Exemples : (1) $\mathbb{C}/\mathbb{R}$ est séparable et $[\mathbb{C}:\mathbb{R}]_s = 2$

(2) Soit p-premier, $L := \mathbb{F}_p(T)$ et $K := L^p = \mathbb{F}_p(T^p)$.

Alors $[L:K] = p$. Si $\sigma : L \to \overline{K}$ est un prolongement de $K \xrightarrow{i} \overline{K}$, alors $\sigma(T) = \sigma(T^p)^{1/p} = i(T^p)^{1/p}$, d'où σ est uniquement déterminé par i, car $X^p - i(T^p) = (X - \sigma(T))^p$ dans $\overline{K}[X]$. Donc, $[L:K]_s = 1 < p = [L:K]$.

(3) Si car $K = 0$, L/K-alg. $\Rightarrow$ L/K-séparable.
Si $L/\mathbb{F}_p$-alg., alors $L/\mathbb{F}_p$-séparable (car $\mathbb{F}_p$-parfait).

Rmq. (1) Soient $\sigma_1 : K \hookrightarrow \overline{K_1}$ et $\sigma_2 : K \hookrightarrow \overline{K_2}$ deux clôtures alg. de K. Par la prop. 4.4, comme $\overline{K_1}/K$ est algébrique, il existe $\varphi : \overline{K_1} \hookrightarrow \overline{K_2}$. Soit $\alpha \in \overline{K_2}$ et $P_\alpha(X) \in K[X]$

$$\begin{tikzcd} \overline{K_1} \arrow[rr, hook, "\varphi"] & & \overline{K_2} \\ & K \arrow[ul, "\sigma_1"] \arrow[ur, "\sigma_2"'] & \end{tikzcd}$$

son pol. minimal, c-à-d $(\sigma_2 P_\alpha)(\alpha) = 0$, où $(\sigma_2 P_\alpha)(X) \in \overline{K_2}[X]$ et donc $(X - \alpha) \mid (\sigma_2 P_\alpha)(X)$ dans $\overline{K_2}[X]$. Comme $\overline{K_1}$ est alg. clos, $\varphi(\overline{K_1})$ l'est aussi, donc $\sigma_2 P_\alpha = (\varphi \circ \sigma_1) P_\alpha \in \varphi(\overline{K_1})[X]$ est scindé dans $\varphi(\overline{K_1})[X] \subseteq \overline{K_2}[X]$, d'où $X - \alpha \in \varphi(\overline{K_1})[X]$ et $\alpha \in \varphi(\overline{K_1})$.
On a que φ est un K-isomorphisme. (Si $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$, $\sigma P(X) := \sum_{i=0}^{n} \sigma(a_i) X^i \in \sigma(K)[X]$)

(2) Soit L/K une ext. de corps algébrique. Soient $\sigma_1 : K \to \overline{K_1}$ et $\sigma_2 : K \to \overline{K_2}$ deux clôt. alg. de K. Alors

$$\begin{aligned} \{\pi : L \to \overline{K_1} \mid \pi \text{ prolonge } \sigma_1\} &\longrightarrow \{\psi : L \to \overline{K_2} \mid \psi \text{ prolonge } \sigma_2\} \\ \pi &\longmapsto \varphi \circ \pi \end{aligned}$$

est une bijection, donc $[L:K]_s$ ne dépend pas de la clôture alg. de K.

(3) Si L/K n'est pas algébrique, alors $[L:K]_s = 0$. Sinon, $[L:K]_s > 0$ par la prop. 4.4.

Lemme 6.2. Soit $M/L/K$ une tour de corps algébrique. Alors
$$[M:K]_s = [M:L]_s \cdot [L:K]_s.$$

Preuve: Soit $\overline{K}/K$ une clôt. alg. Soit $(\sigma_i)_{i\in I}$ la famille des K-plongements $L \hookrightarrow \overline{K}$, d'où $[L:K]_s = \text{Card}(I)$. Pour $i \in I$ fixé, $\sigma_i : L \hookrightarrow \overline{K}$ est une clôt. algébrique de L, donc elle a $[M:L]_s$ prolongements à $M \hookrightarrow \overline{K}$ (voir la remarque précédente); notons les $(\varphi_j^i)_{j\in J}$ avec $[M:L]_s = \text{Card}(J)$. Alors les prolongements de $K \hookrightarrow \overline{K}$ à $M \hookrightarrow \overline{K}$ sont en bijection avec $(\varphi_j^i)_{(i,j)\in I\times J}$, d'où $[M:K]_s = \text{Card}(I\times J) = [M:L]_s \cdot [L:K]_s$. ∎

Thm. 6.3. Soit L/K une extension finie.

(1) S'il existe $S \subseteq L$ fini et consistant d'élts. séparables dans L/K, alors L/K est séparable. Un élt. $\alpha \in L$ est dit séparable dans L/K si son polynôme min. sur K est séparable.

(2) On a $[L:K]_s \leq [L:K]$, avec égalité ssi L/K est séparable.

<u>Preuve</u> : Si $L = K(\alpha)$ avec $P_\alpha \in K[X]$ le pol. min. de $\cancel{\alpha}$, alors $[L:K]_s$ est le nombre de racines diff. de P_α dans $\overline{K}$ ~~et~~ est au plus $[L:K]$ par le cor. 3.5, d'où $[L:K]_s \leq [L:K]$, avec égalité ssi P_α a $(\deg P_\alpha)$ racines dans $\overline{K}$, donc ssi P_α est séparable. Ici $\overline{K}$ est une clôt. alg. de K.

- Soit $L = K(S)$. Comme L/K finie, on peut supposer que S est fini. Écrivons $S = \{\alpha_1, \dots, \alpha_n\}$. En appliquant la multiplicativité du ~~E~~ degré et du degré séparable à la tour de corps
$$K \subseteq K(\alpha_1) \subseteq \dots \subseteq K(\alpha_1, \dots, \alpha_n) \subseteq L,$$
on obtient $[L:K]_s \leq [L:K]$ par le paragraphe précédent.

- Si $\{\alpha_1, \dots, \alpha_n\}$ consiste d'élts. séparables dans L/K, alors $\forall i$, α_i est séparable dans $K(\alpha_1, \dots, \alpha_i)/K(\alpha_1, \dots, \alpha_{i-1})$ (car le pol. min de α_i sur $K(\alpha_1, \dots, \alpha_{i-1})$ divise le pol. min. de α_i sur K, et ce dernier n'a pas de racines mult. dans $\overline{K}$), donc $[L:K]_s = [L:K]$ dans ce cas par le premier paragraphe.

