposition 8.26. *La conjecture de Sato-Tate est vérifiée si et seulement si la suite $(\psi(p))$ ($p \neq \ell$ premier de bonne réduction) est équirépartie (au sens du chapitre 2) dans les classes de conjugaison du groupe compact* $\mathrm{SU}_2(\mathbb{C})$.

Démonstration. Rappelons que :

— Par définition et par la proposition 8.24, la suite $(\psi(p))$ est équirépartie dans les classes de conjugaison de $\mathrm{SU}_2(\mathbb{C})$ si et seulement si

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p\leq N} f(\mathrm{tr}(\psi(p))) = \int_{\mathrm{SU}_2(\mathbb{C})/\mathrm{conj.}} (f\circ \mathrm{tr}) d\nu$$

pour toute fonction continue $f : [-2,2] \to \mathbb{R}$, où ν est l'image de la mesure de Haar de $\mathrm{SU}_2(\mathbb{C})$ sur $\mathrm{SU}_2(\mathbb{C})/\mathrm{conj.}$. Par la proposition 8.25, nous avons de plus que

$$\int_{\mathrm{SU}_2(\mathbb{C})/\mathrm{conj.}} (f\circ \mathrm{tr}) d\nu = \int_{-2}^{2} f(x)\sqrt{4-x^2}dx.$$

— Par la proposition 2.23, la variable aléatoire (θ_p) est répartie selon une densité $2/\pi \sin^2\theta \; 1_{[0,\pi]}$ si et seulement si

$$\lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p\leq N} f(\theta_p) = \frac{2}{\pi}\int_0^\pi f(\theta)\sin^2\theta d\theta$$

pour toute fonction continue $f : [0,\pi] \to \mathbb{R}$.

Pour obtenir l'équivalence souhaitée, il suffit alors de se rappeler que $\mathrm{tr}(\psi(p)) = 2\cos(\theta_p)$ et de noter que si $x = 2\cos\theta_p$, alors $\sqrt{4-x^2}dx = \sin^2\theta_p d\theta_p$.

□

6.3. Reformulation en utilisant le critère d'équirépartition de Weyl

Les représentations irréductibles de $\mathrm{SU}_2(\mathbb{C})$ (comme groupe compact) sont données par les *puissances symétriques* de la représentation naturelle

$$\rho_1 : \mathrm{SU}_2(\mathbb{C}) \to \mathrm{GL}_2(\mathbb{C}).$$

Plus précisément, pour tout $m \geq 1$, soit $S^m(\mathbb{C}^2)$ l'espace vectoriel des polynômes homogènes de degré m dans $K[X,Y]$. En identifiant X et Y avec les deux éléments d'une base de $\mathbb{C}^2$, nous obtenons une action linéaire de $\mathrm{SU}_2(\mathbb{C})$ sur $S^m(\mathbb{C}^2)$ et une représentation

$$\rho_m : \mathrm{SU}_2(\mathbb{C}) \to \mathrm{GL}(S^m(\mathbb{C}^2))$$

appelée $m^{ème}$ *puissance symétrique* de ρ_1. Par la proposition 8.24, tout élément de $\mathrm{SU}_2(\mathbb{C})$ est conjugué à un élément de la forme $A_\theta = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta}\end{pmatrix}$ pour un

certain $\theta \in [0, 2\pi]$. L'action de $\rho_m(A_\theta)$ sur la base $\{X^m, X^{m-1}Y, \ldots, Y^m\}$ est alors donnée par

$$\rho_m(A_\theta)X^aY^{m-a} = e^{i\theta(2a-m)}X^aY^{m-a}$$

pour $0 \leq a \leq m$. Par conséquent, le caractère $\chi_m : \mathrm{SU}_2(\mathbb{C}) \to \mathbb{C}$ associé à ρ_m est donné par

$$\chi_m(A_\theta) = e^{-i\theta m}\sum_{a=0}^{m} e^{2ai\theta} = \frac{e^{-i\theta(m+1)} - e^{i\theta(m+1)}}{e^{-i\theta} - e^{i\theta}} = \frac{\sin((m+1)\theta)}{\sin\theta}. \quad (8.3)$$

