Gaspar Daguet

Maths : DM ᚢᚷ

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	ᚠ	fé
1	ᚢ	ur
2	ᚦ	tur
3	ᚨ	an
4	ᚱ	rai
5	ᚲ	kau
6	ᚷ	gèb
7	ᚹ	wun
8	ᚺ	hag
9	ᚾ	nau
10	ᛃ	je
11	ᛇ	ei
$=$	ᛝ	ing/i ng
$+$	ᛏ	ti
$-$	ᛉ	al
$\times$	ᛞ	dag
$\div$	ᛚ	lag
$\in$	ᛋ	so
$\forall$	ᛈ	per
$\exists$	ᛒ	ber
$\exists!$	!ᛒ	\
$>$	ᛗ	man
$<$	ᛖ	e
$\geq$	ᛗᛝ	maning
$\leq$	ᛖᛝ	ehwing
$\neq$	ᛜ	naing
$\subset$	ᛦ	suz
$\supset$	ᛧ	zus

ᚷᚹ ↑ << ᛝᚢᚠᚠ ce qui est équivalant à $79 + 65 = 144$

$$e^{ᛊ}_{ᛊ \to ᚠ} ᛝ \uparrow ᛊ \uparrow \frac{ᛊ^{ᚦ}}{ᚦ!} \uparrow \cdots \uparrow \frac{ᛊ^{ᚺ}}{ᚺ!} \uparrow o\left(ᛊ^{ᚺ}\right)$$

est équivalant à

$$e^x \underset{x \to 0}{=} 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{x!} + o(x^n)$$

Problème ⊦ : nombres algébrique et extensions de corps

Partie I. extensions de corps

N=° ∩. Premiers exemples a.

il est évidant que $\mathbb{R}$ est un sous-corps de $\mathbb{C}$ et de plus $\mathbb{C}$ est de dimension finis,
donc $\mathbb{C}$ est une extention finie de $\mathbb{R}$

de plus soit $\mathcal{A} \leq \mathbb{C}$ alors

$$\mathcal{A} \mathcal{G}, \mathcal{B} \leq \mathbb{R}, \mathcal{A} = \mathcal{G} \uparrow i \mathcal{B} \Leftrightarrow \mathcal{A} \leq \mathrm{Vect}(\cap, i)$$

Ainsi comme $\cap$ et i ne sont pas colinéaire dans $\mathbb{R}$, $\mathrm{Vect}(\cap, i)$ forme une base de $\mathbb{C}$
Ainsi $[\mathbb{C} : \mathbb{R}] = \vdash$

soit $\oplus$ un sous-corps qui contient $\mathbb{R}$
comme $[\mathbb{R} : \mathbb{R}] = \cap$ et que l'on vient de prouver que $[\mathbb{C} : \mathbb{R}] = \vdash$
il apparait donc comme condition que, $\cap \neq [\oplus : \mathbb{R}] \neq \vdash$
Ainsi $[\oplus : \mathbb{R}] = \cap$ ou $[\oplus : \mathbb{R}] = \vdash$
Et ansi $\oplus = \mathbb{R}$ ou $\oplus = \mathbb{C}$

b.

