

Considérons l'application logarithmique

$$\Lambda: K^x \longrightarrow \mathbb{R}^{r_1+r_2}$$

$$z \longmapsto (\log |\varphi_1(z)|, \dots, \log |\varphi_{r_1+1}(z)|^2, \dots, \log |\varphi_{r_1+r_2}(z)|^2)$$

C'est un morphisme de groupes.

Lemme: $\ker(\Lambda) \cap \mathcal{O}_K$ est l'ensemble des racines de l'unité contenues dans K . C'est un groupe fini.

Preuve: Si $z \in \ker(\Lambda) \cap \mathcal{O}_K$, alors la taille de z est égale à 1 car $|\varphi_i(z)| = 1$ pour tout $i=1, \dots, r_1+r_2$, et donc pour tout $i=1, \dots, n$. Comme il n'y a qu'un nombre fini d'éléments de K de taille bornée,

$\ker(\Lambda) \cap \mathcal{O}_K$ est fini.

Si $z \in \ker(\Lambda) \cap \mathcal{O}_K$, alors $z^k \in \ker(\Lambda) \cap \mathcal{O}_K$ pour tout k , donc il existe des entiers $k, d > 0$ tels que $z^k = z^{k+d}$ et z est une racine de l'unité. Réciproquement, si z est une racine de l'unité dans K , alors z est un entier algébrique

et $|\varphi_i(z)| = 1$ pour tout i , d'où $z \in \text{Ker}(\Lambda) \cap \mathbb{Q}_n$ $\square$

Exemple: si $z \in K$ est une racine de l'unité d'ordre n , alors K est le corps cyclotique (cyclotique) $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ qui est de degré $\varphi(n)$. Les seuls valeurs de n pour lesquelles $\varphi(n) \leq 2$ sont

$$n = 1, 2, 3, 4, 6$$

En effet, si $n = \prod p_i^{k_i}$, alors

$$\varphi(n) = \prod p_i^{k_i-1} \cdot (p_i - 1)$$

et les seules valeurs possibles de p_i sont 2, 3. Pour $n = 2^a 3^b$, on trouve $\varphi(n) = 2^{a-1} \cdot 3^{b-1} \cdot 2$. Si $a, b \geq 1$, donc $n = 6$.

Par conséquent, si K est quadratique, alors les seuls racines de l'unité dans K sont ± 1 sauf si K est un des corps

$$K = \mathbb{Q}(e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt{-3}) \quad \Phi_3 = X^2 + X + 1$$

$$K = \mathbb{Q}(e^{\frac{2\pi i}{4}}) = \mathbb{Q}(i)$$

$$K = \mathbb{Q}(e^{\frac{2\pi i}{6}}) = \mathbb{Q}(\sqrt{-3}) \quad \Phi_6 = \Phi_3(-X)$$

$$\therefore |M_K| = \begin{cases} 2 & \text{si } K = \mathbb{Q}(i) \\ 4 & \text{si } K = \mathbb{Q}(\sqrt{-3}) \\ 6 & \end{cases}$$

Notons $\mathcal{O}_K^\times = \mathcal{O}_K^\times$ le groupe des unités dans l'anneau des entiers. Rappelons que

$$z \in \mathcal{O}_K^\times \iff N_K(z) = \pm 1$$

($\Rightarrow$) soit $w \in \mathcal{O}_K^\times$ tel que $zw = 1$, alors $N_K(z)N_K(w) = 1$, donc $N_K(z) \in \mathbb{Z}$ est un entier inversible

($\Leftarrow$) si $N_K(z) = \pm 1$, le polynôme minimal de z à terme constant ± 1 , donc $1/z$ est annihilé par un polynôme entier à coefficients entiers)

Comme $N_K(z) = \varphi_1(z) \dots \varphi_n(z)$, si $N_K(z) = \pm 1$,

alors

$$\begin{aligned} 0 = \log |N_K(z)| &= \log |\varphi_1(z)| + \dots + \log |\varphi_n(z)| \\ &= \log |\varphi_1(z)| + \dots + \log |\varphi_{n_1}(z)| \\ &\quad + \log |\varphi_{n_1+1}(z)|^2 + \dots + \log |\varphi_{n_1+n_2}(z)|^2 \end{aligned}$$

$\Lambda(\mathcal{O}_K^\times)$ est contenu dans l'hyperplan

$$H \subset \mathbb{R}^{n_1+n_2} \quad t_1 + \dots + t_{n_1+n_2} = 0$$

Théorème: $\Lambda(\mathcal{O}_K^\times)$ est un réseau de rang

$$n_1 + n_2 - 1.$$

Corollaire (Théorème des unités de Dirichlet)

Soit K un corps de nombres et soit μ_K le groupe des racines de l'unité dans K . Le groupe $\mathcal{U}_K$ est isomorphe à $\mu_K \times \mathbb{Z}^{r_1+r_2-1}$.

