Racines de polynômes

Soit K un corps.

<u>Lemme 3.1</u> Si $P(X) \in K[X]$ a une racine α dans K, alors $(X-\alpha) \mid P(X)$ dans $K[X]$.

<u>Preuve:</u> Division euclidienne. ▨

<u>Corollaire 3.2</u> Si $P(X) \in K[X]$ est de degré d, alors P a au plus d racines dans K.

<u>Preuve:</u> Par récurrence sur d. ▨

On dira que $P(X) \in K[X]$ est <u>scindé</u> si $P(X) = c\prod_{i=1}^{d}(X-\alpha_i)$ dans $K[X]$. Autrement dit, les facteurs irréductibles de $P(X)$ sont de degré 1. Ici, $c \in K$.

si $P(X) \notin K$

<u>Exemple:</u> X^4-1 est scindé dans $\mathbb{C}[X]$, mais pas dans $\mathbb{R}[X]$

<u>Déf. 3.3</u> Soit L/K une extension de corps et $P(X) \in K[X]$ irréductible. Alors L est dit un <u>corps de rupture de $P(X)$</u> si $\exists \alpha \in L$ t.q. $P(\alpha) = 0$ et $L = K(\alpha)$.

<u>Exemples:</u> (1) $\mathbb{C}$ est un corps de rupture de $X^2+1 \in \mathbb{R}[X]$.

(2) $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de $X^2-2 \in \mathbb{Q}[X]$.

(3) $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$ sont des corps de rupture de $X^3-2 \in \mathbb{Q}[X]$

(4) $\mathbb{Q}(\sqrt[5]{3})$ est un corps de rupture de $X^5-3 \in \mathbb{Q}[X]$.

Rmq. Un corps de rupture n'est pas en général un corps dans lequel le polynôme est scindé, c'est à dire, il ne contient [2] pas en général "toutes" les racines du polynôme.

Prop. 3.4 Soit $P(X) \in K[X]$ irréductible. Pour toute extension L/K et toute racine $\alpha \in L$ de P, on a un unique K-morphisme de corps $K_P := K[X]/(P(X)) \longrightarrow L$ t.q. $X + (P(X)) \mapsto \alpha$. En particulier, si L est un corps de rupture de $P(X)$, alors ce morphisme est un isomorphisme. On a alors $[L:K] = \deg P$.

Preuve: Prenons le K-morphisme $E_\alpha : K[X] \longrightarrow L$, $Q(X) \mapsto Q(\alpha)$. Alors $E_\alpha((P(X))) = 0$, et on conclut par la propriété universelle de l'anneau quotient. Remarquons que l'image de E_α est $K[\alpha] \subseteq L$, donc si L est un corps de rupture de $P(X)$, on a $L = K[\alpha] = K(\alpha)$, d'où E_α est surjectif, et le K-morphisme $K_P \to L$, $X + (P(X)) \mapsto \alpha$, est un isomorphisme. On a alors $[L:K] = [K_P : K] = \deg P$. ▨

Rmq. Rappelons que si $\alpha \in L$ est algébrique dans L/K, alors $K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1} \mid a_i \in K\}$, où $d := \deg P$. De plus, $\{1, \alpha, \dots, \alpha^{d-1}\}$ est une base du K espace vectoriel $K[\alpha] = K(\alpha)$.

Corollaire 3.5. Soit $P(X) \in K[X]$ irréductible et L/K un corps de rupture. Soit M/K une extension dans laquelle P a une racine. Il existe un K-morphisme $L \hookrightarrow M$ et le nombre de tels morphismes est le nombre de racines de $P(X)$ dans M. C'est donc au plus $\deg P = [L:K]$, avec égalité si P a $\deg P$ - racines dans M

<u>Preuve:</u> Par la proposition 3.4, il existe un K-morphisme $L \overset{\varphi}{\hookrightarrow} M$. Soit $\alpha \in L$ une racine de $P(X) \in K[X]$. Si $P(X) = a_0 + a_1 X + \dots + a_n X^n$ alors $a_0 + a_1\alpha + \dots + a_n \alpha^n = 0$ et $\varphi(a_0 + a_1\alpha + \dots + a_n\alpha^n) = a_0 + a_1 \varphi(\alpha) + \dots + a_n \varphi(\alpha)^n = 0$, d'où $P(\varphi(\alpha)) = 0$. On a donc que $P(\varphi(\alpha)) = 0$, c-à-d, $\varphi(\alpha)$ est une racine de $P(X)$ dans M. Comme φ est un K-morphisme et que l'on peut supposer $L = K(\alpha)$, on a que φ est uniquement déterminé par $\varphi(\alpha)$, donc le nombre de tels morphismes est égal au nombre de racines de $P(X)$ dans M. ■

<u>Thm 3.6</u> Soit L/K une extension de corps engendrée par des racines d'un polynôme $P(X) \in K[X]$. Soit M/K une extension dans laquelle P est scindé. Il existe un K-morphisme de corps $L \hookrightarrow M$. Il y a au plus $[L:K]$ tels morphismes, avec égalité si $P(X)$ a $(\deg P)$ racines dans M.

<u>Preuve:</u> Soit $L = K(\alpha_1, \dots, \alpha_n)$, où $\alpha_1, \dots, \alpha_n \in L$ sont des racines de P dans L. Soit $P_{\alpha_1} \in K[X]$ le pol. min. de α_1 dans L/K. Comme $P(\alpha_1) = 0$, on a que $P_{\alpha_1} | P$ dans $K[X] \subseteq M[X]$, d'où $P_{\alpha_1}(X)$ est scindé sur M, avec $\deg P_{\alpha_1}$ racines dans M si P a $\deg P$ racines dans M. Par le corollaire 3.5, il existe un K-morphisme de corps $K(\alpha_1) \overset{\varphi_1}{\hookrightarrow} M$, et le nombre de tels morphismes est au plus $[K(\alpha_1):K]$, avec égalité dans le cas où P (et donc P_{α_1}) a $\deg P$ (resp. $\deg P_{\alpha_1}$) racines

dans M.

