N° d'ordre :13/ 2014- M / MT
REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE-ALGER
Faculté de Mathématiques

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En: MATHÉMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par: **Mihoub BOUDERBALA**

Sujet

Valeurs explicites de mesures de Mahler

Soutenu publiquement, le 17/05/2014, devant le jury composé de:

M/ F. BENCHERIF, Professeur à l'USTHB	Président
Mme/L. CHERCHEM BENFERHAT, Maître de Conférences /A à L'USTHB	Directrice de Mémoire
M/ B. BENSEBA, Maître de Conférences /A à L'USTHB	Examinateur 1
Mme/ C. SELMANE, Maître de Conférences /A à L'USTHB	Examinateur 2

Table des matières

Abstract

Ce mémoire est basé sur l'étude d'un article de Lehmer (1933) intitulé : "Factorization of certain cyclotomic functions", où il posa sa fameuse question, connue sous le nom de "Problème de Lehmer".

Plusieurs recherches ont été effectuées pour résoudre ce problème mais il reste encore ouvert aujourd'hui.

La mesure de Mahler de polynômes de plusieurs variables à coefficients complexes apparaît dans plusieurs domaines mathématiques dont la théorie ergodique, la théorie des noeuds et la théorie des nombres. Elle est connue, en particulier, pour son rôle dans le problème de Lehmer.

Nous donnons donc les démonstrations détaillées de plusieurs résultats liés à cette mesure avec une étude des caractères de groupes abéliens finis, des caractères et des séries de Dirichlet.

Remerciements

J'exprime toute ma gratitude à ALLAH (Dieu) qui m'a donné l'effort, le courage et la patience pour accomplir ce travail, et qui grâce à lui ce travail a été achevé.

J'exprime tous mes remerciements les plus distingués à mon Professeur, Madame Leila BENFERHAT, Maître de Conférence (A) à l'USTHB , qui m'a encadré durant toute la période de mon mémoire avec beaucoup de patience, de générosité et de compétence. je tiens en particulier à la remercier pour ses précieux conseils, en ce qui concerne la rédaction.

Je tiens à exprimer mes meilleurs remerciements à mon Professeur Monsieur Farid BENCHERIF, Professeur à l'USTHB, qui me fait l'honneur de présider le jury de ce mémoire.

Je remercie vivement mon professeur Boualem BENSEBA , Maître de Conférence (A) à l'USTHB, d'avoir accepté d'examiner ce travail.

Mes sincères remerciements vont à Madame Schehrazad SELMANE , Maître de Conférence (A) à l'USTHB pour avoir accepté de faire partie du jury et avoir examiné ce travail.

Mes derniers remerciements vont à mes amis, à toute ma famille, pour leur soutien et leur encouragement durant durant toute la période de mon mémoire , et tout particulièrement mon épouse qui a toujours été présente à mes côtés.

INTRODUCTION

La mesure de Mahler est apparue pour la première fois en 1933 dans un article de Lehmer [10]. Elle doit son nom à Kurt Mahler qui l'introduisit sous une forme équivalente en 1961 dans ses travaux sur la transcendance [24]. Pour les polynômes $P \in \mathbb{C}[x_1, x_2, ..., x_n] \setminus \{0\}$, il a défini la fonction

$$m(P) := \int_0^1 \cdots \int_0^1 \log \left| P(e^{2i\pi\theta_1}, \cdots, e^{2i\pi\theta_n}) \right| d\theta_1 \cdots d\theta_n,$$

dite mesure logarithmique de Mahler de P.

La mesure de Mahler de P est définie par

$$M(P) := \exp(m(P)).$$

Si $P \in \mathbb{Z}[x]$ tel que

$$P(x) = a_d \prod_{i=1}^{d} (x - \alpha_i), \ \alpha_i \in \mathbb{C},$$

grâce à la formule de Jensen, la mesure de Mahler de P est le nombre réel

$$M(P) = |a_d| \prod_{i=1}^{d} \max(|\alpha_i|, 1).$$

Pour les polynômes en une seule variable, cette fonction représente la moyenne géométrique de $|P(z)|$ sur le cercle unité. Elle apparaît dans plusieurs domaines des mathématiques dont la théorie ergodique, la théorie des noeuds et la théorie des nombres. Elle est connue, en particulier, pour son rôle dans le problème de Lehmer suivant :

Soit $\varepsilon > 0$. Existe-t-il un polynôme de la forme

$$P(x) = x^r + a_1 x^{r-1} + \cdots + a_r,$$

tel que la valeur absolue du produit des racines de P extérieures au disque unité soit compris entre 1 et $1 + \varepsilon$?

Ce problème a sucité de nombreuses recherches et il reste encore ouvert à ce jour pour les polynômes réciproques.

Une réponse partielle a été donnée par Smyth [17], en 1971 : si P est non réciproque alors $M(P) > 1.32471795\cdots$, où $\theta_0 = 1.32471795\cdots$. Le nombre θ_0 est le plus petit nombre de Pisot, racine supérieure à 1 de $x^3 - x - 1$.

Dans [4], Boyd montre que la question de Lehmer nécessite l'investigation de mesures de Mahler de polynômes de plusieurs variables grâce au résultat suivant

si P est un polynôme non nul, $P \in \mathbb{C}[x_1, x_2]$

$$M(P(x_1, x_2)) = \lim_{n \to +\infty} M(P(x, x^n)).$$

Ce résultat a été généralisé par Lawton [28], en 1983, à un nombre quelconque de variables :

$P \in \mathbb{C}[x_1, ..., x_n]$

$$\lim_{r_2 \to \infty} \cdots \lim_{r_n \to \infty} m(P(x, x^{r_2} \cdots, x^{r_n})) = m(P(x_1, ..., x_n)).$$

Les deux mesures suivantes, de Smyth (1981), furent le début des mesures de Mahler explicites.

$$m(x + y + 1) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-s}, 2), \tag{1}$$

où

$$L(\chi_{-s}, s) = \sum_{n \geq 1} \frac{\chi_{-s}(n)}{n^2}, \tag{2}$$

désigne la série de Dirichlet de caractère le symbole de Legendre $\chi_{-s}(n) = \left(\frac{-s}{n}\right)$.

et

$$m(1 + x + y + z) = \frac{7}{2\pi^2} \zeta(3),$$

où ζ désigne la fonction zêta de Riemann.

En 2008, N. Kurokawa, M. Lalin et H. Ochiai introduisirent, dans leur article [25], la mesure de Mahler supérieure qui est un cas particulier de la mesure de Mahler supérieure multiple.

Soit $P_1, P_2, ..., P_l \in \mathbb{C}[x_1, x_2, \ldots x_n] \setminus \{0\}$.

La mesure de Mahler supérieure multiple de $P_1, P_2, ..., P_l$ est définie par

$$m(P_1, ..., P_l) := \int_0^1 \cdots \int_0^1 \left(\log \left|P_1(e^{2\pi i\theta_1}, ..., e^{2\pi i\theta_r}\right|\right) \ldots \left(\log \left|P_l(e^{2\pi i\theta_1}, ..., e^{2\pi i\theta_r}\right|\right) d\theta_1 ....d\theta_r.$$

Si les P_i, $1 \leq i \leq l$, sont tous égaux à P, alors la mesure $k-$ supérieure de Mahler de P est définie par

$$m_k(P) := \int_0^1 \cdots \int_0^1 \log \left|P^k\left(e^{2\pi i\theta_1}, ..., e^{2\pi i\theta_r}\right)\right| d\theta_1 ....d\theta_r.$$

Comme la question de Lehmer est intéressante pour la mesure de Mahler classique, on pourrait se poser la même question pour la mesure de Mahler $k-$ supérieure en considérant la limite de l'ensemble

$$L = \{m_k(P) : P \text{ est à coefficients entiers}\}$$

En 2011, M. Lalin et K. Sinha [26] montrèrent que :
si $P(x) \in \mathbb{Z}[x]$ n'est pas un monôme, alors pour tout $h \geq 1$

$$m_{2h}(P) \geq \begin{cases} \left(\frac{\pi^2}{12}\right)^h & \text{si } P(x) \text{ est réciproque} \\ \left(\frac{\pi^2}{48}\right)^h & \text{si } P(x) \text{ n'est pas réciproque.} \end{cases}$$

Ce théorème révèle que pour m_{2h}, on a une réponse négative à la question de Lehmer.

Ils montrèrent également que :
si $P_n(x) = \dfrac{x^n - 1}{x - 1}$, pour $h \geq 1$, fixé, alors

$$\lim_{n \to \infty} m_{2h+1}(P_n) = 0.$$

Dans ce cas, on a une réponse positive à la question de Lehmer pour m_{2h+1}.

Ce mémoire est constitué de trois chapitres.

Dans le premier chapitre, nous expliquons le problème de Lehmer ainsi que sa méthode pour exhiber de très grands nombres. Nous rappelons quelques notions fondamentales telles que la mesure de Mahler d'un polynôme d'une seule et de plusieurs variables ainsi qu'un résulat de Boyd, généralisé par Lawton, qui fait le lien entre la mesure de Mahler d'un polynôme d'une seule variable et celle d'un polynôme de plusieurs variables. Nous rappelons également les notions de mesure de Mahler supérieure, mesure de mahler supérieure multiple, mesure zêta de Mahler.

Les caractères de Dirichlet et leurs séries L furent introduits par Dirichlet, en 1831, dans le but de prouver le théorème de Dirichlet à propos de l'infinité des nombres premiers dans les progressions arithmétiques. L'extension aux fonctions holomorphes fut accomplie par Bernhard Riemann.

Dans le second chapitre, nous étudions de façon détaillée les caractères de groupes abéliens finis et les caractères de Dirichlet modulo k. Nous donnons des exemples de calcul et, en particulier, un calcul explicite pour les valeurs de $k = 2, \cdots, 15$. Nous rappelons la notion de conducteur d'un caractère et la méthode qui nous permet de le déterminer effectivement avec quelques exemples. Nous étudions également les propriétés des séries L de Dirichlet.

Dans le troisième chapitre, nous donnons les outils et techniques de calcul qui permettent de donner des valeurs explicites de mesures de Mahler de polynômes de plusieurs variables, de mesures de Mahler supérieures et supérieures multiples. Nous exposons donc, les démonstrations détaillées de plusieurs résultats, notamment, ceux de Smyth, Sana Boughzala, Kurokawa, Lalin, Ochiai et Sinha.

Chapitre 1

Mesure de Mahler de polynômes de plusieurs variables

1.1 Introduction

Dans ce chapitre, nous expliquons le problème de Lehmer ainsi que sa méthode pour exhiber de très grands nombres. Nous rappelons quelques notions fondamentales telles que la mesure de Mahler d'un polynôme d'une seule et de plusieurs variables ainsi qu'un résulat de Boyd, généralisé par Lawton, qui fait le lien entre la mesure de Mahler d'un polynôme d'une seule variable et celle d'un polynôme de plusieurs variables. Nous rappelons également la notion de mesure de Mahler supérieure, mesure de mahler supérieure multiple, mesure zêta de Mahler.

Pour plus de détails se référer à [6], [8], [10] et [13].

1.2 Problème de Lehmer

Définition 1 *Un corps C est dit algébriquement clos si tout polynôme de degré plus grand ou égal à 1 dans $C[x]$ possède au moins une racine dans C.*

Soit K un corps contenu dans un corps algébriquement clos C. Soient f et g deux polynômes de $K[x]$, de degrés m et n respectivement. On pose

$$\begin{aligned} f(x) &= a\prod_{1\leq i\leq m}(x-\alpha_i) \text{ et} \\ g(x) &= b\prod_{1\leq j\leq n}(x-\beta_j) \end{aligned}$$

dans $C[x]$.

Définition 2 *Le résultant des deux polynômes non nuls f et g, noté* Res (f,g), *est défini par*

$$Res\ (f,g) = a^n b^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} \left(\alpha_i - \beta_j\right).$$

Si $f=0$ ou $g=0$, on pose Res $(f,g)=0$.

Dans le but d'exhiber de grands nombres premiers, en 1933, Lehmer s'intéresse à la quantité

$$\Delta_n = \Delta_n(f) := \prod_{i=1}^{d} (\alpha_i^n - 1) = \mathrm{Res}\ (f, x^n-1) \in \mathbb{Z},$$

où, $f \in \mathbb{Z}[x]$ et

$$f = x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0 = \prod_{i=1}^{d}(x-\alpha_i),$$

ayant pour racines $\alpha_1, \alpha_2, ..., \alpha_d$ dans $\mathbb{C}$.

On peut remarquer que si m divise n, alors Δ_m divise Δ_n. Ainsi, Lehmer parvient à montrer que la factorisation de Δ_n nécessite, dans un premier temps, de tester la divisibilité de Δ_n par les premier p qui sont d'ordre w modulo n et qui vérifient $p \le \Delta_n^{1/2w}$, pour $w \in [1,d]$. Donc, si Δ_n est petit, les facteurs premiers éventuels de Δ_n sont en nombre peu élevé. En utilisant cette méthode, Lehmer montre que

$$\begin{aligned} \Delta_{113}(x^3-x-1) &= 63088004325217 \\ \Delta_{127}(x^3-x-1) &= 3233514251032733 \end{aligned}$$

sont premiers et il se met à la recherche de polynômes pour lesquels Δ_n croît aussi lentement que possible.

Proposition 3 *Si f est non nul et sans racine de module* 1, *alors*

$$\lim_{n\to+\infty} \left| \frac{\Delta_{n+1}(f)}{\Delta_n(f)} \right| = \prod_{i=1}^{d} \max\left(|\alpha_i|, 1\right) \tag{1.1}$$

Démonstration. On a

$$\Delta_n(f) := \prod_{i=1}^{d} (\alpha_i^n - 1)$$

et

$$\Delta_{n+1}(f) := \prod_{i=1}^{d} \left(\alpha_i^{n+1} - 1\right).$$

On a deux cas à étudier : $|\alpha_i| < 1$ et $|\alpha_i| > 1$, pour $i \in 1, 2, ..., d$.

· Le cas ou $|\alpha_i| < 1$ implique $\lim_{n\to+\infty} \left|\frac{\alpha_i^{n+1}-1}{\alpha_i^n-1}\right| = 1$.

· le cas ou $|\alpha_i| > 1$ implique $\lim_{n\to+\infty} \left|\frac{\alpha_i^{n+1}-1}{\alpha_i^n-1}\right| = |\alpha_i|$.

Dans les deux cas,

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

■

Théorème 4 (formule de Jensen) *Soit $f(z)$ une fonction holomorphe dans un ouvert contenant le disque unité, $f(0) \neq 0$. Si $\alpha_1, \alpha_2, ..., \alpha_t$ désignent les zéros de $f(z)$ dans $|z| \leq 1$ comptés avec leurs multiplicités, alors*

$$\frac{1}{2\pi}\int_0^{2\pi} \log\left|f\left(e^{i\theta}\right)\right| d\theta = \log|f(0)| - \sum_{j=1}^{t} \log|\alpha_j|$$

Proposition 5 *Si f est irréductible, non cyclotomique*

$$\lim_{n\to+\infty} \frac{1}{n} \log|\Delta_n(f)| = \log M(f)$$

$$\lim_{n\to+\infty} |\Delta_n(f)|^{1/n} = M(f) \tag{1.2}$$

où

$$M(f) := \prod_{i=1}^{d} \max(|\alpha_i|, 1)$$

Démonstration. Nous démontrons la première formule et la deuxième s'en déduit rapidement.

On a

$$\begin{aligned}\Delta_n(f) &= \prod_{j=1}^{d}\left(\alpha_j^n - 1\right) = \prod_{j=1}^{d}\prod_{k=1}^{n}\left(\alpha_j - e^{\frac{2\pi ik}{n}}\right)\\ &= \prod_{k=1}^{n}\prod_{j=1}^{d}\left(\alpha_j - e^{\frac{2\pi ik}{n}}\right) = (-1)^d \prod_{k=1}^{n} f(e^{\frac{2\pi ik}{n}}).\end{aligned}$$

Donc

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\log|\Delta_n| &= \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\log\left|f(e^{\frac{2\pi ik}{n}})\right|\\ &= \frac{1}{2\pi}\int_0^{2\pi}\log\left|f(e^{i\theta})\right| d\theta.\end{aligned}$$

En utilisant la formule de Jensen, on a

$$\lim_{n\to\infty} \frac{1}{n} \log |\Delta_n| = \log M(f)$$

■

Lehmer estime donc le taux d'accroissement de Δ_n en évaluant les racines de P hors du disque unité et se met à la recherche de polynômes minimisant (1.2).

Or, par le théorème de Kronecker, pour f irréductible ne s'annulant pas en 0,

$$\prod_{i=1}^{d} \max(|\alpha_i|, 1) = 1 \Leftrightarrow f \text{ est cyclotomique.}$$

Ceci le conduit naturellement à poser la question suivante connue sous le nom de

Problème de Lehmer

Etant donné ε positif, existe-t-il un polynôme unitaire à coefficients entiers dont le produit des racines à l'extérieur du disque unité fermé soit compris, en valeur absolue, entre 1 et $1+\varepsilon$?

Lehmer détermine les polynômes minimisant (1.2) en degré 2, 3 et 4. Il met également en évidence les meilleurs trinômes en degré 5, 6 et 7 et les meilleurs polynômes symétriques en degré 2, 4, 6 et 8. Cette dernière classe de polynômes retient son attention et une recherche non exhaustive parmi ceux de degré 10, 12 et 14 ne lui permet pas de trouver mieux que

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \tag{1.3}$$

pour lequel (1.2) vaut $1,1762808....$

Quoi qu'il en soit, bien des années et des calculs plus tard, le polynôme (1.3) constitue toujours le record en la matière. Ce qui rend encore plus intéressant le problème de Lehmer.

1.3 Méthode de Lehmer

Soit $f \in \mathbb{Z}[x]$,

$$f = x^r + a_{d-1}x^{r-1} + ... + a_1 x + a_0 = \prod_{i=1}^{r}(x - \alpha_i),$$

et

$$\Delta_n = \Delta_n(f) := \prod_{i=1}^{r} (\alpha_i^n - 1) = \mathrm{Res}\ (f, x^n - 1) \in \mathbb{Z}.$$

On désigne par Φ_m le $m^{ème}$ polynôme cyclotomique, c'est à dire, ayant pour racines, les racines primitives $m^{ème}$ de l'unité.

On définit l'entier rationnel

$$\Phi_m^* := \Phi_m^*(f) := \prod_{i=1}^{r} \Phi_m(\alpha_i).$$

Il résulte alors de la formule

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

que

$$\alpha_i^n - 1 = \prod_{d|n} \Phi_d(\alpha_i).$$

Par suite,

$$\Delta_n(f) := \prod_{i=1}^{r} (\alpha_i^n - 1) = \prod_{i=1}^{r} \prod_{d|n} \Phi_d(\alpha_i) = \prod_{d|n} \prod_{i=1}^{r} \Phi_d(\alpha_i).$$

Soit

$$\Delta_n(f) = \prod_{d|n} \Phi_d^*,$$

c'est à dire une factorisation partielle de Δ_n en entiers rationnels.

D'où si Φ_n^*, $d \mid n$ exactement, est connu, la factorisation de $\Delta_n(f)$ ne sera complète que si l'on connait tous les Φ_d^*.

Le facteur Φ_n^* est appelé facteur essentiel de Δ_n.

Si $p \mid \Delta_n$ et $p \nmid \Delta_d$ pour $d \mid n$, on dit que p est un facteur premier caractéristique.

Théorème 6 *Le facteur essentiel Φ_n^* de Δ_n est divisible par tous les facteurs premiers caractéristiques de Δ_n.*

Démonstration. Soit p un facteur premier caractéristique de Δ_n. Alors $p \mid \Phi_d^*$ pour $d \mid n$. Si $d < n$ alors $p \mid \Delta_d$ et ceci est impossible. D'où $d = n$ et $p \mid \Phi_n^*$. ■

Théorème 7 *Un facteur premier caractéristique p de Δ_n ne divise pas n.*

Démonstration. Supposons $n = p.d$, alors

$$\Delta_{p.d} = \prod_{i=1}^{r} (\alpha_i^{p.d} - 1) = (-1)^r \left[1 - \sum_{i=1}^{r} \alpha_i^{p.d} + \sum_{i,j} (\alpha_i \alpha_j)^{p.d} + ... \right]$$

$$\begin{aligned}(\Delta_d)^p &= (-1)^{r.p}\left[1-\sum_{i=1}^{r}\alpha_i^d+\sum_{i,j}(\alpha_i\alpha_j)^d+....\right]^p\\ &\equiv (-1)^r\left[1-\sum_{i=1}^{r}\alpha_i^{p.d}+\sum_{i,j}(\alpha_i\alpha_j)^{p.d}+....\right] \mod(p).\end{aligned}$$

Par le petit théorème de Fermat, on a

$$(\Delta_d)^p \equiv \Delta_d \mod(p).$$

D'où $\Delta_{p.d} \equiv \Delta_d \bmod(p) \implies p \mid \Delta_d$ (contradiction). ■

Remarque 8 *Le facteur essentiel Φ_n^* peut avoir un facteur commun avec n. Par exemple si $f(x)=x^3+x+1$ alors $\Delta_3=\Phi_1^*.\Phi_3^*$ et $\Phi_1^*=-3,\ \Phi_3^*=3$.*

Théorème 9 *Soit p un facteur premier caractéristique de $\Delta_n(f)$ et e, la puissance maximale de p tels que $p^e \mid \Delta_n(f)$. Soit $f \in \mathbb{Z}[x]$ un polynôme irréductible de degré r et*

$$\omega = \inf_k \left\{k>0/\ p^k \equiv 1 \bmod(n)\right\},$$

alors $\omega \leq r$ et $\omega \mid e$.

Démonstration. Comme $p \nmid n$ alors $\left\{k>0\ /\ p^k \equiv 1 \bmod(n)\right\} \neq \varnothing$. Soit α racine de f et $K=\mathbb{Q}(\alpha)$.

$$(\alpha^n-1,p) \neq 1 \text{ dans } K.$$

En effet, si $(\alpha^n-1,p)=1$, $\exists\ x,\ y\ \in \mathbb{Z}_{\mathbb{Q}(\alpha)}$ tels que $x(\alpha^n-1)=p.y+1$. D'où

$$N_{K/\mathbb{Q}}(x).N_{K/\mathbb{Q}}(\alpha^n-1)=N(x).\Delta_n(f) \equiv 1 \bmod(n).$$

Ceci est impossible car $p \mid \Delta_n(f)$.

L'idéal engendré par α^n-1 s'écrit

$$(\alpha^n-1)=\Re.\wp_1^{e_1}.....\wp_t^{e_t}, \quad (\Re,\wp_i)=1,\ 1\leq i\leq t.....(\bigstar)$$

Les $\wp_i$ intervenant dans la décomposition en idéaux premiers de l'idéal $\langle p\rangle$.

D'où

$$\wp_i \mid (\alpha^n-1) \iff \alpha^n \equiv 1 \bmod(\wp_i),\ (\wp_i \nmid \alpha).$$

Soit

$$\varepsilon_i = \inf_k \left\{k\ /\ \alpha^k \equiv 1 \bmod(\wp_i)\right\}.$$

On a

$$\alpha^n \equiv 1 \bmod(\wp_i) \implies \varepsilon_i \mid n.$$

En effet, par définition $\varepsilon_i \leq n$, donc $n=q.\varepsilon_i+r,\ 0\leq r<\varepsilon_i$.

D'où $\alpha^n = (\alpha^{\varepsilon_i})^q . \alpha^r = (1 + c_i)^q \, \alpha^r = \alpha^r + b_i,\ c_i \in \wp_i,\ b_i \in \wp_i$.
Par conséquent $\alpha^r \equiv 1 \bmod (\wp_i)$. Contradiction.

Donc $(\alpha^{\varepsilon_i} - 1) = C.\wp_i$, C idéal de K. En prenant les normes

$$N(\alpha^{\varepsilon_i} - 1) = \Delta_{\varepsilon_i} = N(C).N(\wp_i) = N(C).p^{f_i}.$$

Ce qui implique que $\Delta_{\varepsilon_i} \equiv 0 \bmod(p^{f_i})$.

D'où $\varepsilon_i = n$ car p caractéristique. Or, $\wp_i \nmid \alpha$. D'après le théorème de Fermat dans les corps de nombres $\alpha^{p^{f_i}} \equiv i \bmod(\wp_i)$.

D'où $n = \varepsilon_i$ et $\varepsilon_i \mid p^{f_i} - 1$, soit, $p^{f_i} \equiv 1 \bmod(n)$. Alors $\omega \mid f_i \ \ , \forall i,\ 1 \leq i \leq t$. Or, $f_i \leq r$, d'où $\omega \leq r$.

Ecrivons $f_i = \sigma_i.\omega$ et prenons les normes dans ($\bigstar$)

$$\Delta_n(f) = N(\Re).p^{f_1 e_1 + ... + f_t e_t} = N(\Re).p^{\omega \sum\limits_i \sigma_i e_i} = N(\Re).p^{\omega\tau}.$$

Or,

$$(\Re, \wp_i) = 1 \implies (N(\Re), p) = 1 \implies e = \omega\tau.$$

■

On peut alors montrer deux régles pour trouver les facteurs caractéristiques de $\Delta_n(f)$.

1. On fait une liste des nombres premiers, puis de leurs carrés, etc..., enfin de leurs puissances ($r^{iémes}$ $r = d^\circ f$). Dans cette liste les nombres de la forme $n.x + 1$ sont les diviseurs potentiels de Δ_n.

2. On essaie comme diviseurs de $\Delta_n(f)$, les nombres premiers de la forme $n.x + 1$, inférieurs à $\sqrt{\Delta_n}$. Puis les premiers de la forme $n.x + z$, où $z^2 \equiv 1 \bmod(n)$ tels que $z \neq 1$ et inférieurs à $\Delta_n^{\frac{1}{4}}$ (car $p^2 \equiv 1 \bmod(n)$). Puis les premiers de la forme $n.x + w$, où $w^3 \equiv 1 \bmod(n)$ et inférieurs à $\Delta_n^{1/6}$. Le procédé s'arrête avec les premiers inférieurs à $\Delta_n^{1/2r}$ de la forme $n.x + u$ avec $u^r \equiv 1 \bmod(n)$.

