# La conjecture d'André-Oort pour le produit des courbes modulaires

**Ziyang GAO**

Directeur : Emmanuel ULLMO

Résumé. Dans cet article, on donne une preuve inconditiennelle de la conjecture d'André-Oort pour le produit des courbes modulaires d'après J.Pila. Ici la méthode principale est la théorie d'o-minimalité, une partie de la théorie de modèle, et nous suivons une strategie proposée par Zannier. En particulier, on montre le théorème d'Ax-Lindermann, qui est le coeur de l'article. La borne inférieure dans ce cas est un résultat de ceux classiques.

**Mots clés :** Ensemble définissable, point rationnel, Pila-Wilkie, la conjecture d'André-Oort

## Remerciements

Tout d'abord, je remercie sincèrement mon directeur de mémoire, Monsieur Emmanuel Ullmo, pour tout ce qu'il a apporté dans ma vie. Il m'a introduit ce sujet et il a passé beaucoup de temps ensemble avec moi pour discuter et partager ses connaissances et idées mathématiques. Il a aussi proposé un sujet de recherche avec ses expériences.

C'est grâce au programme Erasmus ALGANT que j'ai eu l'occasion de faire les études en europe et bénéficie de l'Université Paris-Sud et l'Université de Milan pour ses excellentes conditions. Je suis heureux de pourvoir exprimer ici ma gratitude à tous ceux qui y ont participé, surtout les professeurs dont j'ai reçu l'enseignement pendant les deux ans, y compris Jean-Benoît Bost, Elisabeth Bouscaren, David Harari et Yves Laszlo à Orsay, Daniel Bertrand à Paris 6, Huayi Chen à Paris 7, Luca Barbieri-Viale, Fabrizio Andreatta, Van Geemen et Paolo Stellari à Milan.

Je tiens particulièrement à remercier Monsieur Huayi Chen qui m'a aidé réaliser mon rêve d'étudier en europe, et Monsieur David Harari qui m'a aidé trouver le directeur de thèse.

# Table des matières

CHAPITRE 1

# Introduction

## 1. Description du problème

Dans cet article on va donner une preuve sans condition de la conjecture d'André-Oort pour le produit des courbes modulaires en utilisant la théorie d'o-minimalité.

Soit $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires, alors on définit pour le cas $X = \mathbb{C}^n$ :

**Définition 1.1.** (1) Un *point spécial* de $\mathbb{C}^n$ est un point $c = (c_1, ..., c_n)$ tel que toute $c_i$ est le $j$-invariant d'une courbe elliptique avec multiplication complexe. $\mathbb{C}^0$ est aussi considéré comme un point spécial.

(2) Une *sous-variété spéciale* de $\mathbb{C}^n$ est une composante irréductible d'un produit cartesien des produits fibrés des courbes modulaires et des points spéciaux. Explicitement, ça veut dire :

Soit $S_0 \sqcup S_1 \sqcup ... \sqcup S_w$ une partition de $\{1, ..., n\}$ avec $w \geqslant 0$ et $S_i$ non-vide si $i \neq 0$. Soient $j_i \in \mathbb{C}$ pour chaque $i \in S_0$ un point spécial, $s_i$ l'élément le plus petit de $S_i$ pour chaque $i \geqslant 1$ et $\Phi_{N_{ij}} \in \mathbb{Z}[X, Y]$ pour chaque $j \in S_i$, $j \neq s_i$ un polynôme modulaire. Une *sous-variété spéciale* de $\mathbb{C}^n$ est une sous-variété de la forme

$$T(S_i, j_i, \Phi_{N_{ij}}) := \{(c_1, ..., c_n) \in \mathbb{C}^n | c_i = j_i, i \in S_0, \Phi_{N_{ij}}(c_{s_i}, c_j) = 0, i = 1, ..., w, j \in S_i, j \neq s_i\}.$$

La dimension de $T(S_i, j_i, \Phi_{N_{ij}})$ est $w$.

(3) Si de plus $S_0 = \emptyset$, on appelle cette sous-variété spéciale *élémentaire*.

**Remarque 1.2.** La condition $\Phi_{N_{ij}}(c_{s_i}, c_j) = 0$ est équivalente à dire que $E_{s_i}$ *et* $E_j$ *se sont isogénieuse.*

Les définitions générales pour $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires arbitraires seront donées dans Chapitre 3, Définition (1.3).

Par définition, un point spécial est justement une sous-variété spéciale de dimension 0. Il est claire que dans une sous-variété spéciale de dimension strictement positive, il y a toujours un nombre infini des points spéciaux (l'ensemble des points spéciaux est même Zariski dense). Ainsi que si $V \subset X$ contient une sous-variété spéciale de dimension strictement positive, $V$ contient un nombre infini des points spéciaux.

La version faible de "André-Oort" est l'inverse de l'énoncé au dessus, c'est à dire :

*Si $V \subset X$ contient un nombre infini des points spéciaux, alors elle contient une sous-variété spéciale de dimension strictement positive.*

Mais pour nous, nous allons montrer la version forte, i.e.

**Théorème 1.3.** *Soit $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires. Si $V \subset X$ est une sous-variété, alors elle ne contient qu'un nombre fini des sous-variétés spéciales maximales.*

À priori, on ne demande pas que $V$ soit irréductible ou soit définie sur $\overline{\mathbb{Q}}$, mais on se ramène à ce cas immédiatement car tous les points spéciaux sont algébriques.

## 2. Structure de l'article

L'article est organisé comme ça :

- Dans Chapitre 2, on va introduire les notions et théorèmes élémentaires de la théorie d'o-minimalité. Tous les résultats seront énoncés sans preuve. En fin de ce chapitre, plusieurs versions de Pila-Wilkie (concernant la distribution des points rationnels et algébriques de degré borné d'un ensemble définissable de $\mathbb{R}^n$) seront énoncées et comparées. Pour nous, elles sont toutes utiles. Ceci nous donne une "borne supérieure" recherchée.
- D'ailleurs, Chapitre 4 nous donnera une "borne inférieure" en termes de la complexité. Cette partie est principalement classique, en combinant la théorie de multiplication complexe et la borne inférieure de Siegel pour le nombre des classes d'un ordre quadratique imaginaire.
- Chapitre 3, étant le coeur de l'article, consacre à montrer que les points spéciaux hors de toutes les sous-variétés spéciales de dimension strictement positive dont la hauteur ne dépasse pas $T$ sont essentiellement "transcendantaux". Ceci nous permet de combiner les deux bornes (dans Chapitre 5) et atteindre une incompatibilité sauf s'il y a un sous-ensemble semi-algébrique de dimension strictement positive dedans.
- Finalement on conclude dans Chapitre 5 après montrer un résultat dont on a besoin autour la possibilité des sous-variétés spéciales élémentaires qui admettent des "bonnes" tranlatés dans $V$.

## 3. Quelques développements récemment

Cette méthode a été généralisée au sens suivants : J.Pila et J.Tsimerman ont montré dans [**PT1**] la conjecture d'André-Oort pour $\mathcal{A}_2^r$, i.e. le produit des espaces modulaires pour les surfaces abéliennes principalement polarisées, et dans [**PT2**] l'Ax-Lindermann pour $\mathcal{A}_g^r$, i.e. le produit des espaces modulaires pour les variétés abéliennes principalement polarisées, qui permet de conclure la conjecture pour $g \leqslant 6$. D'ailleures, E.Ullmo et A.Yafaev ont montré l'Ax-Lindermann pour toutes les variétés de Shimura projectives dans [**UY**], et E.Ullmo a expliqué dans [**Ul**] comment en déduire la conclusion si l'on sait déjà l'Ax-Lindermann et une borne inférieure propre (pour les orbites de Galois).

CHAPITRE 2

# Préliminaire : structure o-minimale sur $(\mathbb{R}, +, \cdot)$

Dans ce chapitre, on va introduire les notions et théorèmes élémentaires de la théorie d'o-minimalité (on se restrient à $(\mathbb{R}, +, \cdot)$). Tous les résultats seront énoncés sans preuve.

## 1. Structures sur $(\mathbb{R}, +, \cdot)$

**Définition 1.1.** (1) Une *structure sur le corps réel* $(\mathbb{R}, +, \cdot)$ est une suite $\mathcal{S} = (\mathcal{S}_n, n \geqslant 1)$ où $\mathcal{S}_n$ est une collection des sous-ensembles de $\mathbb{R}^n$ telle que pour tous $n, m \geqslant 1$,
- $\mathcal{S}_n$ est une algèbre de Boole.
- $\mathcal{S}_n$ contient tous les ensembles semi-algébriques de $\mathbb{R}^n$.
- si $A \in \mathcal{S}_n$ et $B \in \mathcal{S}_m$, alors $A \times B \in \mathcal{S}_{n+m}$.
- si $m \geqslant n$ et $A \in \mathcal{S}_m$, alors $\pi(A) \in \mathcal{S}_n$ où $\pi : \mathbb{R}^m \to \mathbb{R}^n$ est la projection vers les premières $n$ coordonnées.

(2) Pour une structure $\mathcal{S}$ sur $(\mathbb{R}, +, \cdot)$, on dit qu'un ensemble $A \subset \mathbb{R}^n$ est *définissable* si $A \in \mathcal{S}_n$, et une application (pas forcéement continue) $f : A \to \mathbb{R}^n$ avec $A \subset \mathcal{S}^m$ est *définissable* si le graphe $\Gamma(f) \subset \mathbb{R}^{m+n}$ est un ensemble définissable.

**Remarque 1.2.** On contruit une structure sur $(\mathbb{R}, +, \cdot)$ souvent dans la façon suivante (par ajoutant des opérateurs élémentaires) :

On se donne deux structure $\mathcal{S} = (\mathcal{S}_n)$ et $\mathcal{S}' = (\mathcal{S}'_n)$ sur $(\mathbb{R}, +, \cdot)$, et on dit $\mathcal{S} \subset \mathcal{S}'$ si $\mathcal{S}_n \subset \mathcal{S}'_n$ pour tous $n \in \mathbb{N}$. Ceci munit l'ensemble de toutes les structures sur $(\mathbb{R}, +, \cdot)$ d'un ordre partiel. Soient $f_j : \mathbb{R}^{n(j)} \to \mathbb{R}$ (avec $j$ dans un ensemble d'indices $J$) quelques fonctions, on note $\mathcal{S}(\mathbb{R}, +, \cdot, (f_j)_{j \in J})$ la structure la plus petite sur $(\mathbb{R}, +, \cdot)$ contenant tous les graphes des fonctions $f_j$'s. On appelle cette structure *la structure sur* $(\mathbb{R}, +, \cdot)$ *engendrée par les* $f_j$*'s.*

**Exemple 1.3.** On va donner quelques exemples des structures sur $(\mathbb{R}, +, \cdot)$. La remarque précédente sera utile.

(1) Évidemment il y a une structure la plus grande sur $(\mathbb{R}, +, \cdot)$, notamment celle obtenue par mettant $\mathcal{S}_n$ la collection de tous les sous-ensembles de $\mathbb{R}^n$ pour tout $n \in \mathbb{N}$. C'est une structure triviale.

(2) Il y a aussi une structure la plus petite sur $(\mathbb{R}, +, \cdot)$, notamment la collection de tous les sous-ensembles semi-algébriques de $\mathbb{R}^n$ pour tout $n \in \mathbb{N}$. Ça nous donne une structure grâce au théorème de Tarski-Seidenberg (pour la condition de la projection, en cadre de l'élimination des quantifiers).

(3) $\mathbb{R}_{an} := \mathcal{S}(\mathbb{R}, +, \cdot, (f))$ où $f$ se varie dans toutes les *fonctions analytiques restreintes*, c'est à dire les fonctions $\mathbb{R}^n \to \mathbb{R}$ ($n \in \mathbb{N}$) qui s'annulent hors de $[-1, 1]^n$ et dont les restrictions à $[-1, 1]^n$ sont analytiques. $\mathbb{R}_{an}$ est une structure d'après

le théorème de Gabrielov (pour ce qui bien connait la théorie de modèle, $\mathbb{R}_{an}$ est libre des quantifiers dans le langage $\mathcal{L}_{an}^{D}$ où $D(x, y) = x/y$ si $0 < |x| < |y|$ et 0 sinon).

(4) $\mathbb{R}_{\exp} := \mathcal{S}(\mathbb{R}, +, \cdot, \exp)$ est aussi une structure d'après Wilkie.

(5) $\mathbb{R}_{an,\exp} := \mathcal{S}(\mathbb{R}, +, \cdot, (f), \exp)$ qui est engendrée par $\mathbb{R}_{an}$ et $\mathbb{R}_{\exp}$ est aussi une structure. Elle contient l'ensemble $\Gamma(\exp)$ qui n'est pas définissable dans $\mathbb{R}_{an}$, et elle contient aussi l'ensemble globalement sous-analytique $\{(x, y) \in \mathbb{R}^2 | y = \sin(x),\ x \in [-1, 1]\}$ qui n'est pas définissable dans $\mathbb{R}_{\exp}$.

**Définition 1.4.** Une structure $\mathcal{S}$ sur $(\mathbb{R}, +, \cdot)$ est *o-minimale* si la borne d'un ensemble arbitraire dans $\mathcal{S}_1$ est finie.

**Proposition 1.5.** *Toutes les structures (et surtout $\mathbb{R}_{an,\exp}$) introduites avant sauf la première sont o-minimales.*

## 2. Points réguliers d'un ensemble définissable

À partir de cette section, on se concentre toujours sur des structures o-minimales.

Tout d'abord, on introduit la notion d'une *famille des ensembles définissables*, c'est à dire un ensembles définissalbe $Z$ dans $\mathbb{R}^n \times \mathbb{R}^m$ considéré comme la famille des fibres

$$Z_y = \{x \in \mathbb{R}^n | (x, y) \in Z\}, \quad y \in \mathbb{R}^m.$$

Pour une famille des ensembles définissables, $Y := \{y \in \mathbb{R}^m | Z_y \neq \emptyset\}$ est définissable car il est l'image de $Z$ sous la projection $\mathbb{R}^{n+m} \to \mathbb{R}^m$.

