

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	Ɔ	wun
8	ℋ	hag
9	ƚ	nau
10	↷	je
11	∫	ei
=	℔	ing/i ng
+	↑	ti
−	Υ	al
×	ℳ	dag
÷	∫	lag
∈	ℷ	so
∀	ℷ	per
∃	℔	ber
∃!	!℔	\
>	ℳ	man
<	ℳ	e
≥	ℳ℔	maning
≤	ℳ℔	ehwing
≠	◊	naing
⊂	ƚ	suz
⊃	ƚ	zus

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

$$e^{\mathfrak{A}} \mathbb{X} \cap \uparrow \mathfrak{A} \uparrow \frac{\mathfrak{A}^{\mathfrak{A}}}{\mathfrak{A}!} \uparrow \dots \uparrow \frac{\mathfrak{A}^{\mathfrak{A}}}{\mathfrak{A}!} \uparrow o(\mathfrak{A}^{\mathfrak{A}})$$

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 $\alpha \in \mathbb{Q}(\sqrt{p})$ 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 $\alpha \in \text{Vect}(\mathbb{R}, \sqrt{p})$

et supposons par l'absurde $\exists \lambda, \mu \in \mathbb{Q}, \alpha = \lambda + \mu \sqrt{p} \neq 0$

alors $\frac{\alpha}{\lambda} \in \mathbb{Q}(\sqrt{p})$ 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 $P(\sqrt{p}) \neq 0$

prenons la division euclidienne de $X^2 - p$ par P

ce qui nous donne $X^2 - p = PQ + R$ 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} on obtient :

$$(\sqrt{p})^2 - p = \underbrace{P(\sqrt{p})}_{\neq 0} + R(\sqrt{p})$$

donc $R(\sqrt{p}) = 0$ et donc $\deg R = 0$

ainsi P divise $X^2 - p$

Ainsi Comme P divise $X^2 - p$ et que $\deg P = 1$,

alors P et $X^2 - p$ possède deux racines en commun dont \sqrt{p}

et comme $X^2 - p = (X - \sqrt{p})(X + \sqrt{p})$ 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 $P \in \mathbb{Q}[X]$, $P(\sqrt[n]{p}) \notin \mathbb{Q}$

ii.

Par un raisonnement analogue à la question 1.b on montre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{p})$,
De plus soit $\mathfrak{A} \in \mathbb{Q}(\sqrt[n]{p})$ alors soient $\mathfrak{A}, \mathfrak{A}^p, \mathfrak{A}^{p^2}, \dots, \mathfrak{A}^{p^{n-1}} \in \mathbb{Q}$ et $\mathfrak{A} \notin \mathbb{Q}$ car $\sqrt[n]{p} \notin \mathbb{Q}$
donc $\mathfrak{A} \in \text{Vect}\left(\mathbb{Q}, \sqrt[n]{p}, \sqrt[n]{p}^2, \dots, \sqrt[n]{p}^{n-1}\right)$
donc $\mathbb{Q}(\sqrt[n]{p})$ est une extensions finis et $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] \leq n$

d.

Soient $\mathfrak{A}_1, \dots, \mathfrak{A}_n \in \mathbb{Q}$ tels que $\sum_{i=1}^n \mathfrak{A}_i \ln(p_i) \notin \mathbb{Q}$,
alors

$$\ln\left(\prod_{i=1}^n p_i^{\mathfrak{A}_i}\right) \notin \mathbb{Q} \text{ Donc } \prod_{i=1}^n p_i^{\mathfrak{A}_i} \notin \mathbb{Q}$$

Or comme $1 \leq i \leq [1; n]$, $\mathfrak{A}_i \in \mathbb{Q}$ donc $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_n \in \mathbb{N}$, $1 \leq i \leq [1; n]$, $\mathfrak{A}_i \leq \frac{p_i}{p_i - 1}$. Ainsi

$$\left(\prod_{i=1}^n p_i^{\mathfrak{A}_i}\right)^{\frac{1}{p_i}} \notin \mathbb{Q} \Leftrightarrow \prod_{i=1}^n p_i^{\frac{\mathfrak{A}_i}{p_i}} \notin \mathbb{Q}$$

