Magistère de Cachan 1995-1996.
Mémoire de première année.

LES SERIES DE DIRICHLET

Par Mathieu COLIN

Sous la direction de Pascal BOYER

Le but de ce mémoire est d'utiliser les séries de Dirichlet pour démontrer un certain nombre de résultats. Celles-ci interviennent en effet dans beaucoup de domaines de la théorie des nombres et sont souvent source de démonstrations élégantes. Nous calculerons le nombre de classes d'idéaux d'un corps cyclotomique. Nous démontrerons aussi au passage le théorème de Dirichlet sur la densité des nombres premiers dans une progression arithmétique. Enfin, nous verrons quel est le lien entre le nombre de classes d'idéaux d'un corps de nombres et un cas simple du théorème de Fermat. Nous donnerons pour finir un critère de régularité pour les nombres premiers.

I INTRODUCTION

I.1 Définition

Définition I.1.1 *Soit $K/\mathbb{Q}$ une extension de corps de degré fini. Un nombre algébrique est une racine dans $\mathbb{C}$ d'un polynôme $\sum a_i X^i$, où $a_i \in \mathbb{Z}$. Un entier algébrique est une racine dans $\mathbb{C}$ d'un polynôme $X^n + \sum a_i X^i$. L'ensemble des entiers algébriques, noté O_K, s'appelle l'anneau des entiers algébriques.*

Définition I.1.2 *Soit v un élément de K. Soit M_v l'application de K dans K définie par $M_v(x) = x * v$. On définit la norme de v par*

$$N(v)_{K|\mathbb{Q}} = \det(M_v).$$

La trace de v est définie par

$$Tr(v) = \mathrm{trace}(M_v).$$

La norme est multiplicative et la trace est additive.

Définition I.1.3 *Soit $w_1, ..., w_n$ des éléments de K. On appelle discriminant de la famille (w_i) le scalaire*

$$\delta(w_1, ..., w_n) = \det((Tr(w_i * w_j))_{1 \leq i,j \leq n}).$$

Proposition I.1.1 *Le discriminant prend ses valeurs dans $\mathbb{Z}$.*

I.2 Premiers Résultats

Lemme I.2.1 *Soient $w_1, ..., w_n$ des éléments de K. Alors $w_1, ..., w_n$ est une base de K si et seulement si $\delta(w_1, ..., w_n) \neq 0$.*

Supposons $w_1, ..., w_n$ linéairement dépendants. Il existe $(a_i)_{1 \leq i \leq n}$ non tous nuls tel que $\sum a_i * w_i = 0$. Dans une base de K, il existe alors un vecteur qui est combinaison linéaire de tous les autres. Ainsi, $\delta(w_1, ..., w_n) = 0$.

Réciproquement, si $w_1, ..., w_n$ est une base de K et si $\delta(w_1, ..., w_n) = 0$, alors le système

$$(\sum_{i=1}^{n} a_i Tr(w_i * w_j) = 0)_{1 \leq j \leq n}$$

admet une solution non triviale. Ainsi il existe

$$v = \sum_{i=1}^{n} a_i w_i \neq 0$$

tel que

$$Tr(v * w_i) = 0, \ \ \forall \ 1 \leq i \leq n.$$

D'où, $\forall x \in K$ on a

$$Tr(v * x) = 0.$$

En particulier, pour $x = v^{-1}$ $\quad Tr(1) = 0$, ce qui est impossible car la caractéristique de K est nulle.

Lemme I.2.2 *Soit $\mathcal{I}$ un idéal de O_K. Alors $\mathcal{I}$ contient une base de K.*

Soit v un nombre algébrique et

$$P(X) = \sum_{i=1}^{n} a_i X^i$$

son polynôme annulateur. On a $a_n^n * v^n + a_{n-1} * a_n^{n-1} * v^{n-1} + ... + a_0 * a_n^{n-1} = 0$. Ainsi $w = a_n * v$ est un entier algébrique.

Soient $v_1, ..., v_n$ une base de K. Il existe $(a_i) \in \mathbb{Q}$ tel que $a_1 * v_1, ..., a_n * v_n$ soient des entiers algébriques. Soit $a = ppcm(a_i)$. Les éléments $a * v_1, ..., a * v_n$ sont aussi des entiers algébriques. Si $v \neq 0$ et $v \in \mathcal{I}$, $a * v * v_1, ..., a * v * a_n$ est alors une base de K incluse dans $\mathcal{I}$.

Proposition I.2.1 *Soit $\mathcal{I}$ un idéal de O_K. Il existe $v_1, ..., v_n \in \mathcal{I}$ tel que $\mathcal{I} = \mathbb{Z}v_1 \oplus .. \oplus \mathbb{Z}v_n$.*

On choisit parmi les bases de K sur $\mathbb{Q}$ contenues dans $\mathcal{I}$ une base dont le discriminant est minimal en valeur absolue: $v_1, ..., v_n$. Soit $v \in \mathcal{I}$, $v = \sum a_i * v_i$. On veut montrer que $\forall \ 1 \leq i \leq n$, $a_i \in \mathbb{Z}$. Supposons $a_1 \notin \mathbb{Z}$, on écrit alors $a_1 = (a_1) + [a_1]$ où (a_1) désigne la partie entière de a_1 et $[a_1]$ sa partie fractionnaire. Soit

$$w = [a_1] * v_1 + \sum_{i=2}^{n} a_i * v_i.$$

Soit P la matrice de passage de la base $w, v_2, ..., v_n$ dans la base $v_1, ..., v_n$. On a $det(P) < 1$. De plus $\delta(w, v_2, ..., v_n) = det(P)^2 * \delta(v_1, ..., v_n)$. Cela contredit la minimalité de $v_1, ..., v_n$.

Définition I.2.1 *En posant $O_K = \mathbb{Z}v_1 \oplus ... \oplus \mathbb{Z}v_n$, on définit le discriminant de K comme étant égale à $|\delta(v_1, ..., v_n)|$.*

Proposition I.2.2 *Soit $\mathcal{I}$ un idéal de K. Alors $O_K/\mathcal{I}$ est de cardinal fini. O_K est alors noethérien. C'est un anneau de Dedekind.*

On admettra ce résultat.

I.3 Norme d'un idéal

Proposition I.3.1 *Soient A un anneau commutatif, $\mathcal{I}_1, ..., \mathcal{I}_r$ des idéaux de A premiers entre eux tel que $\forall\ i \neq j \quad \mathcal{I}_i + \mathcal{I}_j = A$. Alors*

$$A/(\mathcal{I}_1 ... \mathcal{I}_r) \simeq A/\mathcal{I}_1 \oplus ... \oplus A/\mathcal{I}_r.$$

Etablissons d'abord le résultat pour $r = 2$.

$$\mathcal{I}_1 + \mathcal{I}_2 = A \Longrightarrow \mathcal{I}_1 \cap \mathcal{I}_2 = \mathcal{I}_1 \mathcal{I}_2.$$

Ce résultat est évident. Considérons maintenant l'application

$$\begin{aligned} S :\ & A \to A/\mathcal{I}_1 \oplus A/\mathcal{I}_2 \\ & a \to (a + \mathcal{I}_1, a + \mathcal{I}_2). \end{aligned}$$

Elle est surjective. En effet

$$\mathcal{I}_1 + \mathcal{I}_2 = A \Longrightarrow \exists (x_1, x_2) \in \mathcal{I}_1 \cap \mathcal{I}_2 \ \ tel \ \ que \ \ x_1 + x_2 = 1.$$