**Définition 2.1.**

(1) Pour un ensemble définissable $Z$ et un couple $\kappa, p \in \mathbb{N}$, on défini *l'ensemble des points p-réguliers de $Z$ de dimension $\kappa$*, noté par $\mathrm{Reg}_{\kappa}^{p}(Z)$, comme l'ensemble de $x \in Z$ tel qu'il existe un voisinage ouvert $U$ de $x$ avec $U \cap Z$ une sous-variété de dimension $\kappa$ qui est un $C^p$-plongement dans $\mathbb{R}^n$.

(2) Un *point réguler de dimension $\kappa$* est un point 1-régulier de dimension $\kappa$.

(3) Pour un ensemble définissable $Z$, $\dim(Z)$ est la grande $\kappa$ telle que $Z$ possède un point régulier de dimension $\kappa$.

La fonction de dimension se comporte bien au sens de :

**Propriété 2.2.** *Si $Z$ est un ensemble définissable, alors $\mathrm{Reg}_{\kappa}^{p}(Z)$ l'est aussi pour n'importe quels $\kappa, p \in \mathbb{N}$, d'où la fonction $Z \mapsto \dim(Z)$ est définissable.*

En effet, la propriété reste vrai aussi sur une famille, i.e.

**Propriété 2.3.** *Pour une famille définissable $Z$, l'ensemble*

$$\{z = (x, y) \in Z | x \in \mathrm{Reg}_{\kappa}^{p}(Z_y)\}$$

*est aussi définissable.*

Après, on va introduire la notion de *bloque* pour finalement énoncer le théorème de Pila-Wilkie de l'estimation (forte) du nombre des points rationnels (et algébriques) d'un ensemble définissable. En fait, "bloque" est une généralisation de l'ensemble semi-algébrique.

**Définition 2.4.** (1) Un *bloque (définissable)* de dimension $w$ et de degré $d$ dans $\mathbb{R}^n$ est un ensemble connexe $W \subset \mathbb{R}^n$ de dimension $w$, régulier en tous les points, tel qu'il y a un ensemble semi-algébrique $A \subset \mathbb{R}^n$ de dimension $w$ et de degré $\leqslant d$, régulier en tous les points, et $W \subset A$.

(2) Une *famille des bloques (définissables)* de dimension $w$ et de degré $d$ est une famille définissalbe $W \subset \mathbb{R}^n \times \mathbb{R}^m$ telle que toutes les fibres non-vides $W_y$, $y \in \mathbb{R}^m$ est un bloque de dimension $w$ et de degré $\leqslant d$.

**Remarque 2.5.** Un peu de discussion sur les bloques.

(1) En dimension 0, un point est toujours un bloque.

(2) En dimension strictement positive, pour un bloque, à priori, tous ses points sont réguliers. En chaque point, on peut trouver un petit voisinage tel que l'intersection de ce voisinage et ce bloque est semi-algébrique de dimension strictement positive. Du coup un bloque est un union (peut-être infini) des ensembles semi-algébriques de dimension strictement positive connexes. Donc on peut voir que la notion du bloque est vraiment une généralisation de celle de l'ensemble algébrique !

## 3. Pila-Wilkie : points rationnels (et algébriques) d'un ensemble définissable

Dans cette section, on va donner les résultats de Pila-Wilkie sur l'estimation (forte) du nombre des points rationnels (et algébriques) d'un ensemble définissable. Il y a plusieurs versions, qui sont plus de plus précisées. Rugueusement, le théorème nous dit que :

*Si $Z \subset \mathbb{R}^n$ est définissable (dans une structure o-minimale), alors $Z$ ne contient qu'un peu de points rationnels (ou algébriques de degré borné) de hauteur $\leqslant T$ (à quelque sens) quand $T \to \infty$, sauf si $Z$ contient un sous-ensemble semi-algébrique de dimension strictement positive.*

Pour le préciser, on se donne la notion de la partie algébrique d'un ensemble définissable :

**Définition 3.1.** (1) Soit $Z \subset \mathbb{R}^n$ est définissable, alors la *partie algébrique* de $Z$ qui est notée $Z^{alg}$, est l'union de tous les sous-ensembles semi-algébriques de dimension strictement positive connexes de $Z$.

(2) Une application est dit *semi-algébrique* si elle est définissable dans la structure des ensembles semi-algébriques, i.e. une application $f : B \to \mathbb{R}^m$ où $B \subset \mathbb{R}^n$ est semi-algébrique telle que $\Gamma(f) \subset \mathbb{R}^{n+m}$ est semi-algébrque.

On fixe quelques notations. Pour un ensemble $Z \subset \mathbb{R}^n$, un intègre $k \geqslant 1$ et un nombre réel $T \geqslant 1$, mettons

$$Z(k,T) := \{z = (z_1, ..., z_n) \in Z | \max_i [\mathbb{Q}(z_i) : \mathbb{Q}] \leqslant k, \ \max_i H(z_i) \leqslant T\}$$

et

$$N_k(Z,T) := \#Z(k,T).$$

Maintenant, on peut préciser le paragraphe italique :

**Théorème 3.2.** *(Pila-Wilkie, la première version) Soient $Z \subset \mathbb{R}^n$ définissable, $k \geqslant 1$ et $\varepsilon > 0$, alors il existe une constante $c(Z,k,\varepsilon)$ telle que pour tout $T \geqslant 1$,*

$$N_k(Z - Z^{alg}, T) \geqslant c(Z,k,\varepsilon)T^{\varepsilon}.$$

La preuve du théorème commence en montrant que les points dans la question résident dans $O_{Z,\varepsilon}(T^\varepsilon)$ hypersurfaces de degré $d(\varepsilon)$, en suite elle marche par récurrence de la dimension de $Z$. Ceci nous dirige à faire une estimation de la même forme comme avant pour les intersections des hypersurfaces, et en même temps avec une constante uniforme pour toutes les intersections de $Z$ avec des hypersurfaces de degré fixé, i.e. un résultat pour une famille définissable.

**Théorème 3.3.** *(Pila-Wilkie, la deuxième version) Soient $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable, $k \geqslant 1$ et $\varepsilon > 0$, alors il existe une constante $c(Z, k, \varepsilon)$ telle que pour chaque fibre $X = Z_y$ de $Z$, on a*

$$N_k(X - X^{alg}, T) \geqslant c(Z, k, \varepsilon)T^\varepsilon.$$

Pour nous, ça ne suffit pas. Nous avons besoin de renforcer encore.

**Théorème 3.4.** *(Pila-Wilkie, la troisième version) Soient $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable, $k \geqslant 1$ et $\varepsilon > 0$, alors il existe une famille définissable $W = W(Z, \varepsilon)$ avec la propriété suivante : Si $X = Z_y$ est une fibre, alors mettons $X_\varepsilon := W_y$, et on a $X_\varepsilon \subset X^{alg}$ et il existe une constante $c(Z, k, \varepsilon)$ telle que*

$$N_k(X - X_\varepsilon, T) \geqslant c(Z, k, \varepsilon)T^\varepsilon.$$

Finalement, on a la version la plus forte :

**Théorème 3.5.** *(Pila-Wilkie, la dernière version) Soient $Z \subset \mathbb{R}^n \times \mathbb{R}^m$ une famille définissable, $k \geqslant 1$ et $\varepsilon > 0$. Alors il existe un nombre fini $J = J(Z, k, \varepsilon)$ des familles de bloque*

$$W^j \subset \mathbb{R}^n \times (\mathbb{R}^m \times \mathbb{R}^l), \qquad j = 1, ..., J,$$

*de dimension $w_j$ et de degré $d_j$, et une constante $c(Z, k, \varepsilon)$ telles que :*

- *Pour tout $j$ et $(y, \eta) \in \mathbb{R}^m \times \mathbb{R}^l$,*

$$W^j_{(y,\eta)} \subset Z_y.$$

- *Pour tout $y \in \mathbb{R}^m$ et $T \geqslant 1$, $Z_y(k, T)$ est continu dans l'union de au plus*

$$c(Z, k, \varepsilon)T^\varepsilon$$

*bloques définissables de la forme $W^j_{(y,\eta)}$ pour certain $j = 1, ..., J$ et $\eta \in \mathbb{R}^l$.*

**Remarque 3.6.** On voit sans beaucoup de difficulté que la dernière version de Pila-Wilkie implique la troisième : on prend $W = W(Z, \varepsilon)$ comme la fammile dont la fibre en $y$ est l'union de toutes les fibres de $W_j$ en $y$ sur tous $j$ avec $w_j > 0$.

**Exemple 3.7.** On se donnera les exemples suivants expliquant pourquoi les théorèmes de Pila-Wilkie au dessus deviennent vraiment plus en plus fort :

(1) Soit $X = \{(x, y, z) \in \mathbb{R}^3 | 2 < x, y < 3, z = x^y\}$. Alors $X^{alg}$ consiste en un union des segments des courbes algébriques : pour chaque $q \in \mathbb{Q}$ tel que $2 < q < 3$, prenons $y = q$, $z = x^q$. Donc $(X - X^{alg})(\mathbb{Q})$ est vide, donc la première version de Pila-Wilkie est triviale en ce cas. Cependant, $X^{alg}$ n'est pas définissable dans $\mathbb{R}_{an,\exp}$ (en fait dans n'importe quelle structure o-minimale) car elle possède un nombre infini des composantes connexes (un ensemble définissable consiste en seulement un nombre fini de composantes connexes). Donc La troisième version

fait une estimation non-triviale en enlevant un sous-ensemble définissable $X_\varepsilon$ de $X^{alg}$ (dépendant de $\varepsilon$) qui consiste en un nombre fini des segments des courbes.

(2) Soit $X = \{(x, y, z) \in \mathbb{R}^3 | 2 < x, y < 3, z = 2^{x+y}\}$. Alors tous les points se trouvent dans un segment d'une droite $z = 2^c$, $x + y = c$ qui est contenue dans $X$, et ainsi $X^{alg} = X$. Donc toutes les premières trois versions de Pila-Wilkie peuvent s'appliquer trivialement à ce cas. Mais pour obtenir une borne de la forme $O(T^\varepsilon)$, il faut justement enlever les $\log T = O(T^\varepsilon)$ segments tels que $c \in \mathbb{Z}$, $0 \leqslant c \leqslant \log T / \log 2$. Donc la troisième version peut aussi s'appliquer non-trivialement.

(3) Soit $X = \{(x, y) \in \mathbb{R}^2 | 0 < x < 1, 0 < y < e^x\}$. Ici chaque point $(x, y) \in X$ se trouve dans un petit disque ouvert contenu dans $X$. Le disque est semi-algébrique et contient $>> T^4$ points rationnels dont la hauteur est bornée par $T$. Du coup $X^{alg} = X$, et $X^{alg}$ est donc définissable. Dans ce cas, on ne peut pas atteindre une borne du type $O(T^\varepsilon)$ si on n'enlève pas essentiellement $X$ entier. Donc toutes les première trois versions de Pila-Wilkie s'appliquent trivialement à ce cas. Au contraire, bien que $X$ ne soit pas semi-algébrique (car les courbes à sa borne n'en soient pas), $X$ est bien un bloque. Donc on peut utiliser la dernière version de Pila-Wilkie pour obtenir une estimation non-triviale de $X$.

CHAPITRE 3

# Ax-Lindemann-Weierstrass

**Dorénavant, "définissable" veut dire toujours "définissable dans $\mathbb{R}_{an,\exp}$" !**

C'est la partie de coeur de cet article. Dans ce chapitre, on travaillera sur un revêtement (standard) $U$ de $X$. On applique le résultat Pila-Wilkie pour obtenir une borne supérieure du nombre des certains points "pré-spéciaux" dont la hauteur est bornée par un nombre.

## 1. Revêtement de $X$

Soit $X$ une courbe modulaire $\Gamma\backslash\mathbb{H}$, alors on prend :
- $U = \mathbb{H}$ ;
- le groupe (algébrique) $G = SL_2(\mathbb{R})$ agissant sur $\mathbb{H}$ par transformation linéaire ;
- le groupe $\Gamma < G(\mathbb{Z})$ ;
- $\pi : U \to X$ le morphisme standard (c'est un plongement du quotient comme une courbe quasiprojective donnée par un bon choix des fonctions modulaires pour $\Gamma$, par exemple, $\pi = j$ est la $j$-fonction si $X = \mathbb{C}$), qui est invariant sous l'action de $\Gamma$ ;
- le domaine fondamental $\mathbb{F}$ qui est un union fini des $SL_2(\mathbb{Z})$-translatés du domaine fondamental standard pour le groupe modulaire $SL_2(\mathbb{Z})$ ;
- les coordonées réelles sur $U = \mathbb{H} \subset \mathbb{C}$ en utilisant les parties réelle et imaginaire.

Et pour le produit des courbes modulaires, on prend simplement les produits.

**Définition 1.1.** Soit $n \geqslant 0$,

(1) Un point $(u_1, v_1, ..., u_n, v_n) \in U = \mathbb{H}^n$ est *pré-spécial* si tout $\tau_i = u_i + \sqrt{-1}v_i \in \mathbb{H}$ est quadratique.

(2) Soit $S_0 \sqcup S_1 \sqcup ... \sqcup S_w$ une partition de $\{1, ..., n\}$ avec $w \geqslant 0$ et $S_i$ non-vide si $i \neq 0$. Soient $h_i \in \mathbb{H}$ pour chaque $i \in S_0$ un point quelconque, $s_i$ l'élément le plus petit de $S_i$ pour chaque $i \geqslant 1$ et $g_{ij} \in GL_2(\mathbb{Q})^+$ pour chaque $j \in S_i$, $j \neq s_i$. Une *sous-variété quasi-pré-spéciale* de $\mathbb{H}^n$ est une sous-variété de la forme

$$N(S_i, h_i, g_{ij}) := \{(\tau_1, ..., \tau_n) \in \mathbb{H}^n | \tau_i = h_i, i \in S_0, \tau_j = g_{ij}(\tau_{s_i}), i = 1, ..., w, j \in S_i, j \neq s_i\}.$$

(3) Si $h_i$ sont tous quadratiques, on appelle une telle sous-variété *pré-spéciale*.