Ce caractère est irréductible puisqu'en procédant comme dans la preuve de la proposition 8.25, on trouve que $\int_{\mathrm{SU}_2(\mathbb{C})} 1d\mu \cdot (\chi_m, \chi_m)$ est égal à

$$\begin{aligned} & \int_{\mathrm{SU}_2(\mathbb{C})} \chi_m\overline{\chi_m}d\mu \\ = & \int_0^1 dr \int_0^\pi d\varphi_1 \int_0^\pi d\varphi_2 \int_0^{2\pi} d\varphi_3\, r^3 \sin^2\varphi_1 \sin\varphi_2 \chi_m(A_{\varphi_1})\chi_m(A_{-\varphi_1}) \\ = & \frac{\pi}{2}\int_0^\pi \sin^2((m+1)\varphi_1)d\varphi_1 = \frac{\pi^2}{4} = \int_{\mathrm{SU}_2(\mathbb{C})} 1d\mu, \end{aligned}$$

d'où $(\chi_m, \chi_m) = 1$. Pour $m = 0$, on obtient le caractère trivial. On peut montrer que les χ_m $(m \geq 0)$ constituent alors toutes les représentations irréductibles de $\mathrm{SU}_2(\mathbb{C})$. Pour cela, nous renvoyons le lecteur à [Var07].

Par le critère d'équirépartition 4.5, la conjecture de Sato-Tate 8.23 est ainsi équivalente à :

Conjecture 8.27. *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Pour tout $m \geq 1$, on a*

$$\sum_{p \leq N} \frac{\sin((m+1)\theta_p)}{\sin\theta_p} = o(\pi(N)),$$

où p parcourt les premiers de bonne réduction pour E.

Kim et Shahidi ont par exemple montré (voir [Kob82]) que la conjecture 8.27 était vérifiée pour $m \leq 8$. Nous verrons plus d'avancées sur la conjecture de Sato-Tate à la section suivante-

6.4. Reformulation par des fonctions L

A partir des concepts présentés dans le chapitre 4, on peut donner une deuxième reformulation de la conjecture de Sato-Tate comme une question sur des fonctions L. Il s'agit de l'approche de Serre, à partir de laquelle on retrouve l'approche originale de Langlands dans [Lan70].

Dans les notations du chapitre 4, on considère :

— Le groupe compact $\mathrm{SU}_2(\mathbb{C})$ et l'ensemble X de ses classes de conjugaison ;
— L'ensemble $\mathcal{P}$ des premiers de bonne réduction pour E ;
— L'application $\psi : \mathcal{P} \to X$ associant à un premier p de bonne réduction la classe de $\psi(p)$.

A tout caractère irréductible de $\mathrm{SU}_2(\mathbb{C})$ nous avons alors une fonction $L_c(s, \chi)$ associée, holomorphe pour $\mathrm{Re}(s) > 1$. Dans la section précédente, nous avons déterminé les représentations irréductibles χ_m ($m \geq 0$) de $\mathrm{SU}_2(\mathbb{C})$. En notant $L_m(s) := L_c(s, \chi_m)$, on a alors la conjecture suivante :

Conjecture 8.28. *Pour tout $m \geq 1$, la fonction $L_m(s)$ se prolonge analytiquement sur $\mathrm{Re}(s) \geq 1$ sans s'annuler.*

Par le théorème 4.5 du chapitre 4, cette conjecture implique la conjecture de Sato-Tate. Si l'on arrivait à montrer que $L_m(s)$ se prolonge analytiquement sur $\mathrm{Re}(s) \geq 1$ sans s'annuler pour tout $m \geq 1$ à part éventuellement un pôle simple en $s = 1$, alors le théorème 4.5 indique que la conjecture de Sato-Tate est équivalente à l'holomorphie et la non-annulation de $L_m(s)$ en $s = 1$ pour tout $m \geq 1$. En fait, Kumar Murty a montré en 1982 (voir [Kob82, pp. 195-206]) que la non-annulation pouvait se déduire du prolongement à $\mathrm{Re}(s) \geq 1$.

