UNIVERSITÉ DE MONTRÉAL

La mesure de Mahler d'une forme de Weierstrass

par

Antoine Giard

Maîtrise soumise à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

Faculté des Arts et Sciences
Département de Mathématiques et Statistique

5 juin 2019

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

La mesure de Mahler d'une forme de Weierstrass

présenté par

Antoine Giard

a été évalué par un jury composé des personnes suivantes :

Abraham Broer
(président-rapporteur)

Matilde Lalín
(directrice de recherche)

Andrew Granville
(membre du jury)

Mémoire accepté le :

« *On fait des maths ?* »

Fabrice Nonez

Sommaire

Ce mémoire a pour but de donner une introduction simple et brève à la mesure de Mahler et ses liens avec les fonctions-L de courbes elliptiques. Le point culminant de cette théorie se cache dans les conjectures de Bloch-Beĭlinson que nous tentons d'expliquer à la fin du chapitre 2, les deux premiers chapitres servant principalement à développer la matière nécessaire à leur compréhension et à introduire le problème principal de ce mémoire qui est de trouver une relation entre la mesure de Mahler de $y^2+4xy+2y-x^3$ et la fonction-L de la courbe elliptique associée.

À cet effet, nous remarquons que la relation conjecturée par D. Boyd [1] est en fait fausse mais étudions tout de même les cycles d'homologie et les chemins d'intégration associés aux courbes elliptiques $y^2+4xy+2y-x^3=0$ et $(1+x)(1+y)(x+y)+2xy=0$.

Mots-clés : Mesure de Mahler, courbes elliptiques, valeurs spéciales de fonctions-L, polynôme tempéré, polygone de Newton, régulateur elliptique

Summary

This master's thesis goal is to give a simple and brief introduction about Mahler measure and its connections with elliptic curves L-functions. This theory culminates with the Bloch-Beĭlinson conjectures which we try to explain at the end of chapter 2, the first two chapters serving to introduce the necessary requirements to understand them and as a stepping stone to this master's main question which is to find a link between the Mahler measure of $y^2 + 4xy + 2y - x^3$ and the L-function associated to it.

For this purpose, we see that the conjectured relation given by D. Boyd [1] is false but we still study the homology cycles and integration paths associated to the elliptic curves $y^2 + 4xy + 2y - x^3 = 0$ and $(1 + x)(1 + y)(x + y) + 2xy = 0$.

Mots-clés : Mahler measure, elliptic curve, special values of L-functions, tempered polynomial, Newton polygon, elliptic regulator

Remerciements

Deux ans, c'est pas très long. Par contre, j'ai tout de même l'impression qu'une infinité dénombrable d'événements se sont passés au cours de mon mémoire. Au début de ce « périple » , j'étais jeune, naïf, et stupide. Aujourd'hui, je suis jeune, naïf, stupide, et j'ai écrit un mémoire. Il serait cruel de ne pas remercier ici les personnes ayant contribué à ce changement.

Sans l'ombre d'un doute, le remerciement le plus important est à l'égard de ma directrice de recherche, Matilde Lalín. Sa patience infinie, sa motivation non-bornée et ses connaissances sans fin m'ont été d'une aide incroyable, même si ça me donnait un petit complexe d'infériorité. Un énorme merci !

J'aimerais aussi remercier les professeur.e.s du DMS pour avoir développé ma maturité mathématique. Un merci tout particulier va à l'endroit de Yvan Saint-Aubin et Marlène Frigon pour être des modèles en ce qui a trait à l'enseignement.

Merci à ma famille pour m'avoir supporté moralement et m'avoir permis de suivre ma passion.

Même s'ils étaient plus souvent qu'autrement une source de distraction constante, je me dois de remercier mes ami.e.s qui m'ont permis de terminer mon mémoire encore intact psychologiquement et psychiquement. Un gros merci à Raphaël pour ses *sick meelz combos* et pour avoir été avec moi 90% de ces deux dernières années, Justin pour les nombreuses discussions mathématiques et philosophiques et pour avoir prouvé qu'on peut être incroyablement bon en mathématique même avec un passé d'actuaire (Non à l'élitisme !), Julie pour sa joie de vivre hors pair et pour être une présence ineffablement rassurante à tout moment, Paul pour ses blagues de mauvais goût (que j'adore !), Vanessa pour ses nombreuses histoires croustillantes égayant mes journées, Philippe pour être la personne la plus drôle que je connaisse et Youness, Jézabel, Laurie et Charlie pour parler de mathématiques avec moi même en ayant quasiment aucun *background* et pour me sortir de mon univers de la façon la plus intéressante possible. Une mention spéciale à Fabrice pour ses conversations nocturnes et pour incarner la passion même. Je suis persuadé qu'il est responsable à 75% (statistique non-significative) de mon développement mathématique, même s'il me parlait principalement d'ultrafiltres. Je crois avoir légèrement compris ce concept après deux ans.

Table des matières

Table des figures

Introduction

La mesure de Mahler a connu un essor assez important à la fin des années 90 avec l'article *Mahler's Measure and Special Values of L-functions* de David Boyd [1]. Plusieurs résultats numériques ont été présentés reliant la mesure de Mahler de polynômes avec la fonction-L d'une courbe elliptique associée. Une théorie riche et surprenante a été développée autour de ces calculs numériques, mais peu de formules s'avéraient être prouvées. Plusieurs de ces conjectures ont été démontrées au cours des années suivantes sans toujours avoir une preuve de la théorie dans son ensemble.

La mesure de Mahler se trouve être en lien avec une panoplie de domaines mathématiques dépendamment du type de polynôme. Ce mémoire se concentre principalement sur les relations entre la mesure de Mahler et les courbes elliptiques lorsque le polynôme considéré est à deux variables.

À cet effet, le premier chapitre se divise en deux parties. En premier lieu, une introduction sommaire à la géométrie algébrique classique est donnée avec les théorèmes importants associés. Même si notre objet d'étude ne représente qu'un cas particulier de l'introduction (les courbes), nous présentons tout de même les concepts dans leur généralité puisque la théorie se veut en fait plus simple lorsque vue de manière générale.

La deuxième partie du premier chapitre se veut une introduction aux courbes elliptiques sur $\mathbb{Q}$ et $\mathbb{C}$ principalement. Il se trouve que sur ces deux corps, les courbes elliptiques se veulent débordantes de propriétés intéressantes et leur structure relativement simple. Encore une fois, nous avons dû faire un choix afin de ne pas alourdir ce mémoire, mais nous référons les plus curieux.se à l'excellent livre de Silverman [2] pour une introduction plus générale aux courbes elliptique sur d'autres corps (corps finis ou $\mathbb{Q}_p$ par exemple).

Le deuxième chapitre offre une initiation à la mesure de Mahler et ses liens avec les courbes elliptiques. Une approche plutôt historique est tout d'abord donnée pour ensuite complètement définir la mesure de Mahler et ses propriétés. Sans surprises, l'accent est principalement mis sur la mesure de Mahler de polynômes à deux variables. Une

intuition des conjectures de Bloch-Beĭlinson est ensuite donnée, établissant clairement le lien fondamental de ce mémoire.

Le troisième chapitre a pour but d'étudier le problème de maîtrise donné qui était de donner une relation conjecturée par Boyd entre la mesure de Mahler de $y^2+4xy+2y-x^3$ et la fonction-L du polynôme associé. Il se trouve que la relation s'avère fausse, mais cela n'empêche pas l'étude du polynôme et des propriétés de sa mesure de Mahler. Les étapes importantes à l'étude de la relation seront données ce qui permettra avec un peu de chance d'obtenir un théorème sur la forme de la mesure de Mahler de $y^2+4xy+2y-x^3$ et ses liens avec la fonction-L associée (si ils existent).

Les sources principales utilisées sont [2] pour le chapitre 1 et [3] , [4] pour le chapitre 2.

Chapitre 1

Introduction aux courbes elliptiques

> Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik.
> Les mathématiques sont la reine des sciences et la théorie des nombres est la reine des mathématiques.
>
> Carl Friedrich Gauss

Avant de nous attaquer à la mesure de Mahler, il est primordial d'introduire un minimum la théorie reliée aux courbes elliptiques. À cet effet, la première section étudie de façon générale certains concepts fondamentaux des variétés et des courbes algébriques. Ceci aura l'avantage de donner une vision plus claire et plus naturelle à l'étude des courbes elliptiques. La deuxième section se concentre sur les propriétés propres aux courbes elliptiques et des concepts nécessaires à l'étude de la mesure de Mahler.

Ce chapitre suit en majorité [2]. Les preuves des théorèmes peuvent donc se trouver dans cette référence.

1.1 Géométrie algébrique : Variétés

1.1.1 Définitions

1.1.1.1 Le cas affine

Les variétés algébriques se divisent en deux grandes catégories interreliées : les variétés affines et les variétés projectives. Nous commencerons par définir les variétés affines.

Définition 1. On définit le n-espace affine (sur K un corps) comme

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) := \{(x_1, ..., x_n) \ : \ x_i \in \bar{K}\},$$

où $\bar{K}$ est la clôture algébrique de K. De même, l'ensemble des points K-rationnels de $\mathbb{A}(\bar{K})$ est

$$\mathbb{A}^n(K) := \{(x_1, ..., x_n) \ : \ x_i \in K\}.$$

Les plus perspicaces diront que ces ensembles ressemblent énormément à $\bar{K}^n$ et K^n respectivement, et ils auraient totalement raison. Le problème ici est que nous n'allons pas voir $\mathbb{A}^n(\bar{K})$ comme un anneau (ce qui est le cas de $\bar{K}^n$) mais comme une variété affine (ou plus généralement un schéma affine, mais nous n'entrerons pas dans le détails ici). Par exemple, les morphismes entre espaces affines ne seront pas des morphismes d'anneau. Comme nous nous intéressons à d'autres propriétés algébriques du même ensemble, nous utilisons la notation $\mathbb{A}^n$.

Petite remarque en passant : Si $G = \mathrm{Gal}(\bar{K}/K)$ est le groupe de Galois absolu de K, alors on a une action naturelle de G sur $\mathbb{A}^n$ qui consiste à appliquer $\sigma \in G$ à chaque composante, i.e.

$$(x_1, ..., x_n)^\sigma = (x_1^\sigma, ..., x_n^\sigma).$$

On remarque que $\mathbb{A}^n(K)$ est exactement l'ensemble des points fixes de $\mathbb{A}^n$ sous cette action, i.e.

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n \ : \ P^\sigma = P \ , \ \forall \sigma \in G\}.$$

La géométrie algébrique étudie principalement les zéros de polynômes sur un certain anneau polynomial. Nous considérons donc $\bar{K}[X] = \bar{K}[X_1, ..., X_n]$ l'anneau des polynômes à n-variables sur $\bar{K}$.

Définition 2. (i) Soit $I \subseteq \bar{K}[X]$ un idéal de $\bar{K}[X]$. On lui associe l'ensemble

$$V_I := \{P \in \mathbb{A}^n(\bar{K}) \ : \ f(P) = 0, \ \forall f \in I\},$$

i.e. l'ensemble des points s'annulant sur I. On dit que $V \subseteq \mathbb{A}^n(\bar{K})$ est un ensemble algébrique affine si $V = V_I$ pour un certain idéal I.
(ii) Soit $V \subseteq \mathbb{A}^n(\bar{K})$ un sous-ensemble. Alors l'idéal de V est

$$I(V) := \{f \in \bar{K}[X] \ : \ f(P) = 0, \ \forall P \in V\}.$$

(iii) On dit que V est défini sur K si $I(V) = (f_1, ..., f_k)$ avec $f_i \in K[X]$ et on note V/K. Si V est défini sur K, on dénote l'ensemble des points K-rationnels de V comme

$$V(K) := V \cap \mathbb{A}^n(K).$$

De même on définit

$$I(V/K) := \{f \in K[X] \ : \ f(P) = 0, \ \forall P \in V\} = I(V) \cap K[X].$$

Nous avons passé sous le tapis une petite subtilité concernant la définition de $I(V)$. En effet, par le théorème de la base d'Hilbert, $K[X]$ est noethérien et donc tout idéal est de type fini, d'où le fait que $I(V) = (f_1, ..., f_k)$.

Notons aussi que $P \in V_I$ si et seulement si P s'annule sur un ensemble de générateurs de I. Cela permet entre autres de simplifier l'étude V_I et de $I(V)$ en ne considérant qu'un nombre fini de possibilités. Aussi, si $I(V) = (f_1, ..., f_k)$, étudier $I(V)$ revient à étudier les solutions à

$$f_1(X) = ... = f_k(X) = 0.$$

Lorsque $K = \mathbb{Q}$, ceci revient à un système d'équations diophantiennes, sujet extrêmement étudié en théorie des nombres.

Il est très fréquent en mathématiques de vouloir étudier un certain ensemble par ses « parties irréductibles ». Ceci mène naturellement à la définition suivante.

Définition 3. Soit V un ensemble algébrique affine. On dit que V est une variété affine si $I(V)$ est un idéal premier de $\bar{K}[X]$. Si de plus V est défini sur K, l'anneau des

coordonnées affines est

$$K[V] := \frac{K[X]}{I(V/K)}.$$

Le corps de fractions de cet anneau est dénoté par $K(V)$ et appelé le corps de fonctions sur V/K.

Intuitivement, un ensemble algébrique affine est une variété si elle ne peut pas être séparée en deux ensembles algébriques non-triviaux.

Définition 4. Soit V une variété algébrique affine. La dimension de V, notée $\dim(V)$ est le degré de transcendance de $\bar{K}(V)$ sur $\bar{K}$.

Dans le cas le plus simple, nous avons que $\mathbb{A}^n$ est de dimension n puisque $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, ..., X_n)$. Notre objet d'étude, les courbes elliptiques, sont des variétés de dimension 1. En général, une courbe est une variété de dimension 1.

Comme en géométrie différentielle, la géométrie algébrique s'intéresse au concept de variétés lisses. Nous voulons donc une définition qui semble une extension naturelle de cette notion.

Définition 5. Soit V une variété, $P \in V$ et $I(V) = (f_1, ..., f_m)$. Alors on dit que V est lisse en P si la matrice de dimension $m \times n$

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

est de rang $n - \dim(V)$. Si ce n'est pas le cas, on dit que P est un point singulier de V. Si V est lisse en tout point, on dit que V est lisse.

Dans la majorité de nos cas d'intérêt, nous étudierons des variétés définies par un unique polynôme non-constant $f(X_1, ..., X_n)$. On remarque que dans ce cas V est de dimension $n - 1$ et que la « matrice Jacobienne » associée à P est de rang 1 si et seulement si

$$\frac{\partial f}{\partial X_1} = ... = \frac{\partial f}{\partial X_n} = 0.$$

Par exemple, considérons la variété définie par

$$V_1 : \ Y^2 = X^3 - 1.$$

Un point $P \in V_1$ est singulier si et seulment si

$$3X^2 = 2Y = 0,$$

et donc V_1 est lisse. Par contraste, la variété

$$V_2 : \ Y^2 = X^3 - X^2$$

a $(0,0)$ comme point singulier. Cette singularité se voit géométriquement en traçant le graphe de cette courbe, puisque l'origine possède deux tangentes distinctes.

Soit V une variété affine et $P \in V$. On définit l'idéal

$$M_P := \{f \in \bar{K}[V] \ : \ f(P) = 0\}.$$

On remarque que M_P est un idéal maximal de $\bar{K}[V]$ puisque l'on a un isomorphisme

$$\begin{aligned} \phi\colon \bar{K}[V]/M_P &\to \bar{K} \\ f &\mapsto f(P). \end{aligned}$$

Définition 6. L'anneau local de V en P, noté $\bar{K}[V]_P$ est la localisation de $\bar{K}[V]$ en l'idéal M_P, i.e.

$$\bar{K}[V]_P := \{F \in \bar{K}(V) \ : \ \text{Il existe } f, g \in \bar{K}[V] \text{ tels que } F = f/g \text{ et } g(P) \neq 0\}.$$

Ceci nous donne toutes les fonctions $F \in \bar{K}(V)$ définies en P : Si $F = f/g \in \bar{K}[V]_P$, on définit

$$F(P) = \frac{f(P)}{g(P)}.$$

Ceci est bien défini puisque $g(P) \neq 0$.

1.1.1.2 Le cas projectif

Intuitivement, l'espace projectif peut être vu comme un « collage » de plusieurs espaces affines et ici nos points seront les lignes de $\mathbb{A}^{n+1}$. Les espaces projectifs nous permettent de formaliser le concept de point à l'infini. L'idée de tels espaces a commencé historiquement par l'étude de la perspective en peinture (Voir [5]).

Définition 7. On définit le plan projectif $\mathbb{P}^n$ par

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) := (\mathbb{A}^{n+1} \backslash \{0\}) / \sim,$$

où deux points $(x_0, ..., x_n), (y_0, ..., y_n)$ sont équivalents s'il existe $c \in \bar{K}^*$ tel que

$$(x_0, ..., x_n) = c(y_0, ..., y_n).$$

On dénote la classe d'équivalence

$$\{c(x_0, ..., x_n) \ : \ c \in \bar{K}^*\}$$

par $[x_0, ..., x_n]$. Les $x_0, ..., x_n$ sont appelés les coordonnées homogènes du point.
De la même façon, on définit

$$\mathbb{P}^n(K) := \{[x_0, ..., x_n] \in \mathbb{P}^n \ : \ x_0, ..., x_n \in K.\}$$

Comme dans le cas affine, si on pose $G = \mathrm{Gal}(\bar{K}/K)$ on remarque que

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n \ : \ P^\sigma = P \ , \ \forall \sigma \in G\}.$$

Définition 8. Un polynôme $f \in \bar{K}[X_1, ..., X_n]$ est dit homogène de degré d si pour tout $c \in \bar{K}$ on a

$$f(cx_0, ..., cx_n) = c^d f(x_0, ..., x_n).$$

Un idéal $I \subseteq \bar{K}[X_1, ..., X_n]$ est homogène s'il est engendré par des polynômes homogènes. Plus intuitivement, un polynôme est homogène de degré d s'il est la somme de monômes de degré d.

Si f est un polynôme homogène, on peut se demander pour quels $P \in \mathbb{P}^n$ on a $f(P) = 0$ (puisque f est homogène, on peut considérer n'importe quel point dans la classe d'équivalence de P). L'approche est similaire au cas affine.

