

Rappel: $\bar{k}$ corps

i) $\exists k \subset \bar{k}$ ext. algébrique avec $\bar{k}$ alg. abs.

ii) Si $k \subset K$ ext algébrique, alors $\exists$ plgement $\iota: K \hookrightarrow \bar{k}$
 $\text{Hom}_{k\text{-alg}}(K, \bar{k}) \ni \iota \hookrightarrow$

iii) Cas particulier: K alg. abs. $\leadsto \iota: K \xrightarrow{\sim} \bar{k}$ Δ ^{Bom} pas unique

En fait $\begin{array}{ccc} K & \xrightarrow{\iota_1} & \bar{k} \\ & \searrow & \downarrow \\ & & \bar{k} \end{array} \quad \exists! \gamma \in \text{Aut}(\bar{k}/k) := \text{Aut}_{k\text{-alg}}(\bar{k})$
 $\text{c}_2 \searrow \quad \text{c}_1 \hookrightarrow \quad \text{c}_2 = \gamma \circ \text{c}_1$

bonne Plus généralement, $\forall K/k$ algébrique, $\begin{array}{ccc} K & \xrightarrow{\iota_1} & \bar{k} \\ & \searrow & \downarrow \\ & & \bar{k} \end{array} \quad \exists \gamma \text{ (pas unique)}$
 $\forall \text{c}_1, \text{c}_2: K \hookrightarrow \bar{k} \quad \gamma \circ \text{c}_1 = \text{c}_2$

En effet: c_1 et c_2 font de $\bar{k}$ une clôture algébrique de K
 donc iii) $\Rightarrow$ existence de γ
 $\hookrightarrow$ pour K ou lieu de k

iv) $f \in k(x)$ $\text{Hom}_{k\text{-alg}}(k(x)/(f), K) \xrightarrow{\sim} \{\text{racines de } f \text{ dans } K\}$
 $K \supset k$ ext
 Si f est irréductible $\rightarrow \{\text{plgts } k(x)/(f) \hookrightarrow K\} \ni \iota \xrightarrow{\text{c}(f)}$
Analogue polynômes/racines $\longleftrightarrow$ $\text{extensions/plongements}$

$k \subset \bar{k}$
Prop: $\alpha, \beta \in \bar{k}$ alors $\begin{array}{l} \Uparrow \text{ i) } \exists \gamma \in \text{Aut}(\bar{k}/k) \text{ s.g. } \gamma(\alpha) = \beta \\ \Downarrow \text{ ii) } f_\alpha = f_\beta \text{ (pol. minimum sur } k) \end{array}$
 $\parallel \rightarrow$ On dit que α et β sont "conjugués" dans $\bar{k}$

$f \in k[x]$ $\varphi: k[x]/(f) \rightarrow A \leftarrow \text{unique}$ $(\text{de } k[x]/(f) \leftarrow)$
 $\leadsto \varphi(\bar{x}) \in A$ vérifie $f(\varphi(\bar{x})) = \varphi(f(\bar{x})) = \varphi(0) = 0$
donc $\varphi(\bar{x}) = \text{"racine" de } f \text{ dans } A$

reciproquement: $\exists \alpha \in A$ tq $f(\alpha) = 0$ dans A
 $\leadsto \text{ev}_\alpha: k[x] \rightarrow A$ $x \mapsto \alpha$ $\text{ev}_\alpha(f) = f(\alpha) = 0$
 $\leadsto \text{ev}_\alpha: k[x]/(f) \xrightarrow{\varphi} A$ $\text{ev}_\alpha(f)$
 $\parallel$
 $\text{Hom}_{k[x]}(k[x]/(f), A) \longleftrightarrow \{\alpha \in A, f(\alpha) = 0\}$

Dém de la proposition:

i) $\Rightarrow$ ii) Soit $\gamma \in \text{Aut}(k[x]/(f))$ tq $\gamma(\bar{x}) = \beta$