– Pour $\alpha_2 \in L$, soit $P_{\alpha_2} \in K(\alpha_1)[X]$ son pol. min. dans $L/K(\alpha_1)$.
Comme $P(\alpha_2) = 0$, on a que $P_{\alpha_2} \mid P$ dans $K(\alpha_1)[X]$, donc
$\varphi_1(P_{\alpha_2})$ est scindé dans $M[X]$ avec $\deg P_{\alpha_2}$ racines si P a
$\deg P$ racines dans M. Cela découle de l'implication ($P_{\alpha_2} \mid P$ dans $K(\alpha_1)[X]$
$\Rightarrow$ ~~$\varphi_1(P_{\alpha_2})$~~ ($\varphi_1(P_{\alpha_2}) \mid \varphi_1(P) = P$ dans $\varphi_1(K(\alpha_1))$). Il existe alors un
$\varphi_1(K(\alpha_1))$ – morphisme $\varphi_1(K(\alpha_1))(\alpha_2) \xrightarrow{\varphi_2} M$ et il y a au
plus $[\varphi_1(K(\alpha_1))(\alpha_2) : \varphi_1(K(\alpha_1))]$ tels morphismes, avec égalité si
P a $(\deg P)$ racines dans M. Remarquons que $[\varphi_1(K(\alpha_1))(\alpha_2) : \varphi_1(K(\alpha_1))]$
$= [K(\alpha_1, \alpha_2) : K(\alpha_1)]$.

– On a donc un K-morphisme

$$\begin{array}{ccccc} K(\alpha_1) & \xrightarrow{\varphi_1} & & & \\ \downarrow & & & & \\ K(\alpha_1,\alpha_2) & \xrightarrow{\sim} & \varphi_1(K(\alpha_1))(\alpha_2) & \xrightarrow{\varphi_2} & M, \\ \alpha_1 & \mapsto & \varphi_1(\alpha_1) & & \\ \alpha_2 & \mapsto & \alpha_2 & & \end{array}$$

avec au plus $\underbrace{[K(\alpha_1, \alpha_2) : K]}_{\text{pour } \varphi_2} \cdot \underbrace{[K(\alpha_1) : K]}_{\text{pour } \varphi_1} \overset{\text{thm. 1.5}}{=} [K(\alpha_1, \alpha_2) : K]$ choix,
avec égalité si P a $(\deg P)$ racines dans M.
On répète ~~ce~~ le même argument n-fois pour arriver à la conclusion. $\blacksquare$

<u>Déf. 3.7</u> Soit $P(X) \in K[X]$. Une extension L/K est dite un <u>corps de décomposition de $P(X)$</u> si $P(X)$ est scindé dans L et que L est engendré par les racines de $P(X)$.

<u>Corollaire 3.8</u> Soit $P(X) \in K[X]$ un polynôme. Il existe une extension L/K qui ~~est~~ est un corps de décomposition de $P(X)$. Tout deux corps de décomposition de $P(X)$ sont K-isomorphes. De plus, $[L:K] \leq$ ...

Preuve: Soit ~~...~~ L_1/K un corps de rupture pour un facteur irréd. de $P(X) \in K[X]$. Soit $L_1 = K(\alpha_1)$ avec $P(\alpha_1) = 0$. Alors $\frac{P(X)}{X-\alpha_1} \in L_1[X]$, et on construit un corps de rupture $L_2 = L_1(\alpha_2)$ d'un facteur irréductible de $\frac{P(X)}{X-\alpha_1} \in L_1[X]$. On continue ainsi jusqu'à ce que $\frac{P(X)}{Q(X)} \in L_{\deg P}[X]$ soit de degré 1. On a alors $[L_1 : K] \leq \deg P$, $[L_2 : L_1] \leq \deg P - 1, \dots, [L_{\deg P} : L_{\deg P-1}] \leq 2$, d'où $[L_{\deg P} : K] \leq (\deg P)!$. Remarquons que $P(X)$ est scindé dans $L_{\deg P}$, et que $L_{\deg P}/K$ est engendré par les racines $\alpha_1, \dots, \alpha_n$ de P dans $L_{\deg P}$. Donc $L := L_{\deg P}$ est un corps de décomposition de $P(X) \in K[X]$ et $[L : K] \leq (\deg P)!$.

Soit ~~...~~ maintenant M/K aussi un ~~...~~ corps de décomposition de $P(X)$. Par le thm. 3.6, il existe des K-morphismes $L \hookrightarrow M$ et $M \hookrightarrow L$, d'où $[M : K] \geq [L : K]$ et $[L : K] \geq [M : K]$. On a donc $[M : K] = [L : K]$, d'où $M \cong L$. ▨

Exemples: (1) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est un corps de décomposition de $X^3 - 2$. (de degré $3! = 6$)

(2) $\mathbb{Q}(i)/\mathbb{Q}$ est un corps de décomposition de $X^4 - 1$. (de degré $2 < 4!$)

(3) Soit $P(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ irréductible et $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ ses racines. Alors ~~...~~ pour deux de ces racines, par exemple α_1, α_2, on a $\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}$ est un corps de décomposition de $P(X)$. On a aussi que $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$, d'où $3 \leq [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \leq 3! = 6$ et

3) $[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]$, donc $[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}] \in \{3, 6\}$.

(4) Pour $P(X)=1+X+\dots+X^{p-1} \in \mathbb{Q}[X]$ avec p premier, un corps de décomposition de $P(X)$ est $\mathbb{Q}(\mu_p)/\mathbb{Q}$ – ext. cyclotomique.