Formulation originale de Langlands Notons que les valeurs propres de $\rho_m(\psi(p)) = \rho_m(A_{\theta_p})$ ($m \geq 1, p \in \mathcal{P}$) sont $e^{i\theta_p(2a-m)}$ pour $0 \leq a \leq m$, donc, par l'équation 8.3,

$$L_m(s) := L_c(s, \rho_m) = \prod_p \prod_{a=0}^{m} \left(1 - \frac{e^{i\theta_p(2a-m)}}{p^s}\right)^{-1}.$$

Dans cette écriture, il s'agit de la formulation originale de Langlands dans un article de 1970. Il y conjecture notamment un lien avec des fonctions L de *représentations automorphes*, dont la théorie générale donnerait un prolongement analytique au plan complexe entier. Pour un compte rendu plus détaillé de ces idées, voir [RMKM09].

Cas particuliers Les deux premières fonctions L_m sont les suivantes :

— Pour $m = 0$, $L_0(s) = \zeta(s)$, qui se prolonge effectivement analytiquement sans s'annuler sur $\mathrm{Re}(s) \geq 1$.
— Pour $m = 1$, la fonction $L_1(s)$ est égale à

$$\prod_{p \in \mathcal{P}} \left(1 - \frac{e^{-i\theta_p}}{p^s}\right)^{-1} \left(1 - \frac{e^{i\theta_p}}{p^s}\right)^{-1} = \prod_{p \in \mathcal{P}} (1 - a_p p^{-s-1/2} - p^{-2s})^{-1}.$$

A normalisation des a_p et facteurs de mauvaise réduction près, il s'agit de la *fonction L attachée à la courbe elliptique*. Le prolongement analytique

à $\mathrm{Re}(s) \geq 1$ est alors une conséquence du théorème de modularité (ou conjecture de Taniyama-Shimura-Weil).

Avancées Les avancées actuelles sur la conjecture de Sato-Tate sont les suivantes [1] :

— Pour $m = 2$, Rankin et Selberg ont montré le prolongement de L_2 à $\mathrm{Re}(s) \geq 1$. Plus tard, Shimura a montré que L_2 se prolonge analytiquement à $\mathbb{C}$ (résultat généralisé plus tard aux corps de nombres).

— Pour $m = 3, 4$, Kim et Shadidi ont démontré vers 2000 que L_3 et L_4 se prolongeaient également analytiquement à $\mathbb{C}$.

— Pour $5 \leq m \leq 9$, ils ont également prouvé que L_m s'étendait en une fonction méromorphe sur $\mathbb{C}$, holomorphe sur $\mathrm{Re}(s) \leq 1$ à part pour $m = 9$ où il pourrait y avoir un pôle en $s = 1$.

— Clozel, Harris et Taylor ont montré récemment que si le j-invariant de E n'est pas entier, alors la conjecture 8.28 est vérifiée.

— En 2006, Taylor, Harris et Shepherd-Barron ont montré que la conjecture de Sato-Tate était vérifiée pour les courbes elliptiques ayant au moins un premier de réduction multiplicative.

1. Certaines de ces informations sont tirées de [Ser02, p. 86] et de [RM09, p.210]. Les références précises des articles cités s'y trouvent.

Perspectives

Pour continuer l'étude des sujets abordés dans ce projet, on pourrait par exemple :

— Etudier certaines des avancées sur la conjecture de Sato-Tate citées dans le dernier chapitre.

— Etudier la conjecture de Lang-Trotter, qui prédit la densité des premiers pour lesquels la réduction d'une courbe E défninie sur $\mathbb{Q}$ non-CM est supersingulière. Plus précisèment, elle prétend que

$$|\{p < x \text{ de bonne réduction } : E_p/\mathbb{F}_p \text{ supersingulière }\}| \sim \frac{c_E\sqrt{x}}{\log x},$$

quand $x \to +\infty$ pour c_E une constante dépendant de E. Un théorème de Serre et Elkies montre que dans ce cas l'ensemble des premiers de réduction supersingulière a densité 0 : pour tout $\varepsilon > 0$,

$$|\{p < x \text{ de bonne réduction } : E_p/\mathbb{F}_p \text{ supersingulière }\}| \ll x^{3/4+\varepsilon}.$$

Elkies a toutefois montré que l'ensemble des premiers de réduction supersingulière est infini.

