

car z est un entier algébrique. La taille de z est donc égale à $\|\Phi(z)\|$. Mais on a vu qu'il n'y a qu'un nombre fini de nombres algébriques de degré d de taille bornée!

• Étape 2: D'après le théorème, $\Phi(\mathcal{O}_K)$ est un réseau de V . Son rang est la dimension maximale d'une famille l.l.e. dans $\Phi(\mathcal{O}_K)$, donc $\leq n = \dim_{\mathbb{R}} V$. Or K est un $\mathbb{Q}$ -espace vectoriel de dimension n . Soient $(\alpha_1, \dots, \alpha_n)$ une base de K sur $\mathbb{Q}$, et soit $D = \text{ppcm}$ des dénominateurs de $\alpha_1, \dots, \alpha_n$. Alors $(D\alpha_1, \dots, D\alpha_n)$ est une base de K formée d'entiers algébriques dont l'image par Φ est une famille l.l.e. de cardinal n . $\square$

⑥ ordres

Définition. Soit K un corps de nombres. Un ordre de K est un sous-anneau $A \subset K$ tel que:

- * A est un groupe additif de type fini
- * A engendre K comme $\mathbb{Q}$ -espace vectoriel

Exemples: $\mathcal{O}_K$ est un ordre de K

Exemple: Soit α un entier algébrique de degré n et soit $K = \mathbb{Q}(\alpha)$. Alors $\mathbb{Z}[\alpha]$ est un ordre de K . En effet, $\mathbb{Z}[\alpha]$ agit sur K sur $\mathbb{Q}$, et la base $1, \alpha, \dots, \alpha^{n-1}$ de K sur $\mathbb{Q}$, et est engendrée comme groupe abélien par elle car tout α^k est combinaison de $1, \dots, \alpha^{n-1}$ à coefficients entiers.

Lemme: Tout ordre de K est contenu dans

$\mathcal{O}_K$ (appelé donc l'ordre maximal)

Preuve: Soit $A \subset K$ un ordre et soit $z_1, \dots, z_m$ une famille génératrice comme groupe abélien. Soit $w \in A$ et écrivons

$$w z_j = \sum_{i=1}^m a_{ij} z_i \quad a_{ij} \in \mathbb{Z}$$

le polynôme caractéristique P de la matrice (a_{ij}) annule l'endomorphisme $M_w: A \rightarrow A$ donné par multiplication par w . Comme $P \in \mathbb{Z}[X]$, entière et $P(w) = 0$, w est un entier algébrique. $\square$

Corollaire: Soit K un corps de nombres de degré n .
En tant que groupe abélien, un ordre de K est
isomorphe à $\mathbb{Z}^n$.

Preuve: Comme A est contenu dans $\mathcal{O}_K$, c'est
un sous-groupe d'un groupe isomorphe à $\mathbb{Z}^n$.
Un tel groupe est isomorphe à $\mathbb{Z}^m$ pour un
 $m \in \{0, \dots, n\}$. Comme A engendre K en tant
que $\mathbb{Q}$ -espace vectoriel, on a $m = n$. □

Définition: Soit A un ordre de K . Le
discriminant de A est le discriminant
d'une $\mathbb{Z}$ -base du groupe abélien A .

Comme $\det_{\mathbb{P}}(\beta') = \pm 1$ pour deux telles
bases β, β' , et que $\text{disc}(\beta') = \det_{\mathbb{P}}(\beta')^2 \text{disc}(\beta)$,
cette notion ne dépend pas du choix de
la base mais seulement de A .

Définition. On appelle discriminant de K
le discriminant de l'ordre $\mathcal{O}_K$.

