NOMBRE DE MORPHISMES DE K-ALGÈBRES À VALEURS DANS UNE EXTENSION DE K

G.BERHUY

Table des matières

1. Un résultat d'algèbre commutative 1
2. Rappels sur les K-algèbres 2
3. K-algèbres de dimension finie 4
4. Énoncé et démonstration du résultat principal 6

Il est bien connu que si E/K est une extension de corps de degré fini, alors il existe au plus $[E : K]$ morphismes de K-algèbres $E \longrightarrow \overline{K}$, et on a égalité si et seulement si E/K est une extension séparable (cf. définition 4.1). On redonnera d'ailleurs une démonstration de ce fait.

Le but de ce texte est de généraliser ce résultat, et d'établir l'inégalité

$$|\mathrm{Hom}_{K-alg}(\mathcal{A}, L)| \leq \dim_K(\mathcal{A}),$$

pour toute extension L/K, et toute K-algèbre $\mathcal{A}$ associative unitaire de dimension finie. On examinera aussi le cas d'égalité lorsque $L = \overline{K}$.

1. Un résultat d'algèbre commutative

Dans ce paragraphe, on démontre un résultat classique d'algèbre commutative. Commençons par rappeler la définition d'un élément nilpotent.

Définition 1.1. Soit A un anneau. Un élément $a \in A$ est *nilpotent* s'il existe $n \geq 1$ tel que $a^n = 0$. L'ensemble des éléments nilpotents est noté $\mathrm{Nil}(A)$.

Le but de ce paragraphe est de démontrer le théorème suivant.

Théorème 1.2. *Soit A un anneau commutatif. Alors,* $\mathrm{Nil}(A)$ *est l'intersection des idéaux premiers de A.*

En particulier, $\mathrm{Nil}(A)$ *est un idéal de A.*

Démonstration. L'égalité à démontrer se récrit $\bigcup_{\mathfrak{p}} A \setminus \mathfrak{p} = A \setminus \mathrm{Nil}(A)$.

Date: 6 février 2024.

On commence par démontrer l'inclusion la plus facile, à savoir $\bigcup_{\mathfrak{p}} A \setminus \mathfrak{p} \subset A \setminus \mathrm{Nil}(A)$.

Soit $a \in \bigcup_{\mathfrak{p}} A \setminus \mathfrak{p}$. Il existe donc un idéal premier $\mathfrak{p}$ tel que $a \in A \setminus \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, $A \setminus \mathfrak{p}$ est stable par produit. Une récurrence immédiate montre alors que pour tout $n \geq 1$, on a $a^n \in A \setminus \mathfrak{p}$. En particulier, $a^n \neq 0$ pour tout $n \geq 1$. Ainsi, $x \in A \setminus \mathrm{Nil}(A)$.

L'autre inclusion est plus délicate. On commence par remarquer si $\alpha \in A$ est tel que $\alpha X + 1 \in A[X]^\times$, alors $\alpha \in \mathrm{Nil}(A)$.

En effet, supposons que $\alpha X + 1 \in A[X]^\times$, et soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ tel que $(\alpha X + 1)P = 1$. On a donc

$$1 = \sum_{k=0}^{n} \alpha a_k X^{k+1} + \sum_{k=0}^{n} a_k X^k = a_0 + \sum_{k=1}^{n} (\alpha a_{k-1} + a_k) X^k + \alpha a_n X^{n+1}.$$

On en déduit que $a_0 = 1$, $a_k = (-\alpha) a_{k-}$ pour tout $k_i n \, [\![1, n]\!]$ et $\alpha a_n = 0$. Les deux premières équations montrent que $a_n = (-\alpha)^n$. La dernière implique alors que $(-1)^n \alpha^{n+1} = 0$, donc que $\alpha^{n+1} = 0$. Par conséquent, $\alpha \in \mathrm{Nil}(A)$.

On va maintenant montrer l'inclusion manquante. Soit $\alpha \in A \setminus \mathrm{Nil}(A)$. Il faut démontrer l'existence d'un idéal premier $\mathfrak{p}$ de A tel que $\alpha \in A \setminus \mathfrak{p}$. D'après ce qui précède, $\alpha X + 1$ n'est pas inverisble. En particulier, l'idéal $(\alpha X + 1)$ est distinct de $A[X]$, donc contenu dans un idéal maximal $\mathfrak{m}$. Soit $f : A \longrightarrow A[X]/\mathfrak{m}$ le morphisme évident, et soit $\mathfrak{p} = \mathrm{Ker}(f)$. Alors, f induit un morphisme d'anneaux injectif $A/\mathfrak{p} \longrightarrow A[X]/\mathfrak{m}$, et $A/\mathfrak{p}$ est donc isomorphe à un sous-anneau de $A[X]/\mathfrak{m}$. Comme $\mathfrak{m}$ est maximal, $A[X]/\mathfrak{m}$ est un corps, donc intègre. Par conséquent, $A/\mathfrak{p}$ est aussi intègre, et $\mathfrak{p}$ est un idéal premier.

Nous affirmons que $\alpha \in A \setminus \mathfrak{p}$. Dans le cas contraire, on a $\alpha \in \mathfrak{p} = \mathrm{Ker}(f)$, ce qui signifie que $\alpha \in \mathfrak{m}$. Mais, $\alpha X + 1 \in \mathfrak{m}$, et par suite $1 = (\alpha X + 1) + (-X)\alpha \in \mathfrak{m}$, ce qui est impossible car $\mathfrak{m}$ est maximal, donc distinct de $A[X]$. Ceci achève la démonstration. □

Remarque 1.3. Si A est un anneau commutatif, on peut démontrer de manière directe que $\mathrm{Nil}(A)$ est un idéal de A.

Dans tout ce qui suit, K est un corps.

2. Rappels sur les K-algèbres

Définition 2.1. Une *K-algèbre* est un couple $(\mathcal{A}, \mu)$, où $\mathcal{A}$ un K-espace vectoriel, et $\mu : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ est une application K-bilinéaire.

