Algèbre M1 Cours 4

Extensions séparables

5 octobre 2010

La théorie de Galois

Théorie de Galois = étude des « bonnes » extensions algébriques

$$
\begin{tikzcd}
 & \text{« bonnes »} \arrow[dl] \arrow[dr] & \\
\text{où sont les racines ?} \arrow[d] & & \text{combien ai-je de racines ?} \arrow[d] \\
\text{polynômes scindés} \arrow[d] & & \text{racines multiples} \arrow[d] \\
\text{extension normale} \arrow[dr] & & \text{extension séparable} \arrow[dl] \\
 & \text{extension galoisienne} \arrow[d] & \\
 & \text{thm de correspondance} &
\end{tikzcd}
$$

Séparabilité

$$\begin{tikzcd}
\text{Polynôme irréductible séparable} \arrow[d, Rightarrow] & \\
\text{Élément séparable} \arrow[d, Rightarrow] & k[X]/(P) \arrow[ul, dotted, Rightarrow] \\
\text{Extension séparable} \arrow[ur, dotted, Rightarrow] &
\end{tikzcd}$$

Le cas des extensions séparables finies

$$\Updownarrow$$

Nombre de prolongements à valeurs dans une extension algébriquement close

Applications : Corps parfaits et théorème de l'élément primitif

Divisibilité et changement de corps

Soit K une extension du corps k et $U, V \in k[X]$ avec $V \neq 0$.

On considère $U = VQ_k + R_k$ la division euclidienne de U par V dans $k[X]$ c'est-à-dire $Q_k, R_k \in k[X]$ et $\deg R_k < \deg V$.

De même, on considère $U = VQ_K + R_K$ la division euclidienne de U par V dans $k[X]$ c'est-à-dire $Q_K, R_K \in K[X]$ et $\deg R_K < \deg V$.

Par unicité de la division euclidienne dans $K[X]$, on obtient $Q_k = Q_K$ et $R_k = R_K$.

Application

1. $V \mid U$ dans $k[X] \quad \Longleftrightarrow \quad V \mid U$ dans $K[X]$.
2. Le pgcd de U et V ne dépend pas du corps : si $P_k = \mathrm{pgcd}(U, V)$ dans $k[X]$ et $P_K = \mathrm{pgcd}(U, V)$ dans $K[X]$ alors il existe $\lambda \in K^\times$ tel que $P_K = \lambda P_k$.

Dérivée d'un polynôme

Définition – Dérivation. Soit $P = \sum_{i=0}^{n} a_i X^i \in k[X]$. On **définit**

$$P'(X) = \sum_{i=0}^{n} i a_i X^{i-1} \in k[X].$$

L'application
$$D\colon \begin{cases} k[X] \longrightarrow k[X] \\ P \longmapsto P' \end{cases}$$

est k-linéaire et vérifie $(PQ)' = PQ' + P'Q$ pour tous $P, Q \in k[X]$.

Preuve. Par bilinéarité, il suffit de vérifier la formule avec $P = X^m$ et $Q = X^n$. Or on a

$$(X^m)'X^n + X^m(X^n)' = nX^{m+n-1} + mX^{m+n-1}$$

et
$$(X^m X^n)' = (n+m)X^{m+n-1}$$

Dérivée d'un polynôme

Lemme – $\mathrm{Ker}\, D$. Soit $P \in k[X]$ tel que $P' = 0$ alors

- Si $\mathrm{car} k = 0$ alors $P = \lambda \in k$ et $\mathrm{Ker}\, D = k1$.
- Si $\mathrm{car} k = p$ alors il existe $Q \in k[X]$ tel que $P = Q(X^p)$ et $\mathrm{Ker}\, D = k[X^p]$.

Preuve. Si $P = \sum_{i=0}^{n} a_i X^i \in \mathrm{Ker}\, D$ alors on a $ia_i = 0$ pour tout i.

- $\mathrm{car} k = 0$. Si $i \in \mathbb{N}^*$ alors $i \neq 0$ dans k (puisque $\mathbb{Q} \hookrightarrow k$) et donc $a_i = 0$ pour tout $i \neq 0$ et P est constant.
- $\mathrm{car} k = p$. Si $p \nmid i$ alors $i \neq 0$ dans k et donc $a_i = 0$ pour tout i qui n'est pas un multiple de p. On en déduit que $P = \sum a_{pi} X^{pi}$ et donc $P = Q(X^p)$ avec $Q = \sum a_{pi} X^i$. Enfin, on a $(X^{mp})' = mpX^{mp-1} = 0$.

