

Maths : DM ⅃Ⅹ

Il est important avant de commencer lire ce DM
d’avoir bien compris le tableau et les exemples suivants

symbole usuel	symbole du DM	prononciation
0	ƒ	fé
1	⅃	ur
2	ƚ	tur
3	ƒ	an
4	ℜ	rai
5	<	kau
6	Ⅹ	gèb
7	ƚ	wun
8	Ⅱ	hag
9	ƚ	nau
10	↷	je
11	↵	ei
=	Ⅹ	ing/i ng
+	↑	ti
−	Υ	al
×	Ⅹ	dag
÷	↑	lag
∈	ℷ	so
∀	ℷ	per
∃	ℷ	ber
∃!	!ℷ	\
>	Ⅱ	man
<	Ⅱ	e
≥	ⅡⅩ	maning
≤	ⅡⅩ	ehwing
≠	◇	naing
⊂	ƚ	suz
⊃	ƚ	zus

$X \uparrow < < \text{Ⅹ} \cap \text{Ⅹ}$ ce qui est équivalent à $79 + 65 = 144$

$$e^{\text{Ⅹ}} \text{Ⅹ} \cap \uparrow \text{Ⅹ} \uparrow \frac{\text{Ⅹ}}{\text{Ⅹ}} \uparrow \dots \uparrow \frac{\text{Ⅹ}}{\text{Ⅹ}} \uparrow o(\text{Ⅹ})$$

est équivalent à

$$e^x \stackrel{x \rightarrow 0}{=} 1 + x + \frac{x^2}{2} + \dots + \frac{x^n}{x!} + o(x^n)$$

Problème 1 : nombres algébrique et extensions de corps

Partie I. extensions de corps

N° 1. Premiers exemples a.

il est évident que \mathbb{R} est un sous-corps de \mathbb{C} et de plus \mathbb{C} est de dimension finie, donc \mathbb{C} est une extension finie de \mathbb{R}

de plus soit $\alpha \in \mathbb{C}$ alors

$$\lambda \alpha, \mu \in \mathbb{R}, \alpha \neq 0 \Rightarrow \lambda \mu \alpha \in \mathbb{R} \Leftrightarrow \alpha \in \text{Vect}(\mathbb{R}, i)$$

Ainsi comme \mathbb{R} et i ne sont pas colinéaire dans \mathbb{R} , $\text{Vect}(\mathbb{R}, i)$ forme une base de \mathbb{C}

Ainsi $[\mathbb{C} : \mathbb{R}] = 2$

soit \mathbb{K} un sous-corps qui contient \mathbb{R}

comme $[\mathbb{R} : \mathbb{R}] = 1$ et que l'on vient de prouver que $[\mathbb{C} : \mathbb{R}] = 2$

il apparaît donc comme condition que, $[\mathbb{K} : \mathbb{R}] = 2$

Ainsi $[\mathbb{K} : \mathbb{R}] = 1$ ou $[\mathbb{K} : \mathbb{R}] = 2$

Et ainsi $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$

b.

Soit $\alpha \in \mathbb{Q}(\sqrt{p})$, alors $\exists \lambda, \mu \in \mathbb{Q}, \alpha = \lambda + \mu \sqrt{p}$, alors prenons $\alpha \neq 0$

ainsi $\alpha \neq 0 \Rightarrow \lambda \neq 0$, donc $\frac{\alpha}{\lambda} \in \mathbb{Q}(\sqrt{p})$ et comme \mathbb{Q} est un corps

de $\mathbb{Q}(\sqrt{p})$

de plus, soit $\alpha \in \mathbb{Q}(\sqrt{p})$ alors $\exists \lambda, \mu \in \mathbb{Q}, \alpha = \lambda + \mu \sqrt{p}$, soit un tel λ, μ

donc $\alpha \neq 0 \Rightarrow \lambda \neq 0$ et $\frac{\alpha}{\lambda} \in \mathbb{Q}(\sqrt{p})$

et supposons par l'absurde $\exists \lambda, \mu \in \mathbb{Q}, \alpha = \lambda + \mu \sqrt{p} \notin \mathbb{Q}$

alors $\frac{\alpha}{\lambda} \notin \mathbb{Q}$ ce qui est absurde car $\frac{\alpha}{\lambda} \in \mathbb{Q}$, donc $\alpha \in \mathbb{Q}$

Ainsi (\mathbb{R}, \sqrt{p}) est une base de $\mathbb{Q}(\sqrt{p})$

Donc $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$

c. i.