- Si $[L:K] = [L:K]_s$, alors $\forall \alpha \in L$, on a $[L:K(\alpha)]_s = [L:K(\alpha)]$, et $[K(\alpha):K]_s = [K(\alpha):K]$, d'où α est séparable dans L/K, et donc L/K est séparable. ∎

<u>Rmq.</u> Si $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{p} \mid p\text{-premier})$, alors $[L:\mathbb{Q}]$ est ∞ dénombrable, mais $\{\sigma : L \to \overline{\mathbb{Q}}\} = \{$choix de $+1$ ou -1 pour chaque p premier$\}$,

$\sigma : \sqrt{p} \mapsto \sqrt{p}$
ou $\sigma : \sqrt{p} \mapsto -\sqrt{p}$

donc $\mathrm{Card}\{\sigma : L \xrightarrow{\mathbb{Q}} \overline{\mathbb{Q}}\} = [L:K]_s$ est ∞ non dénombrable.

Proposition 6.4. Soit $M/L/K$ une tour de corps. Si $\alpha \in M$ est séparable dans M/L et que L/K est séparable, alors α est séparable dans M/K.

Par conséquent, M/K est séparable ssi M/L et L/K le sont.

Preuve: Soit $P_\alpha \in L[X]$ le pol. min. de $\alpha \in M$. Soit K'/K la sous-extension de L/K engendrée par les coéfficients du pol. P_α. Alors K'/K est séparable par le thm. précédent, d'où $[K':K]_s = [K':K]$. Comme $P_\alpha \in K'[X]$, on a que P_α est le pol. min. de α dans M/K', donc α est séparable dans M/K', ce qui implique que $K'(\alpha)/K'$ est séparable (par le thm. 6.3(1)) et donc $[K'(\alpha):K']_s = [K'(\alpha):K']$. On obtient que $[K'(\alpha):K] = [K'(\alpha):K]_s$, c-à-d que l'ext. $K'(\alpha)/K$ est séparable, d'où α est séparable dans M/K.

- Si M/L et L/K sont séparables, alors par le paragraphe précédent, M/K l'est aussi. Si M/K - séparable, alors L/K est séparable par déf. Soit $\alpha \in M$. Alors $P_{\alpha,L} \mid P_{\alpha,K}$ et donc si $P_{\alpha,K}$ est séparable, $P_{\alpha,L}$ l'est aussi, d'où α est séparable dans M/L si elle est séparable dans M/K. ∎

Corollaire 6.5 L'ensemble des élts. séparables d'une extension L/K est une sous-extension séparable sur K. On l'appelle la clôt. séparable de K dans L.

Preuve: Pour $\alpha, \beta \in L$ séparables dans L/K, on a que $K(\alpha,\beta)/K$ - sép., et donc $\alpha-\beta$ et $\alpha\beta^{-1}$ (si $\beta \neq 0$) sont séparables car dans $K(\alpha,\beta)$. ∎

Rmq. (1) Si L/K-algébrique et $L = K(S)$ avec $S \subseteq L$ consistant d'élts séparables, alors L/K est séparable.

(2) On peut définir "la" clôture séparable d'un corps K comme étant la clôt. sép. de K dans $\overline{K}$. On la note $\overline{K}^{sep}$ ou $\overline{K}^{s}$ d'habitude. Elles sont toutes K-isomorphes.

Déf. 6.6 Une extension algébrique L/K est dite purement inséparable ou radicielle si la clôt. sép. de K dans L est K.

Rmq. (1) L'extension $\overline{K}/\overline{K}^{sep}$ est purement inséparable.

(2) S'il existe une extension L/K avec ~~[illegible]~~ $[L:K] > 1$ et purement inséparable, alors car $K > 0$. Donc si car $K = 0$, on a $\overline{K} = \overline{K}^{sep}$.

Exemple: L'extension $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ est pur. inséparable.

Proposition 6.7 (1) Soit K un corps. Alors K est parfait ssi $\overline{K} = \overline{K}^{sep}$.

(2) Si $L/\overline{K}^{sep}$ est séparable, ~~[illegible]~~ on a $L = \overline{K}^{sep}$.

(3) Pour $\alpha \in \overline{K} \setminus \overline{K}^{sep}$, α n'est pas séparable dans $\overline{K}/\overline{K}^{sep}$, et pas séparable dans $\overline{K}/K$.

Preuve: (1) K-parfait $\Leftrightarrow$ (pol. irréd. $\Rightarrow$ séparable) $\Leftrightarrow$ tout pol. minimal d'élts de $\overline{K}$ ~~[illegible]~~ sur K est séparable $\Leftrightarrow$ $\overline{K} = \overline{K}^{sep}$.

(2) $L/\overline{K}^{sep}$-algébrique, donc $\exists\ L \hookrightarrow \overline{K}$ avec L/K-séparable, d'où $L \subseteq \overline{K}^{sep}$ et donc $L = \overline{K}^{sep}$.

$$\begin{tikzcd} L \arrow[r, hook] & \overline{K} \\ \overline{K}^{sep} \arrow[u] \arrow[ur] & \\ K \arrow[u] \arrow[uu, bend left, "alg"] & \end{tikzcd}$$

(3) Voir (2). $\blacksquare$

Déf. 6.8 Un corps K est dit séparablement clos si $K = \overline{K}^{sep}$.

Prop. 6.9 (1) Un corps K est sép. clos ssi tout polynôme irréd. et séparable sur K est ~~[illegible]~~ de degré 1.

(2) Toute extension séparable d'un corps K se plonge dans $\bar{K}^{sep}$!

Preuve: (1) ($\Rightarrow$) Supposons $K = \bar{K}^{sep}$. Soit $P(X) \in K[X]$ irréd. et séparable. Alors ses racines dans $\bar{K}$ sont simples, et donc des élts. séparables dans $\bar{K}/K$, donc des élts. de K, d'où deg $P = 1$. ($\Leftarrow$) Immédiat.