Dérivée d'un polynôme

Exercice – Formules. Soient $P, P_1, \ldots, P_r \in k[X]$ et $n_1, \ldots, n_r \in \mathbb{N}$.

1. Montrer que $(P^n)' = nP'P^{n-1}$.
2. Calculer $(P_1 \cdots P_r)'$
3. Calculer $({P_1}^{n_1} \cdots {P_r}^{n_r})'$.
4. Déterminer les applications k-linéaires $D_1 : k[X] \to k[X]$ telles que $D_1(PQ) = D_1(P)Q + PD_1(Q)$ pour tous $P, Q \in k[X]$.
5. Montrer qu'une telle applications D_1 vérifie la formule de Leibniz

$$ {D_1}^r(PQ) = \sum_{i=0}^{r} \binom{r}{i} {D_1}^i(P){D_1}^{r-i}(Q) $$

Dérivation et multiplicité

Proposition Soient k un corps, $P \in k[X]$ non constant. Dans la suite, Ω désigne une extension algébriquement close de k ; K un corps de décomposition de P sur k et L une extension de k. On a les équivalences suivantes

(i) $\mathrm{pgcd}(P, P') = 1$;

(ii) pour toute L, P et P' sont sans racine commune ;

(iii) P et P' n'ont pas de racine commune dans K ;

(iv) P et P' n'ont pas de racine commune dans Ω ;

(v) pour toute L, P n'a que des racines simples dans L ;

(vi) P n'a que des racines simples dans K ;

(vii) P n'a que des racines simples dans Ω ;

($viii$) il existe L telle que P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans $L[X]$;

(ix) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans $K[X]$;

(x) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans $\Omega[X]$.

Un lemme préliminaire

Lemme Soient $P \in k[X]$ et $a \in k$. Alors a est une racine multiple de P si et seulement si $P(a) = P'(a) = 0$ si et seulement si $(X - a) \mid P$ et $(X - a) \mid P'$.

Preuve du lemme. Si n est la multiplicité de a dans P, on a $P = (X - a)^n Q$ avec $Q(a) \neq 0$. Ainsi $P' = n(X - a)^{n-1} Q + (X - a)^n Q'$. Si $n \geqslant 2$, on obtient $P(a) = P'(a) = 0$. Si $n = 1$ alors $P'(a) = Q(a) \neq 0$.

ATTENTION !

$$(X - a)^n \mid P \implies P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0.$$

Mais la réciproque est fausse. Par exemple, dans $\mathbb{F}_2[X]$, avec $a = 0$ et $P = X^2$. On a $P^{(n)}(0) = 0$ pour tout $n \in \mathbb{N}$.

Exercice Démontrer la réciproque en caractéristique nulle.

Démonstration de la proposition

Par le lemme, on a $(ii) \Leftrightarrow (v)$, $(iii) \Leftrightarrow (vi)$ et $(iv) \Leftrightarrow (vii)$.

On a $(ii) \Rightarrow (iv)$. Le lemme de prolongement donne $(iv) \Rightarrow (iii)$.

$(i) \Rightarrow (ii)$. Soient $U, V \in k[X]$ tels que $1 = UP + VP'$. Si $a \in L$ est une racine commune alors $P(a) = P'(a) = 0$ et $1 = 0$. NON.

$(iii) \Rightarrow (i)$. Soit Q un diviseur commun de P et P'. Comme P est scindé, Q l'est aussi. Ainsi si $\deg Q \geqslant 1$ alors Q a une racine a et $X - a \mid Q \mid P$ et $(X - a) \mid Q \mid P'$. Finalement $P(a) = P'(a) = 0$.

On a $(x) \Rightarrow (viii)$. De plus, $(vi) \Leftrightarrow (ix)$ et $(vii) \Leftrightarrow (x)$ résultent du fait que P est scindé dans $K[X]$ et dans $\Omega[X]$.

$(viii) \Rightarrow (vi)$. On a $P = \prod_{i=1}^{n} (X - a_i) \in L[X]$ avec $a_i \neq a_j$ si $i \neq j$. On pose $K' = k(a_1, \ldots, a_n) \subset L$, c'est un corps de décomposition et on a $P = \prod_{i=1}^{n} (X - a_i) \in K'[X]$ avec $a_i \neq a_j$ si $i \neq j$. On conclut par le théorème d'isomorphisme entre corps de décomposition.

