Théorème de Dirichlet sur les unités d'un corps de nombres.

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

r_1 = nombre de plongements de k dans $\mathbb{R}$ ($\mathbb{Q}$-isomorphismes)

$2r_2$ = nombre de plongement de k dans $\mathbb{C}$ non réels.

$\mathbb{Z}_k$ entiers de k. $\mathbb{Z}_k^\times$ unités de $\mathbb{Z}_k$

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

Rappel $n = r_1 + 2r_2$.

$k = \mathbb{Q}(\alpha)$, $[k:\mathbb{Q}] = n$

$\mathrm{Irr}_{\mathbb{Q}}(\alpha; X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$

$= (X - \alpha_1) \dots (X - \alpha_n)$ dans $\mathbb{C}[X]$

$\alpha_1, \dots, \alpha_n$ conjugués complexes de α.

$N = \mathbb{Q}(\alpha_1, \dots, \alpha_n) \supset \mathbb{Q}(\alpha_1) \simeq k \supset \mathbb{Q}$ normale

$\sigma : k \to \mathbb{C}$ $\mathbb{Q}$-isomorphisme $\Rightarrow \sigma(k) \subset N$

il y en a n

$\alpha_1, \dots, \alpha_{r_1}$ racines réelles $0 \leq r_1 \leq n$

$\alpha_{r_1+1}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+1}}, \dots, \overline{\alpha_{r_1+r_2}}$ racines non réelles

$n = r_1 + 2r_2$. $0 \leq r_2 \leq \frac{n}{2}$

Groupes abéliens (multiplicatifs) de type fini.

G abel. t. f.

$\{x \in G, \exists\, n \in \mathbb{Z}, n \neq 0, x^n = 1\} = G_{tors}$ est un sous-groupe fini de G. et il existe $r \geq 0$ (rang de G), $u_1, \dots, u_r \in G$ tel que tout élément de G s'écrive

de manière unique $\zeta . u_1^{a_1} \dots u_r^{a_r}$

$r = \mathrm{rang}_{\mathbb{Z}} G$

$G/G_{tors} \simeq \mathbb{Z}^r$

avec $\zeta \in G_{tors}$, $a_i \in \mathbb{Z}$ $(1 \leq i \leq r)$.

$G_{tors} \times \mathbb{Z}^r \longrightarrow G$ isomorphisme de groupes

$(\zeta, a_1, \dots, a_r) \longmapsto \zeta . u_1^{a_1} \dots u_r^{a_r}$

$G = \mathbb{Z}_k^\times$ $\quad (\mathbb{Z}_k^\times)_{tors}$ = racines de l'unité dans k.

ζ racine primitive m-ième de 1.

$\zeta \in k$ $\quad [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(m) \leq n$.

$\varphi(m) \to \infty$ quand $m \to \infty$

Lemme. k corps de nombres, $\alpha \in \mathbb{Z}_k$.

Propriétés équivalentes.

(i) $\alpha \in \mathbb{Z}_k^\times$

(ii) $N(\alpha) = \pm 1$

(iii) $N_{k/\mathbb{Q}}(\alpha) = \pm 1$.

(ii) $\Leftrightarrow$ (iii)

$$\begin{array}{c} k \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

$$N_{k/\mathbb{Q}}(\alpha) = N(\alpha)^{[k:\mathbb{Q}(\alpha)]}$$

$$N(\alpha) := N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

(i) $\Rightarrow$ (iii) $\quad \alpha \in \mathbb{Z}_k^\times \quad \exists\, \beta \in \mathbb{Z}_k,\ \alpha\beta = 1$

$$N_{k/\mathbb{Q}}(\alpha\beta) = N_{k/\mathbb{Q}}(\alpha) . N_{k/\mathbb{Q}}(\beta).$$

$$N_{k/\mathbb{Q}} : \begin{array}{ccc} k & \longrightarrow & \mathbb{Q} \\ \cup & & \cup \\ \mathbb{Z}_k & \longrightarrow & \mathbb{Z} \end{array}$$

$1 = \alpha\beta$

$N_{k/\mathbb{Q}}(\alpha\beta) = 1$.

$\alpha \quad \mathrm{irr}_{\mathbb{Q}}(\alpha, X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$.

$N(\alpha) = (-1)^n a_0$.

$N_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}^\times = \{+1, -1\}$

(ii) $\Rightarrow$ (i) $\quad \mathrm{Irr}_{\mathbb{Q}}(\alpha, X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$

$a_0 = \pm 1$.

$$\underbrace{\alpha^n + a_0\alpha^{n-1} + \dots + a_1\alpha}_{= \alpha\beta} = -a_0 = \mp 1.$$

$$\beta = \alpha^{n-1} + a_0\alpha^{n-2} + \dots + a_1 \in \mathbb{Z}_k$$

$\Rightarrow \alpha \in \mathbb{Z}_k^\times$.