Définition 9. (i) Soit $I \subseteq \bar{K}[X]$ un idéal homogène de $\bar{K}[X]$. On lui associe l'ensemble

$$V_I := \{P \in \mathbb{P}^n \ : \ f(P) = 0 \ \forall f \in K[X] \ \ f \text{ homogène}\},$$

On dit que $V \subseteq \mathbb{P}^n(\bar{K})$ est un ensemble algébrique projectif si $V = V_I$ pour un certain idéal homogène I.
(ii) Soit $V \subseteq \mathbb{P}^n(\bar{K})$ un sous-ensemble. Alors l'idéal (homogène) $I(V)$ de V est l'idéal engendré par

$$I(V) := \{f \in \bar{K}[X] \ : \ f(P) = 0, \ \forall P \in V, \ f \text{ homogène}\}.$$

(iii) On dit que V est défini sur K si $I(V) = (f_1, ..., f_k)$ avec $f_i \in K[X]$ homogènes et

on note V/K. Si V est défini sur K, on dénote l'ensemble des points K-rationnels de V comme

$$V(K) := V \cap \mathbb{P}^n(K).$$

De même, $I(V/K)$ est l'idéal engendré par

$$\{f \in K[X] \ : \ f(P) = 0, \ \forall P \in V, \ f \text{ homogène}\} = I(V) \cap K[X].$$

Tout comme le cas affine, nous avons une notion de « partie irréductible » d'un ensemble algébrique projectif.

Définition 10. Un ensemble algébrique projectif est une variété projective si $I(V)$ est un idéal premier homogène de $\bar{K}[X]$.

Comme mentionné au début de cette section, il y a un lien fondamental entre les ensembles affines et ceux projectifs, notamment puisque $\mathbb{P}^n$ est obtenu en « collant » $n+1$ $\mathbb{A}^n$ entre eux. Plus rigoureusement, on a des inclusions pour $0 \leq i \leq n$,

$$\begin{aligned} \phi_i \colon \mathbb{A}^n &\to \mathbb{P}^n \\ (x_1, ..., x_n) &\mapsto [x_1, ..., x_{i-1}, 1, x_i, ..., x_n]. \end{aligned}$$

L'image de ϕ_i est le complémentaire de l'hyperplan

$$H_i := \{[x_0, ..., x_n] \in \mathbb{P}^n \ : \ x_i = 0\}.$$

On obtient donc une bijection

$$\begin{aligned} \phi_i \colon \mathbb{A}^n &\to \mathbb{P}^n \backslash H_i \\ (x_1, ..., x_n) &\mapsto [x_1, ..., x_{i-1}, 1, x_i, ..., x_n], \end{aligned}$$

avec inverse donné par

$$\begin{aligned} \phi_i^{-1} \colon \mathbb{P}^n \backslash H_i &\to \mathbb{A}^n \\ [x_0, ..., x_n] &\mapsto \left(\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i} \right). \end{aligned}$$

Si V est un ensemble algébrique projectif, par $V \cap \mathbb{A}^n$ nous faisons référence à $\phi_i^{-1}(V \cap U_i)$ pour un certain i fixé (très souvent ce sera $i = n$). Donc $V \cap \mathbb{A}^n$ permet de passer d'un ensemble algébrique projectif vers un ensemble affine.

Il se trouve que $V \cap \mathbb{A}^n$ est un ensemble algébrique affine avec idéal

$$I(V \cap \mathbb{A}^n) := \{f(Y_0, ..., Y_{i-1}, 1, Y_{i+1}, ..., Y_n) \ : \ f(X_0, ..., X_n) \in I(V)\}.$$

En fait, le processus d'ajouter un 1 à la i-ème variable de f est appelé la déhomogénéisation de f par rapport à la variable X_i. Ceci permet donc de passer d'un polynôme à $n+1$ variables à un polynôme à n variables. On remarque que $I(V \cap \mathbb{A}^n)$ n'est nul autre que l'idéal des polynômes déhomogénéisés de $I(V)$.

Le processus inverse appelé l'homogénéisation de f par rapport à X_i est donné par

$$f^*(X_0, ..., X_n) := X_i^d f\left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right),$$

où $d = \deg(f)$. De façon plus pratique, l'homogénéisation de f prend le polynôme f et ajoute la variable X_i à chaque monôme de f jusqu'à temps que chaque monôme soit de degré d. Par exemple, l'homogénéisation de

$$Y^2 = X^3 - X - 1$$

est

$$Y^2 Z = X^3 - XZ^2 - Z^3.$$

Avec ce point de vue, chaque ensemble algébrique projectif V est un « collage » des ensembles algébriques affines $\phi^{-1}(V \cap U_0), ..., \phi^{-1}(V \cap U_n)$.

Nous avons vu que nous pouvons passer d'un ensemble algébrique projectif vers un ensemble algébrique affine grâce à ϕ_i^{-1}. Le processus inverse est aussi possible.

Définition 11. Soit V un ensemble algébrique affine avec idéal $I(V)$ et identifions V à l'ensemble projectif $\phi_i(V)$. Alors la fermeture projective $\bar{V}$ de V est l'ensemble algébrique projectif associé à l'idéal homogène $I(\bar{V})$ engendré par

$$\{f^*(X) \ : \ f \in I(V)\}.$$

Proposition 12. (i) Soit V une variété affine. Alors $\bar{V}$ est une variété projetive et $V = \bar{V} \cap \mathbb{A}^n$.

(*ii*) Soit V une variété projective. Alors $V \cap \mathbb{A}^n$ est une variété affine et soit

$$\overline{V \cap \mathbb{A}^n} = \emptyset \quad \text{ou} \quad \overline{V \cap \mathbb{A}^n} = V.$$

(*iii*) Soit V une variété affine. Alors V est définie sur K si et seulement si $\bar{V}$ l'est.
(*iv*) Soit V une variété projective. Alors V est définie sur K si et seulement si $V \cap \mathbb{A}^n$ l'est.

Nous terminons cette section en utilisant $V \cap \mathbb{A}^n$ pour définir certaines propriétés sur les variétés projectives.

Définition 13. Soit V/K une variété projective et soit $\mathbb{A}^n \subset \mathbb{P}^n$ tel que $V \cap \mathbb{A}^n \neq \emptyset$.
(*i*) La dimension de V, notée $\dim(V)$, est la dimension de $V \cap \mathbb{A}^n$.
(*ii*) Le corps de fonctions de V, noté $K(V)$, est le corps de fonctions de $V \cap \mathbb{A}^n$. Notons que cette définition ne dépend pas de la carte affine $\mathbb{A}^n \subset \mathbb{P}^n$ choisie puisque tous les corps de fonctions résultants seront isomorphes.
(*iii*) Soit $P \in V$ tel que $P \in \mathbb{A}^n$ (P est élément de la carte affine choisie). Alors on dit que V est lisse en P si $V \cap \mathbb{A}^n$ est lisse en P et on dit que V est singulier en P dans le cas contraire.
(*iv*) Soit $P \in V$ tel que $P \in \mathbb{A}^n$. L'anneau local de V en P, noté $\bar{K}[V]_P$, est l'anneau local de $V \cap \mathbb{A}^n$ en P. On dit que $F \in \bar{K}(V)$ est définie en P si $F \in \bar{K}[V]_P$.

Lorsque $V = C$ est une courbe et que P est un point lisse, il se trouve que $\bar{K}[C]_P$ est un anneau de valuation discrète. Sa valuation normalisée est définie comme

$$\begin{aligned} \mathrm{ord}_P \colon \bar{K}[C]_P &\to \{0, 1, 2, ...\} \cup \{\infty\} \\ f &\mapsto \sup\{d \in \mathbb{Z} \ : \ f \in M_P^d\}. \end{aligned}$$

On étend cette valuation à tout $\bar{K}(C)$ en posant $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.

Un fonction $t \in \bar{K}(C)$ avec $\mathrm{ord}_P(t) = 1$ est appelée une uniformisante de C en P.

Dans les sections suivantes, nous allons nous concentrer sur les variétés affines et projectives puisqu'elles représentent les « ensembles irréductibles » de la géométrie algébrique.

1.1.2 Fonctions entre variétés

Dans cette section nous mentionnons brièvement les fonctions rationnelles entre variétés et leurs propriétés. Ce mémoire utilise seulement un cas particulier de ces fonctions, celles sur les courbes, ou plus précisément les isogénies entre courbes elliptiques. Nous tenons toutefois à définir les concepts dans leur généralité pour avoir une vue d'ensemble plus claire.

Définition 14. Soit $V_1, V_2 \subseteq \mathbb{P}^n$ des variétés projectives. Une application rationnelle entre V_1 et V_2 est une application de la forme

$$\phi \ : \ V_1 \to V_2, \quad \phi = [f_0, ..., f_n]$$

telle que si les fonctions $f_0, ..., f_n \in \bar{K}(V_1)$ sont toutes définies en $P \in V_1$, alors

$$[f_0(P), ..., f_n(P)] \in V_2.$$

S'il existe $\lambda \in \bar{K}^*$ tel que

$$\lambda f_0, ..., \lambda f_n \in K(V_1),$$

alors on dit que ϕ est définie sur K.

Remarquons que cette définition ne mentionne rien sur ce qu'il se passe si $f_0, ..., f_n$ ne sont pas définies en un point $P \in V_1$. Or, puisque nous travaillons dans un espace projectif, nous pouvons multiplier toutes nos fonctions $f_0, ..., f_n$ par un même scalaire sans ne rien changer. Nous utilisons ce concept pour définir ϕ en plus de points.

Définition 15. Une application rationnelle

$$\phi \ : \ V_1 \to V_2, \quad \phi = [f_0, ..., f_n]$$

est définie (ou régulière) en $P \in V_1$ s'il existe $g \in \bar{K}(V_1)$ tel que $gf_0, ..., gf_n$ sont définies en P et

$$[gf_0(P), ..., gf_n(P)] \neq 0.$$

On pose alors

$$\phi(P) = [gf_0(P), ..., gf_n(P)].$$

Une application rationnelle définie en tout point est appelé en morphisme.

Les applications rationnelles auront la même utilité que les morphismes des structures algébriques. Il est donc naturel de considérer des isomorphismes entre variétés.

Notons que si $V_1/K, V_2/K$ sont deux variétés et si $\phi \ : \ V_1 \to V_2$ est un morphisme, alors ϕ induit un morphisme d'anneau

$$\begin{aligned} \phi^* \colon K[V_2] &\to K[V_1] \\ f &\mapsto f \circ \phi. \end{aligned}$$

Cette correspondance est même fonctorielle. À partir de maintenant, lorsque ϕ est un morphisme de variétés, ϕ^* dénote le morphisme d'anneau associé.

Définition 16. Soient V_1, V_2 des variétés projectives. On dit que V_1 est isomorphe à V_2, noté $V_1 \cong V_2$, s'il existe des morphismes

$$\phi \ : \ V_1 \to V_2 \quad , \quad \psi \ : V_2 \to V_1$$

tels que $\phi \circ \psi$ et $\psi \circ \phi$ sont respectivement l'identité sur V_2 et l'identité sur V_1. On dit que V_1/K et V_2/K sont isomorphes sur K si ϕ et ψ peuvent être définies sur K.

Heureusement, il se trouve que dans notre cas d'étude, i.e. les courbes, nous n'avons pas à nous préoccuper des points où ϕ n'est pas définie.

Proposition 17. Soit C une courbe, $V \subset \mathbb{P}^n$ une variété projective, $\phi \ : \ C \to V$ une application rationnelle et $P \in C$ un point où C est lisse. Alors ϕ est régulière en P. En particulier si C est lisse, ϕ est un morphisme.

1.1.3 Diviseurs

La notion de diviseurs d'une courbe est un concept surprenemment puissant qui permet d'étudier de manière générale la géométrie des points sur celle-ci. Étant donné une certaine courbe C, on considère le groupe abélien libre sur les points de C, i.e. on considère l'ensemble des sommes formelles

$$\mathrm{Div}(C) = \{ \sum_{P \in C} n_P P \ : \ n_p \in \mathbb{Z} \text{ et } n_P = 0 \text{ pour presque tout } P \}.$$

Ici « pour presque tout P » signifie pour tout $P \in C$ sauf un nombre fini. La somme formelle est donc une somme finie.

Si $D = \sum_{P \in C} n_P P$, on définit le degré de D comme

$$\deg(D) = \sum_{P \in C} n_P.$$

Deux sous-groupes de $\mathrm{Div}(C)$ seront importants pour nous. Premièrement, l'ensemble des diviseurs de C de degré 0, noté $\mathrm{Div}^0(C)$, i.e.

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \ : \ \deg(D) = 0\}$$

forme un sous-groupe de $\mathrm{Div}(C)$. On remarque que si C est définie sur K, $\mathrm{Gal}(\bar{K}/K)$ agit de façon naturelle sur $\mathrm{Div}(C)$ et $\mathrm{Div}^0(C)$:

$$D^\sigma = \sum_{P \in C} n_P P^\sigma \ , \text{ pour } \sigma \in \mathrm{Gal}(\bar{K}/K).$$

Deuxièmement, supposons que C est lisse et soit $f \in \bar{K}(C)^*$. Alors, on définit

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P.$$

On peut montrer que cette somme est finie et donc que $\mathrm{div}(f) \in \mathrm{Div}(C)$. En fait, il se trouve même que $\mathrm{div}(f) \in \mathrm{Div}^0(C)$.

Définition 18. On dit qu'un diviseur $D \in \mathrm{Div}(C)$ est principal s'il existe $f \in \bar{K}(C)^*$ tel que $D = \mathrm{div}(f)$. Deux diviseurs D_1, D_2 sont dits linéairement équivalents, noté $D_1 \sim D_2$, si $D_1 - D_2$ est principal.
Le groupe de Picard de C, noté $\mathrm{Pic}(C)$, est $\mathrm{Div}(C)$ modulo le sous-groupe des diviseurs principaux. On définit aussi

$$\mathrm{Pic}_K(C) := \{D \in \mathrm{Pic}(C) \ : \ D^\sigma = D \text{ pour tout } \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

$\mathrm{Pic}^0(C)$ est définit comme $\mathrm{Div}^0(C)$ modulo le sous-groupe des diviseurs principaux et de même on définit

$$\mathrm{Pic}^0_K(C) := \{D \in \mathrm{Pic}^0(C) \ : \ D^\sigma = D \text{ pour tout } \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

Nous pouvons aussi définir un ordre partiel sur $\mathrm{Div}(C)$. Pour ce faire, on dit qu'un diviseur $D = \sum_{P \in C} n_P P$ est effectif (ou positif) si $n_P \geq 0$ pour tout $P \in C$. Le cas échéant, on note $D \geq 0$.

Si l'on a deux diviseurs, on dit que $D_1 \geq D_2$ si $D_1 - D_2 \geq 0$. Ceci établit un ordre partiel sur $\mathrm{Div}(C)$.

Définition 19. Soit $D \in \mathrm{Div}(C)$. On associe à D l'ensemble de fonctions

$$\mathcal{L}(D) = \{f \in \bar{K}(C)^* \ : \ \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Il se trouve que $\mathcal{L}(D)$ est un espace vectoriel de dimension finie sur $\bar{K}$. On dénote sa dimension par $l(D)$.

1.1.4 Différentielle

Nous introduisons ici l'espace vectoriel des formes différentielles sur une courbe C. Le concept de différentielle et plus précisément la différentielle invariante d'une courbe elliptique (Voir 1.2.4) est extrêmement important dans l'étude de la mesure de Mahler et de ses rapports avec la théorie des nombres.

Définition 20. Soit C une courbe. L'espace des formes différentielles sur C, noté Ω_C, est le $\bar{K}(C)$-espace vectoriel généré par les symboles de la forme dx où $x \in \bar{K}(C)$ avec les relations

$$(i)\ d(x+y) = dx + dy,$$
$$(ii)\ d(xy) = xdy + ydx,$$
$$(iii)\ da = 0 \text{ pour } a \in \bar{K}.$$

Si $\phi : C_1 \to C_2$ est un morphisme de courbes et si ϕ^* est le morphisme d'anneau associé, on remarque que ϕ^* induit une fonction sur les différentielles

$$\phi^* \colon \Omega_{C_2} \to \Omega_{C_1}$$
$$\sum f_i dx_i \mapsto \sum \phi^* f_i d(\phi^* x_i).$$

Proposition 21. Soit C une courbe, $P \in C$ et $t \in \bar{K}(C)$ une uniformisante en P. Alors
(i) Ω_C est un $\bar{K}(C)$-espace vectoriel de dimension 1.
(ii) Soit $x \in \bar{K}(C)$. Alors dx est une base de Ω_C si et seulement si $\bar{K}(C)/\bar{K}(x)$ est une extension séparable finie.
(iii) Pour tout $\omega \in \Omega_C$ il existe une unique fonction $g \in \bar{K}(C)$ qui dépend de ω et t telle que

$$\omega = gdt.$$

On dénote g par ω/dt.
(iv) Soit $f \in \bar{K}(C)$ régulière en P. Alors df/dt est aussi régulière en P.
(v) Soit $\omega \in \Omega_C$ avec $\omega \neq 0$. Alors $\mathrm{ord}_P(\omega/dt)$ dépend seulement de ω et P et non de l'uniformisante t. Cette valeur est appelée l'ordre de ω en P et est noté $\mathrm{ord}_P(\omega)$.
(vi) Soit $x, f \in \bar{K}(C)$ et supposons que K est de caractéristique nulle. Alors

$$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1.$$

(*vii*) Soit $0 \neq \omega \in \Omega_C$. Alors $\mathrm{ord}_P(\omega) \neq 0$ pour seulement un nombre fini de $P \in C$.

Il semble naturel après la dernière proposition de définir pour $\omega \in \Omega_C$

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P.$$

On a $\mathrm{div}(\omega) \in \mathrm{Div}(C)$ par (*vii*) de la dernière proposition.

On dit que ω est régulière (ou holomorphe) en P si $\mathrm{ord}_P(\omega) \geq 0$. Si $\mathrm{ord}_P(\omega) \leq 0$, on dit que ω ne s'annule pas en P.

Définition 22. La classe des diviseurs canoniques est l'image des $\mathrm{div}(\omega)$ dans $\mathrm{Pic}(C)$ pour $0 \neq \omega \in \Omega_C$. Tout diviseur dans la classe des diviseurs canoniques est appelé un diviseur canonique.

Théorème 23 (Riemann-Roch)**.** Soit C une courbe lisse et soit K_C un diviseur canonique. Alors il existe un entier $g \geq 0$, appelé le genre de C, tel que pour tout $D \in \mathrm{Div}(C)$ on a

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

1.2 Courbes elliptiques

Nous nous intéressons maintenant plus particulièment aux courbes elliptiques qui sont les objets principaux de ce mémoire et leur étude est fondamentale à la mesure de Mahler. Les prochaines sections survoleront les concepts essentiels des courbes elliptiques, principalement sur $\mathbb{Q}$ ou sur un corps de nombres.

1.2.1 Équation de Weierstrass

Définition 24. Une courbe elliptique est une paire (E, O) où E est une courbe lisse de genre 1 et $O \in E$. On dit que la courbe elliptique E est définie sur K si E est définie sur K en tant que courbe.

