

Chapitre 3 : Extensions de corps, éléments algébriques

EXERCICE 1 : Déterminer le degré des extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$. A-t-on $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2})$?
Pour quels nombres premiers p et q a-t-on $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$?

EXERCICE 2 : Trouver le polynôme minimal de $\sqrt[5]{2}$ dans $\mathbb{Q}$ et dans $\mathbb{Q}(\sqrt{2})$.

EXERCICE 3 : Déterminer le degré des extensions de $\mathbb{Q}$ suivantes et en trouver une base.

1) $\mathbb{Q}(j)$ 2) $\mathbb{Q}(\cos \frac{2\pi}{3})$ 3) $\mathbb{Q}(\sin \frac{2\pi}{3})$

4) $\mathbb{Q}(\cos \frac{2\pi}{5})$, $\mathbb{Q}(e^{\frac{2i\pi}{5}})$ et $\mathbb{Q}(\sqrt{5})$ Quels sont les liens entre ces 3 corps?

(Montrer que $1+X+\dots+X^p$ est irréductible dans $\mathbb{Q}$ et plus généralement $1+X+\dots+X^{p-1}$ est irréductible dans $\mathbb{Q}$ si p est premier)

EXERCICE 4 : Soit $\mathbb{R} \subset \mathbb{K}$ une extension de corps. Soit $\alpha \in \mathbb{K}$ un élément algébrique sur $\mathbb{R}$. Si $P_\alpha \in \mathbb{R}[X]$ est le polynôme minimal de α , montrer que toutes les racines de P_α dans $\mathbb{K}$ admettent P_α comme polynôme minimal.

EXERCICE 5 : Soit $\mathbb{R} \subset \mathbb{C}$ une extension de $\mathbb{R}$ par $\mathbb{C}$. Soit $\alpha \in \mathbb{C}$ un élément algébrique sur $\mathbb{R}$. Montrer que α est racine simple de son polynôme minimal P_α .

EXERCICE 6 : Soit $\mathbb{R} \subset \mathbb{K}$ une extension de corps et $\alpha \in \mathbb{K}$ un élément algébrique sur $\mathbb{R}$. Soit $P_\alpha \in \mathbb{R}[X]$ le polynôme minimal de α . Montrer que l'extension $\mathbb{R}(\alpha)$ sur $\mathbb{R}$ est isomorphe au corps de rupture de P_α .

Chapitre 3 : Extensions de corps, éléments algébriques

EXERCICE 1 : Déterminer le degré des extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$. A-t-on $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2})$?

Pour quels nombres premiers p et q a-t-on $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$?

1. Le réel $\sqrt{2}$ n'est pas rationnel. Il est algébrique sur $\mathbb{Q}$.

Le polynôme $P = X^2 - 2$ vérifie $P(\sqrt{2}) = 0$. Il est irréductible dans $\mathbb{Q}$ sinon $\sqrt{2}$ serait racine d'un polynôme du 1^{er} degré à coefficients dans $\mathbb{Q}$ et $\sqrt{2}$ serait rationnel. On en déduit que le degré de l'extension $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{Q}$ qui est égal au degré du polynôme minimal de $\sqrt{2}$ dans $\mathbb{Q}$ est 2.

De même $P_2 = X^3 - 2$ vérifie $P_2(\sqrt[3]{2}) = 0$. Utilisons le critère d'Eisenstein pour montrer que ce polynôme à coefficients dans $\mathbb{Z}$ est irréductible dans $\mathbb{Q}[X]$. Considérons le nombre premier $p = 2$. Il divise $a_0 = -2$, $a_1 = 0$, $a_2 = 0$ mais ne divise pas $a_3 = 1$. De plus $2^2 = 4$ ne divise pas a_0 et donc ce critère montre que P_2 est irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de $\sqrt[3]{2}$. On en déduit $[\mathbb{Q}(\sqrt[3]{2}); \mathbb{Q}] = 3$.

2. Comme $\sqrt{2}$ et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, on a $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$.

$$\text{Ainsi } \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

$$\text{et } \mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \}$$

On n'a donc pas $\mathbb{Q}(\sqrt{2})$ inclus dans $\mathbb{Q}(\sqrt[3]{2})$.

