Polynômes et extensions séparables

rappel : A anneau $f \in A[X]$ $\sum_{n\geq 0} a_n X^n$ on a $f' := \sum_{n\geq 0} n a_n X^{n-1}$ $(fg)' = f'g + fg'$

Rq : $A = k$ corps. $f' = 0 \overset{?}{\Longrightarrow}$

i) $\mathrm{car}(k) = 0 \Rightarrow \deg(f) = 0$

ii) $\mathrm{car}(k) = p \Rightarrow \exists g \in k[X]$ t.q. $f(X) = g(X^p)$

⚠ $k = \mathbb{F}_p$ $f = X^p$ $f' = 0$

Def : f séparable si $(f, f') =$ idéal unité de $k[X]$

Prop. Pour $f \in k[X]$ (choix clôt. alg. $\bar{k}$ de k) dans $\bar{k}[X]$, on a $f = a_n \prod_{i=1}^{r} (X - \alpha_i)^{v_i}$

i) f séparable

ii) f et f' n'ont pas de racine commune dans $\bar{k}$

iii) les racines de f sont de multiplicité 1

iii)' f possède $\deg(f)$ racines distinctes

iii)'' $k[X]/(f)$ est une k-algèbre réduite $\quad k[X]/(f) \simeq \prod_{i=1}^{r} \bar{k}[X]/(X-\alpha_i)^{v_i}$ réduit si $v_i = 1$

Dem : i) $\Rightarrow$ ii) Bézout $\Rightarrow \exists g, h \in k[X]$ $gf + hf' = 1$

$\Rightarrow f$ et f' toujours premiers entre eux $\bar{k}[X]$

$\Rightarrow$ pas de diviseur irréductible commun dans $\bar{k}[X]$

$\Rightarrow$ pas de racine commune.

ii) $\Rightarrow$ iii) contrapposée. Supp f a une racine multiple dans $\bar{k}$

$\left.\begin{array}{l} \text{on } f = (X-\alpha)^2 \, q \text{ dans } \bar{k}[X] \\ \text{on } f' = (X-\alpha)[2q + (X-\alpha)q'] \end{array}\right\} \Rightarrow$ racine commune à f et f'

iii) $\Rightarrow$ i) Contrapposée. Supp que f et f' ont un diviseur irréd commun $h \in k[X]$

$$f = hg \quad \text{et} \quad f' = hg' + h'g \quad \Rightarrow \quad \underline{h \mid h'g}$$

2 possibilités

i) $h' \neq 0 \Rightarrow h \nmid h'$ car $\deg h' < \deg h$

$\Rightarrow h \mid g \Rightarrow h^2 \mid f \Rightarrow$ toute racine de h est racine de f avec mult ≥ 2

ii) $h' = 0 \Rightarrow k$ est de caract p et $h(X) = e(X^p)$ pour $e \in k[X]$

Soit alors ℓ racine de e dans $\bar{k}$.

On a $X - \ell \mid e$ donc $X^p - \ell \mid h$

Or, si β = racine p-ième de ℓ dans $\bar{k}$, on a

$$X^p - \ell = (X - \beta)^p$$

Donc β racine multiple de h et donc de f

Rq: $\bar{k}[X]/(X-\ell)^\nu$ réduit $\Leftrightarrow \nu = 1$

En effet : $\nu = 1 \Rightarrow \bar{k}[X]/(X-\ell) = \bar{k}$ réduit

$\nu > 1 \Rightarrow \overline{X - \ell}$ nilpotent non nul

Rq: $f \mid g$ alors g séparable $\Rightarrow f$ séparable (grâce à iii))

Application :

Th: $\forall q = p^r$, p premier, $r \geq 1$, $\exists$ corps à q éléments, unique à isomorphisme près, et c'est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Dem Vu la dernière séance, il ne reste qu'à vérifier que le corps de décomp de $X^q - X$ a bien p^r éléments, ie que $X^q - X$ a p^r racines $\neq$.

Fait de m.q $X^{p^r} - X$ est séparable. Or $(X^{p^r} - X)' = -1$ dans $\mathbb{F}_p[X]$

Notation : $\mathbb{F}_q = \mathbb{F}_{p^r}$ ⚠ $\neq \mathbb{Z}/p^r\mathbb{Z}$ si $r > 1$

↳ pas un corps !! si $r > 1$

Extensions séparables :

Rappel : analogie racines d'un pol / plongements d'une extension

$f \in k[X]$ irréd

$\| \quad \{\alpha \in \bar{k},\ f(\alpha) = 0\} \longleftrightarrow \{\iota : k[X]/(f) \hookrightarrow \bar{k}\} = \mathrm{Hom}_{k\text{-alg}}(k[X]/(f), \bar{k})$