Soient $(y_1, y_2) \in A/\mathcal{I}_1 \cap A/\mathcal{I}_2$. Posons $y = y_1 x_1 + y_2 x_2$. On a alors

$$S(y) = (y_1, y_2).$$

Donc S est surjective. De plus son noyau est égal à $\mathcal{I}_1 \cap \mathcal{I}_2 = \mathcal{I}_1 \mathcal{I}_2$. Le résultat est ainsi acquis pour $r = 2$. La démonstration se termine par récurrence. $\mathcal{I}_1, ..., \mathcal{I}_r$ premiers entre eux assure

$$(\mathcal{I}_1 + \mathcal{I}_2)(\mathcal{I}_1 + \mathcal{I}_3) ... (\mathcal{I}_1 + \mathcal{I}_r) = A$$

c'est-à-dire

$$\mathcal{I}_1 + \mathcal{I}_2 ... \mathcal{I}_r = A.$$

Une récurrence immédiate montre que

$$\mathcal{I}_1 \cap \mathcal{I}_2 \cap ... \cap \mathcal{I}_r = \mathcal{I}_1 ... \mathcal{I}_r.$$

Si

$$A/(\mathcal{I}_2...\mathcal{I}_r) \simeq A/\mathcal{I}_2 \oplus ... \oplus A/\mathcal{I}_r$$

alors le résultat établi pour $r = 2$ permet de conclure que

$$A/(\mathcal{I}_1...\mathcal{I}_r) \simeq A/\mathcal{I}_1 \oplus ... \oplus A/\mathcal{I}_r.$$

Proposition I.3.2 *Dans O_K, tout idéal $\mathcal{I}$ se décompose sous la forme*

$$\mathcal{I} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}...\mathcal{P}_r^{e_r}$$

où $\mathcal{P}_1, ..., \mathcal{P}_r$ sont des idéaux premiers.

On dispose maintenant de tous les éléments pour définir la norme d'un idéal $\mathcal{I}$ de O_K. La proposition **I.3.1** assure

$$O_K/\mathcal{I} \simeq O_K/\mathcal{P}_1^{e_1} \oplus ... \oplus O_K/\mathcal{P}_r^{e_r}.$$

Or $\forall\ 1 \leq i \leq r$ $\mathcal{P}_i \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, donc de la forme $p_i\mathbb{Z}$ avec p_i nombre premier. De plus, $O_K/\mathcal{P}_i$ est fini et $|O_K/\mathcal{P}_i| = p_i^{f_i}$ où f_i s'appelle le degré résiduel de $\mathcal{P}_i$. Une récurrence immédiate montre alors que $|O_K/\mathcal{P}_i^{e_i}| = p_i^{e_i f_i}$. On a ainsi

$$|O_K/\mathcal{I}| = \prod_{i=1}^{n} |O_K/\mathcal{P}_i^{f_i}| = \prod_{i=1}^{n} p_i^{e_i f_i}.$$

Définition I.3.1 *La norme d'un idéal $\mathcal{I}$ est*

$$N(\mathcal{I}) = \prod_{i=1}^{n} |O_K/\mathcal{P}_i^{f_i}|.$$

Proposition I.3.3 *La norme ainsi définie est multiplicative.*

Soient

$$\mathcal{I} = \prod \mathcal{P}_i^{e_i} \quad et \quad \mathcal{J} = \prod \mathcal{P}_i^{e_i^{'}}.$$

Alors

$$\mathcal{I}\mathcal{J} = \prod \mathcal{P}_i^{e_i + e_i^{'}}$$

et

$$N(\mathcal{I}\mathcal{J}) = \prod p_i^{e_i f_i + e_i^{'} f_i^{'}} = N(\mathcal{I})N(\mathcal{J}).$$

Proposition I.3.4 *Soit $p \in \mathbb{Z}$ premier. $pO_K = \mathcal{P}_1^{e_1}...\mathcal{P}_r^{e_r}$. Notons f_i le degré résiduel de $\mathcal{P}_i$. On a*

$$\sum_{i=1}^{r} e_i f_i = n.$$

I.4 Classe de diviseurs de K

Définition I.4.1 *Soient* $\mathcal{I}, \mathcal{J}$ *deux idéaux de* O_K. *On dit que* $\mathcal{I}$ *est équivalent à* $\mathcal{J}$*,et on note* $\mathcal{I} \sim \mathcal{J}$, *s'il existe* $x \in O_K$ *et* $y \in O_K$ *tel que* $\mathcal{I}x = \mathcal{J}y$.

Proposition I.4.1 *La relation* $\sim$ *est une relation d'équivalence.*

Théorème I.4.1 *Soit* h_f *le nombre de classe d'équivalence de cette relation. On a* $h_f < \infty$.

II LA FONCTION ZETA DE DEDEKIND

La recherche du nombre h de classes de diviseurs d'un corps K de nombres algébriques repose sur l'examen de la fonction suivante, appelée *fonction Zêta de Dedekind*

$$\zeta_K(s) = \sum_{\mathcal{A} \subset O_K} \frac{1}{N(\mathcal{A})^s}.$$

Nous allons d'abord étudier le cas où $K = \mathbb{Q}$. La fonction Zêta s'appelle alors la fonction Zêta de Riemann, et est en fait un cas particulier des fonctions dites de Dirichlet.

II.1 Séries de Dirichlet.

II.1.1 Lemmes

Lemme II.1.1 *Soit* U *un ouvert de* $\mathbb{C}$, *et* f_n *une suite de fonctions holomorphes sur* U *qui convergent uniformément sur tout compact vers une fonction* f. *La fonction* f *est alors holomorphe dans* U, *et les dérivées* f_n' *des fn convergent uniformément sur tout compact vers la dérivée* f' *de* f.

La démonstration repose sur la formule de Cauchy. Soit D un disque fermé contenu dans U, et soit C son bord orienté, alors on a

$$f_n(z_0) = \int_C \frac{f_n(z)}{z - z_0} dz, \quad \forall\ z_0 \text{ intérieur à D.}$$

Lemme II.1.2 *Soient* (a_n) *et* (b_n) *deux suites. Notons*

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

On a alors

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

Lemme II.1.3 *Soient α et β deux nombres réels, avec $0 < \alpha < \beta$. Soit z=x+iy, avec x,$y \in \mathbb{C}$ et $x > 0$. On a*

$$\mid e^{-\alpha z} - e^{-\beta z} \mid \ \leq \ \mid \frac{z}{x} \mid (e^{-\alpha x} - e^{-\beta x}).$$

On a

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt$$

d'où en passant aux valeurs absolues

$$\mid e^{-\alpha z} - e^{-\beta z} \mid \ \leq \ \mid z \mid \int_{\alpha}^{\beta} e^{-tx} dt = \frac{\mid z \mid}{x}(e^{-\alpha x} - e^{-\beta x}).$$

II.1.2 Séries de Dirichlet

On se donne une suite de réels positifs strictement croissante (λ_n). On appelle série de Dirichlet d'exposants (λ_n) une série de la forme

$$\sum a_n e^{-\lambda_n z} \quad (a_n \in \mathbb{C}, z \in \mathbb{C}).$$

Proposition II.1.1 *Si la série $f(z) = \sum a_n e^{-\lambda_n z}$ converge pour $z = z_0$, elle converge uniformément dans tout domaine de la forme $Re(z - z_0) \geq 0$, $\mid Arg(z - z_0) \mid \leq \alpha$, avec $\alpha < \pi/2$.*

On se ramène à $z_0 = 0$. On suppose donc que la série $\sum a_n$ est convergente. Il faut prouver la convergence uniforme sur tout domaine de la forme

$$Re(z) \geq 0, \quad \frac{\mid z \mid}{Re(z)} \leq k.$$

Ainsi, soit $\varepsilon > 0$ fixé. $\exists N$ tel que si $m, m' \geq N$, on ait $A_{m,m'} \leq \varepsilon$. D'après le lemme **II.1.2**, on a

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

En posant $z = x + iy$, et en appliquant le lemme **II.1.3**, on trouve (pour $m, m' \geq N$)

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

c'est-à-dire

$$| S_{m,m'} | \leq \varepsilon(1 + k(e^{-\lambda_m x} - e^{-\lambda_{m'} x}))$$

d'où

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

et la convergence uniforme est immédiate.

