Suite de la démonstration du théorème des unités de Dirichlet.

Géométrie des nombres (Minkowski)

V $\mathbb{R}$-e.v. dimension finie.

réseau Λ de V = (lattice)

= sous-groupe discret de V de rang n sur $\mathbb{Z}$.

$\underline{e}=(e_1,\dots,e_n)$ base de V sur $\mathbb{R}$

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

Soit Λ un réseau de $\mathbb{R}^n$.

$\Lambda=\mathbb{Z}e_1+\dots+\mathbb{Z}e_n$ $\qquad e_i\in\mathbb{R}^n$

$\underline{\underline{e}}=(e_1,\dots,e_n)$

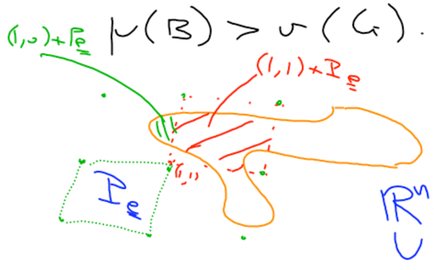
$$P_{\underline{\underline{e}}}=\{x_1e_1+\dots+x_ne_n \;;\; 0\le x_i<1,\ 1\le i\le n\}$$

$\mathbb{R}^n/\Lambda \xrightarrow[\text{bijection}]{} P_{\underline{\underline{e}}}$ $\qquad t_i=[t_i]+x_i$, $x_i=\{t_i\}\in[0,1)$.

$\mu(P_{\underline{\underline{e}}})=v(\Lambda)$ volume du réseau.

Théorème de Minkowski.

G réseau de $\mathbb{R}^n$, $B\subset\mathbb{R}^n$ mesurable $\mu(B)>v(G)$. Alors il existe $x\neq y$ dans B tels que $x-y\in G$.



Démonstration.

$$\mathbb{R}^n=\bigsqcup_{g\in G}(g+P_{\underline{e}})$$
$$\cup$$
$$B=\bigsqcup_{g\in G}(g+P_{\underline{e}})\cap B$$

$$\mu(B)=\sum_{g\in G}\mu((g+P_{\underline{e}})\cap B)$$

$$\mu(P_e\cap(-g+B))=\mu((g+P_{\underline{e}})\cap B)$$ $\qquad \mu(P_e)=v(G)$

$$P_e\cap(-g+B)\subset P_e$$

$$\sum_g \mu(P_e\cap(-g+B))>\mu(P_e)=v(G)$$

Donc les $P_e\cap(-g+B)$, $g\in G$ ne sont pas deux-à-deux disjoints.

$\exists\ g\neq g'$, $\exists\ x,y\in B$,

$g+x=g'+y$ $\qquad x-y=\underbrace{g'-g}_{\neq 0}\in G$

Corollaire. G réseau de $\mathbb{R}^n$,

$B \subset \mathbb{R}^n$ mesurable, symétrique

$(x \in B \Rightarrow -x \in B)$, convexe

$(x, y \in B \Rightarrow \frac{x+y}{2} \in B)$

On suppose $\mu(B) > 2^n v(G)$.

Alors $G \cap B \neq \{0\}$.

$B' = \frac{1}{2} B$

$\mu(B') > v(G)$

$\mu(B') = \frac{1}{2^n}\mu(B)$

$\exists \quad x \neq y$ dans B', $\quad x - y \in G$

$B' = \frac{1}{2} B$

$2x \in B$

$2y \in B \Longrightarrow -2y \in B$ (B symétrique)

$\Bigg\} \Longrightarrow x - y \in B$ (B convexe).

$B \cap G \ni x - y \neq 0$.

Rappel : plongement canonique d'un corps de nombres.

k

$n = r_1 + 2r_2$

$\mathbb{Q}$

$\sigma_1, \dots, \sigma_{r_1} : k \to \mathbb{R}$

$\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2} : k \to \mathbb{C}$

$\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j} \quad , 1 \leq j \leq r_2$.

$k \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = V \quad$ $\mathbb{R}$-e-v. dimension n

$\alpha \longmapsto (\sigma_1(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)) \quad$ σ : homom. de groupes additifs.

Théorème $\sigma(\mathbb{Z}_k)$ est un réseau de V.

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

Reste à montrer que $\sigma(\mathbb{Z}_k)$ est discrète dans $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

$M > 0$, $K = \{ z = (z_1, \dots, z_{r_1+r_2}) \mid |z_i| \leq M \quad 1 \leq i \leq r_1 + r_2 \}$.

$\sigma(\mathbb{Z}_k) \cap K$ finie ?

$E = \{ \alpha \in k \quad |\sigma_i(\alpha)| \leq M \quad \forall i = 1, \dots, r_1 + r_2 \}$ fini ?

