M2 2020 Théorie des nombres

Géométrie des nombres

§1 Réseaux euclidiens

Définition Soit $(V, \|\cdot\|)$ un espace euclidien. On désigne par $\|\cdot\|_{\det}$ la norme sur $\det(V)$ définie par

$$\|\eta\|_{\det} := \inf_{\eta = x_1 \wedge \cdots \wedge x_d} \|x_1\| \cdots \|x_d\|$$

Remarque Si $(e_j)_{j=1}^d$ est une base orthonormée de V, alors on a

$$\|e_1 \wedge \cdots \wedge e_d\|_{\det} = 1 \qquad \text{(Exercice)}$$

Définition On appelle réseau euclidien toute donnée $\overline{E} = (E, \|\cdot\|)$, où E est un $\mathbb{Z}$-module libre de rang fini, et $\|\cdot\|$ est une norme euclienne sur $E_{\mathbb{R}} := E \otimes_{\mathbb{Z}} \mathbb{R}$.

covolume : $\operatorname{covol}(\overline{E}) := \ln \|u_1 \wedge \cdots \wedge u_d\|_{\det}$, où $(u_j)_{j=1}^d$ est une base de E sur $\mathbb{Z}$.

Remarque Si $(u_i')_{i=1}^d$ est une autre base de E sur $\mathbb{Z}$, il existe $A \in GL_d(\mathbb{Z})$ telle que $u_j' = A u_j \ \forall j \in \{1, \dots, d\}$.

On a $u_1' \wedge \cdots \wedge u_d' = \det(A) \cdot (u_1 \wedge \cdots \wedge u_d)$ avec $\det(A) \in \{1, -1\}$

Donc $\|u_1' \wedge \cdots \wedge u_d'\|_{\det} = \|u_1 \wedge \cdots \wedge u_d\|_{\det}$

§2 Comptage de points

On fixe un réseau euclidien $\overline{E} = (E, \|\cdot\|)$. Soit $d = \operatorname{rg}_{\mathbb{Z}}(E)$

Définition Pour tout $A \subset E_{\mathbb{R}}$, soit

$$N_A : E_{\mathbb{R}} \longrightarrow \mathbb{N} \cup \{+\infty\}, \quad x \longmapsto \operatorname{card}(E \cap (A + x))$$

où $A + x := \{y + x \mid y \in A\}$

Proposition La fonction N_A est E-périodique

Preuve $\forall x \in E_{\mathbb{R}}$, $N_A(x) = \operatorname{card}(E \cap (A+x)) = \operatorname{card}((E - x) \cap A)$

où $E - x := \{u - x \mid u \in E\}$

Donc, $\forall u \in E$, $N_A(x+u) = \operatorname{card}((E - x - u) \cap A) = \operatorname{card}((E - x) \cap A)$ ※

Convention On munit $(E_{\mathbb{R}}, \|\cdot\|)$ de la mesure de Haar standard $\operatorname{vol}_{\overline{E}}(\cdot)$

(Si $(e_j)_{j=1}^d$ est une base orthonormée de $(E_{\mathbb{R}}, \|\cdot\|)$, alors
$\operatorname{vol}_{\overline{E}}(\{\lambda_1 e_1 + \cdots + \lambda_d e_d \mid (\lambda_1, \dots, \lambda_d) \in [0,1]^d\}) = 1$)

M2 2020 Théorie des nombres

Proposition Pour tout $A \subset E_{\mathbb{R}}$ borélien, on a
$$\sup_{x\in E_{\mathbb{R}}} N_A(x) \geqslant \frac{\mathrm{vol}_E(A)}{\mathrm{covol}(E)}$$

Preuve Soit $(u_j)_{j=1}^d$ une base de E sur $\mathbb{Z}$, et
$$P = \{\lambda_1 u_1 + \cdots + \lambda_d u_d \mid (\lambda_1, \dots, \lambda_d) \in [0,1[^d\}$$
Soit $\varphi : E_{\mathbb{R}} \longrightarrow E_{\mathbb{R}}/E$ la projection. Soit $\widetilde{\mathrm{vol}}_E = \varphi_*(\mathrm{vol}_E|_P)$
Comme N_A est E-périodique, $\exists!\ \tilde{N}_A : E_{\mathbb{R}}/E \longrightarrow \mathbb{N}\cup\{+\infty\}$ telle que $\tilde{N}_A \circ \varphi = N_A$.
Soient $\alpha \in E_{\mathbb{R}}/E$, $x \in P$ tel que $\varphi(x) = \alpha$. On a
$$\tilde{N}_A(-\alpha) = N_A(-x) = \sum_{u\in E} \mathbb{1}_{A-x}(u) = \sum_{u\in E} \mathbb{1}_{A-u}(x)$$
Donc
$$\int_{E_{\mathbb{R}}/E} \tilde{N}_A(-\alpha)\, \widetilde{\mathrm{vol}}_E(d\alpha) = \int_P N_A(-x)\, \mathrm{vol}_E(dx)$$
$$= \mathrm{vol}_E((A-u)\cap P) = \sum_{u\in E} \mathrm{vol}_E(A\cap(P+u)) = \mathrm{vol}_E(A).$$
On en déduit
$$\sup_{x\in E_{\mathbb{R}}} N_A(x) = \sup_{\alpha\in E_{\mathbb{R}}/E} \tilde{N}_A(-\alpha) \geqslant \frac{\mathrm{vol}_E(A)}{\widetilde{\mathrm{vol}}_E(E_{\mathbb{R}}/E)} = \frac{\mathrm{vol}_E(A)}{\mathrm{covol}(E)}.$$
#

Théorème (1er théorème de Minkowski)
Soit $\Delta \subset E_{\mathbb{R}}$ un corps convexe (sous-ensemble fermé et convexe tel que $\Delta^\circ \neq \emptyset$) symétrique ($x\in\Delta \Rightarrow -x\in\Delta$). On a
$$\mathrm{card}(\Delta\cap E) \geqslant \frac{1}{2^d}\frac{\mathrm{vol}_E(\Delta)}{\mathrm{covol}(E)}$$

Preuve Appliquer la proposition précédente à $A = \frac{1}{2}\Delta$ pour obtenir $x \in E_{\mathbb{R}}$ tel que $N_A(A) = \mathrm{card}(E\cap(A+x)) \geqslant \frac{\mathrm{vol}_E(A)}{\mathrm{covol}(E)} = \frac{1}{2^n}\frac{\mathrm{vol}_E(\Delta)}{\mathrm{covol}(E)} > 0$.
Donc $E\cap(A+x) \neq \emptyset$.
Soit $u_0 \in E\cap(A+x)$, écrit sous la forme $u_0 = \frac{1}{2}y_0 + x$, où $y_0 \in \Delta$.
$\forall\, u = \frac{1}{2}y + x \in E\cap(A+x)$, où $y\in\Delta$, on a
$$u - u_0 = \frac{1}{2}(y - y_0) \in \Delta\cap E \quad (\text{car } \Delta \text{ est convexe et symétrique})$$
On obtient donc
$$\mathrm{card}(\Delta\cap E) \geqslant \mathrm{card}(E\cap(A+x)) \geqslant \frac{1}{2^n}\frac{\mathrm{vol}_E(\Delta)}{\mathrm{covol}(E)}$$
#

M2 2020 Théorie des nombres

§3 Fonction zêta d'Epstein

On fixe un réseau euclidien $\bar{E} = (E, \|\cdot\|)$. Soit $d = \mathrm{rg}_{\mathbb{Z}}(E)$

Définition On désigne par $Z_{\bar{E}}(s)$ la série de fonctions sur $\mathbb{C}$:

$$Z_{\bar{E}}(s) := \frac{1}{2} \sum_{u \in E \setminus \{0\}} \frac{1}{\|u\|^{2s}}$$

Proposition Pour tout $\varepsilon > 0$, $Z_{\bar{E}}(s)$ converge normalement sur $\{s \mid \mathrm{Re}(s) \geq \frac{d}{2} + \varepsilon\}$

Donc définit une fonction holomorphe sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \frac{d}{2}\}$

Preuve Soit $(e_j)_{j=1}^d$ une base de E sur $\mathbb{Z}$. Sans perte de généralité, on peut supposer que $(e_j)_{j=1}^d$ est une base orthonormée (équivalence de normes)

Pour tout $x \in \mathbb{R}_{\geq 0}$, soit

$$S(x) := \mathrm{card}\{(a_1, \dots, a_d) \in \mathbb{Z}^d \mid 0 < a_1^2 + \dots + a_d^2 \leq x\}$$

On a $S(x) \leq (2\sqrt{x} + 1)^d \leq 3^d x^{\frac{d}{2}}$ $\quad\left(\leq \mathrm{card}\{(a_j)_{j=1}^d \mid \max_j |a_j| \leq \sqrt{x}\}\right)$

$$\sum_{u \in E \setminus \{0\}} \frac{1}{\|u\|^{d+2\varepsilon}} = \sum_{n \in \mathbb{N}_{\geq 1}} \frac{b_n}{n^{\frac{d}{2}+\varepsilon}} \quad \text{avec } b_n = S(n) - S(n-1)$$

$$\left(S(x) = \sum_{1 \leq n \leq x} b_n\right)$$

Lemme Soient $(b_n)_{n \in \mathbb{N}}$ une suite de nombres complexes, $g : [1, +\infty[\to \mathbb{C}$ une fonction continûment différentiable, $S : [0, +\infty[\longrightarrow \mathbb{C}$, $S(x) := \sum_{1 \leq n \leq x} b_n$.

Alors $\displaystyle\sum_{1 \leq n \leq x} b_n g(n) = g(x) S(x) - \int_1^x g'(t) S(t)\, dt$

Preuve

$$\int_1^x g'(t) S(t)\, dt = \sum_{1 \leq n < \lfloor x \rfloor} \int_n^{n+1} g'(t) S(n)\, dt + S(x) \int_{\lfloor x \rfloor}^x g'(t)\, dt$$

$$= \sum_{1 \leq n < \lfloor x \rfloor} S(n) g(n+1) - \sum_{1 \leq n < \lfloor x \rfloor} S(n) g(n) + S(x) g(x) - S(x) g(\lfloor x \rfloor)$$

$$= \sum_{1 \leq n \leq \lfloor x \rfloor} S(n-1) g(n) - \sum_{1 \leq n \leq \lfloor x \rfloor} S(n) g(n) + S(x) g(x)$$

$$= S(x) g(x) - \sum_{1 \leq n \leq \lfloor x \rfloor} b_n g(n) = S(x) g(x) - \sum_{1 \leq n \leq x} b_n g(n)$$

$\divideontimes$

D'après le lemme,

$$\sum_{1 \leq n \leq x} \frac{b_n}{n^{\frac{d}{2}+\varepsilon}} = \frac{S(x)}{x^{\frac{d}{2}+\varepsilon}} + \int_1^x \left(\frac{d}{2} + \varepsilon + 1\right) \frac{S(t)}{t^{\frac{d}{2}+\varepsilon+1}}\, dt$$

$$\leq 3^d \left(x^{-\varepsilon} + \int_1^x \left(\frac{d}{2} + \varepsilon + 1\right) \frac{1}{t^{\varepsilon+1}}\, dt\right) \leq 3^d \frac{d/2 + \varepsilon + 1}{\varepsilon}$$

$\divideontimes$

M2 2020 Théorie des nombres

§4 Fonction Γ

Définition Soit $\varphi : \mathbb{R}_{>0} \to \mathbb{C}$ une fonction. On définit la transformée de Mellin de φ comme

$$M_\varphi(s) := \int_0^{+\infty} \varphi(t)\, t^s \frac{dt}{t} = \int_{-\infty}^{+\infty} e^{-st} \varphi(e^t)\, dt$$