(5) Pour $P(X)=X^3-2$, $[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]=6$

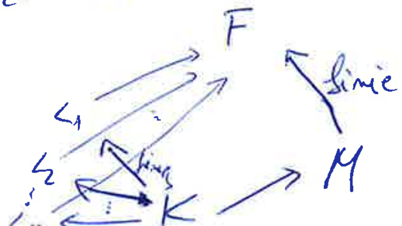
Pour $P(X)=X^3+X^2-2X-1 \in \mathbb{Q}[X]$, $[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]=3$

<u>Corollaire 3.9</u> Soit L/K une extension finie et M/K une extension. Il y a au plus $[L:K]$ K-morphismes $L \hookrightarrow M$. Il existe une extension finie F/M t.q. il existe un K-morphisme $L \to F$.

$$\begin{tikzcd} & F & \\ L \arrow[ur, "\exists"] & & M \arrow[ul, "\text{finie}"'] \\ & K \arrow[ul, "\text{finie}"] \arrow[ur] & \end{tikzcd}$$

<u>Preuve:</u> Soit $L=K(\alpha_1,\dots,\alpha_n)$ où $\alpha_1,\dots,\alpha_n$ sont algébriques dans L/K. Soit $P(X)\in K[X]$ le produit des pol. min. de $\alpha_1,\dots,\alpha_n$ sur K. Soit F/M un corps de décomposition de $P(X)\in K[X] \subseteq M[X]$. Par le thm. 3.6, $\exists\, L \hookrightarrow F$ et le nombre de tels morphismes est au plus $[L:K]$. Tout K-morphisme $L\to M$ induit un K-morphisme $L \to F$, donc il y a au plus $[L:K]$ tels morphismes. ∎

<u>Corollaire 3.10</u> Soient L_i/K, $i=1,2,\dots,n$ des ext. finies et M/K une extension. Il existe une extension finie F/M t.q. ils existent des K-morphismes $L_i \to F$, $i=1,2,\dots,n$.



Preuve: Par le corollaire précédent, il existe M_1/M finie t.q. $\exists$ un K-morphisme $L_1 \hookrightarrow M_1$. On applique maintenant ce même corollaire aux extensions L_2/K et M_1/K pour obtenir une extension M_2/K finie et l'existence d'un K-morphisme $L_2 \hookrightarrow M_2$. En continuant ce procédé, nous arrivons à ~~deux~~ une extension $F := M_n/M$-finie qui satisfait l'énoncé. ▨

Déf. 3.11 Soit $(P_i(X))_{i\in I}$ une famille de polynômes dans $K[X]$. Une extension L/K est dite un corps de décomposition pour la famille $(P_i)_{i\in I}$ si $\forall i \in I$, P_i est scindé dans L avec ensemble de racines R_i, et que $L = K(\bigcup_{i\in I} R_i)$.

Clôture algébrique

Soit K un corps.

Prop. 4.1 Les assertions suivantes sont équivalentes:

(1) Tout $P(X) \in K[X]\setminus K$ a au moins une racine dans K.

(2) Tout $P(X) \in K[X]\setminus K$ est scindé dans K.

(3) Les polynômes irréductibles dans $K[X]$ sont ceux de degré 1.

(4) Si L/K est une extension algébrique, alors $L = K$.

Preuve: (1) $\Rightarrow$ (2) Par récurrence sur $\deg P(X)$. Si $\alpha \in K$ est t.q. $P(\alpha) = 0$, alors $\frac{P(X)}{X-\alpha} \in K[X]$ et $\deg \frac{P(X)}{X-\alpha} = \deg P(X) - 1$, donc $\frac{P(X)}{X-\alpha}$ est scindé $\Rightarrow P(X)$ est scindé.

(2) $\Rightarrow$ (3) Immédiat.

(3) ⟹ (4) Soit L/K — alg. et $\alpha \in L$. Le pol. min. $P_\alpha(X) \in K[X]$ est irréd, donc de degré 1, ce qui implique que $\alpha \in K$ et donc $L = K$.

(4) ⟹ (1) Soit $P(X) \in K[X] \setminus K$. Soit $Q(X) \mid P(X)$ irréductible. Alors $K[X]/(Q(X))$ est une extension finie de K, d'où $K[X]/(Q(X)) \cong K$. De plus, $[K[X]/(Q(X)) : K] = \deg Q$, donc $Q(X)$ est de degré 1. Il existe alors $\alpha \in K$ t.q. $Q(\alpha) = 0 \Rightarrow P(\alpha) = 0$. ∎

<u>Définition 4.2</u> (1) Un corps K satisfaisant les propriétés équivalentes de la proposition est dit <u>algébriquement clos.</u>

(2) Un corps L est dit la <u>clôture algébrique</u> d'un sous-corps K si L est alg. clos et que L/K est algébrique.

<u>Exemples:</u> (1) $\mathbb{C}$ est alg. clos; $\mathbb{R}$ et $\mathbb{Q}$ ne le sont pas; $K(T)$ ne l'est pas non plus.

(2) $\mathbb{C}$ est une clôture alg de $\mathbb{R}$

$\mathbb{C}$ n'est pas une clôt. alg. de $\mathbb{Q}$

(3) Si L/K est une extension de corps avec L alg. clos, alors $\overline{K}^L$ est une clôture algébrique de K. Donc $\overline{\mathbb{Q}}$ est alg. clos, et c'est une clôt. alg. de $\mathbb{Q}$.

<u>Prop. 4.3</u> Une extension L/K. Alors L est une clôt. alg. de K ssi L/K alg. et tout polynôme de $K[X]$ est scindé dans L.

<u>Preuve:</u> (⟹) Immédiat.

(⟸) Mq L est alg. clos. Soit $P(X) \in L[X]$ irréductible. Soit

M/L une extension alg. dans laquelle $P(X)$ a une racine (par exemple, un corps de rupture de $P(X)$). Alors M/K est algébrique. Soit $\alpha \in M$ une racine de $P(X)$. Soit $P_\alpha \in K[X]$ le pol. min. de α. Comme $P(\alpha)=0$, ~~on a que~~ et que $P(X) \in \cancel{K}[X]$ irréductible, on a que $P_\alpha \mid P$ dans $L[X]$. Par hypothèse, P_α est scindé dans L, donc $P(X)$ est scindé dans $L[X]$, d'où $\deg P(X) = 1$, et donc L est alg. clos. Comme L/K -alg., on obtient le résultat. ∎

~~**Lemme:** Soit L/K une ext. algébrique et $\alpha \in L$ $L = K(\alpha)$. Soit P_α le polynôme min. de α. Soit M/K~~

Prop. 4.4 Soit L/K -algébrique et M un corps algébriquement clos. Tout morphisme $i : K \to M$ se prolonge en un morphisme $\varphi : L \to M$, c-à-d

$$\begin{tikzcd} L \arrow[r, "\varphi"] & M \\ & K \arrow[ul] \arrow[u, "i"'] \end{tikzcd}$$

est commutatif.

