Lemme (rappel).

A anneau (intègre) $\quad K$ corps $\supset A$

$x \in K$. Propriétés équivalentes.

(i) α est racine d'un polynôme unitaire à coefficients dans A

(ii) L'anneau $A[\alpha]$ est un A-module de type fini

(iii) Il existe un sous-anneau B de K contenant A et α qui est un A-module de type fini.

Définition α est entier sur A.

Vu (ii) $\Rightarrow$ (iii) $\quad$ (i) $\Rightarrow$ (ii)

Démonstration de (iii) $\Rightarrow$ (i)

$A \subset B \subset K$, $\alpha \in B$ $\quad \wedge\ B = Ax_1 + \dots + Ax_m$. $\exists\, x_1, \dots, x_m \in B$

$[\alpha] : B \longrightarrow B$, $z \mapsto \alpha z$

$$\alpha x_i = \sum_{j=1}^{m} a_{ij} x_j \qquad a_{ij} \in A.$$

$$\alpha I_m - (a_{ij}) : z \mapsto 0.$$

$$P(X) = \det\left(X I_m - (a_{ij})\right) \in A[X] \text{ unitaire}$$

$P(\alpha) = 0$.

Corollaire. A anneau $\subset K$

L'ensemble des éléments de K entiers sur A est un sous-anneau de K qui contient A.

= Fermeture intégrale de A dans K.

Dém. α_1, α_2 entiers.

$A \subset A[\alpha_1] \subset B$

$A[\alpha_1]$: sous-anneau de B, A-module de t.f

$A[\alpha_1, \alpha_2]$ est un A-module de type fini $\ni \alpha_1 + \alpha_2, \alpha_1\alpha_2$.

$A[\alpha_1][\alpha_2] = A[\alpha_1, \alpha_2] \subset B$

Sous-anneau $A[\alpha_1]$-module de type fini

Proposition. (Transitivité de la fermeture intégrale).

$A \subset K \quad A_0$ la fermeture intégrale de A dans K.

$\gamma \in K$ entier sur A_0. Alors $\gamma \in A_0$.

Démonstration.

γ entier sur A_0. $\quad f \in A_0[X]$ unitaire $f(\gamma) = 0$.

$\beta_1, \dots, \beta_m$ les coefficients de f. $\to \in A_0$ entiers sur A

$A \subset A[\beta_1, \dots, \beta_m] \subset A[\beta_1, \dots, \beta_m, \gamma] \subset K$.

$\gamma \in$ anneau + A-module t.f.

$\Rightarrow \gamma$ entier sur A

Définition 2 Un anneau A est intégralement clos s'il est égal à sa clôture intégrale.

Définition 1 La clôture intégrale d'un anneau est sa fermeture intégrale dans son corps des fractions

Exemples ① $A = \mathbb{Z}$ corps des fractions $\mathbb{Q}$.
clôture intégrale de $\mathbb{Z}$ est $\mathbb{Z}$.
$\mathbb{Z}$ est intégralement clos

② $A = \mathbb{Z}$ $K = \mathbb{Q}(i)$ La fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(i)$ est $\mathbb{Z}[i]$.

Proposition. Un anneau factoriel est intégralement clos.

Exemples. $\begin{cases} \mathbb{Z} \\ K[X_1, \dots, X_m] \end{cases}$

A factoriel $\Rightarrow A[X]$ aussi.

Démonstration.

$A \subset K$ corps des fractions.

$\alpha \in K$ α entier sur A

$\exists\ X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$

$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ $a_i \in A$, $\alpha \in K$

$\alpha = \frac{u}{v}$, $u, v \in A$ $\operatorname{pgcd}(u,v) = 1$.

$$u^n + \underbrace{a_{n-1}u^{n-1}v + \dots + a_1 u v^{n-1} + a_n v^n}_{} = 0$$

si $d \mid v$ alors $d \mid u^n$

donc d est une unité ($d \in A^\times$).

donc $v \in A^\times$ et $\frac{u}{v} \in A$

Cas particulier $A = \mathbb{Z}$.