3. Comme p et q sont premiers $\sqrt{p}$ et $\sqrt[3]{q}$ sont algébriques sur $\mathbb{Q}$, leur polynôme minimal étant respectivement $X^2 - p$ et $X^3 - q$. On en déduit que $[\mathbb{Q}(\sqrt{p}), \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{q}), \mathbb{Q}] = 3$. Si $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$ on obtient une tour d'extension de longueur 2 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$ et d'après le théorème de la base télescopique

$$[\mathbb{Q}(\sqrt[3]{q}); \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{q}); \mathbb{Q}(\sqrt{p})] \times [\mathbb{Q}(\sqrt{p}); \mathbb{Q}]$$

ce qui donne $[\mathbb{Q}(\sqrt[3]{q}); \mathbb{Q}(\sqrt{p})] = \frac{3}{2}$, ce qui est impossible.

donc quels que soient les nombres premiers p et q
 $\mathbb{Q}(\sqrt[p]{n})$ n'est pas inclus dans $\mathbb{Q}(\sqrt[q]{n})$.

EXERCICE 2: Trouver le polynôme minimal de $\sqrt[6]{2}$ dans $\mathbb{Q}$ et dans $\mathbb{Q}(\sqrt{2})$.

Le polynôme $P = X^6 - 2$ vérifie $P(\sqrt[6]{2}) = 0$ et $P \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$.
 On a alors $P = \sum_{i=0}^6 a_i X^i$ et le nombre premier 2 divise $a_0 = -2$,
 $a_1 = 0$, $a_2 = 0$, et $a_5 = 0$ mais 2 ne divise pas $a_6 = 1$. De plus 2
 ne divise pas a_0 . D'après le critère d'Eisenstein P est irréductible
 dans $\mathbb{Q}$. Le polynôme P est donc le polynôme minimal de
 $\sqrt[6]{2}$ (et $[\mathbb{Q}(\sqrt[6]{2}) ; \mathbb{Q}] = 6$).

Le polynôme $P = X^6 - 2 \in \mathbb{Q}(\sqrt{2})[X]$ et $P(\sqrt[6]{2}) = 0$.

Mais dans $\mathbb{Q}(\sqrt{2})[X]$ $P = (X^3 - \sqrt{2})(X^3 + \sqrt{2})$.

et $(\sqrt[6]{2})^3 - \sqrt{2} = 0$ donc $P_1 = X^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ et $P_1(\sqrt[6]{2}) = 0$

Si ce polynôme n'est pas irréductible dans $\mathbb{Q}(\sqrt{2})[X]$

$$\begin{aligned} X^3 - \sqrt{2} &= (X + a + b\sqrt{2})(X^2 + (c + d\sqrt{2})X + (e + f\sqrt{2})) \quad a, b, c, d, e, f \in \mathbb{Q} \\ &= X^3 + (c + d\sqrt{2} + a + b\sqrt{2})X^2 + [e + f\sqrt{2} + (a + b\sqrt{2})(c + d\sqrt{2})]X \\ &\quad + (a + b\sqrt{2})(e + f\sqrt{2}) \end{aligned}$$

$$\Leftrightarrow \begin{cases} c + a + (d + b)\sqrt{2} = 0 \\ (e + ac + 2bd) + (f + bc + ad)\sqrt{2} = 0 \\ (ae + 2bf) + (af + be)\sqrt{2} = -\sqrt{2} \end{cases}$$

$$\begin{aligned} \sqrt{2} \notin \mathbb{Q} &\Leftrightarrow \begin{cases} a + c = 0 \\ b + d = 0 \\ e + ac + 2bd = 0 \\ f + bc + ad = 0 \\ ae + 2bf = 0 \\ af + be = -1 \end{cases} \\ &\Leftrightarrow \begin{cases} a = -c \\ d = -b \\ -c^2 - 2b^2 + e = 0 \\ 2cb + f = 0 \\ -ce + 2bf = 0 \\ be - cf = -1 \end{cases} \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow \begin{cases} a = -c \\ d = -b \\ e = c^2 + 2b^2 \\ f = -2cb \\ -c^3 - 2cb^2 - 4b^2c = -c(c^2 + 2b^2 + 4b^2) = 0 \\ bc^2 + 2b^3 + 2c^2b = b(c^2 + 2b^2 + 2c^2) = -1 \end{cases} \end{aligned}$$

