125 — **Extensions de corps. Exemples et applications.**

Not 1 : $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ sont des corps. $car(\mathbb{K})$ est la caractéristique de $\mathbb{K}$.

I) Généralités.

1) Définitions et premières propriétés.

Déf 2 : Une extension du corps $\mathbb{K}$ est la donnée d'un corps $\mathbb{L}$ et d'un morphisme de corps $\varphi : \mathbb{K} \to \mathbb{L}$. On identifiera souvent $\mathbb{K}$ à $\varphi(\mathbb{K})$ et on le verra donc comme un sous-corps de $\mathbb{L}$.

Rq 3 : Si p est premier, $\left\{\begin{array}{l} \mathbb{Z}/p\mathbb{Z}(X) \to \mathbb{Z}/p\mathbb{Z}(X) \\ x \mapsto x^p \end{array}\right.$ est un morphisme de corps non surjectif.

Déf 4 : $\mathbb{L}$ est une sous-extension de $\mathbb{K} \subset \mathbb{M}$ si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$.
Si $\mathbb{K} \subset \mathbb{M}$ et $S \subset \mathbb{M}$ alors $\mathbb{K}(S)$ est le plus petit sous-corps de $\mathbb{M}$ contenant $\mathbb{K}$ et S. Si $S = \{x_1, \dots, x_n\}$ on note $\mathbb{K}(x_1, \dots, x_n) = \mathbb{K}(S)$.

Déf 5 : Le degré de l'extension $\mathbb{K} \subset \mathbb{L}$ est la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel et est noté $[\mathbb{L} : \mathbb{K}]$. On dit que $\mathbb{K} \subset \mathbb{L}$ est une extension finie si $[\mathbb{L} : \mathbb{K}] < +\infty$.

Ex 6 : $\mathbb{K} \subset \mathbb{K}(X)$ est une extension de degré infini ($\{X^n, n \in \mathbb{N}\}$ libre).
$\mathbb{Q} \subset \mathbb{R}$ est une extension de degré infini ($\mathbb{Q}$ dénombrable, $\mathbb{R}$ non).
$\mathbb{R} \subset \mathbb{C}$ est une extension de degré 2 ($\mathbb{C} = \{a + ib, a, b \in \mathbb{R}\}$, $i \notin \mathbb{R}$).
$\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$ est une extension de degré 2.

Déf 7 : Le sous-corps premier de $\mathbb{K}$ est le plus petit sous-corps de $\mathbb{K}$.

Prop 8 : (i) Si $car(\mathbb{K}) = 0$ alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.
(ii) Si $car(\mathbb{K}) = p > 0$ alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Ex 9 : Si $\mathbb{K}$ est un corps fini alors $\mathbb{K}$ est de caractéristique un nombre premier p et $|\mathbb{K}| = p^n$ pour un certain $n \in \mathbb{N}^*$.

Thm 10 (de la base télescopique) : Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ sont des corps tels que $(e_1, \dots, e_n)$ est une $\mathbb{K}$-base de $\mathbb{L}$ et $(f_1, \dots, f_m)$ est une $\mathbb{L}$-base de $\mathbb{M}$ alors $(e_i f_j)_{i \in \{1, \dots, n\}, j \in \{1, \dots, m\}}$ est une $\mathbb{K}$-base de $\mathbb{M}$.

Cor 11 (multiplicativité des degrés) : Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ alors :
$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$ (convention : $n \times +\infty = +\infty \times n = +\infty$).

2) Extensions algébriques.

Déf 12 : Soient $\mathbb{K} \subset \mathbb{L}$. $x \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X] \setminus \{0\}$ tel que $P(x) = 0$. Il existe alors un unique $\Pi_{\mathbb{K},x} \in \mathbb{K}[X]$ unitaire tel que l'idéal de $\mathbb{K}[X]$ engendré par $\Pi_{\mathbb{K},x}$ est $\{P \in \mathbb{K}[X], P(x) = 0\}$; on l'appelle le polynôme minimal de x sur $\mathbb{K}$.
Si x n'est pas algébrique sur $\mathbb{K}$ on dit qu'il est transcendant sur $\mathbb{K}$.

Rq 13 : $\Pi_{\mathbb{K},x}$ est irréductible sur $\mathbb{K}$.