Soit $\mathcal{G} \leq \mathbb{Q}\left(\sqrt{\vdash}\right)$, alors $\exists \mathcal{B}, \mathcal{A} \leq \mathbb{Q}, \mathcal{G} = \mathcal{B} \uparrow \mathcal{A}\ \sqrt{\vdash}$, alors prenons $\mathcal{A} = \bot$
ainsi $\mathcal{G} = \mathcal{B} \leq \mathbb{Q}$, donc $\mathbb{Q} \wr \mathbb{Q}\left(\sqrt{\vdash}\right)$ et comme $\mathbb{Q}$ est un corps
de $\mathbb{Q}\left(\sqrt{\vdash}\right)$
de plus, soit $\mathcal{G} \leq \mathbb{Q}\left(\sqrt{\vdash}\right)$ alors $\exists \mathcal{B}, \mathcal{A} \leq \mathbb{Q}, \mathcal{G} = \mathcal{B} \uparrow \mathcal{B}\ \sqrt{\vdash}$, soit un telle $\mathcal{A}, \mathcal{B}$
donc $\mathcal{G} = \mathcal{A} \uparrow \mathcal{B}\ \sqrt{\vdash} \leq \mathrm{Vect}\left(\cap, \sqrt{\vdash}\right)$
et supposons par l'absurde $\exists \mathcal{G}, \mathcal{B} \leq \mathbb{Q} \setminus \mathbb{Q}^*, \mathcal{G} \uparrow \mathcal{B}\ \sqrt{\vdash} = \bot$
alors $\frac{\mathcal{G}}{\mathcal{B}} = \top\ \sqrt{\vdash}$ ce qui est absurde car $\frac{\mathcal{G}}{\mathcal{B}} \leq \mathbb{Q}$, donc $\mathcal{G} = \mathcal{B} = \bot$
Ainsi $\left(\cap, \sqrt{\vdash}\right)$ est une base de $\mathbb{Q}\left(\sqrt{\vdash}\right)$
Donc $\left[\mathbb{Q}\left(\sqrt{\vdash}\right) : \mathbb{Q}\right] = \vdash$

c. i.

Soit $P \leq \mathbb{Q}[X]$ tel que $P\left(\sqrt[\wr]{\vdash}\right) = \bot$
prenons la divisions euclidienne de $X^\wr \top \vdash$ par P
ce qui nous donne $X^\wr \top \vdash = PQ \uparrow R$ avec $Q \leq \mathbb{Q}_\cap[X]$ et $R \leq \mathbb{Q}[X]$ tel que $\deg R \neq \vdash$
En évaluant notre expression précédente en $\sqrt[\wr]{\vdash}$ on obtient :

$$\left(\sqrt[\wr]{\vdash}\right)^\wr \top \vdash = \bot = \underbrace{P\left(\sqrt[\wr]{\vdash}\right)}_{=\bot} \uparrow R$$

donc $R = \bot$ et donc $\deg R = \bot$
ainsi P divise $X^\wr \top \vdash$

Ainsi Comme P divise $X^\wr \top \vdash$ et que $\deg P = \vdash$,
alors P et $X^\wr \top \vdash$ possède deux racines en commun dont $\sqrt[\wr]{\vdash}$
et comme $X^\wr \top \vdash = \left(X \top \sqrt[\wr]{\vdash}\right)\left(X \top \sqrt[\wr]{\vdash} e^{i\frac{\pi}{\wr}}\right)\left(X \top \sqrt[\wr]{\vdash} e^{i\frac{\vdash\pi}{\wr}}\right)$ donc P à en plus une racine complexe
or un polynôme dans $\mathbb{R}$ qui possède une racine complexe possède sont conjugée

ce qui n'est pas le cas pour P donc $P \not\in \mathbb{Q}[X]$ ce qui est absurde
Donc $\not\exists P \in \mathbb{Q}[X], P\left(\sqrt[p]{p}\right) = 0$

i.

Par un résonnement annaloge à la question 1 .b on montre que $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[p]{p}\right)$,
De plus soit $x \in \mathbb{Q}\left(\sqrt[p]{p}\right)$ alors soient $a, b, c \in \mathbb{Q}, x = a + b\sqrt[p]{p} + c\left(\sqrt[p]{p}\right)^2$
donc $x \in \text{Vect}\left(1, \sqrt[p]{p}, \sqrt[p]{p}^2\right)$
donc $\mathbb{Q}\left(\sqrt[p]{p}\right)$ est une extensions finis et $\left[Q\left(\sqrt[p]{p}\right) : \mathbb{Q}\right] = 2$

d.