— Définir et étudier les fonctions L des courbes elliptiques (reliées à la conjecture de Birch et Swinnerton-Dyer et au théorème de modularité) et leurs relations avec des Grössencharakteren d'Hecke dans le cas CM.

— Etudier le prolongement et l'ordre des fonctions L d'Artin (théorèmes de Brauer et de Hecke), admis pour démontrer le théorème de Chebotarev.

— Continuer l'étude des courbes elliptiques sur les corps finis (par exemple étudier l'invariant de Hasse pour caractériser les courbes singulières d'une autre manière) ou l'étude de la réduction modulo un premier (théorème de Nagell, théorèmes de Deuring).

— Etudier la théorie de la ramification dans les extensions infinies.

— Etudier un théorème de Birch donnant la conjecture de Sato-Tate "à l'envers", c'est-à-dire que l'on fixe un premier et l'on étudie l'ensemble F_p des classes d'isomorphies des courbes elliptiques définies sur $\mathbb{F}_p$. Le théorème montre alors que pour tous $0 \leq \alpha < \beta \leq \pi$,

$$\lim_{p\to+\infty} \frac{|\{E \in F_p : \alpha \leq \theta_p(E) \leq \beta\}|}{|F_p|} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta d\theta.$$

Bibliographie

[Ahl79] Lars Ahlfors : *Complex analysis : an introduction to the theory of analytic functions of one complex variable.* McGraw-Hill, New York, 1979.

[Bou04] N. Bourbaki : *Integration 1 : Chapters 1-6.* Springer, 2004.

[Cox89] David Cox : *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Wiley, New York, 1989.

[Ful89] William Fulton : *Algebraic curves : an introduction to algebraic geometry.* Addison-Wesley Pub. Co., Advanced Book Program, 1989.

[Har77] Robin Hartshorne : *Algebraic geometry.* Springer-Verlag, New York, 1977.

[Hus04] Dale Husemöller : *Elliptic Curves.* Springer-Verlag, New York, deuxième édition, 2004.

[Kna69] S. Knapowski : On a theorem of Hecke. *Journal of Number Theory, vol. 1, no. 2, pp. 235-251*, 1:235–251, avril 1969.

[Kob82] Neal Koblitz : *Number theory related to Fermat's last theorem : proceedings of the conference.* Birkhäuser, Boston, 1982.

[Lan70] R.P. Langlands : Problems in the theory of automorphic forms. *In* C.T. Taam, éditeur : *Lectures in Modern Analysis and Applications III*, volume 170, pages 18–61. Springer, Berlin Heidelberg, 1970.

[Lan87] Serge Lang : *Elliptic functions.* Springer-Verlag, New York, 1987.

[Lan94] Serge Lang : *Algebraic number theory.* Springer-Verlag, New York, 1994.

[Lor96] Dino Lorenzini : *An invitation to arithmetic geometry.* Graduate studies in Mathematics. American Mathematical Society, 1996.

[Mil06] James S. Milne : *Elliptic curves.* BookSurge Publishers, United States, 2006.

[Neu99] Jürgen Neukirch : *Algebraic number theory.* Springer, Berlin, New York, 1999.

[RM09] Maruti Ram Murty : Problems in the theory of automorphic forms. *In* James Cogdell, éditeur : *Lectures on automorphic L-functions*, Lecture Notes in Mathematics, pages 205–281. American Mathematical Society, 2009.

[RMKM09] Maruti Ram Murty et Vijaya Kumar Murty : The Sato-Tate conjecture and generalizations. *Current Trends in Science Platinum Jubilee Special*, pages 639–646, 2009.

[Sam71] Pierre Samuel : *Théorie algébrique des nombres.* Hermann, Paris, 1971.

[Ser02] Jean-Pierre SERRE : *Harvard Lectures on Analytic Number Theory.* non-publiées, 2002.

[Ser72] Jean-Pierre SERRE : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1971/72.

[Sil86] Joseph SILVERMAN : *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1986.

[Sil94] Joseph SILVERMAN : *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.

[ST10] Joseph SILVERMAN et John TATE : *Rational points on elliptic curves.* Springer-Verlag, New York, 2010.

[Var07] Veeravalli S. VARADARAJAN : Groupes de lie (notes de cours). `http://www.math.ucla.edu/~vsv/liegroups2007/liegroups2007.html`, 2007.