Remarque On suppose que φ est continue par morceaux

$$\varphi(t) = \begin{cases} O(t^A) & t \to 0, \\ O(t^B) & t \to +\infty. \end{cases}$$

Alors $M_\varphi(\cdot)$ est bien défini et est holomorphe sur $-A < \mathrm{Re}(s) < -B$

Exemple

$$\Gamma(s) = \int_0^{+\infty} e^{-t} t^s \frac{dt}{t} \quad \text{holomorphe sur } \mathrm{Re}(s) > 0$$

Si $a > 0$ $\Gamma(s,a) = \int_a^{+\infty} e^{-t} t^s \frac{dt}{t}$ holomorphe sur $\mathbb{C}$

Propriétés

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

$$\Gamma(s+1) = s\Gamma(s) \quad \text{(intégration par parties)}$$

Conséquence $\Gamma(\cdot)$ admet un prolongement méromorphe sur $\mathbb{C}$, dont les pôles sont $s = -n$ $(n \in \mathbb{N})$ avec $\mathrm{Res}(\Gamma, -n) = \frac{(-1)^n}{n!}$

§5 Fonction thêta

On fixe $\bar{E} = (E, \|\cdot\|)$ un réseau euclidien, $d = \mathrm{rg}_{\mathbb{Z}}(E)$

Soit $E^\vee := \mathrm{Hom}_{\mathbb{Z}}(E, \mathbb{Z})$, $\|\cdot\|_*$ la norme dual sur $E^\vee \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathrm{Hom}_{\mathbb{R}}(E_{\mathbb{R}}, \mathbb{R})$

Proposition $\|\cdot\|_{*,\det}$ est la norme duale de $\|\cdot\|_{\det}$

Preuve Soient $(e_j)_{j=1}^d$ une base orthonormée de $(E_{\mathbb{R}}, \|\cdot\|)$, $(e_j^\vee)_{j=1}^d$ sa base duale. Alors $(e_j^\vee)_{j=1}^d$ est une base orthonormée de $(E_{\mathbb{R}}^\vee, \|\cdot\|_*)$

Donc $\|e_1 \wedge \cdots \wedge e_d\|_{\det} = \|e_1^\vee \wedge \cdots \wedge e_d^\vee\|_{*,\det}$.

Comme $\{e_1^\vee \wedge \cdots \wedge e_d^\vee\}$ est la base duale de $\{e_1 \wedge \cdots \wedge e_d\}$, $\|\cdot\|_{*,\det} = \|\cdot\|_{\det,*}$

Corollaire $\mathrm{covol}(E^\vee, \|\cdot\|_*) = \mathrm{covol}(E, \|\cdot\|)^{-1}$

Preuve Soient $(u_j)_{j=1}^n$ une base de E sur $\mathbb{Z}$, $(u_j^\vee)_{j=1}^n$ sa base duale dans $E^\vee$. On a $\|u_1 \wedge \cdots \wedge u_n\|_{\det} = \|u_1^\vee \wedge \cdots \wedge u_n^\vee\|_{*,\det}^{-1}$.

#

M2 2020 Théorie des nombres

Définition Pour tout sous-ensemble A de $E_{\mathbb{R}}$, on définit

$$\rho(A) := \sum_{x \in A} e^{-\pi\|x\|^2} \in [0,+\infty]$$

Proposition Pour tout $x \in E_{\mathbb{R}}$ on a $\rho(E+x) < +\infty$, où $E+x := \{u+x \mid u \in E\}$

En outre, la fonction $\rho_E : E_{\mathbb{R}} \to \mathbb{R}$, $\rho_E(x) := \rho(E+x)$ est lisse et E-périodique.

Preuve Soit $(e_j)_{j=1}^{d}$ une base de E sur $\mathbb{Z}$. Il existe $c>0$ telle que

$$\forall\ (a_1,\dots,a_d) \in \mathbb{R}^d \qquad \|a_1e_1+\dots+a_de_d\|^2 \geqslant c\,(a_1^2+\dots+a_d^2)$$

On obtient que, $\forall\ x = b_1e_1+\dots+b_de_d \in E_{\mathbb{R}}$,

$$\rho(E+x) \leqslant \sum_{(a_1,\dots,a_d)\in\mathbb{Z}^d} e^{-c\pi\left((a_1+b_1)^2+\dots+(a_d+b_d)^2\right)}$$

$$= \prod_{l=1}^{d}\left(\sum_{a\in\mathbb{Z}} e^{-c\pi(a+b_l)^2}\right) < +\infty$$

Une dérivée partielle formelle de ρ_E est de la forme $\sum_{u\in E} P(u+x)\, e^{-\pi\|u+x\|^2}$

où P est un polynôme sur $E_{\mathbb{R}}$. Donc $\forall\ \delta>0\ \exists\ C>0$ tel que

$$|P(y)| \leqslant C\, e^{\delta\|y\|^2} \quad \text{pour tout } y \in E_{\mathbb{R}}.$$

Donc cette série converge uniformément. $\Rightarrow$ ρ_E est lisse sur $E_{\mathbb{R}}$.

Proposition Pour tout $\alpha \in E_{\mathbb{R}}^{\vee}$, on a

$$\int_{E_{\mathbb{R}}} e^{-\pi\|x\|^2 - 2\pi i\alpha(x)}\, dx = e^{-\pi\|\alpha\|_*}$$

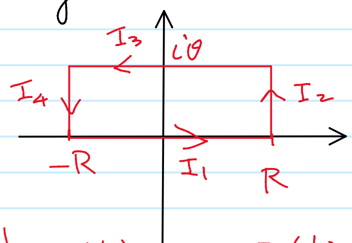
(dx est la mesure de Haar sur $E_{\mathbb{R}}$ telle que le parallélotope engendré par une base orthonormée soit de mesure 1)

Preuve $\forall\ a \in \mathbb{R}$ on a $\int_{\mathbb{R}} e^{-\pi t^2 - 2\pi i a t}\, dt = e^{-\pi a^2}$

$a=0$: $\left(\int_{\mathbb{R}} e^{-\pi t^2} dt\right)^2 = \int_{\mathbb{R}^2} e^{-\pi(x^2+y^2)}\, dx\, dy = \int_0^{+\infty} r\, dr \int_0^{2\pi} e^{-\pi r^2}\, d\theta$

$$= 2\pi\int_0^{+\infty} r e^{-\pi r^2}\, dr = \left[-e^{-\pi r^2}\right]_0^{+\infty} = 1$$

$a \neq 0$ intégrale de la fonction holomorphe $z \mapsto e^{-\pi z^2}$ le long du contour



$$\int_{I_2} e^{-\pi z^2} dz = \int_0^{\theta} e^{-\pi(R^2+2it-t^2)}\, dt \longrightarrow 0 \quad \text{quand } R \to +\infty$$

$$\frac{1}{2} = \int_0^{+\infty} e^{-\pi t^2}\, dt = \int_0^{+\infty} e^{-x}\, \frac{1}{2\sqrt{\pi}}\, \frac{dx}{\sqrt{x}} = \frac{1}{2\sqrt{\pi}}\Gamma\left(\tfrac{1}{2}\right) \Rightarrow \Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi}$$

M2 2020 Théorie des nombres

On suppose que $\alpha \neq 0$. Choisissant une base orthonormée $(e_j)_{j=1}^d$ telle que $(e_j)_{j=1}^{d-1}$ forme une base de $\mathrm{Ker}(\alpha)$. Quitte à remplacer éventuellement e_d par $-e_d$, on peut supposer que $\alpha(e_d) = \|\alpha\|_*$

Par le théorème de Fubini, on obtient

$$\int_{E_{\mathbb{R}}} e^{-\pi\|x\|^2 - 2\pi i \alpha(x)} dx = \left(\int_{\mathbb{R}} e^{-\pi t^2} dt\right)^{d-1} \int_{\mathbb{R}} e^{-\pi t^2 - 2\pi i t \|\alpha\|_*} dt$$
$$= e^{-\pi\|\alpha\|_*^2}$$

$\#$

Théorème Pour tout $x \in E_{\mathbb{R}}$, on a

$$\rho(E+x) = \mathrm{covol}(E)^{-1} \sum_{\alpha \in E^\vee} e^{2\pi i \alpha(x) - \pi\|\alpha\|_*^2}$$

En particulier, $\rho(E) = \mathrm{covol}(\overline{E})^{-1} \rho(E^\vee)$

Preuve Soit $(e_j)_{j=1}^d$ une base de E sur $\mathbb{Z}$.

Soit $D = \{a_1 e_1 + \cdots + a_d e_d \mid (a_1, \ldots, a_d) \in [0,1[^d\}$

On munit $L^2(D, \mathbb{C})$ du produit scalaire $\langle , \rangle_{L^2}$

$$\langle f, g\rangle_{L^2} := \mathrm{Covol}(\overline{E})^{-1} \int_D f(x)\, \overline{g(x)}\, dx$$

Alors $(e^{2\pi i \alpha(\cdot)})_{\alpha \in E^\vee}$ forme une base orthonormée de $L^2(D, \mathbb{C})$

Donc la serie de fonction

$$\mathrm{covol}(\overline{E}) \sum_{\alpha \in E^\vee} e^{2\pi i \alpha(\cdot)} \int_D \rho(E+y)\, e^{-2\pi i \alpha(y)} dy$$

Converge dans $L^2(D, \mathbb{C})$ vers $\rho_E|_D$. Par ailleurs

$$\int_D \rho(E+y)\, e^{-2\pi i \alpha(y)} dy = \int_D \sum_{u \in E} e^{-\pi\|y+u\|^2 - 2\pi i \alpha(y)} dy$$
$$= \int_{E_{\mathbb{R}}} e^{-\pi\|x\|^2 - 2\pi i \alpha(x)} dx = e^{-\pi\|\alpha\|_*^2}$$

Comme ρ_E est continue et $\sum_{\alpha \in E^\vee} e^{-\pi\|\alpha\|_*^2} < +\infty$, cette serie converge uniformément, d'où la première égalité.

La deuxieme égalité se découle de la première en prenant $x=0$.

Définition (serie thêta) $\forall t > 0$ $\Theta_{\overline{E}}(t) := \sum_{u \in E} e^{-\pi t\|u\|^2} = \rho(\sqrt{t} E)$

Proposition $\Theta_{\overline{E}}(t) = \mathrm{covol}(\overline{E})^{-1} t^{-\frac{d}{2}} \Theta_{\overline{E}^\vee}(t^{-1})$

$\mathrm{Covol}(\sqrt{t}E, \|\cdot\|)^{-1} \rho(t^{-\frac{1}{2}} E^\vee)$

$\|$

$t^{-\frac{d}{2}} \mathrm{covol}(\overline{E})^{-1} \Theta_{\overline{E}^\vee}(t^{-1})$

M2 2020 Théorie des nombres

§6 Prolongement méromorphe de $Z_E(s)$

Définition On définit $\xi_E(s) = \pi^{-s}\Gamma(s) Z_E(s)$

Théorème On a

$$\xi_E(s) = \frac{\mathrm{covol}(E)^{-\frac12}}{2s-d} - \frac{1}{2s} + \frac12 \sum_{\mu\in E\setminus\{0\}} G(s,\pi\|\mu\|^2) + \frac12 \sum_{\alpha\in E^\vee\setminus\{0\}} G\left(\tfrac{d}{2}-s, \pi\|\alpha\|^2_*\right)$$

où $G(s,a) = a^{-s}\Gamma(s,a) = \int_1^{+\infty} e^{-at} t^s \frac{dt}{t}$.