L'équation 5 implique que $c=0$. L'équation 4 devient alors $2b^3 = -1$ impossible avec $b \in \mathbb{Q}$

$$\left(-\sqrt[3]{\frac{1}{2}} \notin \mathbb{Q} \right)$$

Ainsi on a montré que $X^3 - \sqrt{2}$ était irréductible dans $\mathbb{Q}(\sqrt{2})$. C'est donc le polynôme minimal de $\sqrt[3]{2}$ dans $\mathbb{Q}(\sqrt{2})$.

Mais cette démonstration est un peu longue. En voici une autre :

Montrons d'abord que $\underbrace{\mathbb{Q}(\sqrt{2})}_{\mathbb{Q}[\sqrt{2}]} \subset \underbrace{\mathbb{Q}(\sqrt[6]{2})}_{\mathbb{Q}[\sqrt[6]{2}]}$.

$\mathbb{Q}(\sqrt{2})$ est une extension de degré 2 de $\mathbb{Q}$ puisque $X^2 - 2$ est le polynôme minimal de $\sqrt{2}$ dans $\mathbb{Q}$.

Une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(\sqrt{2})$ est donnée par $\{1, \sqrt{2}\}$. Il suffit de montrer que 1 et $\sqrt{2}$ sont dans $\mathbb{Q}(\sqrt[6]{2})$. Pour 1 c'est évident.

$$\sqrt[6]{2} \times \sqrt[6]{2} \times \sqrt[6]{2} = \sqrt[6]{8} = \sqrt[3]{\sqrt{2} \times \sqrt{2} \times \sqrt{2} \times \sqrt{2} \times \sqrt{2} \times \sqrt{2}} = \sqrt{2}$$

appartient à $\mathbb{Q}(\sqrt[6]{2})$ (puisque c'est un corps la multiplication est stable). Donc $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$

Comme $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ on a une tour d'extension de longueur 2. On a alors

$$\underbrace{[\mathbb{Q}(\sqrt[6]{2}); \mathbb{Q}]}_6 = [\mathbb{Q}(\sqrt[6]{2}); \mathbb{Q}(\sqrt{2})] \times \underbrace{[\mathbb{Q}(\sqrt{2}); \mathbb{Q}]}_2$$

On en déduit que $[\mathbb{Q}(\sqrt[6]{2}); \mathbb{Q}(\sqrt{2})] = 3$ donc le polynôme minimal de $\sqrt[6]{2}$ est de degré 3

$\Rightarrow X^3 - \sqrt{2}$ est le polynôme minimal de $\sqrt[6]{2}$

(qui est donc irréductible dans $\mathbb{Q}(\sqrt{2})$).

Une base du $(\mathbb{Q}(\sqrt{2}))$ -espace vectoriel $\mathbb{Q}(\sqrt[6]{2})$ est

$$\{1, \sqrt[6]{2}, \sqrt[6]{4}\}$$

En effet on a

$$\mathbb{Q}(\sqrt{2}, \sqrt[6]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[6]{2})(\sqrt{2})$$

puisque $\mathbb{Q}[\sqrt{2}, \sqrt[6]{2}] = \mathbb{Q}[\sqrt{2}][\sqrt[6]{2}] = \mathbb{Q}[\sqrt[6]{2}][\sqrt{2}]$

$$= \mathbb{Q}(\sqrt{2})[\sqrt[6]{2}] = \mathbb{Q}(\sqrt{2})(\sqrt[6]{2})$$

car $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ si α est algébrique sur $\mathbb{K}$.

or $\sqrt[6]{2}$ est algébrique sur $\mathbb{Q}$
et $\sqrt[6]{2}$ est algébrique sur $\mathbb{Q}$ donc sur $\mathbb{Q}(\sqrt{2})$.