Cette définition peut sembler assez abstraite (le genre d'une courbe est définie de façon extrêmement non-intuitive), mais il se trouve qu'à isomorphisme près, les courbes elliptiques sont des objets très concrets, ce qui facilite grandement leur étude.

Proposition 25. Soit E une courbe elliptique définie sur K.
(i) Il existe deux fonctions $x, y \in K(E)$ telles que l'application

$$\phi \ : \ E \to \mathbb{P}^n, \quad \phi = [x, y, 1]$$

donne un isomorphisme de E/K vers une courbe avec une équation de la forme

$$C \ : \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

où $a_1, ..., a_6 \in K$ et $\phi(O) = [0, 1, 0]$. La courbe C est appelée une forme de Weierstrass de E et x, y sont des coordonnées de Weierstrass. On appelle $[0, 1, 0]$ le point à l'infini de C.
(ii) Deux formes de Weierstrass de E sont reliées par un changement de variables de la forme

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

où $u \in K^*$ et $r, s, t \in K$.
(iii) Inversement, toute courbe lisse C donnée par une forme de Weierstrass est une courbe elliptique définie sur K avec point de base $O = [0, 1, 0]$.

Par la suite, nous étudierons souvent les courbes elliptiques dans la carte affine $Z = 1$.

Il existe d'autres formes que la forme de Weierstrass pour une courbe elliptique, mais nous allons continuer à utiliser cette dernière pour le reste du mémoire. Donc lorsqu'une courbe elliptique sera définie à partir d'une équation, celle-ci sera toujours une forme de Weierstrass, sauf si spécifié autrement.

Associé à une forme de Weierstrass

$$E \ : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

on définit les quantités

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta, \quad \text{lorsque } \Delta \neq 0.
\end{aligned}$$

On peut montrer que E est non-singulière si et seulement si $\Delta \neq 0$ et donc j est défini seulement dans ces cas. Même si ces quantités semblent extrêmement arbitraires, elles sont couramment utilisées dans l'étude des courbes elliptiques. Δ est appelé le discriminant de E et j est le j-invariant. Par exemple, deux courbes elliptiques sont isomorphes sur $\bar{K}$ si et seulement si elles ont le même j-invariant.

Définition 26. Soit E/K une courbe donnée par une équation de Weierstrass de la forme

$$E \ : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

soit $P = (X_0, Y_0)$ un point singulier de E et soit

$$f(x, y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

Comme $\frac{\partial f}{\partial X}(X_0, Y_0) = \frac{\partial f}{\partial Y}(X_0, Y_0) = 0$, on peut écrire avec le développement de Taylor

$$f(x, y) - f(x_0, y_0) = [(Y - Y_0) - \alpha(X - X_0)][(Y - Y_0) - \beta(X - X_0)] - (X - X_0)^3,$$

pour certains $\alpha, \beta \in \bar{K}$.
On dit que P est un point de rebroussement si $\alpha = \beta$ et dans ce cas il y a une unique tangente en P. Si $\alpha \neq \beta$, on dit que P est un noeud.
Si P est un noeud, on dit que E/K a réduction multiplicative divisée en P si $\alpha, \beta \in K$. Sinon on dit que E/K a réduction multiplicative non-divisée en P.

La proposition suivante nous permet d'utiliser la dernière définition de manière arithmétique.

Proposition 27. Soit E/K une courbe donnée par une équation de Weierstrass et P un point singulier de E. P est un point de rebroussement si et seulement si $c_4 = 0$ et P est un noeud si et seulement si $c_4 \neq 0$.

Définition 28. Soit $E/\mathbb{Q}$ une courbe elliptique définie sur $\mathbb{Q}$. Le discriminant minimal de E est le discriminant où $|\Delta|$ est minimisé parmi toutes les équations de Weierstrass de E de la forme

$$E \ : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

où $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Une équation de Weierstrass de E où $|\Delta|$ est minimisé est appelée une équation minimale de Weierstrass.

Cette définition est bien sûr plus générale que les courbes elliptiques sur $\mathbb{Q}$, mais développer la théorie nous mènerait trop loin.

Nous mentionnons aussi que pour toute courbe elliptique $E/\mathbb{Q}$ il existe une forme de Weierstrass où $a_1, ..., a_6 \in \mathbb{Z}$ et donc la définition ci-dessus a du sens.

Théorème 29. Soit $E/\mathbb{Q}$ une courbe elliptique.
(i) Une équation minimale de Weierstrass est unique à un changement de coordonnées entières près, i.e. à un changement de coordonnées de la forme

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

où $u = \pm 1$, $r, s, t \in \mathbb{Z}$.

1.2.2 Loi du groupe

La principale caractéristique des courbes elliptiques est qu'elles forment des groupes et l'opération associée peut être définie de façon géométrique.

Soit $E \subset \mathbb{P}^2$ une courbe elliptique donnée par une équation de Weierstrass avec point de base $[0, 1, 0]$. On peut donc voir E comme l'ensemble des points $P = (x, y)$ satisfaisant l'équation de Weierstrass avec le point à l'infini O. Soit $D \subset \mathbb{P}^2$ une droite, i.e. D est de la forme

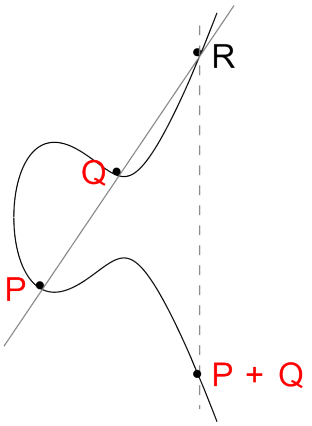
$$D \ : \ aX + bY + cZ = 0, \quad a, b, c \in \bar{K}, \ a, b, c \text{ pas tous nuls.}$$

Comme E est donné par un polynôme de degré 3, par le théorème de Bézout, $D \cap E$ contient exactement 3 points en comptant les multiplicités.

Définition 30. Soit E une courbe elliptique donnée par une équation de Weierstrass, $P, Q \in E$, D la droite passant par P et Q et $\ominus R$ le troisième point d'intersection de D avec E (la notation $\ominus R$ sera claire dans un moment). Soit D' la droite passant par $\ominus R$ et O et R le troisième point d'intersection de D' avec E. Alors on définit

$$P \oplus Q = R.$$

FIGURE 1.1: Addition de points sur une courbe elliptique.



Géométriquement, si l'on regarde dans la carte affine $Z = 1$, la droite entre un point R et O est la droite verticale passant par R. La figure 1.1 montre visuellement comment additionner des points de E.

Proposition 31. La loi d'addition $\oplus$ a les propriétés suivantes :
(i) Si une droite D intersecte E en les points P, Q, R, alors

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

(ii) $P \oplus O = P$ pour tout $P \in E$.
(iii) $P \oplus Q = Q \oplus P$ pour tout $P, Q \in E$.
(iv) Soit $P \in E$. Alors il existe un point, dénoté par $\ominus P$ tel que $P \oplus (\ominus P) = O$. De plus $\ominus P$ est le troisième point de E se trouvant sur la droite passant par P et O.
(v) On a $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ pour tout $P, Q, R \in E$.

La dernière proposition donne à E la structure d'un groupe abélien avec identité O. De plus, l'ensemble des points K-rationnels de E, i.e.

$$E(K) = \{(x, y) \in K^2 \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

est un sous-groupe de E puisque les droites entre deux point sur K peuvent s'écrire avec coefficients dans K.

La prochaine proposition donne un algorithme pour additionner deux points sur E. On utilise maintenant les signe $+$ et $-$ pour signifier $\oplus$ et $\ominus$ respectivement et $[m]P$ signifie m additions successives de P avec lui-même.

Proposition 32. Soit E une courbe elliptique donnée par une équation de Weierstrass

$$E \ : \ y^2 + a_2xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(i) Soit $P_0 = (x_0, y_0) \in E$. Alors

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

(ii) Soit $P_1, P_2, P_3 \in E$, $P_i = (x_i, y_i)$ tels que

$$P_1 + P_2 = P_3.$$

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

$$P_1 + P_2 = O.$$

Sinon, définissons

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, \quad \text{si } x_2 \neq x_1,$$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{si } x_2 = x_1.$$

Alors $y = \lambda x + \nu$ est la ligne passant par P_1 et P_2 et on a

$$P_3 = (x_3, y_3) = \left(\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3\right).$$

Puisque l'addition et la soustraction utilisent des fonctions rationnelles, il est possible de montrer que

$$\begin{aligned} +\colon E \times E &\to E \\ (P, Q) &\mapsto P + Q, \end{aligned}$$

et

$$\begin{aligned} -\colon E &\to E \\ P &\mapsto -P, \end{aligned}$$

sont des morphismes.

1.2.3 Isogénies

Nous avons mentionné plus tôt que les morphismes entre variétés étaient l'équivalent des morphismes en algèbre. Ici, nos courbes elliptiques sont en fait des couples (E, O) où E est une courbe et O est un point distingué. Donc, comme les fonctions continues entre espaces topologiques pointés, un morphisme entre deux courbes elliptiques devrait envoyer le premier point distingué vers le deuxième.

Définition 33. Soit $(E_1, O_1), (E_2, O_2)$ deux courbes elliptiques. Une isogénie de courbes elliptiques est un morphisme

$$\phi \ : \ E_1 \to E_2$$

tel que $\phi(O_1) = O_2$. E_1 et E_2 sont isogènes si $\phi(E_1) \neq O_2$.

Il est possible de montrer que la relation définie par $E_1 \sim E_2$ si E_1 est isogène à E_2 est une relation d'équivalence, et que si

$$\phi \ : \ E_1 \to E_2$$

est une isogénie non-nulle, alors $\phi(E_1) = E_2$. Règle générale, nous allons considérer les courbes elliptiques à isogénie non-nulle près puisque les propriétés entre deux courbes elliptiques isogènes sont souvent les mêmes.

Les isogénies sont donc vues comme les morphismes entre courbes elliptiques. On a même la propriété suivante qui va dans ce sens.

Théorème 34. Soit

$$\phi \ : \ E_1 \to E_2$$

une isogénie. Alors

$$\phi(P + Q) = \phi(P) + \phi(Q), \quad \forall P, Q \in E_1.$$

Si E_1, E_2 sont deux courbes elliptiques, on définit donc

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogénies } E_1 \to E_2\}.$$

Ceci forme un groupe sous l'addition usuelle. De même, on définit

$$\mathrm{End}(E) = \mathrm{Hom}(E, E).$$

C'est un anneau sous l'addition et la composition.

Par exemple le morphisme

$$\begin{aligned}[m]\colon E &\to E\\ P &\mapsto [m]P,\end{aligned}$$

où $m \in \mathbb{Z}_{\geq 0}$, est un élément de $\mathrm{End}(E)$.

Définition 35. Soit E une courbe elliptique et $m \in \mathbb{Z}$, $m \geq 1$. On définit

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

et $E[m]$ est appelé le sous-groupe de m-torsion. On remarque donc que le sous-groupe de torsion de E est

$$E_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E[m],$$

i.e. l'union de tous les points d'ordre fini.
Si E est définie sur K, on note $E_{\mathrm{tors}}(K)$ l'ensemble des points d'ordre fini de $E(K)$.

1.2.4 Différentielle invariante

Soit une E une courbe elliptique avec forme de Weierstrass

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

On définit

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

(Voir Section 1.1.4 pour les différentielles sur les courbes) ω est une différentielle sur E appelée la différentielle invariante de E.

Avant d'introduire le prochain théorème, on définit l'isomorphisme τ_Q comme

$$\tau_Q \ : \ E \to E, \quad \tau_Q(P) = P + Q.$$

Théorème 36. Soit E une courbe elliptique avec différentielle invariante ω.
(i) ω est holomorphe et n'a pas de zéros.
(ii) Soit $P, Q \in E$. Alors

$$\tau_Q^*(\omega) = \omega.$$

Cette condition est la raison pour laquelle ω est appelée la différentielle invariante, puisqu'elle est invariante par translation.

(*iii*) Soit $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$. Alors

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega).$$

1.2.5 Mordell-Weil

Soit K un corps de nombres. Nous avons vu que $E(K)$ est un groupe abélien mais nous ne savons pas grand chose encore sur sa structure. Il se trouve que le groupe associé à une courbe elliptique est surprenamment simple.

Théorème 37 (Mordell-Weil)**.** Soit K un corps de nombres. Alors $E(K)$ est un groupe de type fini, i.e. $E(K)$ a un nombre fini de générateurs.

Ce théorème est en fait plus général et s'applique à toute variété abélienne (Voir [6]).

Le théorème fondamental des groupes abéliens de type fini nous dit que $E(K)$ a la forme

$$E(K) \approx \mathbb{Z}^n \times E_{\mathrm{tors}}(K),$$

où n est un entier uniquement déterminé par E et K. n est appelé le rang algébrique de E/K.

Le rang algébrique d'une courbe elliptique est un invariant (sous isogénie) extrêmement étudié en théorie des nombres. La conjecture de Birch et Swynnerton-Dyer s'intéresse particulièrement à cette quantité (Voir Section 1.2.7).

Maintenant que nous connaissons un peu plus la structure de $E(K)$, nous nous intéressons à $E_{\mathrm{tors}}(K)$. Les prochains théorèmes nous donnent certaines informations sur ce sous-groupe.

Théorème 38 (Mazur)**.** Soit $E/\mathbb{Q}$ une courbe elliptique. Alors $E_{\mathrm{tors}}(\mathbb{Q})$ est isomorphe à un des groupes suivants :

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10 \text{ ou } N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 4.$$

Réciproquement, tous ces groupes apparaissent comme sous-groupe de torsion d'une certaine courbe elliptique $E/\mathbb{Q}$.

Théorème 39 (Merel)**.** Pour tout entier $d \geq 1$ il existe une constante $N(d)$ tel que pour tout corps de nombres $K/\mathbb{Q}$ de degré $\leq d$ et pour toute courbe elliptique E/K on a

$$|E_{\text{tors}}(K)| \leq N(d).$$

Nous mentionnons un dernier théorème qui s'avère être extrêmement utile pour calculer $E_{\text{tors}}(\mathbb{Q})$.

Théorème 40 (Lutz-Nagell)**.** Soit $E/\mathbb{Q}$ une courbe elliptique avec équation de Weierstrass

$$E \ : \ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Soit $O \neq (x, y) \in E_{\text{tors}}(\mathbb{Q})$.
(i) $x, y \in \mathbb{Z}$,
(ii) Soit $[2]P = O$ ou y^2 divise $4A^3 + 27B^2$.

1.2.6 Conducteur

Le conducteur d'une courbe elliptique est un nombre (ou plus généralement un idéal) encodant la complexité arithmétique locale de la courbe, i.e. si la courbe se comporte bien modulo certains idéaux premiers. Le conducteur est donc une quantité globale obtenue en rattachant plusieurs quantités locales. La définition exacte du conducteur nous demanderait de développer trop de théorie et ne sera donc pas donnée mais suffira pour la plupart des cas.

Nous commençons tout d'abord par définir des propriétés locales d'une courbe elliptique.

Définition 41. Soit $E/\mathbb{Q}$ une courbe elliptique sur $\mathbb{Q}$, soit E' une équation minimale de Weierstrass de E et $p \in \mathbb{Z}$ un nombre premier. Comme les coefficients définissant E' sont tous entiers, on peut considérer la courbe modulo p,

$$E'_p \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où $a_1, ..., a_6 \in \mathbb{F}_p$.
(i) E a bonne réduction (ou réduction stable) en p si E'_p est non-singulière.
(ii) E a réduction multiplicative (ou semistable) en p si E'_p possède un noeud.
(iii) E a réduction additive en p si E'_p possède un point de rebroussement.

On remarque avec cette définition que le discriminant minimal de $E/\mathbb{Q}$ est un produit de premiers où E a mauvaise réduction, i.e. réduction multiplicative ou additive. C'est

aussi le cas du conducteur, mais les exposants des premiers seront souvent différents de ceux du discriminant minimal.

Définition 42. Soit $E/\mathbb{Q}$ une courbe elliptique. Le conducteur d'une courbe elliptique est l'entier

$$\mathfrak{f}(E/\mathbb{Q}) = \prod_p p^{f_p(E)},$$

le produit étant sur tous les premiers et où
(i) $f_p(E) = 0$ si E a bonne réduction en p,
(ii) $f_p(E) = 1$ si E a réduction multiplicative en p,
(iii) $f_p(E) = 2 + \delta_p(E)$ si E a réduction additive en p et $\delta_p(E)$ est un entier non-négatif valant 0 si $p \geq 5$.

E a bonne réduction pour presque tous les premiers, i.e. pour tous les premiers sauf un nombre fini, et donc la définition ci-dessus a du sens. Nous ne définirons pas la quantité $\delta_p(E)$ puisqu'elle ne sera pas utilisée au cours de ce mémoire, mais mentionnons qu'elle mesure le degré de « ramification sauvage » des points de E d'ordre p^k pour un certain $k \in \mathbb{N}$ (Voir [7]).

1.2.7 Fonctions-L

Dans la même veine que le conducteur d'une courbe elliptique, la fonction-L permet d'emmagasiner l'information locale (information modulo p pour p un nombre premier) d'une courbe elliptique donnée. L'étude de l'ordre de ses zéros est centrale en théorie des nombres et mène même à la conjecture de Birch et Swynnerton-Dyer, problème notamment célèbre pour la récompense de 1 000 000$ qui lui est associé.

La théorie des fonctions-L associées aux courbes elliptiques sur $\mathbb{Q}$ est beaucoup plus développée que celle sur un corps de nombres arbitraire K et c'est celle que nous allons développer dans cette section.

Définition 43. Soit p un nombre premier et $E/\mathbb{Q}$ une courbe elliptique définie sur $\mathbb{Q}$. Définissons $L_p(T) := 1 - a_pT + pT^2$ où $a_p = p + 1 + \#E'_p$ si E a bonne réduction en p (Ici $\#E'_p$ est le nombre de points de E' modulo p où E' est une équation minimale de E).
Si E a mauvaise réduction en p, on définit

$$L_p(T) = \begin{cases} 1 - T & \text{si } E \text{ a réduction multiplicative divisée en } p, \\ 1 + T & \text{si } E \text{ a réduction multiplicative non-divisée en } p, \\ 1 & \text{si } E \text{ a réduction additive en } p. \end{cases}$$

La fonction-L attachée à E est définie par

$$L_{E/\mathbb{Q}}(s) := \prod_p L_p(p^{-s})^{-1},$$

où le produit est sur tous les nombre premiers p.

On remarque que dans tous les cas on a l'identité

$$L_p(1/p) = \#E'_{p,ns}/p,$$

où $\#E'_{p,ns}$ est l'ensemble des points non-singuliers de E'_p. On peut donc voir la fonction-L comme une fonction englobant le nombre de points de E modulo p^s où p est n'importe quel nombre premier et s n'importe quel naturel.

