

VII. — ÉLÉMENTS ENTIERS

Exercice 1 Éléments entiers sur un anneau

Soient $A \subseteq B$ deux anneaux commutatifs. Les assertions suivantes sont équivalentes pour un élément $b \in B$.

- (i) Il existe $N \in \mathbb{N}$, $a_1, \dots, a_N \in A$ tels que $b^N + a_1 b^{N-1} + \dots + a_N = 0$.
 - (ii) L'anneau $A[b]^\dagger$ est de type fini comme A -module *i.e.* $\exists m \in \mathbb{N}$, $e_1, \dots, e_m \in B$, $A[b] = Ae_1 + \dots + Ae_m$.
 - (iii) Il existe $A[b] \subseteq C \subseteq B$ un sous-anneau qui est de type fini comme A -module.
- a) Montrer $(i) \Rightarrow (ii) \Rightarrow (iii)$.
- b) Si C vérifie (iii) , soit $M = (a_{ij}) \in \mathcal{M}_m(A)$ telle que

$$\forall 1 \leq j \leq m, be_j = \sum_{i=1}^m a_{ij} e_i.$$

Montrer que

$$\forall P(X) \in A[X], \forall 1 \leq j \leq m, P(b)e_j = \sum_{i=1}^m P(M)_{ij} e_i.$$

- c) En déduire $(iii) \Rightarrow (i)$, à l'aide du théorème de Cayley-Hamilton.
On dit que b est entier sur A si $(i), (ii), (iii)$ sont vérifiées.
- d) Montrer que $\sqrt{2}$ est entier sur $\mathbb{Z}$ mais non $\frac{1}{\sqrt{2}}$.
- e) Montrer que si $b_1, b_2 \in B$ sont entiers sur l'anneau A , alors $b_1 \pm b_2, b_1 b_2$ aussi. En déduire que

$$\overline{\mathbb{Z}},$$

ensemble des éléments de $\mathbb{C}$ entiers sur $\mathbb{Z}$, est un sous-anneau de $\mathbb{C}$. Montrer que $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

- f) Soit $x \in \mathbb{C}$. Vérifier que x est entier sur $\mathbb{Z} \Leftrightarrow x$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal unitaire sur $\mathbb{Q}$ est à coefficients entiers.

Exercice 2 Entiers des extensions quadratiques

- a) Soit d un entier $\neq 1$ sans facteur carré. On note $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$. Vérifier que $\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$.
- b) On pose $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. Montrer que $x \mapsto \bar{x}$ est un automorphisme de $\mathbb{Q}(\sqrt{d})$ et que $\bar{x} = x \Leftrightarrow x \in \mathbb{Q}$.
- c) On note $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{d})$. Montrer que $\mathbb{Z}[\sqrt{d}] \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ et que si $d \equiv 1 \pmod{4}$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \leq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
- d) Soit $x = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Montrer que $\bar{x} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ et en déduire que $2a, a^2 - b^2 d \in \mathbb{Z}$.

$\dagger$. $A[b] := \{a_0 + \dots + a_K b^K : K \in \mathbb{N}, a_0, \dots, a_K \in A\}$.

e) En déduire

$$a \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}, a \in \frac{1}{2} + \mathbb{Z} \Rightarrow b \in \frac{1}{2} + \mathbb{Z}.$$

Indication. Utiliser que d est sans facteur carré.

f) Montrer que $(2a)^2 - d(2b)^2 = 0 \pmod{4}$ et conclure que :

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

Exercice 3 Indépendance linéaire des racines carrées d'entiers

a) Montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ et en déduire $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. En déduire le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.

b) **Généralisation.**

Montrer par récurrence sur $N \geq 0$ que si $a_1, \dots, a_N$ sont des entiers > 1 sans facteur carré, deux à deux premiers entre eux, alors

$$[\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_N}) : \mathbb{Q}] = 2^N.$$

Indication. On rappelle que si $K_1 < K_2$ sont des corps, on note $[K_2 : K_1] = \dim_{K_1} K_2$. De plus, si $K_1 < K_2 < K_3$ sont des corps, alors

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$$

(c'est la multiplicativité des degrés).

c) Montrer que les $\sqrt{n}$, $n \in \mathbb{N}_{>0}$, sans facteur carré, sont $\mathbb{Q}$ -linéairement indépendants.

d) Montrer que si $N \geq 0$ et si $a_1, \dots, a_N$ sont des entiers > 0 sans facteur carré, deux à deux premiers entre eux, alors

$$\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_N}) = \mathbb{Q}(\sqrt{a_1} + \dots + \sqrt{a_N}).$$

Indication. Soit $K = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_N})$. Justifier que pour tout $1 \leq i \leq N$, il existe $\varphi_i : K \rightarrow K$ automorphisme de corps tel que $\forall 1 \leq j \leq N$, $\varphi_i(\sqrt{a_j}) = \sqrt{a_j}$ si $j \neq i$, $-\sqrt{a_i}$ si $j = i$. En déduire que le polynôme minimal de $\sqrt{a_1} + \dots + \sqrt{a_N}$ sur $\mathbb{Q}$ a au moins 2^N racines ...