Exemple 10 *Soit* $f(x) = x^2 - x - 1$ *ayant pour racines* $\alpha = \frac{1+\sqrt{5}}{2}$ *et* $\dfrac{-1}{\alpha}$.

$$\Delta_1(f) = -1,$$

$$\Delta_2(f) = \left(\alpha^2 - 1\right)\left(\left(\frac{-1}{\alpha}\right)^2 - 1\right) = -1.$$

D'aprés les formules de Newton $S_n = \alpha^n + \left(\dfrac{-1}{\alpha}\right)^n,\ n \geq 1$.
Donc $S_1 = 1,\ S_2 = S_1 + 2,\ S_{n+1} = S_n + S_{n-1},\ n \geq 2$.

On montre que $\Delta_{2k+1}(f) = -S_{2k+1},\ \Delta_{2k}(f) = 2 - S_{2k}$.
On voit facilement que Δ_n *vérifie la récurrence*

$$\Delta_{n+4} = \Delta_{n+3} + 2\Delta_{n+2} - \Delta_{n+1} - \Delta_n.$$

Le polynôme de la récurrence est

$$x^4 - x^3 - 2x^2 + x + 1 = (x-1)(x^2 - x - 1)(x+1).$$

Le calcul de Δ_n *se fait donc par récurrence. En voici les premières valeurs.*

Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6
$-(1)$	$-(1)$	$-(4)$	$-\underline{(5)}$	$-\underline{(11)}$	$-4^2 \times (1)$

Δ_7	Δ_8	Δ_9	Δ_{10}	Δ_{11}	Δ_{12}
$-\underline{(29)}$	$-5 \times (3)$	$-4\times\underline{(19)}$	$-11 \times (11)$	$-\underline{(199)}$	$-5 \times 4^3 \times (1)$

Δ_{13}	Δ_{14}	Δ_{15}	Δ_{16}	Δ_{17}	Δ_{18}
$-\underline{(521)}$	$-29\times\underline{(29)}$	$-4 \times 11\times\underline{(31)}$	$-9 \times 5 \times (7^2)$	$-\underline{(3571)}$	$-4 \times 19 \times (4 \times 19)$

Δ_{19}	Δ_{20}	Δ_{21}	Δ_{22}	Δ_{23}
$-\underline{(9349)}$	$-5 \times 11 \times (5^2 \times 11)$	$-4 \times 29\times\underline{(211)}$	$-199\times\underline{(199)}$	$-(139 \times 461)$

Les facteurs essentiels sont notés entre parenthèses et soulignés s'ils sont premiers. Ainsi $3571 = -\Delta_{17}$ *est premier car il n'existe pas de nombre premier inférieur à* $\sqrt[4]{3571}$ *dont le carré soit de la forme* $17x + 1$.

1.4 Mesure de Mahler d'un polynôme d'une variable

Soit $f \in \mathbb{Z}[x]$. Notons

$$f(x) = a_d \prod_{i=1}^{d} (x - \alpha_i),\ \alpha_i \in \mathbb{C}.$$

La mesure de Mahler de f est le nombre réel

$$M(f) = |a_d| \prod_{i=1}^{d} \max(|\alpha_i|, 1),$$

et la mesure logarithmique de Mahler de f est le nombre réel

$$m(f) = \log M(f)$$

- La mesure de Mahler est multiplicative $M(fg) = M(f)M(g)$.

- Si $f \in \mathbb{Z}[x] \setminus \{0\}$, alors $M(f) \geqslant 1$.

Quelques exemples

$P(x)$	$m(P)$
$x^8 + x^5 - x^4 + x^3 + 1$	0.2473585132
$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$	0.1623576120
$x^{10} - x^6 + x^5 - x^4 + 1$	0.1958888214
$x^{10} + x^7 + x^5 + x^3 + 1$	0.2073323581
$x^{10} - x^8 + x^5 - x^2 + 1$	0.2320881973
$x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + 1$	0.2368364616
$x^{10} + x^9 - x^5 + x + 1$	0.2496548880
$x^{12} + x^{11} + x^{10} - x^8 - x^7 - x^6 - x^5 - x^4 + x^2 + x + 1$	0.2052121880
$x^{12} + x^{11} + x^{10} + x^9 - x^6 + x^3 + x^2 + x + 1$	0.2156970336
$x^{12} + x^{10} + x^7 - x^6 + x^5 + x^2 + 1$	0.2345928411
$x^{12} + x^{10} + x^9 + x^8 + 2x^7 + x^6 + 2x^5 + x^4 + x^3 + x^2 + 1$	0.2412336268
$x^{14} + x^{11} - x^{10} - x^7 - x^4 + x^3 + 1$	0.1823436598
$x^{14} - x^{12} + x^7 - x^2 + 1$	0.1844998024
$x^{14} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$	0.2351686174
$x^{14} - x^{12} + x^{11} - x^9 + x^7 - x^5 + x^3 - x^2 + 1$	0.2272100851
$x^{14} + x^{13} - x^8 - x^7 - x^6 + x + 1$	0.2368858459
$x^{14} + x^{13} + x^{12} - x^9 - x^8 - x^7 - x^6 - x^5 + x^2 + x + 1$	0.2453300143
$x^{14} + x^{13} - x - x^7 - x^3 + x + 1$	0.2469561884

Soit α un nombre algébrique de degré d.
On pose

$$f_\alpha(x) = a_0 + a_1 x + a_2 x^2 + ... + x^d \in \mathbb{Z}[x],$$

son polynôme minimal et $\alpha_1, \alpha_2, ..., \alpha_d \in \mathbb{C}$, les conjugués de α.

La mesure de Mahler de α est le nombre réel

$$M(\alpha) = M(f_\alpha) = \prod_{i=1}^{d} \max(|\alpha_i|, 1).$$

Si α et β sont deux nombres algébriques, alors $M(\alpha\beta) \leqslant M(\alpha)^n M(\beta)^m, \forall n,\ m \in \mathbb{N}$.

Théorème 11 (Kronecker) *Soit α un entier algébrique non nul de degré d.*

$$f_\alpha(X) = a_0 + a_1 x + a_2 x^2 + ... + x^d,$$

son polynôme minimal. Alors α est une racine de l'unité si et seulement si

$$M(\alpha) = 1.$$

Démonstration. Soit

$$f_\alpha(X) = a_0 + a_1x + a_2x^2 + ... + x^d = (x-\alpha_1)(x-\alpha_2)....(x-\alpha_d),$$

alors

$$a_k = (-1)^{d-k} \sum_{1\le i_1\le i_2\le ...\le i_{d-k}\le d} \alpha_{i_1}\alpha_{i_2}...\alpha_{i_{d-k}},\ 0 \le k \le d-1.$$

D'où

$$|a_k| \le \sum_{1\le i_1\le i_2\le ...\le i_{d-k}\le d} \left|\alpha_{i_1}\alpha_{i_2}...\alpha_{i_{d-k}}\right| \le \left(\sum_{1\le i_1\le i_2\le ...\le i_{d-k}\le d} 1\right) M(\alpha).$$

Comme

$$\left(\sum_{1\le i_1\le i_2\le ...\le i_{d-k}\le d} 1\right) M(\alpha) = \binom{d}{k} M(\alpha),$$

alors

$$|a_k| \le \binom{d}{k} M(\alpha).$$

Supposons que $M(\alpha) = 1$. Considérons la suite $\{\alpha^m\}_{m=1}^{\infty}$.
α^m est aussi un nombre algébrique de degré au plus d et $M(\alpha^m) = 1$. Ainsi les coefficients du polynôme minimal de α^m sont bornés par $\binom{d}{k} \le 2^d$ et il y a seulement un nombre fini d'entre eux. Donc $\alpha^m = \alpha^k$ i.e. α est une racine de l'unité. ■

1.4.1 Conjecture de Schinzel et Zassenhaus

Soit α un entier algébrique dont le polynôme minimal est de degré d. Soient $\alpha_1, \cdots \alpha_d$ ses conjugués. On note

$$\lceil \alpha \rceil = \max_k |\alpha_k| .$$

Nous avons l'inégalité évidente de Schinzel et Zassenhaus

$$M(\alpha)^{\frac{1}{d}} \le \lceil \alpha \rceil \le M(\alpha).$$

Si α est une racine de l'unité alors $M(\alpha) = M(\alpha^{-1})$. Donc

$$\max\left(\lceil \alpha \rceil, \frac{1}{\lceil \alpha \rceil}\right) \le M(\alpha). \tag{1.4}$$

En 1965, Schinzel et Zassenhaus ont prouvé que si $\alpha \ne 0$ est un entier algébrique qui n'est pas racine de l'unité, et, si $2s$ de ses conjugués sont non réels, alors

$$\lceil \alpha \rceil > 1 + 4^{-s-2}.$$

Cette inégalité était le premier pas vers la résolution du problème de Lehmer.

Plus tard, sous les mêmes hypothèses, ils conjecturent

$$\lceil \alpha \rceil \geq 1 + \frac{c}{d}, \tag{1.5}$$

où c est une constante absolue, $c > 0$.

Une réponse positive à la conjecture de Lehmer impliquerait (1.5) car

$$M(\alpha)^{\frac{1}{d}} \leq \lceil \alpha \rceil \Rightarrow \lceil \alpha \rceil \geq 1 + \frac{\log M(\alpha)}{d}.$$

Ainsi, si $M(\alpha) \geq c_0 \geq 1$, alors

$$\lceil \alpha \rceil \geq 1 + \frac{\log c_0}{d}.$$

L'inégalité implique que tout progrès concernant le problème de Lehmer entraînerait l'inégalité de Schinzel-Zassenhaus.

La question de Lehmer a été intensivement étudié afin d'obtenir de nouvelles bornes. Dans ce qui suit, nous citons quelques bornes inférieures partielles, d désignant le degré du polynôme $P(x)$.

1. Blanksby et Montgomery (1971)

$$M(P) > 1 + \frac{1}{52 \log(6d)}.$$

2. Stewart (1978)

$$M(P) > 1 + \frac{c}{10^4 d \log(d)}.$$

3. Dobrowolski (1979)

$$M(P) > 1 + (1 - \varepsilon) \left(\frac{\log \log d}{\log d} \right)^3, \ d > d_0(\varepsilon).$$

4. Cantor et Strauss (1982)

$$M(P) > 1 + (2 - \varepsilon) \left(\frac{\log \log d}{\log d} \right)^3, \ d > d_0(\varepsilon).$$

5. louboutin (1983):

$$M(P) > 1 + (\frac{9}{4} - \varepsilon) \left(\frac{\log \log d}{\log d} \right)^3, \ d > d_0(\varepsilon).$$

Comme nous pouvons le remarquer, 4 et 5 sont une amélioration de la méthode de Dobrowolski en 3.

1.4.2 Théorème de Schinzel

Le lemme suivant est un cas particulier d'un résultat plus général de Schinzel. Il s'agit d'un polynôme avec zéros strictement réels.

Lemme 12 *Pour tout $d \geq 1$, et $y_1, \cdots, y_d > 1$ des nombres réels, alors*

$$(y_1 - 1) \cdots (y_d - 1) \leq \left((y_1 \cdots y_d)^{1/d} - 1 \right)^d.$$

Démonstration. Soit $y_i = x_i + 1$, nous considérons

$$f(x_1, \cdots, x_d) = \prod_{i=1}^{d} (x_i + 1)^{1/d} - 1 - \prod_{i=1}^{d} (x_i)^{1/d},$$

Montrons que $f(x_1, \cdots, x_d) \geq 0$.
Nous avons ici une fonction à plusieurs variables qui est dérivable et continue, où toutes les variables x_i sont ≥ 2, $1 \leq i \leq d$, car $y_i \geq 1$, et $d \geq 1$.

Cherchons les extrémums de cette fonction.
Calculons la dérivée de f par rapport à x_1

$$\begin{aligned}
f'_{x_1} &= \frac{1}{d}(1+x_1)^{1/d-1}(1+x_2)^{1/d} \cdots (1+x_d)^{1/d} - \frac{1}{d} x_1^{1/d-1} x_2^{1/d} \cdots x_d^{1/d}, \\
f'_{x_1} &= 0 \iff (1+x_1)^{1/d-1}(1+x_2)^{1/d} \cdots (1+x_d)^{1/d} = x_1^{1/d-1} x_2^{1/d} \cdots x_d^{1/d} \\
&\iff (1+x_1)^{1-d}(1+x_2) \cdots (1+x_d) = x_1^{1-d} x_2 \cdots x_d \\
&\iff x_1^d (1+x_1)(1+x_2) \cdots (1+x_d) = x_1 x_2 \cdots x_d (1+x_1)^d.
\end{aligned}$$

Comme tous les x_i sont ≥ 2, $(1 \leq i \leq d)$, alors tous les termes ci-dessus sont différents de 0, et nous avons l'égalité si et seulement si tous les x_i, $1 \leq i \leq d$, sont égaux.
Calculons la dérivée seconde de f par rapport à x_1

$$f''_{x_1} = \frac{1}{d}\left(\frac{1}{d} - 1\right)(1+x_1)^{1/d-2}(1+x_2)^{1/d} \cdots (1+x_d)^{1/d} - \frac{1}{d}\left(\frac{1}{d} - 1\right) x_1^{1/d-2} x_2^{1/d} \cdots x_d^{1/d}.$$

Si tous les x_i sont égaux,

$$\begin{aligned}
f''_{x_1} &= \frac{1}{d}\left(\frac{1}{d} - 1\right)(1+x)^{-1} - \frac{1}{d}\left(\frac{1}{d} - 1\right) x^{-1} \\
&= \frac{1}{d}\left(\frac{1}{d} - 1\right)\left(\frac{-1}{x(x+1)}\right).
\end{aligned}$$

On a $f''_{x_1} \geq 0$ car $d \geq 1$ et $x \geq 2$. Donc l'extremum de cette fonction est un minimum.

Comme f''_{x_1} ne peut pas être égale à 0, donc le minimum est unique.

Nous obtiendrons les mêmes résultats pour les dérivées de la fonction par rapport à d'autres x_i $(2 \leq i \leq d)$.

Donc, $f(x_1, \cdots x_d)$ a un minimum quand tous les x_i, $1 \leq i \leq d$, sont égaux

$$f(x, \cdots, x) = \left((1+x)^{1/d}\right)^d - 1 - \left(x^{1/d}\right)^d = 0.$$

Alors f est toujours positif. ■

Théorème 13 (Schinzel) *Soit $P \in \mathbb{Z}[x]$, un polynôme unitaire de degré d, tel que $P(-1)P(1) \neq 0$, et $P(0) = \pm 1$. Si les zéros de P sont tous réels, alors*

$$M(P) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}.$$

Démonstration. On considère $E = \prod_{i=1}^{d} |\alpha_i^2 - 1|$, où les α_i, $1 \leq i \leq d$, sont les racines de $P(x)$.

Puisque P est unitaire, on peut écrire $P(x) = \prod_{i=1}^{d} (x - \alpha_i)$, où $|P(1)| = \prod_{i=1}^{d} |1 - \alpha_i|$ et $|P(-1)| = \prod_{i=1}^{d} |-1 - \alpha_i|$. Alors E peut s'écrire $E = |P(1)P(-1)|$.

On a $E \geq 1$ puisque P est unitaire (son coefficient dominant est 1), et $P(-1)P(1) \neq 0$, par hypothèse.

Ensuite

$$\begin{aligned} E &= \prod_{|\alpha_i|} \left|\alpha_i^2 - 1\right| = \prod_{|\alpha_i|<1} \left|\alpha_i^2 - 1\right| \prod_{|\alpha_i|>1} \left|\alpha_i^2 - 1\right| \\ &= \prod_{|\alpha_i|>1} |\alpha_i|^2 \frac{1}{M(P)^2} \prod_{|\alpha_i|<1} \left|\alpha_i^2 - 1\right| \prod_{|\alpha_i|>1} \left|\alpha_i^2 - 1\right| \frac{P(0)^2}{P(0)^2}. \end{aligned}$$

On a $P(0) \neq 0$ et en factorisant P, on peut écrire $P(0) = \prod_{\alpha_i}(-\alpha_i)$, et alors

$$\begin{aligned} E &= \prod_{|\alpha_i|>1} |\alpha_i|^2 \frac{1}{M(P)^2} \prod_{|\alpha_i|<1} \left|\alpha_i^2 - 1\right| \prod_{|\alpha_i|>1} \left|\alpha_i^2 - 1\right| P(0)^2 \frac{1}{\prod_{|\alpha_i|>1} |\alpha_i|^2} \frac{1}{\prod_{|\alpha_i|<1} |\alpha_i|^2} \\ &= \frac{1}{M(P)^2} \prod_{|\alpha_i|<1} \left|\alpha_i^{-2} - 1\right| \prod_{|\alpha_i|>1} \left|\alpha_i^2 - 1\right|, \text{ puisque } P(0) = \pm 1, \text{ par hypothèse.} \end{aligned}$$

Supposons que $\{\alpha_i\}_{i=1,\ldots,j}$ sont les racines avec une valeur absolue inférieure à 1, et $\{\alpha_i\}_{i=j+1,\ldots,d}$ sont les autres racines, alors

$$E = \frac{1}{M(P)^2} \left(\alpha_1^{-2} - 1\right) \cdots \left(\alpha_j^{-2} - 1\right) \left(\alpha_{j+1}^2 - 1\right) \cdots \left(\alpha_d^2 - 1\right).$$

Nous avons ici une multiplication de d termes où les $\{\alpha_i\}_{i=1,\dots,d}$ sont réelles, donc nous pouvons appliquer le lemme ci-dessus

$$\begin{aligned}
E &\leq \frac{1}{M(P)^2}\left[\left(\left(\alpha_1^{-2}\right)\cdots\left(\alpha_j^{-2}\right)\left(\alpha_{j+1}^{2}\right)\cdots\left(\alpha_d^{2}\right)\right)^{1/d}-1\right]^d \\
&\leq \frac{1}{M(P)^2}\left[\left(\left(\alpha_1^{-2}\right)\cdots\left(\alpha_j^{-2}\right)\left(\alpha_{j+1}^{2}\right)\cdots\left(\alpha_d^{2}\right)\frac{\left(\alpha_{j+1}^{2}\right)\cdots\left(\alpha_d^{2}\right)}{\left(\alpha_{j+1}^{2}\right)\cdots\left(\alpha_d^{2}\right)}\right)^{1/d}-1\right]^d \\
&\leq \frac{1}{M(P)^2}\left[\left(\frac{1}{\pm P(0)^2}\left(\alpha_{j+1}^{4}\right)\cdots\left(\alpha_d^{4}\right)\right)^{1/d}-1\right]^d \\
&\leq \frac{1}{M(P)^2}\left[\left(\prod_{|\alpha_i|>1}\alpha_i^4\right)^{1/d}-1\right]^d.
\end{aligned}$$

On utilise le fait que $M(P)=\prod\limits_{|\alpha_i|>1}|\alpha_i|$ pour obtenir

$$\begin{aligned}
E &\leq \frac{1}{M(P)^2}\left(M(P)^{4/d}-1\right)^d \\
&= \left(M(P)^{2/d}-M(P)^{-2/d}\right)^d.
\end{aligned}$$

Puisque $1\leq E$, il s'ensuit que

$$M(P)^{2/d}-M(P)^{-2/d}\geq 1.$$

Pour résoudre cette inégalité, on pose $x=M(P)^{2/d}$, alors nous avons

$$x-x^{-1}\geq 1 \iff x^2-x-1\geq 0,$$

Cette inégalité est vérifiée pour $x\geq\frac{1+\sqrt{5}}{2}$ et pour $x\leq\frac{1-\sqrt{5}}{2}$.

Si on remplace x dans $x\geq\frac{1+\sqrt{5}}{2}$ par $M(P)^{2/d}$ on trouve

$$M(P)\geq\left(\frac{1+\sqrt{5}}{2}\right)^{d/2}.$$

■

Corollaire 14 *Si $P\in\mathbb{Z}[x]$ a tous les zéros réels. Avec les mêmes conditions que dans le théorème ci-dessus, on a*

$$M(P)\geq\frac{1+\sqrt{5}}{2}.$$

Démonstration. pour $d\geq 2$, il est clair que nous avons $M(P)\geq\frac{1+\sqrt{5}}{2}$.

Si $d=1$, on pose $P(X)=x+b$, tel que $b\in\mathbb{Z}[x]$. Comme $P(0)=\pm 1$. Donc $P(X)=x\pm 1$. Comme la condition $P(-1)P(1)\neq 0$ ne peut être vérifiée, alors il n'existe aucun polynôme de degré $d=1$ qui vérifie le corollaire. Par conséquent, nous appliquerons ce corollaire pour les polynômes de degré $d\geq 2$. ■

1.5 Mesure de Mahler d'un polynôme de plusieurs variables

Soit $P \in \mathbb{C}[x_1, x_2, ..., x_n]$, un polynôme à n variables.

La mesure logarithmique de Mahler du polynôme P et donnée par

$$m(P) := \frac{1}{(2\pi i)^n} \int_{T^n} \log|P(x_1, ..., x_n)| \frac{dx_1}{x_1} .... \frac{dx_n}{x_n},$$

où

$$T^n = \{(x_1, ..., x_n) \in \mathbb{C}^n \ / \ |x_1| = ... = |x_n| = 1\}.$$

En principe P ne devait pas s'annuler sur T^n. On verra plus loin que même si P s'annule sur T^n, $m(P)$ est bien définie .

Posons $x_j = e^{i\theta_j}$

$$\begin{aligned} m(P) &= \frac{1}{(2\pi)^n} \int_{[0,2\pi]^n} \log\left|P(e^{i\theta_1}, ..., e^{i\theta_n}\right| d\theta_1 .... d\theta_n \\ &= \int_0^1 \cdots \int_0^1 \log\left|P(e^{2i\pi\theta_1}, \cdots, e^{2i\pi\theta_n})\right| d\theta_1 \cdots d\theta_n. \end{aligned}$$

La mesure de Mahler de P est par définition

$$M(P) = \exp(m(P))$$

Si $P(X) = a_d(x - \alpha_1) .... (x - \alpha_d)$, $\alpha_j \neq 0$ alors

$$m(P) = \frac{1}{2\pi} \int_0^{2\pi} \log\left|f\left(e^{i\theta}\right)\right| d\theta.$$

D'après la formule de Jensen énoncé précédemment

$$M(P) = |a_d| \prod_{j=1}^{d} \max(|\alpha_j|, 1).$$

En effet, on a

$$\log|P(0)| = \log|a_d| + \log|\alpha_1| + ... + \log|\alpha_d|.$$

D'aprés la formule de Jensen

$$\begin{aligned} m(P) &= \log|P(0)| - \sum_{j=1}^{d} \log|\alpha_j| \\ &= \log|a_d| + \sum_{j=1}^{d} \log^+|\alpha_j|, \end{aligned}$$

où

$$\log^+ |\alpha_j| = \begin{cases} \log |\alpha_j| & si \ \ |\alpha_j| > 1 \\ 0 & \text{sinon} \end{cases}.$$

D'où

$$M(P) = \exp(m(P)) = |a_d| \prod_{j=1}^{d} \max(|\alpha_j|, 1).$$

Nous énonçons un théorème fondamental de Boyd qui montre le lien entre la mesure de Mahler d'un polynôme d'une seule variable et d'un polynôme de plusieurs variables.

Théorème 15 (Boyd 1981) *Si P est un polynôme non nul, $P \in \mathbb{C}[x_1, x_2]$*

$$M(P(x_1, x_2)) = \lim_{n \to +\infty} M(P(x, x^n)).$$

Ce résultat a été généralisé par Boyd et Lawton (83) à un polynôme de plusieurs variables.

Théorème 16 (LAWTON 1983) $P \in \mathbb{C}[x_1, ..., x_n]$

$$\lim_{r_2 \to \infty} \cdots \lim_{r_n \to \infty} m(P(x, x^{r_2} \cdots, x^{r_n})) = m(P(x_1, ..., x_n)).$$

Remarque 17 *Soient P et Q deux polynômes à n variables . On a*

$$\begin{aligned} m(P) + m(Q) &= \frac{1}{(2\pi i)^n} \int_{T^n} \log |P(x_1, ..., x_n)| \frac{dx_1}{x_1} .... \frac{dx_n}{x_n} \\ &\quad + \frac{1}{(2\pi i)^n} \int_{T^n} \log |Q(x_1, ..., x_n)| \frac{dx_1}{x_1} .... \frac{dx_n}{x_n} \\ &= \frac{1}{(2\pi i)^n} \int_{T^n} (\log |P(x_1, ..., x_n)| + \log |Q(x_1, ..., x_n)|) \frac{dx_1}{x_1} .... \frac{dx_n}{x_n} \\ &= \frac{1}{(2\pi i)^n} \int_{\Pi^n} \log |P(x_1, ..., x_n) Q(x_1, ..., x_n)| \frac{dx_1}{x_1} .... \frac{dx_n}{x_n} \\ &= m(PQ) \end{aligned}$$

Montrons maintenant que la mesure de Mahler est bien définie même si P s'annule sur T^n.

Lemme 18 *Soit $P(X) = a_d x^d + ... + a_1 x + a_0 \in \mathbb{Z}[x]$, alors*

$$|a_m| \leq \binom{d}{m} M(P), \ 0 \leq m \leq d.$$

Démonstration. Si $\alpha_1, ..., \alpha_d$ sont les racines de P

$$\frac{a_m}{a_d} = (-1)^{d-m} \sum_{1 \leq j_1 < j_2 < .. < j_{d-m} \leq d} \alpha_{j_1} \alpha_{j_2} .... \alpha_{j_{d-m}}$$

D'où

$$|a_m| \leq \binom{d}{m} M(P).$$

■

Lemme 19 *Soit* $P(x_1, x_2, ...x_n) = \sum a_{m_1 ... m_n} x_1^{m_1} x_2^{m_2} ... x_n^{m_n}$ *un polynôme de degré* d_j *en la variable* x_j.

$$|a_{m_1 m_2 ... m_n}| \leq \binom{d_1}{m_1} ... \binom{d_n}{m_n} M(P)$$

Démonstration. Le lemme 21 se montre par induction à partir du lemme 20.