Preuve étape 1 $\xi_E(s) = \frac12 \int_0^{+\infty} t^{s-1}(\Theta_E(t)-1)\,dt$ sur $\mathrm{Re}(s) > \frac{d}{2}$

Par le théorème de Fubini, le terme à droite est égal à

$$\frac12 \sum_{\mu\in E\setminus\{0\}} \int_0^{+\infty} t^{s-1} e^{-\pi t\|\mu\|^2} dt = \frac12 \sum_{\mu\in E\setminus\{0\}} \Gamma(s)\,\pi^{-s} \frac{1}{\|\mu\|^{2s}}$$

(formul clé : $\forall a>0 \quad a^{-s}\Gamma(s) = \int_0^{+\infty} t^{s-1} e^{-at} dt$)

étape 2 séparation de l'intégrale

$$\int_0^1 t^{s-1}(\Theta_E(t)-1)\,dt = \int_0^1 t^{s-1}\left(\mathrm{covol}(E)^{-1} t^{-\frac{d}{2}} \Theta_{E^\vee}(t^{-1}) - 1\right) dt$$

$$= \mathrm{covol}(E)^{-1} \int_0^1 t^{s-\frac{d}{2}-1}\left(\Theta_{E^\vee}(t^{-1})-1\right) dt + \int_0^1 t^{s-1}\left(\mathrm{covol}(E)^{-1} t^{-\frac{d}{2}} - 1\right) dt$$

$$= \mathrm{covol}(E)^{-1} \int_1^{+\infty} t^{\frac{d}{2}-s-1}\left(\Theta_{E^\vee}(t)-1\right) dt + \frac{\mathrm{covol}(E)^{-1}}{s-\frac{d}{2}} - \frac1s$$

étape 3 Application de Fubini pour la 2ème fois

$$\int_1^{+\infty} t^{s-1}(\Theta_E(t)-1)\,dt = \sum_{\mu\in E\setminus\{0\}} \int_1^{+\infty} t^{s-1} e^{-\pi t\|\mu\|^2} dt = \sum_{\mu\in E\setminus\{0\}} G(s,\pi\|\mu\|^2)$$

$$\int_1^{+\infty} t^{\frac{d}{2}-s-1}(\Theta_{E^\vee}(t)-1)\,dt = \sum_{\alpha\in E^\vee\setminus\{0\}} G(s, \pi\|\alpha\|^2_*)$$

(ces formules sont valable sur $\mathbb{C}$ car il n'y a plus de problème d'intégrale impropre autour de 0)

Corollaire ① ξ_E admet un prolongement méromorphe sur $\mathbb{C}$, dont les pôles sont 0 et $\frac{d}{2}$. Ces pôles sont simples de résidue $-\frac12$ et $\frac{\mathrm{covol}(E)^{-1}}{2}$ ※

② $\xi_E(s) = \mathrm{covol}(E)^{-1} \xi_{E^\vee}\left(\frac{d}{2}-s\right)$

③ $Z_E(0) = -\frac12$, $Z_E(-k) = 0$ pour tout $k \in \mathbb{N}_{\geq 1}$

§7 Diviseurs

Notation K un corps de nombres

$d = [K:\mathbb{Q}]$, $\mathcal{O}_K$ = fermeture intégrale de $\mathbb{Z}$ dans K

$\Omega_K = \{$places de $K\}$

$\Omega_{K,f} = \{$places finies$\}$ $\Omega_{K,\infty} = \{$places infinies$\}$

Si $v \in \Omega_K$, $|\cdot|_v$: valeur absolue sur K dans la classe v qui prolonge la valeur absolue usuelle sur $\mathbb{Q}$ ou une valeur absolue p-adique.

K_v : Complété de K par rapport à $|\cdot|_v$

$\mathbb{Q}_v$: Complété de $\mathbb{Q}$ par rapport à $|\cdot|_v$

$d_v := [K_v : \mathbb{Q}_v]$

Si $\mathfrak{p} \in \Omega_{K,f}$, $N(\mathfrak{p}) := \mathrm{card}(\mathcal{O}_K/\mathfrak{p})$

$\mathrm{ord}_\mathfrak{p} : K^\times \longrightarrow \mathbb{Z}$ valuation discrète associée à $\mathfrak{p}$

Si p est un nombre premier tel que $\mathfrak{p} | p$

$e(\mathfrak{p}/p)$: indice de ramification $(= \mathrm{ord}_\mathfrak{p}(p))$

$f(\mathfrak{p}/p)$: degré d'inertie $(= [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}])$

Remarque - $d_\mathfrak{p} = e(\mathfrak{p}/p) f(\mathfrak{p}/p)$

- $\forall a \in K^\times$ $d_\mathfrak{p} \ln|a|_\mathfrak{p} = -\mathrm{ord}_\mathfrak{p}(a) \ln(N(\mathfrak{p}))$

(il suffit de vérifier le cas où $a = p$:
$-d_\mathfrak{p} \ln(p) = -e(\mathfrak{p}/p) f(\mathfrak{p}/p) \ln(p)$)

- $\displaystyle\sum_{\sigma \in \Omega_{K,\infty}} d_\sigma = d$

Définition On désigne par $\mathrm{Div}(\mathcal{O}_K)$ le groupe abélien libre engendré par $\Omega_{K,f}$, dont les éléments sont appelés diviseurs sur $\mathcal{O}_K$. Si $D \in \mathrm{Div}(\mathcal{O}_K)$, sont coefficient de coordonnée $\mathfrak{p} \in \Omega_{K,f}$ est noté comme $\mathrm{ord}_\mathfrak{p}(D)$.

Ainsi $$D = \sum_{\mathfrak{p} \in \Omega_{K,f}} \mathrm{ord}_\mathfrak{p}(D) \cdot \mathfrak{p}$$

Soit $N : \mathrm{Div}(\mathcal{O}_K) \longrightarrow \mathbb{N}_{\geq 1}$, $N(D) := \displaystyle\prod_{\mathfrak{p} \in \Omega_{K,f}} N(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(D)}$

C'est un morphisme de groupes

M2 2020 Théorie des nombres

Définition Si $a \in K^\times$, on désigne par (a) le diviseur

$$(a) := \sum_{\mathfrak{p} \in \Omega_{K,f}} \mathrm{ord}_{\mathfrak{p}}(a)\, \mathfrak{p}. \quad \text{On note } N(a) := N((a))$$

Un tel diviseur est appelé un diviseur principal. On désigne par $PDiv(\mathcal{O}_K)$ l'image de $(\cdot) : K^\times \longrightarrow Div(\mathcal{O}_K)$. C'est un sous-groupe de $Div(\mathcal{O}_K)$. On désigne par $Cl(\mathcal{O}_K)$ le groupe quotient $Div(\mathcal{O}_K)/PDiv(\mathcal{O}_K)$

Proposition Le noyau de $(\cdot) : K^\times \longrightarrow Div(\mathcal{O}_K)$ s'identifie à $\mathcal{O}_K^\times$

Preuve Soit $a \in K^\times$ tel que $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ pour tout $\mathfrak{p} \in \Omega_{K,f}$. On a alors $a \in \mathcal{O}_K$ et $a^{-1} \in \mathcal{O}_K$, d'où $a \in \mathcal{O}_K^\times$

※

Définition On dit qu'un diviseur $D \in Div(\mathcal{O}_K)$ est effectif si $\forall\, \mathfrak{p} \in \Omega_{K,f}$, $\mathrm{ord}_{\mathfrak{p}}(D) \geq 0$. On note $D \geq 0$ si D est effectif

On désigne par $Div^+(\mathcal{O}_K)$ le semi-groupe des diviseurs effectifs

Si D_1 et D_2 sont deux diviseurs tels que $D_2 - D_1$ soit effectif, on note $D_1 \leq D_2$ (ou $D_2 \geq D_1$)

Si $D \in Div(\mathcal{O}_K)$, on note

$$H^0(D) := \{a \in K^\times \mid (a) + D \geq 0\} \cup \{0\}$$

C'est un sous-$\mathcal{O}_K$-module de K

Proposition Soit $D \in Div(\mathcal{O}_K)$. On a

$$H^0(D) = \prod_{\mathfrak{p} \in \Omega_{K,f}} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(D)}$$

Preuve

$$\begin{aligned} a \in H^0(D)\setminus\{0\} &\iff \forall\, \mathfrak{p} \in \Omega_{K,f},\ \mathrm{ord}_{\mathfrak{p}}(a) \geq -\mathrm{ord}_{\mathfrak{p}}(D) \\ &\iff a\mathcal{O}_K = \prod_{\mathfrak{p} \in \Omega_{K,f}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a)} \subset \prod_{\mathfrak{p} \in \Omega_{K,f}} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(D)} \\ &\iff a \in \prod_{\mathfrak{p} \in \Omega_{K,\mathfrak{p}}} \mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(D)} \end{aligned}$$

※

Remarque Si I est un idéal fractionnaire de K, alors

$$\varphi : I \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow K \qquad x \otimes q \longmapsto qx \quad \text{est une bijection.}$$

En effet, $\exists\, n \neq 0$ suffisamment divisible tel que $\underbrace{n\mathcal{O}_K \subset}_{\Downarrow} I \underbrace{\subset n^{-1}\mathcal{O}_K}_{\Downarrow}$

φ est surjective $\qquad$ φ est injective

§8 Diviseurs arithmétiques

Définition On désigne par $\widehat{\mathrm{Div}}(\mathcal{O}_K)$ l'ensemble des couples $\overline{D}=(D,g)$, où $D\in \mathrm{Div}(\mathcal{O}_K)$ et $g=(g_\sigma)_{\sigma\in\Omega_{K,\infty}}\in\mathbb{R}^{\oplus\Omega_{K,\infty}}$.
Tout $\overline{D}\in\widehat{\mathrm{Div}}(\mathcal{O}_K)$ est appelé un diviseur arithmétique sur $\mathcal{O}_K$.
Si $a\in K^\times$, soit

$$\widehat{(a)} := \left((a), (-\ln|a|_\sigma)_{\sigma\in\Omega_{K,\infty}}\right)$$

Si $\overline{D}=(D,g)\in\widehat{\mathrm{Div}}(\mathcal{O}_K)$, on définit le degré d'Arakelov de $\overline{D}$ comme

$$\widehat{\deg}(\overline{D}) := \ln N(D) + \sum_{\sigma\in\Omega_{K,\infty}} d_\sigma g_\sigma \qquad \text{où } d_\sigma=[K_\sigma:\mathbb{R}]$$

Proposition Pour tout $a\in K^\times$, on a $\widehat{\deg}(\widehat{(a)})=0$. c'est-à-dire

$$\ln N(a) = \sum_{\sigma\in\Omega_{K,\infty}} d_\sigma \ln|a|_\sigma$$

Preuve C'est une reformulation de la formule du produit.