de même $\mathbb{Q}[\sqrt{2}, \sqrt[6]{2}] = \mathbb{Q}[\sqrt[6]{2}][\sqrt{2}] = \mathbb{Q}(\sqrt[6]{2})[\sqrt{2}] = \mathbb{Q}(\sqrt[6]{2})(\sqrt{2})$
et puisque $\mathbb{Q}(\sqrt[6]{2})(\sqrt{2})$ est déjà un corps on a

$$\mathbb{Q}[\sqrt{2}, \sqrt[6]{2}] = \mathbb{Q}(\sqrt{2}, \sqrt[6]{2}).$$

Mais $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$ donc $\mathbb{Q}(\sqrt[6]{2})(\sqrt{2}) = \mathbb{Q}(\sqrt[6]{2})$

On a aussi $[\mathbb{Q}(\sqrt[6]{2}), \mathbb{Q}(\sqrt{2})] = 3$

donc $[\mathbb{Q}(\sqrt{2})(\sqrt[6]{2}), \mathbb{Q}(\sqrt{2})] = 3$

et puisque $\mathbb{Q}(\sqrt{2})(\sqrt[6]{2})$ est une extension algébrique monogène de $\mathbb{Q}(\sqrt{2})$ de degré 3 par l'élément $\sqrt[6]{2}$

Une base du $\mathbb{Q}(\sqrt{2})$ -espace vectoriel $\mathbb{Q}(\sqrt{2})(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[6]{2})$ est donnée par

$$\{1, \sqrt[6]{2}, (\sqrt[6]{2})^2\} = \{1, \sqrt[6]{2}, \sqrt[6]{4}\} = \{1, \sqrt[6]{2}, \sqrt[3]{2}\}.$$

On a aussi l'extension monogène de $\mathbb{Q}$ par $\sqrt{2}$ $\mathbb{Q}(\sqrt{2})$ qui est une extension de degré 2 par l'élément $\sqrt{2}$ et une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(\sqrt{2})$ est donnée par $\{1, \sqrt{2}\}$.

On sait alors que le $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(\sqrt{2})(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[6]{2})$ est donnée par

$$\{1, \sqrt[6]{2}, \sqrt[6]{4}, 1 \times \sqrt{2}, \sqrt[6]{2} \times \sqrt{2}, \sqrt[6]{4} \times \sqrt{2}\}$$
$$= \{1, \sqrt[6]{2}, \sqrt[6]{4}, \sqrt[6]{8}, \sqrt[6]{16}, \sqrt[6]{32}\}$$

Ainsi tout élément de $\mathbb{Q}(\sqrt[6]{2})$ s'écrit

$$\alpha + \beta \sqrt[6]{2} + \gamma \sqrt[6]{4} \quad \text{avec } \alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{2})$$

où encore $a + b\sqrt{2} + c\sqrt[6]{2} + d\sqrt[6]{2}\sqrt[6]{2} + e\sqrt[6]{4} + f\sqrt[6]{2}\sqrt[6]{4}$

$$a, b, c, d, e, f \in \mathbb{Q}.$$

$$a + c\sqrt[6]{2} + e\sqrt[6]{4} + b\sqrt[6]{8} + d\sqrt[6]{16} + f\sqrt[6]{32}$$

EXERCICE 3 : Déterminer le degré des extensions de $\mathbb{Q}$ suivantes et en trouver une base.

1) $\mathbb{Q}(j)$ 2) $\mathbb{Q}(\cos \frac{2\pi}{3})$ 3) $\mathbb{Q}(\sin \frac{2\pi}{3})$

4) $\mathbb{Q}(\cos \frac{2\pi}{5})$, $\mathbb{Q}(e^{\frac{2i\pi}{5}})$, $\mathbb{Q}(\sqrt{5})$. Quels sont les liens entre ces 3 corps ?

1) On sait que $j^2 + j + 1 = 0$ donc le polynôme $p = 1 + X + X^2$ est un multiple du polynôme minimal de j sur $\mathbb{Q}$.
Or $X^2 + X + 1$ n'a pas de racine réelle ($\Delta = 1 - 4 < 0$) donc pas de racine dans $\mathbb{Q}$. Il est donc irréductible dans $\mathbb{Q}$. Ainsi $[\mathbb{Q}(j); \mathbb{Q}] = 2$.
Une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(j)$ est donnée par $\{1, j\}$.

2) On a $\cos \frac{2\pi}{3} = -\frac{1}{2} \in \mathbb{Q}$ donc $\mathbb{Q}(\cos \frac{2\pi}{3}) = \mathbb{Q}(-\frac{1}{2}) = \mathbb{Q}$.