Proposition: Soient K un corps de nombres et
 A un ordre de K . Alors
$$\text{disc}(A) = \text{disc}(K) \cdot |\mathcal{O}_K/A|^2$$

Preuve: Notons $n = [K:\mathbb{Q}]$. Par le théorème de la base adaptée, appliqué au $\mathbb{Z}$ -module libre $\mathcal{O}_K$ et au sous-module A , il existe une base $(w_1, \dots, w_n)$ de $\mathcal{O}_K$ et des entiers $d_1, \dots, d_n \geq 1$ tels que $(d_1 w_1, \dots, d_n w_n)$ soit une base de A . On a donc

$$\begin{aligned} \text{disc}(A) &= \det \left(q_i(d_j w_j) \right)^2 \\ &= (d_1 \dots d_n)^2 \text{disc}(K) \end{aligned}$$

En outre, $\mathcal{O}_K/A \cong \prod \mathbb{Z}/d_i \mathbb{Z}$ est de cardinal $(d_1 \dots d_n)^2$. $\square$

Corollaire: Si $\text{disc}(A)$ est sans facteur carré, alors $A = \mathcal{O}_K$.

Exemple: Soit α une racine de $P = X^3 + X + 1$ et $K = \mathbb{Q}(\alpha)$. Le polynôme P est irréductible dans $\mathbb{Q}[X]$, par exemple car $P \bmod 2 \in \mathbb{F}_2[X]$ n'a pas de racine. Donc $[K:\mathbb{Q}] = 3$ et α est un entier algébrique. Calculons le discriminant de l'ordre $\mathbb{Z}[\alpha]$ de K :

$$\text{disc}(\mathbb{Z}[\alpha]) = \det \left(\text{Tr}_K(z_i z_j) \right)$$

$$= \det \begin{pmatrix} \text{Tr}_K(1) & \text{Tr}_K(\alpha) & \text{Tr}_K(\alpha^2) \\ \text{Tr}_K(\alpha) & \text{Tr}_K(\alpha^2) & \text{Tr}_K(\alpha^3) \\ \text{Tr}_K(\alpha^2) & \text{Tr}_K(\alpha^3) & \text{Tr}_K(\alpha^4) \end{pmatrix}$$

base de $\mathbb{Z}[\alpha]$

$$\text{Tr}_K(1) = 3$$

$\text{Tr}_K(\alpha) = 0$ car le polynôme minimal est $P = X^3 + X + 1$
 Dans la base $(1, \alpha, \alpha^2)$, la matrice de multiplication par α^2 est

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}$$

$$\alpha^3 = -\alpha - 1$$

$$\alpha^4 = -\alpha - \alpha^2$$

donc $\text{Tr}_K(\alpha^2) = -2$. Par suite,

$$\text{Tr}_K(\alpha^3) = \text{Tr}_K(-\alpha - 1) = -3$$

$$\text{Tr}_K(\alpha^4) = \text{Tr}_K(-\alpha - \alpha^2) = 2$$

La matrice est donc:

$$\text{disc}(\mathbb{Z}[\alpha]) = \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & -3 & 2 \end{pmatrix}$$

$$= 3(-4-9) - 2(-4)$$

$$= -31$$

Come $\text{disc}(\mathbb{Z}[\alpha])$ est sans facteur carré,

$$\boxed{\mathcal{O}_K = \mathbb{Z}[\alpha]}$$

Rappelons l'application

$$\Phi: K \longrightarrow \mathbb{R}^{21} \times \mathbb{C}^{22} = \checkmark$$

$$z \longmapsto (\varphi_1(z), \dots, \varphi_{n_1+n_2}(z))$$

$\Phi(A)$ est un réseau de rang n de V

Proposition: Identifions $\mathbb{R}^{21} \times \mathbb{C}^{22}$ à $\mathbb{R}^n$
et soit P un déterminant fondamental de $\Phi(A)$
dans $\mathbb{R}^n$. Alors

$$|\text{disc}(A)| = 4^{n_2} \text{vol}(P)^2$$

Preuve: Soit $w_1, \dots, w_n$ un b.c. de A
et soit $D = (\varphi_j(w_k))$. Les opérations
élémentaires