Proposition Soit $\overline{D}=(D,g)\in\widehat{\mathrm{Div}}(\mathcal{O}_K)$. On munit

$$\begin{array}{ccccccc} H^0(D)\otimes_{\mathbb{Z}}\mathbb{R} & \cong & (H^0(D)\otimes_{\mathbb{Z}}\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{R} & \cong & K\otimes_{\mathbb{Q}}\mathbb{R} & \cong & \bigoplus_{\sigma\in\Omega_{K,\infty}} K_\sigma \\ a\otimes\lambda & & \longmapsto & & (\lambda\sigma(a))_{\sigma\in\Omega_{K,\infty}} & & \end{array}$$

$\|\cdot\|_\sigma = d_\sigma^{\frac{1}{2}} e^{-g_\sigma}|\cdot|_\sigma$

de la norme euclidienne $\|\cdot\|_g$ somme directe orthogonale des $d_\sigma^{\frac{1}{2}} e^{-g_\sigma}|\cdot|_\sigma$
Alors $\mathrm{covol}(H^0(D),\|\cdot\|_g) = \exp(-\widehat{\deg}(\overline{D}))\,\delta_K^{-\frac{1}{2}}$, où $\delta_K=|\mathrm{Disc}_{K/\mathbb{Q}}|$

Preuve Si D_1 et D_2 sont deux diviseurs sur $\mathcal{O}_K$ tels que $D_1\leqslant D_2$, alors

$$H^0(D_2)/H^0(D_1) \cong \bigoplus_{\mathfrak{p}\in\Omega_{K,f}} \left(\mathcal{O}_K/\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(D_2)-\mathrm{ord}_\mathfrak{p}(D_1)}\right)$$

d'où $\mathrm{card}(H^0(D_2)/H^0(D_1)) = \dfrac{N(D_2)}{N(D_1)} = \exp\left(\widehat{\deg}(D_2,g)-\widehat{\deg}(D_1,g)\right)$

Donc $\mathrm{covol}(H^0(D),\|\cdot\|_g)\exp(\widehat{\deg}(D,g))$ ne dépend pas du choix de D.
Par ailleurs, pour D fixé, ce produit ne dépend pas du choix de g.
On peut donc supposer que $\overline{D}=\widehat{(1)}=(0,(0)_{\sigma\in\Omega_{K,\infty}})$ (On note $\|\cdot\|$ la norme)
Soient $(a_j)_{j=1}^d$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$, $(\sigma_j)_{j=1}^d$ l'ensemble des $K\hookrightarrow\mathbb{C}$

$$\forall\,(a,b)\in K^2,\quad \langle a,b\rangle = \sum_{j=1}^d \overline{\sigma_j(a)}\,\sigma_j(b)$$

On étend $\langle,\rangle$ à $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{C}$ pour former un produit hermitien. Soient $(e_j)_{j=1}^d$ une base orthonormée de $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{C}$ et A la matrice de transition de $(e_j)_{j=1}^d$ à $(a_j)_{j=1}^d$.
On a $\mathrm{covol}(\mathcal{O}_K,\|\cdot\|)=|\det A| = \det((\langle a_j,a_k\rangle)_{j,k})^{\frac{1}{2}} = |\det((\sigma_j(a_k))_{j,k})| = \delta_K^{\frac{1}{2}}$

※

§9 Finitude du nombre de classes

Théorème Pour tout $D \in \mathrm{Div}(\mathcal{O}_K)$, il existe $a \in H^0(D)$ tel que

$$N(D+(a)) \leqslant \left(\frac{\pi}{4}\right)^{r_2} \delta_K^{\frac{1}{2}} \left(\frac{d!}{d^d}\right)$$

(Rappel : r_2 = nombre de places complexes)

En outre, $Cl(\mathcal{O}_K)$ est un groupe fini

($\forall T>0$, il n'y a qu'un nombre fini de $\mathfrak{p} \in \mathcal{M}_{K,f}$ telles que $N(\mathfrak{p}) \leq T$. Donc on n'a qu'un nombre fini de choix pour $D+(a)$)

Lemme Pour tout $t>0$, le sous-ensemble

$$X_t = \left\{(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \;\middle|\; |x_1|+\dots+|x_{r_1}|+\sqrt{2}\,(|z_1|+\dots+|z_{r_2}|) \leq t\right\}$$

de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ a pour volume euclidien

$$V(r_1, r_2, t) = t^{r_1+2r_2} \frac{2^{r_1}\pi^{r_2}}{(r_1+2r_2)!} \qquad (*)_{r_1,r_2}$$

Preuve On raisonne par double récurrence en (r_1, r_2)

D'abord $V(0,1,t) = \pi\left(\frac{t}{\sqrt{2}}\right)^2 = \frac{\pi t^2}{2!}$ $\quad V(1,0,t) = 2t$

Supposons $(*)_{r_1,r_2}$, on a

$$V(r_1+1, r_2, t) = 2\int_0^t V(r_1, r_2, t-x)\,dx = \frac{2^{r_1+1}\pi^{r_2}}{(r_1+2r_2)!}\int_0^t (t-x)^{r_1+2r_2}\,dx$$

$$= t^{r_1+1+2r_2} \frac{2^{r_1+1}\pi^{r_2}}{(r_1+1+2r_2)!}$$

coordonnées polaires

$$V(r_1, r_2+1, t) = 2\pi \int_0^{\frac{t}{\sqrt{2}}} x\, V(r_1, r_2, t-\sqrt{2}x)\,dx = \pi \int_0^t x\, V(r_1, r_2, t-x)\,dx$$

$$= \frac{2^{r_1}\pi^{r_2+1}}{(r_1+2r_2)!}\int_0^t \left(t\,(t-x)^{r_1+2r_2} - (t-x)^{r_1+2r_2+1}\right) dx$$

$$= \frac{2^{r_1}\pi^{r_2+1}}{(r_1+2r_2)!}\, t^{r_1+2r_2+2}\left(\frac{1}{r_1+2r_2+1} - \frac{1}{r_1+2r_2+2}\right) = t^{r_1+2(r_2+1)} \frac{2^{r_1}\pi^{r_2+1}}{(r_1+2(r_2+1))!}$$

$\#$

Preuve du théorème

Soit $X_t = \left\{(z_\sigma)_{\sigma\in\Omega_{K,\infty}} \in \prod_{\sigma\in\Omega_{K,\infty}} K_\sigma \;\middle|\; \sum_{\sigma\in\Omega_{K,\infty}} d_\sigma e^{-g_\sigma}|z_\sigma|_\sigma \leqslant t\right\}$.

C'est un corps convexe symétrique dans $H^0(D)\otimes_{\mathbb{Z}}\mathbb{R}$, dont le volume est

$$V(r_1, r_2, t) = t^d \frac{2^{r_1}\pi^{r_2}}{d!}$$

Rappel : r_1 = nombre des places réelles, r_2 = nombre des places complexes

D'après le théorème de Minkowski, $X_t \cap H^0(D) \neq \{0\}$ dès que

$$2^{-d}\, V(r_1, r_2, t) > \mathrm{covol}(H^0(D), \|\cdot\|_g) = \exp(-\widehat{\deg}(D,g))\ \delta_K^{\frac{1}{2}}$$

Comme $H^0(D)$ est discret, $\exists\, a \in H^0(D)\setminus\{0\}$ tel que $\sum_{\sigma\in\Omega_{K,\infty}} d_\sigma e^{-g_\sigma}|a|_\sigma \leqslant \left(\frac{d!\, e^{-\widehat{\deg}(\overline{D})}\delta_K^{\frac{1}{2}}}{(\pi/4)^{r_2}}\right)^{\frac{1}{d}}$

Par l'inégalité arithmético-géométrique, on obtient

$$d\left(\prod_{\sigma\in\Omega_{K,\infty}} e^{-d_\sigma g_\sigma}|a|_\sigma^{d_\sigma}\right)^{\frac{1}{d}} \leqslant \left(\frac{d!\,\delta_K^{\frac{1}{2}}}{(\pi/4)^{r_2}}\, N(D)^{-1} \prod_{\sigma\in\Omega_{K,\infty}} e^{-d_\sigma g_\sigma}\right)^{\frac{1}{d}}$$

Par la formule du produit $N(a) = \prod_{\sigma\in\Omega_{K,\infty}} |a|_\sigma^{d_\sigma}$ on obtient la première inégalité

M2 2020 Théorie des nombres

Corollaire $\delta_K \geq \left(\frac{\pi}{4}\right)^{-2r_2} \frac{d^{2d}}{(d!)^2}$

En particulier, si $K \neq \mathbb{Q}$, alors $\delta_K > 1$

§10 $\mathbb{R}$-diviseurs

Définition On appelle $\mathbb{R}$-diviseur arithmétique sur $\mathcal{O}_K$ tout élément

$$\overline{D} = (D, g) \in \widehat{\mathrm{Div}}_{\mathbb{R}}(\mathcal{O}_K) := \mathbb{R}^{\oplus \Omega_K}$$

où $D \in \mathrm{Div}(\mathcal{O}_K) \otimes_{\mathbb{Z}} \mathbb{R}$, $g = (g_\sigma)_{\sigma \in \Omega_{K,\infty}} \in \mathbb{R}^{\oplus \Omega_{K,\infty}}$

On étend $\mathrm{ord}_p(\cdot)$ en une forme linéaire sur $\mathrm{Div}(\mathcal{O}_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

On dit que $\overline{D}$ est effectif si $\mathrm{ord}_p(D) \geq 0$ pour tout $p \in \Omega_{K,f}$ et si $g_\sigma \geq 0$ pour tout $\sigma \in \Omega_{K,\infty}$

$(\cdot) : K^\times \longrightarrow \mathrm{Div}(\mathcal{O}_K)$ induit une application $\mathbb{R}$-linéaire

$$(\cdot)_{\mathbb{R}} : K^\times_{\mathbb{R}} \longrightarrow \mathrm{Div}(\mathcal{O}_K) \otimes_{\mathbb{Z}} \mathbb{R}$$

$\widehat{(\cdot)} : K^\times \longrightarrow \widehat{\mathrm{Div}}(\mathcal{O}_K)$ induit une application $\mathbb{R}$-linéaire

$$\widehat{(\cdot)}_{\mathbb{R}} : K^\times_{\mathbb{R}} := K^\times \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \widehat{\mathrm{Div}}_{\mathbb{R}}(\mathcal{O}_K)$$

(dont la loi est écrite multiplicativement)

On désigne par $\Lambda : \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{\oplus \Omega_{K,\infty}}$ l'application qui envoie $a \in \mathcal{O}_K^\times$ sur $(-\ln|a|_\sigma)_{\sigma \in \Omega_{K,\infty}}$, qui induit $\Lambda_{\mathbb{R}} : \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}^{\oplus \Omega_{K,\infty}}$

Proposition
1. Le noyau de $(\cdot)_{\mathbb{R}}$ est $\mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R}$
2. $\mathrm{Ker}(\Lambda) = \mu_\infty(K) = \{$racines de l'unité dans $K\}$
3. L'image de Λ est un sous-groupe discret de $\mathbb{R}^{\oplus \Omega_{K,\infty}}$
4. $\widehat{(\cdot)}_{\mathbb{R}}$ est injective

Preuve ① On a vu que le noyau de $(\cdot)$ est $\mathcal{O}_K^\times$. Par la platitude de $\mathbb{R}$ sur $\mathbb{Z}$, on obtient que le noyau de $(\cdot)_{\mathbb{R}}$ est $\mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R}$

②-③ Si $C \subset \mathbb{R}^{\oplus \Omega_{K,\infty}}$ est compact, alors $\Lambda^{-1}(C)$ est fini. En effet, il existe $M > 0$ tel que, $\forall a \in \Lambda^{-1}(C)$, $\forall \sigma : K \to \mathbb{C}$, $|\sigma(a)| \leq M$.

Donc le polynôme minimal de a n'a qu'un nombre fini de choix.

En particulier, $0 \in \Lambda(\mathcal{O}_K^\times)$ est discret $\Rightarrow \Lambda(\mathcal{O}_K^\times) \subset \mathbb{R}^{\oplus \Omega_{K,\infty}}$ est discret

En outre, Λ est un sous-groupe fini de $\mathcal{O}_K^\times$ et donc $\Lambda \subset \mu_\infty(K)$

Réciproquement, si a est une racine de l'unité, alors $\Lambda(a) = 0$

④ Comme $\mathrm{Ker}(\Lambda) = \mu_\infty(K)$ est de torsion, Λ induit un isomorphisme

$$\Lambda_{\mathbb R} : (\mathcal O_K^\times/\mu_\infty(K))\otimes_{\mathbb Z}\mathbb R \cong \mathcal O_K^\times\otimes_{\mathbb Z}\mathbb R \xrightarrow{\sim} \mathrm{Vect}_{\mathbb R}(\Lambda(\mathcal O_K^\times)) \subset \mathbb R^{\oplus\Omega_{K,\infty}}$$

Si $a\in \mathrm{Ker}(\widehat{(\cdot)}_{\mathbb R})$, alors $a \in \mathrm{Ker}(\cdot)_{\mathbb R} = \mathcal O_K^\times\otimes_{\mathbb Z}\mathbb R$

Comme $\widehat{(a)}_{\mathbb R} = ((a)_{\mathbb R}, \Lambda_{\mathbb R}(a))$, on obtient $a=0$ ✠

Théorème (des unités de Dirichlet)

① Soit (D,g) un diviseur arithmétique sur $\mathcal O_K$ tel que $\widehat{\deg}(D,g)\geq 0$. Alors il existe $a\in K_{\mathbb R}^\times$ tel que $\widehat{(a)}_{\mathbb R}+(D,g)$ soit effectif

② Soit $\varphi:\mathbb R^{\oplus\Omega_{K,\infty}}\longrightarrow\mathbb R$ la forme linéaire qui envoie $(g_\sigma)_{\sigma\in\Omega_{K,\infty}}$ sur $\sum_{\sigma\in\Omega_{K,\infty}} d_\sigma g_\sigma$. Alors $\mathrm{Vect}_{\mathbb R}(\Lambda(\mathcal O_K^\times)) = \mathrm{Ker}(\varphi)$.