L'application μ est appelée *loi produit* sur $\mathcal{A}$, et $\mu(x, y)$ est plutôt noté xy. On dit que $(\mathcal{A}, \mu)$ est *associative, resp. commutative,* si la loi produit est associative, resp. commutative, et *unitaire* s'il existe un élément neutre pour la loi produit (nécessairement unique), que l'on note généralement $1_{\mathcal{A}}$.

Un morphisme de K-algèbres $f : \mathcal{A} \longrightarrow \mathcal{B}$ est une application K-linéaire vérifiant

$$f(xy) = f(x)f(y) \quad \text{pour tous } x, y \in \mathcal{A}.$$

Si $\mathcal{A}$ et $\mathcal{B}$ sont unitaires, on exige de plus que $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.

L'ensemble des morphismes de K-algèbres $f : \mathcal{A} \longrightarrow \mathcal{B}$ est un K-espace vectoriel, que l'on note $\mathrm{Hom}_{K-alg}(\mathcal{A}, \mathcal{B})$.

Remarque 2.2. Toute K-algèbre associative unitaire $\mathcal{A}$ est en particulier un anneau, où l'addition est la loi d'addition du K-espace vectoriel $\mathcal{A}$, et la loi produit est la loi produit μ, le neutre pour le produit étant $1_{\mathcal{A}}$. Un morphisme de K-algèbres associatives unitaires est alors un morphisme d'anneau.

Définition 2.3. Soit $\mathcal{A}$ une K-algèbre. Un *idéal* de $\mathcal{A}$ est un sous-espace vectoriel $\mathcal{I}$ tel que pour tout $x \in \mathcal{I}$, et pour tout $a \in \mathcal{A}$, on a $ax \in \mathcal{I}$ et $xa \in \mathcal{I}$.

Si $\mathcal{I}$ est un idéal de $\mathcal{A}$, la loi externe $K \times \mathcal{A} \longrightarrow \mathcal{A}$ induit alors une loi externe

$$\begin{aligned} K \times \mathcal{A}/\mathcal{I} &\longrightarrow \mathcal{A}/\mathcal{I} \\ (\lambda, \overline{x}) &\longmapsto \lambda \cdot \overline{x} = \overline{\lambda \cdot x} \end{aligned}$$

bien définie, et muni $\mathcal{A}/\mathcal{I}$ d'une structure de K-espace vectoriel.

On montre alors que la loi produit $\mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ induit alors une loi interne

$$\begin{aligned} \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} &\longrightarrow \mathcal{A}/\mathcal{I} \\ (\overline{x}, \overline{y}) &\longmapsto \overline{x}\ \overline{y} = \overline{xy} \end{aligned}$$

bien définie, et munit $\mathcal{A}/\mathcal{I}$ d'une structure de K-algèbre, qui est unitaire, resp. associative, resp. commutative dès que $\mathcal{A}$ l'est. De plus, la projection canonique $\pi : \mathcal{A} \longrightarrow \mathcal{A}/\mathcal{I}$ est un morphisme de K-algèbres.

On a alors le résultat suivant, qui se démontre comme pour les anneaux quotients.

Théorème 2.4. *Soit $\mathcal{A}$ une K-algèbre, et soit $\mathcal{I}$ un idéal de $\mathcal{A}$. Alors, pour tout morphisme de K-algèbres $f : \mathcal{A} \longrightarrow \mathcal{B}$ tel que $\mathcal{I} \subset \mathrm{Ker}(f)$, il existe un unique morphisme de K-algèbres $\overline{f} : \mathcal{A}/\mathcal{I} \longrightarrow \mathcal{B}$ tel que $f = \overline{f} \circ \pi$.*

De plus, on a un isomorphisme de K-espaces vectoriels

$$\mathrm{Hom}_{K-alg}(\mathcal{A}/\mathcal{I}, \mathcal{B}) \simeq \mathcal{H} = \{f \in \mathrm{Hom}_{K-alg}(\mathcal{A}/\mathcal{I}, \mathcal{B}) \mid \mathcal{I} \subset \mathrm{Ker}(f)\},$$

les isomorphismes étant donnés par

$$\begin{array}{ccc} \mathrm{Hom}_{K-alg}(\mathcal{A}/\mathcal{I}, \mathcal{B}) & & \mathcal{H} \\ \varphi & \longmapsto & \varphi \circ \pi \\ \overline{f} & \longleftarrow & f \end{array}$$

La remarque suivante est élémentaire, mais particulièrement importante.

Remarque 2.5. Soit $\mathcal{A}$ une K-algèbre associative unitaire. Alors, les idéaux de la K-algèbre $\mathcal{A}$ sont exactement les idéaux de l'anneau $\mathcal{A}$.

En effet, par définition, si $\mathcal{I}$ est un idéal de la K-algèbre $\mathcal{A}$, c'est un idéal de l'anneau $\mathcal{A}$, puisque les lois de l'anneau $\mathcal{A}$ sont les lois de l'algèbre $\mathcal{A}$.

Pour la réciproque, il reste à montrer qu'un idéal $\mathcal{I}$ de l'anneau $\mathcal{A}$ est nécessairement un sous-espace vectoriel. Or, la bilinéarité du produit implique que, pour tout $x \in \mathcal{A}$, et tout $\lambda \in K$, on a

$$\lambda \cdot x = \lambda \cdot (1_{\mathcal{A}} x) = (\lambda \cdot 1_{\mathcal{A}}) x.$$

En particulier, pour tous $x, y \in \mathcal{I}$, et tout $\lambda \in K$, on a

$$\lambda \cdot x + y = (\lambda \cdot 1_{\mathcal{A}}) x + y \in \mathcal{I}.$$

Exemples 2.6. Soit K un corps.

(1) Toute extension de corps L/K est une K-algèbre associative unitaire commutative, la loi externe $K \times L \longrightarrow L$ étant induite par le produit dans L.
(2) L'anneau des polynômes $K[X]$ est une K-algèbre associative unitaire commutative. D'après la remarque précédente, il en est de même de l'anneau quotient $K[X]/(P)$, où $P \in K[X]$.
(3) Pour tout $n \geq 1$, $\mathrm{M}_n(K)$ est une K-algèbre associative unitaire, non commutative dès que $n \geq 2$.