Déf 14 : $\mathbb{K} \subset \mathbb{L}$ est une extension algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Thm 15 : Toute extension finie est algébrique.

Thm 16 : Soit $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Notons n le degré de $\Pi_{\mathbb{K},x}$.
(i) $\mathbb{K}(x)$ est isomorphe au corps $\mathbb{K}[X]/(\Pi_{\mathbb{K},x})$.
(ii) $(1, x, \dots, x^{n-1})$ est une $\mathbb{K}$-base de $\mathbb{K}(x)$.
(iii) Soit $y \in \mathbb{K}(x)$. y est algébrique sur $\mathbb{K}$ et le degré de $\Pi_{\mathbb{K},y}$ divise n.

App 17 : Si $x \in \mathbb{L} \setminus \{0\}$ est algébrique sur $\mathbb{K}$ alors $-x$ et x^{-1} le sont.

Prop 18 : Si $x \in \mathbb{L}$ est transcendant sur $\mathbb{K}$ alors $\mathbb{K}(x)$ est isomorphe à $\mathbb{K}(X)$ en tant que $\mathbb{K}$-algèbres. En particulier $[\mathbb{K}(x) : \mathbb{K}] = +\infty$.

App 19 : Si $x, y \in \mathbb{L}$ sont algébriques sur $\mathbb{K}$ alors $x + y$ et xy le sont.

Ex 20 : Soient $n \in \mathbb{N}^*$ et p un nombre premier. $\sqrt[n]{p}$ est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. i et j sont algébriques sur $\mathbb{Q}$ et $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [\mathbb{Q}(j) : \mathbb{Q}]$.
e et π sont transcendants sur $\mathbb{Q}$.

Prop 21 : Si $\mathbb{K} \subset \mathbb{L}$ et $\mathbb{L} \subset \mathbb{M}$ sont algébriques alors $\mathbb{K} \subset \mathbb{M}$ est algébrique.

Prop 22 : $\mathbb{K} \subset \mathbb{L}$ est une extension finie ssi il existe $n \in \mathbb{N}^*$, $x_1, \dots, x_n \in \mathbb{L}$ algébriques sur $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$.

Déf 23 : $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$ qui est algébriquement close.

Prop 24 : Si $\mathbb{L}$ est une extension algébriquement close de $\mathbb{K}$ alors $\{x \in \mathbb{L}, x \text{ est algébrique sur } \mathbb{K}\}$ est une clôture algébrique de $\mathbb{K}$.

Ex 25 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
$\overline{\mathbb{Q}} := \{x \in \mathbb{C}, x \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

Rq 26 : $[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$ car, en notant $\{p_n, n \in \mathbb{N}^*\}$ les nombres premiers, $\mathbb{Q}(\{\sqrt{p_n}, n \in \mathbb{N}^*\})$ est une sous-extension de $\mathbb{Q} \subset \overline{\mathbb{Q}}$ de degré infini sur $\mathbb{Q}$.

II) Corps de rupture, corps de décomposition et applications.

1) Définitions et premières propriétés.

Déf 27 : Soit $P \in \mathbb{K}[X]$ irréductible. $\mathbb{L}$ est un corps de rupture de P sur $\mathbb{K}$ s'il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(x)$ et $P(x) = 0$.

Prop 28 : Soit $P \in \mathbb{K}[X]$ irréductible.
(i) $\mathbb{K}[X]/(P)$ est un corps de rupture de P sur $\mathbb{K}$.
(ii) Deux corps de rupture de P sur $\mathbb{K}$ sont isomorphes en tant que $\mathbb{K}$-algèbres.

Ex 29 : $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.
$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$.

Déf 30 : Soit $P\in\mathbb{K}[X]$ de degré $n\geq 1$. $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ s'il existe $x_1,\dots,x_n\in\mathbb{L}$, $c\in\mathbb{K}$ tels que $\mathbb{L}=\mathbb{K}(x_1,\dots,x_n)$ et dans $\mathbb{L}[X]$ $P=c\prod_{i=1}^{n}(X-x_i)$.

Prop 31 : Soit $P\in\mathbb{K}[X]$ de degré $n\geq 1$.
(i) P admet un corps de décomposition sur $\mathbb{K}$.
(ii) Deux corps de décomposition de P sur $\mathbb{K}$ sont isomorphes en tant que $\mathbb{K}$-algèbres.