Par exemple si $n = 2$, on écrit

$$\begin{aligned} P(x,y) &= a_{d_2}(x) y^{d_2} + a_{d_2-1}(x) y^{d_2-1} + ... + a_{m_2}(x) y^{m_2} + ... + a_0(x) \\ &= \sum a_{m_1 m_2} x^{m_1} y^{m_2}. \end{aligned}$$

Par suite, $a_{m_1 m_2}$ est le coefficient de x^{m_1} dans $a_{m_2}(x)$. D'aprés le lemme 20

$$|a_{m_1 m_2}| \leq \binom{d_1}{m_1} M(a_{m_2}(x))$$

Ecrivons maintenant

$$P(x,y) = a_{d_2}(x)(y - y_1(x))....(y - y_d(x))$$

D'où

$$|a_{m_2}(x)| \leq |a_{d_2}(x)| \binom{d_2}{m_2} \prod_j \max(|y_j(x)|, 1).$$

Donc

$$\log |a_{m_2}(x)| \leq \log \left(\binom{d_2}{m_2} \right) + \log |a_{d_2}(x)| + \sum_j \log^+ (|y_j(x)|).$$

D'où

$$\underbrace{\frac{1}{2\pi i} \int_{|x|=1} \log |a_{m_2}(x)| \frac{dx}{x}}_{m(a_{m_2}(x))} \leq \log \left(\binom{d_2}{m_2} \right) + \underbrace{\frac{1}{2\pi i} \int_{|x|=1} (\log |a_{d_2}(x)| + \sum_j \log^+ (|y_j(x)|)) \frac{dx}{x}}_{m(P)}.$$

Soit

$$M(a_{m_2}(x)) \leq \binom{d_2}{m_2} M(P).$$

Finalement

$$|a_{m_1 m_2}| \leq \binom{d_1}{m_1}\binom{d_2}{m_2} M(P)$$

■

Lemme 20 *Soit* $P(x_1, x_2, ...x_n) = \sum a_{m_1...m_n} x_1^{m_1} x_2^{m_2} ...x_n^{m_n}$ *un polynôme de degré* d_j *en la variable* x_j.

$$m(P) \leq \sum |a_{m_1...m_n}|$$

On a

$$m(P) = \frac{1}{(2\pi)^n} \int\limits_{[0,2\pi]^n} \log \left| P(e^{i\theta_1}, ..., e^{i\theta_n} \right| d\theta_1 ....d\theta_n$$

L'inégalité $\log |x| < |x|$ donne

$$\begin{aligned} m(P) &< \frac{1}{(2\pi)^n} \int\limits_{[0,2\pi]^n} \left| P(e^{i\theta_1}, ..., e^{i\theta_n} \right| d\theta_1 ....d\theta_n \\ &\leq \frac{1}{(2\pi)^n} \int\limits_{[0,2\pi]^n} (\sum |a_{m_1...m_n}|) d\theta_1 ....d\theta_n \\ &= \sum |a_{m_1...m_n}| \end{aligned}$$

Des lemmes 20, 21, 22, on déduit que $m(P)$ est bien définie pour tout polynôme P.

1.6 Mesure de Mahler $k-$supérieure

Soit $P \in \mathbb{C}[x_1, x_2, \ldots x_n] \setminus \{0\}$ un polynôme à n variables. Sa mesure de Mahler $k-$supérieure est définie par

$$m_k(P) = \frac{1}{(2\pi i)^n} \int\limits_{T^n} \log^k |P(x_1, ..., x_n)| \frac{dx_1}{x_1} .... \frac{dx_n}{x_n}.$$

En général, $m_k(P) + m_k(Q) \neq m_k(PQ)$ lorsque $k > 1$.

Même pour les polynômes les plus simples, la mesure de Mahler supérieure est souvent difficile à calculer.

1.7 Mesure de Mahler supérieure multiple

Soit les polynômes $P_1, P_2, ..., P_l \in \mathbb{C}[x_1, x_2, \dots x_n] \setminus \{0\}$. Leur mesure de Mahler supérieure multiple est définie par

$$m(P_1, ..., P_l) := \int_0^1 \dots \int_0^1 (\log \left|P_1(e^{2\pi i\theta_1}, ..., e^{2\pi i\theta_r)})\right|) \dots (\log \left|P_l(e^{2\pi i\theta_1}, ..., e^{2\pi i\theta_r})\right|) d\theta_1 .... d\theta_r.$$

Cette construction donne la mesure de Mahler supérieure d'un polynôme comme un cas particulier

$$m_k(P) = m(\underbrace{P, \dots, P}_{k}).$$

Lorsque les polynômes sont indépendants, la définition ci-dessus implique que

$$m(P_1) \dots m(P_l) = m(P_1, ..., P_l)$$

1.8 Mesure zêta de Mahler

Définition 21 *Soit $P \in \mathbb{C}[x_1, x_2, \dots x_n] \setminus \{0\}$ un polynôme à n variables. Sa mesure zêta de Mahler est définie par*

$$Z(s, P) := \frac{1}{(2\pi i)^n} \int_{T^n} |P(x_1, \cdots, x_n)|^s \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}.$$

Remarque 22 *Il y a un lien important entre la mesure de Mahler supérieure et la mesure zêta de Mahler. En effet, on a*

$$\begin{aligned} \frac{d^k Z(s, P)}{ds^k} &= \frac{1}{(2\pi i)^n} \int_{T^n} \frac{d^k |P(x_1, \cdots, x_n)|^s}{ds^k} \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n} \\ &= \frac{1}{(2\pi i)^n} \int_{T^n} |P(x_1, \cdots, x_n)|^s \log^k |P(x_1, \cdots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}. \end{aligned}$$

Donc

$$\left[\frac{d^k Z(s, P)}{ds^k}\right]_{s=0} = \frac{1}{(2\pi i)^n} \int_{T^n} \log^k |P(x_1, \cdots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n} = m_k(P).$$

En d'autres mots,

$$Z(s, P) := \sum_{k=0}^{\infty} \frac{m_k(P) s^k}{k!}.$$

Comme elle ne contient pas de logarithme, la mesure Zêta de Mahler peut parfois être plus facile à calculer.

Exemple 23

$$\begin{aligned}
m_2(x-1) &= \frac{\pi^2}{12} \\
m_3(x-1) &= \frac{-3\zeta(3)}{2} \\
m_4(x-1) &= \frac{19\pi^2}{240} \\
m_2(x+y+2) &= \frac{\zeta(2)}{2} \\
m_3(x+y+2) &= \frac{9\zeta(2)}{2}\log 2 - \frac{15}{4}\zeta(3). \\
m(1-x,\ 1-e^{2\pi i\alpha}x) &= \frac{\pi^2}{2}(\alpha^2-\alpha+\frac{1}{6}), \quad 0 \leq \alpha \leq 1.
\end{aligned}$$

Chapitre 2

Caractères et séries L de Dirichlet

2.1 Introduction

Les caractères de Dirichlet et leurs séries L furent introduits par Dirichlet, en 1831, dans le but de prouver le théorème de Dirichlet à propos de l'infinité des nombres premiers dans les progressions arithmétiques. L'extension aux fonctions holomorphes fut accomplie par Bernhard Riemann.

Dans ce chapitre, nous étudions de façon détaillée les caractères de groupes abéliens finis et les caractères de Dirichlet modulo k. Nous donnons des exemples de calcul et, en particulier, un cacul explicite pour les valeurs de $k = 2, \cdots, 15$. Nous rappelons la notion de conducteur d'un caractère et la méthode qui nous permet de le déterminer effectivement avec quelques exemples. Nous étudions également les propriétés des séries L de Dirichlet.

Les références utilisées : [23], [27].

2.2 Caractères de groupes abéliens finis

Définition 24 *Soit G un groupe abélien fini. On appelle caractère de G, tout homomorphisme*

$$\sigma : G \longrightarrow \mathbb{C}^*.$$

L'ensemble des caractères d'un groupe abélien fini G est noté $\hom(G, \mathbb{C}^*)$ *ou bien* $\widehat{G}$.

Définition 25 (Caractère principal) *Le caractère principal est l'homomorphisme $\sigma_0 := \mathrm{I}$ de G dans $\mathbb{C}^*$ défini par $\sigma_0(x) = 1$, $\forall x \in G$.*

Propriété 26 (fondamentale) *Soit G un groupe abélien fini d'ordre $n \geq 1$ et $\sigma \in \hom(G, \mathbb{C}^*)$. Alors $\forall z \in G$, $\sigma(z)$ est une racine $n^{ième}$ de l'unité dans $\mathbb{C}^*$*

$(\sigma(z) \in U_n(\mathbb{C}^*))$, $|\sigma(z)| = 1$ *et* $\overline{\sigma(z)} = \dfrac{1}{\sigma(z)}$.

Démonstration. On a $(\sigma(z))^n = \sigma(z^n) = \sigma(e) = 1$, alors $\sigma(z)$ est une racine $n^{\text{ième}}$ de l'unité dans $\mathbb{C}^*$ et l'on a alors $|\sigma(z)| = 1$ et $\overline{\sigma(z)} = \dfrac{1}{\sigma(z)}$. ■

Définition 27 (Caractère conjugué) $\forall \sigma \in \hom(G, \mathbb{C}^*)$, *le conjugué de* σ, *noté* $\overline{\sigma}$, *est l'homomorphisme défini de* G *dans* $\mathbb{C}^*$ *par* $\overline{\sigma}(x) = \overline{\sigma(x)} = \dfrac{1}{\sigma(x)} = (\sigma(x))^{-1}$.

La loi $(\sigma\tau) : (\sigma\tau)(z) = \sigma(z)\tau(z)$, $\forall z \in G$ munit l'ensemble $\hom(G, \mathbb{C}^*)$ d'une structure de groupe abélien appelé le groupe des caractères de G.
L'élément neutre de $\widehat{G}$ est σ_0 défini par $\sigma_0(z) = 1$, $\forall z \in G$.
Le symétrique de σ est $\overline{\sigma}$ car $\forall x \in G$, on a $(\sigma\overline{\sigma})(x) = \sigma(x)\overline{\sigma(x)} = |\sigma(x)|^2 = 1$ $(\sigma\overline{\sigma} = \overline{\sigma}\sigma = \sigma_0)$.
Comme $\left(\sigma^{-1} = \overline{\sigma} \ \left(\forall \sigma \in \widehat{G}\right)\right)$, alors $\widehat{G} = \left(\widehat{G}\right)^{-1} = \left\{\overline{\sigma} \ / \ \sigma \in \widehat{G}\right\}$.
Le groupe $\widehat{G} = \hom(G, \mathbb{C}^*)$ est appelé groupe dual de G.

Remarque 28 .

1. *Si* $G = \{e\}$ *le groupe trivial, alors* $\hom(G, \mathbb{C}^*) = \{\sigma_0\}$ *où* $\sigma_0(e) = 1$.
2. *Si* $G = \langle x \rangle$, *un groupe cyclique d'ordre* 3, *d'élément neutre* e *et* $\sigma \in \hom(G, \mathbb{C}^*)$, *alors*

$$(\sigma(x))^3 = \sigma\left(x^3\right) = \sigma(e) = 1,$$

d'où $\sigma(x) \in \{1, j, j^2\}$. *On a donc trois caractères du groupe* G

$$\hom(G, \mathbb{C}^*) = \langle\sigma\rangle = \left\{\sigma_0, \sigma, \sigma^2\right\} = \left\langle\sigma^2\right\rangle,$$

où

$$\sigma(x) = j \left(j = \frac{-1 + i\sqrt{3}}{2}, \ j^3 = 1\right).$$

On peut représenter les éléments de $\hom(\{e, x, x^2\}, \mathbb{C}^*)$ *comme suit*

	e	x	x^2	
$\sigma^0 = \sigma_0$	1	1	1	$\Sigma = 3$
σ	1	j	j^2	$\Sigma = 0$
σ^2	1	j^2	j	$\Sigma = 0$
	$\Sigma = 3$	$\Sigma = 0$	$\Sigma = 0$	

$\left(\sigma^2 = \overline{\sigma}\right)$

Remarque 29 *Σ représente la somme des nombres d'une ligne ou d'une colonne. Cette somme est nulle sauf pour la première ligne et la première colonne où elle vaut $|G|$.*

Théorème 30 *Soit G un groupe abélien fini d'ordre $n \geq 2$.*

1. *Si G est cyclique, $G = \langle x \rangle = \{e, x, \ldots, x^{n-1}\}$, alors $\hom(G, \mathbb{C}^*)$ est cyclique d'ordre n, engendré par $\sigma \in \hom(G, \mathbb{C}^*)$, où $\sigma(x) = \xi = \exp\left(i\frac{2\pi}{n}\right)$, une racine primitive $n^{\text{ième}}$ de l'unité dans $\mathbb{C}$. i.e.*

$$\begin{aligned} \hom(G, \mathbb{C}^*) &= \{\sigma^a = f_a \ / \ a \in \{0, \ldots, n-1\}\} = \langle \sigma \rangle \\ \hom(G, \mathbb{C}^*) &\simeq G, \end{aligned}$$

avec $f_a = \sigma^a = \underbrace{\sigma \cdots \sigma}_{a \ fois}$, $\sigma^0 = \mathrm{I} : x \mapsto 1$ et

$$\forall x^\nu \in G, \ on \ a \ \sigma^a(x^\nu) = (\sigma(x))^{a\nu} = \exp\left(i\frac{2a\nu\pi}{n}\right).$$

2. *Si $G = H \odot K$ est un produit direct de deux sous-groupes cycliques tels que*

$$H = \langle x \rangle, \ o(H) = o(x) = r$$

et

$$K = \langle y \rangle, \ o(K) = o(y) = s \ \ (r, s \in \mathbb{N}^* \ et \ n = r \times s),$$

avec $r, s \in \mathbb{N}^*$ et $n = r \times s$, alors

$$\hom(G, \mathbb{C}^*) = \langle \tau \rangle \odot \langle \sigma \rangle,$$

où $\tau, \sigma \in \hom(G, \mathbb{C}^*)$ sont définis par

$$\tau(x) = \xi = \exp\left(i\frac{2\pi}{r}\right) \ et \ \tau(y) = 1$$

et

$$\sigma(y) = \omega = \exp\left(i\frac{2\pi}{s}\right) \ et \ \sigma(x) = 1.$$

On a donc

$$\hom(G, \mathbb{C}^*) = \left\{\tau^a\sigma^b = f_{a,b} \ / \ \ (a, b) \in \{0, \ldots, r-1\} \times \{0, \ldots, s-1\}\right\} :\simeq G,$$

avec

$$f_{a,b}(x) = \left(\tau^a\sigma^b\right)(x) = \xi^a, \ f_{a,b}(y) = \left(\tau^a\sigma^b\right)(y) = \omega^b,$$
$$f_{0,0} = \tau^0\sigma^0 = \mathrm{I},$$

et

$$\forall x^{\nu}y^{\mu} \in G,\ \forall f_{a,b} = \tau^{a}\sigma^{b} \in \hom\left(G, \mathbb{C}^{*}\right),$$

on a

$$f_{a,b}\left(x^{\nu}y^{\mu}\right) = \left(\tau^{a}\sigma^{b}\right)\left(x^{\nu}y^{\mu}\right) = \xi^{a\nu}\omega^{b\mu} = \exp\left(i\left(\frac{a\nu}{r} + \frac{b\mu}{s}\right)2\pi\right).$$

Démonstration. .

1. Puisque $G = \langle x\rangle = \left\{e, x, \ldots, x^{n-1}\right\}$, tout élément de $\hom\left(G, \mathbb{C}^{*}\right)$ est complètement déterminé par la valeur de $\sigma \in \hom\left(G, \mathbb{C}^{*}\right)$. Comme $\left(\sigma\left(x\right)\right)^{n} = \sigma(x^{n}) = \sigma(e) = 1$, alors $\sigma(x)$ est une racine $n^{\text{ième}}$ de l'unité dans $\mathbb{C}$ (il en existe exactement n dans $\mathbb{C}$). Donc, il y a exactement n caractères du groupe G.

Soit $\sigma \in \hom\left(G, \mathbb{C}^{*}\right)$ défini par $\sigma(x) = \xi = \exp\left(i\frac{2\pi}{n}\right)$, la première racine primitive $n^{\text{ième}}$ de l'unité. On vérifie que $o\left(\sigma\right) = n$. En effet, on a

$$\sigma^{m}\left(x\right) = \exp\left(i\frac{2m\pi}{n}\right) \neq 1,\ \forall 1 \leq m < n,$$

et

$$\sigma^{n}\left(x\right) = \exp\left(i\frac{2n\pi}{n}\right) = 1.$$

On remarque que l'ensemble des générateurs de $\hom\left(G, \mathbb{C}^{*}\right)$ est

$$\left\{\sigma^{a} \ / \ 1 \leq a \leq n \text{ et } (a, n) = 1\right\}.$$

2. Soit $\sigma \in \hom\left(G, \mathbb{C}^{*}\right)$. Pour tout $z = x^{\nu}y^{\mu} \in G$, on a

$$\sigma\left(z\right) = \left(\sigma\left(x\right)\right)^{\nu}\left(\sigma\left(y\right)\right)^{\mu}.$$

On en déduit qu'un caractère de G est complètement déterminé par les valeurs de $\sigma(x)$ et $\sigma\left(y\right)$ dans $\mathbb{C}^{*}$.

Puisque

$$\left(\sigma\left(x\right)\right)^{r} = \sigma\left(x^{r}\right) = \sigma(e) = 1,$$

et

$$\left(\sigma\left(y\right)\right)^{s} = \sigma\left(y^{s}\right) = \sigma(e) = 1,$$

alors $\sigma\left(x\right)$ est une racine $r^{\text{ième}}$ de l'unité dans $\mathbb{C}^{*}$ (il en existe exactement r) et $\sigma\left(y\right)$ est une racine $s^{\text{ième}}$ de l'unité dans $\mathbb{C}$ (il en existe exactement s).

Donc $\left|\hom\left(G, \mathbb{C}^{*}\right)\right| = r \times s = \left|G\right|$.

On doit montrer que $o\left(\tau\right) = r$ et $o\left(\sigma\right) = s$ et $\langle\tau\rangle \bigcap \langle\sigma\rangle = \{\mathrm{I}\}$.

Soit $m,\ 1 \leq m < r$. On a

$$\tau^{m}\left(x\right) = \underbrace{\tau\left(x\right) \times \cdots \times \tau\left(x\right)}_{m \text{ fois}} = \xi^{m} = \exp\left(i\frac{2\pi m}{r}\right) \neq 1.$$

Comme $\tau(y) = 1$, alors $\tau^m \neq \mathrm{I}\ (\forall m,\ 1 \leq m < r)$.
On remarque que $\tau^r = \mathrm{I}$ car $\tau^r(x) = \exp\left(i\frac{2\pi r}{r}\right) = 1$ et $\tau^r(y) = 1$.
Alors $o(\tau) = r$. On démontre de la même façon que $o(\sigma) = s$.
Montrons que $\langle\tau\rangle \bigcap \langle\sigma\rangle = \{\mathrm{I}\}$.

Soit $f \in \langle\tau\rangle \bigcap \langle\sigma\rangle$. Alors $f = \tau^\alpha = \sigma^\beta$, où $\alpha \in \{0, 1, \ldots, r-1\}$ et $\beta \in \{0, 1, \ldots, s-1\}$. Il vient que $f(x) = \sigma^\beta(x) = (\sigma(x))^\beta = 1$ et $f(y) = \tau^\alpha(y) = (\tau(y))^\alpha = 1$, d'où $f = \mathrm{I}$.
On a donc $\hom(G, \mathbb{C}^*) = \langle\tau\rangle \odot \langle\sigma\rangle$ isomorphe à G car ils ont la même structure.
Soit $f \in \hom(G, \mathbb{C}^*) = \langle\tau\rangle \odot \langle\sigma\rangle$. Il existe un unique couple

$$(a, b) \in \{0, 1, \ldots, r-1\} \times \{0, 1, \ldots, s-1\}$$

tel que $f = \tau^a\sigma^b$ avec

$$f(x) = \left(\tau^a\sigma^b\right)(x) = (\tau^a)(x)\left(\sigma^b\right)(x) = (\tau(x))^a(\sigma(x))^b = \xi^a,\ \ (\sigma(x) = 1)$$

$$f(y) = \left(\tau^a\sigma^b\right)(y) = (\tau^a)(y)\left(\sigma^b\right)(y) = (\tau(y))^a(\sigma(y))^b = \omega^b,\ \ (\tau(y) = 1).$$

En notant $\sigma = \tau^a\sigma^b$ par $\sigma = f_{a,b}$, on obtient la forme annoncée du groupe $\hom(G, \mathbb{C}^*)$.
$\forall z = x^\nu y^\mu \in G,\ \forall f_{a,b} \in \hom(G, \mathbb{C}^*)$,

$$f_{a,b}(z) = \left(\tau^a\sigma^b\right)(x^\nu y^\mu) = \xi^{a\nu}\omega^{b\mu}.$$

■

Théorème 31 *Soient G un groupe abélien fini non trivial, H un sous-groupe de G.*

1. *Tout $\sigma \in \hom(H, \mathbb{C}^*)$ admet exactement $[G : H]$ prolongements au groupe G.*
2. $|\hom(G, \mathbb{C}^*)| = |G|$.

Théorème 32 *Soit G un groupe abélien fini non trivial, on a alors*

1. *Il existe un nombre r, $r \geq 1$, fini de sous-groupes cycliques de G tel que $G = H_1 \odot \cdots \odot H_r$ et*

$$G \simeq \prod_{i=1}^{r} \hom(H_i, \mathbb{C}^*) \overset{v}{\simeq} \hom(G, \mathbb{C}^*),$$

où v est défini par

$$\left\{ \begin{array}{c} (\sigma_1, \ldots, \sigma_r) \mapsto v((\sigma_1, \ldots, \sigma_r)) = (\sigma_1 \circ s_1) \cdots (\sigma_r \circ s_r)\ \ et \\ s_i : H_1 \odot \cdots \odot H_r \to H_i : h_1 \cdots h_r \mapsto h_i. \end{array} \right\}$$

2. *Si* $G \overset{u}{\simeq} G_1 \times \cdots \times G_r$, *alors* $\prod_{i=1}^{r} \hom(G_i, \mathbb{C}^*) \overset{\widehat{u}}{\simeq} \hom(G, \mathbb{C}^*)$ *où* $\widehat{u}$ *est défini par*

$$\left\{ \begin{array}{c} (\sigma_1, \ldots, \sigma_r) \mapsto \widehat{u}((\sigma_1, \ldots, \sigma_r)) = (\sigma_1 \circ \boldsymbol{p_1} \circ u) \cdots (\sigma_r \circ \boldsymbol{p_r} \circ u) \ \ et \\ \boldsymbol{p_i} : G_1 \times \cdots \times G_r \to G_i : (x_1, \ldots, x_r) \mapsto x_i. \end{array} \right\}$$

Remarque 33 *Si* G *est un groupe abélien d'ordre* 8. *On a trois structures possibles pour* G :

1. G *est cyclique d'ordre* 8 *s'il contient un élément d'ordre* 8.
2. $G = \{e, x, x^2, x^3\} \odot \{e, y\}$ *où* $y \notin \{e, x, x^2, x^3\}$ *et* $o(y) = 2$, *si* G *contient un élément* x *d'ordre* 4.
3. $G = \langle x \rangle \odot \langle y \rangle \odot \langle z \rangle$ *si tous les élément de* G *sont d'ordre* 2.

Théorème 34 (Relations duales d'orthogonalité) *Soient* G *un groupe abélien fini non trivial et* $\widehat{G} := \hom(G, \mathbb{C}^*)$ *son groupe dual. Alors* $\forall\ x, y \in G$ *et* $\forall \sigma, \tau \in \widehat{G}$, *on a*

$$\begin{aligned} S(x) &= \sum_{\sigma \in \widehat{G}} \sigma(x) = \left\{ \begin{array}{c} |G| \ \ si\ x = e \\ 0 \ \ si\ x \neq e \end{array} \right\}, \\ S(\sigma) &= \sum_{x \in G} \sigma(x) = \left\{ \begin{array}{c} |G| \ \ si\ \sigma = \sigma_0 \\ 0 \ \ si\ \sigma \neq \sigma_0 \end{array} \right\}, \\ S(x, y) &= \sum_{\sigma \in \widehat{G}} \sigma(x)\overline{\sigma}(y) = \left\{ \begin{array}{c} |G| \ \ si\ x = y \\ 0 \ \ si\ x \neq y \end{array} \right\}, \\ S(\sigma, \tau) &= \sum_{x \in G} \sigma(x)\tau(x) = \left\{ \begin{array}{c} |G| \ \ si\ \tau = \overline{\sigma} \\ 0 \ \ si\ \tau \neq \overline{\sigma} \end{array} \right\}. \end{aligned}$$

Démonstration. .

La première formule.

Si $x = e$ alors $\sigma(x) = 1\ \forall \sigma \in \widehat{G}$. Par suite $S(x) = \sum_{\sigma \in \widehat{G}} 1 = \left|\widehat{G}\right| = |G|$.