Soient $a_1, \cdots, a_n \in \mathbb{Q}$ tels que $\sum_{i=1}^{n} a_i \ln(p_i) = 0$,
alors

$$\ln\left(\prod_{i=1}^{n} p_i^{a_i}\right) = 0 \text{ Donc } \prod_{i=1}^{n} p_i^{a_i} = 1$$

Or comme $\forall i \in [\![1; n]\!], a_i \in \mathbb{Q}$ donc $\exists k, \exists b_1, \cdots, b_n \in \mathbb{N}, \forall i \in [\![1; n]\!], a_i = \frac{b_i}{k}$. Ainsi

$$\left(\prod_{i=1}^{n} p_i^{b_i}\right)^{\frac{1}{k}} = 1 \Leftrightarrow \prod_{i=1}^{n} p_i^{b_i} = 1$$

Or comme $\forall i \in [\![1; n]\!], p_i^{b_i} \in \mathbb{N}$ Donc $p_1^{b_1} = \cdots = p_n^{b_n} = 1$ Donc $b_1 = \cdots = b_n = 0$
Et donc $a_1 = \cdots = a_n = 0$
Ainsi $(\ln(p_1), \cdots, \ln(p_n))$ est libre
Et donc la dimmension de $\mathbb{R}$ n'est pas finis, donc $\mathbb{R}$ n'est pas une extention finis de $\mathbb{Q}$

N=° 1.

soit $x \in \mathbf{L}$, alors $\exists a_1, \cdots, a_n \in \mathbf{K}$ tel que, $x = \sum_{i=1}^{n} \alpha_i a_i$

Or on a $\forall i \in [\![1, n]\!], \exists b_1, \cdots, b_p \in k, a_i = \sum_{j=1}^{p} \beta_j b_j$

Ainsi $\exists a_1, \cdots, a_n \in \mathbf{K} \in k, \exists b_1, \cdots, b_p \in k, x = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \alpha_i \beta_j a_i b_j$

Donc x s'écrit d'une manière unique comme des élément de k,
donc la famille $\left(\alpha_i \beta_j\right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ est une base de du k-espace vectoriel $\mathbf{L}$
De plus la famille $\left(\alpha_i \beta_j\right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ comporte exactement np éléments
Donc $\mathbf{L}$ est une extensions finis de k et $[\mathbf{L} : k] = [\mathbf{L} : \mathbf{K}][\mathbf{K} : k]$

Partie II. Éléments algébriques

N=° 1.

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

$$\mathfrak{M} \in \{P(\alpha), P \in \mathbb{K}[X]\} \Leftrightarrow \exists \mathfrak{B}_1, \cdots, \mathfrak{B}_n \in \mathbb{K}\ \mathfrak{M} \subset \sum_{\mathfrak{B}=1}^{n} \mathfrak{B}_{\mathfrak{B}} \alpha^{\mathfrak{B}} \in \mathrm{Vect}_{\mathbb{K}}(\alpha^n, n \in \mathbb{N}) \subset \mathbb{K}[\alpha]$$

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

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

- $1 \in \mathbb{K}[\alpha]$
- $\mathfrak{B} + \mathfrak{C} = P(\alpha) + Q(\alpha) = (P + Q)(\alpha)$ et $P + Q \in \mathbb{K}[X]$
- $\mathfrak{B}\mathfrak{C} = P(\alpha)Q(\alpha) = (PQ)(\alpha)$ et $PQ \in \mathbb{K}[X]$

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

Et $\mathrm{Vect}(\alpha^n, n \in \mathbb{N})$ est le plus petit ensemble stable par $+$ et $\times$,
ce qui fais de luis le plus petit sous-anneau contanant 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 $(1, \alpha, \cdots, \alpha^n)$ soit une famille liée
($\Rightarrow$) Supposons que α est algébrique sur $\mathbb{K}$, alors

$$\exists \mathfrak{M} \in \mathbb{K}[X], \mathfrak{M}(\alpha) = 1 \Leftrightarrow \exists n \in \mathbb{N}, \exists \mathfrak{B}_1, \cdots, \mathfrak{B}_n \in \mathbb{K}, \mathfrak{M}(\alpha) = \sum_{\mathfrak{C}=1}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} = 1$$

$$\text{Donc } -1 + \sum_{\mathfrak{C}=0}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} = \mathfrak{B}_1$$

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

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

$$\exists \mathfrak{B}_1, \cdots, \mathfrak{B}_n \in \mathbb{K}, \exists \mathfrak{N} \in \mathbb{N}, \forall\ \alpha^{\mathfrak{N}} = \sum_{\substack{\mathfrak{C}=1 \\ \mathfrak{C} < \mathfrak{N}}}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}}$$

$$\text{Donc } \sum_{\substack{\mathfrak{C}=1 \\ \mathfrak{C} < \mathfrak{N}}}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} - \forall\ \alpha^{\mathfrak{N}} = 1$$

en posant $-\forall = \mathfrak{B}_{\mathfrak{N}}$, on obtient

$$\sum_{\substack{\mathfrak{C}=1 \\ \mathfrak{C} < \mathfrak{N}}}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} - \forall\ \alpha^{\mathfrak{N}} = \sum_{\mathfrak{C}=1}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} = 1$$