[Was08] Lawrence WASHINGTON : *Elliptic curves : number theory and cryptography.* Chapman & Hall/CRC, Boca Raton, 2008.

Chapitre A

Compléments sur les courbes elliptiques

Dans cette annexe, nous donnons quelques compléments sur les courbes elliptiques (isogénies, isogénies duales, forme différentielle invariante), avant de déterminer le degré et la séparabilité des $\mathbb{Z}$-multiplications et des morphismes de Frobenius, complétant ainsi le texte principal.

1. Isogénies

Étant données deux courbes elliptiques, il est naturel de s'intéresser aux morphismes entre elles, en tant que *courbes projectives* ou en tant que *groupes abéliens*. En fait, il se trouve que ces deux types d'objets sont très liés : il suffit qu'un morphisme en tant que courbes projectives préserve l'élément neutre (point de base) pour que ce soit un homomorphisme.

1.1. Morphismes de courbes

Rappelons qu'un morphisme de courbes projectives planes $C_1, C_2 \subset \mathbb{P}^2$ est une application rationnelle $f : C_1 \to C_2$ définie en tout point de C_1, c'est-à-dire que

$$f = [f_0, \dots, f_n]$$

avec $f_i \in \overline{K}[X_0, \dots, X_n]$ des polynômes homogènes de même degré tels que

- $f_1, \dots, f_n$ n'appartiennent pas tous à $I(V_1)$.
- Pour tout $g \in I(V_2)$ on a $g(f_1(X), \dots, f_n(X)) \in I(V_1)$.
- Pour tout $P \in C_1$, $(f_1(P), \dots, f_n(P)) \neq 0$.

Par le résultat suivant, on peut en fait se passer de la dernière hypothèse si la première courbe est lisse.

Théorème A.1. *Si $C_1, C_2 \in \mathbb{P}^2$ sont des courbes projectives avec C_1 lisse, alors toute application rationnelle $f : C_1 \to C_2$ est un morphisme.*

Démonstration. Voir [Ful89, 7.1, Corollaire 1]. □

De plus, les morphismes de courbes projectives ont la particularité suivante :

Théorème A.2. *Un morphisme de courbes projectives $f : C_1 \to C_2$ est constant ou surjectif.*

Démonstration. Voir [Ful89, Problème 8.18]. □

1.2. Isogénies

Définition A.3. Une **isogénie** entre deux courbes elliptiques (E, O) et (E', O') est une application rationnelle

$$f : E \to E'$$

telle que $f(O) = O'$.

Remarque A.4. Par le théorème A.1, toute isogénie est un morphisme.

Théorème A.5. *Toute isogénie non-constante est un homomorphisme de groupes surjectif.*

Démonstration. La preuve est relativement facile si l'on utilise l'isomorphisme $E \to \mathrm{Pic}^0(E)$, voir [Sil86, III.4.8]. □

Définition A.6. On note l'anneau des isogénies entre deux courbes elliptiques E et E' par $\mathrm{Hom}(E, E')$. Le sous-groupe des éléments inversibles des **endomorphismes** $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ de E est noté $\mathrm{Aut}(E)$, le **groupe des automorphismes** de E.

Remarque A.7. Si les courbes elliptiques E, E' de la définition A.3 sont définies sur K, on peut s'intéresser aux isogénies $f \in \mathrm{Hom}(E, E')$ définies sur K. Dans ce cas, notons que si $\sigma \in \mathrm{Gal}(\overline{K}/K)$, alors pour tout $P \in E$,

$$f(\sigma(P)) = \sigma(f(P)).$$

Exemple A.8. Étant donnée une courbe elliptique (E, O), on peut définir pour tout $n \in \mathbb{Z}$ l'application $[n] : E \to E$ de multiplication par n définie de la manière suivante :

$$[n]P = \begin{cases} P + \cdots + P \ (n \text{ fois}) & \text{si } n > 0 \\ [-n](-P) & \text{si } n < 0 \\ O & \text{si } n = 0. \end{cases}$$

Il est clair que $[n] \in \mathrm{Hom}(E, E)$ pour tout $n \in \mathbb{Z}$ puisque les applications

$$+ : E \times E \to E \qquad - : E \to E$$

sont des morphismes et que $[n]O = O$. De plus, notons que pour tout $[n]$, on a une restriction $[n] : E(K) \to E(K)$. En effet, les applications $+$ et $-$ se restreignent également en des morphismes $+ : E(K) \times E(K) \to E(K)$ et $- : E(K) \to E(K)$. On étudiera plus en détails cette famille d'applications ci-dessous.