(4) Si $S_0 = \emptyset$ au dessus, on appelle une telle sous-variété pré-spéciale *élémentaire*.

**Remarque 1.2.** (1) En vue du revêtement de $X = \mathbb{C}^n$, il est claire par définition qu'un point (resp. une sous-variété) est pré-spécial(e) si et seulement s'il est l'image réciproque d'un point (resp. une sous-variété) spécial(e). Ceci nous permet de définir des sous-variétés spéciales de $X = Y_1 \times ... \times Y_n$ pour $X$ un produit des courbes modulaires arbitraires.

(2) Une sous-variété pré-spéciale est un produit d'un point arbitraire dans $\mathbb{H}^m (m \geqslant 0)$ et une sous-variété pré-spéciale élémentaire, et une sous-variété spéciale est un

produit d'un point pré-spécial dans $\mathbb{H}^m (m \geqslant 0)$ et une sous-variété pré-spéciale élémentaire.

**Définition 1.3.** Soit $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires (arbitraires), alors une *sous-variété* de $X$ est l'image sous $\pi : U \to X$ d'une sous-variété pré-spéciale de $U$. En particuler, un point spécial est l'image d'un point pré-spécial.

Un résultat important est le suivant (qui nous permet d'utiliser o-minimalité en cadre de ce revêtement) :

**Propriété 1.4.** *Soit $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires, alors la restriction de $\pi$ en $\mathbb{F}$ est définissable dans $\mathbb{R}_{an,exp}$.*

Démonstration. Pour $X = \mathbb{C}$, la définissabilité de $j$ sur $\mathbb{F}_{\mathbb{C}}$ est claire par la $q$-expansion (car la partie réelle est bornée uniformement sur $\mathbb{F}_{\mathbb{C}}$ et $|j(z)| \to \infty$ quand $z \to \sqrt{-1}\infty$), donc elle est définissable sur n'importe quel domaine fondamental $g\mathbb{F}_{\mathbb{C}} (g \in SL_2(\mathbb{Z}))$ et ainsi sur un union fini des tels domaines.

Maintenant pour une courbe modulaire $X = \Gamma\backslash\mathbb{H}$, comme $j$ est définissable sur le domaine fondamental, $\pi$ en est aussi car c'est une fonction algébrique de $j$. □

## 2. Composantes algébriques complexes

Dans les sections suivantes, on va travailler sur $U$ au lieu de $X$, donc il est natural de considérer

$$\mathcal{Z} := \pi^{-1}(V) \subset U$$

au lieu de $V$ soi-même. Et en analysant $\mathcal{Z}^{alg}$, on considère les ensembles algébriques complexes plutôt que ceux semi-algébriques réels grâce à une sorte de "rigidité" des composantes complexes maximales. On utilisera la continuation analytique pleusieures fois :

**Proposition 2.1.** *Si un ensemble analytique contient un sous-ensemble avec un point adhérent d'une composante d'une variété analytique, alors cet ensemble contient toute cette composante.*

**Définition 2.2.** Avec les notations comme avant, définissons *une composante complexe* de $\mathcal{Z}$ comme une composante connexe $Y$ de dimension strictement positive de $W \cap U$ avec $Y \subset \mathcal{Z}$ où $W$ est un ensemble algébrique complexe fermé irréductible de $\mathbb{C}^n$. La *partie algébrique complexe* de $\mathcal{Z}$, notée comme $\mathcal{Z}^{ca}$, est l'union des telles composantes de $\mathcal{Z}$.

**Remarque 2.3.** En fait, dans la définition, $Y \subset \mathcal{Z}$ est équivalent à

$$Y \cap \mathcal{Z} \quad \text{contient un sous-ensemble ouvert}$$

grâce à Proposition (2.1).

$\mathcal{Z}^{ca}$ peut bien servir comme on a :

**Proposition 2.4.** *Dans ce cadre, $\mathcal{Z}^{alg} = \mathcal{Z}^{ca}$.*

Démonstration. Notons $(x_1, ..., x_{2n})$ les coordonnées réelles sur $U$, et $(z_1, ..., z_n)$ celles complexes. Supposons que $\mathcal{Z} \subset \mathbb{R}^{2n}$ contient un arc d'une courbe algébrique réelle irréductible $C$. Soit $P$ est un point lisse de cet arc, qui peut être supposé comme l'origine de $\mathbb{R}^{2n}$ sans perte du généralité. Alors $t = x_1$, disons, est une uniformisante en $P$, et les

fonctions $x_i$ sur $C$ sont algébriques sur $\mathbb{R}(t) \subset \mathbb{C}(t)$. Les fonctions $z_j$ sur $C$ sont alors algébrique sur $\mathbb{C}(t)$. Supposons $z_j$ est non-constante sur cet arc (il existe une telle $z_j$ car sinon l'arc se réduit à un point). Alors toutes les fonctions $z_i$ sont algébrique sur $\mathbb{C}(z_j)$. Maintenant les fonction $z_i(t)$ sont réellement analytiques dans un voisinage réel de $t = 0$ et donc elles sont complexement analytiques dans un voisinage complexe de $t = 0$. L'image de $t \mapsto (z_1(t), ..., z_n(t))$ dans ce voisinage est un voisinage de $P$ dans une courbe algébrique complexe $\mathcal{C}$. Donc $\mathcal{C}$ contient $C$ dans un voisinage de $P$, et donc une composante $\mathcal{C}'$ de $\mathcal{C}$ contient $C$ dans ce voisinage. Alors $\mathcal{C}' \subset \mathcal{Z}$ car $C \subset \mathcal{Z}$ (Proposition (2.1)).

Comme tous les ensembles semi-algébriques connexes de dimenstion strictement positive peuvent être couvert par des arcs lisses des courbes semi-algébriques irréductibles sauf un nombre fini des points, on peut bien conclure que $\mathcal{Z}^{alg} \subset \mathcal{Z}^{ca}$ (les points exceptionnels sont dans l'adhérence des arcs). L'autre inclusion est claire. □

Cette proposition permet d'étudier les composantes complexes pour comprendre $\mathcal{Z}^{alg}$. Et voici pourquoi elles sont meilleures.

**Proposition 2.5.** *Soit $g : (-1, 1) \to G$ une application semi-algébrique qui est régulière (analytique) pour $t \in (-1, 1)$. Si $g(t)Y \subset \mathcal{Z}$ pour tout $t \in (-1, 1)$ et $g(0)Y$ est une composante complexe maximale (i.e. qui n'est pas contenue dans une composante complexe de dimension plus grande)de $\mathcal{Z}$, alors $g(t)Y = Y$ pour tout $t \in (-1, 1)$.*

Démonstration. Sinon, il existe un point $P \in Y$ tel que $g(t)P \notin g(0)Y$ pour certain $t \in (-1, 1)$. L'application $t \mapsto g(t)P \in U$ s'étend en une application complexe algébrique sur un voisinage complexe de 0, et $g(t)P \in \mathcal{Z}$ pour tel $t$ car $\mathcal{Z}$ est analytique. Par ce qu'on a discuté avant et analyticité, $g(t)P \in g(0)Y$ pour seulement un nombre fini de $t$ dans un voisinage complexe de 0. On prend un voisinage $I$ de 0 tel que $t = 0$ est le seul point satisfaisant $g(t)P \in g(0)Y$. Alors il existe un voisinage $D$ de $P$ tel que $\forall Q \in D \cap Y$ et $t \in I$, $g(t)Q \notin g(0)Y$. L'union de $g(t)(D \cap Y)$ contient un ensemble algébrique complexe de dimension $\dim Y + 1$ dans $\mathcal{Z}$. Par Proposition (2.1), on trouve une composante complexe de dimension $\dim Y + 1$ contenant $Y$ dans $\mathcal{Z}$. □

## 3. Intricacie

**Définition 3.1.** Soit $X$ un produit des courbes modulaires, $\mathbb{F}$ le domaine fondamental pour l'action de $\Gamma$ sur $U$ et $u \in U$. Définissons la $\Gamma$-intricacie de $u$ par rapport à $\mathbb{F}$, notée comme $I^X_{\mathbb{F}}(u)$, par

$$I^X_{\mathbb{F}}(u) := H(g)$$

où $g \in \Gamma$ est l'élément unique tel que $g(u) \in \mathbb{F}$.

**Lemme 3.2.** *Soient $X = \mathbb{C}$, $\mathbb{F} = \mathbb{F}_{\mathbb{C}}$ et $\mathbb{D}$ un domaine fondamental quelconque de la forme $g\mathbb{F}$ pour un $g \in \Gamma$. Soit $\tau \in \mathbb{H}$. Alors il existe un polynôme bivarial $P = P_{\mathbb{D}}$ avec les coefficients positifs tel que*

$$I_{\mathbb{D}}(\tau) << P(|\tau|, \frac{1}{Im(\tau)}).$$

Démonstration. Il suffit de montrer pour $\mathbb{D} = \mathbb{F}$ car la différence entre les cas générals et ce cas spécial est une constante (dépendant de $g$). Pour $\mathbb{D} = \mathbb{F}$, on a

$$\mathrm{Im}(g\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$$

pour $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. $\mathrm{Im}(gz)$ admet un maximum quand $g$ varie sur $\Gamma$, et il est atteint par un $g$ tel que

- soit $c = 0$, $d = \pm 1$ ;
- soit $c = \pm 1$, $d = 0$ ;
- soit

$$|c| \leqslant \frac{1}{\mathrm{Im}(\tau)}$$

et

$$|d| \leqslant |c||\mathrm{Re}(\tau)| << \frac{|\tau|}{\mathrm{Im}(\tau)}.$$

Alors on peut choisir

$$|b| \leqslant |d| << \frac{|\tau|}{\mathrm{Im}(\tau)}$$

et

$$|a| = |\frac{bc+1}{d}| \leqslant |bc+1| \leqslant |c||d| << \frac{|\tau|}{\mathrm{Im}(\tau)^2}.$$

Les premiers deux cas sont facile à verifier. Pour le dernier, choisissons $h = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ tel que $-\frac{1}{2} < \mathrm{Re}(hg\tau) \leqslant \frac{1}{2}$. Alors $hg\tau \in \mathbb{F}$, ainsi que

$$I_{\mathbb{F}}(\tau) = H(hg).$$

Mais

$$|n| \leqslant |g\tau| + 1 \leqslant \frac{|a\tau + b|}{|c||\tau + d/c|} + 1 << \frac{|\tau|(|\tau| + 1)}{\mathrm{Im}(\tau)^3},$$

donc $H(hg)$ est bornée comme on veut. □

**Proposition 3.3.** *Soit $X = \Gamma\backslash\mathbb{H}$. Supposons que*

- *$\phi$ est une fonction algébrique sur $\mathbb{C}$, à valeur réelle sur $\mathbb{R}$ ;*
- *$P \in \mathbb{R}$ et $B$ un disque ouvert centré en $P$ ;*
- *$\overline{B}$ est à distance strictement positive des composantes de $\{\tau \in \mathbb{C} | \phi(\tau) \in \mathbb{R}\}$ d'autres que $\mathbb{R}$ et des pôles de $\phi$ ;*
- *$\phi(B \cap \mathbb{H}) \subset \mathbb{H}$ ;*
- *$\mathbb{D}$ est un domaine fondamental pour $\Gamma$ qui est une translaté de $\mathbb{F}$ par un élément de $\Gamma$ ;*
- *$\tau \in B$.*

*Si $g \in \Gamma$ est tel que $g\tau \in B$, alors*

$$I_{\mathbb{D}}(\phi(g\tau)) << H(g)^c,$$

*où $c = c(X, B, \tau, \phi)$.*

DÉMONSTRATION. Il suffit de montrer pour $X = \mathbb{C}$ et $\mathbb{D} = \mathbb{F} = \mathbb{F}_{\mathbb{C}}$ comme le lemme. On a déjà

$$I_{\mathbb{F}}(\phi(g\tau)) << P_{\mathbb{F}}(|\phi(g\tau)|, \frac{1}{\mathrm{Im}(\phi(g\tau))}).$$

Comme $B$ est à distance strictement positive des pôles de $\phi$, $\phi$ est bornée sur $B$, et donc $\phi(g\tau)$ est borné par une constante (dépendante de $B$ et de $\phi$). Comme $\overline{B}$ est à distance strictement positive des composantes de $\{\tau \in \mathbb{C} | \phi(\tau) \in \mathbb{R}\}$ d'autres que $\mathbb{R}$,

$$Z(\mathrm{Im}(\phi(z))) \cap \overline{B} \subset Z(\mathrm{Im}(z)) \cap \overline{B}$$

où $Z(f)$ est l'ensemble des zéros de $f$. Comme $Z(\mathrm{Im}(\phi(z)))$ et $Z(\mathrm{Im}(z))$ sont tous semi-algébriques, on a

$$\mathrm{Im}(\phi(z)) \geqslant C(\mathrm{Im}(z))^c$$

pour $z \in \overline{B}$ où $C = C(B, \phi)$, $c = c(B, \phi)$ sont constantes.

Maintenant, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a

$$\frac{1}{\mathrm{Im}(\phi(g\tau))} \leqslant \frac{1}{C}(\frac{|c\tau + d|}{\mathrm{Im}(\tau)})^c << H(g)^c.$$

Ceci permet de conclure (avec un différent $c$ de celui dans l'énoncé). □

## 4. Ax-Lindermann

Cette section est consacrée à montrer :

**Théorème 4.1.** *Pour $X$ un produit des courbes modulaires, soit $Y \subset \mathcal{Z}$ est une composante complexe maximale, alors $Y$ est quasi-pré-spéciale.*

DÉMONSTRATION. On prend $U = \mathbb{H}^n$, $G = SL_2(\mathbb{R})^n$ et $\Gamma = SL_2(\mathbb{Z})^n$ comme avant. La preuve sera divisée en quelques étapes.

