Plongement canonique

k $\big|$ $n = r_1 + 2r_2$. $\mathbb{Q}$

$k \overset{\sigma_i}{\hookrightarrow} \mathbb{R}$ $\quad 1 \le i \le r_1$

$k \hookrightarrow \mathbb{C}$ $\quad r_1 < i \le r_1 + r_2$

$\overline{\sigma_{r_1+i}} = \sigma_{r_1+r_2+i}$ $\quad 1 \le i \le r_2$.

$\underline{\Sigma} : k \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

$\uparrow$ $\mathbb{R}$-e.v. dimension n.

$\mathbb{Z}_k$ anneau des entiers de k

$\underline{\Sigma}(\mathbb{Z}_k)$ réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$.

Volume? $\quad$ $\mathbb{Z}_k$ est un sous-$\mathbb{Z}$-module libre de rang n de k.

Lemme. M un sous-$\mathbb{Z}$-module de k de rang $n = [k:\mathbb{Q}]$; $(x_1, \dots, x_n)$ une base de M sur $\mathbb{Z}$. Alors $\underline{\Sigma}(M)$ est un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ de volume

$$2^{-r_2} \cdot \left|\det(\sigma_i x_j)\right|_{1 \le i,j \le n} = v(\underline{\Sigma}(M)).$$

Dém. $\underline{\Sigma} : k \to \mathbb{R}^n$ $\quad$ $\underline{\Sigma}(M)$ est un sous-gpe de $\mathbb{R}^n$ de rang n.. Il existe $d > 0$, $d \in \mathbb{Z}$, $d x_i \in \mathbb{Z}_k$, $1 \le i \le n$. Alors $dM \subset \mathbb{Z}_k$.
$d\,\underline{\Sigma}(M) \subset \underline{\Sigma}(\mathbb{Z}_k)$ discret.

$$\mathrm{Vol}(\underline{\Sigma}(M)) = \left|\det\big(\sigma_1(x_j), \sigma_2(x_j), \dots, \sigma_{r_1}(x_j), \mathrm{Re}\,\sigma_{r_1+1}(x_j), \mathrm{Im}\,\sigma_{r_1+1}(x_j), \dots, \mathrm{Re}\,\sigma_{r_1+r_2}(x_j), \mathrm{Im}\,\sigma_{r_1+r_2}(x_j)\big)\right|$$

$1 \le j \le n$

??

$$= 2^{-r_2} \left|\det(\sigma_i x_j)_{1 \le i,j \le n}\right|$$

$$\begin{vmatrix} X_1 & Y_1 \\ X_2 & Y_2 \end{vmatrix} = X_1Y_2 - X_2Y_1 \qquad \begin{vmatrix} X_1 + iY_1 & X_1 - iY_1 \\ X_2 + iY_2 & X_2 - iY_2 \end{vmatrix} = 2(iY_1X_2 - iX_1Y_2)$$

$$\underbrace{C_{r_1+j} \quad C_{r_1+j+1}}_{\downarrow}$$

$$C_{r_1+j} + iC_{r_1+j+1} \qquad C_{r_1+j} - iC_{r_1+j+1}$$

Application. $M = \mathbb{Z}_k$

$$v(\underline{\Sigma}(\mathbb{Z}_k)) = 2^{-r_2} \cdot |D_k|^{1/2}.$$

Fin de la démonstration du théorème de Dirichlet. Soit k un corps de nombres

Lemme Soit $r > \left(\frac{2}{\pi}\right)^{r_2} \cdot |D_k|^{1/2}$.

Soient $\lambda_1, \dots, \lambda_n > 0$, $\lambda_1 \cdots \lambda_n = r$, $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$ $\quad 1 \le j \le r_2$. Alors $\exists \alpha \in \mathbb{Z}_k$, $\alpha \neq 0$, $|\sigma_j(\alpha)| \le \lambda_j$ $\quad 1 \le j \le n$.

Dém. $0 \neq \underline{\Sigma}(\alpha) \in \underline{\Sigma}(\mathbb{Z}_k)$ réseau.

Compact de $\mathbb{R}^n$ $\quad \{(x_1, \dots, x_n) ;\ |x_i| \le \lambda_i,\ 1 \le i \le n\} = K$.