Ex 32 : $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$. $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

② Applications aux corps finis.

Lemme 33 : Soit p un nombre premier. Soit $n\in\mathbb{N}^*$. Dans $\mathbb{Z}/p\mathbb{Z}[X]$ $X^{p^n}-X$ est le produit des polynômes irréductibles unitaires de $\mathbb{Z}/p\mathbb{Z}[X]$ de degré divisant n.

Lemme 34 : Soit p un nombre premier. Pour tout $n\in\mathbb{N}^*$ il existe un polynôme irréductible unitaire de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Thm 35 : Soit p un nombre premier. Soit $n\in\mathbb{N}^*$. Il existe un corps de cardinal p^n, unique à isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-algèbres près. C'est un corps de décomposition de $X^{p^n}-X$ sur $\mathbb{Z}/p\mathbb{Z}$. On note un tel corps $\mathbb{F}_{p^n}$.

Thm 36 : Soient p un nombre premier, $n\in\mathbb{N}^*$, m un diviseur de n. $\mathbb{F}_{p^n}$ a un unique sous-corps de cardinal p^m. Réciproquement, tout sous-corps de $\mathbb{F}_{p^n}$ a un cardinal de la forme p^d avec d un diviseur de n.

DEV 1

Rq 37 : Si $P\in\mathbb{Z}/p\mathbb{Z}[X]$ est un polynôme irréductible alors tout corps de rupture de P sur $\mathbb{Z}/p\mathbb{Z}$ est un corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$.

Ex 38 : $\mathbb{F}_4=\mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$, $\mathbb{F}_8=\mathbb{Z}/2\mathbb{Z}[X]/(X^3+X+1)$, $\mathbb{F}_{16}=\mathbb{Z}/2\mathbb{Z}[X]/(X^4+X+1)$, $\mathbb{F}_9=\mathbb{Z}/3\mathbb{Z}[X]/(X^2-X-1)$.

Ex 39 : $\mathbb{F}_5$ et $\mathbb{F}_{125}$ sont les sous-corps de $\mathbb{F}_{125}$. $\mathbb{F}_5$, $\mathbb{F}_{25}$ et $\mathbb{F}_{625}$ sont les sous-corps de $\mathbb{F}_{625}$.

Thm 40 : Soit p un nombre premier. Soit $n\in\mathbb{N}^*$. $\bigcup_{k\in\mathbb{N}^*}\mathbb{F}_{p^{k!}}$ est une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$.

③ Applications à l'irréductibilité.

Prop 41 : Soit $P\in\mathbb{K}[X]$ de degré $n\geq 1$. P est irréductible ssi pour toute extension $\mathbb{L}$ de $\mathbb{K}$ vérifiant $2\leq[\mathbb{L}:\mathbb{K}]\leq n$, P n'a aucune racine dans $\mathbb{L}$.

App 42 : $X^4+X+1\in\mathbb{Z}/2\mathbb{Z}[X]$ est irréductible car il n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$ ni dans $\mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$.

Prop 43 : Soit $P\in\mathbb{K}[X]$ irréductible de degré n. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré m premier avec n alors P est irréductible dans $\mathbb{L}[X]$.

C-Ex 44 : $X^4+1\in\mathbb{Q}[X]$ est irréductible et $X^4+1=(X^2-i)(X^2+i)$ dans $\mathbb{Q}(i)[X]$.

App 45 : $X^4+1\in\mathbb{Q}[X]$ est irréductible et $3\wedge 4=1$ donc X^4+1 est irréductible dans $\mathbb{Q}(\sqrt[3]{2})[X]$.

④ Applications aux clôtures algébriques.

Thm 46 : Tout corps admet une extension algébriquement close.

Ex 47 : Tout corps admet une clôture algébrique.

Thm 48 : Deux clôtures algébriques de $\mathbb{K}$ sont isomorphes en tant que $\mathbb{K}$-algèbres.

III Extensions normales, séparables, galoisiennes.

① Définitions et premières propriétés.