***Choix du domaine fondamental***

Prenons les coordonnées $(\tau_1, ..., \tau_n)$ pour $\mathbb{H}^n$. Supposons que $Y$ est de dimension $w$, alors on peut choisir $w$ variables

$$\tau_{f,1}, ..., \tau_{f,w}$$

à paramèteriser $Y$ localement dans un ouvert par les fonctions algébriques

$$\tau_{d,a} = \phi_a(\tau_{f,i}).$$

Les fonctions peuvent se voir comme des fonctions définies sur $\mathbb{H}^w$. Comme $Y$ est analytique, les fonctions $\phi_a$ peuvent s'étendre en des fonctions algébriques sur $U' \subset \mathbb{H}^w$ (peut-être avec des ramifications), où $U'$ est borné par

$$L_{f,i} = \{(\tau_{f,i}) \in \mathbb{H}^w | \mathrm{Im}(\tau_{f,i}) = 0\}$$

et

$$L_{d,a} = \{(\tau_{f,i}) \in \mathbb{H}^w | \mathrm{Im}(\tau_{d,a}) = 0, \text{ i.e. } \mathrm{Im}(\phi_a(\tau_{f,i})) = 0\}.$$

On va classifier les variables dépendantes en deux groupes : celles telles que $L_{f,1} \subset L_{d,a}$, qui seront notées comme $\tau_{d,\alpha}$ ; et celles telles que $L_{f,1} \subset L_{d,a}$, qui seront notées comme $\tau_{d,\beta}$. On peut de plus supposer que telle $\tau_{d,\beta}$ existe (sinon on peut échanger certaine $\tau_{d,a}$ et certaine $\tau_{f,i}$ et renommer les $\tau_{f,i}$). Alors on sait bien que

– $\dim(L_{d,\beta} \cap L_{f,1}) < \dim(L_{d,\beta})$ ;
– si $W$ est une composante de $L_{d,\alpha}$ d'autre que $L_{f,1}$, alors $\dim(W \cap L_{f,1}) < \dim(W)$.
Donc on peut prendre
– un point $P \in \mathbb{H}^w$ tel que $P \in L_{f,1}$ et $P \notin L_{f,i}$ $(i \neq 1)$,
– un demi-disque $U_{f,1}$ dans $\mathbb{H}_1$ et des disques $U_{f,i}$ dans $\mathbb{H}_i$ pour $(i \neq 1)$,
tels que

$$U^* := U_{f,1} \times \prod_{i \neq 1} U_{f,i}$$

est à distance strictement positive de $L_{d,\beta}$ et toutes les composantes de $L_{d,\alpha}$ d'autres que $L_{f,1}$.

Notons

$$V_{d,a} := \phi_a(U^*), \qquad \Phi := (\phi_a,\ a = 1, ..., n - w)$$

et

$$Y^* := \{(u, \Phi(u)) | u \in U^*\} \subset Y.$$

$Y^*$ est clairement définissable.

Prenons maintenant des domaines fondamentals (ou l'union fini) dans $\mathbb{H}$

$$\mathbb{D}_{f,1} \subset U_{f,1}, \qquad \text{et } \mathbb{D}_{f,i} \supset U_{f,i}\ (i \neq 1)$$

et

$$\mathbb{D}_{d,\alpha} \subset V_{d,\alpha}, \qquad \text{et } \mathbb{D}_{d,\beta} \supset V_{d,\beta}.$$

Alors

$$\mathbb{D}^* := \mathbb{D}_{f,1} \times \prod_{i \neq 1} \mathbb{D}_{f,i} \times \prod_{\alpha} \mathbb{D}_{d,\alpha} \times \prod_{\beta} \mathbb{D}_{d,\beta}$$

est un union fini des domaines fondamentals pour l'action $\Gamma$ sur $U$, donc

$$Z^* := \mathcal{Z} \cap \mathbb{D}^*$$

est définissable grâce à Propriété (1.4).

Après on va utiliser plutôt $Y^*$ et $Z^*$ à la place de $Y$ et $Z$ car l'intricacie sera appliquée plus facilement dans ce cadre.

***Une famille des translatés dans $G$ sous laquel $Y$ est invariante***

Pour $a/c \in \partial U_{f,1} \cap \mathbb{R}$, fixons

$$g_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

considérons le groupe à un paramètre

$$G(g_0) := \{g(t) \in G | g_{f,1}(t) = \begin{pmatrix} a & b + ta \\ c & d + tc \end{pmatrix},\ t \in \mathbb{R},\ g_{f,i} = 1\ (i \neq 1)\}.$$

On va considérer le sous-ensemble

$$H := \{g \in G(g_0) | \dim(gY^* \cap Z^*) = w\}.$$

Il est définissalbe car tous apparaissant dans la définition sont définissable (tous les ensembles et aussi la fonction "dim").

Tout d'abord, on a

$$g_{f,1}(t)\mathbb{D}_{f,1} \subset U_{f,1}$$

pour $t \in \mathbb{Z}$ assez grand. Donc pour $g(t) = (g_{f,i}(t)) \in G(g_0)$ et

$$\mathcal{E} := \mathbb{D}_{f,1} \times \prod_{i \neq 1} U_{f,i},$$

on a

$$Y_{g(t),\mathcal{E}} := \{(\tau_f, \Phi(g_{f,1}(t)\tau_1, \tau_i)) | \tau_f \in \mathcal{E}\} \subset \mathcal{Z},$$

ainsi qu'aussi toutes ses translatés par l'élément de $\Gamma$. Choisissons maintenant $h(t) \in \Gamma$ qui est trivial en toutes les variables libres pour amener un point régulier de dimension pleine dans $\mathbb{D}^*$. Cet $h(t)$ peut être choisi satisfaisant

$$h_{f,i}(t) = 1, \qquad h_\beta(t) = 1.$$

C'est à dire

$$(\tau_{f,1}, \tau_{f,i}, \tau_{d,a}) \in g(t)Y^* \subset g(t)Y$$

où

$$\tau_{d,\alpha} = h_\alpha(t)\phi_\alpha(g_{f,1}(t)\tau_{f,1}, \tau_{f,i}),$$
$$\tau_{d,\beta} = \phi_\beta(g_{f,1}(t)\tau_{f,1}, \tau_{f,i}),$$

et

$$g(t) = (g_{f,1}(t)^{-1}, 1, ..., 1, h_a(t),\ a = 1, ..., n - w).$$

De plus, ce point-ce est régulier de dimension pleine, donc $h(t) \in H$.

Par intricacie (Proposition (3.3)), on peut toujours choisir un tel $h(t) \in H$ de la hauteur

$$<< t^c,$$

donc pour $T$ suffisamment grand,

$$N_{\mathbb{Q}}(H, T) >> T^\delta$$

pour certain $\delta > 0$. Donc pour $\delta/2 > 0$, d'après Chapitre 2, Théorème (3.4), il y a un sous-ensemble algébrique $H'$ de $H$ tel que $\dim(H') > 0$ et qui admet

$$>> T^{\delta/2}$$

points rationnels réguliers.

On va montrer que $t$ se varie sur $H'$, d'où on conclude $\dim(Stab(Y)) > 0$ d'après Proposition (2.5). Comme les sous-ensembles semi-algébriques de $H'$ (apparaissant dans Chapitre 2, Théorème (3.5)) sont de degré borné indépendant de $T$, ses intersections avec

$$\{g \in G | g_{f,1} = t_0\}$$

avec $t_0$ constante sont de degré borné, dont les nombres des points singuliers (rationnels) sont bornés. Maintenant si $t$ ne se varie pas sur $H'$, alors on peut trouver un point régulier d'un arc dans cet intersection. Comme cet arc donne une famille des composantes complexes maximales qui n'est pas constante, on obtient une contradiction de Proposition (2.5).

***Les identités qu'on veut***

Pour un voisinage ouvert de $H'$ (on peut supposer que 0 est dedans), $g(t)Y = g(0)Y$ par Proposition (2.5). Comme $\dim(Y) = w$ et $\tau_{f,1}, ..., \tau_{f,w}$ sont fixées, on sait que

$$h_a(t)\phi_a(g_{f,1}(t)\tau_{f,1}, \tau_{f,i})$$

en sont aussi. Donc en fait $\phi_\beta$ et donc $\tau_{d,\beta}$ est indépendant de $\tau_{f,1}$.

Quand à $\tau_{d,\alpha}$, fixons $t_0$ tel que

$$h_\alpha(t)\phi_\alpha(g_{f,1}(t)\tau_{f,1},\tau_{f,i}) = h_\alpha(t_0)\phi_\alpha(g_{f,1}(t_0)\tau_{f,1},\tau_{f,i})$$

identiquement. Fixons $\tau_{f,i}$, $i \neq 1$, mettons

$$g := g_{f,1}(t)g_{f,1}(t_0)^{-1} = \begin{pmatrix} 1-ac(t-t_0) & a^2(t-t_0) \\ -c^2(t-t_0) & 1+ac(t-t_0) \end{pmatrix}$$

qui est parabolique avec le point fixé $a/c$, et $h := h(t)^{-1}h(t_0)$, on a une identité

$$\phi_\alpha(g\tau) = h\phi_\alpha(\tau). \tag{4.1.1}$$

On va montrer que $\phi_\alpha$ est alors 1-à-1.

Il est claire que $\phi_\alpha$ n'est pas constante. Supposons qu'elle est génériquement $k$-à-1 avec $k \geqslant 2$, et $b_1, ..., b_K$ les points mauvais (en lesquels $\phi_\alpha$ est ramifié ou n'est pas $k$-à-1). On peut toujours trouver un $x_0 = a/c$ satisfaisant

$$\phi_\alpha(x_0) \neq \phi_\alpha(g^i(b_j))$$

pour $i = 1, ..., k$, $j = 1, ..., K$. Dans ce cas, quelque soit $x_1$ tel que $\phi_\alpha(x_1) = \phi_\alpha(x_0)$ le satisafait aussi. On a

$$\phi_\alpha(gx_1) = h\phi_\alpha(x_1) = h\phi_\alpha(x_0) = \phi_\alpha(gx_0) = \phi_\alpha(x_0),$$

donc $\phi_\alpha(g^n x_1) = \phi_\alpha(x_0)$ pour tous $n = 1, 2, ..., k$. Mais ceci imdique que $g$ admet un point pré-périodique sauf le point fixé, qui contracte au fait que $g$ est parabolique.

On peut échanger $\tau_{f,1}$ et $\tau_{d,\alpha}$, donc $\phi_\alpha^{-1}$ est aussi 1-à-1. Comme $\phi_\alpha(\mathbb{R}) \subset \mathbb{R}$, on conclude $\phi_\alpha \in SL_2(\mathbb{R})$ quand $\tau_{f,i}$ $(i \neq 1)$ sont fixés.

Quand $\tau_{f,i}$ $(i \neq 1)$ se varie, $\phi_\alpha$ est un élément de $SL_2(\mathbb{R})$, et $\tau_{f,i} \mapsto \phi_\alpha$ est complexe analytique, donc est constante.

En résumé, il y a deux types des variables dépendantes : soit ne dépend pas de $\tau_{f,1}$, soit ne dépend que de $\tau_{f,1}$.

***De*** $SL_2(\mathbb{R})$ ***à*** $GL_2(\mathbb{Q})^+$

Maintenant pour conclure, il faut justement expliquer $\phi_\alpha \in GL_2(\mathbb{Q})^+$. Par ce qui est discuté, on sait que dans l'identité (4.1.1), pour $>> T^{\delta/2}$ choix de $s = t - t_0 \in \mathbb{Z}$ (donc de $g$), $h$ est un point rationnel. C'est à dire

$$\phi_\alpha g \phi_\alpha^{-1} = \lambda h, \quad \lambda \in \mathbb{R}, \quad h \in GL_2(\mathbb{Q})^+. \tag{4.1.2}$$

Pour $\phi_\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL_2(\mathbb{R})$, on peut montrer facilement que $\phi_\alpha$ est de la forme qu'on veut si $A, B, C, D = 0$. Par exemple si $C = 0$, prennons $a = 1$, $c = 0$ dans $g$ et alors

$$\begin{pmatrix} 1-sAC & sA^2 \\ -sC^2 & 1+sAC \end{pmatrix}$$

est de la forme $\lambda h$, $\lambda \in \mathbb{R}$, $h \in GL_2(\mathbb{Q})^+$. Comme $C = 0$, $A^2 \in \mathbb{Q}$ et $AD = 1$ implique $A/D \in \mathbb{Q}$ et $D \neq 0$. Si $B = 0$, on a rien d'autre à montrer. Si $B \neq 0$, prenons $a = 0$, $c = 1$ dans $g$ et

$$\begin{pmatrix} 1-sBD & sB^2 \\ -sD^2 & 1+sBD \end{pmatrix}$$

est de la forme $\lambda h$, $\lambda \in \mathbb{R}$, $h \in GL_2(\mathbb{Q})^+$. Ceci implique $B/D \in \mathbb{Q}$. Donc $\phi_\alpha$ est de la forme qu'on veut.