Or $\sum_{\mathfrak{C}=1}^{n} \mathfrak{B}_{\mathfrak{C}} \alpha^{\mathfrak{C}} \in \mathbb{R}[X]$
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 $(1, \alpha, \cdots, \alpha^n)$ est liée

N=° <.

Soit $\mathfrak{I} \in \mathbb{L}$, alors $\mathfrak{I}$ est algébrique de degré $\mathfrak{n}$ sur $\mathbb{K}$ si et seulement si $(\mathfrak{n}, \mathfrak{I})$ est liée
si et seulement si il existe $\mathfrak{A} \in \mathbb{K}, \mathfrak{I} \in \mathfrak{A}\,\mathfrak{M}\,\mathfrak{n} \in \mathfrak{A}$ si et seulement si $\mathfrak{I} \in \mathbb{K}$
Donc on a bien $(\mathfrak{n}, \mathfrak{I})$ liée $\Leftrightarrow \mathfrak{I} \in \mathbb{K}$

N=° X.

Supposons que $\mathbb{L}$ est une extention finie de $\mathbb{K}$ et soit $\mathfrak{I} \in \mathbb{L}$
alors $\mathfrak{I}$ est algébrique sur $\mathbb{K}$ si:

$$a$$

N=° P. a.

On sait par la définitions que $\left(1, \alpha, \cdots, \alpha^{d \vee \mathfrak{n}}\right)$ est libre
Et $\mathrm{Vect}(\alpha^n, n \in \mathbb{N}) \in \mathrm{Vect}(\alpha^n, n \in [\![\mathfrak{n}; d \vee \mathfrak{n}]\!])$
Ainsi $\mathrm{Vect}(\alpha^n, n \in [\![\mathfrak{n}; d \vee \mathfrak{n}]\!])$ est une base de $\mathbb{K}[\alpha]$

b.

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

- linéarité:

Soient $\mathfrak{A} \in \mathbb{K}, \mathfrak{I}, \mathfrak{K} \in \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{A}\,\mathfrak{I} \uparrow \mathfrak{K}) \in \beta\,\mathfrak{A}\,\mathfrak{I} \uparrow \beta\,\mathfrak{K} \in \mathfrak{A}\; f_\beta(\mathfrak{I}) \uparrow f_\beta(\mathfrak{K})$ donc f_β ets linéaire

- bijectivité:

soit $\mathfrak{I} \in \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{I}) \in \mathfrak{F}$
alors $\beta\,\mathfrak{I} \in \mathfrak{F}$ donc $\mathfrak{I} \in \mathfrak{F}$ car $\beta \diamond \mathfrak{F}$
donc $\mathrm{Ker}(f_\beta) \in \{\mathfrak{F}\}$. Donc f_β est injéctive
Et soient $\mathfrak{I}, \mathfrak{K} \in \mathbb{K}[\alpha]$, $f_\beta(\mathfrak{I}) \in \mathfrak{K}$
alors $\mathfrak{I} \in \frac{\mathfrak{K}}{\beta}$ car $\beta \diamond \mathfrak{F}$, 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: $\mathbb{K} \vdash \mathbb{K}[\alpha]$, donc $\mathbb{K}$ est un sous-corps de $\mathbb{K}[\alpha]$
De plus comme $\left(1, \alpha, \cdots, \alpha^{d \vee \mathfrak{n}}\right)$ est une base de $\mathbb{K}[\alpha]$ qui comporte d élément
Ainsi $\mathbb{K}[\alpha]$ est une extensions finie de $\mathbb{K}$, avec $[\mathbb{K}[\alpha] : \mathbb{K}] \in d$

e.