Comme dans le cas des fonctions zêtas et de leurs généralisations, $L_{E/\mathbb{Q}}(s)$ s'étend analytiquement et satisfait une équation fonctionnelle. Tout d'abord, on définit

$$\xi_E(s) = \mathfrak{f}_E^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s),$$

où $\mathfrak{f}_E$ est le conducteur défini à la section précédente et $\Gamma(s)$ est la fonction gamma, i.e.

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt.$$

Théorème 44. Soit $E/\mathbb{Q}$. La fonction $\xi_E(s)$ peut être étendue analytiquement sur tout le plan complexe et satisfait l'équation fonctionnelle

$$\xi_E(s) = w\xi_E(2-s),$$

où $w = \pm 1$.
w est appelé le signe de l'équation fonctionnelle et détermine si l'ordre d'annulation de $L_E(s)$ en $s = 1$ est pair ou impair.

L'ordre du zéro de $L_E(s)$ en $s = 1$, i.e. le plus petit entier r tel que

$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} \neq 0$$

est appelé le rang analytique de E. La conjecture de Birch et Swynnerton-Dyer affirme que le rang analytique d'une courbe elliptique $E/\mathbb{Q}$ est égal à son rang algébrique.

1.2.8 Courbes elliptiques sur $\mathbb{C}$

La théorie des courbes elliptiques sur $\mathbb{C}$ est surprenamment riche et devrait avoir un chapitre complet qui lui est consacré. Or, par soucis de concision, nous ne développerons que le nécessaire à l'étude de la mesure de Mahler. Pour une compréhension plus approfondie de la matière, nous vous référons au chapitre VI de [2].

Soit $E/\mathbb{C}$ une courbe elliptique sur $\mathbb{C}$. Il se trouve que E est isomorphe à une équation de Weirstrass de la forme

$$E \ : \ y^2 = 4x^3 - ax - b, \quad a, b \in \mathbb{C}.$$

De plus $E = E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ ayant une opération de groupe donnée par des fonctions partout localement analytiques, E possède naturellement une structure de groupe (compact) de Lie complexe, i.e. une variété différentiable avec une opération de groupe lisse. On peut rendre cette remarque encore plus explicite.

Définition 45. Soit $\Lambda \subset \mathbb{C}$ une lattice, i.e. $\Lambda = \{n_1 w_1 + n_2 w_2 \ : \ n_1, n_2 \in \mathbb{Z}\}$ avec $w_1, w_2 \in \mathbb{C}$ linéairements indépendants sur $\mathbb{R}$. Alors la fonction $\wp$ de Weierstrass (relative à Λ) est définie par

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

La somme associée à $\wp$ converge absolument et uniformément pour tout sous-ensemble compact de $\mathbb{C} \backslash \Lambda$, et donc la définition ci-dessus a du sens. $\wp$ est une fontion méromorphe ayant come seuls pôles (doubles) les points de Λ avec résidu 0. Sa dérivée satisfait

$$\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3,$$

où $g_2, g_3 \in \mathbb{C}$. Les quantités $g_2 = g_2(\Lambda), g_3 = g_3(\Lambda)$ reviendront dans le prochain théorème.

De plus, comme Λ est un sous-groupe du groupe additif de $\mathbb{C}$, on a

$$\wp(z; \Lambda) = \wp(z + w; \Lambda), \quad \forall w \in \Lambda.$$

$\wp$ est donc une fonction sur $\mathbb{C}/\Lambda$, le plan complexe modulo la lattice Λ. $\mathbb{C}/\Lambda$ possède naturellement une structure de groupe de Lie et est en fait équivalent à un tore. C'est cette association qui nous permet de rapprocher la topologie différentielle et les courbes elliptiques. Avant d'entrer dans le coeur de cette équivalence, rappelons que deux lattices

$\Lambda_1, \Lambda_2 \subset \mathbb{C}$ sont homothétiques s'il existe $\alpha \in \mathbb{C}^*$ tel que $\Lambda_1 = \alpha\Lambda_2$. Il s'agit clairement d'une relation d'équivalence.

Proposition 46. Soient $g_2 = g_2(\Lambda), g_3 = g_3(\Lambda)$ les quantités définies plus haut associées à une lattice $\Lambda \in \mathbb{C}$. Alors

$$E \ : \ y^2 = 4x^3 - g_2x - g_3$$

est une courbe elliptique sur $\mathbb{C}$ et l'association

$$\begin{aligned} \phi \ : \ \mathbb{C}/\Lambda &\to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \\ z &\mapsto [\wp(z), \wp'(z), 1], \end{aligned}$$

est un isomorphisme analytique de groupes de Lie, i.e. c'est un isomorphisme de surface de Riemann compatible avec l'opération de groupe.

La proposition précédente nous dit qu'à chaque lattice sur $\mathbb{C}$ nous pouvons associer une courbe elliptique sur $\mathbb{C}$. En fait, cette correspondance est même une bijection.

Théorème 47. (i) Soit $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ deux lattices. Alors l'association

$$\begin{aligned} \{\alpha \in \mathbb{C} \ : \ \alpha\Lambda_1 \subset \Lambda_2\} &\to \{\phi \ : \ \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \ : \ \phi \text{ est holomorphe et } \phi(0) = 0\} \\ \alpha &\mapsto \phi_\alpha, \end{aligned}$$

où $\phi_\alpha(z) = \alpha z (\text{mod } \Lambda_2)$, est une bijection.
(ii) Soient E_1, E_2 deux courbes elliptiques sur $\mathbb{C}$ associées à des lattices Λ_1, Λ_2 respectivement. Alors l'inclusion

$$\{\text{isogénies } \phi \ : \ E_1 \to E_2\} \to \{\phi \ : \ \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \ : \ \phi \text{ est holomorphe et } \phi(0) = 0\}$$

est une bijection.
(iii) Soit $E/\mathbb{C}$ une courbe elliptique. Alors il existe une lattive $\Lambda \subset \mathbb{C}$, unique à homothétie près, telle que

$$\begin{aligned} \phi \ : \ \mathbb{C}/\Lambda &\to E(\mathbb{C}), \\ z &\mapsto [\wp(z;\Lambda), \wp'(z;\Lambda), 1], \end{aligned}$$

est un isomorphisme analytique de groupes de Lie.

On peut interpréter les résultats précédents de façon catégorique en disant qu'il y a équivalence entre les catégories suivantes :
(a) Objets : Courbes elliptiques sur $\mathbb{C}$.
Morphismes : Isogénies.

(a) Objets : Courbes elliptiques sur $\mathbb{C}$.
Morphismes : Fonctions analytiques envoyant O sur O.
(a) Objets : Lattices $\Lambda \subset \mathbb{C}$, à homothétie près.
Morphismes : Fonctions(Λ_1,Λ_2) = $\{\alpha \in \mathbb{C} \ : \ \alpha\Lambda_1 \subset \Lambda_2\}$.

1.2.9 Premier groupe d'homologie

Nous avons vu dans la dernière section que si l'on a une courbe elliptique $E/\mathbb{C}$, alors $E(\mathbb{C})$ est une surface de Riemann compacte, plus précisément homéomorphe à un tore plat de dimension 2. Nous pouvons donc définir les groupes d'homologie de $E(\mathbb{C})$ ainsi qu'une théorie de l'intégration sur cette surface.

Soient $\mathcal{R}$ une surface de Riemann et $\mathcal{T}$ une triangulation orientée de celle-ci. On définit C_0 comme l'ensemble des sommes formelles de points de la triangulation $\mathcal{T}$, i.e. C_0 est le groupe abélien libre sur les points P_i de la triangulation. De même C_1 est le groupe abélien libre sur les arêtes orientées et C_2 est le groupe abélien libre sur les triangles orientés. Les ensembles C_0, C_1, C_2 sont appelés des 0-chaînes, 1-chaînes et 2-chaînes respectivement. On dénote par $-\gamma_i$ l'arête γ_i avec orientation inverse et similairement pour D_i un triangle.

Par (P_1, P_2) nous voulons dire l'arête orientée commençant par P_1 et finissant par P_2. De même, (P_1, P_2, P_3) signifie le triangle orienté d'arêtes (P_1, P_2), (P_2, P_3) et (P_3, P_1). On définit les opérateurs frontières δ par

$$\delta_1(P_1, P_2) = P_2 - P_1, \quad \delta_2(P_1, P_2, P_3) = (P_1, P_2) + (P_2, P_3) + (P_3, P_1).$$

Nous étendons la définition de δ à tout C_1 et C_2 par $\mathbb{Z}$-linéarité. Nous obtenons donc deux homomorphismes de groupes

$$\delta_1 \ : \ C_1 \to C_0, \quad \delta_2 \ : \ C_2 \to C_1.$$

Il se trouve que $\delta_1 \circ \delta_2 = 0$ et donc que $\mathrm{Im}(\delta_2) \subset \ker(\delta_1)$.

Définition 48. Soient $Z = \ker(\delta_1)$ et $B = \mathrm{Im}(\delta_2)$. Alors le premier groupe d'homologie (simpliciale) est

$$H_1(\mathcal{R}, \mathbb{Z}) := Z/B.$$

On peut montrer que $H_1(\mathcal{R}, \mathbb{Z})$ ne dépend pas de la triangulation.

Il se trouve que toute courbe orientée fermée et continue γ' sur $\mathcal{R}$ est homotope à un élément de Z et donc à un élément de Z/B. Nous pouvons donc avoir une théorie de l'intégration sur $\mathcal{R}$. À cet effet on définit

Définition 49. Soit $\mathcal{R}$ une surface de Riemann. Alors $H^1(\mathcal{R}, \mathbb{R})$ est le dual de $H_1(\mathcal{R}, \mathbb{Z})$, i.e.

$$H^1(\mathcal{R}, \mathbb{R}) := \{f \ : \ H^1(\mathcal{R}, \mathbb{Z}) \to \mathbb{R} \ : \ f \text{ est linéaire et continue}\}.$$

Si l'on a une forme différentielle ω sur $\mathcal{R}$, alors la fonction

$$\begin{aligned} f \ : \ H_1(\mathcal{R}, \mathbb{Z}) &\to \mathbb{R} \\ [\gamma] &\mapsto \int_\gamma \omega. \end{aligned}$$

est un élément de $H^1(\mathcal{R}, \mathbb{R})$. C'est principalement ces éléments que nous étudierons dans ce mémoire.

Notons aussi ce fait intéressant. Si $\mathcal{R}$ est connexe par arcs, on peut considérer son groupe d'homotopie $\pi(\mathcal{R})$, i.e. l'ensemble des lacets autour d'un point fixé x modulo la relation d'équivalence donnée par l'homotopie et où l'opération est donnée par la concaténation des lacets. Alors, on a un isomorphisme canonique entre $H_1(\mathcal{R}, \mathbb{Z})$ et l'abélianisation de $\pi(\mathcal{R})$, i.e.

$$H_1(\mathcal{R}, \mathbb{Z}) \simeq \pi(\mathcal{R})/[\pi, \pi],$$

où $[\pi, \pi]$ est le commutateur de $\pi(\mathcal{R})$.

Chapitre 2

La Mesure de Mahler

La mesure de Mahler ? Ça Mahler intéressant !
HAHAHAHAHAHAHA !!!

La majorité de mon entourage

Le but ultime de ce mémoire est d'étudier la mesure de Mahler d'un polynôme à deux variables représenté par une courbe elliptique et ses rapports avec la fonction-L associée. Nous pourrions donc directement définir la mesure de Mahler dans le cas plus général, or il semble plus naturel de commencer par le début, c'est-à-dire de définir la mesure de Mahler tout d'abord pour un polynôme à une variable puis de monter dans la « hiérarchie » des définitions.

2.1 Le cas à une variable

L'étude de la mesure de Mahler débute en 1933 avec D.H. Lehmer dans *Factorization of certain cyclotomic functions* [8]. Cet article mentionne dans son introduction les différentes manières d'obtenir de grands nombres premiers. Bien sûr, les techniques d'aujourd'hui sont beaucoup plus raffinées avec l'arrivée de l'ordinateur.
La méthode principale de l'article est de trouver des nombres premiers comme valeurs spéciales de fonctions numériques. À cet effet, Lehmer définit pour un polynôme unitaire

$$F(x) = x^r + a_{r-1}x^{r-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$$

la quantité

$$\Delta_n(F) = \prod_{i=1}^{r}(\alpha_i^n - 1),$$

où n est un entier positif et α_i sont les racines de $F(x)$ sur $\mathbb{C}$.
Le rapport ici avec les polynômes cyclotomiques est que si l'on définit

$$Q_m^* = Q_m^*(F) = \prod_{i=1}^{r} Q_m(\alpha_i),$$

où $Q_m(x)$ est le m-ième polynôme cyclotomique, i.e. le polynôme minimal de $e^{2\pi i/m}$, alors on a

$$\Delta_n(F) = \prod_{m|n} Q_m^*$$

puisque $\prod_{m|n} Q_m(x) = x^n - 1$. Notons que $\Delta_n(F) \in \mathbb{Z}$ puisqu'il s'agit d'un produit de tous les conjugués algébriques de F. De plus, nous allons nous intéresser au cas où F ne contient pas de racines de l'unité puisque sinon $\alpha_i^N = 1$ pour un certain N et $\Delta_M(F) = 0$ pour tout M divisible par N.
À la fin de son article, Lehmer étudie certains polynômes F pour lesquels la suite $\Delta_n(F)$ augmente lentement, i.e. pour lesquels

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(F)}{\Delta_n(F)} \right|$$

est petit. Il montre que dans ces cas, $\Delta_n(F)$ a plus de chances de produire des nombres premiers, ou des nombres avec peu de facteurs premiers. Par exemple, en prenant $F(x) = x^3 - x - 1$, Lehmer montre que

$$\Delta_{113} = 63\ 088\ 004\ 325\ 217 \quad \text{et} \quad \Delta_{127} = 3\ 233\ 514\ 251\ 032\ 733$$

sont premiers. Ceci nous mène donc à étudier le ratio de la suite Δ_n.

Proposition 50. Soit $F(x) \in \mathbb{Z}[x]$ unitaire tel qu'aucune racine n'est de norme 1. Alors
(i)

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(F)}{\Delta_n(F)} \right| = \prod_{i=1}^{r} \max\{1, |\alpha_i|\},$$

où α_i sont les racine de F sur $\mathbb{C}$.
(ii) Si $n|m$, alors $\Delta_n(F)|\Delta_m(F)$.

Pour produire des nombres premiers à l'aide de Δ_n, la proposition précédente nous dit donc que n doit être premier.

Il se trouve que la suite $\left|\frac{\Delta_{n+1}(F)}{\Delta_n(F)}\right|$ converge si et seulement si aucune racine de F ne se trouve sur le cercle unité.

La proposition précédente mène naurellement à la définition suivante.

Définition 51. Soit un polynôme non-nul

$$F(x) = a_r x^r + ... + a_1 x + a_0 = a_d \prod_{i=1}^{r} (x - \alpha_i)$$

sur $\mathbb{C}[x]$. Alors la mesure de Mahler de F est

$$M(F) = |a_r| \prod_{i=1}^{r} \max\{1, |\alpha_i|\}.$$

Il est de convention de poser

$$m(F) = \log M(F),$$

et $m(F)$ est appelé la mesure de Mahler logarithmique. Il se trouve que $m(F)$ possède de belles propriétés et donc les généralisations subséquentes de la mesure de Mahler généraliseront $m(F)$ et non $M(F)$. Dans les sections précédentes, nous appelerons donc $m(F)$ la mesure de Mahler tout simplement.

La mesure de Mahler tient son nom de Kurt Mahler qui étudia la quantité $M(F)$ dans deux articles [9], [10] et ses relations avec d'autres « hauteurs » de polynômes comme

$$L(F) = \sum_{i=0}^{r} |a_i|, \quad H(F) = \max_{i=0,...,r} \{|a_i|\}.$$

$L(F)$ et $H(F)$ sont souvent appelées la longueur et la hauteur de F respectivement. Mahler prouva que ces trois mesures ont le même ordre de grandeur, i.e.

$$H(F) \ll M(F) \ll L(F),$$
$$L(F) \ll M(F) \ll H(F).$$

L'intérêt d'étudier la mesure de Mahler est qu'elle est multiplicative, i.e. $M(F_1F_2) = M(F_1)M(F_2)$. Ceci permet entre autres de comparer $L(F_1F_2)$ avec $L(F_1)$ et $L(F_2)$ et similairement pour $H(F_1F_2)$.

Pour en revenir au taux de croissance de la suite $\Delta_n(F)$, il semble intéressant de chercher des polynômes $F(x) \in \mathbb{Z}[x]$ tel que $M(F)$ est minimale et strictement plus grande que 1. C'est dans cette optique que Lehmer [8] considéra le polynôme

$$G(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

qui a mesure de Mahler $M(G) = 1,176280818\ldots$. Ce polynôme a la plus petite mesure de Mahler connue à ce jour. L'existence d'une constante absolue $\mu > 1$ telle que $M(P) \geq \mu$ lorsque $M(P) \neq 1$ pour $P \in \mathbb{Z}[x]$ est appelée la conjecture de Lehmer. On estime que $\mu = 1,176280818\ldots$ satisfait cette conjecture.

Comme mentionné plus haut, $m(F)$ possède certaines propriétés qui avantagent son étude, la plus connue prouvée par Mahler [9]. Nous prouvons tout d'abord un lemme important.

Théorème 52 (Formule de Jensen)**.** Pour tout $\alpha \in \mathbb{C}$ on a

$$\int_0^1 \log|\alpha - e^{2\pi i\theta}|d\theta = \log\max\{1, |\alpha|\}.$$

Démonstration. Si $\alpha = 0$ le résultat est trivial. Supposons donc que $\alpha \neq 0$. Supposons aussi pour le moment que $|\alpha| \neq 1$. Si $|\alpha| < 1$, on écrit

$$\int_0^1 \log|\alpha - e^{2\pi i\theta}|d\theta = \int_0^1 \log|1 - \alpha e^{-2\pi i\theta}|d\theta = \int_0^1 \log|1 - \alpha e^{2\pi i\theta}|d\theta.$$

Si $|\alpha| > 1$, on écrit

$$\int_0^1 \log|\alpha - e^{2\pi i\theta}|d\theta = \log|\alpha| + \int_0^1 \log|1 - \alpha^{-1}e^{2\pi i\theta}|d\theta.$$

Il suffit donc de prouver que pour $\beta \in \mathbb{C}$ avec $|\beta| < 1$ on a

$$\int_0^1 \log|1 - \beta e^{2\pi i\theta}|d\theta = 0.$$

On remarque que $\log|z| = \Re(\log z)$. On obtient donc

$$\begin{aligned}
\int_0^1 \log|1 - \beta e^{2\pi i\theta}|d\theta &= \Re\int_0^1 \log(1 - \beta e^{2\pi i\theta})d\theta \\
&= \Re\int_0^1 \left(-\sum_{n=1}^{\infty}\frac{\beta^n}{n}e^{2\pi i\theta n}\right)d\theta \\
&= \Re\left(-\sum_{n=1}^{\infty}\frac{\beta^n}{n}\int_0^1 e^{2\pi i\theta n}d\theta\right) \\
&= 0.
\end{aligned}$$

Ici on a pu rentrer l'intégrale dans la somme puisqu'elle converge uniformément.