Si $x \neq e$ alors il existe $\tau \in \widehat{G}$ tel que $\tau(x) \neq 1$. En effet, soit le sous-groupe $H = \langle x \rangle$ $(o(H) = m \mid |G|)$. On considère l'homomorphisme $v \in \hom(H, \mathbb{C}^*)$ défini par

$$v(x) = \exp\left(i\frac{2\pi}{m}\right) \neq 1.$$

Soit τ un prolongement de v à G. Alors $\tau \in \widehat{G}$ et vérifie

$$\tau(x) = v(x) = \exp\left(i\frac{2\pi}{m}\right) \neq 1.$$

On remarque que $\widehat{G} = \tau\widehat{G}$. Donc

$$S(x) = \sum_{\sigma\in\widehat{G}} \sigma(x) = \sum_{\sigma\in\widehat{G}} (\tau\sigma)(x) = \tau(x) \sum_{\sigma\in\widehat{G}} \sigma(x) = \tau(x)S(x).$$

Il en vient $(1 - \tau(x)) S(x) = 0$. Puisque $\tau(x) \neq 1$ alors $S(x) = 0$.
La deuxième formule.
Si $\sigma = \sigma_0$, alors

$$S(\sigma) = S(\sigma_0) = \sum_{x\in G} 1 = |G|.$$

Si $\sigma \neq \sigma_0$, alors il existe $y \in G$, $y \neq e$ et $\sigma(y) \neq 1$. Sachant que $G = yG$, alors

$$S(\sigma) = \sum_{x\in G} \sigma(yx) = \sigma(y) \sum_{x\in G} \sigma(x) = \sigma(y)S(\sigma).$$

Il en vient que $(1 - \sigma(y)) S(\sigma) = 0$. Puisque $\sigma(y) \neq 1$ alors $S(\sigma) = 0$.
La troisième formule.
Si $x = y$, alors $\forall\sigma \in \widehat{G}$, on a $\sigma(x)\overline{\sigma}(x) = |\sigma(x)|^2 = 1$, d'où

$$S(x, y) = \sum_{\sigma\in\widehat{G}} 1 = \left|\widehat{G}\right| = |G|.$$

Si $x \neq y$, on a trois cas à étudier : $(x = e \text{ et } y \neq e)$, $(x \neq e \text{ et } y = e)$ et $(x \neq e \text{ et } y \neq e)$.
Dans le premier cas, on aura d'après la première formule

$$S(x, y) = \sum_{\sigma\in\widehat{G}} \sigma(x)\overline{\sigma}(y) = \sum_{\sigma\in\widehat{G}} \overline{\sigma}(y) = \sum_{\sigma\in\widehat{G}} \sigma(y) = 0.$$

Dans le deuxième cas, on aura

$$S(x, y) = \sum_{\sigma\in\widehat{G}} \sigma(x) = 0.$$

Dans le troisième cas, on utilise le fait que $G = xG$, d'où il existe $t \in G$, $t \neq e$ tel que $y = xt$. Par suite $S(x, y)$ devient

$$S(x, y) = \sum_{\sigma\in\widehat{G}} \sigma(x)\overline{\sigma}(xt) = \sum_{\sigma\in\widehat{G}} \sigma(x)\overline{\sigma}(x)\overline{\sigma}(t) = \sum_{\sigma\in\widehat{G}} |\sigma(x)|^2 \overline{\sigma}(t) = \sum_{\sigma\in\widehat{G}} \overline{\sigma}(t) = 0.$$

La quatrième formule.
Si $\tau = \overline{\sigma}$, alors $\forall x \in G$, $\sigma(x)\overline{\sigma}(x) = |\sigma(x)|^2 = 1$. Par suite $\sum_{x\in G} 1 = |G|$.
Si $\tau \neq \overline{\sigma}$, sachant que le symétrique de σ est $\overline{\sigma}$, alors $\sigma\tau \neq \sigma_0$. Donc, il existe

$y \in G$, $y \neq e$ et $(\sigma\tau)(y) \neq 1$.
Remarquons que $G = yG$. Alors

$$\begin{aligned} S(\sigma,\tau) &= \sum_{x\in G} \sigma(x)\tau(x) = \sum_{x\in G} (\sigma\tau)(x) = \sum_{x\in G} (\sigma\tau)(xy) \\ &= (\sigma\tau)(y) \sum_{x\in G} (\sigma\tau)(x) = ((\sigma\tau)(y))\, S(\sigma,\tau), \end{aligned}$$

d'où $S(\sigma,\tau)((\sigma\tau)(y) - 1) = 0$.
Puisque $(\sigma\tau)(y) \neq 1$, alors $S(\sigma,\tau) = 0$. ■

2.3 les caractères du groupe G(k)

$\forall\ k \in \mathbb{N}^*$, on note $G(k)$, le groupe multiplicatif $\left(\frac{\mathbb{Z}}{k\mathbb{Z}}\right)^*$ des nombres entiers inversibles modulo k. L'ordre du groupe $G(k)$ est égal à

$$\varphi(k) = \sum_{1\leq m\leq k,\ (m,k)=1} 1,$$

où φ est la fonction d'Euler.

Puisque $G(k)$ est un groupe abélien fini, alors $G(k) \simeq \hom(G(k), \mathbb{C}^*)$.

Pour les valeurs $k = 1, 2, 3, 4$, les groupes $\hom(G(k), \mathbb{C}^*)$ se calculent facilement et l'on a :

- $G(1) = G(2^0) = \{\overline{1}\} = \{\mathbb{Z}\}$ et $\hom(G(1), \mathbb{C}^*) = \{\sigma_0\}$ $\left(\sigma_0(\overline{1}) = 1\right)$.
- $G(2) = \{\overline{1}\} = \{1 + 2\mathbb{Z}\}$ et $\hom(G(2), \mathbb{C}^*) = \{f_0\}$ où $f_0\left(\overline{1}\right) = 1$.
- $G(3) = \{\overline{1}, \overline{2}\} = \{1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$ et $\hom(G(3), \mathbb{C}^*) = \{f_0 = \sigma^0,\ f_1 = \sigma\}$, où
  $\sigma(2 + 3\mathbb{Z}) = -1$ et donc $f_0(\overline{1}) = f_0(\overline{2}) = 1$, $f_1(\overline{1}) = 1$ et $f_1(\overline{2}) = -1$.
- $G(4) = G(2^2) = \{\overline{1}, \overline{3}\} = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$ et $\hom(G(4), \mathbb{C}^*) = \{f_0 = \sigma^0, f_1 = \sigma\}$, où
  $\sigma(3 + 4\mathbb{Z}) = -1$ et donc $f_0(\overline{1}) = f_0(\overline{3}) = 1$, $f_1(\overline{1}) = 1$ et $f_1(\overline{3}) = -1$.

Pour $k \geq 4 : k = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$, $2 \leq p_1 < \cdots < p_r$, $r \geq 1$ et les $\alpha_i \geq 1$, on peut suivre l'une des deux méthodes suivantes pour déterminer effectivement le groupe $\hom(G(k), \mathbb{C}^*)$ dual de $G(k)$.
La première méthode utilise la décomposition de $G(k)$ en produit direct de sous-groupes cycliques .
La deuxième mèthode utilise le théorème suivant:

Théorème 35 *Soit* $k = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$ $(k \geq 2)$, $2 \leq p_1 < \cdots < p_r$, $r \geq 1$ *et les* $\alpha_i \geq 1$. *On a* $\sigma \in \hom(G(k), \mathbb{C}^*)$ *si et seulement si il existe un unique* $r-$*uplet*

$$(\sigma_1, \ldots, \sigma_r) \in \prod_{i=1}^{r} \hom\left(G(p_i^{\alpha_i}), \mathbb{C}^*\right)$$

tel que $\forall \overline{n} \in G(k)$,

$$\sigma(\overline{n}) = \sigma(n + k\mathbb{Z}) = \sigma_1(n + p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times \sigma_r(n + p_r^{\alpha_r}\mathbb{Z}).$$

Démonstration. D'après le théorème des restes chinois l'application

$$u^* : G(k) \longrightarrow G(p_1^{\alpha_1}) \times \cdots \times G(p_r^{\alpha_r})$$

définie par

$$u^*(\overline{n}) = (n + p_1^{\alpha_1}, \ldots, n + p_r^{\alpha_r}), \ \forall \overline{n} \in G(k),$$

est un isomorphisme de groupes. Il existe un isomorphisme de groupes noté $\widehat{u^*}$ défini de $\prod_{i=1}^{r} \hom\left(G(p_i^{\alpha_i}), \mathbb{C}^*\right)$ dans $\hom(G(k), \mathbb{C}^*)$ par

$$(\sigma_1, \ldots, \sigma_r) \mapsto (\sigma_1 \circ \boldsymbol{p_1} \circ u^*) \cdots (\sigma_r \circ \boldsymbol{p_r} \circ u^*),$$

où $\boldsymbol{p_i}$ est la ième projection canonique définie de $G(p_1^{\alpha_1}) \times \cdots \times G(p_r^{\alpha_r})$ dans $G(p_i^{\alpha_i})$ par

$$(n_1 + p_1^{\alpha_1}, \ldots, n_r + p_r^{\alpha_r}) \mapsto n_i + p_i^{\alpha_i}\mathbb{Z}.$$

L'isomorphisme $\widehat{u^*}$ donne l'assertion annoncée. ■

Le théorème 39 réduit le calcul effectif des caractères du groupe $G(k)$ au calcul des caractères des groupes $G(p^\alpha)$, où p est un nombre premier et $\alpha \in \mathbb{N}^*$. Pour p, premier impair, le groupe $G(p^\alpha)$ est cyclique d'ordre $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, engendré par

$$x = \overline{r^{p^{\alpha-1}}(1+p)},$$

où $r + p\mathbb{Z}$ est un générateur quelconque du groupe cyclique $G(p)$.
Alors le groupe dual $\hom(G(p^\alpha), \mathbb{C}^*)$ est cyclique d'ordre $\varphi(p^\alpha)$, engendré par l'homomorphisme σ, défini par $\sigma(x) = \xi = \exp\left(i\frac{2\pi}{\varphi(p^\alpha)}\right)$, qui est la première racine primitive de l'unité. On a donc

$$\left\{ \begin{array}{l} \hom(G(p^\alpha), \mathbb{C}^*) = \{f_a = \sigma^a \ / \ a \in \{0, 1, \ldots, \varphi(p^\alpha) - 1\}\} \\ f_a = \sigma^a = \overbrace{\sigma \cdots \sigma}^{a \text{ fois}} \text{ pour } 1 \leq a \leq \varphi(p^\alpha) - 1 \text{ et } f_0 = \sigma^0 = \mathrm{I} \end{array} \right\},$$

i.e $\forall y = x^s \in G(p^\alpha)$, $\forall f_a = \sigma^a \in \hom(G(p^\alpha), \mathbb{C}^*)$

$$f_a(y) = (f_a(x))^s = (\sigma^a(x))^s = (\sigma(x))^{as} = \exp\left(i\frac{2as\pi}{\varphi(p^\alpha)}\right).$$

On remarque que l'ensemble des générateurs de $\hom(G(p^\alpha), \mathbb{C}^*)$ est

$$\{\sigma^a \ / \ 1 \leq a \leq \varphi(p^\alpha) \text{ et } (a, \varphi(p^\alpha)) = 1\}.$$

2.3.1 Détermination du groupe $\hom\left(G\left(2^{\alpha}\right),\mathbb{C}^{*}\right),\ (\alpha\geq 0)$.

Les groupes $\hom\left(G(2^0),\mathbb{C}^{*}\right)$, $\hom\left(G(2^1),\mathbb{C}^{*}\right)$ et $\hom\left(G(2^2),\mathbb{C}^{*}\right)$ sont déjà déterminés.
Pour $\alpha\geq 3$, nous avons le résultat suivant

a) Le groupe $G\left(2^{\alpha}\right)$ n'est pas cyclique.
b) Dans $G\left(2^{\alpha}\right)$, la classe de 5 est d'ordre $p^{\alpha-2}$.
c) Tout élément de $G\left(2^{\alpha}\right)$ s'écrit sous la forme $\pm\overline{5}^{k}$.
d) Les éléments de $G\left(2^{\alpha}\right)$ sont d'ordre 2^k, avec $k\leq\alpha-2$.
En d'autres termes

$$G\left(2^{\alpha}\right)=\left\langle\overline{-1}\right\rangle\odot\left\langle\overline{5}\right\rangle=\left\{\left(\overline{-1}\right)^{\nu}\left(\overline{5}\right)^{\mu}\ /\ (\nu,\mu)\in\{0,1\}\times\left\{0,1,\ldots,2^{\alpha-2}-1\right\}\right\}.$$

Alors, $\hom\left(G\left(2^{\alpha}\right),\mathbb{C}^{*}\right)=\langle\tau\rangle\odot\langle\sigma\rangle$, où

$$\tau\left(\overline{-1}\right)=\xi=-1\text{ et }\tau\left(\overline{5}\right)=1.$$

Donc $o\left(\tau\right)=o\left(\overline{-1}\right)=2$,

$$\left(\sigma\left(\overline{5}\right)=\omega=\exp\left(i\frac{2\pi}{2^{\alpha-2}}\right)=\exp\left(i\frac{\pi}{2^{\alpha-3}}\right)\text{ et }\sigma\left(\overline{-1}\right)=1\right).$$

Il vient que

$$o(\sigma)=o\left(\overline{5}\right)=2^{\alpha-2}.$$

On a donc

$$\left\{\begin{array}{c}\hom\left(G\left(2^{\alpha}\right),\mathbb{C}^{*}\right)=\left\{f_{a,b}=\tau^{a}\sigma^{b}\ /\ (a,b)\in\{0,1\}\times\left\{0,1,\ldots,2^{\alpha-2}-1\right\}\right\},\\ \text{où, }f_{a,b}\left(\overline{-1}\right)=\left(\tau^{a}\sigma^{b}\right)\left(\overline{-1}\right)=(-1)^{a}\text{ et }f_{a,b}\left(\overline{5}\right)=\left(\tau^{a}\sigma^{b}\right)\left(\overline{5}\right)=\omega^{b}\\ \left(f_{0,0}:\overline{-1}\mapsto 1\text{ et }\overline{5}\mapsto 1,\ f_{0,0}\text{ est l'élément neutre de }\hom\left(G\left(2^{\alpha}\right),\mathbb{C}^{*}\right)\right).\end{array}\right\}$$

i.e.

$$\left(\forall x=\left(\overline{-1}\right)^{\nu}\left(\overline{5}\right)^{\mu}\in G\left(2^{\alpha}\right)\right),\ \forall\tau^{a}\sigma^{b}=f_{a,b}\in\hom\left(G\left(2^{\alpha}\right),\mathbb{C}^{*}\right).$$

En conclusion

$$f_{a,b}\left(x\right)=\left(\tau^{a}\sigma^{b}\right)\left(\left(\overline{-1}\right)^{\nu}\left(\overline{5}\right)^{\mu}\right)=(-1)^{a\nu}\,\omega^{b\mu}.$$

On peut écrire aussi

$$f_{a,b}\left(x\right)=(-1)^{a\nu}\,\omega^{b\mu}=\exp\left\{i\pi a\nu+\frac{i2\pi b\mu}{s}\right\}=\exp\left\{i\pi a\nu+\frac{i\pi b\mu}{2^{\alpha-3}}\right\}.$$

Le théorème 39 et le calcul explicite des groupes $\hom\left(G\left(p^{\alpha}\right),\mathbb{C}^{*}\right)$ permettent de calculer les caractères du groupe abélien $G\left(k\right)$ pour toute valeur de k là où le

permettent les capacités des ordinateurs. Pour les petites valeurs de k, on peut faire le calcul à la main.

Dans ce qui suit, on présente les groupes $\hom(G(k),\mathbb{C}^*)$ sous forme de tableaux pour les valeurs $k=3,\ldots,10$. On remarque que les formules de dualité et d'orthogonalité sont vérifiées dans toutes les tables suivantes.

$\hom(G(3),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{2}$
f_0	1	1
f_1	1	-1

$\hom(G(4),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{3}$
f_0	1	1
f_1	1	-1

$\hom(G(5),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
f_0	1	1	1	1
f_1	1	i	$-i$	-1
f_2	1	-1	-1	1
f_3	1	$-i$	i	-1

$\hom(G(6),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{5}$
f_0	1	1
f_1	1	-1

$\hom(G(7),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
f_0	1	1	1	1	1	1
f_1	1	ω^2	ω	$-\omega$	$-\omega^2$	-1
f_2	1	$-\omega$	ω^2	ω^2	$-\omega$	1
f_3	1	1	-1	1	-1	-1
f_4	1	ω^2	$-\omega$	$-\omega$	ω^2	1
f_5	1	$-\omega$	$-\omega^2$	ω^2	ω	-1

où $\omega=\exp\left(\frac{i\pi}{3}\right)=\frac{1+i\sqrt{3}}{2},\ \omega^3+1=0$).

$\hom(G(8),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$f_{0,0}$	1	1	1	1
$f_{0,1}$	1	-1	-1	1
$f_{1,0}$	1	-1	1	-1
$f_{1,1}$	1	1	-1	-1

$\hom(G(9),\mathbb{C}^*)$:

$\overline{n}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
f_0	1	1	1	1	1	1
f_1	1	ω	ω^2	$-\omega^2$	$-\omega$	-1
f_2	1	ω^2	$-\omega$	$-\omega$	ω^2	1
f_3	1	-1	1	-1	1	-1
f_4	1	$-\omega$	ω^2	ω^2	$-\omega$	1
f_5	1	$-\omega^2$	$-\omega$	ω	ω^2	-1

où,

$$\omega = \exp\left(\frac{i\pi}{3}\right) = \frac{1+i\sqrt{3}}{2},\ \omega^3+1=0.$$

Pour le groupe $\hom\left(G\left(10\right),\mathbb{C}^*\right)$,
on a

$$h \in \hom\left(G\left(10\right),\mathbb{C}^*\right) \text{ si et seulement si } h = fg,$$

où $f \in \hom\left(G\left(2\right),\mathbb{C}^*\right)$ et $g \in \hom\left(G\left(5\right),\mathbb{C}^*\right)$ telles que

$$h\left(n+10\mathbb{Z}\right) = f\left(n+10\mathbb{Z}\right)g\left(n+10\mathbb{Z}\right),\ \ (n,10)=1.$$

Puisque $f\left(n+10\mathbb{Z}\right)=1$ alors $h\left(n+10\mathbb{Z}\right)=g\left(n+10\mathbb{Z}\right)$, $(n,10)=1$.

$\hom\left(G\left(10\right),\mathbb{C}^*\right)$:

$\overline{n}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
f_0	1	1	1	1
f_1	1	$-i$	i	-1
f_2	1	-1	-1	1
f_3	1	i	$-i$	-1

2.4 les caractères de Dirichlet modulo $k \in \mathbb{N}^*$

une fonction arithmétique $g:\mathbb{Z}\to\mathbb{C}$ est dite complètement multiplicative si elle vérifie

$$g(1)=1 \ \ et \ \ g(nm)=g(n)g(m),\ \forall n,m\in\mathbb{Z}.$$

Soit l'application $\chi:\mathbb{Z}\to\mathbb{C}^*$. Soit k un entier positif. Les deux assertions suivantes sont équivanlentes:

Proposition 36 *1. L'application χ est nulle sur les nombres entiers non premiers avec k, elle est complètement multiplicative et vérifie $\chi\left(n+Nk\right)=\chi(n)$, $\forall n,N\in\mathbb{Z}$.*

2. Il existe un unique $f\in\hom\left(G\left(k\right),\mathbb{C}^*\right)$ tel que $\forall n\in\mathbb{Z}$,

$$\chi(n)=\left\{\begin{array}{c} f\left(\overline{n}\right)\ si\ (n,k)=1 \\ 0\ sinon \end{array}\right\}.$$

On dit alors que χ est associée à f et f est associée à χ. L'ensemble des caractères modulo k est noté $\widehat{G}\left(k\right)$.

Démonstration. .

$\left(\mathbf{a}\right)\Rightarrow\left(\mathbf{b}\right)$: On considère la correspondance f définie de $G(k)$ dans $\mathbb{C}^*$ par $\overline{n}\mapsto\overline{\chi(n)\ (\overline{n}\in G\left(k\right)\Leftrightarrow(n,k)=1)}$.

On vérifie que f est une application.
Soient $\overline{n}=\overline{m}$ dans $G(k)$. On a donc $n=m+Nk$, où $N\in\mathbb{Z}$.
D'après la troisième condition de χ, $\chi(n)=\chi(m)$, d'où $f\left(\overline{n}\right)=f\left(\overline{m}\right)$.

Comme χ est complètement multiplicative, alors $f(\overline{nm}) = f(\overline{n})\, f(\overline{m})$, $\forall \overline{n}, \overline{m} \in G(k)$. Donc $f \in \hom(G(k), \mathbb{C}^*)$. Enfin, la définition de f et la première condition de χ impliquent

$$\chi(n) = \left\{ \begin{array}{c} f(\overline{n}) \text{ si } (n,k) = 1,\ \bar{n} \in G(k) \\ 0 \text{ si } (n,k) \neq 1 \end{array} \right\},\ \forall n \in \mathbb{Z}.$$

$\underline{(\mathbf{b}) \Rightarrow (\mathbf{a}) :}$ Par définition $\chi(n) = 0$, $\forall n \in \mathbb{Z}$, $(n,k) \neq 1$.
Montrons que χ est complètement multiplicative.

Soit n, $m \in \mathbb{Z}$. On a deux cas :
si $(n,k) = (m,k) = 1$, alors

$$\chi(nm) = f(\overline{nm}) = f(\overline{nm}) = f(\overline{n})\, f(\overline{m}) = \chi(n)\, \chi(m)$$

et

si $(n,k) \neq 1$ ou $(m,k) \neq 1$, alors $(nm,k) \neq 1$ et donc

$$\chi(nm) = \chi(n)\, \chi(m) = 0.$$

Pour vérifier la troisième condition : soit $n \in \mathbb{Z}$. On a deux cas :
si $(n,k) = 1$, alors $\forall N \in \mathbb{Z}$, on a $(n + Nk, k) = 1$.
Comme $\overline{n} = \overline{n + Nk}$ dans $G(k)$ alors $f(\overline{n}) = f\left(\overline{n + Nk}\right)$. Ce qui est équivalent à $\chi(n) = \chi(n + Nk)$.
Si $(n,k) \neq 1$ alors, $\forall N \in \mathbb{Z}$, $(n + Nk, k) \neq 1$, donc $\chi(n) = \chi(n + Nk) = 0$. ■

Conséquence :
$\forall \chi \in \widehat{G}(k)$, $\forall n \in \mathbb{Z}$, $(n,k) = 1$, le nombre complexe $\chi(n)$ est une racine $(\varphi(k))^{\text{ième}}$ de l'unité dans $\mathbb{C}$, $|\chi(n)| = 1$ et $\chi(1) = 1$.
En effet, par définition, il existe $f \in \hom(G(k), \mathbb{C}^*)$ telle que

$$\chi(n) = \left\{ \begin{array}{c} f(\overline{n}) \text{ si } (n,k) = 1,\ \bar{n} \in G(k) \\ 0 \text{ si } (n,k) \neq 1 \end{array} \right\}.$$

Sachant que $|G(k)| = \varphi(k)$, alors si $(n,k) = 1$ $(\Leftrightarrow \overline{n} \in G(k))$, on aura

$$(\overline{n})^{\varphi(k)} = \overline{1} \text{ et } (\chi(n))^{\varphi(k)} = (f(\overline{n}))^{\varphi(k)} = f\left((\overline{n})^{\varphi(k)}\right) = f\left(\overline{1}\right) = 1.$$

L'égalité $(\chi(n))^{\varphi(k)} = 1$ implique

$$\left|(\chi(n))^{\varphi(k)}\right| = |(\chi(n))|^{\varphi(k)} = 1,$$

d'où $|(\chi(n))| = 1$.
Il est bien clair que $\chi(1) = f(\overline{1}) = 1$.

Soit $k \in \mathbb{N}^*$. Une fonction arithmétique χ définie de $\mathbb{Z}$ dans $\mathbb{C}$ est appelée caractère modulo k ou caractère de Dirichlet si elle vérifie l'une des deux assertions équivalentes dans la proposition 41.

Comme il existe un entier positif k tel que $\chi(n) = \chi(n+k)$ pour tous les n, on peut dire que le caractère est périodique de période k.

Un exemple de caractère de Dirichlet est la fonction $\chi(n) = (-1)^{\frac{n-1}{2}}$ pour les entiers impairs et $\chi(n) = 0$ pour les entiers pairs. Ce caractère est de période 4.

Si p est un nombre premier, alors la fonction $\chi(n) = \left(\frac{n}{p}\right)$ (le symbole de Legendre) est un caractère de Dirichlet de période p.

La fonction arithmétique χ_0 définie par

$$\begin{cases} \chi_0(n) = 1 \text{ si } (n,k) = 1 \\ \chi_0(n) = 0 \text{ si } (n,k) \neq 1 \end{cases}$$

est appelée caractère principal modulo k.

Pour $k = 1$, on a $\chi_0(n) = 1$, pour tout $n \in \mathbb{Z}$. De plus χ_0 est associé à f_0. L'élément neutre de $\hom\left(G\left(k\right), \mathbb{C}^*\right)$ est défini par $f_0\left(\overline{n}\right) = 1$, $\forall \overline{n} \in G\left(k\right)$.

Définition 37 (Caractère conjugué) *Pour tout $\chi \in \widehat{G}\left(k\right)$, la fonction arithmétique $\overline{\chi}$ définie de $\mathbb{Z}$ dans $\mathbb{C}$ par*

$$\overline{\chi}\left(n\right) = \overline{\chi(n)},$$

où, $\overline{\chi(n)}$ est le nombre complexe conjugué de $\chi(n)$, est un caractère modulo k appelé le caractère conjugué de χ.

Pour tout $n \in \mathbb{Z}$, $(n,k) = 1$, on a

$$\chi(n)\overline{\chi}\left(n\right) = \chi(n)\overline{\chi(n)} = |\chi(n)|^2 = 1.$$

De plus, si $f \in \hom\left(G(k), \mathbb{C}^*\right)$ est associée à χ et $g \in \hom\left(G(k), \mathbb{C}^*\right)$ est associée à $\overline{\chi}$, alors $g = \overline{f}$.

Définition 38 *Un caractère χ est dit réel si $\chi = \overline{\chi}$.*

Définition 39 (Caractère pair et impair) *Un caractère χ est dit pair (respectivement impair) si $\chi(-1) = 1$ (respectivement $\chi(-1) = -1$).*

2.4.1 Le groupe $\widehat{G}\left(k\right)$ des caractères modulo k

La loi de composition interne $\left(\chi_1\chi_2\right)\left(n\right) = \chi_1\left(n\right)\chi_2\left(n\right)$ munit l'ensemble $\widehat{G}\left(k\right)$ d'une structure de groupe abélien appelé le groupe des caractères modulo k. L'élément neutre du groupe $\widehat{G}\left(k\right)$ est χ_0 et pour tout $\chi \in \widehat{G}\left(k\right)$, le symétrique de χ est $\overline{\chi}$ car

$$\left(\chi\overline{\chi}\right)\left(n\right) = \chi(n)\overline{\chi(n)} = \left\{ \begin{array}{c} 1 \text{ si } (n,k) = 1 \\ 0 \text{ sinon} \end{array} \right\} := \chi_0(n).$$

Théorème 40 *On a*

1. *L'application* $u : \hom\left(G\left(k\right), \mathbb{C}^*\right) \longrightarrow \widehat{G}\left(k\right)$ *définie par* $f \mapsto u\left(f\right) : \mathbb{Z} \to \mathbb{C}$ *avec*
$$\left(u\left(f\right)\right)\left(n\right) = \left\{ \begin{array}{c} f\left(\overline{n}\right) \ \ si \ \ \left(n,k\right) = 1 \ \ \left(\overline{n} \in G\left(k\right)\right) \\ 0 \ sinon. \end{array} \right\}$$
est un isomorphisme de groupes.

2. *Les trois groupes* $G(k)$, $\widehat{G}(k)$ *et* $\hom\left(G\left(k\right), \mathbb{C}^*\right)$ *sont isomorphes d'ordre* $\varphi\left(k\right)$.