- Rappel : "nombre algébrique" = élément de $\mathbb{C}$ algébrique sur $\mathbb{Q}$
- "Entier algébrique" = élément de $\mathbb{C}$ entier sur $\mathbb{Z}$

{entiers algébriques} est un sous-anneau du corps $\overline{\mathbb{Q}}$ des nombres algébriques.

K corps de nombres (= extension finie de $\mathbb{Q}$)

L'anneau des entiers de K est la fermeture intégrale de $\mathbb{Z}$ dans K

$\mathcal{O}_K = \mathbb{Z}_K = \{\alpha \in K,\ \text{entier sur } \mathbb{Z}\}$

idéal d'un corps de nombres = idéal de $\mathbb{Z}_K$.

unité d'un corps de nombres = unité de $\mathbb{Z}_K$

$\mathbb{Z}_K^\times$

Structure de $\mathbb{Z}_K$.

Théorème. Soit K un corps de nombres, $[K:\mathbb{Q}]=n$. Alors $\mathbb{Z}_K$ est un $\mathbb{Z}$-module libre de rang n.

Il existe $e_1, \dots, e_n \in K$ entiers sur $\mathbb{Z}$ tels que $\mathbb{Z}_K = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$.

Exemples ① $K=\mathbb{Q}$ $\quad \mathbb{Z}_K = \mathbb{Z}$ $\quad n=1$ $\quad e_1 = 1$ (ou $e_1=-1$)

② $n=2$ $\quad K/\mathbb{Q}$ extension quadratique

$K = \mathbb{Q}(\sqrt{d})$ $\quad d \in \mathbb{Z}$ sans facteur carré.

Entiers de $\mathbb{Q}(\sqrt{d}) =$
$a + b\sqrt{d}$, $\quad a, b \in \mathbb{Q}$.
racines d'un polynôme unitaire $\in \mathbb{Z}[X]$.

$\mathbb{Z} \subset \mathbb{Z}_K$

$\sqrt{d} \in \mathbb{Z}_K$ $\qquad X^2 - d$.

$\mathbb{Z}\sqrt{d} \subset \mathbb{Z}_K$. $\qquad \mathbb{Z} + \mathbb{Z}\sqrt{d} \subset \mathbb{Z}_K$.

$d=-1$ $\quad \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ $\quad \mathbb{Z}+\mathbb{Z}i = \mathbb{Z}[i] = \mathbb{Z}_{\mathbb{Q}(i)}$

$d=2$ $\quad \mathbb{Q}(\sqrt{2})$ entiers $\mathbb{Z}+\mathbb{Z}\sqrt{2} = \mathbb{Z}[\sqrt{2}]$

$d=-3$ $\quad \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3)$

$\zeta_3 = \frac{1+i\sqrt{3}}{2}$ $\qquad X^2+X+1$

anneau des entiers de $\mathbb{Q}(i\sqrt{3})$ est $\mathbb{Z}+\mathbb{Z}\zeta_3 = \mathbb{Z}[\zeta_3]$

$\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3)$

Nombre d'or $\quad \frac{1+\sqrt{5}}{2} = \phi$ $\qquad X^2-X-1$

entier algébrique.

anneau des entiers de $\mathbb{Q}(\phi) = \mathbb{Q}(\sqrt{5})$ est $\mathbb{Z}[\phi] = \mathbb{Z}+\mathbb{Z}\phi$

Résultat (Exercice). $\quad d$ entier $\in \mathbb{Z}$ sans facteur carré, $d \neq 0$, $d \neq 1$.