Maintenant si $|\alpha| = 1$, on écrit

$$\int_0^1 \log|\alpha - e^{2\pi i\theta}|d\theta = \frac{1}{2\pi}\int_0^{2\pi} \log|1 - e^{i\theta}|d\theta.$$

Posons

$$J = \int_0^{2\pi} \log|1 - e^{i\theta}|d\theta.$$

On remarque que $|1 - e^{i\theta}| = 2\sin(\theta/2)$ et donc

$$J = 2\pi \log 2 + 2\int_0^{\pi} \log\sin x dx.$$

Cette intégrale existe puisque $\lim_{x\to 0} \frac{\sin x}{x} = 1$. On note aussi que $\sin x = 2\sin\frac{x}{2}\cos\frac{x}{2}$ et donc

$$\begin{aligned}\int_0^{\pi} \log\sin x dx &= \pi\log 2 + \int_0^{\pi} \log\sin\frac{x}{2}dx + \int_0^{\pi} \log\cos\frac{x}{2}dx \\ &= \pi\log 2 + 2\int_0^{\pi/2} \log\sin x dx + 2\int_0^{\pi/2} \log\cos x dx \\ &= \pi\log 2 + 2\int_0^{\pi} \log\sin x dx.\end{aligned}$$

On en conclut donc que $\int_0^{\pi} \log\sin x dx = -\pi\log 2$ et donc $J = 0$. □

Théorème 53 (Mahler)**.** Pour tout polynôme $F \in \mathbb{C}[x]$ non-nul, on a

$$m(F) = \int_0^1 \log|F(e^{2\pi i\theta})|d\theta.$$

Démonstration. Soit $\alpha \in \mathbb{C}$. La formule de Jensen nous donne

$$\int_0^1 \log|e^{2\pi i\theta} - \alpha|d\theta = \log\max\{1, |\alpha|\}.$$

En factorisant F de la forme

$$F(x) = a_r\prod_{i=1}^{r}(x - \alpha_i)$$

et en appliquant la formule de Jensen sur chaque facteur, on obtient le résultat. □

Nous connaissons des bornes assez précises sur la mesure de Mahler de certaines familles de polynômes. La plus connue d'entre elles est la famille des polynômes réciproques.

Définition 54. Soit $F \in \mathbb{C}[x]$ de degré r. Posons $F^*(x) := x^r F(x^{-1})$. On dit que F est réciproque si $F = \pm F^*$. Dans le cas inverse, on dit que F est non-réciproque.

La définition usuelle d'un polynôme réciproque demande que $F = F^*$, mais comme $M(F) = M(-F)$, la définition ci-dessus semble plus naturelle dans notre cas d'étude. Un polynôme réciproque est en fait un polynôme qui est symétrique par rapport à ses coefficients. Il se trouve que les polynômes non-réciproques ont généralement une mesure de Mahler plus grande que ceux réciproques.

Théorème 55 (Smyth)**.** Soit $F \in \mathbb{Z}[x]$ non-réciproque avec $F(1)F(0) \neq 0$. Alors

$$m(F) \geq m(x^3 - x - 1) = 0.281....$$

On remarque que multiplier n'importe quel polynôme réciproque par $x-1$ le rend non-réciproque et ne change pas sa mesure de Mahler. Il est donc naturel d'avoir la condition $F(1) \neq 0$. Ce théorème nous dit donc que $x^3 - x - 1$ est le polynôme non-réciproque ayant la plus petite mesure de Mahler sous les conditions mentionnées.

Un autre cas particulier où une borne inférieure sur la mesure de Mahler est connue est celui où toutes les racines du polynôme sont réelles.

Théorème 56 (Schinzel)**.** Soit $F \in \mathbb{Z}[x]$ avec toutes ses racines réelles. Alors

$$m(F) \geq \log\left(\frac{1+\sqrt{5}}{2}\right) = 0.481....$$

Maintenant, comme expliqué plus tôt dans cette section, il est important de connaître les cas où $M(F) \neq 1$ ou similairement les cas où $m(F) \neq 0$. Il se trouve que si $F \in \mathbb{Z}[x]$ est tel que $F(0) \neq 0$ et F est primitif, i.e. que le *pgcd* de ses coefficients est 1, alors $m(F) = 0$ si et seulement si tous les zéros de F sont racines de l'unité. Nous aurons besoin d'un résultat important avant de prouver ce théorème.

Théorème 57 (Kronecker)**.** Soit $\alpha \neq 0$ un entier algébrique et supposons que ses conjugués $\alpha_1, ..., \alpha_r$ (avec $\alpha_1 = \alpha$) sont tous de norme ≤ 1. Alors α est une racine de l'unité.

Démonstration. Considérons les polynômes

$$F_n(x) = \prod_{i=1}^{r}(x - \alpha_i^n).$$

Comme les conjugués de α_i^n sont tous de la forme α_j^n, on remarque que les F_n sont des polynômes unitaires à coefficients entiers. Comme $|\alpha_i^n| \leq 1$, les coefficients des F_n sont bornés uniformément par r et donc l'ensemble $\{F_n \ : \ n \in \mathbb{N}\}$ est fini. Il existe donc $n_2 > n_1$ tel que

$$F_{n_1} = F_{n_2}.$$

Nous avons alors l'égalité des deux ensembles

$$\{\alpha_1^{n_1}, ..., \alpha_r^{n_1}\} = \{\alpha_1^{n_2}, ..., \alpha_r^{n_2}\}.$$

Il existe donc une permutation $\tau \in S_r$ telle que

$$\alpha_i^{n_1} = \alpha_{\tau(i)}^{n_2}.$$

En élevant le tout à la n_1-ième puissance, on obtient

$$\alpha_i^{n_1^2} = \left(\alpha_{\tau(i)}^{n_1}\right)^{n_2} = \alpha_{\tau^2(i)}^{n_2^2}.$$

De même, on a

$$\alpha_i^{n_1^l} = \alpha_{\tau^l(i)}^{n_2^l}$$

pour tout l entier non-négatif. En particulier, si s est l'ordre de τ, on obtient

$$\alpha_i^{n_1^s} = \alpha_i^{n_2^s},$$

et alors

$$\alpha_i^{n_1^s}\left(\alpha_i^{n_2^s - n_1^s} - 1\right) = 0.$$

Comme $\alpha_i \neq 0$, on en conclut que α_i est une racine de l'unité. □

Nous pouvons maintenant nous attaquer au théorème mentionné plus haut.

Théorème 58. Soit $0 \neq F \in \mathbb{Z}[x]$ primitif et tel que $F(0) \neq 0$. Alors $m(F) = 0$ si et seulement si toutes les racines de F sont des racines de l'unité.

Démonstration. Si toutes les racines de F sont des racines de l'unité, alors F divise $x^N - 1$ pour un certain N non-négatif et on en conclut que le premier coefficient de F est ± 1. Par la définition de $m(F)$, on voit directement que $m(F) = 0$.

Réciproquement, supposons que $m(F) = 0$. Encore par la définition de $m(F)$ on voit que le premier coefficient de F doit être ± 1 et donc les racines de F sont des entiers algébriques. Comme $m(F) = 0$, on doit avoir $|\alpha_i| \leq 1$ pour toute racine α_i de F. Par le théorème de Kronecker, les racines de F sont toutes des racines de l'unité. □

2.2 Le cas à plusieurs variables

Nous avons vu dans la section précédente que si $0 \neq F \in \mathbb{C}[x]$, alors

$$m(F) = \int_0^1 \log |F(e^{2\pi i\theta})| d\theta.$$

Ceci nous donne une manière naturelle de généraliser la mesure de Mahler pour les polynômes à plusieurs variables.

Définition 59. Soit $F \in \mathbb{C}[x_1, ..., x_n]$ non-nul. Alors la mesure de Mahler de F est

$$m(F) = \int_0^1 \dots \int_0^1 \log |F(e^{2\pi i\theta_1}, \dots, e^{2\pi i\theta_n})| d\theta_1 \dots d\theta_n.$$

En d'autres termes, si on pose $M(P) = e^{m(P)}$, alors $M(P)$ est la moyenne géométrique de $|P|$ sur le n-tore $\mathbb{T}^n$.

Il se trouve que cette intégrale existe toujours en tant qu'intégrale impropre et $m(F) \geq 0$ si $F \in \mathbb{Z}[x_1, \dots, x_n]$.

Il est aussi naturel d'étendre cette définition aux polynômes de Laurent

$$F \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$$

en notant que la mesure de Mahler de tout monôme est nulle et que $m(FG) = m(F) + m(G)$.

Même si à première vue la définition de la mesure de Mahler donnée ci-haut ne semble pas reliée à la théorie des nombres, certaines valeurs spéciales peuvent être exprimées en termes de concepts fondamentaux de cette théorie.

Proposition 60. On a les identités suivantes :
(i) $m(2 + x_1 + x_2) = \log 2$,
(ii) $m(1 + x_1 + x_2) = \frac{3\sqrt{3}}{4\pi} L(\chi, 2)$, où $L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ est la fonction-L de Dirichlet de χ où $\chi(n) = \left(\frac{n}{3}\right)$ est le symbole de Legendre,
(iii) $m(1 + x_1 + x_2 + x_3) = \frac{7}{2\pi^2}\zeta(3)$ où $\zeta(s)$ est la fonction zêta de Riemann.

La mesure de Mahler peut donc être mise en relation avec la fonction zêta de Riemann classique et sa torsion avec un caractère de Dirichlet. Dans le cas qui nous intéresse, la mesure de Mahler sera reliée à la fonction-L d'une courbe elliptique.

Comme dans le cas à une variable, les cas où $m(F) = 0$ peuvent être complètement caractérisés lorsque F est à coefficients entiers.

Théorème 61 (Smyth)**.** Soit $F \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ primitif. Alors $m(F) = 0$ si et seulement si F est un produit de monômes et de polynômes cyclotomiques évalués en des monômes.

Un concept fondamental à l'étude de la mesure de Mahler de polynômes à coefficients entiers est celui du polygone de Newton. Historiquement, le polygone de Newton était un outil pour étudier les polynômes dans les corps locaux, principalement $K((X))$ le corps de fractions de l'anneau des séries formelles avec indéterminé X où K est le corps réel ou complexe, mais aussi dans $\mathbb{Q}_p$ le corps p-adique et ses extensions finies. Pour plus d'informations, voir [11].
Nous définissons ici seulement le cas à deux variables puisque nous n'utiliserons pas les généalisations.

Définition 62. Soit $F \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ non-nul avec développement

$$F(x, y) = \sum_{(i,j) \in \mathbb{Z}^2} a_{i,j} x^i y^j,$$

où $a_{i,j} = 0$ pour presque tous les couples (i, j). Alors, le polygone de Newton de F, noté $\mathcal{C}(F)$, est l'enveloppe convexe des $(i, j) \in \mathbb{Z}^2$ tels que $a_{i,j} \neq 0$.
On dit que F est extrême-unitaire si les coefficients associés aux sommets de $\mathcal{C}(F)$ sont de norme 1, i.e. si (i, j) est un sommet de $\mathcal{C}(F)$, alors $|a_{i,j}| = 1$.

Les pentes et les longueurs des côtés du polygone de Newton nous donnent beaucoup d'informations sur la valuation (p-adique) des racines de F. La propriété « logarithmique » de la valuation présage une propriété similaire pour les polygones de Newton.

Proposition 63. Soit $F, G \in \mathbb{C}[x, y]$. Alors,
(i) $\mathcal{C}(FG) = \mathcal{C}(F) + \mathcal{C}(G)$,
(ii) tout sommet de $\mathcal{C}(FG)$ est une unique somme d'un sommet de $\mathcal{C}(F)$ avec un sommet de $\mathcal{C}(G)$,
(iii) si deux de F, G et FG sont extrême-unitaires, alors l'autre l'est aussi.

Ici $\mathcal{C}(F) + \mathcal{C}(G)$ est la somme de Minkowski, i.e.

$$\mathcal{C}(F) + \mathcal{C}(G) = \{a + b \ : \ a \in \mathcal{C}(F), b \in \mathcal{C}(G)\}.$$

Un résultat similaire au théorème 58 existe pour les polynômes extrême-unitaires. Avant de l'énoncer, nous aurons besoin d'une définition.

Définition 64. Un polynôme non-nul $F \in \mathbb{C}[x]$ est dit unité-unitaire si

$$F = a_r x^r + ... + a_1 x + a_0,$$

avec $|a_r| = |a_0| = 1$.

Théorème 65. Soit $F \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ extrême-unitaire. Alors $m(F) = 0$ si et seulement si F est un produit de monômes et de polynômes unité-unitaires évalués en des monômes.

Nous finissons cette section avec une définition qui sera utilisée maintes fois dans les sections suivantes.

Définition 66. Soit $\mathcal{C}(F)$ le polygône de Newton d'un polynôme

$$F(x, y) = \sum_{(i,j)\in\mathbb{Z}^2} a_{i,j} x^i y^j,$$

et orientons $\mathcal{C}(F)$ dans le sens horaire. À chaque côté τ de $\mathcal{C}(F)$ on associe le polynôme

$$F_\tau(t) = \sum_k a_{\tau(k)} t^k,$$

où $\tau(k)$ parcoure dans le sens horaire tous les points de $\mathbb{Z}^2$ se trouvant sur τ (clairement il n'y a qu'un nombre fini de tels points, donc la somme ci-dessus est finie). On dit que F est *tempéré* si les racines de $P_\tau(t)$ ne sont que des racines de l'unité pour tout côté τ de $\mathcal{C}(F)$. Si F est unitaire à coefficients entiers, par le théorème de Kronecker, ceci est équivalent à ce que $m(P_\tau) = 0$ pour tout côté τ.

2.3 Relations avec la théorie des nombres et les courbes elliptiques

À l'origine, la mesure de Mahler a été introduite par Mahler [10] en 1962 pour donner une preuve plus simple de l'inégalité de *Gel'fond-Mahler* qui stipule que pour $P_1, ..., P_n \in \mathbb{C}[x_1, ..., x_r]$ des polynômes multivariés de degré respectif $q_1, \ldots, q_n$, alors

$$\|P_1\| \ldots \|P_n\| \leq C_n^q \|P_1 \ldots P_n\|, \quad \text{où } q = q_1 + \ldots + q_n,$$

où C_n est une constante ne dépendant possiblement que de n et

$$\|P\| = \sup_{|t|=1} |P(t)|.$$

Gel'fond [12] prouva cette inégalité avec $C_n = e$ et Mahler [9] avec $C_n = 2$. David Boyd [13] prouva ce résultat avec les meilleures constantes possibles, où

$$C_n = \exp\left(\frac{\pi}{n} I\left(\frac{\pi}{n}\right)\right), \quad \text{où } I(\theta) = \int_0^\theta \log\left(2\cos\frac{t}{2}\right) dt.$$

La mesure de Mahler était aussi utilisée pour décrire l'entropie de certains systèmes dynamiques []. Ce n'est que dans les années 90 que ses liens avec la théorie des nombres commencèrent à devenir apparents. Plus précisément, Deninger [14] et Boyd [1] trouvèrent de nombreux rapports avec les fonctions-L de courbes elliptiques et les conjectures de Bloch-Beĭlinson. Nous donnons ici une brève introduction (ou plutôt une intuition) derrière ces conjectures fondamentales.

Soit $K/\mathbb{Q}$ un corps de nombres et $\mathcal{O}_K$ son anneau des entiers. Nous définissons la fonction zêta de K comme

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s},$$

où la somme parcourt tous les idéaux non-nuls de $\mathcal{O}_K$ et $N\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$. Remarquons que lorsque $K = \mathbb{Q}$, $\zeta_K(s)$ est la fonction zêta de Riemann classique.

$\zeta_K(s)$ converge absoluement pour $\Re(s) > 1$ et possède une extension méromorphe sur tout le plan complexe avec un unique pôle simple en $s = 1$. La formule du nombre de classes nous dit que le résidu est

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot h_K}{w_K \sqrt{|D_K|}}.$$

où r_1 est le nombre de plongements de K dans $\mathbb{R}$, r_2 est le nombre de plongement de K dans $\mathbb{C}$ à conjugaison près, Reg_K est le régulateur de K, h_K est la cardinalité du groupe de classes de K, w_K est le nombre de racines de l'unité contenu dans K et D_K est le discriminant de l'extension $K/\mathbb{Q}$ (Pour plus d'informations sur ces définitions, consultez [11]).

En particulier, on peut montrer que lorsque $F \subset \mathbb{R}$ est une extension réelle quadratique de $\mathbb{Q}$, alors $\mathcal{O}_F^*$ est un $\mathbb{Z}$-module de rang 1 et

$$\zeta_K'(0) \sim_{\mathbb{Q}^*} \log|\epsilon|, \quad \epsilon \in \mathcal{O}_F^*,\ \epsilon \neq \pm 1.$$

Ici $a \sim_{\mathbb{Q}^*} b$ signifie que $a/b \in \mathbb{Q}^*$, où $a, b \in \mathbb{C}^*$.

Les conjectures de Bloch-Beĭlinson généralisent ce résultat. Les composantes sont : (1) un objet géométrique / arithmétique $\mathcal{O}$ ($\mathcal{O}_F$ dans notre exemple),

(2) un groupe abélien $K(\mathcal{O})$ de type fini de rang 1 associé ($\mathcal{O}_F^*$ dans notre exemple),
(3) une fonction-L associée $L(\mathcal{O}, s)$ avec un zéro simple en $s = 0$ ($\zeta_F(s)$ dans notre exemple), et
(4) un morphisme non-nul $r : K(\mathcal{O})/K(\mathcal{O})_{\text{tors}} \to \mathbb{R}$ (la fonction $\log(|\cdot|)$ dans notre exemple).
Dans ce contexte, l'identité ci-dessus devient

$$L'(\mathcal{O}, 0) \sim_{\mathbb{Q}^*} r(\alpha), \quad \alpha \in K(\mathcal{O})/K(\mathcal{O})_{\text{tors}}.$$

Dans le cas de courbes elliptiques $E/\mathbb{Q}$, les composantes seront :
(1) $\mathcal{E}$ un modèle de Néron de E,
(2) $K_2(\mathcal{E})$, le groupe K_2 de la courbe,
(3) la fonction-L de E, i.e. $L(E, s)$, et
(4) r le régulateur de E.
Avec ces conditions, l'identité

$$L'(E, 0) \sim_{\mathbb{Q}^*} r(\alpha), \quad \alpha \in K_2(\mathcal{E})/K_2(\mathcal{E})_{\text{tors}}.$$

constitue les conjectures de Bloch-Beĭlinson.