Preuve: Posons $r = r_1 + r_2 - 1$. Soient $w_1, \dots, w_r$ des éléments de $\mathcal{U}_K$ tels que $\Lambda(w_1), \dots, \Lambda(w_r)$ forment une base de $\Lambda(\mathcal{U}_K)$. Montrons que

$$\begin{aligned} \theta: \mu_K \times \mathbb{Z}^r &\longrightarrow \mathcal{U}_K \\ (z, n_1, \dots, n_r) &\longmapsto z w_1^{n_1} \dots w_r^{n_r} \end{aligned}$$

est un isomorphisme.

θ injectif: si $z w_1^{n_1} \dots w_r^{n_r} = 1$, alors en appliquant Λ

$$n_1 \Lambda(w_1) + \dots + n_r \Lambda(w_r) = 0$$

d'où $n_1 = \dots = n_r = 0$, puis $z = 1$.

θ surjectif: Soit $w \in \mathcal{U}_K$. Il existe $n_1, \dots, n_r$ tels que $\Lambda(w) = n_1 \Lambda(w_1) + \dots + n_r \Lambda(w_r)$.

Alors $w^{-1} w_1^{n_1} \dots w_r^{n_r} \in \mathcal{U}_K$ est dans $\ker \Lambda$, et c'est donc dans μ_K . □

Début de la preuve du théorème :

$\Lambda(V_K)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2}$.

En effet, démontrons que $\Lambda(V_K) \cap B(0, R)$ est fini pour tout $R > 0$. Pour cela, il suffit de voir que l'ensemble des

$$(x_1, \dots, x_{r_1+1}) \in \Lambda(V_K) \text{ avec } |x_j| \leq c$$

est fini, et à savoir que

$$\left| \log |\varphi_j(w)| \right| \leq c$$

n'a qu'un nombre fini de solutions $w \in V_K$.

Un tel w satisfait $|\varphi_j(w)| \leq e^c$ et

avec c est un entier algébrique, sa taille

est bornée par e^c . Il n'y a qu'un

nombre fini de tels $w \in K$! □

Il reste à démontrer que $\Lambda(V_K)$ contient r_1+r_2-1 éléments linéairement indépendants, c'est-à-dire obtenir r_1+r_2-1 unités multiplicativement indépendantes.

Ingrédient clé

Théorème (Mintowski) Soient G un réseau de rang n de $\mathbb{R}^n$, $\|\cdot\|$ une norme sur $\mathbb{R}^n$ et B sa boule unité. Il existe un vecteur non nul $u \in G$ tel que

$$\|u\| \leq 2 \left(\frac{V(G)}{\text{vol}(B)} \right)^{1/n}$$

où $V(G) = |\det(u_1, \dots, u_n)|$ pour une base $\nearrow u_1, \dots, u_n$ de G .

« conclusion »
du réseau

On démontrera ce théorème la prochaine fois.

Proposition: Pour tout $j=1, \dots, r_1+r_2$, il existe $w_j \in \mathbb{V}_K$ tel que

$$\log |\varphi_k(w_j)| < 0 \quad \text{si } k \neq j.$$

(Comme $|N_k(w_j)| = 1$, on obtient alors $\log |\varphi_j(w_j)| > 0$.)

Démonstration: Soit $C = (c_1, \dots, c_{r_1+r_2})$ une famille de réels > 0 . On considère la norme $\|\cdot\|_C$ sur $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ définie par

$$\|(x_1, \dots, x_{r_1}, z_{1,1}, \dots, z_{r_1+r_2})\| =$$

$$= \max \left(\frac{|x_1|}{c_1}, \dots, \frac{|x_{r_1}|}{c_{r_1}}, \frac{|z_{r_1+1}|}{\sqrt{c_{r_1+1}}}, \dots, \frac{|z_{r_1+r_2}|}{\sqrt{c_{r_1+r_2}}} \right)$$

le volume de la boule unité pour cette norme est :

$$\begin{aligned} \text{vol}(B_c) &= 2c_1 \dots 2c_{r_1} (\pi c_{r_1+1}) \dots (\pi c_{r_1+r_2}) \\ &= 2^{r_1} \pi^{r_2} (c_1 \dots c_{r_1+r_2}) \end{aligned}$$

car B_c est l'ensemble des $|x_k| \leq c_k$ et $|z_{r_1+k}| \leq \sqrt{c_{r_1+k}}$.