3. K-algèbres de dimension finie

Dans tout ce qui suit, pour éviter une lourdeur d'écriture, le terme « K-algèbre » signifiera « K-algèbre associative unitaire ». En particulier, les notions d'idéal de $\mathcal{A}$ en tant qu'algèbre ou qu'anneau coïncident, si bien que lorsque l'on considérera des idéaux, on ne précisera pas pour quelle structure.

On alors alors le lemme suivant.

Lemme 3.1. *Soit$\mathcal{A}$ une K-algèbre de dimension finie. Alors, pour tout idéal $\mathcal{I}$ de $\mathcal{A}$, $\mathcal{A}/\mathcal{I}$ est une K-algèbre de dimension finie, et on a*

$$\dim_K(\mathcal{A}/\mathcal{I}) = \dim_K(\mathcal{A}) - \dim_K(\mathcal{A}).$$

En particulier, on a

$$\dim_K(\mathcal{A}/\mathcal{I}) \leq \dim_K(\mathcal{A}),$$

avec égalité si et seulement si $\mathcal{I} = 0$.

Démonstration. Comme $\mathcal{I}$ est en particulier un sous-espace vectoriel de $\mathcal{A}$, il admet un supplémentaire V dans $\mathcal{A}$. On a donc $\mathcal{A} = \mathcal{I} \oplus V$. Or, la projection sur V est K-linéaire, surjective, de noyau $\mathcal{I}$, et induit donc par passage au quotient un isomorphisme de K-espaces vectoriels $\mathcal{A}/\mathcal{I} \simeq V$. Ainsi, $\mathcal{A}/\mathcal{I}$ est de dimension finie, puisque V l'est, et on a

$$\dim_K(\mathcal{A}/\mathcal{I}) = \dim_K(V) = \dim_K(\mathcal{A}) - \dim_K(\mathcal{I}).$$

La dernière partie découle aisément de cette égalité. □

Dans ce paragraphe, on démontre un théorème de structure sur les K-algèbres commutatives de dimension finie sans éléments nilpotents non triviaux.

Le théorème que l'on a en vue est le suivant.

Théorème 3.2. *Toute K-algèbre commutative de dimension finie sans éléments nilpotents non nuls est isomorphe à un produit direct d'un nombre fini d'extensions de K de degrés finis.*

La démonstration étant un peu technique, on la découpe en plusieurs résultats intermédiaires. La première étape consiste à démontrer que tout idéal premier est maximal.

Lemme 3.3. *Toute K-algèbre intègre de dimension finie est un corps.*

Démonstration. Soit $\mathcal{B}$ une telle K-algèbre. Comme $\mathcal{B}$ est intègre, elle est commutative non triviale. Soit $b \in \mathcal{B} \setminus \{0\}$. On vérifie aisément que l'application

$$\begin{aligned} \mathcal{B} &\longrightarrow \mathcal{B} \\ x &\longmapsto xb \end{aligned}$$

est K-linéaire. Puisque $\mathcal{B}$ est intègre, elle est injective, et comme $\mathcal{B}$ est de dimension finie, elle est bijective. Il existe donc $x \in \mathcal{B}$ tel que $xb = 1_{\mathcal{B}}$, et b est donc inversible, d'où le résultat. □

Corollaire 3.4. *Soit $\mathcal{A}$ une K-algèbre commutative de dimension finie. Alors tout idéal premier est maximal.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{A}$. Alors, $\mathcal{A}/\mathfrak{p}$ est une K-algèbre commutative intègre de dimension finie, donc un corps par le lemme précédent. Ainsi, $\mathfrak{p}$ est maximal. □

L'étape suivante est de démontrer qu'une K-algèbre commutative de dimension finie ne possède qu'un nombre fini d'idéaux premiers. Cela s'appuie sur le résultat suivant.

Lemme 3.5. *Soit $\mathcal{A}$ une K-algèbre commutative de dimension finie, et soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux comaximaux. Si $\mathcal{I} \cap \mathcal{J} = \mathcal{I}$, alors $\mathcal{J} = \mathcal{A}$.*

Démonstration. On démontre facilement que l'isomorphisme d'anneaux donné par le théorème chinois est K-linéaire. On a donc un isomorphisme de K-algèbres

$$\mathcal{A}/\mathcal{I} \cap \mathcal{J} \simeq \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{J}.$$

En particulier, on a

$$\dim_K(\mathcal{A}/\mathcal{I} \cap \mathcal{J}) = \dim_K(\mathcal{A}/\mathcal{I}) + \dim_K(\mathcal{A}/\mathcal{J}).$$

L'hypothèse entraîne alors que $\dim_K(\mathcal{A}/\mathcal{J}) = 0$. On a donc $\mathcal{A}/\mathcal{J} = 0$, d'où $\mathcal{J} = \mathcal{A}$. □

On peut alors démontrer le résultat suivant.

Lemme 3.6. *Soit $\mathcal{A}$ une K-algèbre commutative de dimension finie. Alors, deux idéaux premiers distincts sont comaximaux.*

De plus, $\mathcal{A}$ ne possède qu'un nombre fini d'idéaux premiers.

Démonstration. Soient $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers distincts. Ces idéaux sont maximaux par le corollaire 3.4. Or, $\mathfrak{p} + \mathfrak{p}'$ est un idéal de $\mathcal{A}$ contenant

strictement $\mathfrak{p}$ ou $\mathfrak{p}'$ (puisqu'un des deux ensembles $\mathfrak{p}' \setminus \mathfrak{p}$ ou $\mathfrak{p} \setminus \mathfrak{p}'$ est non vide). Par maximalité de $\mathfrak{p}$ et $\mathfrak{p}'$, on a $\mathfrak{p} + \mathfrak{p}' = \mathcal{A}$.

