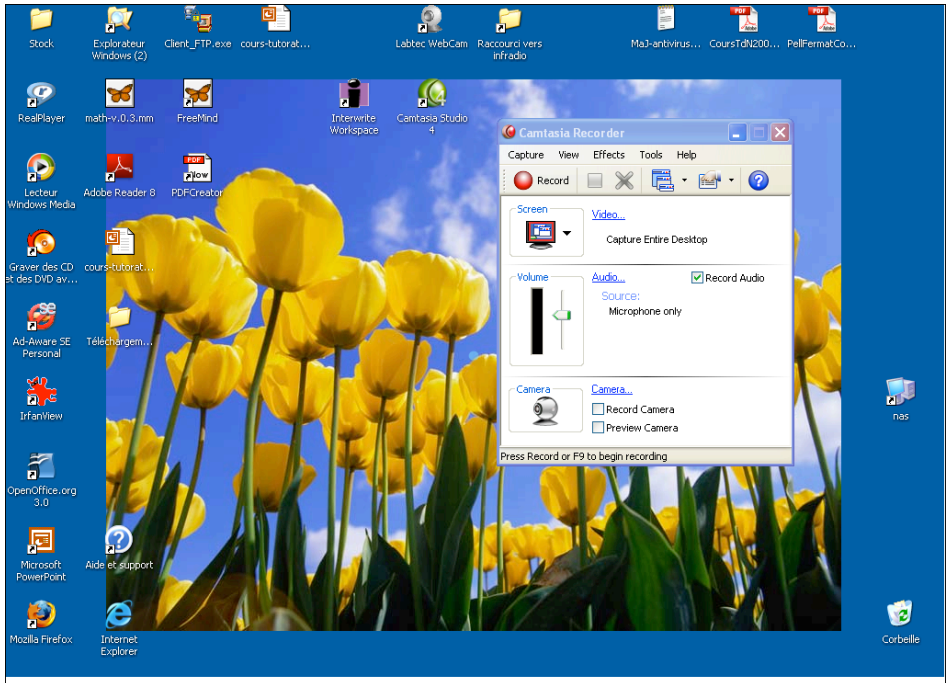


Extensions normales (rappel)

$N \mid k$ est normale si k irréductible
$\forall f \in k[X]$ ayant une racine dans N, f est totalement décomposé dans N.

Extensions séparables.

$L \mid K$ extension finie
$\alpha \in L$. $f \in K[X]$ irréductible
$f(\alpha) = 0$.
L/K est séparable si $\forall \alpha \in L$
le polyn. irr. de α sur K
est séparable

Un polynôme irréductible est séparable s'il n'a pas de racine multiple dans un corps de décomposition

Exemple d'une extension non séparable.

$\mathbb{F}_2(T) = K$

$K[X]$
$\cup$
$X^2 - T$

T n'est pas un carré dans K
$A, B \in \mathbb{F}_2[T]$
$B \neq 0$
$A^2 = B^2 T$
impossible.

Exercice :
p premier
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
$K = \mathbb{F}_p(T)$
$X^p - T$ est irréd. sur K inséparable
$(X - \sqrt[p]{T})^p$

$X^2 - T$ est irréductible sur K
L = corps de rupture sur K. (= corps de décomposition)
$= K(\sqrt{T})$
$X^2 - T = (X - \sqrt{T})(X + \sqrt{T})$
dans $\mathbb{F}_2$: $X^2 - T = (X - \sqrt{T})^2$

Lemme - p premier K corps de caractéristique p ; $a, b \in K$. Alors
$(a+b)^p = a^p + b^p$.

Exemple : ds $K(X, Y)$, $(X+Y)^p = X^p + Y^p$.

Remarque : dans l'exemple $X^p - T = f(X)$ sur $K = \mathbb{F}_p(T)$ on a $f'(X) = 0$

Multiplicité d'un zéro d'un polynôme
$f \in K[X]$ - $\alpha \in K$
α zéro simple si $f(\alpha) = 0$ et $f'(\alpha) \neq 0$
$\Leftrightarrow$ $X - \alpha \mid f(X)$ dans $K[X]$
$(X - \alpha)^2 \nmid f(X)$ dans $K[X]$.