Soit P un domaine fondamental du réseau $\Phi(\mathcal{O}_K)$ de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Choisissons

$$c_k = t > 0 \quad \text{pour tout } k \neq j$$

$$c_j = \frac{2^n \text{vol}(P)}{2^{r_1} \pi^{r_2} t^{r_1+r_2-1}}$$

Alors $\text{vol}(B_c) = 2^n \text{vol}(P) = 2^n V(\Phi(\mathcal{O}_K))$
 et la théorie de Minkowski donne l'existence
 de d'un entier algébrique non nul $a_t \in \mathcal{O}_K$
 tel que $\Phi(a_t) \in B_c$. De plus,

$$|N_K(a_t)| = |\varphi_1(a_t)| \dots |\varphi_{r_1}(a_t)| |\varphi_{r_1+1}(a_t)|^2 \dots |\varphi_{r_1+r_2}(a_t)|^2$$

$$\leq c_1 \dots c_{r_1+r_2} = \frac{\text{vol}(B_c)}{2^{r_1} \pi^{r_2}}$$

$$\leq \frac{2^{n-r_1}}{\pi^{r_2}} \text{vol}(P)$$

large $t \rightarrow 0$, $|\varphi_k(a_t)| \leq t$ tend vers 0
si $k \neq j$

et $|\varphi_j(a_t)|$ tend vers l'infini. on a donc
une suite infinie d'entiers algébres

distincts de même bornée par un même
nombre réel. Il y a donc une suite infinie
d'éléments de $\mathcal{O}_K$ de même norme $N \in \mathbb{Z}$.

le groupe additif $\mathcal{O}_K / N\mathcal{O}_K \cong (\mathbb{Z}/N\mathbb{Z})^n$

est fini. Quelle qu'en soit une sous-
suite, il existe $(a_m)_m$ suite dans $\mathcal{O}_K$
de même norme N et deux à deux congrus
modulo N .

lemme: Soient $a, b \in \mathcal{O}_K$ tels que
 $N_K(a) = N_K(b) = N$ et $a - b \in N\mathcal{O}_K$.

Alors $\frac{a}{b}$ est une unité de K .

preuve: Posons $w = \frac{a}{b}$ et $a = b + Nc$
avec $c \in \mathcal{O}_K$. Comme $N = N_K(b)$, il existe
 $b' \in \mathcal{O}_K$ tel que $N = b b'$. Alors

$$a = b + b b' c = b(1 + b' c)$$

$$w = \frac{a}{b} = \frac{b + b b' c}{b} = 1 + b' c$$

$\Rightarrow w$ est un entier algébrique

De même, $\frac{b}{a}$ est un entier algébrique, et donc u est une unité de K

□

Pour tout $m \geq 0$, posons $v_m = \frac{a_{x_m}}{a_{x_1}}$.

D'après le lemme, c'est une unité de K . Ces unités sont deux à deux distinctes. Pour

$$k \neq j, \quad |\varphi_k(w_m)| = \frac{|\varphi_k(a_{x_m})|}{|\varphi_k(a_{x_1})|} \xrightarrow{m \rightarrow \infty} 0. \text{ Il}$$

existe en particulier $w_j \in \mathcal{O}_K$ tel que

$$|\varphi_k(w_j)| < 1, \text{ donc } \log |\varphi_k(w_j)| < 0$$

□

∴ on a construit des unités

$$w_1, \dots, w_{r_1+r_2-1}$$

et il faut montrer que

$$\Lambda(w_1), \dots, \Lambda(w_{r_1+r_2-1})$$

sont linéairement indépendants dans $\mathbb{R}^{r_1+r_2}$.

lemme: Soit $M \in M_n(\mathbb{R})$. Supposons que $m_{ij} < 0$ si $i \neq j$ et $\sum_{i=1}^n m_{ij} > 0$.

Alors M est inversible.

Preuve: Soient $x_1, \dots, x_n \in \mathbb{R}$ tels que

$$\sum_{i=1}^n x_i m_{ij} = 0 \quad \text{pour } j=1, \dots, n$$

(relation de dépendance linéaire entre les lignes)

Soit j tel que $x_j = \max(x_1, \dots, x_n)$. Alors

$$\begin{aligned} 0 &= \sum_{i=1}^n x_i m_{ij} = \sum_{i=1}^n (x_i - x_j) m_{ij} + x_j \sum_{i=1}^n m_{ij} \\ &\geq x_j \sum_{i=1}^n m_{ij} \end{aligned}$$

on a $(x_i - x_j) m_{ij} \geq 0$ si $i \neq j$ et $= 0$ pour $i = j$. Comme $\sum_{i=1}^n m_{ij} > 0$, on trouve $x_j \leq 0$,

c'est-à-dire $x_i \leq 0$ pour tout i .

le même argument appliqué à $-x_i$ montre que $x_i \geq 0$, donc $x_1 = \dots = x_n = 0$ et la matrice est inversible. $\square$

On applique ce lemme à la matrice

$$M = (m_{ij})_{1 \leq i, j \leq r_1 + r_2 - 1}$$

$$\text{où } m_{ij} = \begin{cases} \log |\varphi_i(w_j)| & 1 \leq j \leq r_1 \\ 2 \log |\varphi_i(w_j)| & r_1 + 1 \leq j \leq r_1 + r_2 - 1 \end{cases}$$

Par construction, $m_{ij} < 0$ pour tout $i \neq j$.

En outre,

$$m_{1j} + \dots + m_{r_1+r_2-1,j} = -m_{r_1+r_2,j} > 0$$

donc la matrice M est inversible

□