Preuve

Pour tout $n\in\mathbb N$ tel que $n\geq1$, on choisit $a_n\in H^0(nD)$ tel que

$$\sum_{\sigma\in\Omega_{K,\infty}} d_\sigma e^{-ng_\sigma}|a_n|_\sigma \leq \left(\frac{d!\, e^{-\widehat{\deg}(n\bar D)}\,\delta_K^{\frac12}}{(\pi/4)^{r_2}}\right)^{\frac1d} \leq \left(\frac{d!\,\delta_K^{\frac12}}{(\pi/4)^{r_2}}\right)^{\frac1d} = A_d$$

Rappelons qu'il n'y a qu'un nombre fini de choix pour $nD+(a_n)$. Donc on peut trouver une suite strictement croissante $(n_k)_{k\in\mathbb N}$ dans $\mathbb N\setminus\{0\}$ telle que les $n_kD+(a_{n_k})$ soient identiques

$\forall k\in\mathbb N_{\geq1}$, on a $\frac{1}{n_k-n_0}\left(\frac{a_{n_k}}{a_{n_0}}\right) = D$

Soit $t_k = a_{n_k}^{\frac{1}{n_k-n_0}}\, a_{n_0}^{-\frac{1}{n_k-n_0}}\in K_{\mathbb R}^\times$. On étend $|\cdot|_\sigma$ à une application $\mathbb R$-linéaire $K_{\mathbb R}^\times\longrightarrow\mathbb R_{>0}$ $\circlearrowleft \mathbb R$

$(\lambda,t)\mapsto t^\lambda$

On a $e^{-g_\sigma}|t_k|_\sigma = e^{-g_\sigma}|a_{n_k}|_\sigma^{\frac1{n_k-n_0}}\,|a_{n_0}|_\sigma^{-\frac1{n_k-n_0}}$

$$\leq e^{-g_\sigma}|a_{n_0}|_\sigma^{-\frac1{n_k-n_0}}A_d^{\frac1{n_k-n_0}}e^{\frac{n_k}{n_k-n_0}g_\sigma} = |a_{n_0}|_\sigma^{-\frac1{n_k-n_0}}A_d^{\frac1{n_k-n_0}}e^{\frac{n_0}{n_k-n_0}g_\sigma}$$

Donc $\limsup_{k\to+\infty}(\ln|t_k|_\sigma - g_\sigma)\leq 0$

car $D=(t_k)_{\mathbb R}$

En outre $\sum_{\sigma\in\Omega_{K,\infty}} d_\sigma(\ln|t_k|_\sigma - g_\sigma) = \widehat{\deg}\left(-(D,g)+\widehat{(t_k)}_{\mathbb R}\right) = -\widehat{\deg}(\bar D)$

Donc $(t_k)_{k\in\mathbb N}$ prend valeur dans une partie bornée d'un sous-ensemble affine de rang fini de $K_{\mathbb R}^\times$. Quitte à soustraire une sous-suite, on peut supposer que $(t_k)_{k\in\mathbb N}$ converge vers $a\in K^\times_{\mathbb R}$. Ainsi $\widehat{(a)}_{\mathbb R}+(D,g)\geq0$

Si $\widehat{\deg}(\bar D)=0$, alors $\lim_{k\to\infty} \ln|t_k|_\sigma = g_\sigma$, donc $\widehat{(a)}_{\mathbb R} = (D,g)$. Le cas où $D=0$ et $g\in\mathrm{Ker}(\varphi)$ donne ② ✠

M2 2020 Théorie des nombres

Fonction zêta

§1 Produit infini

Notation Log : $\mathbb{C}\setminus\{0\} \longrightarrow \mathbb{C}$

$z \longmapsto \ln|z| + i\arg(z)$ où $\arg(z) \in]-\pi,\pi]$

Cette fonction est holomorphe sur $\mathbb{C}\setminus\mathbb{R}_{\leq 0}$ et admet le développement

$$\mathrm{Log}(1+z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n} z^n \quad \text{en } 1$$

Il existe donc une fonction holomorphe $\varphi : \mathbb{C}\setminus]-\infty,-1] \longrightarrow \mathbb{C}$ telle que

$$\mathrm{Log}(1+z) = z\varphi(z)$$

On fixe un ensemble infini dénombrable $\mathcal{P}$ et on le munit de la tribu discrète et la mesure de comptage dp

$$\int_A 1\, dp = \mathrm{card}(A)$$

Définition Soit $f : \mathcal{P} \longrightarrow \mathbb{C}\setminus\{0\}$ une application. On dit que le produit $\prod_{p\in\mathcal{P}} f(p)$ converge absolument si $\mathrm{Log}\circ f$ est intégrable sur $\mathcal{P}$, et on définit la valeur de ce produit infini comme

$$\exp\left(\int_{\mathcal{P}} \mathrm{Log}(f(p))\, dp\right)$$

(on a donc $\prod_{p\in\mathcal{P}} |f(p)|$ converge absolument vers $\left|\prod_{p\in\mathcal{P}} f(p)\right|$)

En particulier, si ce produit infini converge absolument, sa valeur est $\neq 0$

Proposition Si $g : \mathcal{P} \longrightarrow \mathbb{C}\setminus\{-1\}$ est intégrable, alors $\prod_{p\in\mathcal{P}} (1+g(p))$ converge absolument.

Preuve Comme g est intégrable, il existe $\mathcal{P}_0 \subset \mathcal{P}$ tel que $\mathcal{P}\setminus\mathcal{P}_0$ soit fini et $|g(p)| \leq t_0^{-1}$ pour tout $p\in\mathcal{P}_0$, où t_0 est l'unique solution de $t_0 \ln(t_0) = 1$ $(\sqrt{2} < t_0 < 2)$

Pour $p \in \mathcal{P}_0$ on a

$$\ln|1+g(p)| \leq \ln(1+|g(p)|) \leq |g(p)|$$

$$-\ln|1+g(p)| \geq -\ln(1-|g(p)|) \leq |g(p)|$$

(par la concavité de $\ln(\cdot)$)

Comme $t_0 > \sqrt{2}$, on a $|\arg(1+g(p))| \leq \frac{\pi}{4}$. Donc

$$|\arg(1+g(p))| \leq |\tan(\arg(1+g(p)))| = \left|\frac{\mathrm{Im}(g(p))}{1+\mathrm{Re}(g(p))}\right| \leq \frac{|g(p)|}{1-|g(p)|} \leq \frac{t_0}{t_0-1}|g(p)|$$

On en déduit $|\mathrm{Log}(1+g(p))| \leq \frac{2t_0-1}{t_0-1}|g(p)|$ sur $\mathcal{P}_0$

·15·

Corollaire ① Soit $(g_n)_{n\in\mathbb{N}}$ une famille d'applications $\mathcal{P}\to\mathbb{C}\setminus\{-1\}$ qui converge simplement vers $g:\mathcal{P}\to\mathbb{C}\setminus\{-1\}$. On suppose qu'il existe $h:\mathcal{P}\to\mathbb{R}_{>0}$ intégrable telle que $|g_n|\leq h$ pour tout $n\in\mathbb{N}$. Alors la suite

$$\prod_{p\in\mathcal{P}}(1+g_n(p)),\ n\in\mathbb{N} \quad \text{converge vers} \quad \prod_{p\in\mathcal{P}}(1+g(p))$$

② Soit $\Omega\subset\mathbb{C}$ une partie ouverte. Soit $g:\mathcal{P}\times\Omega\to\mathbb{C}$ une fonction. Si

- $\forall p\in\mathcal{P}$, $g(p,\cdot)$ est holomorphe sur Ω
- $\forall V\subset\Omega$ compact, il existe $h_V:\mathcal{P}\to\mathbb{R}_{>0}$ intégrable telle que
$$|g(p,s)|\leq h_V(p)\quad\forall s\in V\quad\forall p\in\mathcal{P}$$

Alors $\prod_{p\in\mathcal{P}}(1+g(p,s))$ converge absolument $\forall s\in\Omega$ et définit une fonction holomorphe sur Ω.

§2 Fonctions arithmétiques

Notation $\mathcal{N}$: le monoïde libre engendré par $\mathcal{P}$ (dont la loi est écrite multiplicativement)

$\mathcal{Q}$: le groupe libre engendré par $\mathcal{P}$

Exemple $\mathcal{P}=\{\text{nombre premiers}\}$ $\quad\mathcal{N}=\mathbb{N}\setminus\{0\}$, $\quad\mathcal{Q}=\mathbb{Q}_{>0}\setminus\{0\}$

Si $a\in\mathcal{Q}$, $p\in\mathcal{P}$, $\mathrm{ord}_p(a)$ désigne l'exposant de p dans la décomposition de a en produit des puissance des éléments de $\mathcal{P}$

$$a=\prod_{p\in\mathcal{P}}p^{\mathrm{ord}_p(a)}$$

On munit $\mathcal{Q}$ de la relation d'ordre $|$ « de divisibilité »

$$a\,|\,b \iff \forall p\in\mathcal{P},\ \mathrm{ord}_p(a)\leq\mathrm{ord}_p(b).$$

Définition On appelle fonction arithmétique toute application $f:\mathcal{N}\to\mathbb{C}$.

Si $\forall a\in\mathcal{N}$, on a
$$f(a)=\prod_{p\in\mathcal{P}}f(p^{\mathrm{ord}_p(a)})\quad\text{et si } f(1)=1$$
on dit que f est multiplicative. Soit $M(\mathcal{N})=\left\{\begin{array}{l}\text{fonctions arithmétiques}\\ \text{multiplicatives}\end{array}\right\}$

Si $\quad f(a)=\prod_{p\in\mathcal{P}}f(p)^{\mathrm{ord}_p(a)}\quad$ et si $f(1)=1$

On dit que f est complètement multiplicative.