Nous ne définirons pas le modèle de Néron $\mathcal{E}$ d'une courbe elliptique E puisque cela nous mènerait trop loin du sujet principal (et l'auteur ne comprend pas à la perfection la théorie). Par contre, nous définissons brièvement le régulateur r et nous donnons une idée du groupe $K_2(E)$. Pour les besoins de la cause, $\mathcal{E}$ peut être vue comme une bonne approximation entière de E, un peu comme l'anneau des entiers $\mathcal{O}_K$ est une approximation entière du corps de nombres K. Pour plus d'informations, voir [15].

Soit F un corps. Alors le théorème de Matsumoto nous dit que

$$K_2(F) \cong F^* \otimes_{\mathbb{Z}} F^*/\{x \otimes (1-x) \ : \ x \in F, x \neq 0, 1\}.$$

Lorsque $E/\mathbb{Q}$ est une courbe elliptique définie par un polynôme tempéré $P(x, y) = 0$, on peut considérer $K_2(E) \otimes \mathbb{Q} \subset K_2(\mathbb{Q}(E)) \otimes \mathbb{Q}$ (voir [4]). Si $\mathcal{E}$ désigne le modèle de Néron de E, $K_2(\mathcal{E}) \otimes \mathbb{Q}$ est un sous-groupe de $K_2(E) \otimes \mathbb{Q}$ défini par un nombre fini de conditions.

Soient $x, y \in \mathbb{Q}(E)$. On considère la forme différentielle

$$\eta(x, y) := \log|x| d\arg y - \log|y| d\arg x, \quad d\arg x := \text{Im}(dx/x).$$

On remarque que η est fermée (sa dérivée extérieure est nulle) sur son domaine de définition, antisymétrique et multiplicative et

$$\eta(x, 1-x) = dD(x),$$

où

$$D(x) := \mathrm{Im}(\mathrm{Li}_2(x)) + \arg(1-x)\log|x|$$

est appelé le dilogarithme de Bloch-Wigner et

$$\mathrm{Li}_2(x) = -\int_0^x \frac{\log(1-z)}{z} dz.$$

Nous avons maintenant tous les ingrédients pour définir le régulateur de Bloch-Beĭlinson.

Définition 67. Le régulateur de Bloch [16] et Beĭlinson [17] est défini par

$$\begin{aligned} r_E \colon K_2(E) \otimes \mathbb{Q} &\to H^1(E, \mathbb{R}) \\ \{x, y\} &\mapsto \left\{ [\gamma] \mapsto \int_\gamma \eta(x, y) \right\}. \end{aligned}$$

(Voir section 1.2.9 pour la définition de $H^1(E, \mathbb{R})$).

En étudiant comment la conjugaison complexe agit sur η, on remarque que le régulateur est trivial sur $H_1(E, \mathbb{Z})^+$, les classes invariantes par conjugaison complexe. Donc le régulateur peut être vu comme une fonction sur $H_1(E, \mathbb{Z})^-$, les classes non-invariantes sous conjugaison.

Il se trouve que la mesure de Mahler peut être reliée au régulateur et donc, si l'on en croit les conjectures de Bloch-Beĭlinson, la mesure de Mahler d'un polynôme $P(x, y) = 0$ associé à une courbe elliptique E est reliée à certaines valeurs spéciales de la fonction-L $L(E, s)$. Plus spécifiquement, rappelons-nous que nous avons la suite d'isomorphismes

$$\begin{array}{ccccc} E(\mathbb{C}) & \to & \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) & \to & \mathbb{C}^\times/q^{\mathbb{Z}} \\ T = (\wp(u), \wp'(u)) & \mapsto & u \bmod \Lambda & \mapsto & z = e^{2\pi i u}, \end{array}$$

où $\wp$ est la fonction de Weierstrass, Λ est la lattice $\mathbb{Z} + \tau\mathbb{Z}$ avec $\tau \in \mathbb{H} = \{x \in \mathbb{C} \ : \ \Im(x) > 0\}$ et $q = e^{2\pi i \tau}$.

Définition 68. (Voir [16]) Le dilogarithme elliptique est défini par

$$\begin{aligned} D^E \ : E(\mathbb{C}) &\to \mathbb{C} \\ P &\mapsto \sum_{n \in \mathbb{Z}} D\left(q^n z\right), \end{aligned}$$

où D est le dilogarithme de Bloch-Wigner et $z \in \mathbb{C}^*/q^{\mathbb{Z}}$ est donné par la correspondance ci-dessus.

Nous définissons aussi l'opérateur diamant d'une courbe elliptique.

Définition 69. Soit $\mathrm{Div}(E(\mathbb{C}))$ le groupe des diviseurs de E et posons

$$\mathrm{Div}(E(\mathbb{C}))^- = \mathrm{Div}(E(\mathbb{C}))/\{(P) + (-P) \ : \ P \in E(\mathbb{C})\}.$$

Soient $x, y \in \mathbb{C}(E)^*$. L'opérateur diamant est donné par

$$\begin{aligned} \diamond \ : \ \mathbb{C}(E)^* \otimes_{\mathbb{Z}} \mathbb{C}(E)^* &\to \mathrm{Div}(E(\mathbb{C}))^- \\ \{x, y\} &\mapsto (x) \diamond (y) := \sum_{i,j} m_i n_j (S_i - T_j), \end{aligned}$$

où

$$(x) = \sum_i m_i (S_i), \quad (y) = \sum_j n_j (T_j).$$

Ceci mène au résultat suivant.

Théorème 70 (Bloch)**.** Le dilogarithme elliptique s'étend par linéarité à une fonction de $\mathrm{Div}(E(\mathbb{C}))^-$ à $\mathbb{C}$. Soient $x, y \in \mathbb{Q}(E)$ et $\{x, y\} \in K_2(E)$. Alors

$$r_E(\{x, y\})[\gamma] = D^E((x) \diamond (y)),$$

où $[\gamma]$ est un générateur de $H_1(E, \mathbb{Z})^-$.
En particulier, on a

$$D^E((x) \diamond (1 - x)) = 0, \quad \forall x \in \mathbb{Q}(E).$$

Des formules du type

$$m(P) = \frac{1}{2\pi} r_E(\{x, y\})[\gamma] \tag{2.1}$$

ont d'abord été prédites par Deninger [14] puis intensivement étudiées par Boyd [1].

Par exemple, soit $P(x, y) \in \mathbb{C}[x, y]$ un polynôme de degré 2 en y, i.e. de la forme

$$P(x, y) = P^*(x)(y - y_1(x))(y - y_2(x)),$$

où y_1, y_2 sont des fonctions algébrique en x.

En utilisant la formule de Jensen, on obtient

$$\begin{aligned} m(P) - m(P^*) &= \frac{1}{(2\pi i)^2} \int_{\mathbb{T}^2} \log|P(x,y)| \frac{dx}{x}\frac{dy}{y} - m(P^*) \\ &= \frac{1}{(2\pi i)^2} \int_{\mathbb{T}^2} \left(\log|y - y_1(x)| + \log|y - y_2(x)|\right) \frac{dx}{x}\frac{dy}{y} \\ &= \frac{1}{2\pi i} \int_{|x|=1, |y_1(x)|\geq 1} \log|y_1(x)| \frac{dx}{x} + \frac{1}{2\pi i} \int_{|x|=1, |y_2(x)|\geq 1} \log|y_2(x)| \frac{dx}{x}. \end{aligned}$$

Dans certaines situations, $|y_2(x)| \leq 1$ lorsque $|x| = 1$. Dans ce cas, on peut écrire

$$\begin{aligned} m(P) - m(P^*) &= \frac{1}{2\pi i} \int_{|x|=1, |y_1(x)|\geq 1} \log|y_1(x)| \frac{dx}{x} \\ &= \frac{1}{2\pi} \int_{|x|=1, |y_1(x)|\geq 1} \eta(x, y_1). \end{aligned}$$

Lorsque $P = 0$ définie une courbe elliptique et si l'ensemble $\{|x| = 1, |y_1(x)| \geq 1\}$ peut être vu comme un cycle dans $H_1(E, \mathbb{Z})$, alors on obtient des formules du type (2.1).

Par exemple, Boyd étudia les familles de polynômes

$$R_k(x,y) = (1+x)(1+y)(x+y) - kxy, \tag{2.2}$$

$$P_{k,b}(x,y) = y^2 + kxy + by - x^3, \tag{2.3}$$

où k, b sont considérées comme des paramètres fixes.

Pour la première famille, Boyd conjectura pour $|k| \leq 100$

$$m(R_k(x,y)) \stackrel{?}{=} r_k L'(E_{N(k)}, 0),$$

où $E_{N(k)}$ est la courbe elliptique définie par $R_k(x,y) = 0$, $N(k)$ est le conducteur et r_k est un nombre rationnel avec une petite hauteur, i.e. $r_k = a/b$ avec $\max(a,b)$ petit.

Certaines formules ont été prouvées. Par exemple, Rogers et Zudilin [18] prouvèrent

$$\begin{aligned} m(R_{-2}(x,y)) &= \frac{15}{\pi^2} L(E_{20}, 2) = 3L'(E_{20}, 0), \\ m(R_4(x,y)) &= \frac{10}{\pi^2} L(E_{20}, 2) = 2L'(E_{20}, 0). \end{aligned}$$

Pour la deuxième famille, quand $b = 1$ et $k \in \mathbb{Z}$, Boyd conjectura des formules du type

$$m(P_k(x,y)) \stackrel{?}{=} r_k L'(E_{N(k)}, 0),$$

avec $E_{N(k)}$, $N(k)$ et r_k définis comme ci-dessus.

Dans ce cas, $P_{k,1}(x, y)$ est un polynôme tempéré, ce qui explique la forme de l'équation. Par contre, pour $b = 2$, $P_{k,2}(x, y)$ n'est pas nécessairement tempéré et Boyd prédit des formules de la forme

$$m(P_{k,b}) \stackrel{?}{=} \frac{1}{3} \log b + r_{k,b} L'(E_{k,b}, 0).$$

Presque toutes les formules étudiées par Boyd relèvent de calculs numériques et non de preuves mathématiques.

D'autres formules ont été prouvées par Bertin [19], Bertin and Zudilin [20], Brunault [21], Lalín [22], Lalín et Ramanmonjisoa [23], Lalín and Mittal [24], Lalín, Samart, et Zudilin [25], Mellit [26] et Rodriguez-Villegas [27].

Chapitre 3

Résultats

> Je compte tes *L's* avec une loi de Poisson.
>
> MC Lima-Barbosa

Ce chapitre a pour but de « prouver » la conjecture qu'est mon projet de recherche. « Prouver » se trouve ici malheureusement entre guillemets puisque cette conjecture s'avère en fait fausse malgré la preuve que nous pensions avoir trouvé. Une erreur s'y est malencontreusement glissée et nous l'avons découverte après avoir développé la plupart de la preuve. Certains résultats restent cependant vrais et nous les prouvons ici. Nous mentionnons aussi les résultats qui sont finalement faux, tout en mentionnant où le problème survient.

La conjecture, d'abord donnée par Boyd [1], dit qu'on a l'identité suivante

$$m(P_{4,2}) = m(y^2 + 4xy + 2y - x^3) \stackrel{?}{=} \frac{1}{3}\log 2 + \frac{8}{3}L'(E_{20}, 0).$$

Il se trouve qu'un calcul PARI donne $m(P_{4,2}) = 1,29388262...$ tandis que $\frac{1}{3}\log 2 + \frac{8}{3}L'(E_{20}, 0) = 1,29656143....$

L'idée était de relier la mesure de Mahler de ce polynôme avec celle de

$$R_{-2} = (1 + x)(1 + x)(x + y) + 2xy,$$

puisque ces deux polynômes définissent des courbes elliptiques de conducteur 20. Puisque $m(R_{-2})$ est déjà connue, ceci nous donnait une avenue intéressante pour trouver $m(P_{4,2})$. Avec cette idée en tête, nous avons trouvé un changement de variable transformant $P_{4,2}$ en $\widehat{P_{4,2}}$, où $\widehat{P_{4,2}}$ est un polynôme tempéré. $\widehat{P_{4,2}}$ et R_{-2} étant tempérés, la théorie (voir

[4]) nous dit que leur mesure de Mahler dépend seulement de la classe d'homologie de certains cycles facilement calculables, ce qui nous permet d'avoir une identité entre $m(\widehat{P_{4,2}})$ et $m(R_{-2})$.

Le problème fondamental ici est que le changement de variables entre $P_{4,2}$ et $\widehat{P_{4,2}}$ n'est pas rationnel, ce qui nous empêche d'utiliser la théorie et de relier les mesures de Mahler correspondantes. Par contre, ceci ne nous empêche pas de donner quelques résultats dans le chapitre qui suit.

3.1 Isomorphismes et opérateur diamant

Cette section a pour but de relier $P_{4,2}$ et R_{-2} à des courbes elliptiques. Comme mentionné à la section 2.3, ceci nous donnera une relation entre les régulateurs correspondants.

Soit E_1 la courbe elliptique définie par $\{P_{4,2} = 0\}$ et E_2 par $\{R_{-2} = 0\}$. Alors on a l'isomorphisme de courbes elliptiques suivant

$$\varphi\colon E_2 : (1+x)(1+y)(x+y) + 2xy = 0 \to E_1 : Y^2 + 4XY + 2Y - X^3 = 0$$

donné par

$$X = -\frac{2(x+y+1)}{2+x+y}, \qquad Y = \frac{2(1+y+2x)}{2+x+y}, \tag{3.1}$$

$$x = \frac{X+Y}{2+X}, \qquad y = -\frac{2+3X+Y}{2+X}. \tag{3.2}$$

Les points de torsion rationnels de E_1 sont générés par $P = (-2, 2)$. Plus précisément, on a $E_1(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$ et

$$P = (-2,2),\ 2P = (0,0),\ 3P = (-1,1),\ 4P = (0,-2),\ 5P = (-2,4).$$

Avec cet isomorphisme en main, on relie l'opérateur diamant de X, Y et $x \circ \varphi^{-1}$, $y \circ \varphi^{-1}$. C'est le premier pas pour possiblement trouver une relation entre les intégrales sur $\eta(X, Y)$ et $\eta(x \circ \varphi^{-1}, y \circ \varphi^{-1})$. (La dernière intégrale a déjà été trouvée comme mentionné au début de ce chapitre.)

Proposition 71. On a les relations suivantes dans $\mathrm{Div}(E_1(\mathbb{Q}))^-$

$$(X) \diamond (Y) = 9(2P), \tag{3.3}$$
$$(x \circ \varphi^{-1}) \diamond (y \circ \varphi^{-1}) = -6(P) - 6(2P). \tag{3.4}$$

Démonstration. Tout d'abord, on calcule sur E_1 les diviseurs suivants

$$\begin{aligned}
&(X) = (4P) + (2P) - 2(O),\\
&(Y) = 3(2P) - 3(O),\\
&(X+Y) = (P) + (2P) + (3P) - 3(O),\\
&(2 + 3X + Y) = (4P) + (5P) + (3P) - 3(O),\\
&(2+X) = (P) + (5P) - 2(O).
\end{aligned}$$

Nous obtenons donc sur $\mathbb{Z}[E_1(\mathbb{Q})]^-$

$$(X) \diamond (Y) = 9(2P).$$

On voit que

$$\begin{aligned}
(x \circ \varphi^{-1}) &= \left(\frac{X+Y}{2+X}\right) = (2P) + (3P) - (5P) - (O),\\
(y \circ \varphi^{-1}) &= \left(\frac{2+3X+Y}{2+X}\right) = (4P) + (3P) - (P) - (O).
\end{aligned}$$

Ceci implique donc que

$$(x \circ \varphi^{-1}) \diamond (y \circ \varphi^{-1}) = -6(P) - 6(2P).$$

□

Nous donnons maintenant une relation entre le dilogarithme D^{E_1} (voir Section 2.3) de $(x \circ \varphi^{-1}) \diamond (y \circ \varphi^{-1})$ et $(X) \diamond (Y) \in \mathbb{Z}[E_1(\mathbb{Q})]^-$. Pour ce faire, nous définissons une relation d'équivalence. On dit que $\alpha \sim \beta$ si

$$D^{E_1}(\alpha) = D^{E_1}(\beta).$$

Par le théorème 70, on a que

$$\alpha - \beta = \sum c_i(f_i) \diamond (1 - f_i) \Longrightarrow \alpha \sim \beta,$$

où $f_i \in \mathbb{Q}(E_1)$ et $c_i \in \mathbb{Z}$.

Proposition 72. On a l'identité suivante sur $\mathbb{Z}[E_1(\mathbb{Q})]^-$

$$-8\left((x \circ \varphi^{-1}) \diamond (y \circ \varphi^{-1})\right) \sim 9\left((X) \diamond (Y)\right).$$

Démonstration. Tout d'abord, nous définissons $R = (-\frac{3}{2} + \frac{\sqrt{5}}{2}, 2 - \sqrt{5})$ où R est un point sur E_1 et $R^\sigma = (-\frac{3}{2} - \frac{\sqrt{5}}{2}, 2 + \sqrt{5})$ où σ est l'élément non-trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$. Remarquons que $R + R^\sigma = 3P$.

Nous avons besoin de considérer des fonctions f_i où f_i et $1 - f_i$ traversent E_1 en des points rationnels dans une extension de $\mathbb{Q}$.