Déf 49 : L'extension $\mathbb{K}\subset\mathbb{L}$ est normale si elle est algébrique et si tout polynôme irréductible de $\mathbb{K}[X]$ qui admet une racine dans $\mathbb{L}$ est scindé dans $\mathbb{L}[X]$.
· $x\in\mathbb{L}$ est séparable s'il est algébrique sur $\mathbb{K}$ et si son polynôme minimal sur $\mathbb{K}$ est à racines simples dans un de ses corps de décomposition sur $\mathbb{K}$. L'extension $\mathbb{K}\subset\mathbb{L}$ est séparable si tout élément de $\mathbb{L}$ est séparable sur $\mathbb{K}$.
· Un corps est parfait si toutes ses extensions algébriques sont séparables.
· Une extension est galoisienne si elle est normale et séparable.

Ex 50 : Toute extension algébrique de $\mathbb{Z}/p\mathbb{Z}$ est normale (cf. Rq 37).
Les clôtures algébriques sont normales.
Les corps de caractéristique nulle sont parfaits.
$\mathbb{Q}\subset\overline{\mathbb{Q}}$ et $\mathbb{R}\subset\mathbb{C}$ sont galoisiennes.

C-Ex 51 : $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})$ n'est pas normale.

Thm 52 : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie. $\mathbb{K}\subset\mathbb{L}$ est normale ssi $\mathbb{L}$ est un corps de décomposition d'un polynôme de $\mathbb{K}[X]$ sur $\mathbb{K}$.

Thm 53 (de l'élément primitif) : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie séparable. Il existe $x\in\mathbb{L}$ tel que $\mathbb{L}=\mathbb{K}(x)$.

Ex 54 : $\mathbb{Q}(\sqrt[3]{2},j)=\mathbb{Q}(\sqrt[3]{2}+j)$, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Not 55 : Soient $\mathbb{L}$ et $\mathbb{M}$ des surcorps de $\mathbb{K}$. $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{M})$ est l'ensemble des morphismes de $\mathbb{K}$-algèbres de $\mathbb{L}$ dans $\mathbb{M}$.

Thm 56 : Soient $\mathbb{K}\subset\mathbb{L}$ une extension finie et Ω une clôture algébrique de $\mathbb{K}$. $1\leq|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)|\leq[\mathbb{L}:\mathbb{K}]$ et il y a équivalence entre :
(i) $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)|=[\mathbb{L}:\mathbb{K}]$
(ii) $\exists\, n\in\mathbb{N}^*, x_1,\dots,x_n\in\mathbb{L}$ séparables sur $\mathbb{K}$ $\mathbb{L}=\mathbb{K}(x_1,\dots,x_n)$
(iii) $\mathbb{K}\subset\mathbb{L}$ est séparable.

Thm 57 : Soient p un nombre premier et $\mathbb{K}$ un corps de caractéristique p. $\mathbb{K}$ est parfait ssi le morphisme de Frobenius $\begin{cases}\mathbb{K}\to\mathbb{K}\\ x\mapsto x^p\end{cases}$ est surjectif.

App 58 : Les corps finis sont parfaits. $\mathbb{Z}/p\mathbb{Z}(X)$ n'est pas parfait.

② Théorie de Galois.

Def 59 : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie. Le groupe de Galois de $\mathbb{K}\subset\mathbb{L}$ est le groupe des automorphismes de $\mathbb{K}$-algèbre de $\mathbb{L}$ et est noté $\mathrm{Gal}(\mathbb{K},\mathbb{L})$.

Prop 60 : Soient $\mathbb{K}\subset\mathbb{L}$ une extension finie, $\sigma\in\mathrm{Gal}(\mathbb{K},\mathbb{L})$, $n\in\mathbb{N}^*$, $P\in\mathbb{K}[X_1,\dots,X_n]$. Pour tous $x_1,\dots,x_n\in\mathbb{L}$ $\sigma(P(x_1,\dots,x_n))=P(\sigma(x_1),\dots,\sigma(x_n))$.

App 61 : $\mathrm{Gal}(\mathbb{R},\mathbb{C})$ a deux éléments : l'identité et la conjugaison. $\mathrm{Gal}(\mathbb{Q},\mathbb{Q}(\sqrt[3]{2}))$ n'a qu'un élément : l'identité.

Prop 62 : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie. $|\mathrm{Gal}(\mathbb{K},\mathbb{L})|\leq[\mathbb{L}:\mathbb{K}]$.

