Théorème de l'élément primitif

Pour des sous-corps de $\mathbb{C}$

Soit $\mathbb{K} \subseteq \mathbb{L}(\subseteq \mathbb{C})$ une extension de corps de degrès finie. Alors on dispose de $\alpha \in \mathbb{L}$ tel que:

$$\mathbb{K}[\alpha] = \mathbb{L}$$

Lemme : *(Prolongement des morphismes)*

Soit $\mathbb{K} \subseteq \mathbb{C}$ une extension finie et $\varphi \in (\mathbb{K} \longrightarrow \mathbb{C})$ un morphisme de corps. Alors φ se prolonge à $\mathbb{L}$ en un morphisme $\mathbb{K}$ linéaire de $[\mathbb{L} : \mathbb{K}]$ manières différentes.

Preuve :

On le prouve par réccurence sur $[\mathbb{L} : \mathbb{K}]$

Initialisation : Pour $[\mathbb{L} : \mathbb{K}] = 1$ le résultat est évident.

Hérédité : Supposons $d > 1$ tel que pour tout $k < d$, si $[\mathbb{L} : \mathbb{K}] = k$ le résultat tienne.

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extensions de degrès d et $\varphi \in (\mathbb{K} \longrightarrow \mathbb{C})$ un morphisme. Considérons $\alpha \in \mathbb{L} \setminus \mathbb{K}$ (possible car $d > 1$). On a la suite d'extension suivante:

$$\mathbb{K} \subset \mathbb{K}[\alpha] \subseteq \mathbb{L}$$

La base téléscopique donne:

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}[\alpha]][\mathbb{K}[\alpha] : \mathbb{K}]$$

Cas 1 : $[\mathbb{K}[\alpha] : \mathbb{K}] = d$

On a donc $\mathbb{L} = \mathbb{K}[\alpha]$. On considère:

$$\begin{aligned} \cdot^{\varphi} : \mathbb{K}[X] &\longrightarrow \mathbb{C}[X] \\ \sum_{k=0}^{n} a_k X^k &\longmapsto \sum_{k=0}^{n} \varphi(a_k) X^k \end{aligned}$$

C'est un morphisme d'anneau. On note π_α le polynome minimal de α sur $\mathbb{K}$ qui est donc de degrés $[\mathbb{L} : \mathbb{K}]$ et à racine simple dans $\mathbb{C}$

Pour chaque racine $z \in \mathbb{C}$ de π_α^φ on considère:

$$\begin{aligned} \varphi_z : \mathbb{L} &\longrightarrow \mathbb{C} \\ P(\alpha) &\longmapsto P^{\varphi}(z) \end{aligned}$$

On vérifie aisaiment que φ_z est un morphisme de corps $\mathbb{K}$-linéaire et que $(\varphi_z)_{|\mathbb{K}} = \varphi$ De plus les φ_z sont distinct pour $z \in \mathrm{Rac}(\pi_\alpha^\varphi)$ ce qui permet de conclure.

Cas 2: $[\mathbb{K}[\alpha] : \mathbb{K}] < d$

On a donc, comme $[\mathbb{K}[\alpha] : \mathbb{K}] > 1$ que $[\mathbb{K}[\alpha] : \mathbb{K}] < d$ et $[\mathbb{L} : \mathbb{K}[\alpha]] < d$

L'hypothèse de réccurence permet donc de prolonger φ à $\mathbb{K}[\alpha]$ puis de prolonger les prolongements à $\mathbb{L}$ du bon nombre de manière grâce à la base téléscopique.

$\square$

Preuve :*(Du théorème)*

Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de degrès fini. Notons $\mathcal{A} := \{\alpha \in \mathbb{L} \mid \mathbb{K}[\alpha] \neq \mathbb{L}\}$

On note $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{C})$ l'ensemble des morphismes de corps de $\mathbb{L}$ dans $\mathbb{C}$ qui sont $\mathbb{K}$-linéaire. Montrons que:

$$\mathcal{A} \subseteq \bigcup_{\substack{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{C}) \\ \sigma \neq \mathrm{id}}} \mathrm{Ker}(\sigma - \mathrm{id})$$

Soit $\alpha \in \mathcal{A}$. Comme $[\mathbb{L} : \mathbb{K}[\alpha]] > 1$, l'injection de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ se prolonge en plus d'une manière en un morphisme $\mathbb{K}[\alpha]$-linéaire de $\mathbb{L}$ dans $\mathbb{C}$. Notons σ un de ses prolongements qui soit différent de l'injection de $\mathbb{L}$ dans $\mathbb{C}$. Ainsi:

$$\sigma \neq \mathrm{id}_{\mathbb{L}}$$
$$\sigma(\alpha) = \alpha$$

Par suite, comme σ est $\mathbb{K}[\alpha]$-linéaire, il est en particulier $\mathbb{K}$-linéaire et ainsi, comme $\alpha \in \mathrm{Ker}(\sigma - \mathrm{id})$,

$$\alpha \in \bigcup_{\substack{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{C}) \\ \sigma \neq \mathrm{id}}} \mathrm{Ker}(\sigma - \mathrm{id})$$

Aussi, $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{C})| = [\mathbb{L} : \mathbb{K}]$ et chaque $\mathrm{Ker}(\sigma - \mathrm{id})$ est un sous $\mathbb{K}$-espace vectoriel stricte de $\mathbb{L}$ (car $\sigma \neq \mathrm{id}$). Par suite, $\mathcal{A}$ est inclus dans une réunion finie de fermé d'intérieur vide et ainsi $\mathcal{A}$ est lui aussi d'intérieur vide. Finalement, on dipose de $\alpha \in \mathbb{L} \setminus \mathcal{A}$ et celui-ci vérifie donc:

$$\mathbb{K}[\alpha] = \mathbb{L}$$

□