Proposition II.1.2 *Si f converge pour $z = z_0$, elle converge pour $Re(z) > Re(z_0)$, et la fonction ainsi définie est holomorphe.*

Cela résulte de la proposition **II.2.6** et du lemme **II.1.1**.

Proposition II.1.3 *L'ensemble de convergence de la série f contient un demi-plan ouvert maximal (appelé demi-plan de convergence).*

Proposition II.1.4 *$f(z)$ converge vers $f(z_0)$ lorsque $z \to z_0$, en restant dans le domaine $Re(z - z_0) \geq 0$, $| Arg(z - z_0) | \leq \alpha$, avec $\alpha < \pi/2$.*

Proposition II.1.5 *La fonction f ne peut être identiquement nulle que si tous les coefficients a_n sont nuls.*

II.1.3 Séries de Dirichlet à coefficients positifs.

Proposition II.1.6 *Soit $f(z) = \sum a_n e^{-\lambda_n z}$ une série de Dirichlet dont tous les coefficients sont réels positifs ou nuls. Supposons que f converge pour $Re(z) > \rho$, avec $\rho \in \mathbb{R}$, et que la fonction f puisse être prolongée analytiquement en une fonction holomorphe au voisinage de $z = \rho$. Il existe alors un nombre $\varepsilon > 0$ tel que f converge pour $Re(z) > \rho - \varepsilon$.*

On se ramène a $\rho = 0$. Comme f est holomorphe sur un voisinage de 0 et pour $Re(z) > 0$, elle l'est aussi dans un disque $\mid z - 1 \mid \leq 1 + \varepsilon$. Sa série de Taylor converge dans ce disque. Le lemme **II.1.6** assure que

$$f^{(p)}(z) = \sum a_n (-\lambda_n)^p e^{-\lambda_n z} \quad pour \quad Re(z) > 0,$$

d'où

$$f^{(p)}(1) = (-1)^p \sum \lambda_n^p a_n e^{-\lambda_n}.$$

La série de Taylor s'écrit alors

$$f(z) = \sum_{p=0}^{\infty} \frac{1}{p!} (z-1)^p f^{(p)}(1), \qquad \mid z - 1 \mid \leq 1 + \varepsilon.$$

Pour $z = -\varepsilon$, on a

$$f(-\varepsilon) = \sum_{p=0}^{\infty} \frac{1}{p!} (1+\varepsilon)^p (-1)^p f^{(p)}(1),$$

la série étant bien convergente.

Or $(-1)^p f^{(p)}(1)$ est une série convergente à termes positifs. Il vient donc que la série double à termes positifs

$$f(-\varepsilon) = \sum_{n,p} a_n \frac{1}{p!} (1+\varepsilon)^p \lambda_n^p e^{-\lambda_n}$$

converge. Or, en regroupant les termes, on peut l'écrire

$$\begin{aligned} f(-\varepsilon) &= \sum_n a_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{1}{p!} (1+\varepsilon)^p \lambda_n^p \\ &= \sum_n a_n e^{-\lambda_n} e^{\lambda_n} (1+\varepsilon) \\ &= \sum_n a_n e^{\lambda_n \varepsilon} \end{aligned}$$

ce qui montre que la série de Dirichlet donnée converge pour $z = -\varepsilon$, donc aussi pour $Re(z) > -\varepsilon$.

II.1.4 Séries de Dirichlet proprement dites.

On va étudier le cas $\lambda_n = \text{Log } n$. Les séries correspondantes s'écrivent alors

$$f(s) = \sum_{n=1}^{\infty} a_n/n^s.$$

Proposition II.1.7 *Si les a_n sont bornés, il y a convergence absolue pour $Re(z) > 1$.*

Proposition II.1.8 *Si les sommes partielles*

$$A_{m,p} = \sum_{n=m}^{p} a_n$$

sont bornées, il y a convergence pour $Re(s) > 0$. Pour s réel on a convergence uniforme sur tout domaine $[\sigma, \infty[$ avec $\sigma > 0$, ce qui assure la continuité de f sur $]0, \infty[$.

Il suffit d'utiliser le lemme **II.1.2**.

II.2 La fonction Zêta de Riemann

II.2.1 Produits Eulériens

Définition II.2.1 *Une fonction $f : \mathbb{N} \longrightarrow \mathbb{C}$ est dite multiplicative si l'on a $f(1) = 1$ et pour m, n premiers entre eux*

$$f(mn) = f(m)f(n).$$

Lemme II.2.1 *Soit f une fonction multiplicative et bornée. La série de Dirichlet*

$$\sum_{n=1}^{\infty} f(n)/n^s$$

converge absolument pour $Re(s) > 1$, et sa somme dans ce domaine est égale au produit infini convergent

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

($\mathbb{P}$ désigne l'ensemble des nombres premiers).

Puisque f est bornée, la série converge absolument. Soit S un ensemble fini de nombres premiers, et soit $N(S)$ l'ensemble des entiers naturels dont tous les facteurs premiers appartiennent à S. On a immédiatement

$$\sum_{n \in N(S)} f(n)/n^s = \prod_{p \in S} (\sum_{m=0}^{\infty} f(p^m) p^{-ms}).$$

Quand S croît, le premier membre tend vers :

$$\sum_{n=1}^{\infty} f(n)/n^s.$$

On en déduit que le produit infini converge et que sa valeur est bien égale à

$$\sum_{n=1}^{\infty} f(n)/n^s.$$

Lemme II.2.2 *Si f est multiplicative au sens strict (i.e. si $f(nm) = f(n)f(m)$ pour tout couple $n, m \in \mathbb{N}$), on a*

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{f(p)}{p^s}}.$$

Cela résulte du lemme précédent, combiné avec l'identité $f(p^m) = f(p)^m$.

II.2.2 La fonction Zêta

On applique le paragraphe précédent avec $f = 1$. On obtient alors la fonction Zêta de Riemann.

Définition II.2.2 *On appelle fonction Zêta de Riemann la fonction :*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$$

ces formules ayant un sens pour $Re(s) > 1$.

On peut noter le résultat suivant: si μ désigne la fonction de Moebius, c'est-à-dire

$$\begin{aligned}\mu(n) &= 1 \qquad si\ \ n=1\\ &= (-1)^r\ \ si\ \ n = p_1...p_r\\ &= 0 \qquad sinon\end{aligned}$$

alors, pour $Re(s) > 1$

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = 1$$

ce qui montre au passage que $\zeta(s) \neq 0$ pour $Re(s) > 1$.

Proposition II.2.1 *La fonction ζ est holomorphe et non nulle dans le demi-plan $Re(s) > 1$. De plus on a*

$$\zeta(s) = \frac{1}{s-1} + \varphi(s)$$

où φ est holomorphe pour $Re(s) > 0$.