$K \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

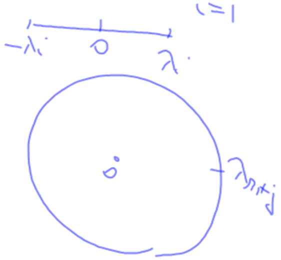
$\cup$

$(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$

$|x_i| \leq \lambda_i \qquad 1 \leq i \leq r_1$

$|z_j| \leq \lambda_{r_1+j} \qquad 1 \leq j \leq r_2$

$$\prod_{i=1}^{r_1} (2\lambda_i) \cdot \prod_{j=1}^{r_2} \pi \lambda_{r_1+j}^2 = 2^{r_1} \pi^{r_2} \lambda_1 \cdots \lambda_n .$$



Plongement logarithmique.

$n_1 = \cdots = n_{r_1} = 1$

$n_{r_1+1} = \cdots = n_{r_1+r_2} = 2$

k

$| n = r_1 + 2r_2$

$\mathbb{Q}$

$$\underline{\lambda} : k^\times \longrightarrow \mathbb{R}^{r_1+r_2}$$
$$\alpha \longmapsto \left(n_i \log|\sigma_i(\alpha)|\right)_{1 \leq i \leq r_1+r_2}$$

$\underline{\lambda}(\mathbb{Z}_k^\times) \subset$ hyperplan H de $\mathbb{R}^{r_1+r_2}$ d'équation $x_1 + \cdots + x_{r_1+r_2} = 0$

unités de k

$$|N_{k/\mathbb{Q}} \alpha| = \prod_{i=1}^{r_1+r_2} |\sigma_i(\alpha)|^{n_i}$$

$\lambda(\mathbb{Z}_k)$ est discret dans $\mathbb{R}^{r_1+r_2}$

réseau ?

$\lambda_i \qquad \lambda_1 \cdots \lambda_n = \kappa > \cdots \qquad \lambda_{r_1+j} = \lambda_{r_1+r_2+j}$

$|\sigma_i(\alpha)| < \lambda_i . \qquad \log|\sigma_i(\alpha)|$

il faudra aussi minorer $|\sigma_i(\alpha)|$ pour majorer $\big|\log|\sigma_i(\alpha)|\big|$.

$\lambda_1 \cdots \lambda_{r_1} \cdot (\lambda_{r_1+1} \cdots \lambda_{r_1+r_2})^2 = \kappa$.

Fin de la démonstration du théorème de Dirichlet.

Soit $\underline{t} = (t_1, \ldots, t_{r_1+r_2}) \in H \subset \mathbb{R}^{r_1+r_2}$.

$t_1 + \cdots + t_{r_1+r_2} = 0$.

$\kappa > \left(\frac{2}{\pi}\right)^{r_2} |D_k|^{1/2}$.

$$\begin{cases} \lambda_j = \kappa^{1/n} e^{t_j/n_j} . & 1 \leq j \leq r_1 + r_2 . \\ \lambda_{r_1+r_2+j} = \lambda_{r_1+j} & 1 \leq j \leq r_2 . \end{cases}$$

$\lambda_1 \cdots \lambda_n = \kappa \qquad t_1 + \cdots + t_{r_1+r_2} = 0$

$$e^{\frac{t_1}{n_1} + \cdots + \frac{t_{r_1+r_2}}{n_{r_1+r_2}} + \frac{t_{r_1+1}}{n_{r_1+1}} + \cdots + \frac{t_{r_1+r_2}}{n_{r_1+r_2}}} .$$
$$= e^{t_1 + \cdots + t_{r_1} + \frac{1}{2}(t_{r_1+1} + \cdots + t_{r_1+r_2}) \times 2} = e^0 = 1 .$$

$\exists\, \alpha \in \mathbb{Z}_k, \alpha \neq 0, \quad |\sigma_j(\alpha)| \leq \lambda_j . \quad 1 \leq j \leq n .$

$\log|\sigma_j(\alpha)| \leq \frac{t_j}{n_j} + \frac{1}{n} \log \kappa . \qquad |N_{k/\mathbb{Q}} \alpha| \leq \kappa .$

$1\le j\le r_1+r_2$ $\quad\alpha\in\mathbb{Z}_k, \alpha\ne 0 \Rightarrow |N_{k/\mathbb{Q}}(\alpha)|\ge 1$

$$|\sigma_j(\alpha)| = |N_{k/\mathbb{Q}}(\alpha)|\cdot\prod_{i\ne j}|\sigma_i(\alpha)|^{-1}.$$

$$\ge \prod_{i\ne j}|\sigma_i(\alpha)|^{-1} \ge \kappa^{-\frac{n-1}{n}}e^{t_j/n_j}$$

$$\frac{t_1}{n_1}+\dots+\frac{t_{r_1+r_2}}{n_{r_1+r_2}}=0$$

$$\log|\sigma_j(\alpha)| \ge \frac{t_j}{n_j}-\frac{n-1}{n}\log\kappa.$$

$$-\frac{n-1}{n}\log\kappa \le \log|\sigma_j(\alpha)|-\frac{t_j}{n_j}\le\frac{1}{n}\log\kappa$$