$\sigma_{r_1+r_2+j}(\alpha) = \overline{\sigma_{r_1+j}(\alpha)} \quad 1 \leq j \leq r_2$.

$\alpha \in E$

$\Rightarrow |\sigma_i(\alpha)| \leq M \quad \forall i = 1, \dots, n = r_1 + 2r_2$.

α racine d'un polynôme unitaire $\in \mathbb{Z}[X]$

degré $\le n$, toutes les racines ont des modules $\le M$.

$$\prod_{i=1}^{d} (X-\alpha_i) = P(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$$

$\alpha_1, \dots, \alpha_d$ conjugués de α. $|\alpha_i| \le M$.

Lemme

$$1+|a_{d-1}|+\dots+|a_0| \le \prod_{i=1}^{d} (1+|\alpha_i|).$$

$\Rightarrow \{\alpha \,;\, |\alpha_i| \le M\}$ est fini.

Pour $\mathbb{Z}_k$ (entiers) on a utilisé le plongement canonique dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$

Pour $\mathbb{Z}_k^\times$ (unités) on introduit le plongement logarithmique.

$$\begin{array}{ccc} k^\times & \xrightarrow{\ \ \lambda\ \ } & \mathbb{R}^{r_1+r_2} \\ \cup & & \in \\ \mathbb{Z}_k^\times \ni \alpha & \longmapsto & \left(n_i \log|\sigma_i(\alpha)|\right)_{1\le i\le r_1+r_2} \end{array}$$

homomorphisme de groupes. (non injectif)

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

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

Rappel. $\alpha \in \mathbb{Z}_k$.

$\alpha \in \mathbb{Z}_k^\times \iff N_{k/\mathbb{Q}}(\alpha) = \pm 1$.

$$\lambda(\alpha) = \big(\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \dots, 2\log|\sigma_{r_1+r_2}(\alpha)|\big)$$

$$= (t_1, \dots, t_{r_1+r_2})$$

$t_1 + \dots + t_{r_1+r_2} = \log|N_{k/\mathbb{Q}}(\alpha)|$.

H hyperplan de $\mathbb{R}^{r_1+r_2}$ d'équation $t_1 + \dots + t_{r_1+r_2} = 0$.

$\{\alpha \in k^\times \,;\, \lambda(\alpha) \in H\} = \{\alpha \in k^\times, N_{k/\mathbb{Q}}(\alpha) = \pm 1\}$

Pour $\alpha \in \mathbb{Z}_k$ on a $\lambda(\alpha) \in H \iff \alpha \in \mathbb{Z}_k^\times$.

Forme précisée du théorème de Dirichlet

$\lambda(\mathbb{Z}_k^\times)$ est un réseau de H.

H hyperplan de $\mathbb{R}^{r_1+r_2}$

$\dim H = r_1 + r_2 - 1$.

Noyau de λ $\quad \alpha \in k^\times \quad \lambda(\alpha) = 0$

$\iff |\sigma_i(\alpha)| = 1$. $\forall i = 1, \dots, n$.

Résultat $\quad \ker\lambda \cap \mathbb{Z}_k = k^\times_{tors}$.

$\lambda : k^\times \longrightarrow \mathbb{R}^{r_1+r_2}$.

$\zeta \in k^\times_{tors}$ $\exists m, \zeta^m = 1$

$\zeta \in \mathbb{Z}_k$.

$\forall \sigma : k \to \mathbb{C}$, $\sigma(\zeta^m) = \sigma(\zeta)^m = 1$

$|\sigma(\zeta)| = 1$.

Donc $\zeta \in \ker \lambda$.

Réciproque.

$\alpha \in \mathbb{Z}_k \cap \ker \lambda$ $|\sigma_i(\alpha)| = 1 \quad \forall i$

$\lambda(\alpha^m) = m\lambda(\alpha) = 0$ $|\sigma_i(\alpha^m)| = 1$

$\forall m \geq 0$. $\{\alpha^m, m \geq 0\}$ fini ($M = 1$ dans la dém. préc.)

$\exists \ell \geq 1, \alpha^\ell = 1$.

Kronecker : Si un entier algébrique α a tous ses conjugués de module ≤ 1, alors $\alpha = 0$ ou α est une racine de l'unité.

$\lim_{n \to \infty} \varphi(n) = +\infty$ (φ Euler).

k corps de nombres $\Rightarrow$ $k^\times_{tors}$ est un s/groupe fini de $k^\times$ (et même de $\mathbb{Z}_k^\times$)

$\lambda(\mathbb{Z}_k^\times)$ réseau de H

$\Rightarrow \mathbb{Z}_k^\times$ est un groupe de type fini et de rang $r = r_1 + r_2 - 1$

Dém. $k^\times_{tors}$ est le sous-groupe de torsion de $\mathbb{Z}_k^\times$

$$\mathbb{Z}_k^\times \longrightarrow \lambda(\mathbb{Z}_k^\times) \subset H$$

$$\lambda(\mathbb{Z}_k^\times) \cong \mathbb{Z}^r$$

$\lambda(\mathbb{Z}_k^\times)$ réseau de H

$\Rightarrow \lambda(\mathbb{Z}_k^\times)$ est un groupe abélien libre de rang $r = r_1 + r_2 - 1$.