La première partie est évidente. Pour prouver la seconde, on remarque que

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s}dt = \sum_{n=1}^{\infty}\int_n^{n+1} t^{-s}.$$

On a alors

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty}(\frac{1}{n^s} - \int_n^{n+1} t^{-s}dt) = \frac{1}{s-1} + \sum_{n=1}^{\infty}\int_n^{n+1}(n^{-s} - t^{-s})dt.$$

Posons

$$\varphi_n(s) = \int_n^{n+1}(n^{-s} - t^{-s})dt \quad et \quad \varphi(s) = \sum_{n=1}^{\infty}\varphi_n(s).$$

Les fonctions φ_n sont holomorphes sur $Re(s) > 0$. De plus la série $\sum\varphi_n$ converge normalement sur tout compact pour $Re(s) > 0$ car

$$|\varphi_n(s)| \leq \frac{|s|}{n^{R(s)+1}}$$

ce qui assure la convergence cherchée sur $Re(s) \geq \varepsilon$.

Corollaire II.2.1 *La fonction Zêta a un pôle simple pour $s = 1$.*

Corollaire II.2.2 *Lorsque* $s \to 1$*, on a*

$$\sum_{p \in \mathbb{P}} p^{-s} \sim Log(\frac{1}{s-1})$$

alors que

$$\sum_{p,k \geq 2} \frac{1}{p^{ks}}$$

reste borné.

On a

$$Log(\zeta(s)) = \sum_{p \in \mathbb{P}} \sum_{k \geq 1} \frac{1}{kp^{ks}} = \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \psi(s)$$

avec

$$\psi(s) = \sum_{p \in \mathbb{P}} \sum_{k \geq 2} \frac{1}{p^{ks}}.$$

La série ψ est majorée par la série

$$\sum_{p \in \mathbb{P}} \sum_{k \geq 0} \frac{1}{p^{ks}} = \sum_{p \in \mathbb{P}} \frac{1}{p^s(p^s-1)} \leq \sum_{p \in \mathbb{P}} \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.$$

On en conclut que ψ est bornée et comme $Log(\zeta(s)) \sim Log(\frac{1}{s-1})$, le corollaire est démontré.

II.3 La Fonction Zêta de Dedekind

Passons au cas général. On définit la fonction Zêta de Dedekind par

$$\zeta_K(s) = \sum_{\mathcal{A}} \frac{1}{N(\mathcal{A})^s}.$$

On va étendre les formules trouvées au **II.1**. On dispose principalement des deux théorèmes suivants.

Théorème II.3.1 *La fonction Zêta admet une décomposition en produit infini de la forme*

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - \frac{1}{N(\mathcal{P})^s}}$$

le produit étant étendu à tous les diviseurs premiers du corps K. Cette formule s'appelle l'identité d'Euler.

Pour tout $\mathcal{P}$ premier, on a

$$\frac{1}{1-\frac{1}{N(\mathcal{P})^s}} = \sum_{i=0}^{\infty} \frac{1}{N(\mathcal{P})^{si}}.$$

Soit N un entier naturel. Soient $\mathcal{P}_1, ..., \mathcal{P}_r$ des diviseurs premiers de norme inférieure où égale à N. On a alors

$$\prod_{N(\mathcal{P})\leq N} \frac{1}{1-\frac{1}{N(\mathcal{P})^s}} = \sum_{k_1,..,k_r} \frac{1}{N(\mathcal{P}_1^{k_1}...\mathcal{P}_r^{k_r})^s} = \sum_{\mathcal{A}} \frac{1}{N(\mathcal{A})^s},$$

où $\mathcal{A}$ parcourt tous les diviseurs de K dont la décomposition en produit de puissances de diviseurs premiers contient seulement des éléments dont la norme est inférieure où égale à N. Dans la dernière série, on retrouve tous les éléments premiers dont la norme ne dépasse pas N. On a donc :

$$\left| \prod_{N(\mathcal{P})\leq N} \frac{1}{1-\frac{1}{N(\mathcal{P})^s}} - \zeta_K(s) \right| \leq \sum_{N(\mathcal{A})>N} \frac{1}{N(\mathcal{A})^s}.$$

Or pour $s > 1$ la série $\zeta_K(s)$ converge. Donc

$$\sum_{N(\mathcal{A})>N} \frac{1}{N(\mathcal{A})^s} \longrightarrow_{N\to\infty} 0$$

ce qui assure le résultat.

Théorème II.3.2 *Soit K un corps de nombres algébriques de degré n=s+2t. On a alors*

$$lim_{s\to 1+0}(s-1)\zeta_K(s) = kh,$$

où k est une constante liée au corps K.

$$k = \frac{2^{s+t}\pi^t R}{mD^{\frac{1}{2}}}.$$

D et R sont respectivement le discriminant et le régulateur de K, et m est le nombre de racines de l'unité contenues dans K.

On admettra ce théorème. Il est démontré dans le livre: **Théories des nombres** par **Z.I.BOREVITCH**.

III CALCUL DU NOMBRE DE CLASSES D'UN CORPS CYCLOTOMIQUE A L'AIDE DES SERIES L

III.1 Caractères de groupes abéliens finis

Soit G un groupe abélien fini, noté multiplicativement.

Définition III.1.1 *Un caractère de G est un homomorphisme de G dans $\mathbb{C}^*$ le groupe multiplicatif des nombres complexes.*

Les caractères de G forment un groupe Hom(G,$\mathbb{C}^*$) que l'on appelle le dual de G et que l'on note $\widehat{G}$.

Proposition III.1.1 *Soit H un sous groupe de G. Tout caractère de H peut être prolongé en un caractère de G.*

On raisonne par récurrence sur l'indice $(G{:}H)$ de H dans G. Le résultat est clair pour $(G{:}H)$=1. Supposons le acquis pour $(G{:}H)$=n. Soit x un élément de G qui ne soit pas dans H et p le plus petit entier≥2 tel que $x^p \in H$. Soit χ un caractère de H et t=$\chi(x^n)$. Il existe w tel que $w^n = t$. Notons H' le sous groupe de G engendré par H et x. Tout élément de H' s'écrit $h' = h * x^a$, avec $a \in \mathbb{Z}$ *et* $h \in H$. Posons $\chi'(h') = \chi(\mathrm{h}) * w^a$. On vérifie aussitôt que ce nombre ne dépend pas de la décomposition de h', et que χ' est un caractère de H' prolongeant χ. L'hypothèse de récurrence permet de conclure.

Proposition III.1.2 *Le groupe $\widehat{G}$ est un groupe fini de même ordre que G.*

On raisonne par récurrence sur l'ordre n de G, le cas n=1 étant trivial. Si $n \geq 2$, on choisit un sous-groupe cyclique H non trivial de G. L'ordre de $\widehat{G}$ est le produit des ordres de $\widehat{H}$ et de $\widehat{G/H}$. Mais l'ordre de H (resp. de G/H) est égal à celui de son dual, puisque H est cyclique (resp. puisque G/H est d'ordre strictement plus petit que n). On en déduit que l'ordre de $\widehat{G}$ est le produit des ordres de H et de G/H, et il est bien égal à l'ordre de G.

Proposition III.1.3 *L'homomorphisme $\varepsilon : G \to \widehat{\widehat{G}}$, défini par*

$$\varepsilon(x)(\chi) = \chi(x)$$

est un isomorphisme.

D'après ce qui précède G et $\widehat{\widehat{G}}$ ont même ordre: il suffit donc de montrer que ε est injective. Soient $x \neq 1$ et H le sous-groupe cyclique de G engendré par x. Il est clair qu'il existe un caractère de H tel que $\chi(x) \neq 1$, et la proposition 1 permet de prolonger χ en un caractère de G, d'où le résultat cherché.