Théorème 41 *Pour tout* $k \in \mathbb{N}^*$, *on a les formules suivantes :*

$$S(n) = \sum_{\chi \in \widehat{G}(k)} \chi(n) = \left\{ \begin{array}{c} \varphi\left(k\right) \ \ si \ n \equiv 1 \left(mod \ k\right) \\ 0 \ sinon \end{array} \right\}, \ \forall n \in \mathbb{Z}.$$

$$S(\chi) = \sum_{n=1}^{k} \chi(n) = \left\{ \begin{array}{c} \varphi\left(k\right) \ \ si \ \chi = \chi_0 \\ 0 \ si \ \chi \neq \chi_0 \end{array} \right\}.$$

$$\begin{aligned} S(n,m) &= \sum_{\chi \in \widehat{G}(k)} \chi(n)\overline{\chi}\left(m\right) \\ &= \left\{ \begin{array}{c} \varphi\left(k\right) \ \ si \ \ \left(nm,k\right) = 1 \ et \ n \equiv m \left(mod \ k\right) \\ 0 \ sinon \end{array} \right\}, \ \forall n, m \in \mathbb{Z}. \end{aligned}$$

$$S(\chi_1, \chi_2) = \sum_{n=1}^{k} \chi_1(n)\chi_2\left(n\right) = \left\{ \begin{array}{c} \varphi\left(k\right) \ \ si \ \chi_2 = \overline{\chi_1} \\ 0 \ sinon \end{array} \right\}.$$

Théorème 42 *Soit* $k \in \mathbb{N}^*$, $k = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$, *où* $r \geq 1$, $2 \leq p_1 < \cdots < p_r$ *et les* $\alpha_i \geq 1$. *On a* $\chi \in \widehat{G}\left(k\right)$, *si et seulement si, il existe un* $r-$*uplet unique*

$$\left(\chi_1, \ldots, \chi_r\right) \in \widehat{G}\left(p_1^{\alpha_1}\right) \times \cdots \times \widehat{G}\left(p_r^{\alpha_r}\right),$$

tel que pour tout $n \in \mathbb{Z}$, $(n,k) = 1$, *on a*

$$\chi\left(n\right) = \chi_1\left(n\right) \times \cdots \times \chi_r\left(n\right).$$

Démonstration. On a $f \in \hom\left(G(k), \mathbb{C}^*\right)$, si et seulement si, il existe un unique $r-$uplet $\left(f_1, \ldots, f_r\right) \in \prod_{i=1}^{r} \hom\left(G(p_i^{\alpha_i}), \mathbb{C}^*\right)$ tel que, $\forall \overline{n} \in G(k)$, on a

$$f\left(\overline{n}\right) = f\left(n + k\mathbb{Z}\right) = f_1\left(n + p_1^{\alpha_1}\mathbb{Z}\right) \times \cdots \times f_r\left(n + p_r^{\alpha_r}\mathbb{Z}\right).$$

Soit $\chi \in \widehat{G}(k)$ et $f \in \hom(G(k), \mathbb{C}^*)$ son homomorphisme associé. On a alors, pour tout $n \in \mathbb{Z}$, $(n,k)=1$,

$$\chi(n) = f(n+k\mathbb{Z}) = f_1\left(n+p_1^{\alpha_1}\mathbb{Z}\right) \times \cdots \times f_r\left(n+p_r^{\alpha_r}\mathbb{Z}\right).$$

Si, pour chaque $i=1,\ldots,r$, on note par $\chi_i \in \widehat{G}\left(p_i^{\alpha_i}\right)$ le caractère associé à $f_i \in \hom\left(G(p_i^{\alpha_i}), \mathbb{C}^*\right)$, on aura

$$\chi(n) = \chi_1(n) \times \cdots \times \chi_r(n),$$

d'où l'assertion annoncée. ■

Le théorème 50 réduit la détermination des caractères modulo k, $k \geq 2$, à celui des caractères modulo p^α, où p est un nombre premier et $\alpha \geq 1$.

2.4.2 Détermination du groupe $\widehat{G}(k)$ des caractères modulo k, $k = 2, \cdots, 15$.

Les caractères modulo k, $k=1$, 2, 3, 4.

On a $\widehat{G}(1) = \{\chi_0\}$ où $\chi_0(n) = 1$, $\forall n \in \mathbb{Z}$.

Les caractères modulo $k=2$.

On a $\widehat{G}(2) = \{\chi_0\}$ où $\chi_0(n) = \left\{ \begin{array}{c} 1 \text{ si } (n,2)=1 \\ 0 \text{ sinon} \end{array} \right\}$.

Les caractères modulo $k = 2^{\mathbf{2}} = 4$.

On a $\widehat{G}(4) = \{\chi_0, \chi_1\}$, où χ_0 et χ_1 sont définis comme suit

$$\chi_0(n) = \left\{ \begin{array}{c} 1 \text{ si } n \equiv 1,3 \pmod 4 \\ 0 \text{ si } n \text{ est pair} \end{array} \right\}, \ \chi_1(n) = \left\{ \begin{array}{c} 1 \text{ si } n \equiv 1 \pmod 4 \\ -1 \text{ si } n \equiv 3 \pmod 4 \\ 0 \text{ si } n \text{ est pair} \end{array} \right\}.$$

Les caractères modulo k, $k = 2^{\boldsymbol{\alpha}}$ **avec** $\alpha \geq 3$.

On rappelle que $G(2^\alpha) = \left\langle \overline{-1} \right\rangle \odot \left\langle \overline{5} \right\rangle$.

Comme $\chi \in \widehat{G}(2^\alpha)$, si et seulement si, il existe un unique élément $f_{a,b} \in \hom\left(G(2^\alpha), \mathbb{C}^*\right)$ tel que

$$\chi(n) = \left\{ \begin{array}{c} f_{a,b}(\bar{n}) \text{ si } (n,2)=1 \\ 0 \text{ sinon} \end{array} \right\},$$

alors, la description du groupe $\hom\left(G(2^\alpha), \mathbb{C}^*\right)$ permet d'obtenir la structure du groupe $\widehat{G}(2^\alpha)$.

On a

$$\widehat{G}(2^\alpha) = \left\{ \chi_{a,b} \ / \ a \in \{0,1\} \times \left\{0,1,\ldots,2^{\alpha-2}-1\right\} \right\}$$

où, pour tout couple $(a,b) \in \{0,1\} \times \{0,1,\ldots,2^{\alpha-2}-1\}$, le caractère $\chi_{a,b}$ est défini de $\mathbb{Z}$ dans $\mathbb{C}$ par :

$$\chi_{a,b}(-1) = (-1)^a,$$

$$\chi_{a,b}(5)=\omega^b=\exp\left(i\frac{\pi b}{2^{\alpha-3}}\right)\left(\omega=\exp\left(i\frac{\pi}{2^{\alpha-3}}\right)\right)$$

et pour tout nombre entier n, on a

$$\chi_{a,b}(n)=\left\{\begin{array}{c}(-1)^{\nu a}\omega^{\mu b}=\exp\left(i\left(\pi\nu a+\frac{\pi\mu b}{2^{\alpha-3}}\right)\right)\text{ si }n\equiv(-1)^{\nu}5^{\mu}\pmod{2^{\alpha}}\\ 0\text{ si }n\text{ est pair}\end{array}\right\}.$$

On précise que $\widehat{G}(2^{\alpha})=\langle\chi_{1,0}\rangle\odot\langle\chi_{0,1}\rangle$, où

$$\left\{\begin{array}{c}\left(\chi_{1,0}(-1)=-1,\ \chi_{1,0}(5)=1\right)\text{ et }\left(\chi_{0,1}(-1)=1,\ \chi_{0,1}(5)=\omega\right),\\ \omega=\exp\left(i\frac{\pi}{2^{\alpha-3}}\right),\ o\left(\chi_{1,0}\right)=2\text{ et }o\left(\chi_{0,1}\right)=2^{\alpha-2}.\end{array}\right\}$$

Les caractères modulo k, $k=p^{\alpha}$ avec $\alpha\geq 1$, p impair.

Soient $r+p\mathbb{Z}$ un générateur du groupe $G(p)$ et $\overline{s}=\overline{(p+1)\,r^{p^{\alpha-1}}}$, le générateur du groupe cyclique $G(p^{\alpha})$ associé à $r+p\mathbb{Z}$

$$G(p^{\alpha})=\left\{\overline{1},\overline{s},\ldots,\overline{s}^{\varphi(p^{\alpha})-1}\right\},\ \left(\varphi(p^{\alpha})=p^{\alpha-1}(p-1)\right).$$

La description du groupe $\hom(G(p^{\alpha}),\mathbb{C}^*)$ permet de décrire le groupe $\widehat{G}(p^{\alpha})$.

On a

$$\widehat{G}(p^{\alpha})=\left\{\chi_0,\chi_1,\ldots,\chi_{\varphi(p^{\alpha})-1}\right\}=\langle\chi_1\rangle,\ o(\chi_1)=\varphi(p^{\alpha}),$$

où, pour tout $a\in\{0,1,\ldots,m-1\}$, le carctère χ_a est défini de $\mathbb{Z}$ dans $\mathbb{C}$ par

$$\chi_a(s)=\omega^a=\exp\left(i\frac{2a\pi}{p^{\alpha-1}(p-1)}\right),\ \omega=\exp\left(i\frac{2\pi}{\varphi(p^{\alpha})}\right)$$

et pour tout nombre entier n, on a

$$\chi_a(n)=\left\{\begin{array}{c}\omega^{a\nu}=\exp\left(i\frac{2a\nu\pi}{p^{\alpha-1}(p-1)}\right)\text{ si }\overline{n}=\overline{s}^{\nu}\in G(p^{\alpha})\\ 0\text{ sinon}\end{array}\right\}.$$

On remarque que χ_a est un générateur de $\widehat{G}(p^{\alpha})$ si et seulement si $1\leq a\leq\varphi(p^{\alpha})$ et $(a,\varphi(p^{\alpha}))=1$

On trouve ci-dessous les groupes des caractères modulo $k=2,\cdots,15$ présentés sous forme de tableaux qui diffèrent légèrement des tableaux des groupes $\hom(G(k),\mathbb{C}^*)$. Dans ces tables, les formules du théorème 49 sont toutes vérifiées.

$k=2$:

n	1	2
χ_0	1	0

, $k=3$:

n	1	2	3
χ_0	1	1	0
χ_1	1	-1	0

, $k=4$:

n	1	2	3	4
$\chi_0(n)$	1	0	1	0
$\chi_1(n)$	1	0	-1	0

$k=5:$

n	1	2	3	4	5
χ_0	1	1	1	1	0
χ_1	1	i	$-i$	-1	0
χ_2	1	-1	-1	1	0
χ_3	1	$-i$	i	-1	0

, $k=6:$

n	1	2	3	4	5	6
χ_0	1	0	0	0	1	0
χ_1	1	0	0	0	-1	0

$k=7:$

n	1	2	3	4	5	6	7
χ_0	1	1	1	1	1	1	0
χ_1	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
χ_2	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
χ_3	1	1	-1	1	-1	-1	0
χ_4	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
χ_5	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

, $\omega=\exp\left(\frac{i\pi}{3}\right)=\frac{1+i\sqrt{3}}{2}$, $\omega^3+1=0$.

$k=8:$

n	1	2	3	4	5	6	7	8
χ_0	1	0	1	0	1	0	1	0
χ_1	1	0	-1	0	-1	0	1	0
χ_2	1	0	-1	0	1	0	-1	0
χ_3	1	0	1	0	-1	0	-1	0

.

Pour $k=8$, le caractère réel χ_2 est de période fondamentale : $=4$.

$k = 9:$

n	1	2	3	4	5	6	7	8	9
χ_0	1	1	0	1	1	0	1	1	0
χ_1	1	ω	0	ω^2	$-\omega^2$	0	$-\omega$	-1	0
χ_2	1	ω^2	0	$-\omega$	$-\omega$	0	ω^2	1	0
χ_3	1	-1	0	1	-1	0	1	-1	0
χ_4	1	$-\omega$	0	ω^2	ω^2	0	$-\omega$	1	0
χ_5	1	$-\omega^2$	0	$-\omega$	ω	0	ω^2	-1	0

$\omega = \exp\left(\frac{i\pi}{3}\right)=\frac{1+i\sqrt{3}}{2}$, $\omega^3+1=0$.

Pour $k=9$, le caractère réel χ_3 est de période fondamentale : $=3$.

$k = 10:$

n	1	2	3	4	5	6	7	8	9	10
χ_0	1	0	1	0	0	0	1	0	1	0
χ_1	1	0	i	0	0	0	$-i$	0	-1	0
χ_2	1	0	-1	0	0	0	-1	0	1	0
χ_3	1	0	$-i$	0	0	0	i	0	-1	0

Les caractères $\chi_1,\ \chi_2,\ \chi_3$ sont de période fondamentale : $=10$.

$k = 11$:

n	1	2	3	4	5	6	7	8	9	10	11
χ_0	1	1	1	1	1	1	1	1	1	1	0
χ_1	1	ω	$-\omega^3$	ω^2	ω^4	$-\omega^4$	$-\omega^2$	ω^3	$-\omega$	-1	0
χ_2	1	ω^2	$-\omega$	ω^4	$-\omega^3$	$-\omega^3$	ω^4	$-\omega$	ω^2	1	0
χ_3	1	ω^3	ω^4	$-\omega$	ω^2	$-\omega^2$	ω	$-\omega^4$	$-\omega^3$	-1	0
χ_4	1	ω^4	ω^2	$-\omega^3$	$-\omega$	$-\omega$	$-\omega^3$	ω^2	ω^4	1	0
χ_5	1	-1	1	1	1	-1	-1	-1	1	-1	0
χ_6	1	$-\omega$	$-\omega^3$	ω^2	ω^4	ω^4	ω^2	$-\omega^3$	$-\omega$	1	0
χ_7	1	$-\omega^2$	$-\omega$	ω^4	$-\omega^3$	ω^3	$-\omega^4$	ω	ω^2	-1	0
χ_8	1	$-\omega^3$	ω^4	$-\omega$	ω^2	ω^2	$-\omega$	ω^4	$-\omega^3$	1	0
χ_9	1	$-\omega^4$	ω^2	$-\omega^3$	$-\omega$	ω	ω^3	$-\omega^2$	ω^4	-1	0

$\omega = \exp\left(i\frac{\pi}{5}\right),\ \omega^5 + 1 = 0.$

Remarque 43 *La dernière égalité implique*

$$\omega^4 - \omega^3 + \omega^2 - \omega + 1 = 0,$$

donc

$$\left(\omega - \omega^4\right)^2 - \left(\omega - \omega^4\right) - 1 = 0,$$

alors

$$\omega - \omega^4 = 2\cos\left(\frac{\pi}{5}\right) = \frac{\sqrt{5}+1}{2}.$$

On en déduit alors les expressions algébriques de ω, ω^2, ω^3, ω^4 :

$$\omega = a + ib,\ \omega^2 = \frac{1}{4a} + i\frac{\sqrt{5}}{4b},\ \omega^3 = -\frac{1}{4a} + i\frac{\sqrt{5}}{4b}\ \textit{et}\ \omega^4 = -a + ib,$$

où

$$a = \frac{\sqrt{5}+1}{4},\ b = \frac{\sqrt{10-2\sqrt{5}}}{4}$$

$k = 12$:

n	1	2	3	4	5	6	7	8	9	10	11	12
χ_0	1	0	0	0	1	0	1	0	0	0	1	0
χ_1	1	0	0	0	1	0	-1	0	0	0	-1	0
χ_2	1	0	0	0	-1	0	1	0	0	0	-1	0
χ_3	1	0	0	0	-1	0	-1	0	0	0	1	0

.

Le caractère χ_2 modulo 12 est de période fondamentale : $= 6$.

$k = 13:$

n	1	2	3	4	5	6	7	8	9	10	11	12	13
χ_0	1	1	1	1	1	1	1	1	1	1	1	1	0
χ_1	1	ω	ω^4	$-\omega^4$	ω^3	$-\omega$	ω^5	$-\omega^3$	$-\omega^2$	ω^2	$-\omega^5$	-1	0
χ_2	1	ω^2	$-\omega^2$	$-\omega^2$	-1	ω^2	$-\omega^4$	-1	ω^4	ω^4	$-\omega^4$	1	0
χ_3	1	ω^3	1	-1	$-\omega^3$	$-\omega^3$	ω^3	ω^3	1	-1	$-\omega^3$	-1	0
χ_4	1	ω^4	ω^4	ω^4	1	ω^4	$-\omega^2$	1	ω^2	$-\omega^2$	$-\omega^2$	1	0
χ_5	1	ω^5	$-\omega^2$	ω^2	ω^3	$-\omega^5$	ω	$-\omega^3$	$-\omega^4$	$-\omega^4$	$-\omega$	-1	0
χ_6	1	-1	1	1	-1	-1	-1	-1	-1	1	-1	1	0
χ_7	1	$-\omega$	ω^4	$-\omega^4$	$-\omega^3$	ω	$-\omega^5$	ω^3	ω^2	ω^2	ω^5	-1	0
χ_8	1	$-\omega^2$	$-\omega^2$	$-\omega^2$	1	$-\omega^2$	ω^4	1	$-\omega^4$	ω^4	ω^4	1	0
χ_9	1	$-\omega^3$	1	1	ω^3	ω^3	$-\omega^3$	$-\omega^3$	-1	-1	ω^3	-1	0
χ_{10}	1	$-\omega^4$	ω^4	$-\omega^4$	-1	$-\omega^4$	ω^2	-1	ω^2	$-\omega^2$	ω^2	1	0
χ_{11}	1	$-\omega^5$	$-\omega^2$	$-\omega^2$	$-\omega^3$	ω^5	$-\omega$	ω^3	$-\omega^4$	$-\omega^4$	ω	-1	0
χ_{12}	1	1	1	-1	1	1	1	1	-1	1	1	1	0

$$\omega = \exp\left(\frac{i\pi}{6}\right) = \frac{\sqrt{3}+i}{2},\ \omega^6+1=0.$$

$k = 14:$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
χ_0	1	0	1	0	1	0	0	0	1	0	1	0	1	0
χ_1	1	0	ω	0	$-\omega^2$	0	0	0	ω^2	0	$-\omega$	0	1	0
χ_2	1	0	ω^2	0	$-\omega$	0	0	0	$-\omega$	0	ω^2	0	1	0
χ_3	1	0	-1	0	-1	0	0	0	1	0	1	0	1	0
χ_4	1	0	$-\omega$	0	ω^2	0	0	0	ω^2	0	$-\omega$	0	1	0
χ_4	1	0	$-\omega^2$	0	ω	0	0	0	$-\omega$	0	ω^2	0	1	0

$$\omega = \exp\left(\frac{i\pi}{3}\right) = \frac{1+i\sqrt{3}}{2},\ \omega^3+1=0.$$

$k = 15:$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
χ_0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0
χ_1	1	i	0	-1	0	0	i	$-i$	0	0	1	0	$-i$	-1	0
χ_2	1	-1	0	1	0	0	-1	-1	0	0	1	0	-1	1	0
χ_3	1	$-i$	0	-1	0	0	$-i$	i	0	0	1	0	i	-1	0
χ_4	1	-1	0	1	0	0	1	-1	0	0	-1	0	1	-1	0
χ_5	1	$-i$	0	-1	0	0	i	i	0	0	-1	0	$-i$	1	0
χ_6	1	1	0	1	0	0	-1	1	0	0	-1	0	-1	-1	0
χ_7	1	i	0	-1	0	0	$-i$	$-i$	0	0	-1	0	i	1	0

Remarque 44 *Pour $k = 60 = 2^2 \times 3 \times 5$, on pose*

$$\begin{aligned}\widehat{G}(4) &= \left\{\chi_0^{(4)}, \chi_1^{(4)}\right\},\\ \widehat{G}(3) &= \left\{\chi_0^{(3)}, \chi_1^{(3)}\right\},\\ \widehat{G}(5) &= \left\{\chi_0^{(5)}, \chi_1^{(5)}, \chi_2^{(5)}, \chi_3^{(5)}\right\}.\end{aligned}$$

Alors

$$\begin{aligned}\widehat{G}(60) = &\left\{\chi_0^{(4)}\chi_0^{(3)}\chi_i^{(5)}\right\}_{i=0,1,2,3} \bigcup \left\{\chi_0^{(4)}\chi_1^{(3)}\chi_i^{(5)}\right\}_{i=0,1,2,3}\\ &\bigcup \left\{\chi_1^{(4)}\chi_0^{(3)}\chi_i^{(5)}\right\}_{i=0,1,2,3} \bigcup \left\{\chi_1^{(4)}\chi_1^{(3)}\chi_i^{(5)}\right\}_{i=0,1,2,3}.\end{aligned}$$

2.5 Caractères équivalents

Lemme 45 *Soient k, n, d trois nombres entiers tous non nuls tels que $(n, d) = 1$. On pose*

$$q = \prod_{p|k \ \text{et}\ p\nmid n} p,$$

le produit de tous les facteurs premiers de k qui ne divisent pas n. On pose $m = n + qd$. Donc $m \equiv n \pmod{d}$ et on a $(m, k) = 1$.

Définition 46 *Soient $k, k' \in \mathbb{N}^*$.*
Deux caractères $\chi \in \widehat{G}(k)$ et $\chi' \in \widehat{G}(k')$ sont dits équivalents s'ils vérifient $(n \in \mathbb{Z}$ et $(n, kk') = 1) \Rightarrow \chi(n) = \chi'(n)$. On écrit alors $\chi \sim \chi'$.

Propriétés:

1. Soit $k \in \mathbb{N}^*$. Tout caractère modulo k est équivalent à lui même : $\forall \chi \in \widehat{G}(k)$, $\chi \sim \chi$.

2. Soient $1 \leq k_1 \mid k_2 \mid k_3$ dans $\mathbb{N}^*$, $\chi_1 \in \widehat{G}(k_1)$, $\chi_2 \in \widehat{G}(k_2)$ et $\chi_3 \in \widehat{G}(k_3)$. On a alors
$$(\chi_1 \sim \chi_2 \text{ et } \chi_2 \sim \chi_3) \Rightarrow \chi_1 \sim \chi_3.$$

   En effet, soit $n \in \mathbb{Z}$. On suppose $(n, k_1k_3) = 1$. On a donc $(n, k_3) = 1$. Comme $k_1 \mid k_2 \mid k_3$, alors $(n, k_1k_2) = 1$, par suite $\chi_1(n) = \chi_2(n)$.
   On a aussi $(n, k_2) = (n, k_3) = 1$ donc $(n, k_2k_3) = 1$, d'où, $\chi_3(n) = \chi_2(n)$.
   D'où $\chi_1(n) = \chi_3(n)$.

3. Quel que soit d un diviseur de k, on a $\chi_0^{(k)} \sim \chi_0^{(d)} \sim \chi_0^{(1)}$, $\chi_0^{(1)}$ étant le caractère principal et unique modulo 1.

4. Quel que soit d un diviseur de k et $\forall \chi \in \widehat{G}(k)$, si χ est équivalent à un caractère $\chi^{(d)} \in \widehat{G}(d)$, alors $\chi^{(d)}$ est unique. C'est à dire que l'implication suivante a lieu

$$\left(\chi \sim \chi_1 \in \widehat{G}(d) \text{ et } \chi \sim \chi_2 \in \widehat{G}(d)\right) \Rightarrow \chi_1 = \chi_2.$$

En effet,
soit $n \in \mathbb{Z}$. On a deux cas à étudier $(n,d) \neq 1$ et $(n,d) = 1$.
Dans le premier cas, on a $\chi_1(n) = \chi_2(n) = 0$.
Dans le deuxième cas, on considère le nombre $n + qd$ où, $q = \prod_{p|k \text{ et } p\nmid n} p$. On sait que $(n+qd, k) = 1$ et comme $(\chi \sim \chi_1 \text{ et } \chi \sim \chi_2)$, alors

$$\left\{ \begin{array}{l} \chi(n+qd) = \chi_1(n+qd) = \chi_1(n) \\ \chi(n+qd) = \chi_2(n+qd) = \chi_2(n) \end{array} \right\}.$$

Ce qui implique

$$\chi_1(n) = \chi_2(n).$$

Remarque 47 *Pour $k = 15$, on a vu que*

$$\chi \in \widehat{G}(15) \Leftrightarrow \chi = \chi_i^{(3)} \chi_j^{(5)},$$

où

$$\chi_i^{(3)} \in \widehat{G}(3)$$

et

$$\chi_j^{(5)} \in \widehat{G}(5).$$

De ce fait, on a :

$$\chi_0 \sim \chi_0^{(3)} \sim \chi_0^{(1)},$$

$$\chi_0 \sim \chi_0^{(5)} \sim \chi_0^{(1)},$$

$$\begin{aligned} \chi_1 = \chi_0^{(3)} \chi_1^{(5)} &\sim \chi_1^{(5)}, \\ \chi_2 = \chi_0^{(3)} \chi_2^{(5)} &\sim \chi_2^{(5)}, \\ \chi_3 = \chi_0^{(3)} \chi_3^{(5)} &\sim \chi_3^{(5)}, \end{aligned}$$

et

$$\chi_4 = \chi_1^{(3)} \chi_0^{(5)} \sim \chi_1^{(3)}.$$

(Voir les tables de $\widehat{G}(3)$, $\widehat{G}(5)$, $\widehat{G}(15)$).

2.6 Conducteur d'un caractère

Lemme 48 *Soient $k \in \mathbb{N}^*$ et $\chi \in \widehat{G}(k)$. Pour tout diviseur d de k, les trois assertions suivantes sont équivalentes.*

1. $(\forall n \in \mathbb{Z})$, *on a* $[(n,k)=1$ *et* $n \equiv 1 \,(mod\ d)] \Rightarrow \chi(n)=1$.
2. $(\forall n,m \in \mathbb{Z})$, *on a* $[(n,k)=(m,k)=1$ *et* $n \equiv m \,(mod\ d)] \Rightarrow \chi(n)=\chi(m)$.
3. *Le groupe* $\widehat{G}(d)$ *contient un caractère* χ^* *équivalent à* χ *(on a vu que* χ^* *est unique).*

Définition 49 *Le plus petit diviseur d de k vérifiant l'une des trois assertions est appelé conducteur du caractère χ et il est noté par f_χ.*

Donc f_χ est le plus petit diviseur d de k tel que $\widehat{G}(d)$ contient un caractère χ^* équivalent à χ.