K corps
$\alpha \in K$
$f \in K[X]$
h entier ≥ 0

α est un zéro d'ordre h de f
(h est la multiplicité de f en α)
si $(X-\alpha)^h \mid f$ dans $K[X]$
et $(X-\alpha)^{h+1} \nmid f$

si $f(X) = (X-\alpha)^h g(X)$ alors $g \in K[X]$
Dans ce cas $f(\alpha) = \dots = f^{(h-1)}(\alpha) = 0$ $g(\alpha) \neq 0$.
où $f' = \frac{d}{dX} f$, $f'' = \frac{d}{dX} f'$, ...

$f^{(h)}(\alpha) = h!\, g(\alpha)$ (est nul si $\operatorname{car} K = p$ avec $p \leq h$)

Polynôme irréductible séparable sur K

Déf. $f \in K[X]$ irréd. est séparable si les racines de f dans un corps de décomposition de f sur K sont toutes simples.

Lemme. soit $f \in K[X]$ irréductible. Alors f est séparable $\iff f' \neq 0$.

Démonstration.
Si $f' = 0$ de f sur K. L un corps de décomposition $\alpha \in L$ $f(\alpha) = 0$ Alors $f'(\alpha) = 0$ Donc α n'est pas racine simple. et f n'est pas séparable. D'où $\Longrightarrow$

$\Longleftarrow$ Supposons f non séparable.
$f \in K[X]$ irréd L corps de décomposition de f sur K. ; $\alpha \in L$ $f(\alpha) = 0$
α pas racine simple. $f'(\alpha) = 0$.
(f) est l'idéal des polynômes de $K[X]$ nuls en α. Donc $f' \in (f)$
$f' = fg$ $g \in K[X]$.
$f(X) = a_0 X^d + \dots + a_d \in K[X]$ $a_0 \neq 0$
$f'(X) = d a_0 X^{d-1} + (d-1) a_1 X^{d-2} + \dots + a_1$
$\Rightarrow f' = 0$ $g = 0$

K corps
$f \in K[X]$ irréductible non séparable

$f(X) = \sum_{i=0}^{d} a_{d-i} X^i = a_0 X^d + \dots + a_d$ $d = \deg f$ $a_0 \neq 0$.

$f'(X) = \sum_{i=0}^{d} i\, a_{d-i} X^{i-1} = 0$
$d a_0 X^{d-1} + (d-1) a_1 X^{d-2} + \dots + a_{d-1}$

$i\, a_{d-i} = 0$ $\forall i$ $d a_0 = 0$ $a_0 \neq 0$.

$\Rightarrow \operatorname{car} K = p$ $p \mid d$.

$a_{d-i} \neq 0 \Rightarrow p \mid i$ $i = pj$

Donc $f(X) = \sum_{\substack{0 \leq i \leq d \\ p \mid i}} a_{d-i} X^i = \sum_{j=0}^{d/p} b_j X^{pj}$

$$f(X) = \sum_{i=0}^{d} a_{d-i} X^i = \sum_{\substack{0 \le i \le d \\ p \mid i}} a_{d-i} X^i$$

$a_{d-i} = 0$ si $p \nmid i$

$a_0 \neq 0$ $\quad p \mid d$ $\quad b_j = a_{d-pj}$ $\quad 0 \le j \le \frac{d}{p}$

$$f(X) = \sum_{j=0}^{d/p} b_j X^{pj} = g(X^p)$$

avec $g \in K[X]$.

f irréd. non séparable sur $K \Rightarrow$
car $k = p$ et $\exists\, g \in K[X]$, $f(X) = g(X^p)$.

Inversement $g \in K[X]$, $f(X) = g(X^p)$
car $k = p \Rightarrow f' = 0$

Thm. 2.19. N/k extension normale finie
K/k extension séparable.
$d = [K : k]$.

Alors il existe exactement d k-isomorphismes de K dans N.

Démonstration par récurrence sur d.

* $d = 1$ $\quad K = k$ $\quad \longrightarrow$ un seul k-isomorphisme $k \to N$: l'identité.
* Si l'extension K/k est monogène
il existe un élément primitif $\alpha \in K$
pour K/k : $\quad K = k(\alpha)$.