$\gamma: \bar{x} \mapsto \beta$
 $\gamma: \bar{k}(x) \mapsto \bar{k}(\beta)$

Si $f \in \bar{k}[x]$, on a $\gamma(f(\bar{x})) = \gamma(f)(\gamma(\bar{x}))$
 Par $f = f_k$, on a $0 = f_k(\beta)$ $\rightarrow f_k \mid f_k$
 $\hookrightarrow f(f_k) = f_k$ car $f_k \in k[x]$ $\rightarrow$ De même $f_k \mid f_\beta$

$\text{Aut}(k/k)$
 $\parallel$
 $\{\text{autom de } k\text{-alg de } k\}$
 $\parallel$
 $\{\text{autom des corps } k \text{ } k\text{-linéaires}\}$
 $\parallel$
 $\{\text{autom des corps } k \text{ qui sont "identités" sur } k\}$

ii) $\Rightarrow$ i) Supp $f_k = f_\beta =: f$ irréductible dans $k[x]$

$\Rightarrow k[x]/(f) \xrightarrow{\text{ev}_\alpha} k[\alpha] \subset \bar{k}$ vu précédemment
 $\text{ev}_\beta \xrightarrow{\sim} k[\beta] \subset \bar{k}$

Donc: $\gamma(\bar{x}) = \gamma(\text{ev}_\alpha(\bar{x})) = \text{ev}_\beta(\bar{x}) = \beta$

Exemple: $k = \mathbb{R} \subset \bar{k} = \mathbb{C}$ $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma\}$
 $\hookrightarrow$ conj. complexe

i) ici "conjugué" = "conjugué complexe"

ii) $k = \mathbb{Q}$ $\bar{k} := \bar{\mathbb{Q}} := \bar{\mathbb{Q}}^c$ $\sqrt[3]{2}$ $j = \frac{1 + i\sqrt{3}}{2}$

(... ? ...)

$$\{\text{conjugués de } \zeta\} = \{\text{racines de } X^3 - 2\} = \{\zeta, j\zeta, j^2\zeta\}$$

Prop: $k \subset K \subset \bar{k}$ $\begin{cases} \uparrow \text{ i) } \forall \alpha \in K, \{\text{racines de } f_\alpha \text{ de } \bar{k}\} \subset K \\ \downarrow \text{ ii) } \forall \sigma \in \text{Aut}(\bar{k}/k), \sigma(K) \subset K \end{cases}$
 On dit que K est ext "normale" de $\bar{k}$

Dém: i) $\Rightarrow$ ii) Soit $\gamma \in \text{Aut}(\bar{k}/k)$ et $\alpha \in K$
 Prop préc. $\Rightarrow \gamma(\alpha)$ est racine de $f_\alpha \Rightarrow \gamma(\alpha) \in K$
 ii) $\Rightarrow$ i) Soit $\alpha \in K$ et β racine de f_α
 Prop préc. $\Rightarrow \exists \gamma$ tq $\gamma(\alpha) = \beta \Rightarrow \beta \in K$

Corollaire: Soit $K \subset \bar{k}$ ~~est~~ ext normale, l'application
 de restriction à K induit $\text{Aut}(\bar{k}/k) \rightarrow \text{Aut}(K/k)$
 morphisme surjectif $\begin{matrix} \uparrow \\ \text{Prop. préc.} \end{matrix}$

Dém: existence du morphisme $\Leftarrow$ prop. préc (et déf de "normale")

Surjectivité: $\left(\begin{array}{l} \text{Soit } \sigma \in \text{Aut}(K/k) \\ \text{Soit } K \subset \bar{k} \end{array} \right) \xrightarrow{\text{vu précédemment}} \exists \gamma \text{ tq } \gamma|_K = \sigma$
 $\begin{array}{ccc} K & \subset & \bar{k} \\ \sigma \downarrow & \searrow & \downarrow \\ K & \subset & \bar{k} \end{array}$