Proposition III.1.4 *Soit $n = card(G)$, et soit $\chi \in \widehat{G}$.*
on a:

$$\begin{aligned} \sum_{x \in G} \chi(x) &= n \qquad si \;\; \chi = 1 \\ &= 0 \qquad si \;\; \chi \neq 1 \end{aligned}$$

La première formule est évidente. Pour prouver la seconde choisissons $y \in G$ tel que $\chi(y) \neq 1$. On a

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x)$$

d'où

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$

Comme $\chi(y) \neq 1$, on a

$$\sum_{x \in G} \chi(x) = 0.$$

Proposition III.1.5 *Soit $x \in G$. On a*

$$\begin{aligned} \sum_{\chi \in \hat{G}} \chi(x) &= n \qquad si \;\; x = 1 \\ &= 0 \qquad si \;\; x \neq 1 \end{aligned}$$

Définition III.1.2 *A tout caractère χ de $\mathbb{Z}/p\mathbb{Z}$, on peut associer la fonction χ^* définie dans $\mathbb{N}$ par:*

$$\begin{aligned} \chi^*(n) &= \chi(\bar{n}) \qquad si \qquad (n,p) = 1 \\ &= 0 \qquad\quad sinon. \end{aligned}$$

La fonction χ^* est appelée caractère modulaire modulo m. On notera aussi χ pour χ^*.

III.2 Les corps cyclotomiques

Soit m un entier naturel et ξ une racine $m^{ième}$ de l'unité. Les racines $m^{ième}$ de l'unité divisent le cercle en m parties égales. Le corps $\mathbb{Q}(\xi)$ est alors appelé le corps de division du cercle en m parties égales. C'est le $m^{ième}$ corps cyclotomique. Pour l'étude du nombre de classes dans $\mathbb{Q}(\xi)$, nous avons besoin de connaître deux résultats essentiels :

_le degré de $\mathbb{Q}(\xi)$.

_la loi de décomposition dans $\mathbb{Q}(\xi)$.

Théorème III.2.1 *Le degré de $\mathbb{Q}(\xi)$ est égale à $\varphi(m)$, où φ est la fonction indicatrice d'Euler.*

Ce théorème résulte des propositions suivantes, propositions qui seront énoncées ici sans démonstration. On rappelle que le degré de $\mathbb{Q}(\xi)$ est égal au degré du polynôme minimal de ξ sur le corps $\mathbb{Q}$.

Définition III.2.1 *On appelle $m^{ième}$ polynôme cyclotomique le polynôme*

$$\phi_m(t) = \prod_{(k,m)=1} (t - \xi^k).$$

Le degré de $\phi_m(t)$ est égal $\varphi(m)$.

Proposition III.2.1 *Les coefficients de ϕ_m sont des rationnels.*

Proposition III.2.2 *ϕ_m est irréductible sur $\mathbb{Q}$.*

Proposition III.2.3 *ϕ_m est le polynôme minimal de ξ.*

On obtient ainsi que $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$. Pour la loi de décomposition, on dispose du théorème fondamental suivant.

Théorème III.2.2 *Soit p un nombre premier ne figurant pas dans m. Désignons par f le plus petit entier naturel tel que $p^f \equiv 1\,[m]$.*

Soit $g = \frac{\varphi(m)}{f}$. Alors dans $\mathbb{Q}(\xi)$, p admet la décomposition $p = \mathcal{P}_1 ... \mathcal{P}_g$, où $\mathcal{P}_1, ..., \mathcal{P}_g$ sont premiers, deux à deux distincts et $N(\mathcal{P}_i) = p^f$, $\forall\ 1 \leq i \leq g$.

III.3 Expression de h a l'aide des séries L

Dans l'identité d'Euler, regroupons tous les facteurs $\mathcal{P}$ qui divise un même nombre rationnel premier p. On obtient

$$\zeta_K(s) = \prod_p \prod_{\mathcal{P}/p} \frac{1}{1 - \frac{1}{N(\mathcal{P})^s}}.$$

Soit

$$G(s) = \prod_{\mathcal{P}/m} \frac{1}{1 - \frac{1}{N(\mathcal{P})^s}}.$$

Si $(p, m) = 1$, alors

$$\forall\, \mathcal{P}/p, \;\; N(\mathcal{P}) = p^{f_p}.$$

où f_p est l'ordre de p modulo m. Or le nombre de diviseurs $\mathcal{P}$ distincts qui divisent p est égale à $\frac{\varphi(m)}{f_p}$. On obtient donc

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} (1 - \frac{1}{p^{f_p s}})^{-\frac{\varphi(m)}{f_p}}.$$

Posons maintenant

$$\varepsilon = \varepsilon_p = cos(\frac{2\pi}{f_p}) + i * sin(\frac{2\pi}{f_p}).$$

On peut écrire

$$1 - (\frac{1}{p^s})^{f_p} = \prod_{k=0}^{f_p - 1} (1 - \frac{\varepsilon^k}{p^s}).$$

Nous allons maintenant utiliser les résultats obtenus sur les caractères du groupe $(\mathbb{Z}/m\mathbb{Z})^*$. On désignera également par p la classe de p modulo m. Pour chaque caractère χ de ce groupe, $\chi(p)$ qui est une racine de l'unité est égale à un certain ε^k. Réciproquement, si l'on choisit arbitrairement une des racines ε^k, il existe sur le sous-groupe $\{p\}$ un caractère χ et un seul tel que $\chi(p) = \varepsilon^k$. D'après le théorème **III.1.1** χ se prolonge en un caractère de $\mathbb{Z}/m\mathbb{Z}$. Ainsi si χ parcourt tous les caractères de $\mathbb{Z}/m\mathbb{Z}$, $\chi(p)$ parcourt toutes les racines $\varepsilon^k, (k = 0, ..., f_p - 1)$; chacune de ces racines étant obtenue $\frac{\varphi(m)}{f_p}$ fois. Finalement, on obtient

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \prod_{\chi} (1 - \frac{\chi(p)}{p^s})^{-1}.$$

On considère maintenant, à la place des caractères de $\mathbb{Z}/m\mathbb{Z}$, les caractères modulaires. Puisque $\chi(p) = 0$ pour tout p figurant dans m, on peut écrire

$$\zeta_K(s) = G(s) \prod_p \prod_\chi (1 - \frac{\chi(p)}{p^s})^{-1}.$$

Cette dernière égalité va nous permettre de donner une définition des séries L.

Définition III.3.1 *On définit les séries L par*

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

On a alors

$$\zeta_K(s) = G(s) \prod_\chi L(s, \chi)$$

ce qui est quand même une définition plus sympathique de la fonction Zêta. Si χ est le caractère unité χ_0, on a

$$L(s, \chi_0) = \prod_{(p,m)=1} \frac{1}{1 - \frac{1}{p^s}} \qquad (s > 1).$$

Or par définition de la fonction Zêta de Riemann, on a

$$\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}.$$

D'où

$$L(s, \chi_0) = (\prod_{p/m} \frac{1}{1 - \frac{1}{p^s}})^{-1} \zeta(s).$$

Ainsi posant

$$F(s) = \prod_{\mathcal{P}/m} (1 - \frac{1}{N(\mathcal{P})^s})^{-1} . \prod_{p/m} (1 - \frac{1}{p^s}),$$

on a

$$\zeta_K(s) = F(s) \zeta(s) \prod_{\chi \neq \chi_0} L(s, \chi).$$

Du fait qu'un caractère est une fonction multiplicative, on a facilement

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

Faisons maintenant appel aux résultats démontrés dans la partie **II.1** à propos des séries de Dirichlet. Ils assurent clairement la proposition suivante.