Soit $P \in \mathbb{Q}[X]$ tel que $P(\sqrt[p]{a}) \neq 0$

prenons la division euclidienne de X^p par P

ce qui nous donne $X^p = PQ + R$ avec $Q \in \mathbb{Q}[X]$ et $R \in \mathbb{Q}[X]$ tel que $\deg R < \deg P$

En évaluant notre expression précédente en $\sqrt[p]{a}$ on obtient :

$$\underbrace{\left(\sqrt[p]{a}\right)^p}_{=a} = P\left(\sqrt[p]{a}\right) + R\left(\sqrt[p]{a}\right)$$

donc $R = 0$ et donc $\deg R = 0$

ainsi P divise X^p

Ainsi Comme P divise X^p et que $\deg P < p$,

alors P et X^p possède deux racines en commun dont $\sqrt[p]{a}$

et comme $X^p = (X - \sqrt[p]{a})(X - \sqrt[p]{a}e^{i\frac{2\pi}{p}})(X - \sqrt[p]{a}e^{i\frac{4\pi}{p}})\dots(X - \sqrt[p]{a}e^{i\frac{(p-1)2\pi}{p}})$ donc P a en plus une racine complexe ou un polynôme dans \mathbb{R} qui possède une racine complexe possède sont conjuguée

ce qui n'est pas le cas pour P donc $P \not\subset \mathbb{Q}[X]$ ce qui est absurde
Donc $P \subset \mathbb{Q}[X]$, $P(\sqrt[p]{p}) \not\subset \mathbb{Q}$

ii.

Par un raisonnement analogue à la question 1.b on montre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt[p]{p})$,
De plus soit $\mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$ alors soient $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}'' \subset \mathbb{Q}, \mathfrak{A} \not\subset \mathfrak{A}' \subset \mathfrak{A}'' \subset \mathbb{Q}(\sqrt[p]{p})$
donc $\mathfrak{A} \subset \text{Vect}(\mathbb{Q}, \sqrt[p]{p}, \sqrt[p]{p}^2)$
donc $\mathbb{Q}(\sqrt[p]{p})$ est une extensions finis et $[\mathbb{Q}(\sqrt[p]{p}) : \mathbb{Q}] \not\equiv 1$

d.

Soient $\mathfrak{A}_1, \dots, \mathfrak{A}_n \subset \mathbb{Q}$ tels que $\sum_{\mathfrak{A} \in \mathfrak{A}_i} \mathfrak{A}_i \ln(p_i) \not\subset \mathbb{Q}$,
alors

$$\ln \left(\prod_{\mathfrak{A} \in \mathfrak{A}_i} p_i^{\mathfrak{A}_i} \right) \not\subset \mathbb{Q} \text{ Donc } \prod_{\mathfrak{A} \in \mathfrak{A}_i} p_i^{\mathfrak{A}_i} \not\subset \mathbb{Q}$$

Or comme $\mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$, $\mathfrak{A}_i \subset \mathbb{Q}$ donc $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_n \subset \mathbb{N}$, $\mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$, $\mathfrak{A}_i \not\subset \mathbb{Q}$. Ainsi

$$\left(\prod_{\mathfrak{A} \in \mathfrak{A}_i} p_i^{\mathfrak{A}_i} \right)^{\frac{1}{p}} \not\subset \mathbb{Q} \Leftrightarrow \prod_{\mathfrak{A} \in \mathfrak{A}_i} p_i^{\frac{\mathfrak{A}_i}{p}} \not\subset \mathbb{Q}$$