Remarque. $X^n + b_{n-1}X^{n-1} + \dots + b_1 X + 1$

$b_i \in \mathbb{Q}$ pas tous entiers — irréd. dans $\mathbb{Q}[X]$.

α une racine $\quad N(\alpha) = \pm 1$

$\alpha \notin \mathbb{Z}_k$.

Sous-groupes de $\mathbb{R}^n$. (additifs).

Sous-groupes de $\mathbb{R}$.

K compact de $\mathbb{R}$

$K \cap G$ fini

discrets $\{ (0), \quad \mathbb{Z}x \quad x \in \mathbb{R}_{>0}$

denses $\{ \mathbb{Z} + \mathbb{Z}\sqrt{2}, \dots, \quad \mathbb{Q}, \mathbb{R}$

$t \in \mathbb{R} \quad \varepsilon > 0$

$\exists\, x \in G, \ |x - t| < \varepsilon$

Exercice. Si G est un sous-groupe discret de $\mathbb{R}$ ie existe $x \in G$, $x > 0$, $G = \mathbb{Z}x$. Si G est un sous-groupe de $\mathbb{R}$ non discret, G est dense.

Lemme. Un sous-groupe G de $\mathbb{R}^n$ est discret si et seulement si il existe U ouvert de $\mathbb{R}^n$ contenant 0, tel que $G \cap U$ soit discret.

$\Longrightarrow$ G discret $U = \mathbb{R}^n$. $G \cap \mathbb{R}^n = G$.

$\Longleftarrow$ Supposons G non discret.
$\exists z \in \mathbb{R}^n$ point d'accumulation.
$\forall \varepsilon > 0$ $\exists x \in G$, $0 < |x - z| < \varepsilon$

$|x|$ = norme euclidienne

$x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ $\quad |x| = \left(\sum_{i=1}^{n} x_i^2\right)^{1/2}$.

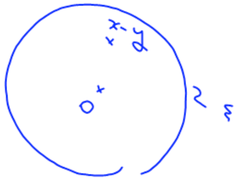
$x \in G$

$\exists y \in G$, $\quad 0 < |z - y| < |z - x| < \varepsilon$

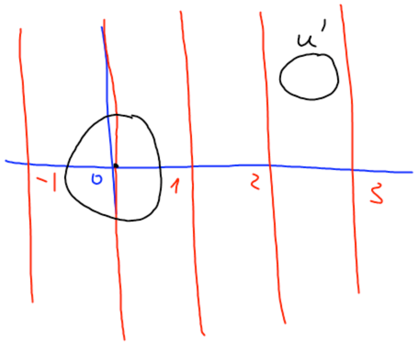
$0 < |x - y| \leq |z - y| + |z - x| < 2\varepsilon$

$x - y \in G$. $\longrightarrow$ 0 est un point d'accumulation de G.

G non discret $\Longrightarrow$ $\forall\, U$ voisinage ouvert de 0, $U \cap G$ n'est pas discret.



Exemple. $\mathbb{Z} \times \mathbb{R} = G \subset \mathbb{R}^2$



Proposition. G sous-groupe discret de $\mathbb{R}^n$. Il existe t, $0 \leq t \leq n$, et $e_1, \ldots, e_t \in G$ linéairement indépendants sur $\mathbb{R}$, tels que $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_t$.

Dans une base commençant par $e_1, \ldots, e_t$,

$$G = \mathbb{Z}^t \times (0)^{n-t} = \{(a_1, \ldots, a_t, 0, \ldots, 0)\,;\ a_i \in \mathbb{Z}\}$$

$t = 1$
$n = 2$

libre de type fini de rang t.

Démonstration.

$n=2$ $G=\mathbb{Z}^2$
$f_1=(2,0)$
$f_2=(0,3)$
$K=\{(t_1,t_2);\ 0\le t_1<2,\ 0\le t_2<3\}$

$G\subset\mathbb{R}^n$ discret

$f_1,\dots,f_t \in G$ linéairement indépendants sur $\mathbb{R}$, t maximal.

V l'esp. vect sur $\mathbb{R}$ engendré par G, t sa dimension. base formée d'élts de G. $\mathbb{Z}f_1+\dots+\mathbb{Z}f_t\leq G$.

K compact contenant $\{x_1f_1+\dots+x_tf_t;\ 0\le x_i<1;\ 1\le i\le t\}$

$K\cap G$ est fini.