Sinon,

$$\psi := \begin{pmatrix} 1 & 0 \\ -C/A & 1 \end{pmatrix}\phi_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & (D/B - C/A)\alpha \end{pmatrix}$$

satisfait la même équalité (4.1.2), et donc $\psi \in GL_2(\mathbb{Q})^+$, et donc $\phi_\alpha$ aussi. □

CHAPITRE 4

# La borne inférieure

## 1. Complexité d'un point pré-spécial

**Définition 1.1.** Soit $u = (\tau_1, ..., \tau_n) \in U$ un point pré-spécial, $E_i$ la courbe elliptique correspandante à $\tau_i$, $R_i := \mathrm{End}(E_i)$. Définissons $D_i := \mathrm{disc}(R_i/\mathbb{Z})$ le discriminant de $R_i$ sur $\mathbb{Z}$, alors la *complexité de u* est définie par

$$\Delta(u) := \max(|D_1|, ..., |D_n|).$$

En ce cas simple, $D_i$ peut se voir facilement comme le discriminant de $\tau_i$ (à signe près), c'est à dire

**Lemme 1.2.** *Soit $\tau \in \mathbb{H}$ un point pré-spécial, avec le polynôme minimal de $\tau$ (sur $\mathbb{Z}$) étant*

$$at^2 + bt + c$$

*avec $a > 0$, alors $D := \mathrm{disc}(\mathrm{End}(E_\tau)/\mathbb{Z})$ égale à $\Delta(\tau) := b^2 - 4ac$ à signe près.*

Démonstration. Soit $\alpha \in \mathrm{End}(E_\tau)$, alors il existe

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(\mathbb{Z})$$

telle que

$$\alpha \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix}.$$

Ainsi qu'on a

$$B\tau^2 - (A - D)\tau - C = 0$$

et

$$\alpha^2 - (A + D)\alpha + (AD - BC) = 0.$$

Donc

$$\mathrm{disc}(1, \alpha) = (A + D)^2 - 4(AD - BC) = k^2\Delta(\tau)$$

avec $k \in \mathbb{Z}$ à signe près car le polynôme minimal de $\tau$ est $at^2 + bt + c$. En particulier, si on prend

$$B = a,\ C = -c,\ A = D + b$$

avec $D \in \mathbb{Z}$ quelconque, alors le $\alpha \in \mathrm{End}(E_\tau)$ correspondant satisafait

$$\mathrm{disc}(1, \alpha) = b^2 - 4ac.$$

Ceci permet de conclure. □

**Proposition 1.3.** *Soit $X$ un produit des courbes modulaires, alors il existe une constante strictement positive $c_{hauteur}(X)$ telle que si $u = (\tau_1, ..., \tau_n) \in \mathbb{F}$ est un point pré-spécial, alors*

$$H(u) \leqslant c_{hauteur}(X)\Delta(u).$$

Démonstration. Il suffit de montrer pour une coordonnée, et on utilise les notations dans le lemme précédent. En suite, observons qu'il suffit de montrer le cas $X = \mathbb{C}$ et $\mathbb{F} = \mathbb{F}_{\mathbb{C}}$.

$\tau \in \mathbb{F}_{\mathbb{C}}$ implique

$$-\frac{1}{2} < \mathrm{Re}(\tau) \leqslant \frac{1}{2} \qquad \text{et} \qquad |\tau| \geqslant 1,$$

et donc $|b| \leqslant a \leqslant c$ par relations de Viète. Alors

$$4ac = b^2 - D \leqslant ac - D$$

d'où

$$a, a^2 \leqslant \frac{|D|}{3}.$$

Écrivons $\tau = x + \sqrt{-1}y$, alors

$$x = -\frac{b}{2a} \qquad \text{et} \qquad y = \frac{\sqrt{|D|}}{2a}.$$

Par , on a donc

$$H(x) \leqslant \max\{b, 2a\} \leqslant 2a \leqslant \frac{2|D|}{3}$$

et

$$H(y) \leqslant \max\{4a^2, |D|\} \leqslant \frac{4|D|}{3}.$$

Ceci permet de conclure car $H(\tau) << \max\{H(x), H(y)\}$. □

Maintenant, on énonce le résultat le plus important dans ce chapitre. Toutes les sections suivantes de ce chapitre seront consacrées à le montrer.

**Proposition 1.4.** *Soit $X$ un produit des courbes modulaires, alors il existe une constante $c_{deg}(X)$ telle que si $u \in U$ est un point pré-spécial, alors*

$$[\mathbb{Q}(\pi(u)) : \mathbb{Q}] \geqslant c_{deg}(X)\Delta(u)^{1/2-\nu}$$

Démonstration. Il suffit de montrer pour une seule coordonnée, i.e.

$$[\mathbb{Q}(j(E_\tau)) : \mathbb{Q}] >> \Delta(\tau)^{1/2-\nu}$$

avec $\tau$ un point MC dans $\mathbb{H}$. C'est une combinaison de

$$[\mathbb{Q}(j(E_\tau)) : \mathbb{Q}] = \#\mathcal{C}l(\mathrm{End}(E_\tau)) \qquad \text{par Théorème (3.4) et le remarque après}$$

et la borne inférieure de Siegel pour le nombre de classes d'un ordre d'un corps quadratique imaginaire (Théorème (5.1)). □

## 2. Théorie MC : première partie

Pour simplifier, on se restreint au cas d'ordre maximal $\mathcal{O}_K$ où $K$ est un corps quadratique imaginaire. La théorie générale est pareille.

On se donne la notation

$$\begin{aligned}\mathcal{E}ll(R) := &\quad \{\text{courbes elliptiques E}/\mathbb{C} \text{ telles que } \mathrm{End}(E) \simeq R\}/\text{isomorphisme sur } \mathbb{C} \\ = &\quad \{\text{réseaux } \Lambda \text{ tels que } \mathrm{End}(E_\Lambda) \simeq R\}/\text{homothetie}\end{aligned}$$

On va introduire deux propositions des courbes ellipiques avec multiplication complexe : on construit une action simplement transitive de $\mathcal{C}l(\mathcal{O}_K)$ sur $\mathcal{E}ll(\mathcal{O}_K)$, et on montre que chaque courbe elliptique avec multiplication complexe peut être définie sur une extension algébrique de $\mathbb{Q}$. Les preuves sont omises. Elles se trouvent, par exemple, dans [**S2**].

**Proposition 2.1.** (1) *Soient $\Lambda$ un réseau tel que $E_\Lambda \in \mathcal{E}ll(\mathcal{O}_K)$, et $\mathfrak{a}$, $\mathfrak{b}$ deux idéaux fractionnaires non-nuls de $K$, alors*

- $\mathfrak{a}\Lambda := \{\alpha_1\lambda_1 + ... + \alpha_r\lambda_r | \alpha_i \in \mathfrak{a},\ \lambda_i \in \Lambda\}$ *est un réseau dans $\mathbb{C}$ ;*
- *La courbe elliptique $E_{\mathfrak{a}\Lambda}$ satisfait $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \simeq \mathcal{O}_K$ ;*
- *$E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ si et seulement si $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ dans $\mathcal{C}l(\mathcal{O}_K)$.*

*Donc il existe une action bien-définie de $\mathcal{C}l(\mathcal{O}_K)$ sur $\mathcal{E}ll(\mathcal{O}_K)$ déterminée par*

$$\overline{\mathfrak{a}} * E_\Lambda := E_{\mathfrak{a}^{-1}\Lambda}.$$

(2) *Cette action est simplement transitive. En particuler,*

$$\#\mathcal{C}l(\mathcal{O}_K) = \#\mathcal{E}ll(\mathcal{O}_K).$$

**Proposition 2.2.** (1) *Soient $E/\mathbb{C}$ une courbe elliptique et $\sigma : \mathbb{C} \to \mathbb{C}$ un automorphisme de $\mathbb{C}$, alors*

$$\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E).$$

(2) *Soit $E/\mathbb{C}$ une courbe elliptique avec multiplication complexe, alors son $j$-invariant $j(E) \in \overline{\mathbb{Q}}$.*

(3) *Toutes les courbes elliptique avec multiplication complexe sont définies sur $\overline{\mathbb{Q}}$, i.e.*

$$\mathcal{E}ll(\mathcal{O}_K) \simeq \{\textit{courbes elliptiques } E/\overline{\mathbb{Q}} \textit{ avec } \mathrm{End}(E) \simeq \mathcal{O}_K\}/\textit{isomorphisme sur } \overline{\mathbb{Q}}.$$

**Corollaire 2.3.** *Les deux propositions au dessus nous donnent une inégalité*

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leqslant h_K$$

*où $E$ est une courbe elliptique telle que $\mathrm{End}(E) \simeq \mathcal{O}_K$ et $h_K := \#\mathcal{C}l(\mathcal{O}_K)$.*

Voici une proposition très importante :

**Proposition 2.4.** *Soient $E/\overline{\mathbb{Q}}$ une courbe elliptique représentant un élément de $\mathcal{E}ll(\mathcal{O}_K)$, $\overline{\mathfrak{a}} \in \mathcal{C}l(\mathcal{O}_K)$ et $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, alors*

$$(\overline{\mathfrak{a}} * E)^\sigma = \overline{\mathfrak{a}}^\sigma * E^\sigma.$$

La proposition a l'air claire, mais en fait elle n'est pas triviale du tout. Elle donne une relation entre l'action algébrique de $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et l'action analytique de multiplication par $\overline{\mathfrak{a}}$. L'idée de la preuve est trouver une description algébrique de $\overline{\mathfrak{a}} * E$.

Démonstration. Choisissons un réseau $\Lambda$ tel que $E \simeq E_\Lambda = \mathbb{C}/\Lambda$. Fixons une résolution

$$\mathcal{O}_K^m \xrightarrow{A} \mathcal{O}_K^n \to \mathfrak{a} \to 0,$$

avec $A$ une $m \times n$ matrice dont les coefficients sont dans $\mathcal{O}_K$.

Dorénavant dans la preuve, Hom toujours s'agit de $\mathrm{Hom}_{\mathcal{O}_K}$. On a un diagramme commutatif :

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathfrak{a},\Lambda) & \longrightarrow & \mathrm{Hom}(\mathfrak{a},\mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathfrak{a},E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n,\Lambda) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n,\mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n,E) \\
 & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} \\
0 & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m,\Lambda) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m,\mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m,E)
\end{array}$$

En appliquant $\mathrm{Hom}(\mathcal{O}_K^n, M) \simeq M^n$, $\mathrm{Hom}(\mathfrak{a},\Lambda) = \mathfrak{a}^{-1}\Lambda$ et $\mathrm{Hom}(\mathfrak{a},\mathbb{C}) = \mathfrak{a}^{-1}\mathbb{C} = \mathbb{C}$, on obtient un autre diagramme commutatif :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{a}^{-1}\Lambda & \longrightarrow & \mathbb{C} & \longrightarrow & \mathrm{Hom}(\mathfrak{a},E) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Lambda^n & \longrightarrow & \mathbb{C}^n & \longrightarrow & E^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \\
0 & \longrightarrow & \Lambda^m & \longrightarrow & \mathbb{C}^m & \longrightarrow & E^m & \longrightarrow & 0
\end{array}$$

Les deux lignes en bas sont exactes à droite car elles sont des copies de la suite exacte :

$$0 \to \Lambda \to \mathbb{C} \to E \to 0.$$

En appliquant le lemme de serpent au diagram au dessus (les deux lignes en bas), on obtient une suite exacte

$$0 \to \mathfrak{a}^{-1}\Lambda \to \mathbb{C} \to \mathrm{Ker}(E^n \xrightarrow{A^t} E^m) \to \Lambda^n/A^t\Lambda^m.$$

Comme $\Lambda^n/A^t\Lambda^m$ est discrèt et $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ est connexe par rapport à la topologie complexe, cette suite nous donne

$$(\mathfrak{a} * E)(\mathbb{C}) = \mathbb{C}/\mathfrak{a}^{-1}\Lambda \simeq \text{la composante neutre de } \mathrm{Ker}(E^n \xrightarrow{A^t} E^m).$$

D'ailleurs, $E^n \xrightarrow{A^t} E^m$ est un morphisme algébrique des groups algébriques car $A^t$ est une $m \times n$ matrice dont les coefficients sont éléments de $\mathrm{End}(E) = \mathcal{O}_K$. Donc $\mathrm{Ker}(E^n \xrightarrow{A^t}$

$E^m$) est un groupe algébrique. Donc en fin, on a donné une description algébrique de $\mathfrak{a}*E$ en termes d'un morphisme algébrique $E^n \xrightarrow{A^t} E^m$.

Maintenant, on peut conclure en moyen de

$$\begin{aligned}(\mathfrak{a}*E)^\sigma = & \quad (\text{la composante neutre de } \mathrm{Ker}(E^n \xrightarrow{A^t} E^m))^\sigma \\ = & \quad \text{la composante neutre de } \mathrm{Ker}((E^\sigma)^n \xrightarrow{(A^t)^\sigma} (E^\sigma)^m) \\ = & \quad \mathfrak{a}^\sigma * E^\sigma.\end{aligned}$$

□

De cette proposition on peut définir un morphisme des groupes de façon suivante :

**Définition-Proposition 2.5.** *Pour $K$ un corps quadratique imaginaire, on définit un morphisme des groupes :*

$$F : \mathrm{Gal}(\overline{K}/K) \to \mathcal{C}l(\mathcal{O}_K)$$

*uniquement déterminé par la condition*

$$E^\sigma = F(\sigma) * E$$

*pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K)$ et toute $E \in \mathcal{E}ll(\mathcal{O}_K)$.*

Démonstration. Par l'action simplement transitive de $\mathcal{C}l(\mathcal{O}_K)$ sur $\mathcal{E}ll(\mathcal{O}_K)$ et que $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$, on sait qu'il existe une unique $\overline{\mathfrak{a}} \in \mathcal{C}l(\mathcal{O}_K)$ telle que

$$E^\sigma = \overline{\alpha} * E.$$

Donc pour une $E$ fixée, on peut définir un morphisme des groupes $F$ déterminé par la propriété décrite avant. Le fait que $F$ est un morphisme des groupes est facile à vérifié. Donc il reste à vérifier que la définition de $F$ ne dépend pas du choix de $E \in \mathcal{E}ll(\mathcal{O}_K)$.