Preuve: Si L/K -finie, cela découle du corollaire .
Dans le cas général, on utilise le lemme de Zorn. On considère

$$\mathcal{E} := \{(E, \varphi) \mid L/E/K \text{ et } \varphi : E \to M \text{ prolonge } i\},$$

avec la relation d'ordre : $(E_1, \varphi_1) \leq (E_2, \varphi_2)$ si $E_1 \subseteq E_2$ et $\varphi_{2|E_1} = \varphi_1$.

Pour une chaîne $\{(E_i, \varphi_i)\}_{i \in I}$, le corps $\bigcup_{i \in I} E_i \subseteq L$ est une ext. alg. de K et $\varphi : \bigcup_{i \in I} E_i \to M$ t.q. $\varphi_{|E_i} = \varphi_i$ est un K-morphisme qui prolonge i.

Par le lemme de Zorn, $\mathcal{E}$ contient un élt. maximal (F, θ).

– Soit $\alpha \in L$. Comme α est algébrique dans L/F, par le thm. 3.6 on peut prolonger $\theta : F \to M$ à un morphisme $F(\alpha) \to M$, d'où par la maximalité de (F, θ)

nous obtenons $F(\alpha) = F$ et donc $\alpha \in F$, d'où $L = F$. $\blacksquare$

Prop. 4.5 Soit M/K - algébrique.

(1) Si M-alg. clos, toute ext. alg. L/K est K-isomorphe à un sous-corps de M. (à une sous-extension de M/K) De plus, M est une clôt alg. de L.

(2) Si toute extension finie L/K est isomorphe à une sous-extension de M/K, alors M est alg. clos.

Preuve: (1) Voir la ~~prop. 4.4~~ et conclure en remarquant que M/L-alg.

(2) Soit $P(X) \in K[X]$ - irréductible. ~~Soit $E = M(\alpha)$ un corps de~~

~~rupture de $P(X)$. Comme M/K-alg, on a que α est algébrique dans E/K et $K(\alpha)/K$ une extension finie. Il existe alors un K-morphisme $K(\alpha) \hookrightarrow M$ par hypothèse. Soit $P_\alpha \in K[X]$ le pol. min. de α dans E/K. Comme $P(X) \in M[X]$ est irréductible dans $M[X]$. De plus, $\varphi(\alpha)$ est une racine de $P_\alpha(X)$. On a que $P(X) \mid P_\alpha(X)$ dans $M[X]$.~~

Par la proposition 4.3, il suffit de m.q. $P(X)$ est scindé dans M. Soit L/K un corps de décomposition de $P(X)$. Alors il existe un K-morphisme $L \hookrightarrow M$, d'où $P(X)$ est scindé dans M. $\blacksquare$

Rmq. Soit M/K une extension avec M-alg. clos. Alors, par la prop., pour tout polynôme $P(X) \in K[X]$, M contient ~~un~~ exactement un corps de décomposition de $P(X)$.

De même pour le corps de décomposition d'une famille de polynômes $(P_i)_{i \in I}$ de $K[X]$.

Thm. 4.6 (Steinitz 1910) Soit K un corps. Il existe une clôture algébrique de K. Deux clôtures algébriques de K sont K-isomorphes.

Preuve: Voir le TD.

Rmq. Si $\varphi : K \to K'$ est un isomorphisme de corps et que M, resp. M' est une clôture algébrique de K, resp. K', alors φ se prolonge en un isomorphisme (non uniquement en général) de corps $\psi : M \to M'$.

$$\begin{tikzcd} K \arrow[r, "\sim", "\varphi"'] \arrow[d, hook] \arrow[dr] & K' \arrow[d, hook] \\ M \arrow[r, "\sim", "\psi"'] & M' \end{tikzcd}$$

l'ext. M'/K implique que M' est une clôt. alg. de K, donc M est K isomorphe à M'

Exemple: $\mathbb{R}(i) \longrightarrow \mathbb{R}(i)$ pour $\varphi : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$

$\psi_1 : \quad i \mapsto i$

$\psi_2 : \quad i \mapsto -i$

Déf./Notation 4.7 Dû au thm. de Steinitz, par abus de langage/notation, on parlera parfois de "la clôture algébrique" d'un corps K, et on "la" notera par $\overline{K}$.

Exemples: (1) $\overline{\mathbb{Q}} \subsetneq \overline{\mathbb{Q}(\pi)} \subsetneq \mathbb{C}$
↳ dénombrable

(2) En général, il est difficile de "décrire" $\overline{K}$ pour un corps K.

E.g. $\overline{k(T)}$ pour un corps k arbitraire.

Éléments conjugués

__Déf. 4.8__ Soit L/K une ext. de corps. Deux élts $\alpha, \beta \in L$ algébriques sont dit __conjugués__ sur K si $P_\alpha(X) = P_\beta(X) \in K[X]$, c-à-d ils ont les mêmes polynômes min. sur K.

__Exemples:__ (1) $i, -i$ sont conjugués dans $\mathbb{C}/\mathbb{R}$.

(2) $\sqrt[3]{2}, j\sqrt[3]{2}$ sont conjugués dans $\mathbb{C}/\mathbb{Q}$.

(3) $\sqrt{3}, i\sqrt{3}$ ne sont pas conjugués dans $\mathbb{C}/\mathbb{Q}$.

__Prop. 4.9__ Soit L/K une ext. de corps. Les énoncés suivants sont équivalents:

(1) α, β sont conjugués dans L/K,

(2) il existe un K-isomorphisme de corps $K(\alpha) \xrightarrow{\sim} K(\beta)$, $\alpha \mapsto \beta$.

__Preuve:__ (1) $\Rightarrow$ (2) Si $P_\alpha = P_\beta$ dans $K[X]$ alors $K(\alpha) \cong K[X]/(P_\alpha)$, $\alpha \mapsto X + (P_\alpha)$ et $K(\beta) \cong K[X]/(P_\beta(X))$, $\beta \mapsto X + (P_\beta)$, d'où $K(\alpha) \xrightarrow{\sim} K(\beta)$, $\alpha \mapsto \beta$.