Soient maintenant $\mathfrak{p}_1, \ldots, \mathfrak{p}_{r+1}$ des idéaux premiers deux à deux distincts, avec $r \geq 1$. Alors, $\mathfrak{p}_1, \ldots, \mathfrak{p}_{r+1}$ sont deux à deux comaximaux par ce qui précède. Il est alors bien connu que $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ et $\mathfrak{p}_{r+1}$ sont aussi comaximaux. Comme $\mathfrak{p}_{r+1} \neq \mathcal{A}$, le lemme 3.5 montre que $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{r+1} \subsetneq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$. Puisqu'un idéal de $\mathcal{A}$ est un sous-espace vectoriel de dimension finie, on a alors

$$\dim_K(\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{r+1}) < \dim_K(\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r).$$

Si $\mathcal{A}$ possédait une infinité d'idéaux premiers, on obtiendrait grâce à l'inégalité précédente une suite infinie d'entiers positifs strictement décroissante, ce qui est impossible, d'où le résultat voulu. □

On peut maintenant démontrer le théorème 3.2.

Démonstration. [du théorème 3.2] Soit $\mathcal{A}$ une K-algèbre commutative de dimension finie telle que $\mathrm{Nil}(\mathcal{A}) = 0$. D'après le lemme 3.6, $\mathcal{A}$ possède un nombre fini d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. D'après le théorème 1.2, on a alors $\mathrm{Nil}(\mathcal{A}) = 0 = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$. Puisque ces idéaux premiers sont deux à deux comaximaux par le lemme 3.6, le théorème chinois fournit un isomorphisme de K-algèbres

$$\mathcal{A} \simeq \mathcal{A}/(0) \simeq \mathcal{A}/\mathfrak{p}_1 \times \cdots \times \mathcal{A}/\mathfrak{p}_r.$$

Comme les $\mathfrak{p}_i$ sont maximaux d'après le corollaire 3.4, chaque $\mathcal{A}/\mathfrak{p}_i$ est un corps qui contient un sous-corps isomorphe à K, puisque le morphisme de K-algèbres

$$\begin{aligned} K &\longrightarrow \mathcal{A}/\mathfrak{p}_i \\ \lambda &\longmapsto \overline{\lambda} \end{aligned}$$

est nécessairement injectif (car K est un corps et $\mathcal{A}/\mathfrak{p}_i$ est non trivial). Un tel corps est isomorphe à une extension de K (i.e. un corps contenant K comme sous-corps) par le tour de passe passe ensembliste habituel. Puisque $\mathcal{A}$ est de dimension finie, chaque $\mathcal{A}/\mathfrak{p}_i$ aussi, et on a fini. □

4. Énoncé et démonstration du résultat principal

Comme dans le paragraphe précédent, « K-algèbre » signifiera « K-algèbre associative unitaire ».

Avant d'énoncer le théorème que l'on a en vue, rappelons une définition utile.

Définition 4.1. Une extension de corps E/K est dite *séparable* si elle est algébrique, et si pour tout $\alpha \in E$, son polynôme minimal $\mu_{\alpha,K}$ n'a que des racines simples dans $\overline{K}$.

Remarque 4.2. Si E/K est séparable, alors pour toute sous-extension M/K de E/K, l'extension E/M est séparable.

En effet, cela provient du simple fait que pour tout $\alpha \in E$, on a $\mu_{\alpha,M} \mid \mu_{\alpha,K}$.

Le but de ce paragraphe est de démontrer le théorème suivant.

Théorème 4.3. *Soit L/K une extension de corps, et soit $\mathcal{A}$ une K-algèbre de dimension finie. Alors, $|\mathrm{Hom}_{K-alg}(\mathcal{A}, L)| \leq \dim_K(\mathcal{A})$.*

De plus, on a $|\mathrm{Hom}_{K-alg}(\mathcal{A}, \overline{K})| \leq \dim_K(\mathcal{A})$ si et seulement si $\mathcal{A}$ est isomorphe à un produit direct d'extensions séparables de K de degrés finis.

Encore une fois, nous découperons la démonstration en plusieurs parties. On commence par le cas particulier d'une extension E/K de degré fini. Tout le jeu consistera ensuite à se ramener à ce cas.

Remarque 4.4. Le théorème 4.5, le lemme 4.6 et la proposition 4.7 sont des résultats très classiques, et qui sont en principe démontrés dans un cours clasique de théorie des corps. Le lecteur familier déjà familier avec cette théorie peut passer directement au lemme 4.8 sans nuire à sa compréhension de la suite.

L'outil essentiel pour régler le cas des extensions finies est le théorème de prolongement des isomorphismes.

Notation. Si $\rho : A \longrightarrow B$ est un morphisme d'anneaux commutatifs, il existe un unique morphisme d'anneaux $A[X] \longrightarrow B[X]$ prolongeant ρ et envoyant X sur X. Si $P \in A[X]$, on note alors $\rho(P)$ son image par le morphisme précédent.

Autrement dit, si $P = \sum_{n\geq 0} a_n X^n \in A[X]$, on a $\rho(P) = \sum_{n\geq 0} \rho(a_n) X^n \in B[X]$.

Le théorème de prolongement des isomorphismes s'énonce alors comme suit.

Théorème 4.5 (de prolongement des isomorphismes)**.** *Soit E/K une extension, et soit $\alpha \in E$ un élément algébrique sur K. Soit L un corps quelconque, et soit $\iota : K \longrightarrow L$ un morphisme d'anneaux. Alors, l'ensemble des morphismes d'anneaux $\sigma : K(\alpha) \longrightarrow L$ prolongeant ι est en bijection avec l'ensemble des racines*[1] *de $\iota(\mu_{\alpha,K})$ dans L.*

Plus précisément :

(1) *pour tout morphisme d'anneaux $\sigma : K(\alpha) \longrightarrow L$ prolongeant ι, $\sigma(\alpha)$ est une racine de $\iota(\mu_{\alpha,K})$ dans L ;*

(2) *pour toute racine $\beta \in L$ de $\iota(\mu_{\alpha,K})$, il existe un unique morphisme d'anneaux $\sigma_\beta : K(\alpha) \longrightarrow M$ tel que*

$$\sigma_\beta(\alpha) = \beta \quad \text{et} \quad \sigma_{\beta|_K} = \iota.$$

Il est défini par

$$\sigma_\beta\big(P(\alpha)\big) = \iota(P)(\beta), \qquad \text{pour tout } P \in K[X];$$

(3) *les deux applications*

$$\begin{array}{ccc} \sigma & \longmapsto & \sigma(\alpha) \\ \sigma_\beta & \longleftarrow & \beta \end{array}$$

sont bijectives, et inverses l'une de l'autre.