Lemme 50 (Détermination effective du conducteur d'un caractère) *Soient $k \in \mathbb{N}^*$ et $\chi \in \widehat{G}(k)$.*
Pour tout diviseur d de k, on pose $H(d,k) := H = \{\overline{n} \in G(k) \ / \ n \equiv 1 \,(mod\ d)\}$.
Le sous-ensemble H est un sous-groupe de $G(k)$.

Démonstration. On a $\overline{1} \in H$ car $1 \equiv 1 \,(\text{mod } d)$.
Soit $\overline{n}$, $\overline{m} \in H$. On a alors $(n,k)=(m,k)=1$, donc $(nm,k)=1$, $n \equiv 1 \,(\text{mod } d)$ et $m \equiv 1 \,(\text{mod } d)$. Par conséquent $nm \equiv 1 \,(\text{mod } d)$.
Par suite $\overline{nm} \in G(k)$. Soit $\overline{n} \in H$ et $\overline{m}$ le symétrique de $\overline{n}$ dans $G(k)$. On a $\overline{nm} = \overline{1}$ modulo k, c'est à dire, $nm \equiv 1 \,(\text{mod } d)$.
On doit s'assurer que $m \equiv 1 \,(\text{mod } d)$.
On a $nm = 1 + \alpha d$ et $n = 1 + \beta d$, où $\alpha, \beta \in \mathbb{Z}$, alors $(1+\beta d)\, m = 1 + \alpha d$, d'où $m - 1 = (\alpha - \beta m)\, d$, donc $\overline{m} \in H$. ■

En vertu du lemme 56, l'assertion (1) du lemme 58 devient $[\chi(n) = 1 \ \ (\forall \overline{n} \in H(d,k))]$. Sachant que le sous-groupe $H(d,k)$ se calcule facilement, la dernière formulation permet de déterminer facilement le conducteur de χ.

Exemple 51 *Soit $k \in \mathbb{N}^*$.*

1. *Le caractère principal $\chi_0^{(k)}$ est de conducteur égal à 1 car $H(1,k) = G(k)$ et $\chi_0^{(k)}(n) = 1$ $(\forall \overline{n} \in G(k))$.*
2. *Tout caractère non principal χ est de conducteur d tel que $1 < d \leq k$, car $H(1,k) = G(k)$ et il existe au moins $\overline{n} \in G(k)$ tel que $\chi(n) \neq 1$.*
3. *Pour $k = 15$, les caractères $\chi_1 = \chi_0^{(3)}\chi_1^{(5)}$, $\chi_2 = \chi_0^{(3)}\chi_2^{(5)}$ et $\chi_3 = \chi_0^{(3)}\chi_3^{(5)}$ sont de conducteur 5. Le caractère $\chi_4 = \chi_1^{(3)}\chi_0^{(5)}$ est de conducteur 3. Les caractères χ_5, χ_6 et χ_7 sont de conducteur 15.*

4. $\forall \chi \in \widehat{G}(p)$, $\chi \neq \chi_0$, *où* p *est un nombre premier,* $p \geq 3$, χ *est de conducteur* p.

Lemme 52 *Soit* $k = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, $k > 2$, $r \geq 2$, *et les* $\alpha_i \geq 1$.
Soit

$$\chi \in \widehat{G}(k) : \chi = \chi_1 \chi_2 \cdots \chi_r,\ \chi \neq \chi_0,\ \chi_i \in \widehat{G}(p_i^{\alpha_i}).$$

On a alors

$$f_\chi = f_{\chi_1} f_{\chi_2} \cdots f_{\chi_r}.$$

2.7 Caractère primitif et caractère primitif induit

Définition 53 (Caractère primitif et imprimitif) *Soit* $k \in \mathbb{N}^*$.
Un caractère $\chi \in \widehat{G}(k)$ *est dit primitif si son conducteur est égal à* k
Dans le cas contraire, i.e. $1 \leq \mathfrak{c}(\chi) < k$, $\mathfrak{c}(\chi) \mid k$, *on dit que* χ *est un caractère imprimitif.*

Par convention, le caractère principal modulo $k = 1$, $\chi_0^{(1)}$, est considéré primitif.

Caractère primitif induit.

Soient $k \in \mathbb{N}^*$ et $\chi \in \widehat{G}(k)$, un caractère imprimitif, donc de conducteur $f_\chi = d$, d est un diviseur propre de k, $d \mid k$ et $1 \leq d < k$.

L'unique caractère $\chi^* \in \widehat{G}(d)$, équivalent à χ ($\chi^* \sim \chi$), est primitif à cause de la minimalité de d. il est appelé "caractère primitif induit de χ".

Remarque 54 *Pour tout* $\chi \neq \chi_0$ *modulo* $k > 2$, *on a :*

$$\chi \text{ est primitif} \iff \mathfrak{c}(\chi) = k \iff \chi = \chi^*.$$

Exemple 55 .

1. $\forall k \geq 2$, *le caractère principal* χ_0 *modulo* k *est imprimitif car il est équivalent au caractère* $\chi_0^{(1)}$ *modulo* $k = 1$, $f_{\chi_0} = 1 < k$, $k \geq 2$, *et* $\chi_0^* = \chi_0^{(1)}$.

2. *Si* $k = p$, *un nombre premier, alors tout caractère non principal modulo* k *est primitif, car l'unique diviseur propre de* k *est* 1, *et, étant non principal,* χ *n'est pas équivalent à* $\chi_0^{(1)}$.

3. *Pour* $k = 15$, *les caractères imprimitifs sont* χ_0, χ_1, χ_2, χ_3, χ_4 *et l'on a* $\chi_0^* = \chi_0^{(1)}$, $\chi_1^* = \chi_1^{(5)}$, $\chi_2^* = \chi_2^{(5)}$ *et* $\chi_3^* = \chi_3^{(5)}$.
Les caractères primitifs sont χ_5, χ_6 *et* χ_7 *(Voir les tables de* $\widehat{G}(3)$, $\widehat{G}(5)$, $\widehat{G}(15)$*).*

Lemme 56 *Soit* $k > 2$,

$$k = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r},$$

où $r \geq 2,\ 2 \leq p_1 < p_2 < \cdots < p_r$ *et les* $\alpha_i \geq 1$.
Soit $\chi = \chi_1\chi_2\cdots\chi_r \in \widehat{G}(k)$, $\chi_i \in \widehat{G}(p_i^{\alpha_i})$. *On a alors:*

1. χ *est primitif si et seulement si* χ_i *est primitif dans* $\widehat{G}(p_i^{\alpha_i})$, $\forall i = 1, \ldots, r$.
2. *Si* χ *est imprimitif, alors* $\chi^* = \chi_1^*\chi_2^*\cdots\chi_r^*$, *en précisant que* χ *est primitif si et seulement si* $\chi = \chi^*$. *S'il existe* $i \in \{1, \ldots, r\}$ *tel que* $\chi_i = \chi_0^{\left(p_i^{\alpha_i}\right)}$, *alors* $\chi_i^* = \chi_0^{(1)}$.

Exemple 57 .

1. *Pour* $k = 15$, *les caractères primitifs sont* $\chi_5 = \chi_1^{(3)}\chi_1^{(5)}$, $\chi_6 = \chi_1^{(3)}\chi_2^{(5)}$ *et* $\chi_7 = \chi_1^{(3)}\chi_3^{(5)}$. *Chacun de ces caractères est un produit de deux caractères primitifs.*
2. *Pour* $k = 8$, *les caractères primitifs sont :* $\chi_1 = \chi_{0,1} : \chi_{0,1}(-1) = (-1)^0 = 1$ *et* $\chi_{0,1}(5) = \exp\left(i\frac{\pi}{2^{3-3}}\right) = -1$, $\chi_3 = \chi_{1,1} : \chi_{1,1}(-1) = (-1)^1 = -1$ *et* $\chi_{1,1}(5) = \exp\left(i\frac{\pi}{2^{3-3}}\right) = -1$.

Lemme 58 *Soient* p *un nombre premier,* $p \geq 3$, $\alpha \in \mathbb{N}^*$, $\alpha \geq 2$, $r + p\mathbb{Z}$ *un générateur du groupe* $G(p)$. *Soit* $\overline{s} = \overline{(p+1)\, r^{p^{\alpha-1}}}$ *le générateur du groupe* $G(p^\alpha)$ *obtenu à partir de* r *et* $\beta \in \mathbb{N}^*$ *tels que* $1 \leq \beta \leq \alpha$ *(on précise que* $(s, p) = 1$*).*

1. *Tout caractère* $\chi \in \widehat{G}\left(p^\beta\right)$ *est complètement déterminé par* $\chi(s)$.
2. $\widehat{G}\left(p^\beta\right) = \left\{\chi_0, \chi_1, \ldots, \chi_{\varphi\left(p^\beta\right)-1}\right\}$, *où pour tout* $b \in \left\{0, 1, \ldots, \varphi\left(p^\beta\right) - 1\right\}$, *le caractère* χ_b *est défini par* $\chi_b(s) = \exp\left(i\frac{2\pi b}{\varphi\left(p^\beta\right)}\right)$.

Démonstration. 1 - Soient $\chi \in \widehat{G}\left(p^\beta\right)$, $f \in \hom\left(G\left(p^\beta\right), \mathbb{C}^*\right)$, où f est l'homomorphisme associé à χ. Soit $n \in \mathbb{Z}$, n premier avec p^β.
Il est évident que $\left(n, p^\beta\right) = 1 \Leftrightarrow (n, p) = 1 \Leftrightarrow (n, p^\alpha) = 1$.
Puisque $G(p^\alpha) = \langle\overline{s}\rangle$ alors il existe un unique $\nu \in \{0, 1, \ldots, \varphi(p^\alpha) - 1\}$ tel que $n \equiv s^\nu \pmod{p^\alpha}$ et comme p^β divise p^α, alors $n \equiv s^\nu \pmod{p^\beta}$.
Par définition de χ, on a $\chi(n) = f(\overline{n}) = f\left(\overline{s^\nu}\right) = (f(\overline{s}))^\nu = (\chi(s))^\nu$ (si $(n, p) \neq 1$, $\chi(n) = 0$).
On voit bien que les valeurs de $\chi(s)$ détermine explicitement le caractère χ.

2 - Soit $z \in \left\{1, \ldots, \varphi\left(p^\beta\right) - 1\right\}$, $z \in G\left(p^\beta\right)$ tel que $s \equiv z \pmod{p^\beta}$.
Montrons que $\overline{z} = z + p^\beta\mathbb{Z}$ est un générateur de $G\left(p^\beta\right)$.

Pour cela, on considère l'homomorphisme $u : G(p^\alpha) \to G(p^\beta)$ défini par $n + p^\alpha\mathbb{Z} \mapsto n + p^\beta\mathbb{Z}$, $(n,p) = 1$.
Puisque u est surjectif et $s+p^\alpha\mathbb{Z}$ est un générateur de $G(p^\alpha)$, alors $u(s + p^\alpha\mathbb{Z}) = s + p^\beta\mathbb{Z} = z + p^\beta\mathbb{Z}$ est un générateur de $G(p^\beta)$.
Alors $\widehat{G}(p^\beta) = \left\{\chi_0, \chi_1, \ldots, \chi_{\varphi(p^\beta)-1}\right\}$, où pour tout $b \in \{0, 1, \ldots, \varphi(p^\beta) - 1\}$, le caractère χ_b est défini par $\chi_b(z) = \exp\left(i\frac{2\pi b}{\varphi(p^\beta)}\right)$.
Puisque $s \equiv z \pmod{p^\beta}$, alors $\chi_b(s) = \chi_b(z) = \exp\left(i\frac{2\pi b}{\varphi(p^\beta)}\right)$, d'où l'assertion annocée. ■

Théorème 59 .

1. *Un caractère non principal $\chi_{a,b} \in \widehat{G}(2^\alpha)$ est primitif si et seulement si b est un nombre impair.*
2. *Un caractère non principal $\chi_a \in \widehat{G}(p^\alpha)$, $(\alpha \geq 2)$, est primitif si et seulement si a est premier avec p.*

2.8 Séries de Dirichlet

Définition 60 *Soit $(\lambda_n)_{n\in\mathbb{N}}$ une suite strictement croissante de nombres réels positifs tendant vers l'infini. Une série de Dirichlet $f : \mathbb{C} \longmapsto \mathbb{C}$ d'exposants $(\lambda_n)_{n\in\mathbb{N}}$ est de la forme:*

$$f(s) := \sum_{n\in\mathbb{N}} a_n e^{-\lambda_n s},\ a_n \in \mathbb{C},\ s \in \mathbb{C}$$

Convergence des séries de Dirichlet

Proposition 61 *Si la série $f(s) := \sum_{n\in\mathbb{N}} a_n e^{-\lambda_n s}$ (série de Dirichlet d'exposants $(\lambda_n)_{n\in\mathbb{N}}$)) converge pour $s = s_0$, alors elle converge uniformément dans tout domaine de la forme $\mathrm{Re}(s - s_0) \geq 0$, $\arg(s - s_0) \leq \alpha$, avec $0 \leq \alpha < \frac{\pi}{2}$.*

Avant de démontrer cette proposition, nous allons exposer deux lemmes qui nous seront utiles dans la démonstration.

Lemme 62 (Abel) *Soient (a_n) et (b_n) deux suites complexes.*
Posons :

$$A_{m,p} = \sum_{n=m}^{p} a_n \quad \text{et } S_{m,m'} = \sum_{n=m}^{m'} a_n b_n.$$

Alors,

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'}b_{m'}$$

Lemme 63 *Soient α, β deux nombres réels, avec $0 < \alpha < \beta$ et soit $s = x + iy$, avec $x, y \in \mathbb{R}$ et $x > 0$. On a :*

$$\left|e^{-\alpha s} - e^{-\beta s}\right| \leq \left|\frac{z}{x}\right| \left(e^{-\alpha x} - e^{-\beta x}\right).$$

Démonstration. Pour commencer, nous pouvons écrire $e^{-\alpha s} - e^{-\beta s}$ sous la forme $-s\int_\alpha^\beta e^{-ts}dt$. Si on applique la valeur absolue à l'expression $e^{-\alpha s} - e^{-\beta s}$, nous obtenons alors:

$$\begin{aligned}
\left|e^{-\alpha s} - e^{-\beta s}\right| &= \left|-s\int_\alpha^\beta e^{-ts}dt\right| \\
&= |s|\left|\int_\alpha^\beta e^{-ts}dt\right| \\
&\leq |s|\int_\alpha^\beta \left|e^{-ts}\right| dt
\end{aligned}$$

Transformons e^{-tz} en utilisant la formule d'Euler:

$$e^{-ts} = e^{-tx-ity} = e^{-tx}e^{-ity} = e^{-tx}\left(\cos(-ty) + i\sin(-ty)\right).$$

Or, $|(\cos(-ty) + i\sin(-ty)| = 1$, nous avons donc

$$\left|e^{-ts}\right| = \left|e^{-tx}\right|.$$

D'où

$$\begin{aligned}
\left|e^{-\alpha s} - e^{-\beta s}\right| &\leq |s|\int_\alpha^\beta \left|e^{-ts}\right| dt \\
&= |s|\int_\alpha^\beta \left|e^{-tx}\right| dt.
\end{aligned}$$

e^{-tx} étant strictement plus grand que 0,

$$|s|\int_\alpha^\beta \left|e^{-tx}\right| dt = |s|\int_\alpha^\beta e^{-tx}dt.$$

Si on réécrit l'expression sous la forme initiale, nous avons bien

$$|s| \int_{\alpha}^{\beta} e^{-tx} dt = \frac{|s|}{x} \left(e^{-\alpha x} - e^{-\beta x} \right).$$

Avec $x > 0$,

$$\frac{|s|}{x} \left(e^{-\alpha x} - e^{-\beta x} \right) = \left| \frac{s}{x} \right| \left(e^{-\alpha x} - e^{-\beta x} \right).$$

Nous avons donc bien que

$$\left| e^{-\alpha s} - e^{-\beta s} \right| \leq \left| \frac{s}{x} \right| \left(e^{-\alpha x} - e^{-\beta x} \right).$$

Nous pouvons maintenant grâce aux deux lemmes précédents démontrer la proposition de la manière suivante :
supposons d'abord que $s_0 = 0$ (pour les cas $s_0 \neq 0$, il nous suffit de faire une translation sur s). Ceci implique

$$f(s_0) = \sum_{n \in \mathbb{N}} a_n e^{-\lambda_n 0} = \sum_{n \in \mathbb{N}} a_n.$$

Ainsi, on doit démontrer que si la série $\sum_{n \in \mathbb{N}} a_n$ converge, $f(s)$ converge uniformément sur tout domaine de la forme $\mathrm{Re}(s) \geq 0$, $\dfrac{|s|}{\mathrm{Re}(s)} \leq k$.
Soit $\varepsilon > 0$. Le fait que $\sum_{n \in \mathbb{N}} a_n$ converge implique qu'il existe un N tel que si $m,\ m' \geq N$, alors, si on reprend les notations du lemme, $|A_{m,m'}| \leq \varepsilon$. Par ce même lemme, avec $b_n = e^{-\lambda_n s}$, nous avons:

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}) + A_{m,m'} e^{-\lambda_{m'} s}.$$

On a

$$\begin{aligned} |S_{m,m'}| &= \left| \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}) + A_{m,m'} e^{-\lambda_{m'} s} \right| \\ &\leq \left| \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}) \right| + \left| A_{m,m'} e^{-\lambda_{m'} s} \right|. \end{aligned}$$

Par l'inégalité du triangle,

$$|S_{m,m'}| \leq \sum_{n=m}^{m'-1} \left| A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) \right| + \left| A_{m,m'} e^{-\lambda_{m'} z} \right|$$

$\left|e^{-\lambda_{m'}z}\right|$ étant strictement positif et $|A_{m,m'}| \leq \varepsilon$, on peut dire que

$$|S_{m,m'}| \leq \sum_{n=m}^{m'-1} \varepsilon \left|(e^{-\lambda_n s} - e^{-\lambda_{n+1} s})\right| + \varepsilon \left|e^{-\lambda_{m'} s}\right|.$$

D'après le lemme et en prenant $s = x + iy$, on peut écrire

$$\begin{aligned} |S_{m,m'}| &\leq \sum_{n=m}^{m'-1} \varepsilon \left(\left|\frac{s}{x}\right| (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})\right) + \varepsilon \left|e^{-\lambda_{m'} s}\right| \\ &= \varepsilon \left(\left|\frac{s}{x}\right| \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) + \left|e^{-\lambda_{m'} s}\right|\right). \end{aligned}$$

Par la formule d'Euler, nous pouvons transformer l'expression $\left|e^{-\lambda_{m'} s}\right|$:

$$\begin{aligned} \left|e^{-\lambda_{m'} s}\right| &= \left|e^{-\lambda_{m'} x} (\cos(-\lambda_{m'} y) + i \sin(-\lambda_{m'} y))\right| \\ &= \left|e^{-\lambda_{m'} x}\right| \leq 1. \end{aligned}$$

On en déduit donc que :

$$|S_{m,m'}| \leq \varepsilon \left(\left|\frac{s}{x}\right| \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) + 1\right).$$

La série $\sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})$ est une série téléscopique. On a donc

$$|S_{m,m'}| \leq \varepsilon \left(1 + \left|\frac{s}{x}\right| (e^{-\lambda_m x} - e^{-\lambda_{m'} x})\right).$$

$(e^{-\lambda_m x} - e^{-\lambda_{m'} x})$ étant plus petit que 1 car $0 < e^{-\lambda_{m'} x} < e^{-\lambda_m x}$ et que $x > 0$ implique que $e^{-\lambda_m x} < 1$. On a donc

$$|S_{m,m'}| \leq \varepsilon \left(1 + \left|\frac{s}{x}\right|\right).$$

Or nous nous intéressons au domaine de la forme $\dfrac{|s|}{\mathrm{Re}(z)} \leq k$. Nous avons donc

$$|S_{m,m'}| \leq \varepsilon (1 + k).$$

Ceci nous montre bien la convergence uniforme de $f(s)$ dans le domaine précité. Nous avons ainsi démontré qu'une série de Dirichlet d'exposants λ_n convergeant pour un z_0, converge uniformément dans tout domaine de la forme $\mathrm{Re}(s - s_0) \geq 0$, $\arg(s - s_0) \leq \alpha$, avec $0 \leq \alpha < \dfrac{\pi}{2}$. ■

2.8.1 Séries de Dirichlet proprement dites

Les séries de Dirichlet proprement dites sont obtenues en posant $\lambda_n = \log(n)$ dans les séries de Dirichlet, c'est à dire

$$f(s) := \sum_{n\in\mathbb{N}} a_n e^{-\lambda_n s} = \sum_{n\in\mathbb{N}} a_n e^{-s\log(n)} = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s}$$

où s, $a_n \in \mathbb{C}$.

Convergence des séries de Dirichlet proprement dites

Les séries de Dirichlet proprement dites :

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

ont les propriétés suivantes :

Proposition 64 *Si les a_n sont bornés, il y a convergence absolue pour* $\mathrm{Re}(s) > 1$.

Démonstration. Nous savons que la série $\sum_{n=1}^{\infty} \frac{1}{n^\alpha}$, $\alpha \in \mathbb{R}$, converge pour $\alpha > 1$. Or, la suite a_n étant bornée par k, on peut écrire

$$f(s) \leq \sum_{n=1}^{\infty} \frac{k}{n^s} = k\sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Cette série converge absolument pour $\mathrm{Re}(s) > 1$ et donc $f(s)$ converge absolument pour $\mathrm{Re}(s) > 1$. ■

Proposition 65 *Si les sommes partielles $A_{m,p} = \sum_{n=m}^{p} a_n$ sont bornées, il y a convergence (non nécessairement absolue) pour* $\mathrm{Re}(s) > 0$.

Démonstration. Par le lemme 70, on a

$$|S_{m,m'}| = \left| \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'}b_{m'} \right|.$$

Donc,

$$|S_{m,m'}| \leq \sum_{n=m}^{m'-1} |A_{m,n}|\,|b_n - b_{n+1}| + |A_{m,m'}|\,|b_{m'}|\,.$$

Supposons que $|A_{m,p}| \leq K$, car les sommes partielles sont bornées, alors

$$|S_{m,m'}| \leq K \left(\sum_{n=m}^{m'-1} (b_n - b_{n+1}) + |b_{m'}| \right).$$

Soit $b_n = 1/n^s$, alors

$$|S_{m,m'}| \leq K \left(\sum_{n=m}^{m'-1} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \left| \frac{1}{m'^s} \right| \right).$$

Cette série est une somme télescopique et nous avons donc

$$|S_{m,m'}| \leq K \left(\left| \frac{1}{m^s} - \frac{1}{(m'-1+1)^s} \right| + \left| \frac{1}{m'^s} \right| \right).$$

En simplifiant, on obtient

$$|S_{m,m'}| \leq K/m^s.$$

Il y a donc bien convergence pour $\mathrm{Re}(s) > 0$. ■

Définition 66 *Une fonction $f : \mathbb{N} \longrightarrow \mathbb{C}$ est dite strictement multiplicative si l'on a*

$$f(nm) = f(n)f(m)$$

pour tout $n,\ m \in \mathbb{N}$.

Dans la suite, on considère une fonction f strictement multiplicative et bornée et soit P, l'ensemble des nombres premiers.

Lemme 67 *La série de Dirichlet $\sum_{n=1}^{\infty} f(n)/n^s$ converge absolument pour $\mathrm{Re}(s) > 1$, et sa somme dans ce domaine est égale au produit infini convergent*

$$\prod_{p \in P} (1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots)$$

Démonstration. Commençons par écrire $(1+f(p)p^{-s}+\ldots+f(p^m)p^{-ms}+\ldots)$ sous forme de série :

$$(1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots) = \sum_{m=0}^{\infty} f(p^m)p^{-ms}.$$

f étant multiplicative, on peut écrire

$$\sum_{m=0}^{\infty} f(p^m)p^{-ms} = \sum_{m=0}^{\infty} \left(f(p)p^{-s} \right)^m.$$

Cette série est une série géométique:

$$\sum_{m=0}^{\infty} \left(f(p)p^{-s}\right)^m = \frac{1}{1-f(p)p^{-s}}.$$

Soit p_k le $k-$ème élément de P. Nous avons alors

$$\prod_{k=1}^{l} \frac{1}{1-f(p_k)p_k^{-s}} = \prod_{k=1}^{l}\sum_{m=0}^{\infty} \left(f(p_k)p_k^{-s}\right)^m.$$

Par Cauchy,

$$\begin{aligned}\prod_{k=1}^{l}\sum_{m=0}^{\infty} \left(f(p_k)p_k^{-s}\right)^m &= \sum_{m_1,\ldots,m_l=0}^{\infty} \left(f(p_1)p_1^{-s}\right)^{m_1} \ldots\ldots \left(f(p_l)p_l^{-s}\right)^{m_l} \\ &= \sum_{m_1,\ldots,m_l=0}^{\infty} f(p_1^{m_1})p_1^{-m_1 s}\ldots\ldots f(p_l^{m_l})p_l^{-m_l s}.\end{aligned}$$

Par le théorème fondamental de l'arithmétique, on peut décomposer tout entier n en produit de nombres premiers de manière unique :

$$n = p_1^{m_1}\ldots\ldots p_l^{m_l}.$$

On obtient alors

$$\begin{aligned}\prod_{p\in P} \frac{1}{1-f(p_k)p_k^{-s}} &= \lim_{l\to+\infty}\prod_{k=1}^{l} \frac{1}{1-f(p_k)p_k^{-s}} \\ &= \lim_{l\to+\infty}\sum_{m_1,\ldots,m_l=0}^{\infty} f(p_1^{m_1})p_1^{-m_1 s}\ldots\ldots f(p_l^{m_l})p_l^{-m_l s} \\ &= \sum_{n=1}^{\infty} f(n)/n^s.\end{aligned}$$

■

2.8.2 Fonction zêta de Riemann

En considérant les séries de Dirichlet proprement dites $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ avec $a_n = 1$. On a la fonction zêta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_{p,\text{ premier}} \frac{1}{1-\frac{1}{p^s}},\ \ \mathrm{Re}(s) > 1$$

.

Théorème 68 *1. La fonction ζ a un prolongement méromorphe à $\mathbb{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ de résidu 1.*

2. Si $n \in \mathbb{Q}$, alors

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1};$$

en particulier $\zeta(-n) \in \mathbb{Q}$.
Les B_n sont des nombres rationnels appelés nombres de Bernoulli définis comme suit :

$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}$$

Hypothèse de Riemann: les zéros non triviaux de la fonction zêta de Riemann ont tous pour partie réelle $\frac{1}{2}$. Cette **Hypothèse,** formulée en 1859 par Riemann, n'a pas encore été démontrée**.**

2.8.3 Fonction L de Dirichlet

Soit χ un caractère de Dirichlet de conducteur f.