(2) Soit L/K-sép. et $\bar{K}$ une clôt. alg. de K. Alors il existe

$$\begin{tikzcd} L \arrow[r, hook, "\varphi"] & \bar{K} \\ & K \arrow[ul] \arrow[u] \end{tikzcd}$$

et son image est séparable sur K, d'où

$$\begin{tikzcd} L \arrow[r, hook, "\varphi"] & \bar{K}^{sep} \arrow[r, hook] & \bar{K}. \\ K \arrow[u] \arrow[ur] \end{tikzcd}$$

Théorème de l'élément primitif

~~[illegible]~~

Thm 6.10 Soit K un corps et $L = K(\alpha_1, \ldots, \alpha_n)$ une extension finie de K. Si $\alpha_2, \alpha_3, \ldots, \alpha_n$ sont séparables dans L/K, alors $\exists \beta \in L$ telle que $L = K(\beta)$. On dit dans ce cas que L/K est une extension simple.

Preuve: Ier cas: K - infini.

Il suffit de montrer le résultat pour $n = 2$. Soient $P_{\alpha_1}, P_{\alpha_2}$ les pol. min. de α_1, α_2 resp., sur K. Soit M/L un corps de décomposition de $P_{\alpha_1} P_{\alpha_2}$. Alors dans $M[X]$, on a

$$P_{\alpha_1}(X) = \prod_{i=1}^{s} (X - x_i) \text{ avec } x_1 = \alpha_1 \text{ et } P_{\alpha_2}(X) = \prod_{j=1}^{t} (X - y_j) \text{ avec}$$

$y_1 = \alpha_2$ et $y_{j_1} \neq y_{j_2}$ pour tout $j_1 \neq j_2$. Soit $\gamma \in K \setminus \left\{ \frac{x_i - \alpha_1}{\alpha_2 - y_j} \mid j \neq 1, \begin{smallmatrix} i=1,\dots \\ j=2,\dots \end{smallmatrix} \right\}$
Ce γ existe car K est supposé infini.

– Soit $\beta := \alpha_1 + \gamma \cdot \alpha_2 \in K$. Montrons que $K(\beta) = K(\alpha_1, \alpha_2)$. Par construction, on a que $P_{\alpha_1}(\beta - \gamma\alpha_2) = P_{\alpha_1}(\alpha_1) = 0$ et $P_{\alpha_2}(\beta - \gamma y_j) \neq 0$ si $j \neq 1$. Les polynômes $P_{\alpha_2}(X)$ et $R(X) := P_{\alpha_1}(\beta - \gamma X)$ dans $K(\beta)[X]$ ont $\alpha_2 \in L$ comme racine commune unique, d'où $\operatorname{pgcd}(P_{\alpha_2}(X), R(X)) = (X - \alpha_2)$. Comme le pgcd ne dépend pas du corps ambiant, $X - \alpha_2 \in K(\beta)[X]$, d'où $\alpha_2 \in K(\beta)$, et donc $\alpha_1 = \beta - \gamma\alpha_2 \in K(\beta)$. On obtient ainsi $K(\alpha_1, \alpha_2) \subseteq K(\beta)$ et $K(\beta) \subseteq K(\alpha_1, \alpha_2)$ par la construction de β.

<u>IIème cas:</u> K – fini, donc L – fini aussi car $\dim_K L = [L:K] < \infty$.

<u>Lemme 6.11 (Rappel):</u> Soit K un corps. Tout sous-groupe fini de $(K^\times, \cdot)$ est cyclique.

On a que $L^\times$ est cyclique comme groupe. Soit $x \in L^\times$ un générateur.
Alors $L = K(x) = K[x]$. ∎

<u>Exemples:</u> (1) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est séparable et donc simple;
$\mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}(\sqrt[3]{2} + j)$

<u>N.B.</u> Ce n'est, en général, pas évident de trouver x t.q. $L = K(x)$.

(2) Soit $L = \mathbb{F}_p(X, Y)$ et $K = L^p = \mathbb{F}_p(X^p, Y^p)$. Alors L/K n'est pas simple:

- $\{ X^i Y^j \mid 0 \le i, j \le p-1 \}$ est une base de L/K, donc $[L:K] = p^2$
- $\forall \alpha \in L$, α est une racine de $T^p - \alpha^p \in K[T]$, d'où son pol. min. sur K divise $T^p - \alpha^p$, et donc est de degré $\le p$. Cela implique $[K(\alpha):K] \le p$ et donc $L \neq K(\alpha)$.

Thm. 6.12. Soit L/K - ext. finie. LASSE :

(1) Il n'y a qu'un nombre fini de corps intermédiaires E entre K et L.

(2) Il existe $\alpha \in L$ t.q. $L = K(\alpha)$, c-à-d L/K est simple.

Preuve : Dans le cas où K est fini, l'énoncé est clair. Supposons K - infini.

(1) $\Rightarrow$ (2) Soit $L = K(\alpha_1, .., \alpha_n)$. Il suffit de traiter le cas $n = 2$. La famille d'extensions E/K donnée par $\{K(\alpha_1 + \lambda\alpha_2)\}_{\lambda \in K}$ étant finie, il existent $u \neq v \in K$ t.q. $K(\alpha_1 + u\alpha_2) = K(\alpha_1 + v\alpha_2)$.

Alors $\alpha_2 = \dfrac{(\alpha_1 + v\alpha_2) - (\alpha_1 + u\alpha_2)}{v - u} \in K(\alpha_1 + u\alpha_2)$, d'où $\alpha_1 \in K(\alpha_1 + u\alpha_2)$

et on obtient $K(\alpha_1, \alpha_2) = K(\alpha_1 + u\alpha_2)$.

(2) $\Rightarrow$ (1) Soit $L = K(\alpha)$ avec P_α le pol. min. de α sur K. Soit E un corps t.q. $K \subseteq E \subseteq L$. Alors le pol. min. $P_{\alpha, E}$ de α sur E satisfait $P_{\alpha, E} \mid P_\alpha$ dans $E[X] \subseteq L[X]$. Remarquons que $P_\alpha(X)$ n'a qu'un nombre fini de div. unitaires dans $L[X]$. Soit $E \supseteq E_0 \supseteq K$ le corps engendré sur K par les coefficients de $P_{\alpha, E}$. Alors $P_{\alpha, E}$ est irréductible sur $E_0[X]$, donc c'est le pol. min. de α sur E_0. On a donc $[L : E_0] = \deg P_{\alpha, E} = [L : E]$, d'où $E = E_0 \Rightarrow E$ peut se construire à partir de $P_{\alpha, E}$.