1. S'il en existe !

Démonstration. Soit $\sigma : K(\alpha) \longrightarrow L$ un morphisme d'anneaux prolongeant le morphisme $\iota : K \longrightarrow L$. Pour tout $P \in K[X]$, on a

$$\sigma\big(P(\alpha)\big) = \sigma(P)\big(\sigma(\alpha)\big), \quad \text{pour tout } P \in K[X].$$

Comme $P \in K[X]$ et que σ prolonge ι, cette égalité se récrit

$$\sigma\big(P(\alpha)\big) = \iota(P)\big(\sigma(\alpha)\big), \quad \text{pour tout } P \in K[X]. \qquad (*)$$

En appliquant cela à $P = \mu_{\alpha,K}$, on obtient que $\sigma(\alpha) \in L$ est une racine de $\iota(\mu_{\alpha,K}) \in L[X]$, d'où (1).

Montrons (2). Soit $\beta \in L$ une racine de $\iota(\mu_{\alpha,K})$. Supposons qu'il existe un morphisme d'anneaux $\sigma_\beta : K(\alpha) \longrightarrow L$ prolongeant ι tel que $\sigma_\beta(\alpha) = \beta$. L'égalité $(*)$ montre alors que

$$\sigma_\beta\big(P(\alpha)\big) = \iota(P)(\beta), \quad \text{pour tout } P \in K[X].$$

Comme α est algébrique sur K, tout élément de $K(\alpha)$ est de la forme $P(\alpha)$, avec $P \in K[X]$. Ainsi, si σ_β existe, il est unique, et défini par la formule précédente. Il reste à démontrer qu'un tel morphisme existe bel et bien.

Puisque $\beta \in L$ est une racine de $\iota(\mu_{\alpha,K})$, le morphisme

$$\begin{aligned} K[X] &\longrightarrow L \\ P &\longmapsto \iota(P)(\beta) \end{aligned}$$

se factorise en un morphisme d'anneaux

$$\begin{aligned} \varphi\colon K[X]/(\mu_{\alpha,K}) &\longrightarrow L \\ \overline{P} \qquad &\longmapsto \iota(P)(\beta). \end{aligned}$$

On a alors un isomorphisme de K-algèbres

$$K[X]/(\mu_{\alpha,K}) \xrightarrow{\sim} K(\alpha),$$

qui envoie $\overline{X}$ sur α. En composant φ et l'inverse de cet isomorphisme, on obtient un morphisme $\sigma_\beta : K(\alpha) \longrightarrow L$ vérifiant les propriétés voulues.

Le point (3) est alors une conséquence immédiate des deux premiers points. Cela achève la démonstration. □

On commence par le cas d'une extension simple, i.e. le cas où $E = K(\alpha)$.

Lemme 4.6. *Soit $\alpha \in \overline{K}$, et soit $E = K(\alpha)$.*

Alors, tout morphisme d'anneaux $\iota : K \longrightarrow L$ possède au plus $[E : K]$ prolongements $\sigma : E \longrightarrow L$ à E. En particulier, on a

$$|\mathrm{Hom}_{K-alg}(E, L)| \leq [E : K].$$

De plus, les propriétés suivantes sont équivalentes :

(1) *tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ admet exactement $[E : K]$ prolongements à E ;*
(2) *on a l'égalité $|\mathrm{Hom}_{K-alg}(E, \overline{K})| = [E : K]$;*
(3) *α est séparable sur K.*

Démonstration. Gardons les notations de l'énoncé.

D'après le théorème de prolongement des isomorphismes, ι possède autant de prolongements à L que le polynôme $\iota(\mu_{\alpha,K})$ possède de racines distinctes dans L. En particulier, il y a au plus $\deg\big(\iota(\mu_{\alpha,K})\big)$ prolongements. Or, on a

$$\deg\big(\iota(\mu_{\alpha,K})\big) = \deg(\mu_{\alpha,K}) = [E : K],$$

d'où la première partie.

Un morphisme de K-algèbres $E \longrightarrow L$ n'étant rien d'autre qu'un prolongement de l'inclusion $K \subset L$, on en déduit que $|\mathrm{Hom}_{K-alg}(E, L)|$ est le nombre de racines distinctes de $\mu_{\alpha,K}$ dans L. On obtient alors l'inégalité

$$|\mathrm{Hom}_{K-alg}(E, L)| \leq [E : K],$$

ainsi que la chaîne d'implications « $(1) \Longrightarrow (2) \Longrightarrow (3)$ ».

Il reste à démontrer « $(3) \Longrightarrow (1)$ ». Soit $\iota : K \longrightarrow \overline{K}$, et soit E'/K la sous-extension de $\overline{K}$ engendrée par les racines de $\mu_{\alpha,K}$ dans $\overline{K}$. Cette extension étant algébrique (puisqu'elle est engendrée par des éléments algébriques), ι se prolonge en un morphisme $\tau : E' \longrightarrow \overline{K}$ (appliquer plusieurs fois le théorème des prolongements des isomorphismes). On a alors $\iota(\mu_{\alpha,K}) = \tau(\mu_{\alpha,K})$. Ainsi, si $\mu_{\alpha,K} = \prod_{i=1}^{n}(X - \alpha_i) \in E'[X] \subset \overline{K}[X]$, on a $\iota(\mu_{\alpha,K}) = \prod_{i=1}^{n}(X - \tau(\alpha_i)) \in \overline{K}[X]$. Comme τ est injectif, on en déduit que $\mu_{\alpha,K} \in K[X]$ n'a que des racines simples dans $\overline{K}$ si, et seulement si, $\iota(\mu_{\alpha,K}) \in \overline{K}[X]$ ne possède que des racines simples dans $\overline{K}$.