3) On a $\sin \frac{2\pi}{3} = \frac{\sqrt{3}}{2}$. donc $\mathbb{Q}(\sin \frac{2\pi}{3}) = \mathbb{Q}(\frac{\sqrt{3}}{2}) = \mathbb{Q}(\sqrt{3})$

Le polynôme minimal de $\sqrt{3}$ dans $\mathbb{Q}$ est $X^2 - 3$ puisque $(\sqrt{3})^2 - 3 = 0$ et c'est un polynôme irréductible dans $\mathbb{Q}$.
Donc $[\mathbb{Q}(\sqrt{3}); \mathbb{Q}] = 2$ et une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(\sqrt{3})$ est donnée par $\{1, \sqrt{3}\}$.
(tout élément de $\mathbb{Q}(\sqrt{3})$ s'écrit $a + b\sqrt{3}$ avec $a, b \in \mathbb{Q}$)

4) Soit $\zeta = e^{\frac{2i\pi}{5}}$. cette racine 5 ième de l'unité ($\zeta^5 = 1$) est non rationnelle

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Le polynôme $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{Q}$.

En effet si on pose $X = Y + 1$ on obtient

$$(Y+1)^4 + (Y+1)^3 + (Y+1)^2 + (Y+1) + 1 = \frac{(Y+1)^5 - 1}{Y+1 - 1}$$

$$= \frac{(Y+1)^5 - 1}{Y} = \frac{\sum_{k=0}^5 C_5^k Y^k}{Y} = \sum_{k=1}^5 C_5^k Y^{k-1} = \sum_{i=0}^4 a_i Y^i$$

Or C_5^k est divisible par 5 pour $k=1,2,3,4$

Donc le nombre premier 5 divise $a_0 = C_5^1$; $\dots$; $a_i = C_5^{i+1}$; $\dots$; $a_4 = C_5^5$
ne divise pas $a_4 = C_5^5 = 1$ et $5^2 = 25$ ne divise pas $a_0 = 5$.

D'après le critère d'Eisenstein le polynôme

$$X^4 + X^3 + X^2 + X + 1 = \sum_{i=0}^4 a_i Y^i \text{ est irréductible dans } \mathbb{Q}$$

Donc $[\mathbb{Q}(\zeta); \mathbb{Q}] = 4$.

Or $\zeta = e^{\frac{2i\pi}{5}} = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$ et $\bar{\zeta} = \cos \frac{2\pi}{5} - i \sin \frac{2\pi}{5} = \zeta^4$

donc $2 \cos \frac{2\pi}{5} = \zeta + \zeta^4 = a$

On a $a^2 = \zeta^2 + \zeta^3 + 2 = -a + 1$ puisque $\zeta^2 + \zeta^3 + 1 = -\zeta - \zeta^4 = -a$

donc $X^2 + X - 1 = P_2$ vérifie $P_2(a) = 0$ et de plus
c'est un polynôme irréductible dans $\mathbb{Q}$: $\Delta = 1 + 4 = 5$

donc les racines de P_2 sont $\frac{-1-\sqrt{5}}{2}$ et $\frac{-1+\sqrt{5}}{2}$.

On a aussi $\cos \frac{2\pi}{5} > 0$ donc $a = 2 \cos \frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2} \notin \mathbb{Q}$

et $\cos \frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$. Ainsi $\cos \frac{2\pi}{5} \in \mathbb{Q}(\sqrt{5}) = \mathbb{Q}[\sqrt{5}]$.

et on aura $\mathbb{Q} \subset \mathbb{Q}(\cos \frac{2\pi}{5}) \subset \mathbb{Q}(\sqrt{5})$.

On sait aussi que $[\underbrace{\mathbb{Q}(\sqrt{5}); \mathbb{Q}}_2] = [\mathbb{Q}(\sqrt{5}); \underbrace{\mathbb{Q}(\cos \frac{2\pi}{5})}_2] \times [\underbrace{\mathbb{Q}(\cos \frac{2\pi}{5}); \mathbb{Q}}_2]$

ainsi $[\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\cos \frac{2\pi}{5})] = 1$ ($\mathbb{Q}(a) = \mathbb{Q}(\frac{a}{2})$)

donc $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\cos \frac{2\pi}{5})$.