On a donc une injection $\{\text{corps intermédiaires dans } L/K\} \to \{\text{fact. irréd. unitaires de } P_\alpha \text{ dans } L[X]\}$

$$E \mapsto P_{\alpha, E}$$

d'où le résultat. $\blacksquare$

Corps finis

- Un corps K est dit <u>fini</u> si $\mathrm{Card}(K) < \infty$. On remarque qu'alors car $K \neq 0$ (car on ne peut pas plonger $\mathbb{Q}$ dans K), d'où $\exists\, p$-premier t.q. car $K = p$. Soit $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. On a que $\mathrm{Card}(K) = p^{[K:\mathbb{F}_p]}$, où $[K:\mathbb{F}_p] < \infty$ car K fini et l'extension $K/\mathbb{F}_p$ est due à la caractéristique.

<u>Prop. 6.1</u>] Pour tout p premier et tout $m \in \mathbb{N}_{\geq 1}$, il existe un corps K à p^m élts. Le corps K est un corps de décomposition du polynôme $X^{p^m} - X \in \mathbb{F}_p[X]$, d'où tout deux corps à p^m élts. sont isomorphes.

<u>Preuve</u>: Existence: - Soit K un corps de décomposition de $X^{p^m} - X \in \mathbb{F}_p[X]$. Comme ce dernier est séparable, ses racines dans K sont simples, et leur nombre est p^m. De plus, le sous-ensemble

$K_0 := \{x \in K \mid x^{p^m} = x\}$ de K est un sous-corps (à vérifier), contenant les racines de $X^{p^m} - X$, donc un corps de décomposition de $X^{p^m} - X$ lui même. Par le corollaire 3.8, nous obtenons que $K = K_0$, et donc $\mathrm{Card}(K) = p^m$.

"<u>Unicité</u>": Soit K un corps à p^m élts. Alors $\mathrm{Card}(K^\times) = p^m - 1$, et comme $(K^\times, \cdot)$ est un groupe, nous avons que $\forall x \in K^\times$, $x^{p^m - 1} = 1$, donc $\forall x \in K$, $x^{p^m} = x$. Comme car $K = p$ et que $\mathbb{F}_p \hookrightarrow K$, on a alors que K est un corps de décomposition de $X^{p^m} - X \in \mathbb{F}_p[X]$, car il est minimal pour la propriété : contenir toutes les racines de $X^{p^m}-X$. ▨

$\boxed{5}$

- Encore un abus de notation : on écrira souvent $\mathbb{F}_q$ pour un corps à q éléments. On a $q=p^n$ pour un p-premier et $n \in \mathbb{N}_{\geq 1}$.

<u>Prop. 6.14</u> Soit p un premier et $n, m \in \mathbb{N}_{\geq 1}$. Alors

$$\exists\ \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^n} \iff m \mid n.$$

<u>Preuve</u> : ($\Rightarrow$) Si $\exists$ un morphisme de corps $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$, alors si $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] =: d$, on a que $\mathrm{Card}(\mathbb{F}_{p^n}) = p^n = (\mathrm{Card}\ \mathbb{F}_{p^m})^d = (p^m)^d = p^{md}$, d'où $m \mid n$.

($\Leftarrow$) Soit $n = dm$ pour $d \in \mathbb{N}_{\geq 1}$. Alors $p^m-1 \mid p^n-1$. Écrivons $p^n-1 = (p^m-1)\cdot A$ pour $A \in \mathbb{N}_{\geq 1}$. Remarquons que $\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n-1}-1 \in \mathbb{F}_p[X]$. Comme

$$X^{p^n-1}-1 = X^{A(p^m-1)}-1 = (X^{p^m-1}-1)\cdot Q(X) \quad \text{avec } Q(X) \in \mathbb{F}_p[X]$$

et que $X^{p^n-1}-1$ est séparable, nous obtenons que $X^{p^m-1}-1$ est aussi scindé dans $\mathbb{F}_{p^n}$.

Par le thm. 3.6, il existe un $\mathbb{F}_p$-morphisme $\mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^n}$. ▨

<u>Proposition 6.15</u> Soit p premier. Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors $\forall n \in \mathbb{N}_{\geq 1}$, $\overline{\mathbb{F}_p}$ contient exactement un corps à p^n élts.

<u>Preuve</u> : Comme $\mathbb{F}_{p^n}$ est le corps de décomp. de $X^{p^n}-X \in \mathbb{F}_p[X]$, la clôt. alg. $\overline{\mathbb{F}_p}$ n'en contient qu'une seule copie. ▨

<u>Rmq.</u> $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ – pour voir '$\subseteq$' : soit $x \in \overline{\mathbb{F}_p}$. Alors $\mathbb{F}_p(x)/\mathbb{F}_p$ est alg. et de type fini, donc finie, d'où $\mathrm{Card}(\mathbb{F}_p(x)) < \infty$ avec $\mathrm{car}\, \mathbb{F}_p(x) = p$, d'où $\mathbb{F}_p(x) \cong \mathbb{F}_{p^n}$.

– Trouver un exemple de $K/\mathbb{F}_p$-alg. infinie t.q. $K \neq \overline{\mathbb{F}_p}$.

Théorie de Galois

<u>Déf. 7.1</u> Soit L/K une extension de corps. Le <u>groupe de Galois</u> de L/K, noté $\mathrm{Gal}(L/K)$, est

$$\{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}\}.$$

<u>Exemples :</u> (1) $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\} \cong \mathbb{Z}/2\mathbb{Z}$

(2) $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}) = \{\mathrm{id}\}$

(3) $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = ???$

(4) $\mathrm{Gal}(\mathbb{C}(X_1, \ldots, X_n)/\mathbb{C})$ – groupe de Cremona, en général compliqué $n \geq 3$

<u>Thm 7.2</u> Soit L/K une ext. finie de corps. Alors

$$|\mathrm{Gal}(L/K)| \underset{(1)}{\leq} [L:K]_s \underset{(2)}{\leq} [L:K],$$

avec égalité pour (1) ssi L/K est normale et pour (2) ssi L/K est séparable.

Donc $|\mathrm{Gal}(L/K)| = [L:K]$ ssi L/K est séparable et normale.

<u>Preuve :</u> On a une action naturelle de $G := \mathrm{Gal}(L/K)$ sur $X := \{\sigma : L \to \overline{K} \mid \sigma \text{ un } K\text{-morphisme}\}$, donnée par :

$$g \in \mathrm{Gal}(L/K),\ \sigma \in X,\ \sigma \cdot g := \sigma \circ g \in X.$$

↳ composée de deux morphismes

Remarquons que $\sigma \circ g = \sigma \Rightarrow g = id_L$, car si $\forall x \in L$, $\sigma(g(x)) = g(x)$, et comme σ est injective, on a $g(x) = x$ $\forall x \in L$.