Polynôme séparable

Définition – Polynôme séparable. Soit $P \in k[X]$ un polynôme irréductible. On dit que P est séparable si P vérifie les conditions équivalentes de la proposition précédente.
De plus, si P est irréductible, elles sont aussi équivalentes à

(xi) $P' \neq 0$

(xii) il existe une extension L de k tel que P ait une racine simple.

Preuve. On a $(x) \Rightarrow (xii)$.
$(xii) \Rightarrow (xi)$. Si a est une racine de P dans L, on a $P'(a) \neq 0$ et donc $P' \neq 0$.
$(xi) \Rightarrow (i)$. Comme P est irréductible, on a $\mathrm{pgcd}(P, P') \in \{1, P\}$ et $\mathrm{pgcd}(P, P') = P$ si et seulement si $P \mid P'$ si et seulement si $P' = 0$ car $\deg P' < \deg P$.

Polynôme séparable et caractéristique

Remarque – Polynôme irréductible et dérivation. Soit $P \in k[X]$ un polynôme irréductible. Alors $\mathrm{pgcd}(P, P') = 1$ ou alors $P' = 0$. Ce deuxième cas ne peut intervenir qu'en caractéristique p et si $k^{[p]} := \{x^p,\ x \in k\} \neq k$.
En effet, si $P = \sum a_i X^i$ vérifie $P' = 0$ alors $P = Q(X^p)$ avec $Q = \sum a_{pi} X^i$. Si $k^{[p]} = k$ alors on écrit $a_{pi} = {b_i}^p$ et on a $P = R(X)^p$ avec $R = \sum b_i X^i$ et P n'est pas irréductible.

Exemple En caractéristique nulle, tout polynôme irréductible est séparable.
Soit k un corps fini alors tout polynôme irréductible sur k est séparable.

Élément et extension séparable

Définition – Élément séparable. Soient K une extension de k et $x \in K$. On dit que x est séparable sur k si le polynôme minimal de x sur k est séparable. Un élément séparable est algébrique.

Définition – Extension algébrique. Soit K une extension de k. On dit que K est une extension séparable de k si toute élément de K est séparable sur k. Une extension séparable est algébrique.

Remarque – Lien polynôme séparable et extension séparable. Soient $P \in k[X]$ un polynôme irréductible. Alors $k[X]/(P)$ séparable sur k si et seulement si P est séparable.

En effet, si $k[X]/(P)$ est séparable sur k alors P qui est le polynôme minimal de x la classe de X est séparable.

Réciproquement, soit $y = Q(x) \in k[X]/(P)$. Il s'agit de montrer que le polynôme minimal de y est séparable. Pour cela, on a besoin d'autres caractérisations de la séparabilité...

Corps parfait

Proposition-définition. – Corps parfait. Soit k un corps de caractéristique p. Si $p = 0$, on note $k^{[p]} := k$. Si p est premier, on note $k^{[p]} := \{x^p \in k,\ x \in k\}$. Soit Ω une clôture algébrique de k. Les propositions suivantes sont équivalentes

(i) $k = k^{[p]}$;

(ii) tout élément irréductible de $k[X]$ est séparable ;

(iii) tout extension algébrique de k est séparable ;

(iv) Ω est une extension séparable de k.

Un corps vérifiant ces conditions est appelé corps parfait.

Preuve. On a toujours $(ii) \Rightarrow (iii)$ et $(iii) \Rightarrow (iv)$.
$(iv) \Rightarrow (ii)$. Considérons P un polynôme irréductible. Comme Ω est algébriquement clos, il existe une racine x de P dans Ω et P est le polynôme minimal de x sur k. Comme Ω est séparable, on en déduit que P est séparable.
Un corps de caractéristique nulle vérifie immédiatement (i) et (ii).
Supposons $\mathrm{car}\, k = p$. On a vu que $k = k^{[p]}$ implique (ii).

$(ii) \Rightarrow (i)$

Lemme Soient k un corps de caractéristique p avec p premier et $k \neq k^{[p]}$. Pour $a \in k \smallsetminus k^{[p]}$, le polynôme $P = X^{p^n} - a$ est irréductible. De plus, si $n \geqslant 1$, P n'est pas séparable.