(2) $\Rightarrow$ (1) On a que $P_\alpha(\beta) = 0$ et $P_\beta(\alpha) = 0$, d'où $P_\beta \mid P_\alpha$ et $P_\alpha \mid P_\beta$ dans $K[X]$ donc $P_\alpha(X) = P_\beta(X)$. ∎

__Rmq.__ Dans $\bar{K}$, les conjugués de $\alpha \in \bar{K}$ sont les racines de $P_\alpha \in K[X]$. Si L/K ext., et $\alpha \in L$ alg. dans L/K, alors les conjugués de α dans L sont les racines de $P_\alpha \in K[X]$, et il y a au plus $\deg P_\alpha$.

__Exemple:__ (1) Dans $\mathbb{F}_p(T)$, le polynôme min. de $\sqrt[p]{T} \in \overline{\mathbb{F}_p(T)}$ est donné par $X^p - T = (X - \sqrt[p]{T})^p$. Donc le seul conjugué de $\sqrt[p]{T}$ dans $\overline{\mathbb{F}_p(T)}$ est lui même.

(2) $\sqrt[3]{2}$ est son seul conjugué dans $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Prop. 4.10 Deux élts. $\alpha, \beta \in \overline{K}$ sont conjugués sur K ssi il existe un K-isomorphisme $\overline{K} \to \overline{K}$, $\alpha \mapsto \beta$.

Preuve: ($\Leftarrow$) Immédiat.

($\Rightarrow$) Il existe un ~~K-isomorphisme~~ $K(\alpha) \to K(\beta)$, $\alpha \mapsto \beta$. Il se prolonge en un isomorphisme

$$\begin{array}{ccc} & K & \\ K(\alpha) & \xrightarrow{\sim} & K(\beta) \\ \downarrow & & \downarrow \\ \overline{K(\alpha)} & \xrightarrow{\sim} & \overline{K(\beta)} \\ \alpha & \mapsto & \beta \end{array}$$

Comme $K(\alpha)/K$ et $K(\beta)/K$ sont algébriques, $\overline{K(\alpha)}$ et $\overline{K(\beta)}$ sont K-isomorphes à $\overline{K}$. ■

Extensions normales

Déf 5.1 Une ext. algébrique L/K est dite normale si $\forall P(X) \in K[X]$ irréductible, ($P(X)$ a une racine dans L) $\Rightarrow$ ($P(X)$ est scindé dans $L[X]$).

Exemples: (1) $\overline{K}/K$ est normale

(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale, ~~$\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ l'est~~

$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas normale

(3) $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ - normales

Prop. 5.2 Soit L/K - algébrique, $\overline{K}$ une clôt. alg. de K et $L \hookrightarrow \overline{K}$.
Les énoncés suivants sont équivalents:

(1) L/K - normale

(2) Pour $\alpha \in L$, les conjugués de α dans $\overline{K}/K$ sont des élts de L.

(3) Tout K-isomorphisme de $\overline{K}$ envoi L sur lui-même.

(4) L est le corps de décomposition d'une famille $(P_i(X))_{i\in I}$ avec $P_i \in K[X]$.

Preuve: (1) ⇒ (4) Si L/K normale, alors L est le corps de décomp. ~~d'une~~ ~~famille $(P_i(X))_{i\in I}$~~ de la famille des pol. min. des élts de L sur K.

(4) ⇒ (3) Soit $\varphi : \overline{K} \to \overline{K}$ un K-iso. Soit $R_i \subseteq \overline{K}$ l'ensemble des racines de $P_i(X)$ dans $\overline{K}$, $i \in I$. Alors $L = K(\bigcup_{i\in I} R_i)$. De plus, $\varphi(R_i) = R_i$ $\forall i \in I$, car φ fixe les coefficients de $P_i(X)$. Donc $\varphi(K(\bigcup_{i\in I} R_i)) = K(\bigcup_{i\in I} R_i)$.

(3) ⇒ (2) Soit $\alpha \in L$ et $\beta \in \overline{K}$ un conjugué de α dans $\overline{K}/K$. Alors il existe un K-iso $\varphi : \overline{K} \to \overline{K}$, $\alpha \mapsto \beta$, d'où $\beta = \varphi(\alpha) \in \varphi(L) = L$.

(2) ⇒ (1) Soit $P(X) \in K[X]$ irréd. et $\alpha \in L$ t.q. $P(\alpha) = 0$. Quitte à multiplier par un élt. de K (pour rendre P unitaire), on peut supposer que $P_\alpha = P$ dans $K[X]$. Les racines de P_α dans $\overline{K}$ sont précisément les conjugués de α dans $\overline{K}/K$, donc ce sont des élts. de L, d'où P est scindé sur L. ∎

Corollaire 5.3 Soit $M/L/K$ une tour de corps. Si M/K est normale, alors M/L l'est aussi.

Preuve: Immédiat par l'équivalence (1)⇔(4) de l'énoncé précédent. ∎

Corollaire 5.4 Une ext. L/K est normale et finie ⇔ L est le corps de décomp. d'un polynôme sur K.

Preuve: (⇒) Par l'équivalence (1)⇔(4) de la proposition, L est le corps de décomp. d'une famille $(P_i)_{i\in I}$ de polynômes sur K. Écrivons $L = K(S)$. Comme L/K est alg., $K(S) = K[S]$ car $\forall \alpha \in K(S)$, ~~[illegible]~~ $\alpha = \frac{\beta}{\gamma}$ avec $\beta, \gamma \in K[S]$ et $\gamma^{-1} \in K[\gamma] = K(\gamma)$, d'où $\gamma^{-1} \in K[\gamma] \subseteq K[S]$, donc $\alpha \in K[S]$. On a donc $\dim_K K[\gamma] < \infty$. ~~[illegible]~~

Preuve : ($\Leftarrow$) Immédiat par l'éq. (1)$\Leftrightarrow$(4) de la prop. 5.2.

