1. Soit $\alpha \in \mathbb{C}$. Comme l'application

$$[P \mapsto P(\alpha)]$$

est un morphisme d'anneaux de $\mathbb{Q}[X]$ dans $\mathbb{C}$, le noyau

$$I_\alpha = \left\{P \in \mathbb{Q}[X] \ : \ P(\alpha) = 0\right\}$$

de cette application est bien un idéal de $\mathbb{Q}[X]$, dit **idéal annulateur** de α.

Si le nombre α est supposé algébrique, alors l'idéal I_α n'est pas réduit au polynôme nul et il existe alors un unique polynôme unitaire Π qui engendre cet idéal et en particulier tel que $\Pi(\alpha) = 0$: le **polynôme minimal** de α.

► Vérifions maintenant que le polynôme minimal est irréductible.

Si le polynôme minimal Π admet une factorisation $\Pi = P.Q$ où P et Q sont des polynômes à coefficients rationnels, alors

$$\Pi(\alpha) = P(\alpha).Q(\alpha) = 0$$

et comme $\mathbb{C}$ est un corps, alors $P(\alpha) = 0$ ou $Q(\alpha) = 0$.

Supposons (par exemple) que $P(\alpha) = 0$. Dans ce cas, $P \in I_\alpha$ et en particulier Π divise P. Mais P divise Π par définition, donc P et Π sont associés et le cofacteur Q est inversible.

Cela prouve que Π est irréductible dans $\mathbb{Q}[X]$.

✍ *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Les polynômes irréductibles de $\mathbb{R}[X]$ sont d'une part les polynômes de degré 1 et d'autre part les polynômes de degré 2 dont le discriminant est strictement négatif.

En revanche, il existe dans $\mathbb{Q}[X]$ des polynômes irréductibles de degré arbitrairement grand...

► Supposons pour finir qu'il existe un polynôme irréductible et unitaire P tel que $P(\alpha) = 0$. Ce polynôme appartient à I_α, donc il est divisible par le polynôme minimal Π, qui est irréductible et unitaire. Par conséquent, $P = \Pi$.

✍ *Un polynôme irréductible P n'est divisible que par deux types de polynômes : les polynômes inversibles (= les polynômes constants non nuls) et les polynômes qui lui sont associés.*

Il existe donc un, et un seul, polynôme irréductible et unitaire Π tel que $\Pi(\alpha) = 0$ et c'est le polynôme minimal de α.

2. Il est clair que

$$\mathbb{Q}_{d-1}[\alpha] \subset \mathbb{Q}[\alpha].$$

Réciproquement, soit $x \in \mathbb{Q}[\alpha]$: il existe donc un polynôme $P \in \mathbb{Q}[X]$ tel que $x = P(\alpha)$. Effectuons la division euclidienne de P par Π (polynôme unitaire et donc non nul) :

$$P = Q.\Pi + R$$

avec $\deg R < \deg \Pi = d$ et donc $R \in \mathbb{Q}_{d-1}[X]$.

En substituant α à X, on en déduit que

$$x = P(\alpha) = Q(\alpha).\Pi(\alpha) + R(\alpha) = R(\alpha) \in \mathbb{Q}_{d-1}[\alpha].$$

Par double inclusion, on a démontré que

$$\mathbb{Q}_{d-1}[\alpha] = \mathbb{Q}[\alpha].$$

✍ *On en déduit que, en tant que sous-espace vectoriel de $\mathbb{C}$ (considéré comme un espace vectoriel sur le corps $\mathbb{Q}$), le sous-espace $\mathbb{Q}[\alpha]$ est engendré par la famille finie*

$$(1, \alpha, \dots, \alpha^{d-1})$$

et que sa dimension est par conséquent finie, inférieure à d.

Plus précisément, si la famille

$$(1, \alpha, \dots, \alpha^{d-1})$$

était liée dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha]$, alors il existerait une famille

$$(q_0, \dots, q_{d-1}) \neq (0, \dots, 0)$$

dans $\mathbb{Q}^d$ telle que

$$\sum_{k=0}^{d-1} q_k \alpha^k = 0$$

et le polynôme

$$\sum_{k=0}^{d-1} q_k X^k \in \mathbb{Q}[X]$$

serait un polynôme annulateur non nul de α dont le degré serait inférieur à $(d-1)$ et donc strictement inférieur au degré du polynôme minimal de α : impossible !

Donc $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = d = \deg \Pi$.

3. On sait que $\mathbb{Q}[\alpha]$ est la sous-algèbre de $\mathbb{C}$ engendrée par α, donc c'est en particulier un sous-anneau de $(\mathbb{C}, +, \times)$.

Soit $x_0 \in \mathbb{Q}[\alpha]$, non nul.

✍ *En tant que nombre complexe non nul, x_0 est inversible : il existe un nombre complexe x_1 tel que $x_0.x_1 = 1$. Mais pour le moment, on ne sait pas si x_1 appartient, ou pas, à $\mathbb{Q}[\alpha]$.*

L'application

$$[x \mapsto x_0.x]$$

est clairement un endomorphisme de $\mathbb{Q}[\alpha]$. Comme $x_0 \neq 0$ et que $\mathbb{Q}[\alpha] \subset \mathbb{C}$, le noyau de cet endomorphisme est réduit à $\{0\}$. Comme $\mathbb{Q}[\alpha]$ est un espace vectoriel de dimension finie, cet endomorphisme est donc un automorphisme et il existe en particulier un élément $x_1 \in \mathbb{Q}[\alpha]$ tel que

$$x_0.x_1 = 1.$$

Donc x_0 est bien inversible en tant qu'élément de l'anneau $\mathbb{Q}[\alpha]$.

Ainsi $\mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$ dans lequel tout élément distinct de 0 admet un inverse : c'est bien un sous-corps de $\mathbb{C}$.

✍ *Si on* admet *que tous les éléments de $\mathbb{Q}[\alpha]$ sont également des nombres algébriques, alors tout élément non nul de $\mathbb{Q}[\alpha]$ admet un polynôme minimal unitaire et irréductible (comme on l'a démontré pour α).*

Le seul polynôme unitaire et irréductible divisible par X est X lui-même, c'est-à-dire le polynôme minimal de 0.

Si $x_0 \neq 0$ est algébrique, alors son polynôme minimal est irréductible et non divisible par X, donc son coefficient constant est différent de 0 :

$$\exists\, (q_0, q_1, \dots, q_r) \in \mathbb{Q}^{r+1}, \quad q_r x_0^r + \cdots + q_1 x_0 + \underbrace{q_0}_{\neq 0} = 0$$

et par conséquent

$$x_0 \underbrace{\left(\sum_{k=1}^{r} \frac{-q_k}{q_0} \cdot x_0^{k-1} \right)}_{\in \mathbb{Q}[x_0] \subset \mathbb{Q}[\alpha]} = 1$$

ce qui prouve que x_0 est inversible dans $\mathbb{Q}[\alpha]$.