$\alpha \longmapsto \overline{ev}_\alpha$

$\iota(\bar{X}) \longleftarrow \iota$

Prop : K/k finie. Alors $\left|\mathrm{Hom}_{k\text{-alg}}(K, \bar{k})\right| \leq [K : k]$

Dem : $\mathrm{Hom}_{k\text{-alg}}(K, \bar{k}) \overset{\text{Adjonction}}{\simeq} \mathrm{Hom}_{\bar{k}\text{-alg}}(\bar{k} \otimes_k K, \bar{k})$

$\bar{k}$-algèbre de dim $[K : k]$ ↵

Lemme : Soit A une $\bar{k}$-algèbre de dim finie. Alors $\mathrm{Hom}_{\bar{k}\text{-alg}}(A, \bar{k})$ est fini et on a :

$$\left|\mathrm{Hom}_{\bar{k}\text{-alg}}(A, \bar{k})\right| \leq \dim_{\bar{k}} A$$

avec égalité ssi A est réduite

Dem : 1) On a une bijection $\mathrm{Hom}_{\bar{k}\text{-alg}}(A, \bar{k}) \longleftrightarrow \mathrm{Max}(A) = \mathrm{Spm}(A)$

$\varphi \longmapsto \ker \varphi$

$\varphi_m \quad A \twoheadrightarrow A/m \longleftarrow m$

$\bar{k} \hookrightarrow$ ↖ isom car A/m = ext finie de $\bar{k}$ et $\bar{k}$ alg clos

ii) Th des restes Chinois

$m_1, \dots, m_r \in \mathrm{Max}(A)$ distincts 2 à 2 $\Rightarrow A \xrightarrow{\pi} A/m_1 \times \cdots \times A/m_r$ (surjectif)

donc $r \leq \dim_k A$

De plus : $r = \dim_k A \Rightarrow \pi$ bijective $\Rightarrow A$ = produit de corps $\Rightarrow A$ réduite

- A réduite $\Leftrightarrow 0 = \sqrt{0} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \bigcap_{m \in \mathrm{Max}(A)} m = \ker \pi$

car $\mathrm{Max}(A) = \mathrm{Spec}(A)$

Déf : $k \subset K$ ext algébrique, $\alpha \in K$ "séparable sur k" si $f_\alpha \in k[X]$ séparable

Th :
i) $\forall \alpha \in K$, α séparable / k
ii) $|\mathrm{Hom}_{k\text{-alg}}(K, \bar{k})| = [K:k]$
iii) $\bar{k} \otimes_k K$ est réduite

On dit alors que l'ext $k \subset K$ est "séparable"

Dem : ii) $\Leftrightarrow$ iii) découle du lemme

i) $\Rightarrow$ ii) récurrence sur # générateurs de l'extension K/k

* $r = 1$ $\quad K = k(\alpha_1) \cong k[X]/(f_{\alpha_1})$

i) $\Rightarrow \alpha_1$ séparable

$\Rightarrow |\mathrm{Hom}_{k\text{-alg}}(K, \bar{k})| \leftrightarrow \{$ racines de f_{α_1} dans $\bar{k}\}$

Cardinal $\deg(f_{\alpha_1}) = [K:k]$

* $r > 1$ $\quad K = k(\alpha_1, \dots, \alpha_r)$

$k' = k(\alpha_1, \dots, \alpha_{r-1})$

Par restriction $\sigma \mapsto \sigma_{|k'}$ $\quad \mathrm{Hom}_{k\text{-alg}}(K, \bar{k}) \twoheadrightarrow \mathrm{Hom}(k', \bar{k})$

$\sigma \mapsto \sigma_{|k'}$

Cette application est surjective :

$$\begin{array}{ccc} k & \dashrightarrow^{\exists} & \bar{k} \\ \cup & & \\ k' & \xrightarrow{\sigma'} & \end{array}$$

la fibre au-dessus de $\iota' : k' \hookrightarrow \bar{k}$

$= \{ \iota : k \hookrightarrow \bar{k}$ prolongeant $\iota' \}$

$= \mathrm{Hom}_{k'\text{-alg}, \iota'}(k, \bar{k})$

$\rightarrow$ on voit $\bar{k}$ comme k'-algèbre via ι'

Donc $\left| \mathrm{Hom}_{k\text{-alg}}(k, \bar{k}) \right| = \sum_{\iota' \in \mathrm{Hom}_{k'\text{-alg}}(k', \bar{k})} \left| \mathrm{Hom}_{k'\text{-alg}, \iota'}(k, \bar{k}) \right|$

(on a partitionné les plongements $k \hookrightarrow \bar{k}$ selon leur restriction à k')