Or comme $1 \leq i \leq [1; n]$, $p_i^{\frac{\mathfrak{A}_i}{p_i}} \in \mathbb{N}$ Donc $p_1^{\frac{\mathfrak{A}_1}{p_1}} \notin \mathbb{Q} \dots \notin p_n^{\frac{\mathfrak{A}_n}{p_n}} \notin \mathbb{Q}$ Donc $p_1 \notin \mathbb{Q} \dots \notin p_n \notin \mathbb{Q}$
Et donc $\mathfrak{A}_1 \notin \mathbb{Q} \dots \notin \mathfrak{A}_n \notin \mathbb{Q}$

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}

$N = 0$.

soit $\mathfrak{A} \in L$, alors $\mathfrak{A} = \sum_{i=1}^n \alpha_i \mathfrak{A}_i$

Or on a $1 \leq i \leq [1; n]$, $\mathfrak{A}_i \in \mathbb{Q}$, $\mathfrak{A}_i \leq k$, $\mathfrak{A}_i \in \mathbb{Q}$ et $\sum_{i=1}^p \beta_i \mathfrak{A}_i$

Ainsi $\mathfrak{A} = \sum_{i=1}^n \alpha_i \mathfrak{A}_i \in \mathbb{Q}$, $\mathfrak{A}_i \in \mathbb{Q}$, $\mathfrak{A}_i \leq k$, $\mathfrak{A}_i \in \mathbb{Q}$ et $\sum_{i=1}^p \beta_i \mathfrak{A}_i$

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

donc la famille $(\alpha_i \beta_j)_{1 \leq i \leq n, 1 \leq j \leq p}$ est une base de du k -espace vectoriel L

De plus la famille $(\alpha_i \beta_j)_{1 \leq i \leq n, 1 \leq j \leq p}$ comporte exactement np éléments

Donc L est une extensions finis de k et $[L : k] \leq [L : K][K : k]$

Partie II. Éléments algébriques

$N = \circ \uparrow$.

pour montrer que $\mathbb{K}[\alpha] \not\cong \{P(\alpha), P \in \mathbb{K}[X]\}$,
on montre que $\{P(\alpha), P \in \mathbb{K}[X]\} \not\cong \text{Vect}_{\mathbb{K}}(\alpha^n, n \in \mathbb{N})$
pour cela,

$$\mathfrak{M} \in \{P(\alpha), P \in \mathbb{K}[X]\} \Leftrightarrow \exists \gamma_1, \dots, \gamma_n \in \mathbb{K} \text{ et } \sum_{\substack{\mathfrak{M} \in \mathbb{K} \\ \gamma \in \mathbb{K}}} \gamma_{\mathfrak{M}} \alpha^{\mathfrak{M}} \in \text{Vect}_{\mathbb{K}}(\alpha^n, n \in \mathbb{N}) \not\cong \mathbb{K}[\alpha]$$

Donc $\{P(\alpha), P \in \mathbb{K}[X]\} \not\cong \mathbb{K}[\alpha]$

soient $\mathfrak{M}, \gamma \in \mathbb{K}[\alpha]$, alors $\exists P, Q \in \mathbb{K}[X], P(\alpha) \not\cong \mathfrak{M}$ et $Q(\alpha) \not\cong \gamma$, alors:

- $\gamma \in \mathbb{K}[\alpha]$
- $\mathfrak{M} \gamma \not\cong P(\alpha) \gamma \not\cong Q(\alpha) \not\cong (P \gamma Q)(\alpha)$ et $P \gamma Q \in \mathbb{K}[X]$
- $\mathfrak{M} \mathfrak{M} \gamma \not\cong P(\alpha) \mathfrak{M} Q(\alpha) \not\cong (P \mathfrak{M} Q)(\alpha)$ et $PQ \in \mathbb{K}[X]$

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 \uparrow et \mathfrak{M} ,
ce qui fait de lui le plus petit sous-anneau contenant α et \mathbb{K}

$N = \circ \uparrow$.