Premièrement, considérons $f_1 = -2X - Y$. On calcule

$$\begin{aligned}(-2X - Y) &= (2P) + 2(5P) - 3(O),\\ (1 + 2X + Y) &= (3P) + (R) + (R^\sigma) - 3(O),\end{aligned}$$

et

$$\begin{aligned}(-2X - Y) \diamond (1 + 2X + Y) =& 5(P) - (2P) + 3(R) + 3(R^\sigma) - 2(R + P) - 2(R^\sigma + P) - (R - 2P)\\ &- (R^\sigma - 2P).\end{aligned}$$

Ensuite nous posons $f_2 = \frac{X^2+X-Y}{X^2+X}$ et nous obtenons

$$\begin{aligned}\left(\frac{X^2 + X - Y}{X^2 + X}\right) &= (P) - 2(3P) - (4P) + (R) + (R^\sigma),\\ \left(\frac{Y}{X^2 + X}\right) &= 2(2P) - 2(3P) - (4P) + (O),\end{aligned}$$

et

$$\left(\frac{X^2+X-Y}{X^2+X}\right)\diamond\left(\frac{Y}{X^2+X}\right) = -5(P)+(2P)+3(R)+3(R^\sigma)+(R+P)+(R^\sigma+P) \\ +2(R-2P)+2(R^\sigma-2P).$$

Finalement, $f_3=\frac{4X+Y+4}{2X+2}$ et

$$\left(\frac{4X+Y+4}{2X+2}\right) = -2(3P)+(5P)-(O)+(R+2P)+(R^\sigma+2P),$$
$$\left(\frac{-2X-Y-2}{2X+2}\right) = 2(P)-2(3P)+(4P)-(O),$$

et

$$\left(\frac{4X+Y+4}{2X+2}\right)\diamond\left(\frac{-2X-Y-2}{2X+2}\right) = 6(P)-9(2P)+3(R+P)+3(R^\sigma+P)+3(R-2P) \\ +3(R^\sigma-2P).$$

En combinant le tout, nous avons

$$((f_1)\diamond(1-f_1))-((f_2)\diamond(1-f_2))+((f_3)\diamond(1-f_3)) = 16(P)-11(2P) \Longrightarrow 16(P)-11(2P)\sim O,$$

ce qui implique

$$\Longrightarrow 16(P)+16(2P)\sim 27(2P)$$
$$\Longrightarrow 48(P)+48(2P)\sim 81(2P)$$
$$\Longrightarrow -8\left((x\circ\varphi^{-1})\diamond(y\circ\varphi^{-1})\right)\sim 9\left((X)\diamond(Y)\right).$$

Ceci conclut la preuve. □

3.2 Polynôme tempéré

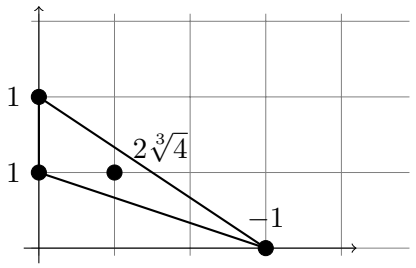
Le polynôme $P_{4,2}$ n'étant pas tempéré, les conjectures de Boyd (voir Section 2.3) prédisent un terme logarithmique dans une formule pour sa mesure de Mahler. L'idée

est donc de relier la mesure de Mahler de $P_{4,2}$ avec celle d'un polynôme tempéré.

Rappelons-nous que $P_{4,2}$ est le polynôme $Y^2 + 4XY + 2Y - X^3$. En posant $Y = 2\widehat{Y}$, $X = \sqrt[3]{4}\widehat{X}$ et en divisant par 4, on obtient le polynôme

$$\widehat{P_{4,2}} = \hat{Y}^2 + 2\sqrt[3]{4}\hat{X}\hat{Y} + \hat{Y} - \hat{X}^3.$$

On remarque que ce polynôme est tempéré puisque son polygone de Newton est



Avec ce changement de variables, la mesure de Mahler devient

$$\begin{aligned} m(P_{4,2}) &= -\frac{1}{2\pi}\int_{|X|=1\ ,\ |Y_+|\geq 1} \eta(X, Y_+) - \frac{1}{2\pi}\int_{|X|=1\ ,\ |Y_-|\geq 1} \eta(X, Y_-) \\ &= -\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}\ ,\ |\hat{Y}_+|\geq\frac{1}{2}} \eta(\sqrt[3]{4}\hat{X}, 2\hat{Y}_+) - \frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}\ ,\ |\hat{Y}_-|\geq\frac{1}{2}} \eta(\sqrt[3]{4}\hat{X}, 2\hat{Y}_-). \end{aligned}$$

On verra dans la prochaine section que

$$-\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}\ ,\ |\hat{Y}_+|\geq\frac{1}{2}} \eta(\sqrt[3]{4}\hat{X}, 2\hat{Y}_+) = 0,$$

et donc en utilisant la multiplicativité de η, on obtient

$$m(P_{4,2}) = -\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}\ ,\ |\hat{Y}_-|\geq\frac{1}{2}} \Big(\eta(\hat{X}, \hat{Y}_-) + \log(\sqrt[3]{4})d\arg\hat{Y}_-\Big) + \log 2.$$

Comme $\widehat{P_{4,2}}$ et R_{-2} sont tempérés, il serait intéressant de relier les classes d'homologie de ces deux polynômes pour ensuite obtenir une relation sur leur mesure de Mahler respective. Or, nous ne pouvons pas le faire puisque $\widehat{P_{4,2}}$ n'est pas un polynôme rationnel et nous n'avons toujours pas trouvé un moyen de contourner ce problème.

3.3 Le chemin d'intégration

Nous identifions maintenant dans quels cas les chemins d'intégration dans la mesure de Mahler sont fermés. Ceci nous permet de ne considérer qu'une intégrale sur η.

À la place de considérer $P_{4,2}(X,Y)$, nous faisons le changement de variables $Y = ZX$ et divisons le polynôme résultant pas X^2. Ceci nous donne

$$T(X,Z) = Z^2 + 4Z + \frac{2}{X}Z - X.$$

Si $|X| = 1$, i.e. $X = e^{i\theta}$, on peut écrire

$$Z_\pm = -e^{-i\theta} - 2 \pm \sqrt{4 + 4e^{-i\theta} + e^{i\theta} + e^{-2i\theta}}.$$

Nous prenons ici toujours la branche principale de la racine carrée, i.e.

$$\sqrt{z} = \sqrt{|z|}e^{i\frac{\arg z}{2}}, \quad -\pi < \arg z \leq \pi.$$

Proposition 73. $|X| = 1,\ |Z_-| \geq 1$, et $|X| = 1,\ |Z_+| \leq 1$ sont des chemins fermés.

Démonstration. Puisque $|Z_-||Z_+| = |X| = 1$, nous avons seulement besoin de prouver que $|Z_-| \geq 1$ lorsque $|X| = 1$.

Comme $|X| = 1$, nous avons

$$\begin{aligned} |Z_-| &= |\sqrt{4 + 4e^{-i\theta} + e^{i\theta} + e^{-2i\theta}} + e^{-i\theta} + 2| \\ &= |\sqrt{5\cos(\theta) + \cos(2\theta) + 4 - 3i\sin(\theta) - i\sin(2\theta)} + e^{-i\theta} + 2|. \end{aligned}$$

Posons $R = \sqrt{5\cos(\theta) + \cos(2\theta) + 4 - 3i\sin(\theta) - i\sin(2\theta)}$. Alors

$$\begin{aligned} |Z_-| &= \sqrt{(R + e^{-i\theta} + 2)(\overline{R} + e^{i\theta} + 2)} \\ &= \sqrt{|R|^2 + 2\mathrm{Re}(R)\cos(\theta) - 2\mathrm{Im}(R)\sin(\theta) + 4\mathrm{Re}(R) + 4\cos(\theta) + 5}. \end{aligned}$$

Donc nous avons besoin de montrer que

$$|R|^2 + 2\mathrm{Re}(R)\cos(\theta) - 2\mathrm{Im}(R)\sin(\theta) + 4\mathrm{Re}(R) + 4\cos(\theta) + 5 \geq 1.$$

Nous concentrons notre attention lorsque $\theta \in (0, \pi)$. Remarquons que

$$|R|^2 = 2\left(4\cos\left(\frac{\theta}{2}\right) + \cos\left(\frac{3\theta}{2}\right)\right)$$

et

$$\arg(R^2) = -\frac{\theta}{2}.$$

Alors

$$R = \sqrt{2}\sqrt{(4\cos(\theta/2) + \cos(3\theta/2))}e^{-i\frac{\theta}{4}}.$$

Notre équation devient maintenant

$$\begin{aligned}|Z_-|^2 =& |R|^2 + 2|R|\cos(\theta)\cos(\theta/4) + 2|R|\sin(\theta)\sin(\theta/4) + 4|R|\cos(\theta/4) + 4\cos(\theta) + 5\\ =& |R|\left(|R| + 4\cos(\theta/4) + 2\cos(3\theta/4)\right) + 4\cos(\theta) + 5\\ =& 8\cos(\theta/2) + 4\cos(\theta) + 2\cos(3\theta/2)\\ &+ \sqrt{2}\left(4\cos(\theta/4) + 2\cos(3\theta/4)\right)\sqrt{4\cos(\theta/2) + \cos(3\theta/2)} + 5.\end{aligned}$$

Séparons cette équation en deux. La dérivée de

$$\left(4\cos(\theta/4) + 2\cos(3\theta/4)\right)\sqrt{4\cos(\theta/2) + \cos(3\theta/2)}$$

est

$$\frac{-4\sin(\theta/4) - 8\sin(3\theta/4) - 10\sin(5\theta/4) - 4\sin(7\theta/4) - 3\sin(9\theta/4)}{2\sqrt{4\cos(\theta/2) + \cos(3\theta/2)}},$$

qui est négative sur $(0, \pi)$. Similairement, la dérivée de

$$8\cos(\theta/2) + 4\cos(\theta) + 2\cos(3\theta/2)$$

est

$$-4\sin(\theta/2) - 4\sin(\theta) - 3\sin(3\theta/2),$$

qui est aussi négative sur $(0, \pi)$. Alors, $|Z_-|^2$ est décroissante sur $(0, \pi)$. Puisque $|Z_-|$ est une fonction paire de période 2π, $|Z_-|$ atteint un minimum en $\theta = \pi$. Nous voyons dans ce cas que $|Z_-| = 1$ et donc $|Z_-| \geq 1$ lorsque $|X| = 1$.

Ceci conclut la preuve. □

Proposition 74. $|x| = 1$, $|y_-| \geq 1$ est un chemin fermé.

Démonstration. (Voir [24], preuve du Lemme 11)
Faisons le changement de variables $x = x_1^2$ et $y_1 = y/x_1$. Nous voulons donc prouver que $|x_1| = 1$, $|y_{1-}| \geq 1$ est un chemin fermé, où

$$\begin{aligned} y_{1-} &= \frac{-(x_1^2 + 4 + x_1^{-2}) - \sqrt{x_1^4 + 4x_1^2 + 10 + 4x_1^{-2} + x_1^{-4}}}{2(x_1 + x_1^{-1})} \\ &= \frac{-(2 + (x_1 + x_1^{-1})^2) - \sqrt{4 + (x_1 + x_1^{-1})^4}}{2(x_1 + x_1^{-1})}. \end{aligned}$$

Lorsque $x_1 = e^{i\theta}$, nous obtenons

$$y_{1-} = \frac{-(1 + 2\cos^2\theta) - \sqrt{1 + 4\cos^4\theta}}{2\cos\theta}.$$

Puisque y_{1-} est réel et que $1 + 4\cos^4\theta \leq (1 + 2\cos^2\theta)^2$, nous avons

$$|y_{1-}| = \frac{1 + 2\cos^2\theta + \sqrt{1 + 4\cos^4\theta}}{2|\cos\theta|} \geq \frac{\sqrt{1 + 4\cos^4\theta}}{|\cos\theta|} = \sqrt{\frac{1}{\cos^2\theta} + 4\cos^2\theta} > 1.$$

Ceci conclut la proposition. □

En résumé, $\gamma_1 = \{(X, Z_-) \ : \ |X| = 1\}$ est le cycle d'intégration pour la mesure de Mahler de $P_{4,2}$ et $\gamma_2 = \{(x, y_-) \ : \ |x| = 1\}$ est celui pour R_{-2}. En utilisant la multiplicativité de η et le fait que $Y_\pm = Z_\pm X$, nous obtenons

Proposition 75. Soit Y_- la racine de $P_{4,2} = 0$ correspondant à $Y_- = Z_- X$ et y_- la racine de R_{-2} satisfaisant $|y_-| \geq 1$ lorsque $|x| = 1$. Alors

$$\begin{aligned} m(T) = m(P_{4,2}) &= -\frac{1}{2\pi}\int_{|X|=1} \eta(X, Y_-), \\ m(R_{-2}) &= -\frac{1}{2\pi}\int_{|x|=1} \eta(x, y_-). \end{aligned}$$

3.4 La classe d'homologie

Le but de cette section est de calculer les classes d'homologie de E_1 et E_2 et de montrer qu'elles se trouvent dans $H_1(E_1, \mathbb{Z})^-$.

Cette section comportera une ambiguïté de signe en travaillant avec les racines carrées, mais comme la mesure de Mahler est toujours positive, cela ne représente pas un problème.

Soit ω la différentielle holomorphique invariante sur $\widehat{P_{4,2}} = 0$. Pour caractériser $[\gamma]$ correspondant au chemin fermé de la dernière section, nous calculons $\int_\gamma \omega$.

Tout d'abord, rappelons-nous la définition de

$$K(k) := \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2\sin\theta^2}} = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}},$$

l'intégrale elliptique complète de première espèce.

Proposition 76. On a

$$\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \omega = \pm \frac{2i\sqrt{2(-1+\sqrt{5})}K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right)}{\sqrt[3]{4}},$$

où l'intégrale est faite sur le chemin $|\hat{X}| = \frac{1}{\sqrt[3]{4}}$, $|\hat{Y}_-| \geq \frac{1}{2}$.

Démonstration. Nous avons vu que

$$\hat{Y}_- = \frac{-2\sqrt[3]{4}\hat{X} - 1 - \sqrt{(2\sqrt[3]{4}\hat{X}+1)^2 + 4\hat{X}^3}}{2}. \tag{3.5}$$

Donc nous avons

$$\begin{aligned}
\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \omega &= \int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \frac{d\hat{X}}{2\hat{Y}_- + 2\sqrt[3]{4}\hat{X} + 1} \\
&= \int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \frac{-d\hat{X}}{\sqrt{4\sqrt[3]{16}\hat{X}^2 + 4\sqrt[3]{4}\hat{X} + 1 + 4\hat{X}^3}} \\
&= \pm\frac{1}{\sqrt[3]{4}} \int_{-\pi}^{\pi} \frac{id\theta}{\sqrt{4 + 4e^{-i\theta} + e^{-2i\theta} + e^{i\theta}}} \\
&= \pm\frac{1}{\sqrt[3]{4}} \left(\int_{-\pi}^{0} \frac{id\theta}{\sqrt{4 + 4e^{-i\theta} + e^{-2i\theta} + e^{i\theta}}} + \int_0^{\pi} \frac{id\theta}{\sqrt{4 + 4e^{-i\theta} + e^{-2i\theta} + e^{i\theta}}} \right) \\
&= \pm\frac{1}{\sqrt[3]{4}} \left(\int_0^{\pi} \frac{id\theta}{\sqrt{4 + 4e^{i\theta} + e^{2i\theta} + e^{-i\theta}}} + \int_0^{\pi} \frac{id\theta}{\sqrt{4 + 4e^{-i\theta} + e^{-2i\theta} + e^{i\theta}}} \right) \\
&= \pm\frac{2i}{\sqrt[3]{4}} \mathrm{Re}\left(\int_0^{\pi} \frac{d\theta}{\sqrt{4 + 4e^{-i\theta} + e^{-2i\theta} + e^{i\theta}}} \right).
\end{aligned}$$

En faisant le changement de variables $t = 1 + e^{i\theta}$, nous obtenons

$$\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \omega = \pm\frac{2i}{\sqrt[3]{4}}\mathrm{Re}\left(\int_0^2 \frac{-idt}{(t-1)\sqrt{(t-1)^{-2}t(t^2+t-1)}}\right)$$
$$= \pm\frac{2i}{\sqrt[3]{4}}\mathrm{Re}\left(\int_0^2 \frac{-idt}{\sqrt{t(t^2+t-1)}}\right),$$

où le chemin d'intégration est sur le demi-cercle supérieur de rayon 1 centré en 1. Nous fermons ce chemin avec le segment réel $[0,2]$. L'intégrande ne possède pas de pôles dans l'intérieur de la région mais possède des points de branchement en 0 et $\frac{\sqrt{5}-1}{2}$. Nous prenons le cercle de rayon ϵ autour de 0 et obtenons une intégrale de la forme

$$\int_a^b \frac{i\epsilon e^{i\theta}}{\sqrt{\epsilon e^{i\theta}((\epsilon e^{i\theta})^2+\epsilon e^{i\theta}-1)}},$$

qui tend vers 0 lorsque $\epsilon \to 0$. La même situation se produit en $t = \frac{\sqrt{5}-1}{2}$ et nous concluons que l'intégrale sur la frontière est 0. Alors, la dernière intégrale sur le demi-cercle supérieur est égale à celle correspondant au segment réel $[0,2]$.

Notons que $t(t^2+t-1)$ est négative sur $(0, \frac{\sqrt{5}-1}{2})$ et positive sur $(\frac{\sqrt{5}-1}{2}, 2)$. Nous obtenons donc

$$\mathrm{Re}\left(\int_0^2 \frac{-idt}{\sqrt{t(t^2+t-1)}}\right) = \int_0^{\frac{\sqrt{5}-1}{2}} \frac{-idt}{\sqrt{t(t^2+t-1)}}.$$

En utilisant le changement de variables

$$z = \frac{i(t^2+1)}{\sqrt{4t(t^2+t-1)}}, \quad dz = \frac{i(t^4+2t^3-6t^2-2t+1)}{4(t(t^2+t-1))^{3/2}}dt.$$

Nous voyons que le chemin $f(t) = \left|\frac{(t^2+1)}{\sqrt{4t(t^2+t-1)}}\right|$ lorsque $t \in (0, \frac{\sqrt{5}-1}{2})$ atteint son minimum en $t_0 = \frac{-1-\sqrt{5}+\sqrt{2(5+\sqrt{5})}}{2}$, $f(t_0) = \sqrt{\frac{1+\sqrt{5}}{2}}$, et tend vers ∞ lorsque $t \to 0^+$, $t \to \frac{\sqrt{5}-1}{2}^-$. Par conséquent

$$\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \omega = \pm\frac{2i}{\sqrt[3]{4}}\left(2\int_{\sqrt{\frac{1+\sqrt{5}}{2}}}^{\infty} \frac{dz}{\sqrt{z^4-z^2-1}}\right).$$

En posant $x = \frac{\sqrt{\frac{1+\sqrt{5}}{2}}}{z}$, nous obtenons

$$\begin{aligned}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} \omega &= \pm\frac{4i}{\sqrt[3]{4}}\sqrt{\frac{1}{2}(1+\sqrt{5})}\left(\int_0^1 \frac{dx}{\sqrt{(1-x^2)(x^2+\frac{3+\sqrt{5}}{2})}}\right)\\ &= \pm\frac{4i}{\sqrt[3]{4}}\sqrt{\frac{1}{2}(1+\sqrt{5})}\left(\frac{2}{1+\sqrt{5}}\right)K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right)\\ &= \pm\frac{2i}{\sqrt[3]{4}}\sqrt{2(-1+\sqrt{5})}\;K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right).\end{aligned}$$

Ceci conclut la preuve. □

Proposition 77. Nous avons

$$\int_{\varphi_*(|x|=1)} \omega = \pm\frac{2i\sqrt{2(-1+\sqrt{5})}K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right)}{\sqrt[3]{4}},$$

est l'intégrale est faite sur le chemin $|x| = 1$, $|y_-| \geq 1$.