M2 2020 Théorie des nombres

Définition On désigne par $\mathbb{A}(N)$ l'ensemble des fonction arithmétiques. Cet ensemble est muni des lois de composition suivantes

(1) addition $(f+g)(n) := f(n)+g(n)$

(2) multiplication par un scalaire : $(cf)(n) := cf(n)$

(3) multiplication $(fg)(n) = f(n)g(n)$

(4) convolution

$$(f*g)(n) := \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b)$$

Proposition ① $*$ est commutative et associative

② $(\mathbb{A}(N), +, *)$ est une $\mathbb{C}$-algèbre commutative, dont l'élément unité est $\delta : N \to \mathbb{C}$, $\delta(n) = \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{si } n \neq 1 \end{cases}$

③ $f \in \mathbb{A}(N)$ est inversible pour $*$ si et seulement si $f(1) \neq 0$

④ $\mathbb{M}(N) \subset \mathbb{A}(N)^\times$ est un sous-groupe

Preuve ① $$((f*g)*h)(n) = \sum_{abc=n} f(a)g(b)h(c) = (f*(g*h))(n)$$

② $$(\delta * f)(n) = \sum_{d|n} \delta(d) f\left(\frac{n}{d}\right) = \delta(1)f(n) = f(n)$$

③ Si f est inversible et g est l'inverse de f, alors
$$(f*g)(1) = f(1)g(1) = \delta(1) = 1 \quad \Rightarrow f(1) \neq 0$$
Réciproquement, si $f(1)\neq 0$, on construit l'inverse de f de façon récursive comme : $g(1) = f(1)^{-1}$
$$g(n) = -f(1)^{-1} \sum_{d|n,\, d\neq 1} f(d)\, g\left(\frac{n}{d}\right)$$

④ Supposons $(f,g) \in \mathbb{M}(N)^2$. $(f*g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ab=n} \prod_{p\in\mathcal{P}} f(p^{\mathrm{ord}_p(a)})\, g(p^{\mathrm{ord}_p(b)})$
$$= \prod_{p\in\mathcal{P}} \sum_{j+k=\mathrm{ord}_p(n)} f(p^j)\, g(p^k) = \prod_{p\in\mathcal{P}} (f*g)(p^{\mathrm{ord}_p(n)}).$$
Soient $f\in \mathbb{M}(N)$ et h l'inverse de f. Montrons que $h(n) = \prod_{p\in\mathcal{P}} h(p^{\mathrm{ord}_p(n)})$ par récurrence sur $\sum_p \mathrm{ord}_p(n)$
$$h(n) = -\sum_{\substack{ab=n\\ a\neq 1}} \prod_{p\in\mathcal{P}} f(p^{\mathrm{ord}_p(a)})\, h(p^{\mathrm{ord}_p(b)}) = \prod_p h(p^{\mathrm{ord}_p(n)}) - \boxed{\prod_p \sum_{j+k=\mathrm{ord}_p(n)} f(p^j)\, h(p^k)} = \prod_p \delta(p^{\mathrm{ord}_p(n)})$$

M2 2020 Théorie des nombres

Exemples - Fonction constante $\mathbb{1}$

$\mathbb{1}(n) = 1 \quad \forall n \in \mathcal{N}$

- $\Omega : \mathcal{N} \to \mathbb{N}$

$\Omega(n) = \sum_{p \in \mathcal{P}} \mathrm{ord}_p(n)$

- Fonction de Möbius μ : inverse de $\mathbb{1}$

$$\mu(p^k) = -\sum_{j=0}^{k-1} \mu(p^j) = \begin{cases} 1, & k=0 \\ -1, & k=1 \\ 0, & k \geq 2 \end{cases}$$

Donc
$$\mu(n) = \begin{cases} \prod_{p \in \mathcal{P}} (-1)^{\mathrm{ord}_p(n)}, & \text{si } \forall p \in \mathcal{P},\ \mathrm{ord}_p(n) \leq 1 \\ 0, & \text{sinon} \end{cases}$$

§3 Fonction L

On fixe desormais une fonction complètement multiplicative $N : \mathcal{N} \to \mathbb{R}_{\geq 1}$

Définition Si f est une fonction arithmétique. On désigne par $L(f,s)$ la série de fonctions sur $\mathbb{C}$:
$$L(f,s) = \sum_{n \in \mathcal{N}} \frac{f(n)}{N(n)^s}$$

Proposition Soit $R \in \mathbb{R}$, si $\sum_{n \in \mathcal{N}} \frac{|f(n)|}{N(n)^R} < +\infty$, alors la serie $L(f,s)$ converge normalement sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geq R\}$ et définit une fonction holomorphe sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > R\}$

Preuve Si $\mathrm{Re}(s) \geq R$, alors
$$\left| \frac{f(n)}{N(n)^s} \right| = \frac{|f(n)|}{N(n)^{\mathrm{Re}(s)}} \leq \frac{|f(n)|}{N(n)^R}.$$
$\not\forall$

Proposition Soit f une fonction multiplicative. Soit $R \in \mathbb{R}$. On suppose que, $\forall \varepsilon > 0$, $\sum_{p \in \mathcal{P}} \sum_{k=1}^{+\infty} \frac{|f(p^k)|}{N(p)^{k(R+\varepsilon)}} < +\infty$

Alors, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > R$,

① La série $L(f,s)$ converge absolument, et la convergence est normale sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geq R + \varepsilon\}$ quel que soit $\varepsilon > 0$

② Le produit infini $\prod_{p \in \mathcal{P}} \sum_{k \in \mathbb{N}} \frac{f(p^k)}{N(p)^{ks}}$ converge absolument vers $L(f,s)$

③ $L(f,\cdot)$ est holomorphe et non nul sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > R\}$

Preuve On choisit une suite $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \cdots \subset \mathcal{P}_k \subset \cdots$ de sous-ensembles finis de $\mathcal{P}$ telle que $\bigcup_{k\in\mathbb{N}} \mathcal{P}_k = \mathcal{P}$

Le produit infini

$$\prod_{p\in\mathcal{P}} \sum_{j\in\mathbb{N}} \frac{f(p^j)}{N(p)^{js}} \quad \text{Converge absolument sur } \{s\in\mathbb{C} \mid \mathrm{Re}(s)\geq R+\varepsilon\} \quad (\forall \varepsilon>0)$$

En outre

$$(*) \quad \lim_{k\to+\infty} \prod_{p\in\mathcal{P}_k} \sum_{j=0}^{k} \frac{f(p^j)}{N(p)^{js}} = \prod_{p\in\mathcal{P}} \sum_{j\in\mathbb{N}} \frac{f(p^j)}{N(p)^{js}}$$

$$(**) \quad \lim_{k\to\infty} \prod_{p\in\mathcal{P}_k} \sum_{j=0}^{k} \frac{|f(p^j)|}{N(p)^{j(R+\varepsilon)}} = \prod_{p\in\mathcal{P}} \sum_{j\in\mathbb{N}} \frac{|f(p^j)|}{N(p)^{j(R+\varepsilon)}} < +\infty$$

$(**)$ montre que

$$\lim_{k\to+\infty} \sum_{\substack{n\in\mathcal{N} \\ \forall p\in\mathcal{P}_k,\ \mathrm{ord}_p(n)\leq k \\ \forall p\in\mathcal{P}\setminus\mathcal{P}_k,\ \mathrm{ord}_p(n)=0}} \frac{|f(n)|}{N(n)^{R+\varepsilon}} = \sum_{n\in\mathcal{N}} \frac{|f(n)|}{N(n)^{R+\varepsilon}} < +\infty, \quad \text{et donc}$$

$L(f,s)$ converge normalement sur $\{s\in\mathbb{C} \mid \mathrm{Re}(s)\geq R+\varepsilon\}$, et définit une fonction holomorphe sur $\{s\in\mathbb{C} \mid \mathrm{Re}(s)> R\}$

De plus

$$\lim_{k\to\infty} \sum_{\substack{n\in\mathcal{N} \\ \forall p\in\mathcal{P}_k,\ \mathrm{ord}_p(n)\leq k \\ \forall p\in\mathcal{P}\setminus\mathcal{P}_k,\ \mathrm{ord}_p(n)=0}} \frac{f(n)}{N(n)^s} = \lim_{k\to\infty} \prod_{p\in\mathcal{P}_k} \sum_{j=0}^{k} \frac{f(p^j)}{N(p)^{js}}$$

donne

$$L(f,s) = \prod_{p\in\mathcal{P}} \sum_{j\in\mathbb{N}} \frac{f(p^j)}{N(p)^{js}} \neq 0$$

#

Exemple Fonction ζ de Dedekind

Soient K un corps de nombres, $\mathcal{P}=\Omega_{K,f}$, $\mathcal{N}=\mathrm{Div}^+(\mathcal{O}_K)=\{\text{diviseurs effectifs}\}$

$$N : \mathrm{Div}^+(\mathcal{O}_K) \longrightarrow \mathbb{R}_{\geq 1} \qquad N(D)=\prod_{\mathfrak{p}\in\Omega_{K,f}} \mathrm{card}(\mathcal{O}_K/\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(D)}$$

Si $\mathfrak{p}\mid p$, alors $N(\mathfrak{p})\geq p$. En outre $\sum_{\mathfrak{p}\mid p} 1 \leq \sum_{\mathfrak{p}\mid p} [K_\mathfrak{p}:\mathbb{Q}_p] = [K:\mathbb{Q}]$

Donc, $\forall\varepsilon>0$

$$\sum_{\mathfrak{p}\in\Omega_{K,f}} \sum_{k=1}^{+\infty} \frac{1}{N(\mathfrak{p})^{k(1+\varepsilon)}} = \sum_{p \text{ premier}} \sum_{\mathfrak{p}\mid p} \sum_{k=1}^{+\infty} \frac{1}{N(\mathfrak{p})^{k(1+\varepsilon)}} \leq [K:\mathbb{Q}] \sum_{p \text{ premier}} \sum_{k=1}^{\infty} \frac{1}{p^{k(1+\varepsilon)}}$$

$$\leq 2[K:\mathbb{Q}] \sum_{p \text{ premier}} \frac{1}{p^{1+\varepsilon}} < +\infty.$$

Donc $\zeta_K(s) = L(\mathbb{1},s) = \prod_{\mathfrak{p}\in\Omega_{K,f}} \frac{N(\mathfrak{p})^s}{N(\mathfrak{p})^s-1}$ Converge absolument sur $\mathrm{Re}(s)>1$.

§4 Formule intégrale de Hecke

Notations

K : corps de nombres $\qquad \mathcal{O}_K$: fermeture intégrale de $\mathbb{Z}$ dans K

$d = [K:\mathbb{Q}] \qquad \delta_K = |\mathrm{Disc}_{K/\mathbb{Q}}|$

$\Omega_K = \{\text{places de } K\} \quad \Omega_{K,f} = \{\text{places finies}\} \quad \Omega_{K,\infty} = \{\text{places infinies}\}$

r_1 = nombre de places réelles, r_2 = nombre de places complexes, $r = r_1 + r_2 - 1$

$\forall \sigma \in \Omega_{K,\infty}$, soit $d_\sigma = [K_\sigma : \mathbb{R}]$. On a $\sum_{\sigma \in \Omega_{K,\infty}} d_\sigma = d$.

$\mathrm{Div}(\mathcal{O}_K) = \mathbb{Z}^{\oplus \Omega_{K,f}} \qquad \mathrm{Div}^+(\mathcal{O}_K) = \{D \in \mathrm{Div}(\mathcal{O}_K) \mid \forall \mathfrak{p}, \mathrm{ord}_\mathfrak{p}(D) \geq 0\}$

$\mathrm{PDiv}(\mathcal{O}_K) = \{(a) := \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(a) \cdot \mathfrak{p} \mid a \in K^\times\} \qquad Cl(\mathcal{O}_K) = \mathrm{Div}(\mathcal{O}_K)/\mathrm{PDiv}(\mathcal{O}_K)$

$h_K = \mathrm{card}(Cl(\mathcal{O}_K)) \qquad w_K = \mathrm{card}(\mu_\infty(K))$

Rappel : $a^{-s}\Gamma(s) = \int_0^{+\infty} t^{-s-1} e^{-\frac{a}{t}} dt = 2\int_\mathbb{R} e^{-2st - ae^{2t}} dt \qquad (*)$

On fixe une famille $(\theta_j)_{j=1}^r$ d'éléments de $\mathcal{O}_K^\times$ dont les images dans $\mathcal{O}_K^\times/\mu_\infty(K)$ forment une base de ce dernier sur $\mathbb{Z}$.