Or comme $\mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$, $p_i^{\frac{\mathfrak{A}_i}{p}} \not\subset \mathbb{Q}$ Donc $p_1^{\frac{\mathfrak{A}_1}{p}} \not\subset \mathbb{Q} \dots \not\subset p_n^{\frac{\mathfrak{A}_n}{p}} \not\subset \mathbb{Q}$ Donc $\mathfrak{A}_1 \not\subset \mathbb{Q} \dots \not\subset \mathfrak{A}_n \not\subset \mathbb{Q}$
Et donc $\mathfrak{A}_1 \not\subset \mathbb{Q} \dots \not\subset \mathfrak{A}_n \not\subset \mathbb{Q}$

Ainsi $(\ln(p_1), \dots, \ln(p_n))$ est libre

Et donc la dimension de \mathbb{R} n'est pas finis, donc \mathbb{R} n'est pas une extension finis de \mathbb{Q}

$\mathbb{N} = \mathbb{Z}$.

soit $\mathfrak{A} \subset \mathbb{L}$, alors $! \mathfrak{A} \subset \mathbb{K}$ tel que, $\mathfrak{A} \not\subset \sum_{\mathfrak{A} \in \mathfrak{A}_i} \alpha_{\mathfrak{A}} \mathfrak{A}_i$

Or on a $\mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$, $! \mathfrak{A} \subset \mathbb{Q}(\sqrt[p]{p})$, $\mathfrak{A}_i \subset \mathbb{Q}$, $\mathfrak{A}_i \not\subset \mathbb{Q}$, $\mathfrak{A}_i \not\subset \mathbb{Q}$, $\mathfrak{A}_i \not\subset \mathbb{Q}$

Ainsi $! \mathfrak{A} \subset \mathbb{K}$, $! \mathfrak{A} \subset \mathbb{K}$, $! \mathfrak{A} \subset \mathbb{K}$, $\mathfrak{A} \not\subset \sum_{\substack{\mathfrak{A} \in \mathfrak{A}_i \\ \mathfrak{A} \in \mathfrak{A}_i}} \alpha_{\mathfrak{A}} \beta_{\mathfrak{A}} \mathfrak{A}_i \mathfrak{A}_i$

Donc \mathfrak{A} s'écrit d'une manière unique comme des élément de \mathbb{K} ,

donc la famille $(\alpha_i \beta_j)_{\substack{\mathfrak{A} \in \mathfrak{A}_i \\ \mathfrak{A} \in \mathfrak{A}_i}} \mathfrak{A}_i \mathfrak{A}_i$ est une base de du k -espace vectoriel \mathbb{L}

De plus la famille $(\alpha_i \beta_j)_{\substack{\mathfrak{A} \in \mathfrak{A}_i \\ \mathfrak{A} \in \mathfrak{A}_i}} \mathfrak{A}_i \mathfrak{A}_i$ comporte exactement np éléments

Donc \mathbb{L} est une extensions finis de k et $[\mathbb{L} : k] \not\equiv [\mathbb{L} : \mathbb{K}][\mathbb{K} : k]$

Partie II. Éléments algébriques

N° 1.

pour montrer que $\mathbb{K}[\alpha] \cong \{P(\alpha), P \in \mathbb{K}[X]\}$,
on montre que $\{P(\alpha), P \in \mathbb{K}[X]\} \cong \text{Vect}_{\mathbb{K}}(\alpha^n, n \in \mathbb{N})$
pour cela,

$$\mathfrak{M} \cong \{P(\alpha), P \in \mathbb{K}[X]\} \Leftrightarrow \exists \gamma_1, \dots, \gamma_n \in \mathbb{K} \text{ s.t. } \sum_{i=1}^n \gamma_i \alpha^i \in \text{Vect}_{\mathbb{K}}(\alpha^n, n \in \mathbb{N}) \cong \mathbb{K}[\alpha]$$

Donc $\{P(\alpha), P \in \mathbb{K}[X]\} \cong \mathbb{K}[\alpha]$

soient $\mathfrak{M}, \gamma \in \mathbb{K}[\alpha]$, alors $\exists P, Q \in \mathbb{K}[X], P(\alpha) \in \mathfrak{M}$ et $Q(\alpha) \in \gamma$, alors:

- $\gamma \in \mathbb{K}[\alpha]$
- $\mathfrak{M} + \gamma \cong P(\alpha) + Q(\alpha) \cong (P + Q)(\alpha)$ et $P + Q \in \mathbb{K}[X]$
- $\mathfrak{M} \gamma \cong P(\alpha) \gamma \cong (P \gamma)(\alpha)$ et $P \gamma \in \mathbb{K}[X]$

Donc $\mathbb{K}[\alpha]$ est un sous-anneau de \mathbb{L}

Et $\text{Vect}(\alpha^n, n \in \mathbb{N})$ est le plus petit ensemble stable par $+$ et \cdot ,
ce qui fait de lui le plus petit sous-anneau contenant α et \mathbb{K}

N° 2.

procédons par double inclusion pour prouver que α est algébrique sur \mathbb{K} si et seulement si
il existe $n \in \mathbb{N}$ tel que $(1, \alpha, \dots, \alpha^n)$ soit une famille liée
(\Rightarrow) Supposons que α est algébrique sur \mathbb{K} , alors

$$\exists \mathfrak{M} \in \mathbb{K}[X], \mathfrak{M}(\alpha) = 0 \Leftrightarrow \exists n \in \mathbb{N}, \exists \mathfrak{M}_1, \dots, \mathfrak{M}_n \in \mathbb{K}, \mathfrak{M}(\alpha) = \sum_{i=1}^n \mathfrak{M}_i \alpha^i = 0$$

$$\text{Donc } \sum_{i=1}^n \mathfrak{M}_i \alpha^i \in \mathfrak{M}_1$$

Donc $(1, \alpha, \dots, \alpha^n)$ est liée

(\Leftarrow) Supposons que $(1, \alpha, \dots, \alpha^n)$ soit liée, alors:

$$\exists \mathfrak{M}_1, \dots, \mathfrak{M}_n \in \mathbb{K}, \exists \lambda \in \mathbb{N}, \forall \alpha^{\lambda} \in \sum_{i=1}^n \mathfrak{M}_i \alpha^i$$

$$\text{Donc } \sum_{i=1}^n \mathfrak{M}_i \alpha^i \in \sum_{i=1}^n \mathfrak{M}_i \alpha^i$$

en posant $\forall \alpha^{\lambda} \in \sum_{i=1}^n \mathfrak{M}_i \alpha^i$, on obtient

$$\sum_{i=1}^n \mathfrak{M}_i \alpha^i \in \sum_{i=1}^n \mathfrak{M}_i \alpha^i$$

$$\text{Or } \sum_{i=1}^n \mathfrak{M}_i \alpha^i \in \mathbb{K}[X]$$

Donc α est algébrique

Par le principe de double inclusion

α est algébrique si et seulement si il existe $n \in \mathbb{N}$ tel que $(1, \alpha, \dots, \alpha^n)$ est liée

$N = \circ <$.

Soit $\mathfrak{A} \leq \mathbb{L}$, alors \mathfrak{A} est algébrique de degré \mathfrak{n} sur \mathbb{K} si et seulement si $(\mathfrak{n}, \mathfrak{A})$ est liée si et seulement si il existe $\mathfrak{B} \leq \mathbb{K}$, $\mathfrak{A} \not\leq \mathfrak{B} \not\leq \mathfrak{B} \not\leq \mathfrak{B}$ si et seulement si $\mathfrak{A} \leq \mathbb{K}$

Donc on a bien $(\mathfrak{n}, \mathfrak{A})$ liée $\Leftrightarrow \mathfrak{A} \leq \mathbb{K}$

$N = \circ \chi$.

Supposons que \mathbb{L} est une extension finie de \mathbb{K} et soit $\mathfrak{A} \leq \mathbb{L}$

alors \mathfrak{A} est algébrique sur \mathbb{K} si:

a

$N = \circ \mathfrak{P}$. a.