Supposons maintenant que $\mu_{\alpha,K} \in K[X]$ ne possède que des racines simples dans $\overline{K}$, et soit $\iota : K \longrightarrow \overline{K}$ un morphisme d'anneaux. D'après ce qui précède, $\iota(\mu_{\alpha,K})$ ne possède que des racines simples dans $\overline{K}$. Les considérations faites en début de démonstration montrent alors que ι possède $[E : K]$ prolongements à E, ce qui achève la démonstration. □

Passons maintenant au cas d'une extension quelconque.

Proposition 4.7. *Soit L/K une extension de corps, et soit E/K une extension de degré fini.*

Alors, tout morphisme d'anneaux $\iota : K \longrightarrow L$ admet au plus $[E : K]$ prolongements $\sigma : E \longrightarrow L$ à E. En particulier, on a

$$|\mathrm{Hom}_{K-alg}(E, L)| \leq [E : K].$$

De plus, les propriétés suivantes sont équivalentes :

(1) *tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ admet exactement $[E : K]$ prolongements à E ;*
(2) *on a l'égalité $|\mathrm{Hom}_{K-alg}(E, L)| = [E : K]$;*
(3) *l'extension E/K est séparable.*

Démonstration. Montrons le résultat par récurrence sur $[L : K]$. Plus précisément, pour tout $n \geq 1$, soit (H_n) la propriété suivante :

(H_n) Pour tout corps K, toute extension L/K, et toute extension E/K de degré $\leq n$, l'énoncé de la proposition est vrai.

Si $n = 1$, alors $E = K$ et toutes les propriétés de l'énoncé sont trivialement vraies. Soit $n \geq 1$ un entier, et supposons que la propriété (H_n) soit vraie. Montrons que (H_{n+1}) est vraie. Soit K un corps, soit L/K une extension, et soit E/K une extension de degré $\leq n+1$. On peut toujours supposer que $[E : K] = n+1 \geq 2$, car sinon il suffit d'appliquer (H_n). En particulier, $E \neq K$. Soit $\alpha \in E \setminus K$. On a donc $K(\alpha) \neq K$, et par conséquent $[E : K(\alpha)] \leq n$.

Remarquons maintenant que tout prolongement de ι à E s'obtient par extension d'un prolongement de ι à $K(\alpha)$. En effet, si $\sigma : E \longrightarrow L$ est un prolongement de ι à E, alors $\sigma_{|_{K(\alpha)}}$ est un prolongement de ι à $K(\alpha)$. Inversement, tout prolongement de ι à $K(\alpha)$ possède au plus $[E : K(\alpha)]$ extensions à E par hypothèse de récurrence, donc au moins une.

De plus, il y a exactement n_α prolongements de ι à $K(\alpha)$ par le théorème de prolongement des isomorphismes, où n_α est le nombre de racines de $\iota(\mu_{\alpha,K})$ dans $\overline{K}$. On en déduit que ι admet au plus $n_\alpha[E : K(\alpha)]$ extensions à E. Comme $n_\alpha \leq [K(\alpha) : K]$ et que $[K(\alpha) : K][E : K(\alpha)] = [E : K]$, cela démontre le premier point.

Notons que tout cela est valable pour un élément $\alpha \in E \setminus K$ arbitraire.

Montrons maintenant l'équivalence des trois propriétés $\big($toujours sous l'hypothèse $(H_n)\big)$.

(1) $\Longrightarrow$ (2). Il suffit d'appliquer la propriété (1) à l'inclusion $K \subset \overline{K}$.

(2) $\Longrightarrow$ (3). On procède par contraposition. Supposons que E/K ne soit pas séparable. Il existe donc $\alpha \in E \setminus K$ non séparable[2]. Les considérations précédentes appliquées à l'inclusion $K \subset \overline{K}$ montrent alors que le nombre de plongements est $< [E : K(\alpha)][K(\alpha) : K] = [E : K]$, d'où l'implication voulue.

(3) $\Longrightarrow$ (1). Supposons que E/K soit séparable, et soit $\iota : K \longrightarrow \overline{K}$ un morphisme d'anneaux. Comme $E \neq K$, on peut choisir un élément $\alpha \in E \setminus K$. Un tel élément est séparable par hypothèse. Ainsi, ι admet $[K(\alpha) : K]$ prolongements à $K(\alpha)$. De plus, l'extension $E/K(\alpha)$ est aussi séparable d'après la remarque 4.2. Par hypothèse de récurrence, n'importe quel prolongement de ι à $K(\alpha)$ admet lui-même $[E : K(\alpha)]$ prolongements. Mais alors, ι possède $[K(\alpha) : K][E : K(\alpha)] = [E : K]$ prolongements à E.

Cela achève la récurrence, ainsi que la démonstration. □

Cette dernière proposition montre que le théorème 4.3 est vraie pour les extensions de degré fini de K. Nous allons maintenant montrer comment réduire la démonstration du théorème à ce cas particulier.

Pour cela, nous aurons besoin de plusieurs lemmes.

Lemme 4.8. *Soit $[\mathcal{A}, \mathcal{A}]$ l'idéal de $\mathcal{A}$ engendré par les éléments $xy - yx$, avec $x, y \in \mathcal{A}$. Alors, $\mathcal{A}/[\mathcal{A}, \mathcal{A}]$ est une K-algèbre commutative, et on a une bijection*

$$\mathrm{Hom}_{K-alg}(\mathcal{A}, L) \simeq \mathrm{Hom}_{K-alg}(\mathcal{A}/[\mathcal{A}, \mathcal{A}], L).$$