Si $\lambda = (\lambda_j)_{j=1}^r$ est un élément de $[0,1]^r$, soit $\|\cdot\|_\lambda : \mathbb{R}^{\oplus \Omega_{K,\infty}} \longrightarrow \mathbb{R}_{\geq 0}$

$$\|(y_\sigma)_{\sigma \in \Omega_{K,\infty}}\|_\lambda := \sum_{\sigma \in \Omega_{K,\infty}} d_\sigma y_\sigma^2 \left(\prod_{j=1}^r |\theta_j|_\sigma^{\lambda_j}\right)$$

Remarque Soit $\Psi : \mathbb{R}^{\oplus \Omega_{K,\infty}} \longrightarrow \mathbb{R}^{\oplus \Omega_{K,\infty}}$, $(x_\sigma)_{\sigma \in \Omega_{K,\infty}} \longmapsto (d_\sigma x_\sigma)_{\sigma \in \Omega_{K,\infty}}$

On considère deux normes $\|\cdot\|$ et $\|\cdot\|'$ sur $\mathbb{R}^{\oplus \Omega_{K,\infty}}$, $\|x\| = \left(\sum_\sigma d_\sigma x_\sigma^2\right)^{\frac{1}{2}}$, $\|x\|' = \left(\sum_\sigma x_\sigma^2\right)^{\frac{1}{2}}$

Alors $\dfrac{\|\cdot\|'_{\det}}{\|\cdot\|_{\det}} = \prod_{\sigma \in \Omega_{K,\infty}} d_\sigma^{-\frac{1}{2}}$, d'où $\dfrac{\|\det(\Psi)(\eta)\|'_{\det}}{\|\eta\|_{\det}} = \prod_{\sigma \in \Omega_{K,\infty}} d_\sigma^{\frac{1}{2}} = 2^{\frac{r_2}{2}}$

On considère deux formes linéaires φ et φ' sur $\mathbb{R}^{\oplus \Omega_{K,\infty}}$, $\varphi(x) = \sum_\sigma d_\sigma x_\sigma$, $\varphi'(x) = \sum_\sigma x_\sigma$

Si $\{x^{(1)}, \dots, x^{(r)}\}$ est une base de $\mathrm{Ker}(\varphi)$, alors $\{\Psi(x^{(1)}), \dots \Psi(x^{(r)})\}$ est une base de $\mathrm{Ker}(\varphi')$

Soit $y = (1, \dots, 1)$. On a $y \perp_{\|\cdot\|} \mathrm{Ker}(\varphi)$, $y \perp_{\|\cdot\|'} \mathrm{Ker}(\varphi')$, $\Psi(y) - \frac{d}{r_1+r_2} y \in \mathrm{Ker}(\varphi')$

Donc
$$\|\Psi(x^{(1)}) \wedge \dots \wedge \Psi(x^{(r)})\|_{\mathrm{Ker}(\varphi'), \det} = \frac{\|\Psi(x^{(1)}) \wedge \dots \wedge \Psi(x^{(r)}) \wedge \Psi(y)\|'_{\det}}{\frac{d}{r_1+r_2}\|y\|'}$$

$$= 2^{\frac{r_2}{2}} \frac{\|x^{(1)} \wedge \dots \wedge x^{(r)} \wedge y\|_{\det}}{d/\sqrt{r_1+r_2}} = 2^{\frac{r_2}{2}} \frac{\sqrt{r_1+r_2}}{d} \|x^{(1)} \wedge \dots \wedge x^{(r)}\|_{\mathrm{Ker}(\varphi), \det} \cdot \|y\|$$

$$= 2^{\frac{r_2}{2}} \sqrt{\frac{r_1+r_2}{d}} \|x^{(1)} \wedge \dots \wedge x^{(r)}\|_{\mathrm{Ker}(\varphi), \det}.$$

Proposition Pour tout $s\in\mathbb{C}$ tel que $Re(s)>\frac{d}{2}$ et tout $a\in K^\times$, on a

$$2^{-r_2 s}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}N(a)^{-s}=\frac{dR_K}{w_K}2^{r_1-1}\Gamma\left(\frac{ds}{2}\right)\sum_{\theta\in\mathcal{O}_K^\times}\int_{[-\frac12,\frac12]^r}\|a\theta\|_\lambda^{-ds}d\lambda$$

(On précisera la valeur de R_K dans la preuve)

Preuve D'après la formule du produit, on a

$$N(a)^{-s}=\prod_{\sigma\in\Omega_{K,\infty}}|a|_\sigma^{-d_\sigma s}$$

En outre, on a $2^{-r_2}=\prod_{\sigma\in\Omega_{K,\infty}}d_\sigma^{-\frac{d_\sigma}{2}}$. Donc

$$2^{-r_2 s}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}N(a)^{-s}=\prod_{\sigma\in\Omega_{K,\infty}}\left(d_\sigma|a|_\sigma^2\right)^{-\frac{d_\sigma s}{2}}\Gamma\left(\frac{d_\sigma s}{2}\right)$$

$$=2^{r_1}\int_{(\mathbb{R}^{\oplus\Omega_{K,\infty}},\|\cdot\|')}\exp\left(-s\sum_\sigma d_\sigma x_\sigma-\sum_\sigma d_\sigma|a|_\sigma^2e^{2x_\sigma}\right)\eta'(dx)$$

mesure de Lebesgue associée à $\|\cdot\|'$

$$=2^{r_1+\frac{r_2}{2}}\int_{\underset{=\mathbb{R}y\oplus Ker(\varphi)}{(\mathbb{R}^{\oplus\Omega_{K,\infty}},\|\cdot\|)}}\exp\left(-s\sum_\sigma d_\sigma x_\sigma-\sum_\sigma d_\sigma|a|_\sigma^2e^{2x_\sigma}\right)\eta(dx)$$

celle associée à $\|\cdot\|$

$x=u+ty$

$$=2^{r_1+\frac{r_2}{2}}\int_{Ker(\varphi)}\eta_{Ker(\varphi)}(du)\int_{\mathbb{R}}\sqrt{d}\exp\left(-std-\sum_\sigma d_\sigma|a|_\sigma^2e^{2u_\sigma}e^{2t}\right)dt$$

$$=\sqrt{d}\,2^{r_1+\frac{r_2}{2}-1}\Gamma\left(\frac{sd}{2}\right)\int_{Ker(\varphi)}\left(\sum_\sigma d_\sigma|a|_\sigma^2e^{2u_\sigma}\right)^{-\frac{ds}{2}}\eta_{Ker(\varphi)}(du)$$

$$=\sqrt{d}\,2^{r_1+\frac{r_2}{2}-1}\Gamma\left(\frac{sd}{2}\right)\sum_{[\theta]\in\mathcal{O}_K^\times/\mu_\infty(K)}\operatorname{covol}\left(\Lambda(\mathcal{O}_K^\times),\|\cdot\|_{Ker(\varphi)}\right)\int_{[-\frac12,\frac12]^r}\|a\theta\|_\lambda^{-ds}d\lambda$$

mesure usuelle

$$=\frac{1}{w_K}\sqrt{d}\,2^{r_1+\frac{r_2}{2}-1}\Gamma\left(\frac{sd}{2}\right)\operatorname{covol}\left(\Phi(\Lambda(\mathcal{O}_K^\times)),\|\cdot\|'_{Ker(\varphi)}\right)\cdot2^{-\frac{r_2}{2}}\sqrt{\frac{d}{r_1+r_2}}$$
$$\sum_{\theta\in\mathcal{O}_K^\times}\int_{[-\frac12,\frac12]^r}\|a\theta\|_\lambda^{-ds}d\lambda$$

$$=\frac{dR_K}{w_K}2^{r_1-1}\Gamma\left(\frac{sd}{2}\right)\sum_{\theta\in\mathcal{O}_K^\times}\int_{[-\frac12,\frac12]^r}\|a\theta\|_\lambda^{-ds}d\lambda$$

où le régulateur R_K est défini comme

$$R_K:=\frac{\operatorname{covol}\left(\Phi(\Lambda(\mathcal{O}_K^\times)),\|\cdot\|'_{Ker(\varphi)}\right)}{\sqrt{r_1+r_2}}$$

Définition On définit $\xi_K(s) := \left(2^{-r_2}\delta_K^{\frac{1}{2}}\pi^{-\frac{d}{2}}\right)^s \Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$

Théorème Pour tout $\alpha \in Cl(\mathcal{O}_K)$, on choisit $D_\alpha \in Div(\mathcal{O}_K)$ tel que $-D_\alpha \in \alpha$

On a
$$\frac{w_K}{2^{r_1} d R_K}\xi_K(s) = \sum_{\alpha \in Cl(\mathcal{O}_K)} \frac{\delta_K^{\frac{s}{2}}}{N(D_\alpha)^s}\int_{\lambda \in [-\frac{1}{2},\frac{1}{2}]^r} \xi_{(H^0(D_\alpha),\, \|\cdot\|_\lambda)}\left(\frac{ds}{2}\right) d\lambda$$

Preuve Par définition, on a
$$\zeta_K(s) = \sum_{D \in Div^+(\mathcal{O}_K)} \frac{1}{N(D)^s} = \sum_{\alpha \in Cl(\mathcal{O}_K)} \sum_{D \in \alpha} \frac{1}{N(D)^s}$$
$$= \sum_{\alpha \in Cl(\mathcal{O}_K)} \sum_{[a] \in (H^0(D_\alpha)\setminus\{0\})/\mathcal{O}_K^\times} \frac{1}{N\left((a)+D_\alpha\right)^s}$$
$$= \sum_{\alpha \in Cl(\mathcal{O}_K)} \frac{1}{N(D_\alpha)^s} \sum_{[a] \in (H^0(D_\alpha)\setminus\{0\})/\mathcal{O}_K^\times} \frac{1}{N(a)^s}$$

D'après la proposition précédente,
$$2^{-r_2 s}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$$
$$= \frac{dR_K}{w_K}2^{r_1-1}\Gamma\left(\frac{ds}{2}\right)\sum_{\alpha \in Cl(\mathcal{O}_K)}\frac{1}{N(D_\alpha)^s}\sum_{[a] \in (H^0(D_\alpha)\setminus\{0\})/\mathcal{O}_K^\times}\ \sum_{\theta \in \mathcal{O}_K^\times}\int_{[-\frac{1}{2},\frac{1}{2}]^r}\frac{1}{\|a\theta\|_\lambda^{ds}}d\lambda$$
$$= \frac{dR_K}{w_K}2^{r_1-1}\Gamma\left(\frac{ds}{2}\right)\sum_{\alpha \in Cl(\mathcal{O}_K)}\frac{1}{N(D_\alpha)^s}\int_{[-\frac{1}{2},\frac{1}{2}]^r}\sum_{a \in H^0(D_\alpha)\setminus\{0\}}\frac{1}{\|a\|_\lambda^{ds}}d\lambda$$
$$= \frac{dR_K}{w_K}2^{r_1}\sum_{\alpha \in Cl(\mathcal{O}_K)}\frac{1}{N(D_\alpha)^s}\int_{[-\frac{1}{2},\frac{1}{2}]^r}\Gamma\left(\frac{ds}{2}\right)Z_{(H^0(D_\alpha),\, \|\cdot\|_\lambda)}\left(\frac{ds}{2}\right)d\lambda$$

Donc $\xi_K(s) = \left(2^{-r_2}\delta_K^{\frac{1}{2}}\pi^{-\frac{d}{2}}\right)^s\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$
$$= \frac{dR_K\delta_K^{\frac{s}{2}}}{w_K}2^{r_1}\sum_{\alpha \in Cl(\mathcal{O}_K)}\frac{1}{N(D_\alpha)^s}\int_{[-\frac{1}{2},\frac{1}{2}]^r}\underbrace{\pi^{-\frac{ds}{2}}\Gamma\left(\frac{ds}{2}\right)Z_{(H^0(D_\alpha),\|\cdot\|_\lambda)}\left(\frac{ds}{2}\right)}_{=\ \xi_{(H^0(D_\alpha),\|\cdot\|_\lambda)}\left(\frac{ds}{2}\right)}d\lambda$$