Proposition III.3.1 *Pour tout caractère $\chi \neq \chi_0$, $L(s,\chi)$ est convergente pour $s > 0$ et est une fonction continue de s dans l'intervalle $]0, \infty[$.*

D'après la proposition **II.2.1**, on a

$$lim_{s \to 1+0} (s-1)\zeta(s) = 1.$$

On peut donc écrire

$$lim_{s \to 1+0}\, \zeta_K(s) = F(1) \prod_{\chi \neq \chi_0} L(1,\chi).$$

En rapprochant cette formule de celle établie dans le théorème **II.2.3**, on peut enfin obtenir une expression satisfaisante de h.

Théorème III.3.1 *C'est d'une main fébrile que je peux enfin écrire la formule suivante*

$$h = \frac{wD^{\frac{1}{2}}}{s^{s+t}\pi^t R} F(1) \prod_{\chi \neq \chi_0} L(1,\chi)$$

où w désigne le nombre de racines de l'unité contenues dans K.

Cependant, dans un souci d'amélioration toujours croissant, on ne peut se contenter de cette formule, celle-ci contenant des séries infinies.

On va revenir sur les séries $L(s,\chi)$. En éliminant dans celle-ci les termes nuls et en remarquant que $\chi(a) = \chi(b)$ pour $a \equiv b[m]$, on obtient

$$L(s,\chi) = \sum_{(x,m)=1} \chi(x) \sum_{n \equiv x[m]} \frac{1}{n^s}.$$

La somme intérieure peut être écrite sous la forme

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

avec

$$\begin{aligned} c_n &= 1 \quad \textit{pour } n \equiv x[m] \\ &= 0 \quad \textit{pour } n \not\equiv x[m]. \end{aligned}$$

On peut écrire c_n sous une autre forme en se servant de la formule

$$\begin{aligned} \sum_{k=0}^{m-1} \zeta^{rk} &= m \quad \textit{pour } r \equiv 0[m] \\ &= 0 \quad \textit{pour } r \not\equiv 0[m] \end{aligned}$$

où

$$\zeta = cos(\frac{2\pi}{m}) + i * sin(\frac{2\pi}{m})$$

est une racine primitive de l'unité. On peut donc écrire

$$c_n = \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k}.$$

Ainsi

$$L(s,\chi) = \sum_{(x,m)=1} \chi(x) \sum_{n=1}^{\infty} \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k} \frac{1}{n^s} = \frac{1}{m} \sum_{k=0}^{m-1} (\sum_{(x,m)=1} \chi(x)\zeta^{xk}) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

La dernière égalité nous permet de donner la définition d'une somme de Gauss.

Définition III.3.2 *On appelle somme de Gauss la somme*

$$\tau_a(\chi) = \sum_{(x,m)=1} \chi(x)\zeta^{ax}.$$

Si χ n'est pas le caractère unité, alors

$$\tau_0(\chi) = \sum_{(x,m)=1} \chi(x) = 0.$$

On a donc

$$L(s,\chi) = \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

D'après la proposition **II.1.8**, la série

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}$$

converge pour $0 < s < 1$ et est une fonction continue de la variable s. Nous pouvons donc faire $s = 1$ dans la dernière égalité. On obtient

$$L(1, \chi) = \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(x) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n}.$$

Pour évaluer la somme de la série intérieure, on considère la série entière $\sum \frac{z^n}{n}$. On sait qu'elle converge pour $|z| < 1$ et est égale dans ce domaine à $-Log(1 - z)$. Puisque cette série entière converge au point $z = \zeta^{-k}$, alors, d'après le théorème d'Abel,

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n} = -Log((1 - \zeta^{-k}),$$

ce qui entraine

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) Log(1 - \zeta^{-k}).$$

On possède donc maintenant une forme définitive de l'expression de h.

Théorème III.3.2 *On a, finalenent*

$$h = -\frac{1}{m} \frac{wD^{\frac{1}{2}}}{s^{s+t} \pi^t R} F(1) \prod_{\chi \neq \chi_0} \sum_{k=1}^{m-1} \tau_k(\chi) Log(1 - \zeta^{-k}).$$

IV LE THEOREME DE DIRICHLET

Le théorème de Dirichlet assure que dans une progression arithmétique, il y a une infinité de nombres premiers. L'énoncé exacte en est le suivant.

Théorème IV.0.3 *Soient a et m des entiers naturels non nuls, premiers entre eux. Il existe une infinité de nombres premiers p tels que*

$$p \equiv a[m].$$

Un des points essentiels de la démonstration est de remarquer que $L(1,\chi)$ est non nul.

Théorème IV.0.4 *Pour tout caractère $\chi \neq \chi_0$, $L(1,\chi) \neq 0$.*

Ce théorème résulte immédiatement du théorème **III.3.1**.

On désigne toujours par $\mathbb{P}$ l'ensemble des nombres premiers. Soit A une partie de $\mathbb{P}$. Nous dirons que A a pour densité k lorsque le rapport

$$(\sum_{p\in A}\frac{1}{p^s})/(log(\frac{1}{s-1})$$

tend vers k lorsque $s \to 1$. Notons tout de suite que si $A = \mathbb{P}$, alors A a une densité égale à 1 d'après le corollaire **II.2.2**. Avec cette définition, il est clair qu'un ensemble A fini a une densité nulle. Notons $\mathbb{P}_a$ l'ensemble des nombres p premiers tel que $p \equiv a[m]$. Nous allons calculer la densité de $\mathbb{P}_a$.

Proposition IV.0.2 *L'ensemble $\mathbb{P}_a$ a pour densité $1/\varphi(m)$.*

Pour montrer ce théorème, nous aurons besoin de trois lemmes préliminaires.

Lemme IV.0.1 *Soit χ un caractère de $\mathbb{Z}/m\mathbb{Z}$. Posons*

$$f_\chi(s) = \sum_{p \not| m} \frac{\chi(p)}{p^s}.$$

Pour $\chi = 1$, on a

$$f_\chi \sim Log(\frac{1}{s-1}) \quad \textit{quand } s \to 1.$$

Le corollaire **II.2.2** assure que

$$\sum_{p\in\mathbb{P}} \frac{1}{p^s} \sim Log(\frac{1}{s-1})$$

au voisinage de 1, et f ne diffère de la série $\sum 1/p^s$ que par un nombre fini de termes.

Lemme IV.0.2 *Si $\chi \neq 1$, f_χ reste bornée au voisinage de 1.*

On va utiliser le logarithme des fonctions L. $L(s,\chi)$ est définie comme un produit $\prod 1/(1-\chi(p)/p^s)$. Pour $Re(s) > 1$, chaque facteur est de la forme $1/(1-\alpha)$. On définit alors

$$Log(\frac{1}{1-\alpha}) = \sum_{n=1}^{\infty} \frac{\alpha^n}{n}.$$

Ainsi le logarithme de L est égal à

$$Log(L(s,\chi)) = \sum_{n,p} \frac{\chi(p)^n}{np^{sn}}.$$

On peut décomposer $Log(L(s,\chi))$ en deux morceaux

$$Log(L(s,\chi)) = f_\chi(s) + F_\chi(s)$$

où

$$F_\chi(s) = \sum_{p,n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Le théorème **IV.0.3** associé à la proposition **II.2.1** et au corollaire **II.2.2** assure que $Log(L(s,\chi))$ et $F_\chi(s)$ restent bornés au voisinage de 1. Il en est donc de même pour $f_\chi(s)$.