2. Formes différentielles

Pour C une courbe projective définie sur K, notons Ω_C le K-espace vectoriel des formes différentielles sur $\overline{K}(C)$ (voir [Ful89, 8.4] ou [Sil86, II.4] pour plus de détails).

Étant donné un morphisme non-constant $f : C_1 \to C_2$ de courbes projectives planes, l'application $f^* : \overline{K}(C_2) \to \overline{K}(C_1)$ induite par composition sur les corps de fonctions induit à son tour une application $f^* : \Omega_{C_2} \to \Omega_{C_1}$ définie par

$$f^*\left(\sum g_i dx_i\right) = \sum (f^* g_i) d(f^* x_i).$$

Au travers des formes différentielles, on obtient un critère très utile pour déterminer quand un morphisme de courbes est séparable :

Proposition A.9. *Soit C une courbe et $f : C_1 \to C_2$ un morphisme de courbes non-constant. Alors f est séparable si et seulement si $f^* : \Omega_{C_2} \to \Omega_{C_1}$ est non-nulle.*

Démonstration. Voir [Sil86, II.4.2]. □

2.1. La forme différentielle invariante

Pour toute courbe elliptique E sous la forme de Weierstrass $E : y^2 = x^3 + ax^2 + bx + c$, on peut considérer la forme différentielle $\omega = \frac{dx}{2y} \in \Omega_E$, appelée **forme différentielle invariante**. Ce nom vient du fait de son invariance par translation :

Proposition A.10. *Pour tout $P \in E$, on a $\tau_P^* \omega = \omega$, où $\tau_P : E \to E$ est la translation par C.*

Démonstration. Voir [Sil86, III.5.1]. □

La forme différentielle invariante possède également la remarquable propriété suivante :

Proposition A.11. *Soient E_1, E_2 des courbes elliptiques et $f, g : E_1 \to E_2$ des isogénies. Alors on a*

$$(f+g)^*\omega = f^*\omega + g^*\omega.$$

Démonstration. Voir [Sil86, III.5.2]. □

Par la proposition A.9, les formes différentielles sont un outil pratique pour déterminer quand un morphisme de courbes est séparable, puisque c'est le cas si et seulement si l'application induite sur l'espace des formes différentielles est non-nulle. Par sa compatibilité avec la loi de groupe sur les courbes elliptiques, la forme différentielles invariante est un bon candidat pour tester cette non-annulation.

3. Isogénies duales et degrés

La notion d'*isogénie duale* est un outil important, utile pour déterminer le degré de certaines isogénies, au vu de la relation qu'il existe entre les deux notions.

En utilisant [Sil86, proposition II.3.6], on voit qu'une isogénie $f : E_1 \to E_2$ induit un homomorphisme $f^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$ défini par

$$f^*(\overline{(Q)}) = \sum_{P \in f^{-1}(Q)} e_f(P)\overline{(P)}.$$

Par conséquent, on a un homomorphisme

$$E_2 \xrightarrow{\cong} \mathrm{Pic}^0(E_2) \xrightarrow{f^*} \mathrm{Pic}^0(E_1) \xrightarrow{\cong} E_1.$$

En fait, il se trouve que cet homomorphisme est une application rationnelle (voir [Sil86, III.6.1]), respectant les points de base, donc une isogénie, appelée *isogénie duale*. Il est de plus caractérisé par la propriété suivante, le reliant au degré de l'isogénie de départ.