Exemples: $k = \mathbb{Q}$ $\bar{k} = \bar{\mathbb{Q}}$ $X^3 - 1 = (X-1)(X^2 + X + 1)$ $\hookrightarrow f_j$

i) $\mathbb{Q}[j]$ si $\sigma \in \text{Aut}(\bar{\mathbb{Q}})$, $\sigma(j)$ = racine de $f_j \in \{j, j^2\}$
 $\xrightarrow{\text{si } j^2}$ $\text{normale} \Leftarrow \parallel \begin{array}{l} \Rightarrow \sigma(j) \in \mathbb{Q}[j] \\ \Rightarrow \sigma(\mathbb{Q}[j]) \subset \mathbb{Q}[j] \end{array}$

ii) $\mathbb{Q}[\sqrt[3]{2}]$ $j\sqrt[3]{2}, j^2\sqrt[3]{2} \in \{\text{racines de } X^3 - 2\}$

Après

pas normale

$$\notin \mathbb{Q}[\sqrt{2}]$$

car $j \notin \mathbb{Q}[\sqrt{2}]$ puisque $[\mathbb{Q}(j):\mathbb{Q}] = 2 \nmid [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$$\text{iii) } \mathbb{Q}[j, \sqrt{2}] \xrightarrow{\text{map } \sigma} \sigma(\text{Aut}(\bar{\mathbb{Q}}/\mathbb{Q})) \begin{cases} \sigma(j) \in \{j, j^2\} \\ \sigma(\sqrt{2}) \in \{\sqrt{2}, j^2\sqrt{2}, j\sqrt{2}\} \end{cases}$$

$$\implies \sigma(\mathbb{Q}(j, \sqrt{2})) \subset \mathbb{Q}(j, \sqrt{2})$$

$\Rightarrow$ normale

Prop: Soit $k \subset K$ ext. alg.

i) $\forall x \in k$, f_k est scindé dans $K[x]$

ii) Si $\iota_1, \iota_2: k \hookrightarrow \bar{k}$ alors $\iota_1(k) = \iota_2(k)$

iii) Si $\iota: k \hookrightarrow \bar{k}$ alors $\iota(k) = \text{split normale de } \bar{k}$

On dit alors que l'extension est "normale"

Dém: i) $\Rightarrow$ ii) Soit $\alpha \in k$. On cherche $\beta \in k$ tq $\iota_2(\alpha) = \iota_1(\beta)$

$$f_k \text{ scindé ds } K[x] \Rightarrow f_k(x) = \prod_{i=1}^n (x - \alpha_i)^{v_i} \quad \alpha_i \neq \alpha_j$$

$\Rightarrow \iota_1$ et ι_2 induisent bijections $\{\text{rac de } f_k \text{ ds } k\} \leftrightarrow \{\text{rac de } f_k \text{ ds } \bar{k}\}$

$$\text{car } \iota_1(f_k) = \prod_{i=1}^n (x - \iota_1(\alpha_i))^{v_i}$$

En particulier $\exists!$ racine β de f_k ds k tq $\iota_1(\alpha) = \iota_2(\beta)$

On a donc $\iota_2(k) \subset \iota_1(k)$ Symétriquement on a $\iota_1(k) \subset \iota_2(k)$

ii) $\Rightarrow$ iii) $\forall \gamma \in \text{Aut}(\bar{k}/k)$, $\gamma(\iota(k)) = \underline{\gamma \circ \iota(k)} = \iota(k)$

$\Rightarrow \iota(k) = \text{split normale}$

iii) $\Rightarrow$ i) Soit $\iota: k \hookrightarrow \bar{k}$

$$\iota(f_k) \in \bar{k}[x] \text{ scindé } \Rightarrow \iota(f_k) = \prod_{i=1}^n (x - \alpha_i)^{v_i} \quad \alpha_i \in \bar{k} \quad \alpha_i \neq \alpha_j$$

$$\begin{aligned} \text{iii)} \Rightarrow \forall i, x_i \in \mathcal{L}(K) \quad (\mathcal{L}(K) = \text{ss/ext normale}) \\ \Rightarrow x_i \in \mathcal{L}(K_i) \\ \Rightarrow f_K = \prod_{i=1}^n (x - x_i)^{v_i} \quad \text{scindé dans } K[X] \end{aligned}$$