Donc on a une application injective :

$$\begin{array}{ccc} G & \xrightarrow{\varphi_\sigma} & X \\ g & \longmapsto & \sigma \circ g \end{array}$$ (injective car si $\sigma \circ g_1 = \sigma \circ g_2 \Rightarrow \sigma \circ (g_1 g_2^{-1}) = \sigma \Rightarrow g_1 = g_2$).

pour un $\sigma \in X$ fixé.

Cela implique que $\mathrm{Card}(G) \leq \mathrm{Card}(X) = [L:K]_s$.

L'injection φ_σ est surjective ssi $\forall \sigma' \in X$, $\exists g \in G$ t.q. $\sigma' = \sigma \circ g$, c-à-d si l'action de G sur X est transitive. Cela est vrai ssi $\forall \varphi : L \longrightarrow \overline{K}$, $\varphi(L)$ est toujours le même, c-à-d

$$\begin{tikzcd} L \arrow[rr] & & \overline{K} \\ & K \arrow[ul] \arrow[ur] & \end{tikzcd}$$

(voir le Corollaire 5.5).

ssi L/K est normale ■

- Pour l'inégalité (2), voir le thm. 6.3.

Rmq. On a en particulier égalité dans le thm. précédent si L/K est "le" corps de décomposition d'un polynôme séparable.

Exemples: (1) Dans $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$,

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]_s = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(2) Dans $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$, on a $|\mathrm{Gal}(\mathbb{F}_p(T)/\mathbb{F}_p(T^p))| = [\mathbb{F}_p(T) : \mathbb{F}_p(T^p)]_s = 1$ et $[\mathbb{F}_p(T) : \mathbb{F}_p(T^p)] = p$.

Rmq. ~~Rmq~~ L'inégalité (1) du thm reste vrai pour toute extension algébrique (même preuve). Si L/K est normale, alors on a "=" pour (1). Si on a "=" pour (1), cela n'implique pas L/K normale.

Soit L un corps et $G \leq \mathrm{Aut}(L)$. Soit

$$L^G := \{\alpha \in L \mid g(\alpha) = \alpha \ \forall g \in G\}$$

le sous-corps de L fixé par G. Remarquons que $G \leq \mathrm{Gal}(L/L^G)$.

Thm. 7.3 (Artin) Si G fini, on a

$$[L : L^G] = \mathrm{Card}(G),$$

et L/L^G est une ext. finie, normale et séparable avec $\mathrm{Gal}(L/K^G) = G$.

Preuve: Soit $K := L^G$ et $x \in L$. Soit $Q_x(X) := \prod_{y \in G\cdot x} (X - y)$, où $G\cdot x = \{g(x) \mid g \in G\} \subseteq L$.

Alors $\forall g \in G$, on a $g \cdot Q_x(X) = Q_x(X)$, où $g \cdot (\sum_{i=0}^{m} a_i X^i) = \sum_{i=0}^{m} g(a_i) X^i$, c-à-d tout élt. de G fixe les coeff. de $Q_x(X)$, d'où $Q_x(X) \in K[X]$.

De plus, $Q_x(X)$ est séparable, d'où x est séparable, et L/K séparable.

On a que $P_x(X) \in K[X]$ - le pol min. de x satisfait $\deg P_x \leq |G|$, car $P_x(X) \mid Q_x(X)$.

- Soit $\alpha \in L$ t.q. $\deg P_\alpha$ est maximal parmi $\deg P_x$, $x \in L$.

L'extension $K(\alpha, x)/K$ est séparable et finie, donc par le thm. d'élt. primitif, $\exists z \in K(\alpha, x)$ t.q. $K(\alpha, x) = K(z)$. Comme $K(z)$ est un corps de rupture de $P_z(X) \in K[X]$, on a que $[K(z):K] = \deg P_z \leq \deg P_\alpha = [K(\alpha):K] \leq [K(z):K]$, d'où $[K(\alpha):K] = [K(z):K]$ et $K(\alpha, x) = K(\alpha) = K(z)$. ~~En particulier~~ Cela implique que $x \in K(\alpha)$, et donc que $L = K(\alpha)$. En particulier, L/K finie.

On a

$$|G| \leq |\mathrm{Gal}(L/K)| \overset{\text{thm. 7.2}}{\leq} [L : K] \leq |G|, \text{ d'où } |G| = |\mathrm{Gal}(L/K)| = [L:K],$$

et on conclu par le thm. 7.2.

∎

Déf. 7.4 Une extension L/K est dite galoisienne si elle est normale et séparable.

Rmq. Une ext. finie L/K est galoisienne ssi $[L:K] = |Gal(L/K)|$.

Rmq. Soit $M/L/K$ une tour de corps. Si M/K est galoisienne, alors M/L l'est aussi, mais L/K en général non. De plus,
$Gal(M/L) = \{\sigma : M \to M \text{ autom.} \mid \sigma_{|L} = id_L\} \subseteq Gal(M/K)$.

Thm. 7.5. Soit L/K une extension. LASSE:

(1) L est le corps de décomp. d'un polynôme séparable sur K,
(2) L/K est finie et $K = L^{Gal(L/K)}$,
(3) $K = L^G$ pour un $G \leq Aut(L)$ fini,
(4) L/K est galoisienne finie.

Preuve: (1) ⇒ (2) Clairement, L/K est finie. Soit $K' := L^{Gal(L/K)}$. Par le thm. 7.3, $Gal(L/K') = Gal(L/K)$. De plus, comme L/K est séparable et normale (cor. 5.4 et thm. 6.3), par le thm. 7.2, on a que $|Gal(L/K)| = [L:K]$. De manière similaire, comme un polo séparable sur K est aussi séparable sur K' ($\supseteq K$) on a que L/K' est normale et séparable, d'où $|Gal(L/K')| = [L:K']$. On a donc $[L:K] = [L:K']$, ce qui implique $K = K'$.

(2) ⇒ (3) Pour $G := Gal(L/K)$, on a $G \leq Aut(L)$. Par le thm. 3.5, on a $|G| \leq [L:K] < +\infty$, donc G est fini.

(3) ⇒ (4) Voir le thm. 7.3.

(4) ⇒ (1) Voir le cor 5.4 et le thm. 6.3 ∎

<u>Prop. 7.6</u> Soit L/K une ext. de corps séparable. La clôture normale de L dans une clôt. algébrique $\bar{K}/L/K$ de K est séparable, donc galoisienne sur K. On l'appelle la <u>clôture galoisienne</u> de L dans $\bar{K}$.