Théorème A.12. *Si $f : E_1 \to E_2$ est une isogénie, alors il existe une unique isogénie $\hat{f} : E_2 \to E_1$ telle que $\hat{f} \circ f = [\deg f] \in \mathrm{End}(E_1)$, où $[-]$ dénote la $\mathbb{Z}$-multiplication.*

Démonstration. Voir [Sil86, III.6.1]. Il s'agit de se ramener aux cas particuliers d'un morphisme séparable ou du morphisme de Frobenius. Dans le premier cas, on montre (voir [Sil86, III.4.11]) en utilisant le théorème fondamental de la théorie de Galois appliqué à des extensions de corps de fonctions que si $f_1, f_2 : E_1 \to E_2$ sont des isogénies séparables telles que $\ker f_1 \subset \ker f_2$, alors il existe une unique isogénie $g : E_2 \to E_1$ telle que $f_2 = gf_1$. Par le théorème de Lagrange et la proposition 5.15, le résultat est alors immédiat. □

Les propriétés suivantes sont vérifiées :

Proposition A.13. *Si $f, g : E_1 \to E_2$ sont des isogénies, alors*

1. $\hat{f} \circ f = [\deg f] \in \mathrm{End}(E_1)$ *et* $f \circ \hat{f} = [\deg f] \in \mathrm{End}(E_2)$.
2. $\widehat{f \circ g} = \hat{g} \circ \hat{f}$ *et* $\widehat{f + g} = \hat{f} + \hat{g}$.
3. $\deg \hat{f} = \deg f$.
4. $\hat{\hat{f}} = f$.
5. *Pour tout $m \in \mathbb{Z}$,* $\widehat{[m]} = [m]$.

Démonstration. Voir [Sil86, III.6.2]. □

4. Degré et séparabilité de la multiplication

Pour étudier les propriétés de la multiplication, on commence par observer que l'action de la multiplication sur la forme différentielle invariante est très simple.

Lemme A.14. *Soit E une courbe elliptique et $\omega \in \Omega_E$ la forme différentielle invariante. Pour tout $m \in \mathbb{Z}$ non-nul, on a $[m]^*\omega = m\omega$.*

Démonstration. Le résultat est vérifié pour $m = 1$ puisque $[1] = \mathrm{id}_E$. De plus, par la proposition A.11, pour tout $m \geq 2$

$$[m]^*\omega = ([m-1] + [1])^*\omega = [m-1]^*\omega + \omega,$$

donc le résultat suit par récurrence pour $m \geq 2$. Pour $m < 0$, on procède de même. □

Intéressons-nous maintenant à la séparabilité de la multiplication.

Proposition A.15. *Soit (E, O) une courbe elliptique. Pour tout $m \in \mathbb{Z}$, la multiplication $[m] \in \mathrm{End}(E)$ est séparable.*

Démonstration. Par le lemme précédent, on voit que $[m]^*\omega \not\equiv O$, d'où $[m]$ est séparable par la proposition A.9. □

Proposition A.16. *Soit E une courbe elliptique. Pour tout $m \neq 0$, le morphisme $[m]$ de multiplication par m est non-constant.*

Démonstration. Par le lemme précédent, on voit directement que $[m] \neq 0$ (sinon on aurait que $[m]^*\omega = 0 \neq \omega$). □

Corollaire A.17. *Pour toute courbe elliptique E, l'application*

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathrm{Hom}(E,E) \\ m & \mapsto & [m] \end{array}$$

est un homomorphisme de groupes injectif.

Démonstration. Il est clair que l'application est un homomorphisme. De plus, si $[m] = 0$, alors la proposition A.16 implique que $m = 0$. □

Proposition A.18. *Soit (E,O) une courbe elliptique et $[m]$ la multiplication par $m \in \mathbb{Z}$. Alors* $\deg[m] = m^2$.

Démonstration. Par définition de l'isogénie duale, par le théorème A.12 et les points 1) et 5) de la proposition A.13,

$$[\deg[m]] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2],$$

donc $[\deg[m] - m^2] \equiv O$, ce qui implique que $\deg[m] = m^2$ par le corollaire A.17. □

5. Degré et séparabilité de l'endomorphisme de Frobenius

Soit K un corps parfait de caractéristique p et q une puissance de p. Considérons une courbe elliptique E définie sur K et le q-morphisme de Frobenius

$$\hat{\varphi} : E \to E^{(q)}$$

(voir exemple 5.2). On a une application induite $(\hat{\varphi})^* : K(E^{(q)}) \to K(E)$ entre les corps de fonctions.