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

$$\exists \mathfrak{M} \in \mathbb{K}[X], \mathfrak{M}(\alpha) \not\cong \gamma \Leftrightarrow \exists n \in \mathbb{N}, \exists \mathfrak{M}_1, \dots, \mathfrak{M}_n \in \mathbb{K}, \mathfrak{M}(\alpha) \not\cong \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \not\cong \gamma$$

$$\text{Donc } \gamma \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \not\cong \mathfrak{M}_1$$

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

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

$$\exists \mathfrak{M}_1, \dots, \mathfrak{M}_n \in \mathbb{K}, \exists \gamma \in \mathbb{N}, \not\cong \alpha^{\gamma} \not\cong \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma}$$

$$\text{Donc } \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \not\cong \not\cong \alpha^{\gamma} \not\cong \gamma$$

en posant $\gamma \not\cong \mathfrak{M}_{\gamma}$, on obtient

$$\sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \not\cong \not\cong \alpha^{\gamma} \not\cong \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \not\cong \gamma$$

$$\text{Or } \sum_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq \alpha}} \mathfrak{M}_{\gamma} \alpha^{\gamma} \in \mathbb{K}[X]$$

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 $\mathfrak{B} \leq \mathbb{K}$, $\mathfrak{A} \not\leq \mathfrak{B}$ et $\mathfrak{n} \nmid [\mathfrak{B} : \mathbb{K}]$ 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

$N = \circ \vdash$. a.

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

Et $\text{Vect}(\alpha^n, n \in \mathbb{N}) \not\leq \text{Vect}(\alpha^n, n \in \llbracket \mathfrak{n}; d-1 \rrbracket)$

Ainsi $\text{Vect}(\alpha^n, n \in \llbracket \mathfrak{n}; d-1 \rrbracket)$ est une base de $\mathbb{K}[\alpha]$

b.

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

• linéarité:

Soient $\mathfrak{B} \leq \mathbb{K}$, $\mathfrak{A}, \mathfrak{C} \leq \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{B} \mathfrak{A} \uparrow \mathfrak{C}) \leq \beta \mathfrak{B} \mathfrak{A} \uparrow \beta \mathfrak{C} \leq \beta \mathfrak{B} f_\beta(\mathfrak{A}) \uparrow f_\beta(\mathfrak{C})$ donc f_β est linéaire

• bijectivité:

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

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

donc $\text{Ker}(f_\beta) \leq \{\mathbb{V}\}$. 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 $\beta \diamond \mathbb{V}$, 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.

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

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

Ainsi $\mathbb{K}[\alpha]$ est une extensions finie de \mathbb{K} , avec $[\mathbb{K}[\alpha] : \mathbb{K}] \leq d$

d.

Il est évident que $\mathbb{Q}(\sqrt[d]{p}) \leq \mathbb{C}$, et comme \mathbb{Q} est un sous groupe et que $\sqrt[d]{p} \in \mathbb{C}$, alors par les questions précédente:

$\mathbb{Q}(\sqrt[d]{p})$ 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{H}

ii) \Rightarrow iii) Supposons que $\alpha \in \mathbb{K} \setminus \mathbb{L}$, alors
 $\exists \text{ un } P \in \mathbb{K}[X], P(\alpha) = 0$, soit P un tel polynôme, alors:

$$\begin{aligned} P(\alpha) = 0 &\Leftrightarrow \alpha \text{ est racine de } P \\ &\Leftrightarrow \alpha \text{ est algébrique sur } \mathbb{K} \end{aligned}$$

Posons $P \in \mathbb{K}[X]$, ainsi $P(\alpha) = 0$

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 $\mathbb{L} \Leftrightarrow \alpha \in \mathbb{K} \setminus \mathbb{L} \Leftrightarrow \alpha$ est algébrique sur \mathbb{K}

Partie III. Polynôme minimal d'un élément algébrique

$\mathbb{N}^* \rightarrow$.