La fonction L de Dirichlet associée à χ est définie comme suit :

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

où $s \in \mathbb{C}$, $\mathrm{Re}\,(s) > 1$.

Par prolongement analytique, cette fonction peut être étendue à une fonction méromorphe sur le plan complexe entier.

Comme χ est une fonction multiplicative, la série L associée possède un produit eulérien

$$\begin{aligned} L(s, \chi) &= \prod_{p \geq 2} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \frac{\chi(p^3)}{p^{3s}} + \cdots\right) \\ &= \prod_{p \geq 2} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \frac{\chi(p)^3}{p^{3s}} + \cdots\right) \\ &= \prod_{p \geq 2} \frac{1}{1 - \frac{\chi(p)}{p^s}}, \ (\mathrm{Re}\,(s) > 1) \end{aligned}$$

Nous avons également que $L(s, \chi_0) = \zeta(s)$, où

$$\begin{cases} \chi_0(n) = 1 \text{ si } (n, f) = 1 \\ \chi_0(n) = 0 \text{ si } (n, f) \neq 1 \end{cases}.$$

Chapitre 3

Valeurs explicites de mesures de Mahler

Dans ce dernier chapitre, nous donnons les outils et techniques de calcul qui permettent de donner des valeurs explicites de mesures de Mahler de polynômes de plusieurs variables, de mesures de Mahler supérieures et supérieures multiples. Nous exposons donc, les démonstrations détaillées de plusieurs résultats, notamment, ceux de Smyth, Sana Boughzala, Kurokawa, Lalin, Ochiai et Sinha.

Les références utilisées sont : [19], [20], [25], [7] et [26].

3.1 Exemples de Mesures de Mahler logarithmiques de polynômes de 2 et 3 variables

Dans ce qui suit, un caractère réel impair de conducteur f sera noté χ_{-f}.

En 1980, Smyth a prouvé les deux relations suivantes

$$m(x+y+1) = \frac{3\sqrt{3}}{4\pi} L(2, \chi_{-3})$$

$$m(x+y+z+1) = \frac{7}{2\pi^2}\zeta(3),$$

où, χ_{-3} est le caractère de Dirichlet réel impair de conducteur 3 défini par

$$\chi_{-3}(n) = \begin{cases} 0 \text{ si } n \equiv 0 \bmod(3) \\ 1 \text{ si } n \equiv 1 \bmod(3) \\ -1 \text{ si } n \equiv 2 \bmod(3) \end{cases},$$

$L(2, \chi_{-3})$ est la fonction L de Dirichlet associée à χ_{-3} pour $s = 2$ et ζ, la fonction zêta de Riemann.

Proposition 69 *On a*

$$m(x+y+1) = \frac{3\sqrt{3}}{4\pi} L(2, \chi_{-3}).$$

Démonstration. On a

$$\begin{aligned}
m(x+y+1) &= \frac{1}{(2\pi i)^2} \int_{|x|=1} \int_{|y|=1} \log|x+y+1| \, \frac{dx}{x} \frac{dy}{y} \\
&= \frac{1}{2\pi i} \int_{|x|=1} \log^+|1+x| \, \frac{dx}{x} \quad \text{(d'après la formule de Jensen)} \\
&= \frac{1}{2\pi} \int_{-\pi}^{\pi} \log^+\left|1+e^{i\theta}\right| d\theta \\
&= \frac{1}{2\pi} \int_{\frac{-2\pi}{3}}^{\frac{2\pi}{3}} \log\left|1+e^{i\theta}\right| d\theta, \text{ car } \left|1+e^{i\theta}\right| > 1 \text{ pour } \frac{-2\pi}{3} < \theta < \frac{+2\pi}{3} \\
&= \frac{2}{3}\log 2 + \frac{2}{\pi} \int_0^{\frac{\pi}{3}} \log(\cos t) \, dt.
\end{aligned}$$

On a

$$\int \log(\cos\theta) \, d\theta = \theta \log(\cos\theta) - \theta \log(1+e^{2i\theta}) + \frac{i}{2}\mathbf{Li}_2(-e^{2i\theta}) + i\frac{\theta^2}{2}.$$

Pour cela, il suffit de dériver et d'utiliser le définition suivante de la foncion dilogarithme

$$\mathbf{Li}_2(z) = \sum_{n\geq 1} \frac{z^n}{n^2}, \quad |z| < 1$$

telle que

$$z\frac{d}{dz}\mathbf{Li}_2(z) = -\log(1-z).$$

D'où

$$\begin{aligned}
m(x+y+1) &= \operatorname{Re}\left(\frac{i}{\pi}\mathbf{Li}_2(e^{\frac{-2\pi i}{6}})\right) \\
&= \frac{\sqrt{3}}{4\pi} 2\left(\frac{1}{1^2} + \frac{1}{2^2} - \frac{1}{4^2} - \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{8^2} + \ldots\ldots\right) \\
&= \frac{\sqrt{3}}{4\pi} 2\left(\frac{1}{1^2} - \frac{1}{2^2} + \frac{1}{4^2} - \frac{1}{5^2} + \ldots\ldots\right) \\
&\quad + \frac{\sqrt{3}}{4\pi} 4 \underbrace{\left(\frac{1}{2^2} - \frac{1}{4^2} + \frac{1}{8^2} - \frac{1}{10^2} + \ldots\ldots\right)}_{\frac{1}{4}L(2,\chi_{-3})} \\
&= \frac{3\sqrt{3}}{4\pi} L(2, \chi_{-3}).
\end{aligned}$$

■

Proposition 70 *On a*

$$m(1+x+y+z)=\frac{7}{2\pi^2}\zeta(3).$$

Démonstration. *On pose* $y=zt$

$$\begin{aligned}
A &= m(1+x+y+z)\\
&= m(1+x+zt+z)\\
&= m(1+x+z(1+t))\\
&= \frac{1}{(2\pi i)^3}\int_{|x|=1}\int_{|z|=1}\int_{|t|=1}\log|1+x+z(1+t)|\,\frac{dx}{x}\frac{dz}{z}\frac{dt}{t}\\
&= \frac{1}{(2\pi i)^3}\int_{|x|=1}\int_{|z|=1}\int_{|t|=1}\log|1+t|\,\frac{dx}{x}\frac{dz}{z}\frac{dt}{t}+\frac{1}{(2\pi i)^3}\int_{|x|=1}\int_{|z|=1}\int_{|t|=1}\log\left|\frac{1+x}{1+t}+z\right|\frac{dx}{x}\frac{dz}{z}\frac{dt}{t}\\
&= \frac{1}{(2\pi i)^2}\int_{|x|=1}\int_{|t|=1}\log|1+t|\,\frac{dx}{x}\frac{dt}{t}+\frac{1}{(2\pi i)^2}\int_{|x|=1}\int_{|t|=1}\max(\log\left|\frac{1+x}{1+t}\right|;0)\frac{dx}{x}\frac{dt}{t}\\
&= \frac{1}{(2\pi i)^2}\int_{|x|=1}\int_{|t|=1}\max(\log|1+x|\,;\log|1+t|)\frac{dx}{x}\frac{dt}{t}\\
&= \frac{1}{\pi^2}\int_0^\pi\int_0^\pi\max\left(\log\left|1+e^{i\varphi}\right|,\log\left|1+e^{iu}\right|\right)d\varphi du \ \textit{si}\ x=e^{i\varphi}\ \textit{et}\ t=e^{iu}.
\end{aligned}$$

On a

$$\varphi<u\implies\left|1+e^{i\varphi}\right|>\left|1+e^{iu}\right|,$$

d'où, en intégrant à u *constant, on a*

$$\begin{aligned}
\pi^2A &= \int_0^\pi\left(\int_0^u\log\left|1+e^{i\varphi}\right|d\varphi+\int_u^\pi\log\left|1+e^{iu}\right|d\varphi\right)du\\
&= \int_0^\pi(\pi-u)\log\left|1+e^{iu}\right|du+\int_\Delta\int\log\left|1+e^{i\varphi}\right|dud\varphi.\\
\Delta &= \{(u,\varphi)\mid u<\varphi,\ 0\le u\le\pi\}
\end{aligned}$$

On calcule

$$\int_\Delta\int\log\left|1+e^{i\varphi}\right|dud\varphi$$

à φ constant. On a donc

$$\int\int_{\Delta} \log\left|1+e^{i\varphi}\right| du d\varphi = \int_0^{\pi} (\pi-\varphi)\log\left|1+e^{i\varphi}\right| d\varphi.$$

D'où

$$\begin{aligned} A &= \frac{2}{\pi^2}\int_0^{\pi} (\pi-u)\log\left|1+e^{iu}\right| du \\ &= -\frac{2}{\pi^2}\int_0^{\pi} u\log\left|1+e^{iu}\right| du, \end{aligned}$$

puisque $m(1+x)=0$.
Comme

$$\log\left|1+e^{iu}\right| = \mathrm{Re}\sum_{n\geq 1}\frac{(-1)^{n-1}}{n}e^{inu},$$

une intégration par parties donne alors

$$\begin{aligned} A &= \frac{4}{\pi^2}\sum_{k\geq 0}\frac{1}{(2k+1)^3} = \frac{7}{2\pi^2}\zeta(3) \\ &\left(\zeta(3) = \sum\frac{1}{(2k)^3} + \sum\frac{1}{(2k+1)^3}\right) \end{aligned}$$

■

En 2006, Sana Boughzala a étudié la mesure de Mahler logarithmique de la famille des polynômes

$$P_s = (x^2+x-1)y^2 - sxy - x^2 + x + 1,\ s\in\mathbb{R}.$$

Pour $s = 2\sqrt{5}$, cette mesure s'exprime en fonction de $\mathbf{Li}_2(\chi_{-4},\phi)$, où ϕ est l'inverse du nombre d'or et χ, le caractère de Dirichlet réel impair de conducteur 4.

Théorème 71 *Soit $\phi = \dfrac{\sqrt{5}-1}{2}$, on a alors*

$$m(P_{2\sqrt{5}}) = -\log\phi + \frac{4}{\pi}\mathbf{Li}_2(\chi_{-4},\phi),$$

où

$$\begin{cases} \chi(n) = 1 \ si\ n \equiv 1 \bmod 4 \\ \chi(n) = 0 \ si\ n \equiv 0 \bmod 2 \\ \chi(n) = -1 \ si\ n \equiv 3 \bmod 4 \end{cases}$$

et $\mathbf{Li}_2$ *le dilogarithme donné par*

$$\mathbf{Li}_2(\chi, z) = \sum_{n\geq 1} \frac{\chi(n)}{n^2} z^n$$

Démonstration. Si

$$P_s = (x^2 + x - 1)y^2 - sxy - x^2 + x + 1$$

$$A(x) = x^2 + x - 1,$$

alors

$$AP_{2\sqrt{5}} = \big(y(x^2 + x - 1) - \sqrt{5}x)^2 - (1 + x^2)^2 = P_1 P_2$$

avec

$$P_1 = y(x^2 + x - 1) - \sqrt{5}x + 1 + x^2$$

et

$$P_2 = y(x^2 + x - 1) - \sqrt{5}x - 1 - x^2.$$

D'où

$$m(P_{2\sqrt{5}}) = m(P_1) + m(P_2) - m(A).$$

Or

$$m(P_1) = \frac{1}{4\pi^2} \int_{-\pi}^{\pi}\int_{-\pi}^{\pi} \log|P_1(x, y)|\, dt_1 dt_2$$

avec $x = e^{it_1}$ et $y = e^{it_2}$, d'où

$$\begin{aligned} m(P_1) &= \frac{1}{4\pi^2} \int_{-\pi}^{\pi}\int_{-\pi}^{\pi} \log\left|y(x^2 + x - 1) - \sqrt{5}x + 1 + x^2\right| dt_1 dt_2 \\ &= m(A) + \frac{1}{\pi}\int_0^{\pi} \log^+\left|\frac{x^2 - \sqrt{5}x + 1}{x^2 + x - 1}\right| dt_1, \text{ d'aprés la formule de Jensen.} \end{aligned}$$

D'autre part les polynômes $x^2 - \sqrt{5}x + 1$ et $x^2 + x - 1$ ont un zéro commun, d'où

$$\begin{aligned} m(P_1) &= m(A) + \frac{1}{\pi}\int_0^{\pi} \log^+\left|\frac{2e^{it} - \sqrt{5} - 1}{2e^{it} + \sqrt{5} + 1}\right| dt \\ &= m(A) + \frac{1}{\pi}\int_{\frac{\pi}{2}}^{\pi} \log^+\left|\frac{2e^{it} - \sqrt{5} - 1}{2e^{it} + \sqrt{5} + 1}\right| dt. \end{aligned}$$

De même

$$\begin{aligned} m(P_2) &= m(A) + \frac{1}{\pi}\int_0^{\pi} \log^+ \left| \frac{x^2+\sqrt{5}x+1}{x^2+x-1} \right| dt_2 \\ &= m(A) + \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \log^+ \left| \frac{2e^{it}+\sqrt{5}-1}{2e^{it}-\sqrt{5}+1} \right| dt, \end{aligned}$$

d'où

$$\begin{aligned} m(P_1)+m(P_2)-2m(A) &= \frac{1}{\pi}\int_{\frac{\pi}{2}}^{\pi} \log^+ \left| \frac{2e^{it}-\sqrt{5}-1}{2e^{it}+\sqrt{5}+1} \right| dt \\ &\quad + \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \log^+ \left| \frac{2e^{it}+\sqrt{5}-1}{2e^{it}-\sqrt{5}+1} \right| dt. \end{aligned}$$

En changeant t en $\pi - t$ dans la première intégrale et en simplifiant on obtient

$$\begin{aligned} m(P_1)+m(P_2)-2m(A) &= \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \log \left| \frac{-e^{-it}-\frac{1}{\phi}}{-e^{-it}+\frac{1}{\phi}} \right| dt \\ &\quad + \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \log \left| \frac{e^{it}+\phi}{e^{it}-\phi} \right| dt, \end{aligned}$$

d'où

$$m(P_1)+m(P_2)-2m(A) = \frac{2}{\pi}\int_0^{\frac{\pi}{2}} \log\left|1+\phi e^{-it}\right| dt + \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \log\left|1-\phi e^{-it}\right| dt.$$

On a $|\phi| < 1$, donc

$$m(P_1)+m(P_2)-2m(A) = \frac{2}{\pi}\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \left(\phi - (-\phi)^n\right) \operatorname{Re} \int_0^{\frac{\pi}{2}} e^{-int} dt$$

car

$$\log|1+z| = \operatorname{Re} \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} z^n, \text{ pour } |z| < 1.$$

Or

$$m(P_{2\sqrt{5}}) = m(P_1) + m(P_2) - m(A),$$

d'où

$$m(P_{2\sqrt{5}}) - m(A) = \frac{2}{\pi}\sum_{n\geq 1}\frac{2}{2n+1}\phi^{2n+1}\,\mathrm{Re}\int_0^{\frac{\pi}{2}} e^{-i(2n+1)t}dt$$

$$m(P_{2\sqrt{5}}) - m(A) = \frac{4}{\pi}\sum_{n\geq 1}\frac{(-1)^n}{2n+1}\phi^{2n+1}.$$

Comme $m(A) = -\log\phi$, alors

$$m(P_{2\sqrt{5}}) = -\log\phi + \frac{4}{\pi}\mathbf{Li}_2(\chi_{-4},\phi).$$

■

3.2 Un exemple de calcul de mesure de Mahler multiple

Théorème 72 *Pour* $0 \leq \alpha \leq 1$

$$m(1-x, 1-e^{2\pi i\alpha}x) = \frac{\pi^2}{2}(\alpha^2 - \alpha + \frac{1}{6}).$$

En particulier, on obtient les résultats suivants

$$\begin{aligned} m(1-x,1-x) &= \frac{\pi^2}{12} \\ m(1-x,1+x) &= -\frac{\pi^2}{24} \\ m(1-x,1\pm ix) &= -\frac{\pi^2}{96} \\ m(1-x,1-e^{2\pi i\alpha}x) &= 0 \iff \alpha = \frac{3\pm\sqrt{3}}{6} \end{aligned}$$

Démonstration. Par définition,

$$\begin{aligned} m(1-x,1-e^{2\pi i\alpha}x) &= \int_0^1 \mathrm{Re}\log(1-e^{2\pi i\theta}).\,\mathrm{Re}\log(1-e^{2\pi i(\theta+\alpha)})d\theta \\ &= \int_0^1 \left(-\sum_{k=1}^{\infty}\frac{1}{k}\cos 2\pi k\theta\right)\left(-\sum_{l=1}^{\infty}\frac{1}{l}\cos 2\pi\left(\theta+\alpha\right)\right)d\theta \\ &= \sum_{k,l\geq 1}\frac{1}{kl}\int_0^1 \cos\left(2\pi k\theta\right)\cos 2\pi l\left(\theta+\alpha\right)d\theta. \end{aligned}$$

D'un autre côté,

$$\int_0^1 \cos(2\pi k\theta)\cos 2\pi l\,(\theta+\alpha)\,d\theta = \begin{cases} \frac{1}{2}\cos(2\pi k\alpha) & \text{si } l=k, \\ 0 & \text{sinon.} \end{cases}$$

En remplaçant, nous avons

$$m(1-x,1-e^{2\pi i\alpha}x) = \frac{1}{2}\sum_{k=1}^{\infty}\frac{\cos(2\pi k\alpha)}{k^2} = \frac{\pi^2}{2}(\alpha^2-\alpha+\frac{1}{6}).$$

Pour prouver cela, nous allons trouver la série de Fourier du polynôme en α de

$$\pi^2\alpha^2-\pi^2\alpha+\frac{\pi^2}{6}.$$

Considérons d'abord le cas $0<\alpha<1$, ensuite $0<2\pi\alpha<2\pi$.
On pose $y=2\pi\alpha$. En remplaçant dans le polynôme, nous aurons la fonction :

$$f(y) = \frac{y^2}{4}-\frac{\pi y}{2}+\frac{\pi^2}{6} \text{ pour } 0<y<2\pi.$$

De nouveau, on pose $x=y-\pi$ et nous avons la fonction

$$g(x) = \frac{x^2}{4}-\frac{\pi^2}{12},$$

où $g(x)$ est une fonction périodique de période 2π avec $-\pi<y<\pi$.
La série de Fourier de cette fonction est donné par :

$$S(x) = \frac{a_0}{2}+\sum_{k=1}^{\infty}\left[a_k\cos kx+b_k\sin kx\right],$$

où

$$\begin{aligned} a_0 &= \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)dx, \\ a_k &= \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\cos kx dx, \\ b_k &= \frac{1}{\pi}\int_{-\pi}^{\pi} g(x)\cos kx dx. \end{aligned}$$

Donc

$$\begin{aligned}
a_0 &= \frac{1}{\pi}\int_{-\pi}^{\pi}\left(\frac{x^2}{4}-\frac{\pi^2}{12}\right)dx = \frac{1}{\pi}\left[\frac{x^3}{12}-\frac{\pi^2 x}{12}\right]_{-\pi}^{+\pi} = 0.\\
a_k &= \frac{1}{\pi}\int_{-\pi}^{\pi}\left(\frac{x^2}{4}-\frac{\pi^2}{12}\right)\cos kx dx\\
&= \frac{2}{\pi}\int_{0}^{\pi}\frac{x^2}{4}\cos kx dx - \frac{2}{\pi}\int_{0}^{\pi}\frac{\pi^2}{12}\cos kx dx\\
&= \frac{1}{2\pi}\left[\frac{x^2\sin kx}{k} - 2x\frac{-\cos kx}{k^2} + 2\frac{-\sin kx}{k^3}\right]_0^{\pi} - \frac{2}{\pi}\left[\frac{\pi^2}{12}\frac{\sin kx}{k}\right]_0^{\pi}\\
&= \frac{1}{2\pi}\left[\frac{2\pi\cos kx}{k^2}\right] = \frac{(-1)^k}{k^2}\\
b_k &= \frac{1}{\pi}\int_{-\pi}^{\pi}\left(\frac{x^2}{4}-\frac{\pi^2}{12}\right)\sin kx dx = 0, \text{ car la fonction est impaire.}
\end{aligned}$$

Donc nous obtenons la série de Fourier suivante

$$g(x) = \frac{x^2}{4}-\frac{\pi^2}{12} = \sum_{k=1}^{\infty}\frac{(-1)^n}{k^2}\cos kx.$$

Maintenant, nous remplaçons x par $y-\pi$ et comme

$$\cos\left(k(y-\pi)\right) = \cos ky\cos k\pi - \sin ky\sin k\pi = (-1)^k\cos k\pi,$$

donc

$$f(y) = \frac{y^2}{4}-\frac{\pi y}{2}+\frac{\pi^2}{6} = \sum_{k=0}^{\infty}\frac{\cos ky}{k^2}.$$

Finallement pour $y = 2\pi\alpha$, et $0<\alpha<1$,

$$\pi^2\left(\alpha^2-\alpha+\frac{1}{6}\right) = \sum_{k=0}^{\infty}\frac{\cos 2\pi k\alpha}{k^2}.$$

■

Remarque 73 *Le même calcul montre que*

$$m(1-\alpha x, 1-\beta x) = \begin{cases} \frac{1}{2}\operatorname{Re} Li_2(\alpha\overline{\beta}) & si\ \ |\alpha|, |\beta| \le 1,\\ \frac{1}{2}\operatorname{Re} Li_2(\frac{\alpha\beta}{|\alpha|^2}) & si\ \ |\alpha| \ge 1, |\beta| \le 1,\\ \frac{1}{2}\operatorname{Re} Li_2(\frac{\alpha\beta}{|\alpha\beta|}) + \log|\alpha|\log|\beta| & si\ \ |\alpha|, |\beta| \ge 1, \end{cases}$$

3.3 Exemples de mesures de Mahler $k-$supérieure

En général, la mesure de Mahler $k-$supérieure est très difficile à calculer, même pour les polynômes d'une seule variable.

Le théorème 82 suivant montre un lien direct entre la mesure de Mahler supérieure de $P(x) = 1 - x$ et la fonction zêta de Riemann.

Théorème 74

$$m_k(1-x) = \sum_{b_1+\cdots+b_h=k, b_t\geq 2} \frac{(-1)^k\, k!}{2^{2h}} \zeta\left(b_1, \cdots b_h\right),$$

où

$$\zeta\left(b_1, \cdots b_h\right) := \sum_{0<l_1<\cdots<l_h} \frac{1}{l_1^{b_1} \cdots l_h^{b_h}}.$$

En appliquant le théorème précédent, nous avons

$$\begin{aligned} m_2(x-1) &= \frac{\zeta(2)}{2} \\ m_3(x-1) &= \frac{-3\zeta(3)}{2} \\ m_4(x-1) &= 24\left(\frac{\zeta(4)}{4} + \frac{\zeta(2,2)}{16}\right) \end{aligned}$$

Théorème 75 *Soit $a \in \mathbb{C}$.*
Pour $|a| < 1$, on a

$$\begin{aligned} m_2(x+a) &= \frac{1}{2}\sum_{n=1}^{\infty} \frac{|a|^{2n}}{n^2}, \\ m_3(x+a) &= -\frac{3}{2}\sum_{0<j<n<\infty} \frac{|a|^{2n}}{jn^2}, \end{aligned}$$

et
pour $|a| > 1$, on a

$$\begin{aligned} m_2(x+a) &= \log^2|a| + \frac{1}{2}\sum_{n=1}^{\infty} \frac{1}{|a|^{2n} n^2} \\ m_3(x+a) &= \log^3|a| + \frac{3}{2}\log|a| \sum_{n=1}^{\infty} \frac{1}{|a|^{2n} n^2} - \frac{3}{2}\sum_{0<j<n<\infty} \frac{1}{|a|^{2n} jn^2}. \end{aligned}$$

Avant de démontrer ce résultat, nous rappelons les théorème et lemme suivants :

Théorème 76 (Akatuska) *Soit $a \in \mathbb{C}$ tel que $|a| \neq 1$. On a alors*

$$Z(s, x+a) = \begin{cases} F(\frac{-s}{2}, \frac{-s}{2}; 1; |a|^2) & si\ |a| < 1 \\ |a|^s F(\frac{-s}{2}, \frac{-s}{2}; 1; |a|^{-2}) & si\ |a| > 1 \end{cases},$$

où

$$F(\alpha, \beta; \gamma; z) = \sum_{n=0}^{\infty} \frac{(\alpha)_n (\beta)_n}{(\gamma)_n} \frac{z^n}{n!} \quad (|z| < 1),$$

$(\alpha)_0 = 1$ *et* $(\alpha)_n := \alpha(\alpha+1)\cdots(\alpha+n-1)$ *pour* $n \geq 1$ *et* $Z(s, x+a)$ *est la fonction zêta de Mahler en* $x+a$.

Il est possible de calculer $m_2(x+a)$ et $m_3(x+a)$ en dérivant $Z(s, x+a)$.

Lemme 77 *Soit $z \in \mathbb{C}$ tel que $|z| < 1$ et*

$$G_z(s) = F\left(-\frac{s}{2}, -\frac{s}{2}; 1; z\right) = \sum_{n=0}^{\infty} \left(-\frac{s}{2}\right)_n^2 \frac{z^n}{(n!)^2}.$$

On a les égalités suivantes

$$\begin{aligned} G'_z(0) &= 0 \\ G''_z(0) &= \frac{1}{2} \sum_{n=1}^{\infty} \frac{z^n}{n^2} \\ G'''_z(0) &= -\frac{3}{2} \sum_{0<j<n<\infty} \frac{z^n}{jn^2} \end{aligned}$$

Démonstration. Remarquons que si $f(s) = (as)_n$, on a

$$f'(s) = a \sum_{j=o}^{n-1} \frac{(as)_n}{as+j}.$$

En dérivant une seconde fois, on obtient

$$\begin{aligned} f"(s) &= a \sum_{j=o}^{n-1} \left(\frac{(as)_n}{as+j}\right)' \\ &= a \sum_{j=o}^{n-1} \left(\frac{(as)'_n}{as+j} - \frac{a(as)_n}{(as+j)^2}\right) \\ &= 2a^2 \sum_{0 \leq i < j \leq n-1} \frac{(as)_n}{(as+i)(as+j)}. \end{aligned}$$

En particulier, pour $s = 0$, on a

$$\begin{aligned} f'(0) &= a(n-1)! \\ f"(0) &= 2a^2(n-1)!\sum_{j=1}^{n-1}\frac{1}{j}. \end{aligned}$$

En dérivant

$$\begin{aligned} G'_z(s) &= \sum_{n=0}^{\infty} 2\left(\frac{-s}{2}\right)_n \left(\frac{-s}{2}\right)'_n \frac{z^n}{(n!)^2} \\ G''_z(s) &= \sum_{n=0}^{\infty} 2\left[\left(\frac{-s}{2}\right)'_n \left(\frac{-s}{2}\right)'_n + \left(\frac{-s}{2}\right)_n \left(\frac{-s}{2}\right)''_n\right] \frac{z^n}{(n!)^2} \\ G'''_z(s) &= \sum_{n=0}^{\infty} 2\left[\left(\frac{-s}{2}\right)'_n \left(\frac{-s}{2}\right)''_n + \left(\frac{-s}{2}\right)_n \left(\frac{-s}{2}\right)'''_n\right] \frac{z^n}{(n!)^2}. \end{aligned}$$

Ensuite, en évaluant en $s = 0$, nous obtenons le résultat. ■

Nous donnons maintenant la preuve du théorème 83.