<u>Preuve:</u> Dans la preuve du thm. 5.8, les polynômes $P_s(X)$, $s \in S$, sont séparables car L/K l'est. Donc, l'ensemble $\{$racines de $P_s(X)$ dans $\bar{K}\}$ est séparable dans $\bar{K}/K$ pour tout $s \in S$, d'où la clôt. normale de L dans $\bar{K}$ (c-à-d le corps engendré par $\bigcup_{s \in S} \{$racines de $P_s(X)$ dans $\bar{K}\}$ sur K) est séparable sur K. ∎

<u>Rmq.</u> 1) Si L/K galoisienne, pour $\alpha \in L$ algébrique, les conjugués de α sont les élts. $g(\alpha)$, $g \in Gal(L/K)$. Donc, le polynôme min. de α est donné par $\prod_{g \in Gal(L/K)} (X - g(\alpha))$.

Remarquons que comme L/K est galoisienne, L contient <u>tous</u> les conjugués de α dans une ext algébrique $\bar{K}/L/K$ de K.

2) Soit $P(X) \in K[X]$. Soit L/K une extension de corps et $\alpha \in L$ t.q. $P(\alpha) = 0$. Alors $\forall \sigma \in Gal(L/K)$, comme $P(\sigma(\alpha)) = 0$, le groupe $Gal(L/K)$ permute les racines de $P(X)$ dans L.

On a donc un morphisme de groupes

$$\mathrm{Gal}(L/K) \longrightarrow S_{\{\text{racines de } P(X) \text{ dans } L\}} \quad \left(\begin{matrix}\text{en général}\\ \text{pas injectif.}\end{matrix}\right).$$

Si, par exemple, $L = K(\alpha)$ et $P_\alpha(X) \in K[X]$ est le pol. mini. de α, alors

$$\mathrm{Gal}(L/K) \hookrightarrow S_{Z_{P_\alpha}}, \text{ où } Z_{P_\alpha} := \{\text{racines de } P_\alpha \text{ dans } L\}$$
$$= \mathrm{Gal}(L/K)\cdot\alpha.$$

<u>Prop. 2.7</u> Soit L/K une extension galoisienne. Soit $P(X) \in K[X]$ un pol. séparable et scindé dans L. Alors l'action de $\mathrm{Gal}(L/K)$ sur $\{\text{racines de } P(X) \text{ dans } L\}$ via $\sigma\cdot x = \sigma(x)$, $\sigma \in \mathrm{Gal}(L/K)$ et $x \in L$ t.q. $P(x) = 0$, est transitive ssi $P(X)$ est irréductible sur K.

<u>Preuve:</u> ($\Rightarrow$) Si $P(X) = R(X)\cdot Q(X) \in K[X]$, par la séparabilité de $P(X)$, les polynômes $R(X)$, $Q(X)$ n'ont pas de racines communes dans L. Les élts de $\mathrm{Gal}(L/K)$ envoient les racines de $Q(X)$ sur les racines de $Q(X)$ et idem pour $R(X)$. Donc, l'action de $\mathrm{Gal}(L/K)$ sur $\{\text{racines de } P \text{ dans } L\}$ n'est pas transitive.

($\Leftarrow$) Si $P(X) \in K[X]$ est irréductible, alors pour $\alpha, \beta \in L$ t.q. $P(\alpha) = P(\beta) = 0$, on a un K-isomorphisme $\varphi : K(\alpha) \to K(\beta)$, $\alpha \mapsto \beta$, qui induit les extensions $K(\alpha) \overset{i}{\hookrightarrow} L$ et $K(\alpha) \overset{\varphi}{\hookrightarrow} K(\beta) \overset{i'}{\hookrightarrow} L$.

Comme L/K est galoisienne, par la prop. 5.2, L est le corps de décomp. d'une famille $(P_i(X))_{i\in I}$ de pol. séparables sur K (voir la preuve de $(1)\Rightarrow(4)$, prop. 5.2). En particulier, la famille $(P_i(X))_{i\in I}$ est séparable sur $K(\alpha)$ et les extensions $K(\alpha) \overset{i}{\hookrightarrow} L$ et $K(\alpha) \overset{i'\circ\varphi}{\hookrightarrow} L$ sont des corps ~~.....~~ de décomp. de $(P_i(X))_{i\in I}$ sur $K(\alpha)$, d'où

$$\begin{tikzcd} \exists\, \sigma : L \arrow[rr, "\sim"] & & L \\ & K(\alpha) \arrow[ul, "i"] \arrow[ur, "i'\circ\varphi"'] & \end{tikzcd} \quad \text{avec } \sigma(\alpha)=\beta.$$

Comme $\sigma_{|K} = id_K$, on a que $\sigma \in Gal(L/K)$, d'où l'action est transitive. ∎

Rmq. Pour montrer que deux corps de décomp. d'une famille $(P_i(X))_{i\in I}$ de polyn. sur K sont K-isomorphes, on peut appliquer le thm. de Steinitz.

Exemple: Dans l'extension $\mathbb{Q}(\sqrt[3]{2}, i, j)/\mathbb{Q}$ qui est galoisienne et le corps de décomp. de $(X^3-2)(X^2+1)$, aucun élt. de $Gal(\mathbb{Q}(\sqrt[3]{2}, j, i)/\mathbb{Q})$ n'envoie $\sqrt[3]{2}$ sur i.

Corollaire 7.8. Soit L/K une extension algébrique. LASSE:

(1) $K = L^{Gal(L/K)}$,

(2) L/K est galoisienne.

Preuve: $(1)\Rightarrow(2)$ Soit $\alpha \in L$ et $Q(X) := \prod_{x\in Z_\alpha}(X-x) \in L[X]$, où $Z_\alpha := \{\sigma(\alpha) \mid \sigma \in Gal(L/K)\}$. Comme L/K alg., $Z_\alpha \subseteq L$ est fini. De plus, $\sigma\cdot Q = \sigma$, $\forall \sigma \in Gal(L/K)$, d'où

$Q(X) \in L^{Gal(L/K)}[X] = K[X]$. On a alors $P_\alpha(X) \mid Q(X)$, où $P_\alpha(X) \in K[X]$ est le pol. min. de α, d'où $\deg P_\alpha \leq \deg Q$. De plus, dans L, $\forall x \in Z_{\alpha}$, on a $P_\alpha(x) = 0$, d'où $Q(X) \mid P_\alpha(X)$ dans $L[X]$. Comme P_α, Q sont unitaires, on obtient $Q(X) = P_\alpha(X)$ car $\deg Q \leq \deg P_\alpha$. On a donc que $P_\alpha(X)$ est séparable et L contient toutes ses racines dans une clôt. algébrique $\bar{K}/L/K$. On a donc que L/K est sép. et normale, c-à-d galoisienne.