$\mathbb{Z}_k^\times \simeq k^\times_{tors} \times \mathbb{Z}^r$.

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

$M > 0$ $\{\alpha \in \mathbb{Z}_k^\times$

$-M \leq \log|\sigma_i(\alpha)| \leq M$.

$1 \leq i \leq r_1 + r_2\}$.

fini ?

$|\sigma_i(\alpha)| \leq e^M$ $1 \leq i \leq n$.

$\alpha \in \mathbb{Z}_k$

Reste à vérifier que $\lambda(\mathbb{Z}_k^\times)$ engendre H (sur $\mathbb{R}$)

$z \in \mathbb{H}$. on veut approcher z
par un élément de $\lambda(\mathbb{Z}_k^\times)$.

Rappel. V un $\mathbb{R}$-e-v.
G sous-groupe discret de V

G est un réseau de V $\iff$
$\exists\, B$ borné dans V,

$$V = \bigcup_{g \in G} (B+g).$$

1ère étape : approcher z par $\lambda(\alpha)$, $\alpha \in \mathbb{Z}_k$.
2e étape : passage à $\mathbb{Z}_k^\times$.

$\alpha, \beta \in \mathbb{Z}_k$. $\alpha, \beta \neq 0$.

$\alpha \mathbb{Z}_k$ idéal principal engendré par α

$\alpha \mathbb{Z}_k = \beta \mathbb{Z}_k \iff \alpha = \beta u \quad u \in \mathbb{Z}_k^\times$

Lemme $\kappa > 0$. Il existe un sous-ensemble fini Γ de $\mathbb{Z}_k$ tel que tout $\alpha \in \mathbb{Z}_k$ vérifiant $|N_{k/\mathbb{Q}}(\alpha)| \leq \kappa$ soit de la forme $u\gamma$, $u \in \mathbb{Z}_k^\times$, $\gamma \in \Gamma$.

$x^2 - dy^2 = \pm 1$

Démonstration. $\alpha \in \mathbb{Z}_k$ $\quad N_{k/\mathbb{Q}}(\alpha) = m \in \mathbb{Z}$

$\alpha_1, \dots, \alpha_d$ conjugués dans $\mathbb{C}$

$m = \alpha_1 \cdots \alpha_d$. $\quad \alpha_i$ entiers algébriques

$m = \alpha \beta$ $\quad \beta$ entier algébrique
$\beta \in k$ $\quad \beta \in \mathbb{Z}_k$.

$m \in \alpha \mathbb{Z}_k$.
$m\mathbb{Z}_k \subset \alpha \mathbb{Z}_k$. $\quad \mathbb{Z}_k / m\mathbb{Z}_k$ fini

A/J bijection : id^x de A/J et id^x de A contenant J.

Il n'y a qu'un nombre fini d'idéaux de $\mathbb{Z}_k$ contenant m.

m donné $\in \mathbb{Z}$
L'ensemble des idéaux $\alpha \mathbb{Z}_k$ ayant un générateur α de norme m
$N_{k/\mathbb{Q}}(\alpha) = m$ est fini.

$-\kappa \leq m \leq \kappa$.

$\{\alpha \mathbb{Z}_k ; |N_{k/\mathbb{Q}}(\alpha)| \leq \kappa\}$ fini

pour chacun d'eux on choisit un générateur γ. Γ l'ensemble de ces γ

$|N_{k/\mathbb{Q}}(\alpha)| \leq \kappa \quad \exists \gamma \in \Gamma, \ \alpha \mathbb{Z}_k = \gamma \mathbb{Z}_k$.

$z \in H$? $\alpha \in \mathbb{Z}_k$ $|\lambda(\alpha) - z| \leq C$.

<u>Lemme</u>. (appl. de Minkowski).

Il existe $\kappa > 0$ telle que si

$\lambda_1, \dots, \lambda_n$ réels > 0,

$\lambda_1 \cdots \lambda_n = \kappa$ et $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$

$1 \leq j \leq r_2$

alors il existe $\alpha \in \mathbb{Z}_k$

$$0 < |\sigma_i(\alpha)| \leq \lambda_i, \quad 1 \leq i \leq n.$$

$0 \neq \underline{\sigma}(\alpha) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. B: $|z_i| < \lambda_i$.

$\hat{G} = \underline{\sigma}(\mathbb{Z}_k)$ $G \cap B \neq (0)$?