Lemme IV.0.3 *On a*

$$g_a(s) = \sum_{p\in\mathbb{P}_a} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s).$$

On a

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_{p\not| m} (\sum_\chi \chi(a^{-1})\chi(p)) p^s.$$

Or $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. D'après la proposition **II.1.5**

$$\begin{aligned} \sum_\chi \chi(a^{-1}p) &= \varphi(m) \qquad si\ \ a^{-1}p \equiv 1[m] \\ &= 0 \qquad\qquad sinon. \end{aligned}$$

On trouve donc bien le résultat.

Le théorème de Dirichlet devient alors immédiat. En effet, le lemme **IV.0.1** montre que

$$f_\chi \sim Log(\frac{1}{s-1})$$

pour $\chi = 1$, et le lemme **IV.0.2** montre que les autres f_χ restent bornées. Le lemme **IV.0.3** assure de plus

$$g_a(s) \sim \frac{1}{\varphi(m)} Log(\frac{1}{s-1}).$$

On en déduit donc que $\mathbb{P}_a$ a pour densité $1/\varphi(m)$ et est ainsi infini.

V VERS LE THEOREME DE FERMAT

V.1 Le théorème de Fermat dans un cas simple

L'hypothèse de Fermat est la suivante: pour $l > 2$, l'équation

$$x^l + y^l = z^l$$

n' a pas de solution en nombres entiers non nuls. On peut déjà remarquer que si l'on a montré le résultat pour un entier l, alors on l'a aussi montré pour tous les multiples de l. De plus, tout entier $l > 2$ est soit divisible par 4, soit divisible par un nombre premier impair. Le cas $l = 4$ a été démontrer par Euler. On étudiera ici le cas l premier impair.

Traditionnellement, pour étudier l'équation de Fermat, on envisage les deux situations suivantes :

_ l ne divise aucun des entiers x, y, z.

_ l divise un et un seul de ces entiers.

L'étude se limitera ici au premier cas pour des valeurs de l particulière.

Théorème V.1.1 *Soit l un nombre premier impair et ζ une racine primitive de l'unité. Si le nombre de classes de diviseurs du corps $\mathbb{Q}(\zeta)$ n'est pas divisible par l, alors le premier cas du théorème de Fermat est vrai pour l'exposant l.*

Raisonnons par l'absurde. Supposons qu'il existe x, y, z non divisibles par l et tel que

$$x^l + y^l = z^l$$

x, y, z étant premier entre eux deux à deux. (Cette hypothèse n'est pas du tout restrictive). Dans $\mathbb{Q}(\zeta)$, l'égalité devient

$$\prod_{k=0}^{l-1}(x + \zeta^k y) = z^l.$$

Regardons maintenant les congruences modulo l. Grâce à la formule de Newton

$$(x + y)^l \equiv x^l + y^l \ \ [l].$$

Donc

$$(x + y) \equiv (x + y)^l \equiv z^l \equiv z \ \ [l].$$

Par hypothèse l ne divise pas z. Il est de même pour $x+y$. Pour $m \not\equiv n[l]$, il existe γ_0 et η_0 tels que

$$(x + \zeta^n y)\gamma_0 + (x + \zeta^m y)\eta_0 = 1.$$

En effet, considérons l'ensemble

$$A = \{(x + \zeta^n y)\gamma + (x + \zeta^m y)\eta / \ \ \gamma, \eta \in \mathbb{Z}[\zeta]\}.$$

A est un espace vectoriel sur $\mathbb{Z}[\zeta]$. On a

$$(x + \zeta^n y) - (x + \zeta^m y) = \zeta^n(1 - \zeta^{m-n})y = \zeta^n \varepsilon_{m-n}(1 - \zeta)y$$

et

$$(x + \zeta^n y)\zeta^m - (x + \zeta^m y)\zeta^n = -\zeta^n(1 - \zeta^{m-n})x = -\zeta^n \varepsilon_{m-n}(1 - \zeta)x,$$

ce qui assure que $(1 - \zeta)y \in A$ et $(1 - \zeta)x \in A$ (puisque $\zeta^n \varepsilon_{m-n}$ est une unité de $\mathbb{Z}(\zeta)$).

x et y étant premiers entre eux, $\exists(a, b) \in \mathbb{Q}$ tels que $ax + by = 1$. Donc

$$(1 - \zeta)xa + (1 - \zeta)yb = 1 - \zeta \in A.$$

De plus

$$x + y = (x + \zeta^n y) + (1 - \zeta^n)y = (x + \zeta^n y) + (1 - \zeta)\varepsilon_n y$$

et par suite $x+y \in A$. Puisque l est divisible par $1-\zeta$, alors $l \in A$. $x+y$ et l sont premiers entre eux, donc $\exists u, v$ tel que $(x+y)u + lv = 1$. Ainsi $1 \in A$, ce qui est bien ce qu'il fallait montrer.

On a donc $(x+\zeta^n y)\gamma_0 + (x+\zeta^m y)\eta_0 = 1$. Les idéaux $(x+\zeta^k y)$ sont alors deux à deux premiers entre eux pour $(k = 0, ..., l-1)$. Puisque leur produit est une puissance $l^{ième}$ de (z), chacun d'eux est une puissance $l^{ième}$.

En particulier $(x+\zeta y) = \mathcal{A}^l$. De plus, puisque le nombre de classes de diviseurs de $\mathbb{Q}(\zeta)$ n'est pas divisible par l, $\mathcal{A}$ est principal. En effet, $lu+vh = 1$ par hypothèse et $\mathcal{A}^h$ est principal par définition de h. Ainsi $\mathcal{A}^{lu}$ et $\mathcal{A}^{hv}$ sont aussi principaux, de même que $\mathcal{A}^{lu}\mathcal{A}^{hv} = \mathcal{A}$. Donc $\exists \alpha \in \mathbb{Z}(\zeta)$ tel que $\mathcal{A} = (\alpha)$.

L'égalité $(x+\zeta y) = (\alpha^l)$ entraîne

$$x + \zeta y = \varepsilon \alpha^l$$

où ε est une unité de $\mathbb{Z}(\zeta)$. De même on a

$$x - \zeta z = \varepsilon_1 \alpha_1^l.$$

Montrons que ces deux égalités amènent à une contradiction . On va en fait étudier les congruences correspondantes modulo l dans $\mathbb{Z}(\zeta)$.

Soit $\alpha = a_0 + ... + a_{l-2}\zeta^{l-2}$ $(a_1, ..., a_{l-2}$ entier rationnels). Alors

$$\alpha^l \equiv a_0^l + ... + a_{l-2}^l \zeta^{l(l-2)} \equiv M \;\; [l]$$

avec $M = a_0 + ... + a_{l-2}$. On admet ici le lemme de Kummer qui permet d'écrire $\varepsilon = \zeta^s \eta$ où η est une unité réelle. On a

$$x + \zeta y = \varepsilon \alpha^l \equiv \zeta^s \eta M \equiv \zeta^s \xi \;\; [l]$$

ξ étant un réel appartenant à $\mathbb{Z}(\zeta)$. La congruence s'écrit

$$\zeta^{-s}(x+\zeta y) \equiv \xi \;\; [l].$$

Passant au conjugué, on obtient

$$\zeta^s(x+\zeta^{-1}y) \equiv \overline{\xi} \equiv \xi \;\; [l].$$

D'où

$$\zeta^{-s}(x+\zeta y) \equiv \zeta^s(x+\zeta^{-1}y) \;\; [l]$$

ou encore

$$x\zeta^s + y\zeta^{s-2} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \;\; [l].$$

Or il est clair qu'un nombre représenté sous la forme canonique

$$a_0 + a_1\zeta + ... + a_{l-2}\zeta^{l-2}$$

est divisible par l si et seulement si tous les coefficients $a_0, ..., a_{l-2}$ sont divisibles par l. Or dans la dernière égalité, le nombre de gauche est écrit sous forme canonique. Ses coefficients sont donc tous divisibles par l. Mais alors $x \equiv 0\ [l]$ et $y \equiv 0\ [l]$, ce qui contredit le fait que x et y soient premiers entre eux. Ceci achève la démonstration du théorème.