$f \in k[X]$ irréd. $f(\alpha) = 0$ $\quad \alpha \in K \subset N$

$\Rightarrow f$ est complètement décomposé dans N

K / k séparable $\quad$ α séparable sur k
f ——— dans $k[X]$

donc f a toutes ses racines simples dans N

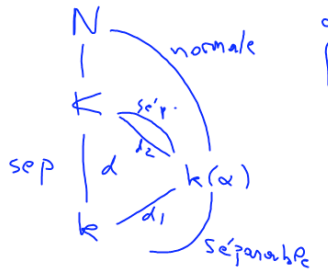
$d = [K : k] = [k(\alpha) : k] = \deg f$.

$f(X) = (X - \alpha_1) \dots (X - \alpha_1)$ avec
$\alpha_1 = \alpha$ $\quad \alpha_i \in N$ $\quad 2$ à 2 distincts.

α a d conjugués dans N.

σ_i k-isomorphisme de $k(\alpha)$ sur $k(\alpha_i) \subset N$
$\sigma_i : k(\alpha) \longrightarrow N$

On complète la démonstration par récurrence.



$\alpha \in K \setminus k$.
$[k(\alpha) : k] > 1$
on peut supposer $K \neq k(\alpha)$

$H(k, K, N) = \{k\text{-isom. de } K \text{ dans } N\}$

$H(k, k(\alpha), N)$ a d_1 éléments
$H(k(\alpha), K, N)$ — d_2 ——— $\quad d = d_1 d_2$

Lemme $\quad H(k, K, N) = H(k, k(\alpha), N) \times H(k(\alpha), K, N)$

Normale : N — K — $L = k(\alpha)$ — k

$H(k; K, N) \longrightarrow H(k, L, N) \times H(K, L, N)$

$\psi \qquad \sigma \longmapsto (\sigma|_L, \psi)$

$K \xrightarrow{\sigma} N$

$\sigma(a) = a \quad \forall a \in k$

$\sigma|_L : L \to N$

? $\begin{cases} \psi : K \to N \\ \psi(\gamma) = \gamma \quad \forall \gamma \in L. \end{cases}$

on peut prolonger σ en un k-automorphisme $\bar\sigma$ de N.

$\bar\sigma : N \to N$

$\bar\sigma|_K = \sigma$

choix : $\psi = \bar\sigma^{-1} \circ \sigma$

Corollaire. Théorème de l'élément primitif.

Soit K/k une extension finie séparable
Alors elle est monogène : $\exists\, \gamma \in K$,
$K = k(\gamma)$.

Cas où k est fini : K aussi
$K^\times$ est cyclique. γ un générateur
$k(\gamma) = K$.

Supposons k infini. $\alpha \in K$ si $k(\alpha) \neq K$

N — K — k : normale

$\sigma_1, \dots, \sigma_d$ les k homomorphismes de K dans N.

$\exists\, i \neq j,\ \sigma_i \alpha = \sigma_j \alpha$

$\{\sigma_i \alpha\}$ = conjugués de α.

$i \neq j \quad V_{ij} = \{\alpha ;\ \sigma_i \alpha = \sigma_j \alpha\} \subsetneq K$
sous-k-espace vectoriel

$\bigcup_{i \neq j} V_{ij} \subsetneq K$?

$\gamma \in K$
$\gamma \notin V_{ij}$ pour $i \neq j$

$\sigma_i \gamma \neq \sigma_j \gamma \quad \forall i \neq j$

γ a d conjugués dans N
$[k(\gamma) : k] = d$.
$k(\gamma) = K$.

Lemme
k corps infini
V k-e.v. dim finie
$V_1, \dots, V_m$ sous-espaces
$V_i \neq V \quad \forall i = 1, \dots, m$
alors $V_1 \cup \dots \cup V_m \neq V$

Dém : prendre un minimal. $V = V_1 \cup \dots \cup V_m$
$V \neq V_1 \cup \dots \cup V_{m-1} \qquad V \neq V_m \qquad x + \epsilon y,\ \epsilon \in k$

Exercice.

$k = \mathbb{F}_2(T_1, T_2)$

$K = k(\sqrt{T_1}, \sqrt{T_2})$

K/k pas monogène