De plus $2 \cos \frac{2\pi}{5} = \zeta + \zeta^4$ donc $\mathbb{Q}(\cos \frac{2\pi}{5}) \subset \mathbb{Q}(\zeta)$.

et on a $[\underbrace{\mathbb{Q}(\zeta); \mathbb{Q}}_4] = [\mathbb{Q}(\zeta), \underbrace{\mathbb{Q}(\cos \frac{2\pi}{5})}_2] \times [\underbrace{\mathbb{Q}(\cos \frac{2\pi}{5}); \mathbb{Q}}_2]$

$\Rightarrow [\mathbb{Q}(\zeta), \mathbb{Q}(\cos \frac{2\pi}{5})] = 2$

EXERCICE 4 : Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Soit $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. Si $P_\alpha \in \mathbb{K}[x]$ est le polynôme minimal de α , montrer que toutes les racines de P_α dans $\mathbb{L}$ admettent P_α comme polynôme minimal.

Soit $\beta \in \mathbb{L}$ telle que $P_\alpha(\beta) = 0$. Ainsi β est algébrique sur $\mathbb{K}$ et P_α est un polynôme annulateur.

Soit $I = \{P \in \mathbb{K}[x] / P(\beta) = 0\}$. Cet idéal est principal. Il admet un unique générateur unitaire P_β , le polynôme minimal de β . Comme $P_\alpha \in I$, α admet P_β comme diviseur. Mais P_α est irréductible sur $\mathbb{K}$, donc $P_\alpha = P_\beta$.

EXERCICE 5 : Soit $\mathbb{K} \subset \mathbb{C}$ une extension de $\mathbb{K}$ par $\mathbb{C}$. Soit $\alpha \in \mathbb{C}$ un élément algébrique sur $\mathbb{K}$. Montrer que α est racine simple de son polynôme minimal P_α .

Supposons que $P_\alpha(x) = (x - \alpha)^k Q(x)$ avec $Q(\alpha) \neq 0$ et $k > 1$. Alors $P'_\alpha(x) = k(x - \alpha)^{k-1} Q(x) + (x - \alpha)^k Q'(x)$

$$= (x - \alpha)^{k-1} [k Q(x) + Q'(x)].$$

On en déduit que $P'_\alpha(\alpha) = 0$. Ainsi P'_α admet α pour racine. Comme $d \vdash P'_\alpha \leq d \vdash P_\alpha$, ceci contredit la définition du polynôme minimal P_α . Donc α est racine simple de P_α .

EXERCICE 6 : Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. Soit $P_\alpha \in \mathbb{K}[x]$ le polynôme minimal de α . Montrer que l'extension $\mathbb{K}(\alpha)$ sur $\mathbb{K}$ est isomorphe au corps de rupture de P_α .

Comme P_α est irréductible, le corps de rupture est $\frac{\mathbb{K}[x]}{(P_\alpha)}$ où (P_α) est l'idéal maximal engendré par le polynôme P_α . Considérons l'application $\varphi: \mathbb{K}[x] \rightarrow \mathbb{K}(\alpha)$ définie par $\varphi(a_0 + \dots + a_m x^m) = a_0 + a_1 \alpha + \dots + a_m \alpha^m$.

Rappelons que comme α est algébrique $\mathbb{R}[\alpha] = \mathbb{R}(\alpha)$.
 Il est clair que φ est un homomorphisme surjectif d'anneaux.
 Son noyau est formé des polynômes $P \in \mathbb{R}[x]$ tel que $P(\alpha) = 0$.
 Ainsi $\text{Ker } \varphi = (P_\alpha)$. Ainsi φ se factorise en un isomor-

$$\begin{array}{ccc} \mathbb{R}[x] & \xrightarrow{\varphi} & \mathbb{R}[\alpha] \\ \downarrow & & \nearrow \tilde{\varphi} \\ \mathbb{R}[x] / \text{Ker } \varphi & & \end{array}$$

Comme $\mathbb{R}[x] / \text{Ker } \varphi$ et $\mathbb{R}[\alpha]$ sont des corps, $\tilde{\varphi}$ est un isomorphisme de corps.