L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est

$$\begin{cases} \mathbb{Z}+\mathbb{Z}\sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4 \\ \mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4. \end{cases}$$

Proposition. α nombre algébrique de degré n. Alors α est entier sur $\mathbb{Z}$

$\Longleftrightarrow$ α est racine d'un polynôme unitaire de degré n à coefficients dans $\mathbb{Z}$

trivial $\Longleftarrow$

$\Longleftrightarrow$ le polynôme $\mathrm{Irr}_{\mathbb{Q}}(\alpha; X) \in \mathbb{Z}[X]$.

$\Longleftrightarrow$ le polynôme minimal $\in \mathbb{Z}[X]$ de α sur $\mathbb{Z}$ est unitaire.

Dém. de : α nombre algébrique de degré n et entier sur $\mathbb{Z}$

son polynôme minimal sur $\mathbb{Z}$ est unitaire.

f

$P(X)$ unitaire $\in \mathbb{Z}[X]$, $P(\alpha)=0$.

$P(X) = f_1(X) \dots f_\ell(X)$ dans l'anneau factoriel $\mathbb{Z}[X]$

$f_j \in \mathbb{Z}[X]$ irréductibles dans $\mathbb{Z}[X]$.

$\Rightarrow$ les f_j sont unitaires.

un des f_j est f.

Lemme. α nombre algébrique.

$\mathrm{Irr}_{\mathbb{Q}}(\alpha; X) \in \mathbb{Q}[X]$ unitaire

$a_0 \in \mathbb{Z}_{>0}$ le + petit dénominateur commun des coefficients

$\rightarrow$ polynôme minimal de α sur $\mathbb{Z}$

$a_0X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$, $n = [\mathbb{Q}(\alpha):\mathbb{Q}]$

$a_0 > 0$ irréductible

$\Rightarrow$ $a_0\alpha$ est un entier algébrique.

Remarque $\{a \in \mathbb{Z},\ a\alpha \text{ entier algébrique}\}$ idéal de $\mathbb{Z}$ contient a_0. Exercice Exemples avec $= a_0\mathbb{Z}$ ou $\neq a_0\mathbb{Z}$.

Remarque. On peut démontrer :

α nombre algébrique. $\alpha_1, \dots, \alpha_n$ ses conjugués

a_0 (= coeff. directeur du polynôme minimal de α sur $\mathbb{Z}$)

est le générateur >0 de l'idéal

$$\left\{ a \in \mathbb{Z} ;\ a\,\alpha_{i_1} \dots \alpha_{i_k} \text{ est entier sur } \mathbb{Z}\ \ \forall \{i_1, \dots, i_k\} \subset \{1, \dots, n\} \right\}$$

Démonstration. de $a_0\alpha$ est entier

$a_0X^n + \dots + a_{n-1}X + a_n \in \mathbb{Z}[X]$

α racine.

$\times\ a_0^{n-1}$.

$$a_0^nX^n + a_1a_0^{n-1}X^{n-1} + a_2a_0^{n-1}X^{n-2} + \dots + a_{n-1}a_0^{n-1}X + a_na_0^{n-1}$$

$$Y^n + a_1Y^{n-1} + a_2a_0Y^{n-2} + \dots + a_{n-1}a_0^{n-2}Y + a_na_0^{n-1}$$

$\in \mathbb{Z}[Y]$ nul en $Y = a_0\alpha$

Résultat auxiliaire.

Théorème de structure des modules de type fini sur un anneau principal. A

- Soit M un A-module libre de rang m.

Soit N un sous-module de M.

Alors N est libre de rang $n \leq m$

De plus il existe une base $e_1, \dots, e_m$ de M sur A et il existe $a_1, \dots, a_n \in A$ tels que $a_1 e_1, \dots, a_n e_n$ soit une base de N sur A et $a_i \mid a_{i+1}$, $1 \leq i \leq n-1$.