Preuve du lemme. On suppose $n \geqslant 1$. Soit L un extension de k dans lequel P a une racine α. On a alors $\alpha^{p^n} = a$ et donc $P = (X - \alpha)^{p^n}$ dans $L[X]$. Si $P = QR$ est une factorisation de P dans $k[X]$ alors $Q = (X - \alpha)^m$ avec $1 \leqslant m \leqslant p^n$. On écrit $m = p^r \ell$ avec $\ell \wedge p = 1$. On a donc $Q = (X^{p^r} - \alpha^{p^r})^\ell$. Le coefficient en $X^{p^r(\ell-1)}$ de Q est alors $-\ell\alpha^{p^r} \in k$. Comme $\ell \wedge p = 1$, on en déduit que $\alpha^{p^r} \in k$. Si $r < n$ alors $a = b^p \in k^{[p]}$ avec $b = (\alpha^{p^r})^{p^{n-r-1}}$. Ainsi $m = p^n$ et P est irréductible.

$(ii) \Rightarrow (i)$. Si $k \neq k^{[p]}$ alors on a un polynôme irréductible non séparable.

Manipuler la séparabilité

Pb 1 On n'a pas montré que P séparable $\Longrightarrow k[X]/(P)$ séparable.

Lemme – Un premier critère. Soient k un corps, K une extension de k et $a \in K$. On a alors les équivalences

(i) a est séparable sur k ;

(ii) a est racine simple du polynôme minimal P de a sur k ;

(iii) il existe $Q \in k[X]$ tel que a soit racine simple de Q

Preuve du lemme. $(i) \Rightarrow (iii)$. On prend $Q = P$.

$(iii) \Rightarrow (ii)$. On a $P \mid Q$ et donc a est racine simple de P (sinon $(X-a)^2 \mid Q$).

$(ii) \Rightarrow (i)$. C'est le critère (xii) de séparabilité

Application – Transitivité de la séparabilité. Soient $k \hookrightarrow K$ et $K \hookrightarrow L$ deux extensions de corps. Alors L séparable sur k si et seulement si L séparable sur K et K séparable sur k.

($\Rightarrow$) K est évidemment séparable sur k. De plus, si $x \in L$ alors le polynôme minimal de a sur k est à coefficient dans K et admet a comme racine. Donc x est séparable sur K.

Pb 2 Il faut démontrer la réciproque.

Degré séparable

Proposition-définition. – Degré séparable. Soit $i : k \hookrightarrow K$ une extension algébrique et $j : k \hookrightarrow \Omega$ une extension algébriquement close de Ω. Alors $|\mathrm{Hom}_{k-\mathrm{alg.}}(K, \Omega)|$ ne dépend ni de Ω ni de j. On définit alors le degré séparable de K sur k

$$[K : k]_{\mathrm{s}} := |\mathrm{Hom}_{k-\mathrm{alg.}}(K, \Omega)| \neq 0.$$

Preuve. Soit $\widetilde{\Omega}$ la clôture algébrique de k contenue dans Ω. On a $\mathrm{Hom}_{k-\mathrm{alg.}}(K, \Omega) = \mathrm{Hom}_{k-\mathrm{alg.}}(K, \widetilde{\Omega})$ car K est algébrique sur k. En effet, si $x \in K$ est annulé par $P \in k[X]$ et $\sigma : K \to \Omega$ un morphisme d'extensions alors $\sigma(x)$ est annulé par P.
Si $j' : k \to \Omega'$ est une extension algébriquement close, on a de même $\mathrm{Hom}_{k-\mathrm{alg.}}(K, \Omega') = \mathrm{Hom}_{k-\mathrm{alg.}}(K, \widetilde{\Omega}')$
Enfin, comme $\widetilde{\Omega}$ et $\widetilde{\Omega}'$ sont des extensions k-isomorphes (disons via $\tau : \widetilde{\Omega} \to \widetilde{\Omega}'$), alors la composition à gauche par τ donne $\mathrm{Hom}_{k-\mathrm{alg.}}(K, \widetilde{\Omega}) \overset{\mathrm{bij.}}{\simeq} \mathrm{Hom}_{k-\mathrm{alg.}}(K, \widetilde{\Omega}')$