Il est évidant que $\mathbb{Q}\left(\sqrt[\mathfrak{p}]{\mathfrak{P}}\right) \vdash \mathbb{C}$, et commme $\mathbb{Q}$ est un sous groupe et que $\sqrt[\mathfrak{p}]{\mathfrak{P}} \in \mathbb{C}$,
alors par les questions précédente:
$\mathbb{Q}\left(\sqrt[\mathfrak{p}]{\mathfrak{P}}\right)$ est un sous-corps de $\mathbb{C}$

N=° H.

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

ii) $\Rightarrow$ iii) Supposons que α est algébrique sur $\mathbb{K}$, alors
$\exists P \neq \mathbb{K}[X]$, $P(\alpha) = 0$, soit P un telle polynôme, alors:

$$\begin{aligned} P(\alpha) = 0 &\Leftrightarrow \alpha \text{ est racine de } P \\ &\Leftrightarrow \alpha \text{ est racine de } P - 0 \end{aligned}$$

Posons $Q = P - 0$ $Q(X) = P \neq \mathbb{K}[X]$, ainsi $Q(\alpha) = 0$
Et donc α est constructible
iii) $\Rightarrow$ i) Supposons que α est algébrique sur $\mathbb{K}$, alors par la question précédente.
$\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{L}$

Ainsi par un raisonnement cyclique,
on a bien que $\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{L} \Leftrightarrow \alpha$ est constructible $\Leftrightarrow \alpha \in \mathbb{K}[\alpha] \Leftrightarrow \alpha$ est algébrique sur $\mathbb{K}$

Partie III. Polynômes minimal d'un élément algébrique

Question 1.

Si I_α na possède pas une polynôme de degré q,
alors soit $P \in I_\alpha$ de degré q, alors soit a sont coefficient dominant
alors le polynome $\frac{P}{a}$ est de degrés q et sont coefficient dominant vaut 1
De plus $\frac{P}{a}(\alpha) = \frac{P(\alpha)}{a} = \frac{0}{a} = 0$ Donc $\frac{P}{a} \in I_\alpha$
Donc I_α possède un polynôme unitaire de degrés q

Soient $P, Q \in I_\alpha$ deux polynômes unitaire de degrés q
Alors $\exists a_0, \cdots, a_{q-1}, b_0, \cdots, b_{q-1} \in \mathbb{K}$, $P = X^q + \sum_{k=0}^{q-1} a_k X^k$ et $Q = X^q + \sum_{k=0}^{q-1} b_k X^k$
Alors $P(\alpha) - Q(\alpha) = \sum_{k=0}^{q-1} a_k \alpha^k - \sum_{k=0}^{q-1} b_k \alpha^k = 0$
donc $\sum_{k=0}^{q-1} (a_k - b_k)\alpha^k$, et comme $\left(1, \alpha, \cdots, \alpha^{q-1}\right)$ est libre, on a: $\forall k \in [\![0; q-1]\!], a_k = b_k$
Ainsi on a bien $P = Q$
Donc il existe un unique polynome unitaire de degré q dans I_α

Question 2.

Supposons par l'absurde que μ_α est réductible,
alors $\exists P, Q \in \mathbb{K}[X], \mu_\alpha = P \times Q$, soient de tels polynômes
Ainsi $\mu_\alpha(\alpha) = P(\alpha) \times Q(\alpha) = 0$ donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$,
donc α est algébrique de degrés inférieur stricte à d, absurde !
Donc μ_α est irréductible

Soit $P \in I_\alpha$, alors $\exists Q \in \mathbb{K}[X], P = \mu_\alpha \times Q$ car $P(\alpha) = 0$, ainsi $I_\alpha = \{\mu_\alpha \times P, P \in \mathbb{K}[X]\}$
Et soit $\exists Q \in \mathbb{K}[X], P = \mu_\alpha \times Q$, alors $P(\alpha) = (\mu_\alpha \times Q)(\alpha) = \mu_\alpha(\alpha) \times Q(\alpha) = 0$,
donc $P \in I_\alpha$ et donc $\{\mu_\alpha \times Q, Q \in \mathbb{K}[X]\} = I_\alpha$
Ainsi par double inclusion $\{\mu_\alpha \times Q, Q \in \mathbb{K}[X]\} = I_\alpha$