Lemme A.19. *On a $(\hat{\varphi})^*(K(E^{(q)})) = \{f^q : f \in K(E)\} = K(E)^q$.*

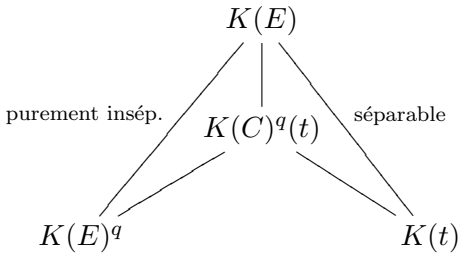
Démonstration. Pour $f \in K[E^{(q)}]$, on a $(\hat{\varphi})^*(f) = f(X^q, Y^q, Z^q)$. Comme on suppose K parfait, il existe $g \in K[C]$ tel que $\tilde{\varphi}(g) = f$, d'où $(\hat{\varphi})^*(f) = g(X,Y,Z)^q$. □

Lemme A.20. *Soit C une courbe projective définie sur un corps K et $P \in C(K)$ un point régulier. Si $t \in K(C)$ est un uniformisateur en P, alors $K(C)/K(t)$ est une extension finie et séparable.*

Démonstration. Voir [Sil86, II.1.4]. □

Proposition A.21. *Le degré du q-morphisme de Frobenius $\hat{\varphi}$ est q.*

Démonstration. Par le lemme A.19, il s'agit de calculer le degré de l'extension $K(E)/K(E)^q$. Soit $P \in E(K)$ un point quelconque et $t \in K(E)$ un uniformisateur en P. Par le lemme A.20, l'extension $K(E)/K(t)$ est finie et séparable, donc il en est de même pour $K(E)/K(E)^d(t)$.



Par définition, l'extension $K(E)/K(E)^q$ est purement inséparable, donc il en est de même pour $K(E)/K(E)^q(t)$. Cette extension est donc séparable et purement inséparable à la fois, d'où $K(E) = K(E)^d(t)$. Nous sommes donc réduits à calculer le degré de l'extension *simple*

$$K(E)^q(t)/K(E)^q.$$

Bien sûr, comme $t \in K(E)$, son polynôme minimal sur $K(E)^d$ divise $X^q - t^q \in K(E)^q[X]$. Comme l'extension est purement inséparable, ce polynôme minimal a la forme $X^{p^k} - a$ pour un certain $k \geq 1$ et $a \in K(E)^q$. Par conséquent, $t^{p^k} = f^q$ pour un certain $f \in K(E)$, d'où $p^k = \operatorname{ord}_P(t^{p^k}) = \operatorname{ord}_P f^q = q \operatorname{ord}_P(f)$, ce qui implique que $p^k = q$ puisque $\operatorname{ord}_P(f) \in \mathbb{Z}$, d'où le résultat. □

Remarque A.22. Ce résultat est encore valable pour des courbes quelconques sur un corps parfait, mais travailler sur une courbe elliptique permet de supposer sans autre l'existence d'un point rationnel (e.g. le point de base).

Finalement, on s'intéresse à la séparabilité de l'application $\mathrm{id} - \varphi$.

Proposition A.23. *Soit $E/\mathbb{F}_q$ une courbe elliptique, avec $\mathbb{F}_q$ un corps fini de caractéristique p. Si φ est le q-morphisme de Frobenius, alors l'application* $\mathrm{id} - \varphi$ *est séparable.*

Démonstration. A nouveau, on utilise la caractérisation de la séparabilité donnée par la proposition A.9 appliquée à la forme différentielle invariante ω, en profitant de la compatibilité de celle-ci avec la loi de groupe. Par la proposition A.11, on a en effet $(\mathrm{id} - \varphi)^*\omega = \mathrm{id}^*\,\omega - \varphi^*\omega = \omega - \varphi^*\omega$. Or

$$\varphi^*\omega = \varphi^*\left(\frac{dx}{2y}\right) = \frac{d(x^q)}{2y^q} = \frac{qx^{q-1}}{2y^q} = 0,$$

d'où $(\mathrm{id} - \varphi)^*\omega = \omega$. Ainsi, $(\mathrm{id} - \varphi)^*$ est non-nulle et la séparabilité suit de la proposition A.9. □