Multiplicativité

Théorème – Multiplicativité du degré séparable. Soient K une extension de k et L une extension de K. Alors on a

$$[L : K]_{\mathrm{s}}[K : k]_{\mathrm{s}} = [L : k]_{\mathrm{s}}\,.$$

Preuve. Soit $j : k \hookrightarrow \Omega$ une extension algébriquement close. Il existe $[K : k]_{\mathrm{s}}$ morphismes d'extensions noté $\sigma_i : K \to \Omega$ pour $i \in I$. On fixe i. Ainsi $\sigma_i : K \hookrightarrow \Omega$ est une extension algébriquement close. Il existe exactement $[L : K]_{\mathrm{s}}$ morphismes d'extensions $\tau_{i\ell} : L \to \Omega$.

$$\begin{tikzcd}
L \arrow[rr, "\tau_{i\ell}"] & & \Omega \\
& K \arrow[ul] \arrow[ur, "\sigma_i"'] & \\
& & k \arrow[ul] \arrow[uu, "j"']
\end{tikzcd}$$

De plus, si $\tau_{i\ell} = \tau_{i'\ell'}$ alors par restriction à K, on a $\sigma_i = \sigma_{i'}$ et donc $i = i'$ puis $\ell = \ell'$.
Enfin si $\tau : L \hookrightarrow \Omega$ est un morphisme d'extensions alors $\tau_{|K} : K \hookrightarrow \Omega$ est un morphisme d'extension donc il existe i tel que $\tau_{|K} = \sigma_i$. Puis il existe ℓ tel que $\tau = \tau_{i\ell}$.

Le cas des extension monogènes

Théorème Soit $k(x)$ une extension algébrique monogène de k. Alors $[k(x) : k]_{\mathrm{s}}$ est le nombre de racines distinctes de P le polynôme minimal de x sur k dans Ω une extension algébriquement close de k

En particulier, on a $[k(x) : k]_{\mathrm{s}} \leqslant [k(x) : k] = \deg P$.

De plus, on a les équivalences

(i) $[k(x) : k]_{\mathrm{s}} = [k(x) : k]$;

(ii) x est séparable sur k ;

(iii) P est séparable sur k ;

(iv) $k(x)$ est séparable sur k.

Preuve. Le premier point est une conséquence immédiate de la propriété universelle des corps de rupture. Le deuxième point est une conséquence immédiate du premier point.

On a $(i) \iff$ le nombre de racines distinctes de P est $\deg P$ $\iff$ les racines de P sont simples $\iff (iii) \iff (ii)$.

On a déjà vu $(iv) \Rightarrow (iii)$.

Le problème 1 : $(i) \Rightarrow (iv)$

$(i) \Rightarrow (iv)$. Soit $y \in k(x)$. On a

$$[k(x) : k] = [k(x) : k(y)][k(y) : k]$$

et

$$[k(x) : k]_{\mathrm{s}} = [k(x) : k(y)]_{\mathrm{s}}[k(y) : k]_{\mathrm{s}}\,.$$

Or $[k(x) : k(y)]_{\mathrm{s}} \leqslant [k(x) : k]$ (puisque $k(x)$ est engendré sur $k(y)$ par x) et $[k(y) : k] \leqslant [k(y) : k]_{\mathrm{s}}$. On en déduit que $[k(y) : k]_{\mathrm{s}} = [k(y) : k]$ et y est séparable sur k.

Application Soit K une extension finie de k alors $[K : k]_{\mathrm{s}} \leqslant [K : k]$. En particulier $[K : k]_{\mathrm{s}} < +\infty$.

On écrit $K = k(x_1, \ldots, x_n)$. On obtient le résultat par multiplicativité du degré séparable :

$$[K : k]_{\mathrm{s}} = [K : K_{n-1}]_{\mathrm{s}} \cdots [K_1 : k]_{\mathrm{s}} \leqslant [K : K_{n-1}] \cdots [K_1 : k] = [K : k]$$

Applications

Corollaire – Une caractérisation de la séparabilité. Soit K une extension finie de k. Alors K est séparable sur k si et seulement si $[K : k]_{\mathrm{s}} = [K : k]$

Preuve. **($\Leftarrow$)** Soit $x \in K$. On a

$$[K : k] = [K : k(x)][k(x) : k]$$

et

$$[K : k]_{\mathrm{s}} = [K : k(x)]_{\mathrm{s}}[k(x) : k]_{\mathrm{s}}\,.$$

Or $[k(x) : k]_{\mathrm{s}} \leqslant [k(x) : k]$ et $[K : k(x)] \leqslant [K : k(x)]_{\mathrm{s}}$. On en déduit que $[k(x) : k]_{\mathrm{s}} = [k(x) : k]$ et x est séparable sur k.