$$L_{n_1+j} \longleftarrow \frac{1}{2} (L_{n_1+j} + L_{n_1+n_2+j})$$

$$L_{n_1+n_2+j} \longleftarrow i (L_{n_1+n_2+j} - L_{n_1+j})$$

Ainsi la matrice

$$D' = \begin{pmatrix} \varphi_1(w_1) & \dots & \varphi_1(w_n) \\ \vdots & & \vdots \\ \varphi_{n_1}(w_1) & \dots & \varphi_{n_1}(w_n) \\ \text{Re } \varphi_{n_1+1}(w_1) & \dots & \text{Re } \varphi_{n_1+1}(w_n) \\ \text{Im } \varphi_{n_1+1}(w_1) & \dots & \text{Im } \varphi_{n_1+1}(w_n) \\ \vdots & & \vdots \\ \text{Re } \varphi_{n_1+n_2+1}(w_1) & \dots & \text{Re } \varphi_{n_1+n_2+1}(w_n) \\ \text{Im } \varphi_{n_1+n_2+1}(w_1) & \dots & \text{Im } \varphi_{n_1+n_2+1}(w_n) \end{pmatrix}$$

et multiplie le déterminant par $(\frac{i}{2})^{r_2}$.
Après r_2 échanges de lignes, on arrive à la matrice

$$D'' = \begin{pmatrix} \vdots & & \\ \operatorname{Re} \varphi_{2r_1+1}(w_1) & \dots & \\ \operatorname{Im} \varphi_{2r_1+1}(w_1) & \dots & \\ \vdots & & \\ \operatorname{Re} \varphi_{2r_1+2r_2}(w_1) & \dots & \\ \operatorname{Im} \varphi_{2r_1+2r_2}(w_1) & \dots & \end{pmatrix}$$

donc le déterminant $|\det(D'')|$ est le volume du domaine fondamental $P = [0,1]w_1 + \dots + [0,1]w_n$ de $\Phi(A)$ dans $\mathbb{R}^n$. On a donc:

$$\operatorname{vol}(P) = |\det(D'')|$$

$$\det(D'')^2 = \operatorname{vol}(P)^2$$

Avec $\det(D'') = (-\frac{i}{2})^{r_2} \det(D)$, on trouve

$$\operatorname{vol}(P)^2 = \left(-\frac{1}{4}\right)^{r_2} \det(D)^2 = \left(\frac{1}{4}\right)^{r_2} \operatorname{disc}(A)$$

c'est-à-dire $\boxed{\operatorname{disc}(A) = (-4)^{r_2} \operatorname{vol}(P)^2} \quad \square$

Remarque: on a donc montré que le signe du discriminant d'un ordre de K est $(-1)^{r_2}$, où r_2 est le nombre de paires conjuguées complexes de K .

Exemple: Soit $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteur carré. Alors

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \pmod{4} \end{cases}$$

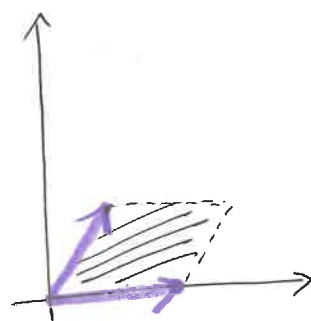
Si $d > 0$, K a $r_1 = 2$ plongements réels et

$$\text{disc}(K) = \begin{cases} \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d & d \not\equiv 1 \pmod{4} \\ \det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = d & \text{si } d \equiv 1 \pmod{4} \end{cases}$$

Si $d < 0$, K a $r_2 = 1$ plongement complexe non conjugué et $\text{disc}(K)$ est négatif.

Si $d = -3$, $\Phi: K \longrightarrow \mathbb{R}^2$

$$\begin{aligned} 1 &\longmapsto (1, 0) \\ \frac{1+\sqrt{-3}}{2} &\longmapsto \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \end{aligned}$$



$$\text{vol} = \frac{\sqrt{3}}{2}$$

⑦ le théorème des unités de Dirichlet

on amène à l'étude de la structure multiplicative de l'anneau des entiers $\mathcal{O}_K$.