2. Les éléments de K sont séparables sur K.

Démonstration. Pour tous $x, y \in \mathcal{A}$, on a

$$\overline{x}\ \overline{y} - \overline{y}\ \overline{x} = \overline{xy - yx} = \overline{0} \in \mathcal{A}/[\mathcal{A}, \mathcal{A}],$$

et $\mathcal{A}/[\mathcal{A}, \mathcal{A}]$ est donc commutative. De plus, pour tout morphisme de K-algèbres $f : \mathcal{A} \longrightarrow L$, et pour tous $x, y \in \mathcal{A}$, on a

$$f(xy - yx) = f(x)f(y) - f(y)f(x) = 0,$$

puisque L est commutatif. Ainsi, on a $[\mathcal{A}, \mathcal{A}] \subset \mathrm{Ker}(f)$. Par conséquent, l'ensemble $\mathrm{Hom}_{K-alg}(\mathcal{A}, L)$ est en bijection avec $\mathrm{Hom}_{K-alg}(\mathcal{A}/[\mathcal{A}, \mathcal{A}], L)$, d'après le théorème de factorisation. □

Lemme 4.9. *Soit $\mathcal{A}$ une K-algèbre commutative. Alors, $\mathcal{A}/\mathrm{Nil}(\mathcal{A})$ n'admet pas d'éléments nilpotents non nuls, et on a une bijection*

$$\mathrm{Hom}_{K-alg}(\mathcal{A}, L) \simeq \mathrm{Hom}_{K-alg}(\mathcal{A}/\mathrm{Nil}(A), L).$$

Démonstration. On remarque tout d'abord que, pour tout morphisme de K-algèbres $f : \mathcal{A} \longrightarrow L$, on a $\mathrm{Nil}(\mathcal{A}) \subset \mathrm{Ker}(f)$.

En effet, soit $x \in \mathrm{Nil}(\mathcal{A})$, et soit $n \geq 1$ tel que $x^n = 0$. Alors, on a

$$f(x)^n = f(x^n) = f(0) = 0.$$

Comme L est un corps, donc intègre, on en déduit que $f(x) = 0$. Le théorème de factorisation nous donne alors la bijection voulue.

Montrons maintenant que $\mathrm{Nil}(\mathcal{A}/\mathrm{Nil}(\mathcal{A})) = 0$. Soit $\overline{x} \in \mathcal{A}/\mathrm{Nil}(\mathcal{A})$ tel qu'il existe $n \geq 1$ vérifiant $\overline{x}^n = \overline{0}$. Alors, $\overline{x^n} = \overline{0}$, si bien que $x^n \in \mathrm{Nil}(\mathcal{A})$. Mais alors, il existe $m \geq 1$ tel que $(x^n)^m = x^{nm} = 0$, et $x \in \mathrm{Nil}(\mathcal{A})$ puisque $nm \geq 1$. Ainsi, $\overline{x} = \overline{0}$. □

Lemme 4.10. *Soient $E_1/K, \ldots, E_r/K$ des extensions de K. Alors, on a une bijection entre $\mathrm{Hom}_{K-alg}(E_1 \times \cdots \times E_r, L)$ et l'union disjointe $\bigsqcup_{i=1}^{r} \mathrm{Hom}_{K-alg}(E_i, L)$.*

Démonstration. Rappelons que $\bigsqcup_{i=1}^{r} \mathrm{Hom}_{K-alg}(E_i, L)$ est l'ensemble des couples (i, f_i), avec $i \in [\![1, r]\!]$ et $f_i \in \mathrm{Hom}_{K-alg}(E_i, L)$.

Si $f_i : E_i \longrightarrow L$ est un morphisme de K-algèbres, on définit un morphisme de K-algèbres $\tilde{f}_i : E_1 \times \cdots \times E_r \longrightarrow L$ en posant

$$\tilde{f}_i(x) = f_i(x_i) \quad \text{pour tout } x = (x_1, \ldots, x_r) \in E_1 \times \cdots \times E_r.$$

Considérons alors l'application

$$\begin{aligned} \varphi \colon \bigsqcup_{i=1}^{r} \mathrm{Hom}_{K-alg}(E_i, L) &\longrightarrow \mathrm{Hom}_{K-alg}(E_1 \times \cdots \times E_r, L) \\ (i, f_i) \qquad &\longmapsto \tilde{f}_i. \end{aligned}$$

Nous allons démontrer que φ est la bijection voulue. Commençons par remarquer que φ est injective. En effet, pour tout $i \in [\![1, r]\!]$, et tout $x_i \in E_i$, on a

$$\varphi((i, f_i))((0, \ldots, 0, x_i, 0, \ldots, 0)) = f_i(x_i).$$

En particulier, si $e_i = (0, \dots, 0, 1_{E_i}, 0, \dots, 0)$, pour tous $i, j \in [\![1, r]\!]$, on a $\varphi((i, f_i))(e_j) = \delta_{ij}$.

Si maintenant $\varphi((i, f_i)) = \varphi((j, g_j))$, avec des notations évidentes, l'évaluation en e_j et l'égalité précédente montrent que $i = j$. Mais alors, l'évaluation en les éléments de la forme $(0, \dots, 0, x_i, 0, \dots, 0), x_i \in E_i$ montrent que $f_i = g_i$, d'où l'injectivité voulue.

Montrons maintenant que φ est également surjective.

Soit $f : E_1 \times \cdots \times E_r \longrightarrow L$ un morphisme de K-algèbres. Avec les notations précédentes, on a alors $e_i^2 = e_i$ pour tout $i \in [\![1, r]\!]$, ainsi que $e_i e_j = 0$ pour tous $i, j \in [\![1, r]\!]$, avec $i \neq j$.

Pour tout $i \in [\![1, r]\!]$, on a donc $f(e_i)^2 = f(e_i)$, et comme L est un corps, on en déduit que $f(e_i) = 0$ ou 1. Remarquons maintenant que

$$e_1 + \cdots + e_r = (1_{E_1}, \dots, 1_{E_r}) = 1_{E_1 \times \cdots \times E_r},$$

et donc

$$f(e_1) + \cdots + f(e_r) = 1.$$

Il existe donc au moins un entier $j \in [\![1, r]\!]$ tel que $f(e_j) = 1$. Mais alors, pour tout $i \in [\![1, r]\!]$, $i \neq j$, on a

$$f(e_i e_j) = f(0) = 0 = f(e_i) f(e_j) = f(e_i).$$

Or, pour tout $x = (x_1, \dots, x_r) \in E_1 \times \cdots \times E_r$, on a $x = x(e_1 + \cdots + e_r)$, d'où

$$f(x) = f(x)f(e_1) + \cdots + f(x)f(e_r) = f(x)f(e_j) = f(xe_j) = f((0, \dots, 0, x_j, 0, \dots, 0)).$$

Notons que l'application

$$\begin{aligned} f_j \colon E_j &\longrightarrow L \\ x_j &\longmapsto f((0, \dots, 0, x_j, 0, \dots, 0)) \end{aligned}$$

est un morphisme de K-algèbres. Tout provient du fait que f est un morphisme de K-algèbres, sauf l'égalité $f_j(1_{E_j}) = 1$, celle-ci étant vraie car $f_j(1_{E_j}) = f(e_j) = 1$.