On sait par la définitions que $(1, \alpha, \dots, \alpha^{d \cdot \mathfrak{n}})$ est libre

Et $\text{Vect}(\alpha^n, n \in \mathbb{N}) \not\leq \text{Vect}(\alpha^n, n \in [\mathfrak{n}; d \cdot \mathfrak{n}])$

Ainsi $\text{Vect}(\alpha^n, n \in [\mathfrak{n}; d \cdot \mathfrak{n}])$ est une base de $\mathbb{K}[\alpha]$

b.

Supposons que $\beta \diamond \mathfrak{V}$, alors prouvons que f_β est linéaire et bijective

• linéarité:

Soient $\mathfrak{B} \leq \mathbb{K}$, $\mathfrak{A}, \mathfrak{C} \leq \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{B} \mathfrak{A} \uparrow \mathfrak{C}) \not\leq \beta \mathfrak{B} \mathfrak{A} \uparrow \beta \mathfrak{C} \not\leq \mathfrak{B} f_\beta(\mathfrak{A}) \uparrow f_\beta(\mathfrak{C})$ donc f_β est linéaire

• bijectivité:

soit $\mathfrak{A} \leq \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{A}) \not\leq \mathfrak{V}$

alors $\beta \mathfrak{A} \not\leq \mathfrak{V}$ donc $\mathfrak{A} \not\leq \mathfrak{V}$ car $\beta \diamond \mathfrak{V}$

donc $\text{Ker}(f_\beta) \not\leq \{\mathfrak{V}\}$. Donc f_β est injective

Et soient $\mathfrak{A}, \mathfrak{C} \leq \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{A}) \not\leq \mathfrak{C}$

alors $\mathfrak{A} \not\leq \frac{\mathfrak{C}}{\beta}$ car $\beta \diamond \mathfrak{V}$, et donc f_β est surjective

et comme f_β va de $\mathbb{K}[\alpha]$ dans $\mathbb{K}[\alpha]$

f_β est un automorphisme

c.

a faire

d.

On a: $\mathbb{K} \leq \mathbb{K}[\alpha]$, donc \mathbb{K} est un sous-corps de $\mathbb{K}[\alpha]$

De plus comme $(1, \alpha, \dots, \alpha^{d \cdot \mathfrak{n}})$ est une base de $\mathbb{K}[\alpha]$ qui comporte d élément

Ainsi $\mathbb{K}[\alpha]$ est une extensions finie de \mathbb{K} , avec $[\mathbb{K}[\alpha] : \mathbb{K}] \not\leq d$

e.

Il est évident que $\mathbb{Q}(\sqrt[p]{p}) \leq \mathbb{C}$, et comme \mathbb{Q} est un sous groupe et que $\sqrt[p]{p} \leq \mathbb{C}$,

alors par les questions précédente:

$\mathbb{Q}(\sqrt[p]{p})$ est un sous-corps de \mathbb{C}

$N = \circ \mathfrak{H}$.

i) \Rightarrow ii) est évident car $\mathbb{K}[\alpha]$ est un corps et donc stable par \mathfrak{M}

ii) \Rightarrow iii) Supposons que $\alpha^{\gamma \cap} \vdash \mathbb{K}[\alpha]$, alors
 $\mathbb{B} \mathfrak{M} \vdash \mathbb{K}[X]$, $\mathfrak{M}(\alpha) \not\leq \alpha^{\gamma \cap}$, soit \mathfrak{M} un telle polynôme, alors:

$$\begin{aligned}\mathfrak{M}(\alpha) \not\leq \alpha^{\gamma \cap} &\Leftrightarrow \alpha \mathfrak{M}(\alpha) \not\leq \alpha \alpha^{\gamma \cap} \not\leq \cap \\ &\Leftrightarrow \alpha \mathfrak{M}(\alpha) \gamma \alpha \not\leq \gamma\end{aligned}$$

Posons $\mathfrak{M} \not\leq X \mathfrak{M}(X) \gamma \cap \leq \mathbb{K}[X]$, ainsi $\mathfrak{M}(\alpha) \not\leq 0$

Et donc α est constructible

iii) \Rightarrow i) Supposons que α est algébrique sur \mathbb{K} , alors par la question 1.
 $\mathbb{K}[\alpha]$ est un sous-corps de \mathbb{L}

Ainsi par un raisonnement cyclique,

on a bien que $\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{L} \Leftrightarrow \alpha^{\gamma \cap} \leq \mathbb{K}[\alpha] \Leftrightarrow \alpha$ est algébrique sur \mathbb{K}

Partie III. Polynômes minimal d'un élément algébrique

$\mathbf{N}^{\circ} \vdash$.