($\Rightarrow$) Raisonnons par récurrence sur $[L:K]$. Si $[L:K]=1$, l'énoncé est clair. Supposons l'énoncé vrai pour tout $d<m$. Soit L/K t.q. $[L:K]=m$. Soit $\alpha_0 \in L\setminus K$ et $P_{\alpha_0} \in K[X]$ son pol. min. Alors $P_{\alpha_0}(X)$ est scindé sur L, et soit $K_0 \subseteq L$ le corps de décomposition de $P_{\alpha_0}(X)$ contenu dans L. Comme $K \subsetneq K_0 \subseteq L$, on a que $[L:K_0]<m$. Comme L/K_0 est normale par le cor. précédent, on a, par l'hypothèse de récurrence, que L est le corps de décomp. d'un $Q(X) \in K_0[X]$. ~~Alors L est le corps de décomposition de $R(X) := P_{\alpha_0}(X)$~~

- Soient $\alpha_1, \ldots, \alpha_m \in L$ les racines de $Q(X)$. On a que $L = K_0(\alpha_1, \ldots, \alpha_m)$, donc $L = K(\alpha_0, \alpha_1, \ldots, \alpha_m)$. Alors L est le corps de décomposition du pol. $R(X) \in K[X]$, obtenu comme produit des pol. min. des α_i sur K pour $i \in \{0,1,\ldots,m\}$. ■

Exemples : (1) Dans la tour $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, l'extension $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est normale, mais $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ne l'est pas.

(2) Dans la tour $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, les extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont normales, mais $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas.

Corollaire 5.5 Soit L/K alg. et M un corps algébriquement clos t.q. M/K. Alors, (Si $\varphi_1 : L \to M$ et $\varphi_2 : L \to M$ sont des K-morphismes, on a $\varphi_1(L) = \varphi_2(L)$) $\Leftrightarrow$ (L/K est une ext. normale).

Preuve : ($\Leftarrow$) Par l'équivalence (1)$\Leftrightarrow$(4) de la prop. 5.2, on a que $\varphi_1(L)$ et $\varphi_2(L)$ coïncident avec l'unique sous-corps de M qui est un corps de décomp. pour la famille $(P_i)_{i\in I}$ dans $K[X]$ qui induit l'ext. L/K.

($\Rightarrow$) Soit $L_0 := \varphi_1(L)$. Soit $P(X) \in K[X]$ irréductible et $\alpha \in L$ t.q.

$P(\alpha)=0$. Soit $\beta \in M$ une racine de $P(X)$. Alors les corps de rupture $K(\alpha)$ et $K(\beta)$ de $P(X)$ sont K-isomorphes et il existe un K-isomorphisme

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sim} & K(\beta) \subseteq M \\ \alpha & \mapsto & \beta \end{array}$$

Cet isomorphisme se prolonge en un K-morphisme $L \xrightarrow{\varphi} M$ via

$$\begin{tikzcd} & & K \arrow[dl, hook] \arrow[dr] & & \\ & K(\alpha) \arrow[r, "\sim"] \arrow[dl] \arrow[d] & & K(\beta) \arrow[d] \arrow[dr, bend left] & \\ L \arrow[r, hook] & \overline{K} \arrow[rr, "\sim"] & & \overline{K} \arrow[r, hook] & M . \end{tikzcd}$$

$\alpha \mapsto \beta$, $\overline{K} = \overline{K}^M$

Alors $\varphi(L) = L_0$ avec $\varphi(\alpha)=\beta \in L_0$. Donc toute racine de $P(X)$ dans M est un élt. de L_0, c-à-d $P(X)$ est scindé sur L_0, et donc dans L, d'où L/K-normale. ■

<u>Corollaire 5.6</u> Soit $M/L/K$ une tour de corps avec M/K-normale. Alors L/K est normal ssi $\forall$ K-automorphisme φ de M, on a $\varphi(L)=L$.

<u>Preuve:</u> Soit $\overline{K}$ t.q. $M \subseteq \overline{K}$. Par le corollaire précédent pour tout K-morphisme $M \xrightarrow{\varphi} \overline{K}$, $\varphi(M)=M$.

(⇒) Soit $\varphi: M \to M$ un K-isomorphisme. Il se prolonge en un K-iso. $\overline{\varphi}: \overline{K} \to \overline{K}$. Si L/K-normale, alors $\overline{\varphi}(L)=L$, donc $\varphi(L)=L$.

(⇐) Soit $\varphi: L \to \overline{K}$ un K-morphisme. Il se prolonge à $\overline{\varphi}: M \to \overline{K}$, d'où $\overline{\varphi}(M)=M$ et par hypothèse, $\overline{\varphi}(L)=L$, donc $\varphi(L)=L$, ce qui, par le cor. précédent, implique que L/K-normale. ■

<u>Corollaire 5.7</u> Soit L/K normale. Tout automorphisme de K se prolonge en un auto. de L.

Preuve : Soit $\varphi : K \to K$ un iso. de corps. Alors il se prolonge à un isomorphisme $\overline{\varphi} : \overline{K} \to \overline{K}$. Comme L/K normale, $\overline{\varphi}(L) = L$ (en supposant $L \subseteq \overline{K}$), donc $\overline{\varphi}_{|L} : L \to L$ est ~~un automorphisme de L~~ un automorphisme de L.

Thm. 5.8 Soit L/K alg. et ~~...~~ M un corps alg. clos t.q. $L \subseteq M$. Il existe une plus petite ext. normale E/K t.q. $L \subseteq E \subseteq M$. On dira que E est la clôture normale de L dans M.

Preuve : - Soit $S \subseteq L$ t.q. $L = K(S)$. Pour $s \in S$, soit $P_s(X) \in K[X]$ son pol. min. Soit E/K l'ext. engendrée par $\bigcup_{s\in S}$ (racines de $P_s(X)$ dans M). Alors E est le corps de décomposition de $(P_s)_{s\in S}$ dans M, donc E/K est normale. De plus, $K \subseteq L \subseteq E \subseteq M$.