($\Rightarrow$) On écrit $K = k(x_1, \ldots, x_n)$. Comme x_{i+1} est séparable sur $K_i = k(x_1, \ldots, x_i)$, on obtient le résultat par multiplicativité du degré séparable : on a

$$[K : k]_{\mathrm{s}} = [K : K_{n-1}]_{\mathrm{s}} \cdots [K_1 : k]_{\mathrm{s}} = [K : K_{n-1}] \cdots [K_1 : k] = [K : k]$$

Le problème 2

Proposition – Transitivité de la séparabilité. Soient $k \hookrightarrow K$ et $K \hookrightarrow L$ deux extensions de corps. Alors L séparable sur k si et seulement si L séparable sur K et K séparable sur k.

Preuve. **($\Rightarrow$)** On l'a déjà vu.
($\Leftarrow$) Soit $x \in L$ alors x annule $P = \sum a_i X^i \in K[X]$ séparable sur K. On en déduit que x est séparable sur $k(a_1, \ldots, a_n)$.
Par ailleurs $k(a_1, \ldots, a_n) \subset K$ séparable sur k. Ainsi, on a

$$[k(a_1, \ldots, a_n) : k]_{\mathrm{s}} = [k(a_1, \ldots, a_n) : k]$$

$$[k(a_1, \ldots, a_n)(x) : k(a_1, \ldots, a_n)]_{\mathrm{s}} = [k(a_1, \ldots, a_n)(x) : k(a_1, \ldots, a_n)]$$

Finalement, on obtient

$$[k(a_1, \ldots, a_n, x) : k]_{\mathrm{s}} = [k(a_1, \ldots, a_n, x) : k]$$

et $k(a_1, \ldots, a_n, x)$ est séparable sur k. En particulier, x est séparable sur k.

Exercices

Exercice – Famille génératrice et séparabilité. Soit K une extension de k.

(i) Montrer que l'ensemble des éléments de K séparables sur k est une sous-extension de K. Elle est notée K_{s} et appelée fermeture séparable de K sur k.

(ii) En déduire que K est séparable sur k si et seulement si K est engendré par des éléments séparables sur k.

(iii) Soit E et F deux sous-extensions de K. On suppose E est une extension séparable de k. Montrer que EF est une extension séparable de F.

Exercice – Extension séparable infinie. Soit K une extension de k. Montrer que K est une extension séparable de k si et seulement si tout sous-extension finie de K est séparable.

Élément primitif

Question : Quand une extension algébrique est-elle engendrée par un seul élément ?

Définition – Élément primitif. Soit K une extension monogène de k. On dit qu'un élément $x \in K$ est primitif si $k(x) = K$.

Proposition – Une caractérisation. Soit K une extension finie de k. Alors K est une extension monogène si et seulement si K admet un nombre fini de sous-extension.

Preuve. Si k est fini alors K aussi et K admet à la fois un nombre fini de sous-corps et un élément primitif (il suffit de choisir un générateur du groupe multiplicatif $K^\times$).
(⇒) On considère x un élément primitif de K sur k. Pour F une sous-extension de k, on note P_F le polynôme minimal de x sur F. Montrons que l'injectivité de l'application

$$\begin{cases} \{\text{Sous-extensions de } K\} \longrightarrow \{\text{Diviseurs unitaires de } P_k\} \\ \qquad F \qquad\qquad\qquad\qquad \longmapsto P_F\,. \end{cases}$$

Fin de la preuve

On fixe F une sous-extension de K et on pose $L = k(a_0, \ldots, a_n) \subset F$ où les a_i sont les coefficients de P_F. On a alors $L = F$ car $[K : F] = [F(x) : F] = \deg P_F = [L(x) : L] = [K : L]$ puisque P_F est irréductible sur F et donc sur L. Ainsi F est entièrement déterminé. Comme il n'y a qu'un nombre fini de diviseurs unitaires de P_k, on obtient le résultat souhaité.

($\Leftarrow$) Prenons x qui n'est dans aucune des sous-extensions strictes de K. Alors $K = k(x)$. Un tel x existe d'après le lemme suivant.