Si I_{α} na possède pas une polynôme de degré q ,

alors soit $\mathfrak{M} \leq I_{\alpha}$ de degré q , alors soit \mathfrak{M} sont coefficient dominant

alors le polynome $\frac{\mathfrak{M}}{\mathfrak{M}}$ est de degrés q et sont coefficient dominant vaut \cap

De plus $\frac{\mathfrak{M}}{\mathfrak{M}}(\alpha) \not\leq \frac{\mathfrak{M}(\alpha)}{\mathfrak{M}} \not\leq \gamma \not\leq \gamma$ Donc $\frac{\mathfrak{M}}{\mathfrak{M}} \leq I_{\alpha}$

Donc I_{α} possède un polynôme unitaire de degrés q

Soient $\mathfrak{M}, \mathfrak{N} \leq I_{\alpha}$ deux polynômes unitaire de degrés q

Alors $\mathbb{B} \mathfrak{M}_{\gamma}, \dots, \mathfrak{M}_{q \gamma \cap}, \mathfrak{N}_{\gamma}, \dots, \mathfrak{N}_{q \gamma \cap} \leq \mathbb{K}$, $\mathfrak{M} \not\leq X^q \uparrow \sum_{\gamma \not\leq \gamma} \mathfrak{M}_{\gamma} X^{\gamma}$ et $\mathfrak{N} \not\leq X^q \uparrow \sum_{\gamma \not\leq \gamma} \mathfrak{N}_{\gamma} X^{\gamma}$

Alors $\mathfrak{M}(\alpha) \gamma \mathfrak{N}(\alpha) \not\leq \sum_{\gamma \not\leq \gamma} \mathfrak{M}_{\gamma} \alpha^{\gamma} \gamma \sum_{\gamma \not\leq \gamma} \mathfrak{N}_{\gamma} \alpha^{\gamma} \not\leq \gamma$

donc $\sum_{\gamma \not\leq \gamma} (\mathfrak{M}_{\gamma} \gamma \mathfrak{N}_{\gamma}) \alpha^{\gamma}$, et comme $(1, \alpha, \dots, \alpha^{q \gamma \cap})$ est libre, on a: $\mathbb{K} \gamma \leq \llbracket \gamma; q \gamma \cap \rrbracket$, $\mathfrak{M}_{\gamma} \not\leq \mathfrak{N}_{\gamma}$

Ainsi on a bien $\mathfrak{M} \not\leq \mathfrak{N}$

Donc il existe un unique polynome unitaire de degré q dans I_{α}

$\mathbf{N}^{\circ} \Downarrow$.

Supposons par l'absurde que μ_{α} est réductible,

alors $\mathbb{B} \mathfrak{M}, \mathfrak{N} \leq \mathbb{K}[X]$, $\mu_{\alpha} \not\leq \mathfrak{M} \mathfrak{N}$, soient de tels polynômes

Ainsi $\mu_{\alpha}(\alpha) \not\leq \mathfrak{M}(\alpha) \mathfrak{N}(\alpha) \not\leq \gamma$ donc $\mathfrak{M}(\alpha) \not\leq \gamma$ ou $\mathfrak{N}(\alpha) \not\leq \gamma$,

donc α est algébrique de degrés inférieure stricte à d , absurde !