$(2) \Rightarrow (1)$ On a $K \subseteq L^{Gal(L/K)} =: K'$. Soit $\alpha \in K'$ et $P_\alpha(X) \in K[X]$ son pol. min. Il est scindé dans L et séparable. Si $\beta \in L$ est t.q. $P_\alpha(\beta) = 0$, par la prop. 2.7, $\exists \sigma \in Gal(L/K)$, t.q. $\sigma(\alpha) = \beta$. Comme $\alpha \in K'$, on a $\sigma(\alpha) = \alpha$, donc $\alpha = \beta$, d'où $\deg P_\alpha = 1$ et $\alpha \in K$. On a $K = K'$. ■

Correspondance de Galois

<u>Thm. 7.9</u> Soit L/K une extension galoisienne finie et $G := \mathrm{Gal}(L/K)$.

(1) L'application

$$\{\text{sous-groupes de } G\} \xrightarrow{\varphi} \{\text{ext. intermédiaires de } L/K\}$$
$$H \longmapsto L^H$$

est une bijection avec inverse

$$\psi : E \longmapsto \mathrm{Gal}(L/E).$$

$$\begin{tikzcd} & & L \\ & & & E = L^H \arrow[ul, "H = \mathrm{Gal}(L/E)"'] \\ & & K \arrow[uu, "G"] \arrow[ur] \end{tikzcd}$$

(2) Soient H_1, H_2 deux sous-groupes de G. Alors $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$, dans quel cas $[H_2 : H_1] = [L^{H_1} : L^{H_2}]$.

(3) Pour $\sigma \in G$, $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$, où $H \leq G$.
Cela équivaut à $\mathrm{Gal}(L/\sigma(E)) = \sigma H \sigma^{-1}$ pour $L/E/K$ avec $H = \mathrm{Gal}(L/E)$.

(4) Pour H un sous-groupe de G, H est distingué ssi l'extension de corps L^H/K est <u>normale</u>. Dans ce cas,
$\Rightarrow$ galoisienne

$\mathrm{Gal}(L^H/K) = G/H$.

$$\begin{tikzcd} L & \\ & L^H \arrow[ul, "H"'] \\ K \arrow[uu, "G"] \arrow[ur, "G/H"'] \end{tikzcd}$$

Preuve: (1) Il suffit de mq $\varphi \circ \psi = \mathrm{id}$ et $\psi \circ \varphi = \mathrm{id}$.

On a que $\mathrm{Gal}(L/L^H) = H$ par le thm. 7.3, donc $\psi(\varphi(H)) = H$.

On a aussi que $L^{\mathrm{Gal}(L/E)} = E$ par le thm. 7.5, car

L/K-galoisienne $\Rightarrow$ L/E-galoisienne.

(2) Si $H_1 \subseteq H_2$, alors $L^{H_2} \subseteq L^{H_1}$ par déf, d'où

$\mathrm{Gal}(L/L^{H_1}) \subseteq \mathrm{Gal}(L/L^{H_2})$, c-à-d $H_1 \subseteq H_2$. On a donc

$H_1 \subseteq H_2 \Rightarrow L^{H_2} \subseteq L^{H_1} \Rightarrow H_1 \subseteq H_2$.

Par le thm 7.3, pour tout $H \leq G$, on a

$$[L : L^H] = |\mathrm{Gal}(L/L^H)| = |H| = [H : \{\mathrm{id}\}].$$

Donc $[L : L^{H_2}] = [L : L^{H_1}] \cdot [L^{H_1} : L^{H_2}]$ et $[H_2 : \{\mathrm{id}\}] =$

$[H_2 : H_1] \cdot [H_1 : \{\mathrm{id}\}]$, d'où $[L^{H_1} : L^{H_2}] = [H_2 : H_1]$.

(3) Pour $\tau \in G$ et $\alpha \in L$, on a

$$\tau(\alpha) = \alpha \iff (\sigma\tau\sigma^{-1})(\sigma(\alpha)) = \sigma(\alpha), \quad \text{c-à-d}$$

τ fixe α ssi $\sigma\tau\sigma^{-1}$ fixe $\sigma(\alpha)$. Donc, pour un corps intermédiaire E de L/K, τ fixe E ssi $\sigma\tau\sigma^{-1}$ fixe $\sigma(E)$. On a alors

$$\mathrm{Gal}(L/\sigma(E)) = \sigma\, \mathrm{Gal}(L/E)\, \sigma^{-1}.$$

Par (1), cela montre que $L^{\sigma H \sigma^{-1}} = \sigma L^H$ pour $H \leq G$.

(4) Par le cor. 5.6, L^H/K est normale ssi $\forall\sigma \in Gal(L/K)$, G1
$\sigma(L^H) = L^H$, donc par (3) ssi $L^{\sigma H \sigma^{-1}} = L^H$ $\forall \sigma \in Gal(L/K)$.
Par l'injectivité de φ dans (1), ~~on a~~ cela équivaut à
$\sigma H \sigma^{-1} = H$ $\forall \sigma \in G$, c-à-d $H \trianglelefteq G$. Pour conclure, on a un
morphisme de gpes surjectif $Gal(L/K) \to Gal(L^H/K)$ avec noyau H.
voir le cor. 5.6 $\quad g \mapsto g_{|L^H}$

Exemple: $Gal(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}) = S_3$; ses sous-groupes sont
$\{Id\}$, $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$, $\langle(123)\rangle$ et S_3, et le seul qui est
distingué est $\langle(123)\rangle$ (d'indice 2).

Pour $H := \langle(13)\rangle$ qui agit sur $\mathbb{Q}(\sqrt[3]{2}, j)$ via

$$(13): \begin{array}{l} \sqrt[3]{2} \mapsto j\sqrt[3]{2} \\ j\sqrt[3]{2} \mapsto \sqrt[3]{2} \\ j^2\sqrt[3]{2} \mapsto j^2\sqrt[3]{2} \end{array}$$

d'où $L^H = \mathbb{Q}(\sqrt[3]{2}, j)^{\langle(13)\rangle} = \mathbb{Q}(j^2\sqrt[3]{2})$. De manière similaire

$$(123): \begin{array}{l} \sqrt[3]{2} \mapsto j\sqrt[3]{2} \\ j\sqrt[3]{2} \mapsto j^2\sqrt[3]{2} \\ j^2\sqrt[3]{2} \mapsto \sqrt[3]{2} \end{array} \Rightarrow L^{\langle(123)\rangle} = \mathbb{Q}(j)$$

$$\Rightarrow j \mapsto j$$

Déf. 7.10 Soit $P(X) \in K[X]$ séparable. Alors le groupe de Galois de P est $Gal(L/K)$, où L est un corps de décomposition de $P(X)$. On le notera par Gal_P.