Si I_α ne possède pas un polynôme de degré q ,

alors soit $P \in I_\alpha$ de degré q , alors soit a son coefficient dominant

alors le polynôme $\frac{P}{a}$ est de degré q et son coefficient dominant vaut 1

De plus $\frac{P}{a}(\alpha) = 0$ donc $\frac{P}{a} \in I_\alpha$

Donc I_α possède un polynôme unitaire de degré q

Soient $P, Q \in I_\alpha$ deux polynômes unitaires de degrés q

Alors $\exists a_0, \dots, a_{q-1}, b_0, \dots, b_{q-1} \in \mathbb{K}, P = \sum_{\lambda=0}^{q-1} a_\lambda X^\lambda$ et $Q = \sum_{\lambda=0}^{q-1} b_\lambda X^\lambda$

Alors $P(\alpha) = Q(\alpha) = 0$ donc $\sum_{\lambda=0}^{q-1} a_\lambda \alpha^\lambda = \sum_{\lambda=0}^{q-1} b_\lambda \alpha^\lambda = 0$

donc $\sum_{\lambda=0}^{q-1} (a_\lambda - b_\lambda) \alpha^\lambda = 0$, et comme $(1, \alpha, \dots, \alpha^{q-1})$ est libre, on a: $\forall \lambda \in \mathbb{N}, 0 \leq \lambda < q, a_\lambda = b_\lambda$

Ainsi on a bien $P = Q$

Donc il existe un unique polynôme unitaire de degré q dans I_α

$\mathbb{N}^* \rightarrow$.

Supposons par l'absurde que μ_α est réductible,

alors $\exists P, Q \in \mathbb{K}[X], \mu_\alpha = PQ$, soient de tels polynômes

Ainsi $\mu_\alpha(\alpha) = 0$ donc $P(\alpha)Q(\alpha) = 0$ donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$,

donc α est algébrique de degré strictement inférieur à d , absurde !

Donc μ_α est irréductible

Soit $P \in I_\alpha$, alors $\exists Q \in \mathbb{K}[X], P = \mu_\alpha Q$ car $P(\alpha) = 0$, ainsi $I_\alpha \subset \{\mu_\alpha P, P \in \mathbb{K}[X]\}$

Et soit $\exists Q \in \mathbb{K}[X], P = \mu_\alpha Q$, alors $P(\alpha) = 0$ donc $\mu_\alpha(\alpha)Q(\alpha) = 0$ donc $Q(\alpha) = 0$,

donc $P \in I_\alpha$ et donc $\{\mu_\alpha Q, Q \in \mathbb{K}[X]\} \subset I_\alpha$

Ainsi par double inclusion $\{\mu_\alpha Q, Q \in \mathbb{K}[X]\} = I_\alpha$

$N = \circ \downarrow$.

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

$$\begin{aligned} \mu(\alpha) \neq 0 & \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \\ & \Leftrightarrow \sqrt{d} + \sqrt{d} \neq 1 \Leftrightarrow \sqrt{d} \neq 1 - \sqrt{d} \Leftrightarrow \sqrt{d} \neq 1 - \sqrt{d} \Leftrightarrow \sqrt{d} \neq 1 - \sqrt{d} \\ & \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \Leftrightarrow (\sqrt{d} + \sqrt{d})^d - 1 \neq 0 \end{aligned}$$

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

$$\begin{cases} \mu \neq 0 \\ \gamma \neq 0 \\ \alpha \neq 0 \\ \beta \neq 0 \end{cases} \Leftrightarrow \begin{cases} \mu \neq 0 \\ \gamma \neq 0 \\ \alpha \neq 0 \\ \beta \neq 0 \end{cases} \Leftrightarrow \begin{cases} \mu \neq 0 \\ \gamma \neq 0 \\ \alpha \neq 0 \\ \beta \neq 0 \end{cases}$$

Ainsi $\mu \in \mathbb{Q}[X] \setminus \mathbb{Q}$ $X^d - 1 \in \mathbb{Q}[X]$, 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 $\alpha, \beta \in \mathbb{Q}[\alpha, \beta]$ et $\alpha, \beta \in \mathbb{Q}[\alpha, \beta]$
 et $\alpha, \beta \in \mathbb{Q}[\alpha, \beta]$ et $\alpha, \beta \in \mathbb{Q}[\alpha, \beta]$
 alors

$$\begin{aligned} & (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \\ & \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \\ & \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \Leftrightarrow (\alpha + \beta) \neq 0 \end{aligned}$$

De même $\alpha(\beta + \epsilon) \neq 0 \Leftrightarrow \alpha \neq 0$

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 $\alpha + \gamma \sqrt{p} = \sqrt{p} \iff \gamma \sqrt{p} = \sqrt{p} - \alpha$ 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}

†/†