Donc μ_{α} est irréductible

Soit $\mathfrak{M} \leq I_{\alpha}$, alors $\mathbb{B} \mathfrak{N} \leq \mathbb{K}[X]$, $\mathfrak{M} \not\leq \mu_{\alpha} \mathfrak{N}$ car $\mathfrak{M}(\alpha) \not\leq \gamma$, ainsi $I_{\alpha} \vdash \{\mu_{\alpha} \mathfrak{M}, \mathfrak{M} \leq \mathbb{K}[X]\}$

Et soit $\mathbb{B} \mathfrak{N} \leq \mathbb{K}[X]$, $\mathfrak{M} \not\leq \mu_{\alpha} \mathfrak{N}$, alors $\mathfrak{M}(\alpha) \not\leq (\mu_{\alpha} \mathfrak{N})(\alpha) \not\leq \mu_{\alpha}(\alpha) \mathfrak{N}(\alpha) \not\leq \gamma$,

donc $\mathfrak{M} \leq I_{\alpha}$ et donc $\{\mu_{\alpha} \mathfrak{N}, \mathfrak{N} \leq \mathbb{K}[X]\} \vdash I_{\alpha}$

Ainsi par double inclusion $\{\mu_{\alpha} \mathfrak{N}, \mathfrak{N} \leq \mathbb{K}[X]\} \not\leq I_{\alpha}$

$N = \circ \downarrow$.

étant donner que μ_α est le plus petit polynômes telle que $\mu_\alpha(\alpha) \neq 0$
 alors $(1, \alpha, \dots, \alpha^q)$ est la plus petite famille liée, donc le degrés de alpha vaut q est d , si bien que:
 $\deg \mu_\alpha \leq d$

$N = \circ \uparrow$.

il est évidant que le polynôme minimal est $X^d - 1$

$N = \circ \uparrow \uparrow$.

Posons $\mu \in \mathbb{Q}[X] \setminus \mathbb{Q}$ $X^d - 1 \in \mathbb{Q}[X]$, avec $\mu, \gamma, \alpha, \beta, \epsilon$ non tous nul
 Alors cherchons $\mu, \gamma, \alpha, \beta, \epsilon$ tel que $\mu(\alpha) \neq 0$
 Ainsi

$$\begin{aligned} \mu(\alpha) \in \mathbb{Q} & \iff (\sqrt{d} - 1)^d - 1 \in \mathbb{Q} \iff (\sqrt{d} - 1)^d - 1 \in \mathbb{Q} \\ & \iff \sqrt{d} - 1 \in \mathbb{Q} \iff \sqrt{d} \in \mathbb{Q} \iff d \in \mathbb{Q} \iff d \in \mathbb{Q} \end{aligned}$$

Alors comme $(1, \sqrt{d}, \sqrt{d}^2, \sqrt{d}^3)$ est libre, on obtient:

$$\begin{cases} \mu(\alpha) - 1 \in \mathbb{Q} \\ \mu(\alpha) - \sqrt{d} \in \mathbb{Q} \\ \mu(\alpha) - \sqrt{d}^2 \in \mathbb{Q} \\ \mu(\alpha) - \sqrt{d}^3 \in \mathbb{Q} \end{cases} \iff \begin{cases} \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \end{cases} \iff \begin{cases} \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \\ \mu(\alpha) \in \mathbb{Q} \end{cases}$$

Ainsi $\mu \in \mathbb{Q} \setminus \mathbb{Q}$ $X^d - 1 \in \mathbb{Q}$, ainsi on prouve que α est algébrique
et que μ est le polynôme minimal de α sur \mathbb{Q} car sinon on aurait $\mu \in \mathbb{Q}$

Partie IV. Nombres algébriques (sur \mathbb{Q})

$N = \circ \uparrow \uparrow$. a.

il est évidant que $\mathbb{Q}[\alpha, \beta]$ est stable par \uparrow et \downarrow
 et deplus, soit $\alpha, \beta \in \mathbb{Q}[\alpha, \beta]$ alors $\beta \in \mathbb{Q}[\alpha, \beta]$, $\alpha' \in \mathbb{Q}[\alpha, \beta]$, $\beta' \in \mathbb{Q}[\alpha, \beta]$, $\alpha'' \in \mathbb{Q}[\alpha, \beta]$, $\beta'' \in \mathbb{Q}[\alpha, \beta]$
 et $\alpha \in \mathbb{Q}[\alpha, \beta]$ et $\beta \in \mathbb{Q}[\alpha, \beta]$ et $\alpha' \in \mathbb{Q}[\alpha, \beta]$ et $\beta' \in \mathbb{Q}[\alpha, \beta]$
 alors