Démonstration. Par le théorème de **Akatsuka,** on sait que pour $|a| < 1$,

$$Z(s, x+a) = G_{|a|^2}(s).$$

Nous avons donc

$$m_k(x+a) = \left.\frac{d^k Z(s,x+a)}{ds^k}\right|_{s=0} = G^{(k)}_{|a|^2}(0).$$

On obtient

$$m_2(x+a) = \frac{1}{2}\sum_{n=1}^{\infty}\frac{|a|^{2n}}{n^2}$$

et

$$m_3(x+a) = -\frac{3}{2}\sum_{0<j<n<\infty}\frac{|a|^{2n}}{jn^2}.$$

Pour $|a| > 1$, de même, on sait que par le théorème de **Akatsuka**

$$Z(s, x+a) = |a|^s G_{|a|^{-2}}(s).$$

Nous avons donc

$$m_k(x+a) = \left.\frac{d^k Z(s,x+a)}{ds^k}\right|_{s=0} = \sum_{j=0}^{k}\binom{k}{j}\log^j|a|\, G^{(k-j)}_{|a|^{-2}}(0).$$

On obtient $m_2(x+a)$ et $m_3(x+a)$ en appliquant le lemme 85. ■

On peut utiliser la même méthode pour calculer $m_k(x+a)$ pour $k>3$. Il suffit de continuer à dériver. L'expression $Z^{(k)}(s,x+a)$ ne dépend que de $|a|$. En d'autres termes, l'argument de a n'affecte pas la valeur de $m_k(x+a)$. **Akatsuka** a calculé $m_k(x+a)$ lorsque $|a|<1$ pour $k\geq 2$, comme suit

$$m_k(x+a)=(-1)^k\,k!\sum_{\frac{k}{2}-1\leq n\leq k-2}\frac{1}{2^{2(k-n-1)}}\sum_{(\varepsilon_1,\cdots\varepsilon_n)\in\{1,2\}^n}\mathbf{L}_{(\varepsilon_1,\cdots\varepsilon_n,2)}\left(|a|^{\,2}\right),$$

où

$$\mathbf{L}_{(b_1,\cdots b_h)}(t):=\sum_{0<n_1<\cdots<n_h}\frac{t^{n^h}}{n_1^{b_1}\cdots n_h^{b_h}}$$

3.3.1 Théorèmes de Lalin et Sinha

Comme la question de Lehmer est intéressante pour la mesure de Mahler classique, on pourrait se poser la même question pour la mesure de Mahler supérieure.

La question de Lehmer peut être reformulée pour la mesure de Mahler $k-$supérieure comme suit : le point 0 est-il un point limite pour les mesures m_k ?

Les deux résultats suivants de Lalin et Sinha montrent qu'on a une réponse négative pour k pair et une réponse positive pour k impair.

Théorème 78 *Si $P(x)\in\mathbb{Z}[x]$, n'est pas un monôme, alors pour tout $h\geq 1$*

$$m_{2h}(P)\geq\begin{cases}\left(\dfrac{\pi^2}{12}\right)^h & \textit{si } P(x) \textit{ est réciproque}\\ \left(\dfrac{\pi^2}{48}\right)^h & \textit{si } P(x) \textit{ est non réciproque}\end{cases}$$

Théorème 79 *si $P_n(x)=\dfrac{x^n-1}{x-1}$, pour $h\geq 1$, fixé, alors*

$$\lim_{n\to\infty}m_{2h+1}(P_n)=0.$$

Nous allons démontrer le théorème 86. Pour cela nous donnons quelques résultats préliminaires.

Lemme 80 *Si $P(x)$ est un polynôme dont toutes les racines sont sur le cercle unité, c'est à dire, sous la forme*

$$P(x)=\prod_{j=1}^{n}(x-e^{2\pi i\alpha_j}),$$

avec $0\leq\alpha_j\leq 1$, alors

$$m_2(P)=\frac{\pi^2}{2}\sum_{1\leq j,k\leq n}\left((\alpha_j-\alpha_k)^{\,2}-|\alpha_j-\alpha_k|+\frac{1}{6}\right).$$

Démonstration. En appliquant le lemme 80, nous pouvons exprimer $m_2(P)$ en fonction des arguments α_i :

$$\begin{aligned} m_2(P) &= \sum_{1\le j,k\le n} \left(m\left(1-e^{2\pi i\alpha_j}x, 1-e^{2\pi i\alpha_k}x\right)\right) \\ &= \sum_{1\le j,k\le n} \left(m\left(1-x, 1-e^{2\pi i|\alpha_k-\alpha_j|}x\right)\right) \\ &= \frac{\pi^2}{2}\sum_{1\le j,k\le n}\left(\left(\alpha_j-\alpha_k\right)^2 - |\alpha_j-\alpha_k| + \frac{1}{6}\right). \end{aligned}$$

■

Théorème 81 *Si P est un produit de monômes et de polynômes cyclotomiques, mais pas un seul monôme, alors*

$$m_2(P) \ge \frac{\pi^2}{12}$$

Démonstration. Puisque $\log|x| = 0$ sur le cercle unité, les facteurs monômes ne changent pas la valeur de $m_2(P)$. Ainsi, on peut supposer que $P(x)$ peut s'écrire

$$P(x) = (x-1)^a (x+1)^b \prod_{j=1}^{2n}(x-e^{2\pi i\alpha_j})$$

avec $0 \le \alpha_1 \le \cdots \le \alpha_{2n} \le 1$ et $\alpha_j = 1-\alpha_{2n+1-j}$. Ainsi, $a, b \in \{0,1\}$ puisque nous pouvons avoir un nombre impair de facteurs $x-1$ et / ou $x+1$ dans le produit.

En utilisant que $m(x-1,x+1) = -\dfrac{\pi^2}{24}$ et d'après le lemme 88, on obtient

$$\begin{aligned}
m_2(P) &= am_2(x-1) + bm_2(x+1) + 2abm(x+1,x-1) \\
&\quad +2am\left(x-1, \prod_{j=1}^{2n}(x-e^{2\pi i\alpha_j})\right) + 2bm\left(x+1, \prod_{j=1}^{2n}(x-e^{2\pi i\alpha_j})\right) \\
&\quad +m_2\left(\prod_{j=1}^{2n}(x-e^{2\pi i\alpha_j}\right) \\
&= \frac{\pi^2}{2}\left(\frac{a+b-ab}{6} + 2a\sum_{j=1}^{2n}\left({\alpha_j}^2 - \alpha_j + \frac{1}{6}\right)\right. \\
&\quad +2b\sum_{j=1}^{2n}\left(\left(\alpha_j - \frac{1}{2}\right)^2 - \left|\alpha_j - \frac{1}{2}\right| + \frac{1}{6}\right) + 4n\sum_{j=1}^{2n}\alpha_j^2 \\
&\quad \left. - \sum_{1\le j,k\le 2n}(2\alpha_j\alpha_j + |\alpha_j - \alpha_j|) + \frac{2n^2}{3}\right) \\
&= \frac{\pi^2}{2}\left(\frac{a+b-ab}{6} + 2\,(a+b)\sum_{j=1}^{2n}\alpha_j^2 - 2a\sum_{j=1}^{2n}\alpha_j - 4b\sum_{j=n+1}^{2n}\alpha_j + bn\right. \\
&\quad +4n\sum_{j=1}^{2n}\alpha_j^2 - 2\sum_{1\le j,k\le 2n}\alpha_j\alpha_k - 2\sum_{j=1}^{2n}j\alpha_j + 2\sum_{j=1}^{2n}(2n+1-j)\,\alpha_j \\
&\quad \left. +\frac{2n(n+a+b)}{3}\right)
\end{aligned}$$

Puisque $\alpha_j = 1 - \alpha_{2n+1-j}$, et que nous avons $\sum_{j=1}^{2n}\alpha_j = n$. Donc

$$\begin{aligned}
m_2(P) &= \frac{\pi^2}{2}\left(2(a+b+2n)\sum_{j=1}^{2n}\alpha_j^2 - 4b\sum_{j=n+1}^{2n}\alpha_j - 4\sum_{j=1}^{2n}j\alpha_j\right. \\
&\quad \left. + 2n(n+1) + \frac{n(2n-4a+5b)}{3} + \frac{a+b-ab}{6}\right).
\end{aligned}$$

Soit $\alpha := \alpha_j$ avec $1 \le j \le n$ et $0 \le \alpha \le \dfrac{1}{2}$. Posons

$$\begin{aligned}
g(\alpha) &: = 2(a+b+2n)(\alpha^2 + (1-\alpha)^2) - 4(j\alpha + (2n+1-j+b)(1-\alpha)) \\
&= 4(a+b+2n)\alpha^2 + 4(1-2j-a)\alpha + 4j + 2a - 2b - 4n - 4.
\end{aligned}$$

Puisque nous avons une équation quadratique, le minimum de $g(\alpha)$ est obtenu en

$$\alpha = \frac{a+2j-1}{2(a+b+2n)}.$$

Donc

$$g(\alpha) \geq -\frac{(a+2j-1)^2}{a+b+2n} + 4j + 2a - 2b - 4n - 4.$$

Nous utilisons la borne de $g(\alpha)$ afin d'obtenir

$$\begin{aligned}
\frac{2}{\pi^2} m_2(P) &\geq \sum_{j=1}^{n} \left(-\frac{(a+2j-1)^2}{a+b+2n} + 4j + 2a - 2b - 4n - 4 \right) \\
&\quad +2n(n+1) + \frac{n(2n-4a+5b)}{3} + \frac{a+b-ab}{6} \\
&= \sum_{j=1}^{n} \left(-\frac{4j^2}{a+b+2n} + \frac{4(a+2n+1)j}{a+b+2n} - \frac{(a-1)^2}{a+b+2n} \right) \\
&\quad -\frac{n(4n-2a+b+6)}{3} + \frac{a+b-ab}{6} \\
&= -\frac{2n(n+1)(2n+1)}{3(a+b+2n)} + \frac{2(b+2n+1)n(n+1)}{a+b+2n} - \frac{(a-1)^2}{a+b+2n} \\
&\quad -\frac{n(4n-2a+b+6)}{3} + \frac{a+b-ab}{6} \\
&= \frac{2n(n+1)(3b+4n+2)}{3(a+b+2n)} - \frac{(a-1)^2}{a+b+2n} \\
&\quad -\frac{n(4n-2a+b+6)}{3} + \frac{a+b-ab}{6} \\
&= \frac{1}{6},
\end{aligned}$$

où la dernière égalité est valide pour $a, b \in \{0,1\}$. Donc

$$m_2(P) \geq \frac{\pi^2}{12} \cong 0.8224670334\cdots$$

■

Théorème 82 *Si $P(x) \in \mathbb{Z}[x]$ est réciproque, alors*

$$m_2(P) \geq \frac{\pi^2}{12}.$$

Pour la preuve de ce théorème, nous utiliserons la proposition suivante.

Proposition 83 *Soit $\tau_1, \ldots, \tau_M$ des nombres réels fixés dans $[0,1]$ et $c_1, \ldots, c_M > 0$. La fonction*

$$f(y_1, \ldots y_M) = \sum_{j=1}^{M} c_i \sum_{n=1}^{\infty} \frac{y_j^n \cos(2\pi n \tau_i)}{n^2}$$

atteint son minimum dans $[0,1]$ à un point où $y_i \in \{0,1\}$ pour chaque i.

Démonstration. Pour $\tau \in [0,1]$, fixé, on étudie d'abord la fonction

$$g(y) = \sum_{n=1}^{\infty} \frac{y^n \cos(2\pi n\tau)}{n^2}$$

dans l'intervalle $[0,1]$. Dans cet intervalle, $g(y)$ atteint son minimum, soit aux extrémités de l'intervalle où quand $g'(y) = 0$. Cependant,

$$g'(y) = \frac{1}{y}\sum_{n=1}^{\infty} \frac{y^n \cos(2\pi n\tau)}{n} = -\frac{1}{y}\log\left|1 - ye^{2\pi i\tau}\right|.$$

Ainsi, nous obtenons un point critique quand $|1 - ye^{2\pi i\tau}| = 1$, c'est à dire quand

$$(1 - y\cos(2\pi\tau))^2 + (y\sin(2\pi\tau))^2 = 1,$$

et donc, $y_0 = 2\cos(2\pi\tau)$. Nous devons déterminer la nature du point y_0.
Remarquons que

$$g''(y) = \frac{1}{y^2}\log\left|1 - ye^{2\pi i\tau}\right| + \frac{1}{y^2}\operatorname{Re}\left(\frac{ye^{2\pi i\tau}}{1 - ye^{2\pi i\tau}}\right).$$

donc,

$$g''(y_0) = \frac{1}{y_0^2}\operatorname{Re}\left(y_0 e^{2\pi i\tau}(1 - y_0 e^{-2\pi i\tau})\right) = \frac{1}{y_0^2}\left(y_0\cos(2\pi\tau) - y_0^2\right) = -\frac{1}{2} < 0.$$

D'où y_0 est un point maximal (local) pour $g(y)$. Donc, le minimum pour $g(y)$ dans $[0,1]$ est soit à $y = 0$ où à $y = 1$. Puisque chaque $c_i > 0$, on conclut que, dans l'intervalle $[0,1]^M$, $f(y_1, ..., y_M)$ atteint son minimum en un point où chaque y_i est soit 0 ou 1. ■

Remarque 84 *D'après ce qui précède, on déduit également que si* $f(y_1, ..., y_M) \geq f(a_1, ..., a_M)$ *pour toutes* $(y_1, ..., y_M) \in (0,1)^M$, *alors chaque* $a_i \in \{0,1\}$.

Nous donnons la preuve du théorème 90.

Démonstration. Soit $P(x) \in \mathbb{Z}[x]$, un polynôme réciproque. Si P n'est pas unitaire, on peut écrire $P(x) = CQ(x)$ avec $C \in \mathbb{Z}$ et

$$m_2(P) = \log^2 C + 2\log C m(Q) + m_2(Q) \geq m_2(Q),$$

où nous supposons que $C \geq 1$ dans l'inégalité.
On peut donc supposer que P est unitaire. Ainsi, nous écrivons

$$P(x) = (x-1)^a(x+1)^b\prod_{j=1}^{J}(x - r_j)(x - r_j^{-1}),$$

où $|r_j| \leq 1$. Posons $r_j = \rho_j e^{2\pi i \mu j}$ avec $0 \leq \rho_j \leq 1$. Ici, nous devons préciser que pour $\rho_j = 0$, le produit $(x - r_j)\left(x - r_j^{-1}\right)$ doit être interprété comme le produit $x.1$. Il est important de faire remarquer que la remarque 81 est encore valable dans ces cas puisque $\mathbf{Li}_2(0) = 0$. De plus le fait que $a, b \in \{0, 1\}$ nous permet d'avoir un nombre impair de facteurs $x - 1$ et /ou $x + 1$ dans le produit. Donc

$$\begin{aligned} m_2(P) &= am_2(x-1) + bm_2(x+1) + 2abm(x+1, x-1) \\ &\quad +2a\sum_{j=1}^{J} m(x-1, x-r_j) \\ &\quad +2b\sum_{j=1}^{J} m(x-1, x-r_j^{-1}) + \sum_{1\leq j_1,\ j_2\leq J} m(x-r_{j_1}, x-r_{j_2}) \\ &\quad + \sum_{1\leq j_1,\ j_2\leq J} m(x-r_{j_1}^{-1}, x-r_{j_2}^{-1}) + 2\sum_{1\leq j_1,\ j_2\leq J} m(x-r_{j_1}, x-r_{j_2}^{-1}). \end{aligned}$$

En utilisant que $m(x+1, x-1) = -\dfrac{\pi^2}{24}$ et en appliquant la remarque 81,

$$\begin{aligned} m_2(P) &= (a+b-ab)\frac{\pi^2}{12} + (a+b)\sum_{j=1}^{J} \operatorname{Re}\mathbf{Li}_2(r_j) \\ &\quad + \sum_{1\leq j_1,\ j_2\leq J} \left(2\operatorname{Re}\mathbf{Li}_2(r_{j_1}\overline{r_{j_2}}) + \log|r_{j_1}|\log|r_{j_2}|\right). \end{aligned}$$

En écrivant le dilogarithme en termes de série, nous obtenons

$$\begin{aligned} m_2(P) &= (a+b-ab)\frac{\pi^2}{12} + m(P)^2 + (a+b)\sum_{j=1}^{J}\sum_{n=1}^{\infty} \frac{\rho_j^n \cos(2\pi n\mu_j)}{n^2} \\ &\quad +2\sum_{1\leq j_1,\ j_2\leq J}\sum_{n=1}^{\infty} \frac{\rho_{j_1}^n \rho_{j_2}^n \cos(2\pi n(\mu_{j_1} - \mu_{j_2}))}{n^2}. \end{aligned}$$

Ainsi, le problème de minimiser $m_2(P)$ réduit le problème de minimisation des termes dans l'expression ci-dessus. Premièrement fixons les arguments μ_j. À la suite de la Proposition 91 et la remarque 92, nous remarquons que le dernier terme impliquant une série atteint son minimum lorsque $\rho_j \in \{0, 1\}$ .Cette condition minimise également l'autre terme impliquant une série, bien que ce terme peut être ignoré si $a = b = 0$. Cela signifie qu'il n'y a pas de racines ayant une valeur absolue supérieure à 1. Cela minimise également le premier terme de $m_2(P)$ qui est positif pour $P(x)$ unitaire et un zéro si la valeur absolue de toutes les racines de $P(x)$ sont (inférieure ou) égale à 1. Maintenant, si les arguments μ_j varient, $m_2(P)$ a atteint son minimum lorsque toutes les racines ont une valeur absolue dans $\{0, 1\}$. Puisque P est réciproque et ses racines ont une valeur absolue égale 1, nous pouvons appliquer le théorème 89 et conclure

que

$$m_2(P) \geq \frac{\pi^2}{12}.$$

■

Lemme 85 *Si $f(x) \in \mathbb{Z}[x]$ est non réciproque, alors*

$$m_2(P) \geq \frac{\pi^2}{48}$$

Démonstration. Soit $d = degP$, et posons

$$Q(x) = x^d P(x^{-1}).$$

Ainsi $P(x)Q(x) \in \mathbb{Z}[x]$ est réciproque. De plus, $m_2(P) = m_2(Q) = m(P,Q)$ et

$$m_2(PQ) = m_2(P) + 2m(P,Q) + m_2(Q) = 4m_2(P).$$

Nous obtenons le résultat en appliquant le théorème 90 à PQ. ■

Nous allons utiliser la borne de $m_2(P)$ afin de trouver une borne pour $m_{2h}(P)$.

Proposition 86 *Pour tout polynôme non nul $P(x) \in \mathbb{Z}[x]$,*

1.

$$m_{2h}(P) \geq m_2(P)^h$$

2.

$$m_{2h}(P) \geq m(P)^{2h}$$

Démonstration. Partie 1. Soit h un entier positif et f et g des fonctions telles que

$$\frac{1}{2\pi i}\int_{|x|=1} |f|^h \frac{dx}{x} < \infty \text{ et } \frac{1}{2\pi i}\int_{|x|=1} |g|^{h/h-1} \frac{dx}{x} < \infty.$$

En utilisant l'inégalité de Hölder, nous obtenons

$$\left(\frac{1}{2\pi i}\int_{|x|=1} |fg| \frac{dx}{x}\right)^h \leq \left(\frac{1}{2\pi i}\int_{|x|=1} |f|^h \frac{dx}{x}\right) \times \left(\frac{1}{2\pi i}\int_{|x|=1} |g|^{h/h-1} \frac{dx}{x}\right)^{h-1} \quad (*).$$

En particulier, en prenant $f(x) = \log^2 |P(x)|$ et $g(x) = 1$, nous obtenons

$$m_2(P)^h \leq m_{2h}(P).$$

Partie 2. D'autre part, en prenant $f(x) = \log|P(x)|$ et $g(x) = 1$, en prenant $2h$ au lieu de h dans $(*)$, nous obtenons

$$m(P)^{2h} \leq m_{2h}(P).$$

■

Enfin la preuve du théorème 86.

Démonstration. En associant le théorème 90, lemme 93, et la partie 1 de la proposition 95, on obtient,

$$m_{2h}(P) \geq m_2(P)^h \geq \begin{cases} \left(\frac{\pi^2}{12}\right)^h & \text{, si } P(x) \text{ est réciproque} \\ \left(\frac{\pi^2}{48}\right)^h & \text{, si } P(x) \text{ est non réciproque.} \end{cases}$$

■

Conclusion

La mesure de Mahler est apparue pour la première fois en 1933 dans un article de Lehmer [10]. Elle doit son nom à Kurt Mahler qui l'introduisit sous une forme équivalente en 1961 dans ses travaux sur la transcendance [24]. Elle trouve ses applications en théorie ergodique, théorie des noeuds et théorie des nombres. Elle est, en particulier, connue pour son rôle dans le problème de Lehmer, un problème encore ouvert aujourd'hui.

Bibliographie

[1] D.W.Boyd, Kronecker's Theorem and Lehmer's Problem for Polynomials in several Variables, J.Number Theory 13 (1981),116-121.

[2] D.W.Boyd, Mahler's Measure and Special Values of L-functions Experimental Mathematics 7, (1998),p.37-82.

[3] D.W.Boyd, Reciprocal polynomials having small measure, Math. Comp.35(1980), 1861-1877.

[4] D.W.Boyd, Speculations concerning the Range of Mahler's Measure, Canada. Math. Bull. 24 (1981), 453-469.

[5] Kronecker's theorem and Lehmer's problem for polynomials in several variables, J. Number Theory 13 (1981), 116-121.

[6] S.Boughzala, Mesure de Mahler de Polynômes de deux variables, Thèse de Doctorat de l'Université Paris VI, (Décembre 2000).

[7] S.Boughzala, Mesure de Mahler d'une famille de polynômes de deux variables, Publicationes Mathematicae Debrecen, Vol.: 68, Fasc.: 1-2, 2006.

[8] L.Benferhat, Variations sur la mesure de Mahler de polynômes de deux variables, Thèse de Doctorat d'Etat, Décembre 2010.

[9] L.Benferhat, Mahler Measure and Integrals of Hypergeometric Functions, JP Journal of Algebra, Number Theory and Applications, Volume 12, Number 1, 2008, Pages 49-59.

[10] D.H. Lehmer, Factorization of certain cyclotomic functions, Ann. of Math. (2), 34 (1933), 461-479.

[11] M. Lalin, Some exemples of Mahler measures as multiple polylogarithms, J.Number Theory, 103 (2003), n°.(1), 85-108.

[12] M. Lalin, On certain Combination of coloured multizeta Values. J. Ramanujan, Math.Soc.20(1): 115-127, 2006.

[13] M. Lalin, Mahler measure of some n-variable polynomial families. J. Number Theory, 116(1) : 102-139, 2006.

[14] M. Lalin, Higher Mahler measure for cyclotomic polynomials and Lehmer's question, Université de Montréal - Canada , Mathémathics Subject classification (2000) 11R06. 11r09. 11C08. 11Y35.

[15] C.J. Smyth, On measures of polynomials in several variables, Bull. Doc 23(1)(1981), 19-63.

[16] C.J. Smyth, The Mahler measure of algebraic number: a survey. Number theory and polynomials, London Math.Soc. Lecture Note Ser, 352:322-349, 2008.

[17] C.J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, Bull. London Math. Soc. (1971), 169-175.

[18] M.J. Bertin, Mesure de Mahler d'une famille de polynômes, J.reine angew. Math. 569 (2004), 175-188.

[19] J.S. Lechasseur, Mesure de Mahler supérieure de certaines fonctions rationnelles, Mémoire pour l'obtention du grade Maître ès sciences, Août 2012.

[20] Z.Issa, A Generalization of a Theorem of Boyd and Lawton, Mémoire pour l'obtention du grade de Maîtrise en sciences, Mai 2012.

[21] H. Davenport, Multiplicative number theory, publié par les editions Springer Verlag, Berlin Heidelberg New Yourk 1967, §4-5 pp 27-42.

[22] T.M. Apostol, Introduction to analytic number theory. Springer- Verlag, New Yourk 1976. Under graduate Textes in Mathematics.

[23] D.A. Burgess, Dirichlet characters and polynomials, Proc. steklov Inst. Math, 132 (1975), 234-236 Trudy Mat. Inst steklov, 132 (1973)pp 203-205.

[24] K. Mahler, On some inequalities for polynomials in several variables. J. London Math. Soc., 37:341-344, 1962.

[25] N. Kurokawa; M. Lalin; H. Ochiai, Higher Mahler measures and Zeta functions. Acta Arith. 135 (2008), no. 3, 269-297.

[26] M.Lalin; K.Sinha. Higher Mahler measure for cyclotomic polynomials and Lehmer's question. Ramanujan J.26 (2011), no. 2,257-294.

[27] G.Tenenbaum, Introduction à la théorie analytique et probabiliste des nombres, Mai 1990.

[28] W.M. Lawton, A generalization of a theorem of Kronecker, J. Sci. Fac. of Chiang Mai Univ. 4 (1977), 15-23.

[29] C.Douche, Mesures de Mahler et racines réelles de certaines familles de polynômes, Thèse de Doctorat de l'Université Bourdeaux I, (21 Juin 2000).