On en déduit
$$\frac{w_K}{2^{r_1}dR_K}\xi_K(s) = \sum_{\alpha \in Cl(\mathcal{O}_K)}\frac{\delta_K^{\frac{s}{2}}}{N(D_\alpha)^s}\int_{[-\frac{1}{2},\frac{1}{2}]^r}\xi_{(H^0(D_\alpha),\, \|\cdot\|_\lambda)}\left(\frac{ds}{2}\right)d\lambda$$

✕

M2 2020 Théorie des nombres

Remarque Pour tout $\lambda \in [-\frac{1}{2}, \frac{1}{2}]^r$ soient

$$g_\lambda = \left(-\sum_{j=1}^{r} \lambda_j \ln|\theta_j|_\sigma\right)_{\sigma \in \Omega_{K,\infty}}$$

$$g_\lambda^{(0)} = \left(g_{\lambda,\sigma} - \frac{1}{d}\widehat{\deg}(D_\alpha, g_\lambda) + \frac{1}{2d}\ln(\delta_K)\right)_{\sigma \in \Omega_{K,\infty}}$$

Alors on a $\|\cdot\|_\lambda = \|\cdot\|_{g_\lambda}$ et $\mathrm{Card}(H^0(D_\alpha), \|\cdot\|_{g_\lambda^{(0)}}) = 1$

On note $\|\cdot\|_\lambda^{(0)} = \|\cdot\|_{g_\lambda^{(0)}} = \exp\left(-\frac{1}{d}\underbrace{\widehat{\deg}(D_\alpha, g_\lambda)}_{= \ln N(D_\alpha)}\right) \delta_K^{\frac{1}{2d}} \|\cdot\|_\lambda$

Ainsi on peut réécrire le théorème précédent :

$$\frac{w_K}{2^{r_1} d R_K} \xi_K(s) = \sum_{\alpha \in Cl(\mathcal{O}_K)} \int_{[-\frac{1}{2}, \frac{1}{2}]^r} \xi_{(H^0(D_\alpha), \|\cdot\|_\lambda^{(0)})}\left(\frac{ds}{2}\right) d\lambda$$

Corollaire ① ξ_K admet un prolongement méromorphe sur tout plan complexe, ayant un seul pôle simple en $s=1$ avec

$$\mathrm{Res}(\xi_K, 1) = 2^{r_1} (2\pi)^{r_2} \frac{h_K R_K}{w_K \delta_K^{\frac{1}{2}}}$$

② $\xi_K(s) = \xi_K(1-s)$

Preuve ① On étend $\xi_{(H^0(D_\alpha), \|\cdot\|_\lambda^{(0)})}\left(\frac{ds}{2}\right)$ à une fonction méromorphe sur $\mathbb{C}$

Cette fonction à deux pôles simples en $s=0$ et $s=1$, dont les résidues sont $-\frac{1}{d}$ et $\frac{1}{d}$ respectivement

On en déduit que ξ_K a deux pôles simples en $s=0$ et $s=1$, dont les résidues sont $-\frac{2^{r_1} R_K h_K}{w_K}$ et $\frac{2^{r_1} R_K h_K}{w_K}$ respectivement

Comme Γ a un pôle en 0, ζ_K n'a pas de pôle en 0. Cependant, elle a un pôle en 1 dont la résidue est

$$\frac{2^{r_1} R_K h_K}{w_K} \frac{2^{r_2} \pi^{\frac{d}{2}}}{\delta_K^{\frac{1}{2}}} \underbrace{\Gamma(\tfrac{1}{2})}_{\sqrt{\pi}}{}^{-r_1} \Gamma(1)^{-r_2} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \delta_K^{\frac{1}{2}}}$$

Préparation pour la preuve de ②

Proposition L'application $\{a\in K \mid \forall x\in\mathcal{O}_K,\ \mathrm{Tr}_{K/\mathbb{Q}}(ax)\in\mathbb{Z}\} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_K,\mathbb{Z})$, $a \longmapsto (x\mapsto \mathrm{Tr}_{K/\mathbb{Q}}(ax))$

est un isomorphisme de $\mathcal{O}_K$-modules

Preuve La forme bilinéaire $K\times K\longrightarrow\mathbb{Q}$, $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$ est non-dégénérée

Pour tout $x\in K$, il exist $n\in\mathbb{Z}\setminus\{0\}$ tel que $nx\in\mathcal{O}_K$.

Si $\mathrm{Tr}_{K/\mathbb{Q}}(ax)=0\ \forall x\in\mathcal{O}_K$, alors $\mathrm{Tr}_{K/\mathbb{Q}}(ax)=0\ \forall x\in K$

et donc $a=0$. Cela montre l'injectivité

Surjectivité : Soit $f:\mathcal{O}_K\to\mathbb{Z}$ une forme $\mathbb{Z}$-linéaire. Alors f induit une forme $\mathbb{Q}$-linéaire $f_{\mathbb{Q}}:\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Q}=K\longrightarrow\mathbb{Q}$. Donc il existe $a\in K$ tel que $f_{\mathbb{Q}}(x)=\mathrm{Tr}_{K/\mathbb{Q}}(ax)$ (par la dégénérescence de $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$)

On obtient alors que $f(x)=\mathrm{Tr}_{K/\mathbb{Q}}(ax)\ \forall x\in\mathcal{O}_K$.

Par définition, $\forall x\in\mathcal{O}_K$ on a $f(x)=\mathrm{Tr}_{K/\mathbb{Q}}(ax)\in\mathbb{Z}$.

Définition D'après la proposition précédente, $\{a\in K\mid\forall x\in\mathcal{O}_K,\ \mathrm{Tr}_{K/\mathbb{Q}}(ax)\in\mathbb{Z}\}$ est un sous-$\mathcal{O}_K$-module de type fini de K, donc est un idéal fractionnaire. On désigne par $\omega_{\mathcal{O}_K/\mathbb{Z}}$ le diviseur dans $\mathrm{Div}(\mathcal{O}_K)$ tel que $H^0(\omega_{\mathcal{O}_K/\mathbb{Z}})$ s'identifie à cet idéal fractionnaire.

Proposition Soit $(D,g)\in\widehat{\mathrm{Div}}(\mathcal{O}_K)$. L'application

$\psi: H^0(\omega_{\mathcal{O}_K/\mathbb{Z}}-D)\longrightarrow H^0(D)^\vee$, $a\longmapsto(b\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(ab))$ est un isomorphisme de $\mathbb{Z}$-modules, qui induit une isométrie entre $\|\cdot\|_{-g}$ et $\|\cdot\|_{g,*}$

Preuve Montrons que l'application est bien défini

Si $a\in H^0(\omega_{\mathcal{O}_K/\mathbb{Z}}-D)\setminus\{0\}$, $(a)+\omega_{\mathcal{O}_K/\mathbb{Z}}-D\geq 0$

Ainsi, pour tout $b\in H^0(D)\setminus\{0\}$, $(ab)+\omega_{\mathcal{O}_K/\mathbb{Z}}=(a)+\omega_{\mathcal{O}_K/\mathbb{Z}}-D+(b)+D\geq 0$

On obtient donc $ab\in H^0(\omega_{\mathcal{O}_K/\mathbb{Z}})$.

On a $H^0(D)\otimes_{\mathbb{Z}}\mathbb{Q}\cong K$. Donc ψ est une application injective.

Comme $H^0(D)$ est un $\mathcal{O}_K$-module, si, $\forall b\in H^0(D)$, $\mathrm{Tr}_{K/\mathbb{Q}}(ab)\in\mathbb{Z}$, alors $ab\in H^0(\omega_{\mathcal{O}_K/\mathbb{Z}})$. Par la non-dégénérescence de $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$, ψ est surjective

M2 2020 Théorie des nombres

Il reste à montrer que l'application définie une isométrie.

Soit $a \in H^0(\omega_{\mathcal{O}_K/\mathbb{Z}} - D)$. On a $\|a \otimes 1\|_{-g}^2 = \sum_{\sigma \in \Omega_{K,\infty}} d_\sigma e^{2g_\sigma} |\sigma(a)|^2$

et $$\|\psi(a)\|_{g,*} = \sup_{b \in K \setminus \{0\}} \frac{|Tr_{K/\mathbb{Q}}(ab)|}{\|b \otimes 1\|_g}$$

$$= \sup_{b \in K \setminus \{0\}} \frac{\left| \sum_{\sigma \in \Omega_{K,\infty}} Re(\sigma(a)\sigma(b)) \right|}{\left(\sum_{\sigma \in \Omega_{K,\infty}} d_\sigma e^{-2g_\sigma} |\sigma(b)|^2 \right)^{\frac{1}{2}}}$$

$$= \sup_{b \in K \setminus \{0\}} \frac{\langle (e^{2g_\sigma}\sigma(a))_{\sigma \in \Omega_{K,\infty}}, (\sigma(b))_{\sigma \in \Omega_{K,\infty}} \rangle_g}{\|(\sigma(b))_{\sigma \in \Omega_{K,\infty}}\|_g}$$

(K est dense) $= \|(e^{2g_\sigma}\sigma(a))_{\sigma \in \Omega_{K,\infty}}\|_g = \sum_{\sigma \in \Omega_{K,\infty}} d_\sigma \, e^{2g} \cdot e^{2g} \cdot e^{-2g} |\sigma(a)|^2$ ⌗

Corollaire $\widehat{\deg}(\omega_{\mathcal{O}_K/\mathbb{Z}}, 0) = \ln N(\omega_{\mathcal{O}_K/\mathbb{Z}}) = \ln(\delta_K)$

Preuve $(H^0(\omega_{\mathcal{O}_K/\mathbb{Z}}), \|\cdot\|_0) \cong (H^0(\mathcal{O}_K)^\vee, \|\cdot\|_{0,*})$

$\Rightarrow N(\omega_{\mathcal{O}_K/\mathbb{Z}}) = e^{-\widehat{\deg}(\omega_{\mathcal{O}_K/\mathbb{Z}}, 0)} = \delta_K^{\frac{1}{2}} \operatorname{covol}(H^0(\omega_{\mathcal{O}_K/\mathbb{Z}}), \|\cdot\|_0)$

$= \delta_K^{\frac{1}{2}} \operatorname{covol}(H^0(\mathcal{O}_K), \|\cdot\|_0)^{-1} = \delta_K^{\frac{1}{2}} \delta_K^{\frac{1}{2}} = \delta_K$

Preuve de ②

$$(H^0(D_\alpha)^\vee, \|\cdot\|_{g_\lambda^{(0)},*}) \cong (H^0(\omega_{\mathcal{O}_K/\mathbb{Z}} - D_\alpha), \|\cdot\|_{-g_\lambda^{(0)}})$$

Car $N(\omega_{\mathcal{O}_K/\mathbb{Z}}) = \delta_K$ $\rightarrow$ $= H^0(\omega_{\mathcal{O}_K/\mathbb{Z}} - D_\alpha), \|\cdot\|_{g_{-\lambda}^{(0)}})$

On en déduit

$$\xi_{(H^0(D_\alpha), \|\cdot\|_\lambda^{(0)})}\left(\frac{ds}{2}\right) = \xi_{(H^0(D_\alpha)^\vee, \|\cdot\|_{g_\lambda^{(0)},*})}\left(\frac{d(1-s)}{2}\right)$$

$$= \xi_{(H^0(\omega_{\mathcal{O}_K/\mathbb{Z}} - D_\alpha), \|\cdot\|_{g_{-\lambda}^{(0)}})}\left(\frac{d(1-s)}{2}\right)$$

En prenant l'intégrale par rapport à λ puis la somme par rapport à α, on obtient $\xi_K(s) = \xi_K(1-s)$.

⌗

M2 2020 Théorie des nombres