Thm 63 : Soient $\mathbb{K}\subset\mathbb{L}$ une extension finie et Ω une clôture algébrique de $\mathbb{L}$. Il y a équivalence entre :
(i) $\mathbb{K}\subset\mathbb{L}$ est galoisienne
(ii) $|\mathrm{Gal}(\mathbb{K},\mathbb{L})|=[\mathbb{L}:\mathbb{K}]$
(iii) $\mathbb{K}\subset\mathbb{L}$ est séparable et $\mathrm{Gal}(\mathbb{K},\mathbb{L})=\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$.

App 64 : $\mathrm{Gal}(\mathbb{Q},\mathbb{Q}(\sqrt[3]{2},j))$ est isomorphe à $\mathfrak{S}_3$.

Not 65 : Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $\mathbb{L}^G=\{x\in\mathbb{L}, \forall\sigma\in G\ \sigma(x)=x\}$.

Prop 66 : Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $\mathbb{L}^G$ est un sous-corps de $\mathbb{L}$.

Thm 67 (d'Artin) : Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $|G|=[\mathbb{L}:\mathbb{L}^G]$.

Ex 68 : $\mathbb{L}^G\subset\mathbb{L}$ est une extension finie galoisienne de groupe de Galois G.

DÉV 2

Not 69 : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie. $\mathcal{K}(\mathbb{K},\mathbb{L})$ est l'ensemble des sous-extensions de $\mathbb{K}\subset\mathbb{L}$ et $\mathcal{G}(\mathbb{K},\mathbb{L})$ est l'ensemble des sous-groupes de $\mathrm{Gal}(\mathbb{K},\mathbb{L})$.

Prop 70 : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie. $\begin{cases}\mathcal{K}(\mathbb{K},\mathbb{L})\to\mathcal{G}(\mathbb{K},\mathbb{L})\\ \mathbb{M}\mapsto\mathrm{Gal}(\mathbb{M},\mathbb{L})\end{cases}$ et $\begin{cases}\mathcal{G}(\mathbb{K},\mathbb{L})\to\mathcal{K}(\mathbb{K},\mathbb{L})\\ H\mapsto\mathbb{L}^H\end{cases}$ sont bien définies et renversent les inclusions.

Thm 71 (correspondance de Galois) : Soit $\mathbb{K}\subset\mathbb{L}$ une extension finie galoisienne. $\begin{cases}\mathcal{K}(\mathbb{K},\mathbb{L})\to\mathcal{G}(\mathbb{K},\mathbb{L})\\ \mathbb{M}\mapsto\mathrm{Gal}(\mathbb{M},\mathbb{L})\end{cases}$ et $\begin{cases}\mathcal{G}(\mathbb{K},\mathbb{L})\to\mathcal{K}(\mathbb{K},\mathbb{L})\\ H\mapsto\mathbb{L}^H\end{cases}$ sont des bijections réciproques l'une de l'autre. De plus, pour tout $\mathbb{M}\in\mathcal{K}(\mathbb{K},\mathbb{L})$, $\mathrm{Gal}(\mathbb{M},\mathbb{L})$ est distingué dans $\mathrm{Gal}(\mathbb{K},\mathbb{L})$ ssi $\mathbb{K}\subset\mathbb{M}$ est galoisienne, et on a alors $\mathrm{Gal}(\mathbb{K},\mathbb{M})$ isomorphe à $\mathrm{Gal}(\mathbb{K},\mathbb{L})/\mathrm{Gal}(\mathbb{M},\mathbb{L})$.

App 72 : Le groupe de Galois de l'extension finie galoisienne $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2},j)$ est isomorphe à $\mathfrak{S}_3$ donc $\mathbb{Q}$, $\mathbb{Q}(j)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$, $\mathbb{Q}(j^2\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2},j)$ sont les seules sous-extensions de $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2},j)$ et on retrouve que $\mathbb{Q}\subset\mathbb{Q}(j)$ est galoisienne et que $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}\subset\mathbb{Q}(j\sqrt[3]{2})$, $\mathbb{Q}\subset\mathbb{Q}(j^2\sqrt[3]{2})$ ne le sont pas.

Bibliographie :

Calais, Extensions de corps.

Chambert-Loir, Algèbre corporelle.

Cox, Galois Theory, Second Edition.

Lidl, Niederreiter, Introduction to finite fields and their applications, Revised Edition.

Perrin, Cours d'algèbre.