Les nombres premiers l tels que le nombre de classes de diviseurs du corps $\mathbb{Q}(\zeta)$ n'est pas divisible par l sont dits réguliers et les autres irréguliers. Kummer a obtenu un critère simple permettant de reconnaître si un nombre premier donné l est régulier ou pas. Pour terminer, on va exposer ce critère.

V.2 Le critère de Kummer

V.2.1 Décomposition de h

La formule obtenue au théorème **III.3.2**, même si elle ne fait plus intervenir de produits infinis, n'est pourtant pas totalement satisfaisante car elle exprime un entier à l'aide de quantités complexes et irrationnelles. On se limitera au corps cyclotomique $\mathbb{Q}(\zeta)$ de degré $l = 2n + 1$, avec

$$\zeta = cos(\frac{2\pi}{l}) + i * sin(\frac{2\pi}{l}).$$

Dans ce cas, on admettra que le facteur$F(s)$ intervenant dans la formule du théorème **III.3.2** est égal à 1. Calculons maintenant le discriminant de $\mathbb{Q}(\zeta)$.

Théorème V.2.1 *Les nombres* $1, \zeta, ..., \zeta^{l-2}$ *forment une base de* $\mathbb{Q}(\zeta)$.

On admettra ce théorème.

Corollaire V.2.1 *Le discriminant du* $l^{ième}$ *corps cyclotomique est égal à*

$$(-1)^{\frac{l-1}{2}} l^{l-2}.$$

Puisque pour $s \not\equiv 0[l]$ le polynôme caractéristique de ζ^s est

$$X^{l-1} + X^{l-2} + ... + X + 1,$$

alors

$$\begin{aligned} Tr(\zeta^s) &= -1 \qquad si\ \ s \not\equiv 0[l] \\ &= l-1 \qquad si\ \ s \equiv 0[l]. \end{aligned}$$

Ainsi le discriminant de $\mathbb{Q}(\zeta)$ est égal au déterminant d'ordre $l-1$

$$\begin{vmatrix} -1 & -1 & \cdots & -1 \\ -1 & -1 & \cdots & l-1 \\ \cdots & \cdots & \cdots & \cdots \\ -1 & l-1 & \cdots & -1 \end{vmatrix}$$

D'où le résultat.
La formule donnant l'expression de h peut alors se mettre sous la forme

$$h = \frac{l^{\frac{l}{2}}}{2^{m-1}\pi^m R} \prod_{\chi \neq \chi_0} L(1,\chi),$$

où R est le régulateur de $\mathbb{Q}(\zeta)$ et $m = (l-1)/2$.

Dans cette formule on peut remplacer $L(1,\chi)$ par $|L(1,\chi)|$ car tous les termes sont réels. Soient g une racine primitive fixée modulo l et θ une racine primitive de degré $l-1$ de 1. Soit χ le caractère tel que

$$\chi(g) = \theta^{-1}.$$

Toutes les puissances $\chi, ..., \chi^{l-1}$ épuisent tout le groupe des caractères modulo l. Soit g_s le plus petit résidu de g^s modulo l. On admettra maintenant les deux formules suivantes

$$|L(1,\chi^{2k})| = \frac{2}{\sqrt{l}} \left| \sum_{r=0}^{m-1} \theta^{2kr} Log|1-\zeta^{g^r}| \right|$$

$$|L(1,\chi^{2k-1})| = \frac{\pi\sqrt{l}}{l^2} \left| \sum_{s=0}^{l-2} g_s \theta^{(2k-1)s} \right|.$$

Soit

$$F(X) = \sum_{s=0}^{l-2} g_s X^s.$$

On peut alors décomposer h sous la forme $h = h_0 h^*$ avec

$$h_0 = \frac{2^{m-1}}{R} \prod_{k=1}^{m-1} \left| \sum_{r=0}^{m-1} \theta^{2kr} Log|1 - \zeta^{g^r}| \right|$$

$$h^* = \frac{1}{(2l)^{m-1}} |F(\theta)F(\theta^2)...F(\theta^{l-2})|.$$

On peut montrer que le facteur h_0 est en fait égal au nombre de classes d'idéaux du sous corps $\mathbb{Q}(\zeta + \zeta^{-1})$ du corps $\mathbb{Q}(\zeta)$ et que h_0 et h^* sont des entiers. L'avantage de décomposer h de la sorte est de pouvoir donner un critère de régularité pour l portant sur h_0 et h^*.

V.2.2 Le critère de Kummer

Puisque $h = h_0 h^*$, le nombre l sera régulier si et seulement si aucun des facteurs h_0 et h^* n'est divisible par l. Les démonstrations des résultats qui vont suivre utilisent explicitement les deux formules ci-dessus et sont essentiellement calculatoires. C'est pour cela qu'ils seront donnés ici sans leur démonstration. Nous disposons d'abord du théorème suivant.

Théorème V.2.2 *Si pour le $l^{ième}$ corps cyclotomique $\mathbb{Q}(\zeta)$ le facteur h^* n'est pas divisible par l, alors le facteur h_0 n'est pas non plus divisible par l.*

Il résulte de celui-ci qu'on peut se limiter à chercher une condition pour que h^* ne soit pas divisible par l.

Théorème V.2.3 *Pour que h^* ne soit pas divisible par l, il faut et il suffit que l'un des nombres*

$$S_k = \sum_{n=1}^{l-1} n^k \quad (k = 2, 4..., l-3)$$

ne soit pas divisible par l^2.

Nous avons donc ainsi un critère de régularité pour un nombre premier l à savoir qu'un nombre premier l est régulier si et seulement si le facteur h^* n'est pas divisible par l. On peut démontrer un résultat un peu plus fort. En effet, si l est régulier, toute unité du corps $\mathbb{Q}(\zeta)$ est congrue modulo l à une puissance $l^{ième}$ d'un nombre entier rationnel. C'est sur cet argument que repose la démonstration du deuxième cas du théorème de Fermat pour des exposants réguliers.

Sommaire

I INTRODUCTION **3**
- I.1 Définition . . . 3
- I.2 Premiers Résultats . . . 3
- I.3 Norme d'un idéal . . . 5
- I.4 Classe de diviseurs de K . . . 7

II LA FONCTION ZETA DE DEDEKIND **7**
- II.1 Séries de Dirichlet. . . . 7
- II.2 La fonction Zêta de Riemann . . . 11
- II.3 La Fonction Zêta de Dedekind . . . 14

III CALCUL DU NOMBRE DE CLASSES D'UN CORPS CYCLOTOMIQUE A L'AIDE DES SERIES L **16**
- III.1 Caractères de groupes abéliens finis . . . 16
- III.2 Les corps cyclotomiques . . . 18
- III.3 Expression de h a l'aide des séries L . . . 19

IV LE THEOREME DE DIRICHLET **23**

V VERS LE THEOREME DE FERMAT **26**
- V.1 Le théorème de Fermat dans un cas simple . . . 26
- V.2 Le critère de Kummer . . . 29

BIBLIOGRAPHIE:

_Théories des nombres par Z.I. BOREVITCH.

_Cours d'arithmétique par J.P. SERRE.