$\mathbb{Z}$-module libre de t.f. rang t

$$G'=\mathbb{Z}f_1+\dots+\mathbb{Z}f_t \subset G\subset \mathbb{Z}\tfrac{1}{m}f_1+\dots+\mathbb{Z}\tfrac{1}{m}f_t$$

$x\in G$. $x=u_1f_1+\dots+u_tf_t$ $u_i\in\mathbb{R}$

$u_i=[u_i]+\{u_i\}$ $[u_i]\in\mathbb{Z}$
$0\le\{u_i\}<1$

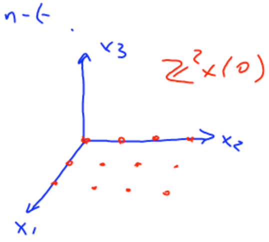
$x=y+z$
$y=[x_1]f_1+\dots+[x_t]f_t\in G'\subset G$
$z=\{x_1\}f_1+\dots+\{x_t\}f_t\in K$
$x,y\in G \Rightarrow z=x-y\in G\cap K$.
$(G:G')\le|G\cap K|$. $\Rightarrow G/G'$ fini ordre m.

Théorème de structure des sous-groupes de $\mathbb{R}^n$.

G sous-groupe de $\mathbb{R}^n$. Il existe un plus grand sous-espace vectoriel V de $\mathbb{R}^n$ contenu dans l'adhérence $\overline{G}$ de G; soit $d=\dim V$, $d+t$ la dimension de l'e.v. engendré par G. $G'=G\cap V$. Il existe G'' sous-groupe discret de G, rang t, tel que
$G=G'\oplus G''$.

Exemples.

1) G discret $\mathbb{Z}^t\times(0)^{n-t}$.
fermé.



$V=(0)$
$d=0$
$G'=(0)$ $G''=G$

2) G dense dans $\mathbb{R}^n$: ~~exple~~ $\mathbb{Z}^2+\mathbb{Z}(\sqrt{2},\sqrt{3})\subset\mathbb{R}^2$ dense

$\{(a+b\sqrt{2},\ c+b\sqrt{3});\ a,b,c\in\mathbb{Z}\}$

exple.
$G_1\times G_2\subset\mathbb{R}^2$
G_1,G_2 denses dans $\mathbb{R}$

$\overline{G}=\mathbb{R}^n=V$ $d=n$ $G'=G$ $G''=(0)$

3) $n=2$ $\quad \underset{\overset{\|}{G}}{\mathbb{Z}\times\mathbb{Q}} \subset \mathbb{R}^2$

$\overline{G} = \mathbb{Z}\times\mathbb{R}$ $\quad V = (0)\times\mathbb{R}$ $\quad d=1$.

$G' = 0\times\mathbb{Q}$ $\quad G'' = \mathbb{Z}(1,b)$

$G'' = \mathbb{Z}\times(0)$ $\quad b\in\mathbb{Q}$

$\downarrow$ $(b=0)$

$G = G'\oplus G''$

$\Downarrow$

(u,v) $\quad (u,v) = (\underset{\underset{\mathbb{Q}}{\cap}}{0,w}) + (u, v-w)$ $\quad \dot{G''}$

$u\in\mathbb{Z}$ $\quad v-w = ub$ $\quad w\in\mathbb{Q}$

$v\in\mathbb{Q}$.

$(u,v) = (0, v-ub) + u(1,b)$ $\quad w = v-ub$.

$G = \mathbb{Z}\times\mathbb{R}$

Démonstration.

$\rho>0$ $\quad B(0,\rho) = \{x\in\mathbb{R}^n ;\ |x|<\rho\}$.

$G\cap B(0,\rho)$ $\quad$ soit V_ρ l'espace vectoriel engendré. $\quad d=\dim V$

$\rho\mapsto \dim V_\rho$ $\nearrow$ $\quad \exists\, \rho_0$ $\quad V_\rho = V_{\rho_0} = V$ $\quad \forall \rho\le\rho_0$.

$G' = G\cap V$ est dense dans V.

$x\in V$ $\quad \varepsilon>0$ $\quad \forall\, \eta\le\rho_0$.

$\exists$ base $e_1,\dots,\underset{\underset{G}{\cap}}{e_d}$ de V $\quad x = x_1e_1+\dots+x_de_d$.

$|e_i|\le\eta$ $\quad g = [x_1]e_1+\dots+x_de_d \in G$

$x = x_1e_1+\dots+x_de_d$ $\quad |e_i|\le\eta$.

$g = [x_1]e_1+\dots+[x_d]e_d$.

$$|x-g| = \left|\sum_{i=1}^d \{x_i\}e_i\right| \le \sum_{i=1}^d |e_i| \le d\eta \le \varepsilon.$$

$\eta = \min\{\rho_0 ;\ \frac{\varepsilon}{d}\}$. $\quad \Rightarrow G'$ dense dans V.

W l'espace vectoriel engendré par G

$\underset{d}{V} \subset \overline{G} \subset \underset{d+k}{W}$ $\quad W = V\oplus V'$

$p : W \longrightarrow V'$ $\quad \ker p = V$

$p(G)$ est un sous-groupe discret de V'

base $p(y_1),\dots,p(y_k)$. $\quad G'' = \mathbb{Z}y_1+\dots+\mathbb{Z}y_k$.