- Soit E'/K une ext. normale t.q. $L \subseteq E' \subseteq M$. Comme $S \subseteq E'$, E' contient toutes les ~~conjugués~~ racines de $P_s(X)$ dans M, $\forall s \in S$, donc $E \subseteq E'$.

Polynômes séparables

Caractéristique d'un corps.

Soit K un corps. L'on peut toujours définir un morphisme d'anneaux $\theta : \mathbb{Z} \longrightarrow K$ t.q. $\theta(n) := \underbrace{1_K + \dots + 1_K}_{n\text{-fois}}$ si $n \geq 0$ et $\theta(n) := \underbrace{(-1)_K + \dots + (-1)}_{|n|\text{-fois}}$ si $n < 0$.

Ier cas : Si $\ker\theta = \{0\}$, on dira que K est de caractéristique nulle et on écrira $\mathrm{car}(K) = 0$.

Dans ce cas, θ se prolonge à $\mathbb{Q} \hookrightarrow K$.
$\frac{a}{b} \mapsto \frac{\theta(a)}{\theta(b)}$

II ème cas : $\mathrm{Ker}\,\theta = p\mathbb{Z}$ (p doit être premier, car $\mathrm{Ker}\,\theta$ est un idéal premier de $\mathbb{Z}$), dans quel cas on a ~~les~~ morphisme induit

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \hookrightarrow K.$$

On dira que K est de caractéristique p et on écrira $\mathrm{car}(K)=p$.

Dans ce cas, l'application

$$\mathrm{Fr}_K : K \longrightarrow K, \quad x \mapsto x^p$$

est un morphisme de corps, dit le morphisme de Frobenius.

Exemples : (1) La car. de $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(T), \mathbb{R}(T), \mathbb{C}(T)$ est nulle.

(2) La car. $\mathbb{F}_p$, $\mathbb{F}_p(T)$, $\mathbb{F}_p(T_1, \dots, T_m)$ est p, pour p un nombre premier fixé quelconque.

- Rappelons que pour $P(X) \in K[X]$ avec $P(X) = \sum_{i=0}^{m} a_i X^i$, on définit sa dérivée $P'(X) = \sum_{i=0}^{m-1} i \cdot a_i X^{i-1}$. C'est aussi un polynôme dans $K[X]$.
Ici, $i \cdot a_i := \theta(i) a_i \in K$.

Rmq. On peut définir l'application dérivée :

$$\partial : K[X] \longrightarrow K[X], \quad P(X) \mapsto P'(X)$$

C'est l'unique application K-linéaire sur $K[X]$ satisfaisant $\partial(PQ) = \partial P\, Q + P\, \partial Q$.

Rmq. Supposons que $P(X) \in K[X]$ est t.q. $P'(X) = 0$.

- Si $\mathrm{car}\, K = 0$, alors $\deg P = 0$
- Si $\mathrm{car}\, K = p > 0$, alors $p \mid i$ $\forall i$ t.q. $a_i \neq 0$, d'où

$\exists!\, Q \in K[X]$ t.q. $P(X) = Q(X^p)$.

Déf. 5.8 Soit L/K une extension de corps et $P(X) \in K[X]$. Alors $\alpha \in L$ est dite une racine de multiplicité m de $P(X)$ si $P(\alpha) = 0$ et que $(X-\alpha)^m \mid P(X)$ dans $L[X]$, mais $(X-\alpha)^{m+1} \nmid P(X)$ dans $L[X]$. Si $m = 1$, α est dite une racine simple de $P(X)$, et sinon une racine multiple.

Rmq. Si $P(X)$ est scindé sur L, alors α est une racine de mult. m $\Leftrightarrow$ $P(X) = (X-\alpha)^m \cdot c \cdot \prod_{i=1}^{s} (X - \beta_i)^{n_i}$ avec $\beta_i \neq \alpha$ pour tout i et $c \in K^\times$.

Déf. 5.9 Un polynôme $P(X) \in K[X]$ est dit séparable si l'idéal $(P'(X), P(X))$ est $K[X]$, c-à-d si P et P' sont premiers entre eux.

Exemples : (1) Si $\deg P = 1$, alors $P(X)$ est séparable.

(2) $X^2 + 1 \in \mathbb{C}[X]$ est séparable.

(3) $X^p - T \in \mathbb{F}_p(T)[X]$ n'est pas séparable.

Lemme 5.10 Un polynôme est séparable ssi il n'a pas de racines multiples dans son corps de décomposition.

Preuve : $(\Rightarrow)$ Soit L/K un corps de décomp. de $P(X) \in K[X]$. Supposons qu'il existe $\alpha \in L$ t.q. $P(\alpha) = 0$ et que $(X-\alpha)^2 \mid P(X)$ dans $L[X]$. Alors $P'(X) = ((X-\alpha)^2 \cdot Q(X))' = 2(X-\alpha) \cdot Q(X) + (X-\alpha)^2 Q'(X)$ pour un $Q(X) \in L[X]$, d'où $\cancel{P'(\alpha)=0}$ $(X-\alpha) \mid P'(X)$ dans $L[X]$, c-à-d

Donc $(X-\alpha) \supseteq (P(X), P'(X))$ $\cancel{\text{dans } L[X]}$ dans $L[X]$, $(P(X), P'(X)) \neq (1)$ dans $L[X]$. Mais pgcd$(P(X), P'(X))$ ne dépend pas du corps (par l'algorithme d'Euclid), ~~donc~~ et $(P(X), P'(X)) =$

(pgcd (P,P')) dans $K[X]$ et dans $L[X]$. Donc, contradiction avec l'hyp. P-séparable.

($\Leftarrow$) Soit $R(X) \in K[X]$ irréductible t.q. $(R(X)) = (P, P')$. Alors $R(X) \mid P(X)$ et $R(X) \mid P'(X)$. Alors dans un corps de décomposition L de $P(X)$, ~~...~~ $\exists \alpha \in L$ t.q. $R(\alpha)=0$, d'où $(X-\alpha) \mid P(X) \Rightarrow P(X) = (X-\alpha) \cdot Q$ et $P'(X) = Q(X) + Q'(X)(X-\alpha)$, et $P'(\alpha)=0 \Rightarrow Q(\alpha)=0$, et donc α est une racine multiple de $P(X)$, absurde. Donc $R(X)$ n'a pas de racines dans $L \Rightarrow R(X) \in K^*$, et donc P-séparable. ▨

<u>Rmq.</u> Le polynôme $P(X) \in K[X]$ est séparable ssi P a exactement $\deg P$ racines dans $\overline{K}$.