$\forall\, \underline{t}\in H\ \exists\ \alpha\in\mathbb{Z}_k, \alpha\ne 0.$ $\quad|N_{k/\mathbb{Q}}(\alpha)|\le\kappa.$

$$\big|t_j-n_j\log|\sigma_j(\alpha)|\big|\le\frac{2}{n}\log\kappa.$$

Il existe un ensemble fini Γ de $\mathbb{Z}_k$ tel que tout élément $\alpha\in\mathbb{Z}_k$ vérifiant $|N_{k/\mathbb{Q}}(\alpha)|\le\kappa$ s'écrit $\varepsilon\gamma$, $\gamma\in\Gamma$, $\varepsilon\in\mathbb{Z}_k^\times$

$\forall t\in H, \exists\ \gamma\in\Gamma, \exists\ \varepsilon\in\mathbb{Z}_k^\times$

$$|t-\underline{\lambda}(\gamma)-\underline{\lambda}(\varepsilon)|\le\kappa'$$

$\underline{\lambda}(\mathbb{Z}_k^\times)$ s/g discret de $\mathbb{R}^{r_1+r_2}$, contenu dans H,

$$|t-\underline{\lambda}(\varepsilon)|\le\kappa'+\max_{\gamma\in\Gamma}|\underline{\lambda}(\gamma)|$$

$[k:\mathbb{Q}]=n=r_1+2r_2$

Il existe r unités indépendantes $r=r_1+r_2-1$ qui engendre un sous-groupe d'indice fini de $\mathbb{Z}_k^\times$

$\varepsilon_1,\dots,\varepsilon_r$ système fondamental d'unités de k

$$\mathbb{Z}_k^\times=\{\zeta\,\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}\ ;\ \zeta\in k^\times_{tors}\ ;\ a_i\in\mathbb{Z}\}_{1\le i\le r}$$

$$\left|\det\left(n_i\log|\sigma_i(\varepsilon_j)|\right)_{\substack{1\le i\le r_1+r_2=r+1,\ i\ne i_0\\ 1\le j\le r}}\right|=R_k$$

régulateur de k

Volume de $\lambda(\mathbb{Z}_k^\times)$.

Si $\eta_1,\dots,\eta_r$ sont r unités de k on définit

$$R(\eta_1,\dots,\eta_r)=\left|\det\left(\log|\sigma_i\eta_j|\right)_{\substack{1\le i\le r_1+r_2+1,\ i\ne i_0\\ 1\le j\le r}}\right|$$

$\eta_1,\dots,\eta_r$ sont linéairement indépendantes sur $\mathbb{Z}$ $\quad(\eta_1^{e_1}\cdots\eta_r^{e_r}=1\iff e_1=\dots=e_r=0)$

$\iff R(\eta_1,\dots,\eta_r)\ne 0$

De plus, $\eta_1,\dots,\eta_r$ est un système fondamental d'unités de k $\iff R(\eta_1,\dots,\eta_r)=R_k$.

Idéaux d'un corps de nombres.

$[k:\mathbb{Q}]=n$

$\mathbb{Z}_k \supset \mathfrak{a}$ $\mathfrak{a}$ idéal de $\mathbb{Z}_k$ (sous-$\mathbb{Z}_k$-module).

$\underline{\sigma}(\mathbb{Z}_k)$ est un réseau de $\mathbb{R}^n=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$.

$\cup$

$\underline{\sigma}(\mathfrak{a})$ Si $\mathfrak{a}\neq 0$ $\exists\,\alpha\in\mathfrak{a},\ \alpha\neq 0$

$\alpha\mathbb{Z}_k\subset\mathfrak{a}\subset\mathbb{Z}_k$.

$\mathbb{Z}_k$ est un $\mathbb{Z}$-module libre de rang n

$\alpha\mathbb{Z}_k$ aussi   donc $\mathfrak{a}$ aussi.

$\mathbb{Z}_k/\mathfrak{a}$ est fini. $\sigma(\mathfrak{a})$ est un réseau de $\mathbb{R}^n$.