Soient $E_1, E_2 \in \mathcal{E}ll(\mathcal{O}_K)$ et $\sigma \in \mathrm{Gal}(\overline{K}/K)$, écrivons $E_i^\sigma = \overline{\mathfrak{a}}_i * E_i$, il faut et il suffit de montrer $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. Par l'action simplement transitive, on peut trouver une $\overline{\mathfrak{b}}$ telle que $E_2 = \overline{\mathfrak{b}} * E_1$, ainsi

$$(\overline{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \overline{\mathfrak{a}}_2 * E_2 = \overline{\mathfrak{a}}_2 * (\overline{\mathfrak{b}} * E_1) = (\overline{\mathfrak{a}}_2 \overline{\mathfrak{b}} \overline{\mathfrak{a}}_1^{-1}) * E_1^\sigma.$$

La conclusion suit du fait $(\overline{\mathfrak{b}} * E_1)^\sigma = \overline{\mathfrak{b}} * E_1^\sigma$. □

## 3. Théorie MC : deuxième partie

Les notations seront les mêmes comme la section précédente.

On se donne deux lemmes sans preuve :

**Lemme 3.1.** *Pour $E \in \mathcal{E}ll(\mathcal{O}_K)$, le degré de l'application naturelle $E \to \overline{\mathfrak{a}}*E$ est $N_{K/\mathbb{Q}}(\mathfrak{a})$ pour $\mathfrak{a}$ un idéal intègre dans $\mathcal{O}_K$.*

**Lemme 3.2.** *Soient $L$ un corps des nombres, $E_i/L$ $(i = 1, 2)$ deux courbes elliptiques et $\mathfrak{P}$ un idéal maximal de $L$ tels que $E_i$ admet une bonne réduction $\widetilde{E_i}$ en $\mathfrak{P}$, alors l'application de la réduction (en $\mathfrak{P}$)*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2}), \qquad \phi \mapsto \widetilde{\phi}$$

*préserve le degré.*

Les preuves peuvent se trouver dans [**S2**].

**Proposition 3.3.** *Il existe un ensemble fini $S \subset \mathbb{Z}$ des primes rationels tel que si $p \notin S$ est un prime qui se scinde dans $K$, disons $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, alors*

$$F(\mathrm{Frob}_{\mathfrak{p}}) = \overline{\mathfrak{p}} \in \mathcal{C}l(\mathcal{O}_K),$$

*où $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ est l'élément de Frobenius correspondant à $\mathfrak{p}$.*

Démonstration. On peut choisir une extensions finie $L/K$ et des représentatives $E_1, ..., E_n$ définies sur $L$ pour les classes d'isomorphisme distinctes de $\mathcal{E}ll(\mathcal{O}_K)$ car $\mathcal{E}ll(\mathcal{O}_K) = \mathcal{C}l(\mathcal{O}_K)$ est fini et toutes les courbes dans $\mathcal{E}ll(\mathcal{O}_K)$ sont définies sur $\overline{\mathbb{Q}}$. Du plus, remplaçons $L$ par une extension finie telle que chaque isogénie entre deux des $E_i$'s est définie sur $L$ (c.f. ). Maintenant mettons $S$ l'ensemble des primes dans $K$ tels que :

– $p$ est ramifié dans $L$,
– il existe une $E_i$ qui admet une mauvaise réduction en un prime de $L$ au dessus de $\mathfrak{p}$,
– $j(E_i) = j(E_k) \pmod{\mathfrak{P}}$ pour quelque $\mathfrak{P}$ au dessus de $\mathfrak{p}$ et quelques $E_i, E_k$.

Maintenant, soient $p \in S$ un primier qui se scinde comme $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ dans $K$ et $\mathfrak{P}$ un prime de $L$ au dessus de $\mathfrak{p}$. Choisissons un idéal intègre premier à $\mathfrak{p}$ tel que

$$\mathfrak{a}\mathfrak{p} = (\alpha)$$

est principal. Si $\Lambda$ est le réseau de $E$ (i.e. $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$), alors on a un diagramme commutatif

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}\Lambda = \mathbb{C}/\alpha^{-1}\Lambda & \xrightarrow[\sim]{z\mapsto \alpha z} & \mathbb{C}/\Lambda \\
\sim\downarrow & & \sim\downarrow & & \sim\downarrow & & \sim\downarrow \\
E & \xrightarrow{\phi} & \overline{\mathfrak{p}} * E & \xrightarrow{\psi} & \overline{\mathfrak{a}} * \overline{\mathfrak{p}} * E = (\alpha) * E & \xrightarrow[\sim]{\lambda} & E
\end{array}.$$

Choisissons ensuite une équation de Weierstrass pour $E/L$ qui est minimale en $\mathfrak{P}$ et mettons $\omega$ le différentiel invariant associé à $E$, alors modulo $\mathfrak{P}$, $\widetilde{\omega}$ est encore un différentiel invariant non-nul sur $\widetilde{E}$. Par le diagramme, on a

$$(\lambda \circ \psi \circ \phi)^*\omega = \alpha\omega$$

et

$$(\widetilde{\lambda} \circ \widetilde{\psi} \circ \widetilde{\phi})^*\widetilde{\omega} = \widetilde{(\lambda \circ \psi \circ \phi)}^*\omega = \widetilde{\alpha}\widetilde{\omega} = \widetilde{0}$$

car $(\alpha) = \mathfrak{a}\mathfrak{p}$ et $\mathfrak{P}$ divise $\mathfrak{p}$. Ainsi que

$$\widetilde{\lambda} \circ \widetilde{\psi} \circ \widetilde{\phi} \text{ est inséparable.}$$

Par Lemme (3.1) et Lemme(3.2), on a

$$\deg \widetilde{\phi} = \deg \phi = N_{K/\mathbb{Q}}\mathfrak{p} = p,$$
$$\deg \widetilde{\psi} = \deg \psi = N_{K/\mathbb{Q}}\mathfrak{a},$$

et

$$\deg \widetilde{\lambda} = \deg \lambda = 1.$$

Comme $N_{K/\mathbb{Q}}\mathfrak{a}$ est premier à $\mathfrak{p}$ par hypothèse, $\widetilde{\psi}$ et $\widetilde{\lambda}$ sont tous séparables, ainsi qu'on conclude que

$$\widetilde{\phi} : \widetilde{E} \to \widetilde{\overline{\mathfrak{p}} * E}$$

est inséparable, et donc se factorise via une application de Frobenius de puissance $q^{\text{ème}}$. Du coup $\deg \widetilde{\phi} = p$ affirme que $\widetilde{\phi}$ peut s'écrire comme la composition

$$\widetilde{E} \xrightarrow[\text{puissance } p^{\text{ème}}]{\text{Frobenius de}} \widetilde{E}^{(p)} \to \sim\widetilde{\mathfrak{p} * E}.$$

En particuler, on a montré

$$j(\overline{\mathfrak{p}} * E) \equiv j(E)^p = j(E)^{N_{K/\mathbb{Q}}\mathfrak{p}} \equiv j(E)^{\mathrm{Frob}_{\mathfrak{p}}} = j(E^{\mathrm{Frob}_{\mathfrak{p}}}) = j(F(\mathrm{Frob}_{\mathfrak{p}}) * E) \qquad (\mathrm{mod}\ \mathfrak{P})$$

car $j(\widetilde{\overline{\mathfrak{p}} * E}) = j(\widetilde{E^{(p)}}) = j(\widetilde{E})^p$. Donc $\overline{\mathfrak{p}} * E \simeq F(\mathrm{Frob}_{\mathfrak{p}}) * E$ par le choix de $S$. L'action simplement transitive nous donne alors

$$F(\mathrm{Frob}_{\mathfrak{p}}) = \overline{\mathfrak{p}}.$$

□

**Théorème 3.4.** *Soit $E$ une courbe elliptique représentant une classe d'isomorphisme dans $\mathcal{E}ll(\mathcal{O}_K)$, alors*

(1) *$K(j(E))$ est le corps de classes de Hilbert de $K$.*
(2) *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = \#\mathcal{C}l(\mathcal{O}_K)$.*

Démonstration. Soit $L/K$ est l'extension finie correspondant au morphisme $F : \mathrm{Gal}(\overline{K}/K) \to \mathcal{C}l(\mathcal{O}_K)$, i.e. $L$ est le corps fixé par le noyau de $F$, alors

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &= \mathrm{Ker}(F) \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | F(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | F(\sigma) * E = E\} \qquad \text{par l'action simplement transitive} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | E^\sigma = E\} \qquad \text{par la définition de } F \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | j(E^\sigma) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | j(E)^\sigma = j(E)\} \\
&= \mathrm{Gal}(\overline{K}/K(j(E))) \qquad .
\end{aligned}$$

Donc $L = K(j(E))$. De plus, comme $F$ envoie $\mathrm{Gal}(L/K)$ dans $\mathcal{C}l(\mathcal{O}_K)$ injectivement, $L/K$ est une extension abélienne.

Ensuite, soit $\mathfrak{c}_{L/K}$ le conducteur de $L/K$ (c.f. [**Ne**] Page 525), i.e. l'idéal intègre qui est maximal parmi ceux qui

– sont divisibles précisement par les idéaux qui sont ramifiés dans $L$,
– satisfaisent

$$\alpha \in K^* \text{ et } \alpha \equiv 1 (\mathrm{mod}\ \mathfrak{c}) \Rightarrow ((\alpha), L/K) = 1.$$

Considérons la composition

$$I(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot, L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} \mathcal{C}l(\mathcal{O}_K),$$

où $I(\mathfrak{c}_{L/K})$ est l'ensemble des idéaux fractionnaires premiers à $\mathfrak{c}_{L/K}$. Montrons que cette composition n'est que la projection naturelle de $I(\mathfrak{c}_{L/K})$ à $\mathcal{C}l(\mathcal{O}_K)$, i.e.

$$F((\mathfrak{a}, L/K)) = \overline{\mathfrak{a}} \qquad \text{pour tout } \mathfrak{a} \in I(\mathfrak{c}_{L/K}).$$

Soient $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$ et $S$ l'ensemble comme dans Proposition (3.3). Grâce au thèorème de Dirichlet ([**Ne**] Chapter VII, Theorem 13.2), il existe un idéal premier $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ tel que

– il existe $\alpha \in K^*$ tel que

$$\alpha \equiv 1 (\text{mod } \mathfrak{c}_{L/K}) \qquad \text{et} \qquad \mathfrak{a} = (\alpha)\mathfrak{p};$$

– $\mathfrak{p}$ n'est pas au dessus d'un prime dans $S$, i.e. $N_{K/\mathbb{Q}}\mathfrak{p} \notin S$.

Alors on a

$$\begin{aligned} F((\mathfrak{a}, L/K)) &= F(((\alpha)\mathfrak{p}, L/K)) && \text{car } \mathfrak{a} = (\alpha)\mathfrak{p} \\ &= F((\mathfrak{p}, L/K)) && \text{car } \alpha \equiv 1 (\text{mod } \mathfrak{c}_{L/K}) \\ &= \overline{\mathfrak{p}} && \text{Proposition (3.3) car } N_{K/\mathbb{Q}}\mathfrak{p} \notin S \\ &= \overline{\mathfrak{a}} && \text{car } \mathfrak{a} = (\alpha)\mathfrak{p}. \end{aligned}$$

En conséquence,

$$F(((\alpha), L/K)) = 1 \qquad \text{pour tous idéaux principaux } (\alpha) \in I(\mathfrak{c}_{L/K}).$$

Le fait que $F : \text{Gal}(L/K) \to \mathcal{C}l(\mathcal{O}_K)$ est injectif implique alors

$$((\alpha), L/K) = 1 \qquad \text{pour tous } (\alpha) \in I(\mathfrak{c}_{L/K}).$$

Par définition du conducteur, on a alors $\mathfrak{c}_{L/K} = (1)$, et donc $L/K$ est partout non-ramifié. Du coup $L$ est contenu dans le corps de classes de Hilbert $H$ de $K$.

D'ailleurs, $F : \text{Gal}(L/K) \to \mathcal{C}l(\mathcal{O}_K)$ est surjectif car $I(\mathfrak{c}_{L/K}) = I((1)) \to \mathcal{C}l(\mathcal{O}_K)$ l'est. Ceci nous donne

$$[L : K] = \#\,\text{Gal}(L/K) = \#\,\mathcal{C}l(\mathcal{O}_K) = \#\,\text{Gal}(H/K) = [H : K],$$

et par conséquence $H = L = K(j(E))$.

Maintenant, on a

$$\#\,\mathcal{C}l(\mathcal{O}_K) = [K(j(E)) : K] \leqslant [\mathbb{Q}(j(E)) : \mathbb{Q}] \leqslant \#\,\mathcal{C}l(\mathcal{O}_K)$$

où la première inégalité est donnée par $[K : \mathbb{Q}] = 2$ et la dernière inégalité est donnée par Corollaire (2.3). Ceci nous permet de conclure. □

**Remarque 3.5.** En général, l'anneau d'endomorphismes d'une courbe elliptique $E$ avec multiplication complexe est justement un ordre $R$ d'un corps quadratique imaginaire. Mais en ce cas, l'égalité dans le théorème principal reste vraie, i.e.

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] = \#\,\mathcal{C}l(R).$$

## 4. Formule du nombre de classes

On commence par un lemme facile pour les réseaux.