<u>Corollaire 5.11</u> (1) Un polynôme $P(X) \in K[X]$ irréductible est séparable ssi $P' \neq 0$.

(2) Si car $K = 0$, alors irréductible $\Rightarrow$ séparable.

(3) Si car $K = p > 0$, alors $P(X) \in K[X]$ irréductible est séparable ssi $P(X) \notin K[X^p]$.

<u>Preuve:</u> (1) $K[X]$ est principal, donc $(P(X), P'(X)) = (R(X))$ pour un $R(X) \in K[X]$, d'où $R(X) \mid P(X)$ dans $K[X]$. Donc $P(X)$ irréductible $\Rightarrow R(X) = \underset{\alpha \in K}{\alpha} \cdot P(X)$ ou $R(X) \in K^*$. Si $P(X)$-séparable, on a que $R(X) \in K^\times$, donc $P'(X) \neq 0$ car $(P(X), 0) = (P(X)) \neq K[X]$. Si $P' \neq 0$, alors $(P, P') \neq (P)$ (car sinon $P \mid P'$, absurde car $\deg P' < \deg P$), d'où $R(X) \in K^\times$, et donc $(P, P') = K[X]$ c-à-d P-séparable.

(2) $P(X)$-irréductible, et $P'(X) = 0 \Rightarrow \deg P = 0$, absurde,

donc $P'(X) \neq 0 \overset{\text{par (1)}}{\Rightarrow} P(X)$-séparable.

(3) Pour $P(x) \in K[X]$ — irréductible, $P(x)$ — sép. $\Leftrightarrow P'(x) \neq 0$

$\Leftrightarrow P(x) \notin K[x^p]$. ∎

<u>Corollaire 5.12</u> $P(X) \in K[X] \setminus K$ est séparable ssi c'est le produit de différents polynômes irréductibles ~~et~~ séparables.

<u>Preuve:</u> ($\Leftarrow$) Soit $P(X) = c \cdot \prod_{i=1}^{m} Q_i(X) \in K[X]$ avec les $Q_i(X)$ - différents, irréductibles ~~et~~ séparables dans $K[X]$. Soit $\overline{K}$ une clot. algébrique de K. Alors Q_i a deg Q_i racines diff. dans $\overline{K}$, on ~~peut~~ peut les supposer unitaires, et donc on peut supposer que Q_i est le pol. min. de ses racines sur K, pour tout i.
Soit $Z_i := \{\alpha \in \overline{K} \mid Q_i(\alpha) = 0\}$ pour $i = 1, 2, \ldots, m$. Alors $Z_i \cap Z_j = \phi$, d'où $Z_P := \bigsqcup_{i=1}^{m} Z_i$ est une union disjointe, égale à l'ensemble des racines de $P(X)$ dans $\overline{K}$. Comme $\mathrm{Card}(Z_P) = \sum_{i=1}^{m} \mathrm{Card}(Z_i) = \sum_{i=1}^{m} \deg Q_i = \deg P$, on a que P est ~~irréductible~~ séparable. ∎

($\Rightarrow$) Immédiat.

<u>Question:</u> Sous quelles conditions irréductible $\Rightarrow$ séparable?

<u>Déf. 5.13</u> Un corps K est dit <u>parfait</u> si tout pol. irréductible sur K est séparable.

~~Rem.~~ <u>Prop. 5.14</u> K est parfait ssi car $K = 0$ ou car $K = p > 0$ et ~~the~~ $K = K^p := \{x^p \mid x \in K\}$. (c-à-d le Frobenius est un isomorphisme)

<u>Preuve:</u> Si car $K = 0$, alors K est parfait par le cor. 5.11 (2).
Supposons car $K = p > 0$, mais que $K \neq K^p$, c-à-d $\exists \alpha \in K \setminus K^p$.

Le polynôme $P(X) := X^p - a \in K[X^p]$ est irréductible, mais non séparable. Pour l'irréductibilité, si $Q(X) \mid P(X)$ est irréductible, alors dans un corps de rupture L/K de $Q(X)$, on a que $Q(X) = (X-\alpha)^i$ pour $1 \leq i \leq p$ et $\alpha \in L$, car $\alpha^p = a$, donc $P(X) = (X-\alpha)^p$ dans $L[X]$. Si $(i,p)=1$, alors $\exists m, n \in \mathbb{Z}$ t.q. $\alpha^{mi+np} = \alpha^1 = \alpha \in K$, absurde car $\alpha^p = a \notin K^p$. Donc $p \mid i$, d'où $i = p$ et $P(X)$ — irréductible.

- Si $K = K^p$, et $P(X) \in K[X]$ est irréductible, mais non séparable, alors $P(X) \in K[X^p]$, d'où $P(X) = Q(X)^p$ avec $Q(X) \in K[X]$, absurde.

<u>Exemples:</u> (1) Tout corps fini est parfait.

(2) Tout corps alg. clos est parfait.

(3) $\mathbb{F}_p(T)$ n'est pas parfait.

Extensions séparables

<u>Déf. 6.1</u> Une ext. de corps L/K - alg. est dite <u>séparable</u> si $\forall \alpha \in L$, le polynôme minimal de α sur K est séparable.

Le <u>degré séparable</u> d'une extension algébrique M/K est

$$\mathrm{Card}(\{\sigma : M \hookrightarrow \bar{K} \mid \sigma \text{ prolonge } K \hookrightarrow \bar{K}\}),$$

où $\bar{K}$ est une clôt. alg. de K. On le notera $[M:K]_s$.

<u>Rmq.</u> La notion de $[M:K]_s$ est bien définie : par le thm. de Steinitz, $[M:K]_s$ ne dépend pas de la clôture algébrique $\bar{K}/K$. De plus, on sait que $[M:K]_s > 0$.