15 Théorème de l'élément primitif

Proposition. *Soit $K \to L$ une extension de degré fini. On note $[L:K]_s$ le nombre de K-morphismes de L dans $\bar{K}$, où $\bar{K}$ est une clôture algébrique de K.*
On a $1 \leqslant [L:K]_s \leqslant [L:K]$, et $[L:K]_s = [L:K]$ si et seulement si l'extension $K \to L$ est séparable.

On dira que $K \to L$ est séparable si tout élément de L est séparable sur K, *i.e.* annulé par un polynôme à coefficients dans K dont toutes les racines sont distinctes dans $\bar{K}$ (on dira aussi qu'un tel polynôme est séparable).

Preuve.
Puisque $K \to L$ est de degré fini, on peut écrire que $L = K[x_1, ..., x_n]$. On montre par récurrence que les extensions intermédiaires $L_k = K[x_1, ..., x_k]$ satisfont les propriétés annoncées.

Pour $k = 0$, c'est trivial, car $[K:K]_s = [K:K] = 1$ et l'extension $K \to K$ est séparable.

Supposons que les propriétés sont vérifiées pour L_k, montrons qu'elles le sont pour $L_{k+1} = L_k[x_{k+1}]$. En premier lieu, $[L_{k+1}:K]_s = [L_{k+1}:L_k]_s[L_k:K]_s$. En effet, tout K-morphisme $L_{k+1} \to \bar{K}$ est obtenu en prolongeant un K-morphisme $L_k \to \bar{K}$. Par hypothèse de récurrence, $[L_k:K]_s \leqslant [L_k:K]$. De plus, $[L_{k+1}:L_k]_s$ est le nombre de racine distinctes (dans $\bar{K}$) du polynôme minimal de x_{k+1} sur L_k, tandis que $[L_{k+1}:L_k]$ est son degré. On en déduit que $[L_{k+1}:L_k]_s \leqslant [L_{k+1}:L_k]$, ainsi on a bien $[L_{k+1}:K]_s \leqslant [L_{k+1}:L_k][L_k:K] = [L_{k+1}:K]$.

Vérifions maintenant la deuxième point. Si $K \to L_{k+1}$ est séparable, alors $K \to L_k$ est aussi séparable donc $[L_k:K]_s = [L_k:K]$ (par hypothèse de récurrence). De plus, x_{k+1} est séparable sur K donc sur L_k, par suite $[L_{k+1}:L_k]_s = [L_{k+1}:L_k]$. On a donc bien $[L_{k+1}:K]_s = [L_{k+1}:K]$. Maintenant si $K \to L_{k+1}$ n'est pas séparable, il existe un élément $x \in L_{k+1}$ qui n'est pas séparable. On a alors $[K(x):K]_s < [K(x):K]$, puis $[L_{k+1}:K]_s < [L_{k+1}:K]$.

□

Théorème. *Toute extension de degré fini séparable est monogène.*

Preuve.
Soit $K \to L$ une telle extension et notons $n = [L:K]_s = [L:K]$. On veut montrer qu'il existe un élément $x \in L$ de degré n sur K (on aura alors $L = K[x]$).

Par hypothèse, il existe des K-morphismes deux à deux distincts σ_1, ..., σ_n de L dans $\bar{K}$. On a donc $\mathrm{Ker}(\sigma_i - \sigma_j) \subsetneq L$ dès que $i \neq j$. Il s'ensuit que $\bigcup_{i<j} \mathrm{Ker}(\sigma_i - \sigma_j) \subsetneq L$, cf. la première proposition du développement 6. Montrons que $x \in L \setminus \bigcup_{i<j} \mathrm{Ker}(\sigma_i - \sigma_j)$ convient. Le polynôme minimal de x sur K admet tous les $\sigma_i(x)$ pour racines (dans $\bar{K}$), qui sont

deux à deux distincts. Ceci prouve que x est de degré $\geqslant n$ sur K, en fait de degré n (car $[K[x] : K] \leqslant [L : K] = n$). $\square$

Leçons possibles
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.
120 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
(**132** Formes linéaires et hyperplans en dimension finie. Exemples et applications.)

Références
[Esc00]
[CL05]