Démonstration. Puisque nous avons

$$\int_{\varphi_*(|x|=1)} \omega = \int_{|x|=1} \varphi^*\omega,$$

nous calculons $\varphi^*\omega$. Nous trouvons tout d'abord $\varphi^*\omega$ en termes de X, Y (les coordonnées du polynôme non-tempéré). En utilisant (3.1) nous obtenons

$$dX = -\frac{2}{(2+x+y)^2}dx - \frac{2}{(2+x+y)^2}dy.$$

En dérivant $R_{-2}(x, y)$, nous obtenons

$$(2x(y+1)+y^2+4y+1)dx+(2y(x+1)+x^2+4x+1)dy = 0 \Longrightarrow dy = -\frac{(2x(y+1)+y^2+4y+1)dx}{2y(x+1)+x^2+4x+1}.$$

En remplaçant, nous trouvons

$$\begin{aligned}dX &= \left(1-\frac{2x(y+1)+y^2+4y+1}{2y(x+1)+x^2+4x+1}\right)\frac{-2}{(2+x+y)^2}dx\\ &= \frac{2(y-x)}{(2+x+y)(2y(x+1)+x^2+4x+1)}.\end{aligned}$$

Nous avons aussi

$$2Y + 4X + 2 = \frac{2(x-y)}{2+x+y}.$$

Par conséquent

$$\frac{dX}{2Y+4X+2} = -\frac{dx}{(2y(x+1)+x^2+4x+1)}, \quad y_\pm = \frac{-1-4x-x^2 \pm \sqrt{1+4x+10x^2+4x^3+x^4}}{2(1+x)}.$$

Par la section précédente, nous prenons y comme étant la racine négative.

Maintenant, en utilisant $X = \sqrt[3]{4}\hat{X}, Y = 2\hat{Y}$, nous trouvons

$$\begin{aligned}
\int_{|x|=1} \varphi^*\omega &= -\int_{|x|=1} \frac{2dx}{\sqrt[3]{4}(2y(x+1)+x^2+4x+1)} \\
&= \pm\frac{2}{\sqrt[3]{4}} \int_{-\pi}^{\pi} \frac{id\theta}{\sqrt{2}\sqrt{5+4\cos(\theta)+\cos(2\theta)}} \\
&= \pm\frac{i}{\sqrt[3]{4}} \int_{-\pi}^{\pi} \frac{d\theta}{\sqrt{2+2\cos(\theta)+\cos^2(\theta)}} \\
&= \pm\frac{i}{\sqrt[3]{4}} \int_{-\pi}^{\pi} \frac{d\theta}{\sqrt{1+(\cos(\theta)+1)^2}} \\
&= \pm\frac{2i}{\sqrt[3]{4}} \int_{0}^{\pi} \frac{d\theta}{\sqrt{1+(\cos(\theta)+1)^2}}.
\end{aligned}$$

Posons $t = \cos\theta$, $\frac{-dt}{\sqrt{1-t^2}} = d\theta$. Alors

$$\int_{|x|=1} \varphi^*\omega = \pm\frac{2i}{\sqrt[3]{4}} \int_{-1}^{1} \frac{dt}{\sqrt{(1-t^2)(1+(t+1)^2)}}.$$

Avec le changement de variables

$$x = \frac{t+\frac{3-\sqrt{5}}{2}}{t+\frac{3+\sqrt{5}}{2}}, \quad dx = \frac{\sqrt{5}}{\left(t+\frac{3+\sqrt{5}}{2}\right)^2}dt,$$

nous obtenons

$$\int_{|x|=1} \varphi^*\omega = \pm\frac{2i}{\sqrt[3]{4}} \int_{\frac{3-\sqrt{5}}{2}}^{\frac{-3+\sqrt{5}}{2}} \frac{dx}{\sqrt{-2+\sqrt{5}-x^2-(2+\sqrt{5})x^4}}.$$

Finalement, si nous posons $x = \sqrt{\frac{1}{2}(7-3\sqrt{5})}u$,

$$\begin{aligned}\int_{|x|=1}\varphi^*\omega &= \pm\frac{2i}{\sqrt[3]{4}}\sqrt{\frac{1}{2}(-1+\sqrt{5})}\int_{-1}^{1}\frac{du}{\sqrt{(1-u^2)(1-(\frac{1}{2}(-3+\sqrt{5}))u^2)}}\\ &= \pm\frac{4i}{\sqrt[3]{4}}\sqrt{\frac{1}{2}(-1+\sqrt{5})}\int_{0}^{1}\frac{du}{\sqrt{(1-u^2)(1-(\frac{1}{2}(-3+\sqrt{5}))u^2)}}\\ &= \pm\frac{2i}{\sqrt[3]{4}}\sqrt{2(-1+\sqrt{5})}K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right).\end{aligned}$$

Ceci conclut la proposition.

□

Cette section implique que les chemins d'intégration donnent la même classe d'homologie. Nous observons aussi que $\pm\frac{2i}{\sqrt[3]{4}}\sqrt{2(-1+\sqrt{5})}K\left(\sqrt{\frac{1}{2}(-3+\sqrt{5})}\right)$ est purement imaginaire et donc la classe d'homologie se trouve dans $H_1(E_1,\mathbb{Z})^-$.

3.5 L'intégrale sur arg $\hat{Y}_-$

Cette section a pour but de calculer l'intégrale sur $d\arg\hat{Y}_-$ comme vu à la section 3.2.

Proposition 78. Soit $\hat{Y}_-$ la racine de $\widehat{P_{4,2}}$ donnée par (3.5.). Alors

$$\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} d\arg\hat{Y}_- = 1.$$

Démonstration.

$$\begin{aligned}\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} d\text{arg}\hat{Y}_- &= \frac{1}{2\pi i}\int_{|X|=1}\frac{d\left(-2X-1-\sqrt{4X^2+4X+1+X^3}\right)}{-2X-1-\sqrt{4X^2+4X+1+X^3}}\\ &= \frac{1}{2\pi i}\int_{\gamma}\frac{du}{u},\end{aligned}$$

où γ est le chemin $-2X-1-\sqrt{4X^2+4X+1+X^3}$ lorsque $|X|=1$. Les seules discontinuités de γ sont lorsque $\text{Im}(r(x))=0$ au moment où $\text{Im}(r(x))$ change d'une valeur positive en une valeur négative, où $r(x)=4X^2+4X+1+X^3$ (nous prenons la branche principale de la racine carrée). Donc γ possède des discontinuités en $e^{\pm\frac{2}{3}i\pi}$.

En ces valeurs, le chemin saute de $\pm i\sqrt{5-2\sqrt{6}}$ à $\pm i(\sqrt{2}+\sqrt{3})$.

Nous complétons γ avec les intervalles imaginaires

$$\left[i\sqrt{5-2\sqrt{6}}, i(\sqrt{2}+\sqrt{3})\right] \quad \text{and} \quad \left[-i(\sqrt{2}+\sqrt{3}), -i\sqrt{5-2\sqrt{6}}\right],$$

et appellons ce chemin $\hat{\gamma}$. Ce chemin est fermé et l'intégrale sur γ est la même que sur $\hat{\gamma}$ puisque nous avons ajouté deux chemins conjugués. Par conséquent

$$\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}} d\arg\hat{Y}_- = \frac{1}{2\pi i}\int_{\hat{\gamma}} \frac{du}{u},$$

ce qui représente l'indice de $\hat{\gamma}$ autour de 0. Comme $\hat{\gamma}$ traverse l'axe réel négatif qu'une seule fois (en $X=1$) et commence sur l'axe réel positif, nous voyons que l'indice de $\hat{\gamma}$ est 1 (voir Figure 3.1). □

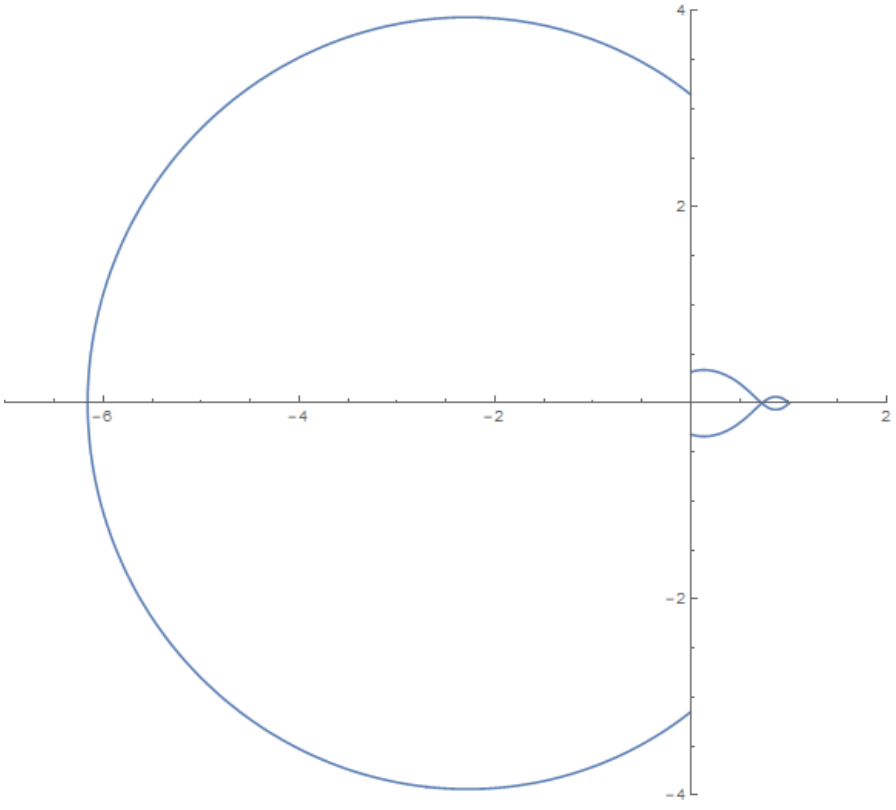


FIGURE 3.1: Le chemin γ

3.6 Fin de la « preuve »

Nous donnons ici la fin de la preuve en supposant que que la théorie s'applique même si le changement de variable entre $P_{4,2}$ et $\widehat{P_{4,2}}$ n'est pas rationnel.

Puisque $\widehat{P_{4,2}}$ et R_{-2} sont tempérés (voir [4]), nous pourrions conclure que les intégrales

$$-\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}}}\eta(\hat{X},\hat{Y}_-) \quad \text{et} \quad -\frac{1}{2\pi}\int_{|x|=1}\eta(x,y_-)$$

dépendent seulement de la classe d'homologie de $\hat{\gamma_1}$ et $\varphi_*(\gamma_2)$ dans $H_1(E,\mathbb{Z})$, où

$$\hat{\gamma_1}=\left\{(\hat{X},\hat{Y}_-)\ :\ |\hat{X}|=\frac{1}{\sqrt[3]{4}}\right\} \quad \text{et} \quad \gamma_2=\{(x,y_-)\ :\ |x|=1\}.$$

Par les Propositions 72, 76 et 77, ceci impliquerait que

$$-\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}\eta(\hat{X},\hat{Y}_-)=-\frac{8}{9}\frac{1}{2\pi}\int_{\varphi_*(|x|=1)}\eta(x\circ\phi^{-1},y_-\circ\phi^{-1}).$$

Les résultats de Rogers et Zudilin [18] donnent

$$-\frac{1}{2\pi}\int_{\varphi_*(|x|=1)}\eta(x\circ\phi^{-1},y_-\circ\phi^{-1})=3L'(E_{20},0),$$

et la Proposition 78 donne

$$-\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}d\arg\hat{Y}_-=-1.$$

Donc par la proposition 75 et la discussion de la Section 3.2, nous obtenons

$$\begin{aligned}
m(P_{4,2}) &= -\frac{1}{2\pi}\int_{|X|=1,|Y_-|\geq 1}\eta(X,Y_-)\\
&= -\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}\eta(\sqrt[3]{4}\hat{X},2\hat{Y}_-)\\
&= -\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}\eta(\hat{X},\hat{Y}_-)-\frac{\log(\sqrt[3]{4})}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}d\arg\hat{Y}_-+\log 2\\
&= \frac{8}{3}L'(E_{20},0)-\log(\sqrt[3]{4})+\log 2\\
&= \frac{8}{3}L'(E_{20},0)+\frac{1}{3}\log 2,
\end{aligned}$$

ce qui terminerait la preuve.

Ici, le problème fondamental vient du fait que puisque $\widehat{P_{4,2}}$ n'est pas rationnel, l'intégrale sur η ne dépend pas seulement du cycle d'homologie, et donc nous n'avons pas l'égalité

$$-\frac{1}{2\pi}\int_{|\hat{X}|=\frac{1}{\sqrt[3]{4}},|\hat{Y}_-|\geq\frac{1}{2}}\eta(\hat{X},\hat{Y}_-)=-\frac{8}{9}\frac{1}{2\pi}\int_{\varphi_*(|x|=1)}\eta(x\circ\phi^{-1},y_-\circ\phi^{-1}).$$

Conclusion

Malgré le manque d'une relation entre $m(y^2+4xy+2y-x^3)$ et la fonction-L associée à la courbe elliptique $y^2+4xy+2y-x^3=0$, il reste toujours un espoir de trouver une autre formule que celle conjecturée par D. Boyd et d'appliquer les résultats du chapitre 3 à cette fin. Une autre avenue intéressante serait d'utiliser les conclusions du dernier chapitre afin d'étudier la mesure de Mahler de $y^2+4xy+2y-x^3$ sur un tore arbitraire (voir [24]) et voir si certains liens apparents en ressortent.

De manière plus générale, il serait extrêmement utile de concevoir des techniques permettant d'étudier et prouver la mesure de Mahler de certaines familles de polynômes puisque la plupart des preuves se basent sur une étude cas par cas. La famille $P_{k,2}$ (voir section 2.3) aurait avantage à être étudiée plus en profondeur puisqu'il s'agit de polynômes non-tempérés et la plupart des relations prouvées viennent de polynômes tempérés. On pourrait aussi naturellement s'intéresser à d'autres familles de polynômes considérés par Boyd, la plus similaire étant

$$F_{k,b} = y^2 + kxy - x^3 - bx$$

pour lesquels les relations conjecturées sont

$$m(F_{k,b}) = \frac{1}{4}\log|b| + rL'(E,0).$$

Le chapitre 3 avait comme idée de relier $P_{4,2}$ avec un polynôme tempéré puis de travailler avec ce dernier. Une autre approche plus « directe » aurait certainement de nombreux avantages puisque nous n'avons toujours pas une théorie assez développée pour étudier les polynômes non-tempérés.

Les conjectures de Bloch-Beĭlinson semblent encore aujourd'hui loin de la portée des mathématicien.nes. Toute percée dans cette direction serait monumentale à la compréhension de ce lien profond et surprenant existant entre les valeurs spéciales de fonctions-L et d'autres concepts *a priori* éloignés.

Bibliographie

[1] D. Boyd. Mahler's measure and special values of L-functions. *Experiment. Math.*, 7 :37–82, 1998.

[2] J. H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition.* Graduate Texts in Mathematics. Springer, 2009.

[3] T. Ward G. Everest. *Heights of Polynomials and Entropy in Algebraic Dynamics.* Springer, 1999.

[4] F. Rodriguez-Villegas. Modular Mahler measures I. *Topics in number theory*, 467 : 17–48, 1997.

[5] A. Beutelspacher. *Projective geometry : from foundations to applications.* Cambridge University Press, 1998.

[6] J. S. Milne. *Abelian Varieties.* 2008. URL https://www.jmilne.org/math/CourseNotes/AV.pdf.

[7] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer, 1999.

[8] D. H. Lehmer. Factorization of certain cyclotomic functions. *Annals of Mathematics*, 34(3) :461–479, 1933.

[9] K. Mahler. An application of jensen's formula to polynomials. *Matematika*, 7 : 98–100, 1960.

[10] K. Mahler. On some inequalities for polynomials in several variables. *Journal of the London Math. Soc*, 37 :341–344, 1962.

[11] S. Lang. *Algebraic Number Theory, Second Edition.* Graduate Texts in Mathematics. Springer, 1994.

[12] A. O. Gel'fond. *Transcendental algebraic numbers.* Dover, 1960.

[13] D. Boyd. Sharp inequalities for the product of polynomials. *Bull. London Math. Soc.*, 26 :449–454, 1994.

[14] C. Deninger. Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^n$-actions. *J. Amer. Math. Soc.*, 10 :259–281, 1997.

[15] M. Raynaud S. Bosch, W. Lütkebohmert. *Néron Models*. Springer, 1990.

[16] S. J. Bloch. Higher regulators, algebraic K-theory, and zeta functions of eliptic curves. *CRM Monograph series*, 11, 2000.

[17] A. A. Beĭlinson. Higher regulators of modular curves. *Applications of algebraic K-theory to algebraic geometry and number theory*, Part I, II :1–34, 1986.

[18] M. Rogers and W. Zudilin. From L-series of elliptic curves to Mahler measures. *Compos. Math*, 148 :385–414, 2012.

[19] M.-J. Bertin. Mesure de Mahler et régulator elliptique : preuve de deux relations "exotiques". *Number theory*, CRM Proc. Lecture Notes(36) :1–12, 2004.

[20] M.-J. Bertin and W. Zudilin. On the Mahler measure of hyperelliptic families. *Ann. Math. Québec*, 41(1) :199–211, 2017.

[21] F. Brunault. *Étude de la valeur en $s = 2$ de la fonction L d'une courbe elliptique*. PhD thesis, Université Paris 7 Denis Diderot, 2005.

[22] M. Lalín. On a conjecture by Boyd. *Int. J. Number theory*, 6 :705–711, 2010.

[23] M. Lalín and F. Ramanmonjisoa. The Mahler measure of a Weierstrass form. *Int. J. Number theory*, 13(8) :2195–2214, 2017.

[24] M. Lalín and T. Mittal. The Mahler measure for arbitrary tori. *Res. Number theory*, 4(2) :4 :16, 2018.

[25] M. Lalín, D. Samart, and W. Zudilin. Futher explorations of Boyd's conjectures and a conductor 21 elliptic curve. *J. Lond. Math. Soc.*, 93 :341–360, 2016.

[26] A. Mellit. Elliptic dilogarithm and parallel lines. *ArXiv e-prints*, 2012.

[27] F. Rodriguez-Villegas. Identities between Mahler measures. *Number theory for the millennium*, III :223–229, 2002.