**Lemme 4.1.** *Soient $D \subset \mathbb{R}^N$ un sous-ensemble et $\Lambda$ un réseau dans $\mathbb{R}^N$ dont le domaine fondamental contenant l'origine est $F$. Supposons que la borne de $D$ est $(N-1)$-Lipschitz paramètrisable, c'est à dire il existe un nombre fini d'applications Lipschitz*

*$\phi_j : [0,1]^{N-1} \to \partial D$ dont les images couvent $\partial D$. Mettons $\lambda(t) = \lambda(t, D, F)$ le nombre des points du réseau $\Lambda$ dans $tD$, alors*

$$\lambda(t) = \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^N + \mathcal{O}(t^{N-1}),$$

*où la constante dans $\mathcal{O}$ ne dépend que $L$, $n$ est les constantes de Lipschitz.*

DÉMONSTRATION. (*esquisse*) Mettons $F_\lambda := F + \lambda$, et

$$n(t) = \#\{\lambda \in \Lambda | F_\lambda \subset (tD)^\circ\},$$

et

$$m(t) = \#\{\lambda \in \Lambda | F_\lambda \cap tD \neq \emptyset\}.$$

Alors

$$n(t) \leqslant \lambda(t) \leqslant m(t).$$

C'est claire que

$$n(t) \leqslant \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^N \leqslant m(t),$$

donc il suffit de montrer que

$$m(t) - n(t) \leqslant \mathcal{O}(T^{N-1}).$$

Pour la fin de la preuve, voyez [**La**]. □

Pour un corps de nombres $K$, on peut associer un plongement

$$\sigma = (\sigma_v)_{v \in \Omega_{K,\infty}} : K \to A_K(\infty) := \prod_{v \in \Omega_{K,\infty}} K_v \simeq \mathbb{R}^N = \mathbb{R}^{r_1 + 2r_2},$$

et $U := \mathcal{O}_K^*$ agit sur $A_K(\infty)$ par

$$u(a_v) := (\sigma_v(u) a_v).$$

Comme seulement les élément $\xi \neq 0$ nous intéresse, on se restreint à

$$J_K(\infty) := \prod_{v \in \Omega_{K,\infty}} K_v^*.$$

Il est claire que $J_K(\infty)$ est stable sous l'action de $U$. Introduisons la norme

$$N(\xi) := \prod_{v \in \Omega_{K,\infty}} |\xi|_v^{N_v},$$

alors on sait que

- si $\xi = u\eta$ avec $u \in U$, alors $N(\xi) = N(\eta)$ ;
- $N(\xi) \neq 0$ si $\xi \neq 0$ ;
- $N(t\xi) = t^N N(\xi)$.

**Proposition 4.2.** *Il existe un domain fondamental $D$ pour l'action de $U$ sur $J_K(\infty)$ tel que $tD = D$ pour tout $t > 0$, et*

$$D(1) := \{\xi \in D | N(\xi) \leqslant 1\}$$

*admet une borne qui est $(N-1)$-Lipschitz paramètrizable, et*

$$\mathrm{Vol}(D(1)) = 2^{r_1} \pi^{r_2} R,$$

*où $R$ est le régulateur de $K$.*

DÉMONSTRATION. On va construire $D$ comme le suivant. Soit

$$g : J_K(\infty) \to \prod_{v\in\Omega_{K,\infty}} \mathbb{R}_v$$

le morphisme de log homogenisé donné par

$$g(\xi) := (..., \log \frac{\|\xi_v\|}{N(\xi)^{N_v/N}}, ...)_{v\in\Omega_{K,\infty}},$$

où $\|\xi_v\| = |\xi_v|^{N_v}$. Alors $\mathrm{Im}(g)$ se trouve dans l'hyperplan $H$ consistant les éléments $z$ tels que

$$\sum_{v\in\Omega_{K,\infty}} z_v = z_1 + ... + z_{r_1+r_2} = 0.$$

Soit $\{\eta_1, ..., \eta_r\}$ les générateurs de $U$ et $g(\eta_i) = y_i$, alors $\{y_1, ..., y_r\}$ est une base d'un réseau dans $H$. Observons que $y_1, ..., y_r$ sont les images usuelles des inversibles $\eta_1, ..., \eta_r$ car $N(\eta_i) = 1$ comme $\eta_i \in U$. Mettons

$$F := \{c_1y_1 + ... + c_ry_r | 0 \leqslant c_q < 1\}$$

le domaine fondamental de ce réseau dans $H$, et

$$D := g^{-1}(F).$$

Il est immédiat que $D$ est un domaine fondamental pour l'action de $U$ sur $J_K(\infty)$. $tD = D$ parce que

$$\frac{\|t\xi_v\|}{N(t\xi)^{N_v/N}} = \frac{\|\xi_v\|}{N(\xi)^{N_v/N}}.$$

$D(1)$ est borné parce que pour toute coordonnée $\xi_v$ d'un élément de $D$, on a

$$|\xi_v| \leqslant N(\xi)^{1/N} e^{Br},$$

où $B$ est une borne pour les éléments $y_i$. Donc si $\xi \in D(1)$, on a

$$|\xi_v| \leqslant e^{Br}.$$

Maintenant, ce qui reste à montrer est que la borne de $D(1)$ est $(N-1)$-Lipschitz paramètrisable, et que calculer $\mathrm{Vol}(D(1))$. Pour ça, on utilise les coordonnées polaires. L'image réciproque $P$ de $D(1)$ dans l'espace de coordonnées polaires est

$$\begin{cases} 0 < \prod_{i=1}^{r_1+r_2} \rho_i^{N_i} \leqslant 1 \\ \log \rho_j - \frac{1}{N} \prod_{i=1}^{r_1+r_2} \rho_i^{N_i} = \sum_{q=1}^{r} c_q \log |\sigma_j \eta_q| \end{cases}$$

avec $0 \leqslant c_q < 1$ pour $q = 1, ..., r = r_1 + r_2 - 1$. Donc on a

$$\mathrm{Vol}(D(1)) = 2^{r_1}(2\pi)^{r_2} \int_P \rho_{r_1+1}...\rho_{r_1+r_2} d\rho_1 ... d\rho_{r_1+r_2}.$$

Considérons $S$ dans l'espace $\mathbb{R}^{r_1+r_2}$ avec les variables $(u, c_1, ..., c_r)$ satisfaisant

$$\begin{cases} 0 < u \leqslant 1 \\ 0 \leqslant c_q < 1 \end{cases}.$$

On a une bijection $f : S \to P$ donnée dans une direction par

$$\rho_j = u^{1/N} \exp(\sum_{q=1}^{r} c_q \log|\sigma_j \eta_q|) = f_j(u, c_1, ..., c_r),$$

et dans l'autre direction on a

$$u = \prod_{i=1}^{r_1+r_2} \rho_i^{N_i},$$

et les $c_q$'s sont uniquement déterminés par $(\rho_1, ..., \rho_{r_1+r_2})$ parce que $\det(|\sigma_j \eta_q|)$ ne s'annule pas, et cet déterminant est le régulateur par définition.

Comme

$$\partial\rho_j/\partial u = \frac{1}{N}\frac{\rho_j}{u} \qquad \text{et} \qquad \partial\rho_j/\partial c_q = \rho_j \log|\sigma_j \eta_q|,$$

on a

$$\begin{aligned} Jac(f) &= \frac{1}{N\rho_{r_1+1}...\rho_{r_1+r_2}} \begin{vmatrix} 1 & \log|\sigma_1\eta_1| & ... & \log|\sigma_1\eta_r| \\ \vdots & \vdots & & \vdots \\ 1 & \log|\sigma_{r_1+r_2}\eta_1| & ... & \log|\sigma_{r_1+r_2}\eta_r| \end{vmatrix} \\ &= \frac{1}{\rho_{r_1+1}...\rho_{r_1+r_2}} 2^{-r_2} R. \end{aligned}$$

La dernière égalité est obtenue par ajouter les premières $r$ lignes à la dernière après multiplier la $j^{\text{ème}}$ par $N_j$.

Donc

$$\text{Vol}(D(1)) = 2^{r_1}(2\pi)^{r_2} \int_S 2^{-r_2} R d\mu = 2^{r_1}\pi^{r_2} R$$

car $\text{Vol}(S) = 1$.

La borne de $D(1)$ est $(N-1)$-paramètrisable car celle de $P$ l'est. Pour le voir, il faut justement remplacer $u$ par $u_1$ tel que $u = u_1^N$. □

**Théorème 4.3.** *Soient $\mathcal{C}$ une classe d'idéaux de $K$, $w$ le nombre des racines d'unité dans $U$ et $j(\mathcal{C}, t)$ le nombre des $\mathfrak{a} \in \mathcal{C}$ tels que $N(\mathfrak{a}) \leqslant t$, alors*

$$j(\mathcal{C}, t) = \frac{2^{r_1}(2\pi)^{r_2} R}{w\sqrt{disc(K/\mathbb{Q})}} + \mathcal{O}(t^{1-1/N}).$$

Démonstration. Soit $\mathfrak{b} \in \mathcal{C}^{-1}$, alors il y a une bijection

$$\{\mathfrak{a} \in \mathcal{C} | N(\mathfrak{a}) = t\} \longrightarrow \{\mathfrak{b}' \subset \mathfrak{b} | \mathfrak{b}' \text{ principal et } N(\mathfrak{b}') = tN(\mathfrak{b})\}$$

$$\mathfrak{a} \qquad \mapsto \qquad \mathfrak{a} \cdot \mathfrak{b}$$

grâce à la décomposition unique des idéaux.

Soit $l(\mathfrak{b}, t)$ le nombre des éléments de $\mathfrak{b}$ dont la norme $\leqslant tN(\mathfrak{b})$, alors par la bijection avant, on a

$$j(\mathcal{C}, t) = \frac{1}{w} l(\mathfrak{b}, t).$$

D'ailleurs, sous les notations de Lemme (4.1), on sait

$$l(\mathfrak{b}, t) = \lambda((t\mathfrak{b})^{1/N}, D(1), \Lambda)$$

où $\Lambda$ est le réseau correspondant à $\mathfrak{b}$ en observant immédiatement

$$(tN(\mathfrak{b}))^{1/N} D(1) = D(tN(\mathfrak{b})).$$

Maintenant on peut conclure en utilisant Lemme (4.1) et Proposition (4.2). □

Maintenant, soient $a_m$ le nombre d'idéaux de $K$ dont la norme est $m$ et $A_M := \sum_{m=1}^{M} a_m$, alors par le théorème, on a

**Corollaire 4.4.**

$$A_M = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}} M + \mathcal{O}(M^{1-1/N})$$

*où* $h = \#\mathcal{C}l(\mathcal{O}_K)$.

**Théorème 4.5.** *Finalement, on a la formule du nombre de classes pour un corps de nombres* $K$ *:*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}}$$

*où* $h = \#\mathcal{C}l(\mathcal{O}_K)$.

Démonstration. Mettons

$$f(s) := \sum_{m=1}^{\infty} (a_m - \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}}) m^{-s},$$

alors $f(s)$ converge pour $s > 1 - 1/N$ car

$$|\sum_{m=1}^{M} (a_m - \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}})| = |A_M - \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}} M| = \mathcal{O}(M^{1-1/N}).$$

(c.f. )

Donc pour $s > 1 - 1/N$, on a

$$\zeta_K(s) = f(s) + \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}} \zeta(s)$$

avec $\zeta(s)$ la fonction de Riemann-zêta, ainsi

$$\begin{aligned}\lim_{s\to 1^+}(s-1)\zeta_K(s) &= \lim_{s\to 1^+}(s-1) f(s) + \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{disc(K/\mathbb{Q})}} \cdot \lim_{s\to 1^+}(s-1)\zeta(s) \\ &= \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{\mathrm{disc}(K/\mathbb{Q})}}.\end{aligned}$$

□

**Corollaire 4.6.** *Soit* $K = \mathbb{Q}(\sqrt{D})$ *un corps quadratique imaginaire, alors le nombre de classes*

$$h \sim L(1,\chi)|D|^{1/2},$$

*où* $\chi$ *est le caractère primitif associé à* $K$*, i.e.*

$$\chi(p) = (\frac{D}{p}).$$

DÉMONSTRATION. (*esquisse*) Dans ce cas particulier, $R = 1$, $w = 1$ ou 2, $\mathrm{disc}(K/\mathbb{Q}) = |D|$ ou $4|D|$, et

$$\zeta_K(s) = \zeta(s)L(1, \chi)$$

par le produit d'Euler et le fait qu'il y a 2, 1, 0 primes de $\mathcal{O}_K$ dont la norme est $p$ si $(\frac{D}{p}) =$ 1, 0, -1. □

## 5. Borne inférieure de Siegel

Dans cette section, on introduit le théorème de Siegel sur le nombre de classes d'un corps quadratique imaginaire.

Soient $K = \mathbb{Q}(\sqrt{D})$ avec $D < 0$ sans facteurs carrés et $h(D)$ le nombre de classes de $K$, alors Siegel a énoncé le théorème célèbre :

**Théorème 5.1.** *Quelque soit $\varepsilon > 0$, on a*

$$h(D) >> |D|^{1/2-\varepsilon}.$$

Par le corollaire (4.6), ce théorème est équivalent à

**Théorème 5.2.** *Soit $\chi$ un caractère primitif mod $q$ ($q \in \mathbb{N}$ est un intègre quelconque). Alors $\forall \varepsilon > 0$, il existe une constante $c(\varepsilon)$ telle que*

$$L(1, \chi) > \frac{c(\varepsilon)}{q^{\varepsilon}}$$

DÉMONSTRATION. (*esquisse*) Cette preuve est d'après [**Go**]. Pour les propriétés des $L$-fonctions, contrôlez [**IK**].

Pour chaque $\varepsilon > 0$, il existe un caractère primitif $\chi'$ modulo $q'$ (où $q' \neq q$) et un $\beta$ (ils ne dépendent pas de $\chi$ !) tels que $1 - \varepsilon < \beta < 1$ et

$$\mu := \zeta(\beta)L(\beta, \chi')L(\beta, \chi)L(\beta, \chi'\chi) \leqslant 0.$$

C'est vrai car s'il n'y a pas de zéro dans $]1 - \varepsilon, 1[$ pour aucune $L(s, \chi)$, alors $\mu < 0$ si $1 - \varepsilon < \beta < 1$ car $\zeta(\beta) < 0$. Sinon on prend $\beta$ un tel zéro et $\chi'$ le caractère correspondant tel que $\mu = 0$.

Mettons

$$\begin{aligned} L(f, s) &:= \zeta(s)L(s, \chi')L(s, \chi)L(s, \chi'\chi) \\ &= \sum_n \lambda_f(n)n^{-s} \end{aligned}$$

Alors on sait bien $\lambda_f(n) \geqslant 0$. Soit $\eta(x)$ est une fonction sur $[0, +\infty[$ telle que

– $0 \leqslant \eta \leqslant 1$ ;
– $\eta(x) = 1$ pour $0 \leqslant x \leqslant 1$ ;
– $\eta(x) = 0$ pour $x \geqslant 2$.