On a $k = k'(\alpha_r) \Rightarrow$ on a vu $\left| \mathrm{Hom}_{k'\text{-alg}, \iota'}(k, \bar{k}) \right| = [k : k']$

car α_r séparable sur k'

Donc $\boxed{\left| \mathrm{Hom}_{k\text{-alg}}(k, \bar{k}) \right| = [k : k'] \times \left| \mathrm{Hom}_{k\text{-alg}}(k', \bar{k}) \right|}$

$\boxed{HR} \Rightarrow \left| \mathrm{Hom}_{k\text{-alg}}(k', \bar{k}) \right| = [k' : k]$

$\Rightarrow \left| \mathrm{Hom}_{k\text{-alg}}(k, \bar{k}) \right| = [k : k'][k' : k] = [k : k]$

iii) $\Rightarrow$ i)

Rq : $k' \subset k \Rightarrow \bar{k} \otimes_k k' \hookrightarrow \bar{k} \otimes_k k$

(injectif)

En effet, si k-base $e_1 \dots e_n$ de k t.q.

$e_1 \dots e_{n'}$ soit k-base de k'

Et on sait que $1 \otimes e_1 \dots 1 \otimes e_n$ = base de $\bar{k} \otimes_k K$

$1 \otimes e_1 \dots 1 \otimes e_{n'}$ = ——— K'

$\rightsquigarrow$ on peut identifier $\bar{k} \otimes_k K'$ à une sous $\bar{k}$-algèbre de $\bar{k} \otimes_k K$

Application : Supposons $\bar{k} \otimes_k K$ réduite.

Soit $\alpha \in K$. Alors $\bar{k} \otimes_k k[\alpha] \subset \bar{k} \otimes_k K$

donc $\bar{k} \otimes_k k[\alpha] \simeq \bar{k}[X]/(f_\alpha)$ est réduite ∎

donc α séparable / k

Rq : $f \in k[X]$ irréductible, f séparable $\Leftrightarrow$ $k[X]/(f)$ séparable

Corollaire (de la preuve) : $k \subset k' \subset K$ ext. finies

k'/k séparable, K/k' séparable $\Rightarrow$ K/k séparable

Application : Si $K = k(\alpha_1 \dots \alpha_n)$ α_i algébrique séparable

$\Rightarrow$ K séparable / k

$\Rightarrow$ Si k est de caract 0, tout pol irréd est séparable

donc toute extension finie est séparable

k caractéristique p : $\mathbb{F}_p(X) \supset \mathbb{F}_p(X^p)$ pol minimal $f(T)$

T non séparable de X sur $\mathbb{F}_p(X^p)$ est : $T^p - X^p$

Th "élément primitif" : Si $k \subset K$ est finie séparable, alors elle est monogène : $\exists \alpha \in K$, $K = k(\alpha)$
$\simeq k[X]/(P_\alpha)$

Dem : on regarde encore la restriction des plongements

$$\begin{array}{ccc} \mathrm{Hom}_{k\text{-alg}}(K, \bar{k}) & \xrightarrow{\text{res}_\alpha} & \mathrm{Hom}_{k\text{-alg}}(k(\alpha), \bar{k}) \\ \iota & \mapsto & \iota_{|k(\alpha)} \end{array}$$

Séparable : dim $[K:k]$; dim $[k(\alpha):k]$

On voit que $K = k(\alpha) \iff [K:k] = [k(\alpha):k]$
$\iff \text{res}_\alpha$ injective

Or, si $\iota_1, \iota_2 : K \hookrightarrow \bar{k}$, $\iota_{1|k(\alpha)} = \iota_{2|k(\alpha)}$

$\iff \iota_1(\alpha) = \iota_2(\alpha)$

Donc res_α pas injective $\iff \exists \iota_1, \iota_2 : K \hookrightarrow \bar{k}$ distincts tq $\iota_1(\alpha) = \iota_2(\alpha)$

$$\iff \alpha \in \bigcup_{\iota_1 \neq \iota_2} \ker(\iota_1 - \iota_2)$$

$\ker(\iota_1 - \iota_2) \in \mathrm{Hom}_{k\text{-ev}}(K, \bar{k})$

Or $\ker(\iota_1 - \iota_2) = $ ss-ev strict de K ($\iota_1 \neq \iota_2$)

lemme : Si k infini et V un k-ev de dim finie. Alors le complémentaire d'une union finie de k-sev stricts est non vide

cf TD

lemme : Si $k = \mathbb{F}_q$, alors $\mathbb{F}_q^\times$ est un groupe cyclique et donc, tout générateur de $\mathbb{F}_q^\times$ est un générateur de $\mathbb{F}_q / \mathbb{F}_p$

cf T.D.