- Si M est un A-module de type fini, c'est un quotient d'un module libre de type fini

M de type fini $\exists$ système générateur $x_1, \dots, x_m$

$$A^m \xrightarrow{\psi} M \qquad \psi \text{ homomorphisme surjectif}$$

$$(a_1, \dots, a_m) \longmapsto a_1 x_1 + \dots + a_m x_m$$

A^m A-module libre de rang m

$M \simeq A^m / \ker \psi$ $\qquad$ $\ker \psi$ est un A-module libre de rang $n \leq m$

Cas particulier $\quad A = \mathbb{Z}$ $\qquad$ $\mathbb{Z}$-modules t.f $=$ groupe abélien de type fini

$$M \simeq \underbrace{M_{tors}}_{\text{fini}} \times \mathbb{Z}^r$$

$[K:\mathbb{Q}] = n$ $\qquad$ $\mathbb{Z}_K$ est un $\mathbb{Z}$-module libre de rang n.

$\exists\, \alpha \in \mathbb{Z}_K$

$K = \mathbb{Q}(\alpha)$ $\qquad$ $\mathbb{Z} + \mathbb{Z}\alpha + \dots + \mathbb{Z}\alpha^{n-1} \subset \mathbb{Z}_K$

$1, \alpha, \dots, \alpha^{n-1} \in \mathbb{Z}_K$. $\qquad$ $\mathbb{Z}$-module libre de rang n.

$\mathbb{Q}$-l-i.

La forme bilinéaire $\quad (x,y) \longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$

est symétrique non dégénérée. $\quad K \times K \longrightarrow \mathbb{Q}$ $\qquad$ $\mathbb{Q}$-e.v

$e_1 = 1, e_2 = \alpha, \dots, e_n = \alpha^{n-1}$ est une base de $K/\mathbb{Q}$.

$\exists\, e_1^*, \dots, e_n^*$ autre base de $K/\mathbb{Q}$, $\quad \mathrm{Tr}_{K/\mathbb{Q}}\, e_i e_j^* = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

$e_i \in \mathbb{Z}_K$. $\quad e_j^* \in K$.

$\exists\, d$ entier > 0 $\qquad d e_j^* \in \mathbb{Z}_K$.

Soit $x \in \mathbb{Z}_K$. $\qquad e_j = \alpha^{j-1} \quad (1 \leq j \leq n)$

$$x = \sum_{j=1}^{m} a_j e_j \qquad a_j \in \mathbb{Q}.$$

$$x e_i^* = \sum_{j=1}^{n} a_j e_j e_i^*$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(x e_i^*) = \sum_{j=1}^{n} a_j \mathrm{Tr}_{K/\mathbb{Q}}(e_j e_i^*) = a_i$$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\underbrace{d e_i^* x}_{\mathbb{Z}_K}) = d a_i \in \mathbb{Z}$$

$$\boxed{\mathrm{Tr}_{K/\mathbb{Q}}(\mathbb{Z}_K) \subset \mathbb{Z}}$$

$$\mathbb{Z}_K \subset \frac{1}{d}(\mathbb{Z}e_1 + \dots + \mathbb{Z}e_n).$$

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

base $\frac{1}{d}e_1, \dots, \frac{1}{d}e_n$.

$\mathbb{Z}_K$ est un $\mathbb{Z}$-module libre rang $\leq n$

contient $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_n \Rightarrow$ rang $= n$

Lemme $Tr_{K/\mathbb{Q}}(\mathbb{Z}_K) \subset \mathbb{Z}$

$N_{K/\mathbb{Q}}(\mathbb{Z}_K) \subset \mathbb{Z}$ et $N_{K/\mathbb{Q}}(\mathbb{Z}_K^\times) \subseteq \{\pm 1\}$

α algébrique. degré n.

$\cap$

K $\qquad [K:\mathbb{Q}] = m \qquad n \mid m$

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

$a_i \in \mathbb{Q}$

$$\begin{cases} N_{K/\mathbb{Q}}(\alpha) = \left((-1)^n a_0\right)^{m/n} = (-1)^m a_0^{m/n} \\ Tr_{K/\mathbb{Q}}(\alpha) = -\frac{m}{n} a_{n-1} \end{cases}$$