Lemme – Réunion de sous-espaces vectoriels. Soient k un corps infini, E un k-espace vectoriel et $E_1, \ldots, E_n$ des sous-espaces vectoriels stricts de E. Alors

$$\bigcup_{i=1}^{n} E_i \neq E$$

Preuve du lemme

Preuve du lemme. Raisonnons par récurrence sur n. Le résultat est vrai pour $n = 0$. Si

$$E_n \subset \bigcup_{i=1}^{n-1} E_i := F_{n-1}$$

le résultat s'obtient grâce à l'hypothèse de récurrence. Sinon, il existe $x \in E_n \smallsetminus F_{n-1}$ et $y \in E \smallsetminus E_n$. On suppose de plus que $E = F_{n-1} \cup E_n$. Pour $\lambda \in k$, on a alors $\lambda x + y \notin E_n$ et donc $\lambda x + y \in F_{n-1}$. Comme k est infini, il existe $\lambda \neq \mu$ et $i \in [\![1\,,\, n-1]\!]$ tel que $\lambda x + y \in E_i$ et $\mu x + y \in E_i$. On en déduit que $x \in E_i$. NON.

Donnons une autre preuve de **($\Leftarrow$)** On a $K = k(x_1, \ldots, x_n)$. Comme k est infini et que K n'a qu'un nombre fini de sous-extensions, il existe $\lambda, \mu \in k$ avec $\lambda \neq \mu$ tels que $k(x_1 + \lambda x_2) = k(x_1 + \mu x_2)$. On en déduit que $x_2, x_1 \in k(x_1 + \lambda x_2)$. Ainsi $k(x_1, x_2, \ldots, x_n) = k(x_1 + \lambda x_2, x_3, \ldots, x_n)$.

Théorème de l'élément primitif

Proposition Soit K une extension séparable et finie de k. Alors K est une extension monogène de k.

Preuve. Soit Ω une extension algébriquement close de k. Pour $\sigma, \tau \in \mathrm{Hom}_{k-\mathsf{alg}}(K, \Omega)$, on considère la sous-extension de k donnée $K_{\sigma,\tau} = \{x \in K, \sigma(x) = \tau(x)\}$. Comme $[K : k]_{\mathrm{s}}$ est fini, il existe $x \in K$ tel que $\sigma(x) \neq \tau(x)$ pour tout $\sigma \neq \tau$. Le choix d'un tel x assure que $[k(x) : k]_{\mathrm{s}} \geqslant [K : k]_{\mathrm{s}}$ puisque chacun des éléments de $\mathrm{Hom}_{k-\mathsf{alg}}(K, \Omega)$ se restreint à $k(x)$ en un morphisme différent. De plus, on a $[k(x) : k]_{\mathrm{s}} \leqslant [K : k]_{\mathrm{s}}$ puisque $k(x) \subset K$.
Enfin, comme K est séparable, $k(x)$ l'est aussi et donc $[k(x) : k] = [k(x) : k]_{\mathrm{s}} = [K : k]_{\mathrm{s}} = [K : k]$. Finalement $K = k(x)$.

Construction

Exemple – Construction explicite d'éléments primitifs.
Soient $K = k(\alpha, \beta)$ une extension finie de corps avec β séparable sur k et Ω une extension algébriquement close de K. On note $\beta = \beta_1, \ldots, \beta_n$ les racines du polynôme minimal Q de β dans Ω et $\alpha = \alpha_1, \ldots, \alpha_m$ les racines du polynôme minimal P de α dans Ω.
On considère $c \in k$ tel que

$$c \notin \left\{ \frac{\alpha - \alpha_j}{\beta_i - \beta}, \quad i \in [\![2\,,\, n]\!],\ j \in [\![1\,,\, m]\!] \right\} \cap k\,.$$

On a alors $k(\alpha, \beta) = k(\alpha + c\beta)$.
En effet, soit $\gamma = \alpha + c\beta$. Alors $P(\gamma - cX) \in k(\gamma)[X]$ admet β comme racine mais aucun des β_i. Ainsi
$X - \beta = \mathrm{pgcd}(P(\gamma - cX), Q)$ puisque Q est séparable. Finalement $\beta \in k(\gamma)$ et comme $c \neq 0$, on a bien $k(\alpha, \beta) = k(\gamma)$.