Considérons la somme

$$Z(\beta, x) = \sum_n \frac{\lambda_f(n)}{n^{\beta}} \eta(\frac{n}{x}) \geqslant 1 \qquad (\text{ car } \lambda_f(1) = 1)$$

pour $\beta \leqslant 1$ assez proche et $x \geqslant 1$. Donc on a (par transforme de Mellin)

$$\begin{aligned} Z(\beta, x) &= \frac{1}{2\pi\sqrt{-1}} \int_{2-\sqrt{-1}\infty}^{2+\sqrt{-1}\infty} L(f, s+\beta) x^s \widetilde{\eta}(s) ds \\ &= L(f,\beta) + L(1,\chi')L(1,\chi)L(1,\chi'\chi)\widetilde{\eta}(1-\beta)x^{1-\beta} \\ &\quad + \frac{1}{2\pi\sqrt{-1}} \int_{\frac{1}{2}-\beta-\sqrt{-1}\infty}^{\frac{1}{2}-\beta+\sqrt{-1}\infty} L(f, s+\beta)\widetilde{\eta}(s) x^s ds, \end{aligned}$$

où $\widetilde{\eta}(s) = \int_0^\infty \eta(y) y^{s-1} dy$ est la transforme de Mellin de $\eta$.

Le dernier intégral est $<< q_1 q_2 x^{1/2-\beta}$. Alors on a

$$L(1,\chi')L(1,\chi)L(1,\chi'\chi)\widetilde{\eta}(1-\beta)x^{1-\beta} \geqslant 1 + \mathcal{O}(q_1 q_2 x^{1/2-\beta}).$$

Prenons $x = c(q_1 q_2)^4$ avec $c$ suffisamment grand, alors la terms à gauche est $> \frac{1}{2}$. Alors $\widetilde{\eta}(1-\beta) << (1-\beta)^{-1}$ car $\widetilde{\eta}(s)$ admet un pôle simple en $s=0$ avec le résidue 1. De plus, on a $L(1,\chi') << \log q'$ et $L(1,\chi'\chi) << \log(q'q)$ (c.f. ). En conséquence des faits, on a

$$L(1,\chi) >> (1-\beta)(q'q)^{-4(1-\beta)}(\log q'q)^{-2},$$

donc on a gagné tenant compte de $1-\varepsilon < \beta$. □

CHAPITRE 5

# Conclusion de la preuve

## 1. Composantes pré-spéciales élémentaires

**Définition 1.1.** Soit $S_0 \sqcup S_1 \sqcup ... \sqcup S_w$ une partition de $\{1, ..., n\}$ avec $w \geqslant 0$ et $S_i$ non-vide si $i \neq 0$. Soient $h_i \in \mathbb{H}$ pour chaque $i \in S_0$ un point quelconque, $s_i$ l'élément le plus petit de $S_i$ pour chaque $i \geqslant 1$ et $h_{ij} \in SL_2(\mathbb{R})$ pour chaque $j \in S_i$, $j \neq s_i$. Une *sous-variété linéaire* de $\mathbb{H}^n$ est une sous-variété de la forme

$$L(S_i, h_i, g_{ij}) := \{(\tau_1, ..., \tau_n) \in \mathbb{H}^n | \tau_i = h_i, i \in S_0, \tau_j = h_{ij}(\tau_{s_i}), i = 1, ..., w, j \in S_i, j \neq s_i\}.$$

Et il s'appelle une sous-variété linéaire *élémentaire* si $S_0 = \emptyset$.

**Remarque 1.2.** (1) Il est claire qu'une sous-variété linéaire est une composante complexe !

(2) Une sous-variété quasi-pré-spéciale est toujours linéaire.

**Lemme 1.3.** *Soit $X$ un produit des courbes modulaires, $V \subset X$ une sous-variété et $\mathcal{Z} := \pi^{-1}(V)$ comme avant. Alors toutes les sous-variétés linéaires maximales dans $\mathcal{Z}$ sont quasi-pré-spéciales.*

Démonstration. Pour $L$ une sous-variété linéaire maximale, comme elle est une composante complexe, elle est continue dans une composante complexe maximale $Y$. On a déjà montré que une telle $Y$ est toujours quasi-pré-spéciale (Ax-Lindermann), donc linéaire soi-même. Donc $L$ est quasi-pré-spéciale soi-même car toutes les sous-variétés quasi-pré-spéciales sont linéaires et que $L$ est maximale comme une sous-variété linéaire. □

Voici un corollaire immédiat :

**Corollaire 1.4.** *Avec les notations comme dans le lemme, les deux ensembles sont le même :*

$$\{\textit{sous-variétés linéaires maximales dans } \mathcal{Z}\}$$

*et*

$$\{\textit{sous-variétés quasi-pré-spéciales maximales dans } \mathcal{Z}\}.$$

On introduit une notion simplifiant le technique dans le suivant. Si $\mathcal{Z}$ contient $Y$, alors il contient tous les $gY$ ($g \in \Gamma$). On appelle l'union

$$\bigcup_{g \in \Gamma} gY$$

un *lieu*. Il est claire que l'image réciproque d'une sous-variété quasi-spéciale de $X$ est un *lieu quasi-pré-spécial*, et un tel lieu est l'union des translatés sous $\Gamma$ d'une sous-variété quasi-pré-spéciale. On a paraillement la notion du *lieu linéaire* et *lieu pré-spécial (élémentaire)*. Et le corollaire peut s'exprimer en moyen de :

**Corollaire 1.5.** *Avec les notations comme avant,*

$$\{\textit{lieux linéaires maximaux dans } \mathcal{Z}\} = \{\textit{lieux quasi-pré-spéciaux maximaux dans } \mathcal{Z}\}$$

**Proposition 1.6.** *Soit $X$ un produit des courbes modulaires, $V \subset X$ une sous-variété et $\mathcal{Z} := \pi^{-1}(V)$ comme avant. Alors il n'y a qu'un nombre fini des lieux pré-spéciaux élémentaires admettant une translaté qui est un lieu quasi-pré-spécial maximal dans $\mathcal{Z}$.*

Démonstration. $Z := \mathcal{Z} \cap \mathbb{F}$ comme avant. Grâce au corollaire au dessus, on peut transformer "quasi-pré-spécial" en "linéaire". L'ensemble des sous-variétés linéaires (élémentaires) est semi-algébrique comme il est un produit des copies de $SL_2(\mathbb{R})$, et ainsi définissable. D'autre part, pour un ensemble analytique $Y$,

$$Y \subset \mathcal{Z} \iff \exists \gamma \in \Gamma, \text{ tel que } \gamma Y \cap Z \text{ est de dimension pleine}$$

par Chapitre 3, Proposition (2.1). Donc l'ensemble des sous-variétés linéaires élémentaires admettant une translaté maximale parmi les sous-variétés linéaires contenues dans $\mathcal{Z}$ est définissable. Comme les sous-variétés linéaires maximales sont quasi-pré-spéciales, et ainsi correspondent aux points algébriques, cet ensemble est fini car il est définissable et dénombrables. □

**Corollaire 1.7.** *Soit $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires et $V \subset X$ une sous-variété, alors il n'y a qu'un nombre fini des sous-variétés spéciales élémentaires admettant une tranlations qui est maximale parmi les sous-variétés quasi-spéciales contenues dans $V$.*

## 2. La fin de la preuve

**Définition 2.1.** Pour $V \subset X$, *l'ensemble spécial* de $V$, noté comme $V^{sp}$, est l'union des sous-variétés spéciales de dimension strictement positives contenues dans $V$.

**Théorème 2.2.** *Soient $X = Y_1 \times ... \times Y_n$ un produit des courbes modulaires et $V \subset X$ une sous-variété de $X$ définie sur un corps de nombres $K$ qui contient un corps de définition pour $X$. Si $V^{sp}$ est une variété, alors $V - V^{sp}$ ne contient qu'un nombre fini des points spéciaux.*

Démonstration. Mettons $\mathcal{Z} := \pi^{-1}(V)$, alors $\mathcal{Z}^{alg}$ consiste de $\mathcal{Z}^{ps} := \pi^{-1}(V^{sp})$ et d'autres lieux quasi-pré-spéciaux qui contiennent aucun point pré-spécial. Mettons $Z^{ps} := \mathcal{Z}^{ps} \cap \mathbb{F}$, on a alors $Z^{alg} = \mathcal{Z}^{alg} \cap \mathbb{F}$, et

$$N_2^{\text{pré-spé}}(Z - Z^{ps}, T) = N_2^{\text{pré-spé}}(Z - Z^{alg}, T) \leqslant N_2(Z - Z^{alg}, T) \leqslant c(Z, 2, \varepsilon)T^{\varepsilon}$$

où $N_2^{\text{pré-spé}}(Z - Z^{ps}, T) := \#\{\text{points pré-spéciaux dans } Z - Z^{ps}\}$.

Supposons que $Z - Z^{ps}$ contient un point pré-spécial $u$ de complexité $\Delta = \Delta(u)$. Alors $x = \pi(u) \in V - V^{sp}$ est spécial et Chapitre 4, Proposition (1.4) nous dit qu'il a au moins

$$c_{deg}(X)\Delta^{1/2-\nu}$$

conjugaisons $x'$ qui sont aussi dans $V - V^{sp}$ ($\forall \nu > 0$). Les conjugaisons ont les images réciproques distinctes $u' \in Z - Z^{ps}$ ayant la complexité

$$\Delta(u') = \Delta(u) = \Delta$$

et donc

$$H(u') \leqslant c_{hauteur}(X)\Delta$$

par Chapitre 4, Proposition (1.3). Mettons $T := c_{sp}(X)\Delta$, alors on a

$$\frac{c_{sp}(X)}{c_{hauteur}(X)^{1/2-\nu}} T^{1/2-\nu} \leqslant N_2^{pré\text{-}spé}(Z - Z^{ps}, T) \leqslant c(Z, 2, \varepsilon)T^{\varepsilon}.$$

Choisissons $\nu$, $\varepsilon$ tels que $1/2 - \nu > \varepsilon$, alors pour $T$ assez grand, i.e. $\Delta$ assez grand, l'inéquality échoue. Donc $\Delta(u)$ est borné pour un point pré-spécial dans $Z - Z^{ps}$, et les points spéciaux de $V - V^{sp}$ viennent un ensemble fini. □

Maintenant, on va conclure. Tout d'abord on se ramène au cas où $V$ est définie sur $\overline{\mathbb{Q}}$ grâce au fait que tous les points algébriques sont définis sur $\overline{\mathbb{Q}}$. On fait la récurrence sur $\dim(X)$. Le cas $\dim(X) = 1$ est immédiat. En général, si $n = \dim(X)$, on peut supposer $V$ est propre dans $X$ grâce au théorème au dessus. Par Corollaire (1.7), on peut fixer une sous-variétés spéciales élémentaires $Y$ et montrer qu'elle n'admet qu'un nombre fini des translatés qui est une sous-variété spéciale maximale dans $V$.

Mettons $m := \#S_0$ et

$$V' := \{s \in \mathbb{C}^m | s \times Y \subset V\},$$

alors $V'$ est une sous-variétés de $\mathbb{C}^m$, et les translatés qu'on veut bijectivement correspondent aux points spéciaux de $V' - (V')^{sp}$ (sinon la translaté ne serait pas maximale). Mais $m < n$, donc par récurrence, $V' - (V')^{sp}$ n'a qu'un nombre fini des points spéciaux. Et ceci permet de conclure finalement !

# Bibliographie


[BG] E.Bombieri et W.Gubler, *Heights in diophantine geometry*, CUP, 2006.

[DM] L.van den Dries et C.Miller, *Geometric categories and o-minimal structures*, DMJ **84**(1996), 497-540.

[Go] D.M.Goldfeld, *A simple proof of Siegel's theorem*, Proc.Nat.Acad.Sci.USA **71**(1974), 1055.

[IK] H.Iwaniec et E.Kowalski, *Analytic number theory*, AMS Colloquium Publications **53**, AMS, 2004.

[La] S.Lang, *Algebraic number theory (2nd edition)*, GTM **110**, Springer-Verlag, 1994.

[Mi] J.S.Milne, *Modular functions and modular forms*, disponible à télécharger de http ://www.jmilne.org/math/CourseNotes/MF.pdf

[Ne] J.Neukrich, *Algebraic number theory*, Springer-Verlag, 1999.

[P1] J.Pila, *O-minimality and the André-Oort conjecture for* $\mathbb{C}^n$, Annuals Math. **173**(2011), 1779-1840.

[P2] J.Pila, *On the algebraic points of a definable set*, Selecta Math. N.S. **15**(2009), 151-170.

[P3] J.Pila, *Rational points of definable sets and results of Andre-Oort–Manin-Mumford type*, IMRN 2009(2009), 2476-2507.

[PT1] J.Pila et J.Tsimerman, *The André-Oort conjecture for the moduli space of Abelian surfaces*, Compositio Math., à apparaître, pré-print disponible à télécharger de http ://arxiv.org/pdf/1106.4023v1.pdf.

[PT2] J.Pila et J.Tsimerman, *Ax-Lindermann for* $\mathcal{A}_g$, pré-print disponible à télécharger de http ://arxiv.org/pdf/1206.2663v1.pdf

[PW] J.Pila et A.J.Wilkie, *The rational points of a definable set*, DMJ **133**(2006), 591-616.

[PZ] J.Pila et U.Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Rend. Lincei Mat. Appl. **19**(2008), 149-162.

[S1] J.H.Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, 1986.

[S2] J.H.Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM **151**, Springer-Verlag, 1999.

[Ul] E.Ullmo, *Quelques applications du théorème d'Ax Lindemann hyperbolique*, pré-print disponible à télécharger de http ://www.math.u-psud.fr/ ullmo/Prebublications/cordAxLind.pdf

[UY] E.Ullmo et A.Yafaev, *The Hyperbolic Ax Lindemann in the compact case*, pré-print disponible à télécharger de http ://www.math.u-psud.fr/ ullmo/Prebublications/AxLindemannNew.pdf