$$\begin{aligned} & (\alpha - 1)(\alpha - \sqrt{d})(\alpha - \sqrt{d}^2)(\alpha - \sqrt{d}^3) = (\alpha' - 1)(\alpha' - \sqrt{d})(\alpha' - \sqrt{d}^2)(\alpha' - \sqrt{d}^3) \\ & \iff (\alpha - 1)(\alpha - \sqrt{d})(\alpha - \sqrt{d}^2)(\alpha - \sqrt{d}^3) = (\alpha' - 1)(\alpha' - \sqrt{d})(\alpha' - \sqrt{d}^2)(\alpha' - \sqrt{d}^3) \\ & \iff \alpha - 1 \in \mathbb{Q} \end{aligned}$$

De même $\alpha(\alpha - 1) \in \mathbb{Q}$ et $\alpha \in \mathbb{Q}$

De plus par la question 1 $\mathbb{Q}[\alpha, \beta]$ est une extention finie de $\mathbb{Q}[\alpha]$

Or $\mathbb{Q}[\alpha]$ est une extensions finis de \mathbb{Q}

Donc $\mathbb{Q}[\alpha, \beta]$ est un corps et est une extention finie de \mathbb{Q}

b.

Pourvons d'abord que $\sqrt{p} \notin \mathbb{Q}(\sqrt{p})$,

Pour cela cherchons $\alpha, \gamma \in \mathbb{Q}, \alpha + \gamma \sqrt{p} = \sqrt{p}$, alors:

$$\alpha + \gamma \sqrt{p} = \sqrt{p} \iff \begin{cases} \alpha = 0 \text{ ou } \gamma = 0 \\ \alpha + \gamma \sqrt{p} = \sqrt{p} \end{cases}$$

Il est évident que $\gamma \neq 0$ car $\gamma \in \mathbb{Q}$ et $\sqrt{p} \notin \mathbb{Q}$ donc $\alpha \neq 0$

Ainsi $\gamma \sqrt{p} = \sqrt{p} - \alpha \iff \gamma = \frac{\sqrt{p} - \alpha}{\sqrt{p}} \notin \mathbb{Q}$ absurde, donc $\sqrt{p} \notin \mathbb{Q}(\sqrt{p})$

Et donc comme \mathbb{Q} est un sous corps de $\mathbb{Q}(\sqrt{p})$ et que $\mathbb{Q}(\sqrt{p})$ est un sous corps de $\mathbb{Q}[\sqrt{p}, \sqrt{p}]$,

et comme $(1, \sqrt{p})$ est une base du \mathbb{Q} -espace vectoriel $\mathbb{Q}(\sqrt{p})$

et que $(1, \sqrt{p})$ est une base du $\mathbb{Q}(\sqrt{p})$ -espace vectoriel $\mathbb{Q}[\sqrt{p}, \sqrt{p}]$

Ainsi par la question 1. $(1, \sqrt{p}, \sqrt{p}, \sqrt{p})$ est une base du \mathbb{Q} -espace vectoriel $\mathbb{Q}[\sqrt{p}, \sqrt{p}]$

Et donc $\mathbb{Q}[\sqrt{p}, \sqrt{p}] = \{ \alpha + \gamma \sqrt{p} + \alpha' \sqrt{p} + \gamma' \sqrt{p}^2, \alpha, \gamma, \alpha', \gamma' \in \mathbb{Q} \}$

$\mathbb{N} = \mathbb{N}$.

Soit $\alpha, \gamma \in \overline{\mathbb{Q}}$. Alors $\mathbb{Q}[\alpha, \gamma]$ est un corps,

et en particulier une extension finie de \mathbb{Q} .

Donc la somme, l'inverse et le produits sont stables dans $\mathbb{Q}[\alpha, \gamma]$,

et donc par la question 3. $\overline{\mathbb{Q}}$ est un corps, et est donc un sous-corps de \mathbb{C}