Remarquons que $Gal(L/K) = Gal_P \hookrightarrow S_n$, où $n = \deg P$,

car $Gal(L/K)$ agit en permutant les racines de $P(X)$

(et cela détermine uniquement l'élt. de Gal_P).

<u>Exemple:</u> L'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne, de degré n.

Remarquons que $F_r \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

$$F_r^{\ell}(x) = x^{p^{\ell}} \quad \text{pour } x \in \mathbb{F}_{p^n}$$

et ~~[illegible]~~ $F_r^{\ell} \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. De plus,

si $i,j \in \{0,1,\dots,n-1\}$ t.q. $i \neq j$, alors $F_r^i \neq F_r^j$, donc

$\operatorname{Card}\{F_r^{\ell} \mid \ell = 0,1,\dots,n-1\} = n \Rightarrow Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle F_r \rangle$.

cyclique d'ordre n

Correspondance de Galois infinie

On admettra:

<u>Proposition 2.11</u> Soit L/K une extension galoisienne. Pour $S \subseteq L$ fini, soit $G(S) := \{\sigma \in Gal(L/K) \mid \sigma(s) = s \ \forall s \in S\}$.

Il existe une unique ~~[illegible]~~ topologie sur $Gal(L/K)$ t.q. $\{G(S) \mid S \subseteq L\text{-fini}\}$ est une base de voisinages de $id \in Gal(L/K)$ et t.q. $Gal(L/K)$ muni de cette topologie est un <u>groupe topologique</u> (c-à-d les applications

$$Gal(L/K) \times Gal(L/K) \to Gal(L/K), \quad (g,h) \mapsto g \circ h$$

et

$$Gal(L/K) \to Gal(L/K), \quad g \mapsto g^{-1}$$

sont continues).

Cette topologie est dite la <u>topologie de Krull</u>.

- Remarquons que $G(S) = \mathrm{Gal}(L|K(S))$. De plus, si $S_0 \subseteq L$ ~~fini~~ est t.q. $\sigma(S_0) = S_0$, $\forall \sigma \in \mathrm{Gal}(L|K)$, alors $\sigma G(S_0)\sigma^{-1} = G(S_0)$, d'où $G(S_0) \trianglelefteq \mathrm{Gal}(L|K)$.

- Pour construire un tel S_0 à partir de $S \subseteq L$ - fini, on peut définir :

$$S_0 := \bigcup_{\sigma \in \mathrm{Gal}(L|K)} \sigma(S) = \bigcup_{s \in S} \{\sigma(s) \mid \sigma \in \mathrm{Gal}(L|K)\} \text{ - fini dans } L.$$

<u>Rmq.</u> Si L/K - gal. finie, on a que $\{id\} = G(S)$ pour $S \subseteq L$ fini t.q. $L = K(S)$, d'où $\{id\}$ et donc $g \cdot \{id\}$, $\forall g \in \mathrm{Gal}(L|K)$, sont ouverts. On a que $\mathrm{Gal}(L|K)$ est muni de la top. discrète dans ce cas.

- Dorénavant, on considérera $\mathrm{Gal}(L|K)$ toujours muni de la top. de Krull.

<u>Lemme 7.12.</u> Soit L/K - galoisienne.

(1) Si $S \subseteq L$ fini, on a que

$$\sigma(S) = S \ \forall \sigma \in \mathrm{Gal}(L|K) \overset{(a)}{\Longrightarrow} G(S) \trianglelefteq \mathrm{Gal}(L|K)$$

et $\sigma(S) = S \ \forall \sigma \in \mathrm{Gal}(L|K) \overset{(b)}{\Longrightarrow} K(S)/K$ est galoisienne finie.

(2) La famille $\{G(S) \mid S \subseteq L\text{-fini}, G(S) \trianglelefteq \mathrm{Gal}(L|K)\}$ est une base de voisinages de id pour la top. de Krull.

<u>Preuve :</u> (1) Pour (a), voir le paragraphe au début de cette page. Pour (b), si $\sigma(S) = S$, $\forall \sigma \in \mathrm{Gal}(L|K)$, on a que $\sigma(K(S)) = K(S)$, $\forall \sigma \in \mathrm{Gal}(L|K)$, d'où $K(S)/K$ est normale par le cor. 5.6, donc $K(S)/K$ est galoisienne.

(2) Soit $G(S')$ un voisinage de $id \in \mathrm{Gal}(L|K)$ avec

$S' \subseteq L$ fini. Pour $S = \bigcup_{\sigma \in Gal(L|K)} \sigma(S')$, on a que $G(S) \subseteq G(S')$ et $G(S) \trianglelefteq Gal(L|K)$. ▨

– On admettra :

<u>Thm. 7.13.</u> Soit $L|K$ une ext. galoisienne. Alors $Gal(L|K)$ est compact séparé et ses comp. connexes sont les singletons.

<u>Thm. 7.14. (Krull)</u> Soit $L|K$ une extension galoisienne et $G := Gal(L|K)$.

(1) Pour $L/E/K$, on a $L^{Gal(L/E)} = E$ et $Gal(L/E)$ est un sous-groupe fermé de G.

(2) Pour $H \leq G$, on a que $Gal(L/L^H) = \overline{H}$ – l'adhérence de H.

(3) L'application

$$\{\text{sous-groupes fermés de } G\} \xrightarrow{\varphi} \{\text{ext. intermédiaires de } L|K\}$$
$$H \longmapsto L^H$$

est bijective avec inverse $\Psi : E \mapsto Gal(L/E)$. De plus, $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$, où $H_1, H_2 \leq G$ sont fermés.

(4) Pour $H \leq G$, on a $L^H = L^{\overline{H}}$.

(5) Pour $\sigma \in G$, $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ avec $H \leq G$. On a aussi $Gal(L/\sigma(E)) = \sigma\, Gal(L/E)\, \sigma^{-1}$ pour $L/E/K$.