__Déf__ $N(\mathfrak{a})=|\mathbb{Z}_k/\mathfrak{a}|$.

__Lemme__. Si $\mathfrak{a}=\alpha\mathbb{Z}_k$, $\alpha\neq 0$, alors $N(\alpha\mathbb{Z}_k)=|N_{k/\mathbb{Q}}(\alpha)|$.

$\alpha\mathbb{Z}_k\subset\mathfrak{a}\subset\mathbb{Z}_k$.

$\mathbb{Z}_k=\mathbb{Z}e_1+\dots+\mathbb{Z}e_n$.

$\exists\, a_1,\dots,a_n\in\mathbb{Z}_{>0}$, $a_1|a_2|\dots|a_n$ $(a_1e_1,\dots,a_ne_n)$ base de $\alpha\mathbb{Z}_k$.

$\mathbb{Z}_k/\alpha\mathbb{Z}_k\simeq\mathbb{Z}/a_1\mathbb{Z}\times\dots\times\mathbb{Z}/a_n\mathbb{Z}$. $\underbrace{a_1\cdots a_n}_{:=N(\mathbb{Z}_k\alpha)}$ cl's

$[\alpha]:\mathbb{Z}_k\longrightarrow\mathbb{Z}_k$ $N_{k/\mathbb{Q}}(\alpha)=$ norme de $[\alpha]$.

$\gamma\longmapsto\alpha\gamma$

image $\alpha\mathbb{Z}_k=\mathbb{Z}a_1e_1+\dots+\mathbb{Z}a_ne_n$.

$\mathbb{Z}_k=\mathbb{Z}e_1+\dots+\mathbb{Z}e_n \xrightarrow[e_i\mapsto a_ie_i]{} \alpha\mathbb{Z}_k$.

$[\alpha]\downarrow$

$\alpha\mathbb{Z}_k$

u endomorphisme de $\mathbb{Z}_k$ sur $\mathbb{Z}$ $e_i\mapsto a_ie_i$

$\dfrac{[\alpha]}{\mathbb{Z}_k}$. $\gamma\mapsto\alpha\gamma$.

injectifs. $\Rightarrow\exists\, v$ automorphisme du $\mathbb{Z}$-module $\alpha\mathbb{Z}_k$

$v(a_ie_i)=\alpha e_i$.

$\det v=\pm 1$ $\Rightarrow|\det u|=|N_{k/\mathbb{Q}}(\alpha)|$.

__Exemple__.

$k=\mathbb{Q}(i)$ $\alpha=1+i$ $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i)=2$

$\mathbb{Z}_k=\mathbb{Z}+\mathbb{Z}i=\mathbb{Z}e_1+\mathbb{Z}e_2$.

$\cup$

$\mathbb{Z}_k\alpha=\{a+bi;\ a,b \text{ même parité}\}$

$=\mathbb{Z}e_1+\mathbb{Z}(2e_2)$

$e_1=1+i$ $a_1=1$

$e_2=1$. $a_2=2$ $N(\alpha\mathbb{Z}_k)=2$.

$\mathfrak{a}$ idéal non nul de k.

Volume de $\sigma(\mathfrak{a})$ réseau de $\mathbb{R}^n$

$$= 2^{-r_2} |D_k|^{1/2} \ N(\mathfrak{a}).$$

Théorème. Soit K un corps de nombres

Soit $\mathfrak{a}$ un idéal non nul de K.

Il existe $\alpha \in \mathfrak{a}$, $\alpha \neq 0$,

$$|N_{K/\mathbb{Q}}(\alpha)| \leqslant M(r_1, r_2) \cdot |D_k|^{1/2} \cdot N(\mathfrak{a})^{1/2}.$$

avec

$$M(r_1, r_2) = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}.$$

$\mathbb{Z}_k \supset \mathfrak{b} \supset \mathfrak{a}$. idéaux $\neq 0$

$$\begin{tikzcd} \mathbb{Z}_k \arrow[r, "s_\mathfrak{b}"] \arrow[d, "s_\mathfrak{a}"'] & \mathbb{Z}_k/\mathfrak{b} \\ \mathbb{Z}_k/\mathfrak{a} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

il existe un unique homomorphisme surjectif φ

$\varphi \circ s_\mathfrak{a} = s_\mathfrak{b}$.

donc $N(\mathfrak{b})$ divise $N(\mathfrak{a})$.

Suite : idéaux premiers

$k = \mathbb{Q}(\sqrt{-5})$ $\quad \mathbb{Z}_k = \mathbb{Z}[i\sqrt{5}] \ni 21 = 3.7$

$= (1+2i\sqrt{5})(1-2i\sqrt{5})$

$-5 \equiv 3 \bmod 4$.