Bref, on a

$$f(x) = f_j(x_j) \quad \text{pour tout } x = (x_1, \dots, x_r) \in E_1 \times \cdots \times E_r,$$

où $j \in [\![1, r]\!]$, et où $f_j \in \mathrm{Hom}_{K-alg}(E_j, L)$, c'est-à-dire $f = \varphi((j, f_j))$. Ceci achève la démonstration. □

On peut maintenant démontrer le résultat attendu.

Démonstration. [du théorème 4.3.]On commence par démontrer la première partie du théorème.

Soit $\mathcal{A}$ une K-algèbre de dimension finie, et soit L/K une extension quelconque. Rappelons que l'on ntoe $[\mathcal{A}, \mathcal{A}]$ l'idéal de $\mathcal{A}$ engendré par les élément de la forme $xy - yx, x, y \in \mathcal{A}$.

D'après le lemme 4.8, $\mathcal{A}/[\mathcal{A}, \mathcal{A}]$ est une K-algèbre commutative de dimension finie, et on a

$$\mathrm{Hom}_{K-alg}(\mathcal{A}, L)| = \mathrm{Hom}_{K-alg}(\mathcal{A}/[\mathcal{A}, \mathcal{A}], L)|.$$

Comme $\dim_K(\mathcal{A}/[\mathcal{A},\mathcal{A}]) \leq \dim_K(\mathcal{A})$ d'après le lemme 3.1, il suffit de démontrer l'inégalité voulue lorsque $\mathcal{A}$ est commutative.

Supposons maintenant $\mathcal{A}$ commutative. D'après le lemme 4.9, $\mathcal{A}/\mathrm{Nil}(\mathcal{A})$ est une K-algèbre commutative sans nilpotents non nuls , et on a

$$\mathrm{Hom}_{K-alg}(\mathcal{A}, L)| = \mathrm{Hom}_{K-alg}(\mathcal{A}/\mathrm{Nil}(\mathcal{A}), L)|.$$

Comme $\dim_K(\mathcal{A}/\mathrm{Nil}(\mathcal{A})) \leq \dim_K(\mathcal{A})$ d'après le lemme 3.1, on peut se réduire au cas où $\mathcal{A}$ est commutative, sans éléments nilpotents non triviaux. Une telle K-algèbre est isomorphe à $E_1 \times \cdots \times E_r$, où chaque E_i/K est une extension de degré fini, d'après le théorème 3.2. Comme un tel isomorphisme induit une bijection entre les ensembles de morphismes (par composition avec l'isomorphisme en question), on peut supposer que l'on a $\mathcal{A} = E_1 \times \cdots \times E_r$. Dans ce cas, le lemme 4.10 montre alors que l'inégalité à établir devient

$$|\mathrm{Hom}_{K-alg}(E_1, L)| + \cdots + |\mathrm{Hom}_{K-alg}(E_r, L)| \leq [E_1 : K] + \cdots + [E_r : K].$$

Or, cette inégalité découle de la proposition 4.7, appliquée à chaque extension E_i/K.

Cela démontre donc la première partie du théorème. Supposons maintenant que $L = \overline{K}$. Supposons que $|\mathrm{Hom}_{K-alg}(\mathcal{A}, \overline{K})| \leq \dim_K(\mathcal{A})$.

Les considérations précédentes et la première partie du théorème montrent que l'on a

$$\dim_K(\mathcal{A}) = |\mathrm{Hom}_{K-alg}(\mathcal{A}, \overline{K})| = |\mathrm{Hom}_{K-alg}(\mathcal{A}/[\mathcal{A},\mathcal{A}], \overline{K})| \leq \dim_K(\mathcal{A}/[\mathcal{A},\mathcal{A}]) \leq \dim_K(\mathcal{A}).$$

Mais alors, on a $\dim_K(A) = \dim_K(\mathcal{A}/[\mathcal{A},\mathcal{A}])$, et par conséquent $[\mathcal{A},\mathcal{A}] = 0$ d'après le lemme 3.1, ce qui signifie que $\mathcal{A}$ est commutative.

Un raisonnement identique en remplaçant $[\mathcal{A},\mathcal{A}]$ par $\mathrm{Nil}(\mathcal{A})$ montre alors que $\mathcal{A}$ n'a pas d'élément nilpotents non nuls. On vient donc de démontrer que si $\mathcal{A}$ vérifie $|\mathrm{Hom}_{K-alg}(\mathcal{A}, \overline{K})| \leq \dim_K(\mathcal{A})$, alors $\mathcal{A}$ est isomorphe à $E_1 \times \cdots \times E_r$, où chaque E_i/K est une extension de degré fini. Mais alors, on a

$$|\mathrm{Hom}_{K-alg}(E_1, \overline{K})| + \cdots + |\mathrm{Hom}_{K-alg}(E_r, \overline{K})| = [E_1 : K] + \cdots + [E_r : K].$$

D'après la proposition 4.7, on a $|\mathrm{Hom}_{K-alg}(E_r, \overline{K})| \leq [E_i : K]$ pour tout $i \in [\![1, r]\!]$. Ainsi, l'égalité précédente aura lieu si et seulement si on a l'égalité $|\mathrm{Hom}_{K-alg}(E_r, \overline{K})| = [E_i : K]$ pour tout $i \in [\![1, r]\!]$. On utilise alors cette même proposition pour conclure. $\square$