Exemple: $\mathbb{Q}(X)/(X^2+1) = \text{ext normale de } \mathbb{Q}$
 $\mathbb{Q}(X)/(X^3-1) = \text{ext non normale de } \mathbb{Q}$

Def: $f \in K[X]$. Un "corps de décomposition de f " est une $\prod_{i=1}^n (X - x_i)$
 extension K/h tq. i) f est scindé dans $K[X]$
 ii) K est engendré par les racines de f

⚠️ f irréductible sur "corps de rupture" = corps où f admet une racine et engendré par cette racine
 tous isomorphes à $K[X]/(f)$

Exemple: $f = X^3 - 2$ $K = \mathbb{Q}$. $\mathbb{Q}(\sqrt[3]{2}) = \text{corps de rupture}$
 $\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \text{corps de décomposition}$

Prop: f admet un corps de décomposition, unique à iso (non unique) près
 De plus, ce corps est une ext normale de K .

Dém: Dans $\bar{K}(X)$, on a $f = \prod_{i=1}^n (X - x_i)$ pour $x_i \in \bar{K}$

Posons $K_f := K(x_1, \dots, x_n)$: c'est un corps de décomposition.

S. $K^{\#} \supset K$ en est un autre

$\exists \iota: K' \hookrightarrow \bar{K}$ $\mathcal{L}(K')$ engendré par racines de f

$\Rightarrow \mathcal{L}(K') = K_f$

$\Rightarrow \iota: K' \xrightarrow{\sim} K_f$

Ex: $n, m \in \mathbb{N}$ $P = X^n - m$ $\mathbb{Q}(\sqrt[n]{m})$ est un corps

$k = \mathbb{Q}$ $\rightarrow$ de décomposition

Rq: $\text{Aut}(K_f/k) \longleftrightarrow \{\text{permutations des racines de } f\} = \mathcal{G}_f$

$\rightarrow$ idée de base de la Théri de Galois

! $\text{Aut}(K_f/k)$ peut être trivial

ex: $k = \mathbb{F}_p(T)$ $f = X^p - T \in k[X]$ $(a+b)^p = a^p + b^p$

$K_f = \mathbb{F}_p[X] / (X^p - T) = \mathbb{F}_p(T^{1/p})$

est un corps de décomposition car $f = X^p - T = (X - T^{1/p})^p$
1 seule racine, mult. p

Donc $\text{Aut}(\mathbb{F}_p(T^{1/p}) / \mathbb{F}_p(T))$ trivial!

Rapels:

* caractéristique d'un corps

$\mathbb{Z} \xrightarrow{\text{can}} k$

$\text{im}(\text{can})$ intègre $\begin{cases} \cong \mathbb{Z} \\ \cong \mathbb{Z}/p\mathbb{Z} \end{cases}$ p premier

$\text{ker}(\text{can}) = (0) \text{ ou } p\mathbb{Z}$

* "sous-corps premier de k " = plus petit ss-corps de k

$\begin{cases} \rightarrow \mathbb{Q} \text{ en car. } 0 \\ \rightarrow \mathbb{F}_p \text{ en car. } p \end{cases}$

Endomorphisme de Frobenius

Si: $A = \mathbb{F}_p$ -algèbre (= anneau où $p \neq 1 = 0$)

$F: A \rightarrow A$ = endomorphisme de $\mathbb{F}_p$ -algèbre.

on note $\iota_A: A \hookrightarrow A^F$

$$A \xrightarrow{\varphi} B \quad \text{abs} \quad \varphi \circ \iota_A = \iota_B \circ \varphi$$

$$\text{On note } A^F := \{x \in A, x^p = x\}$$

Lemme: Si $A = k$ corps, $k^F = \text{ss/corps premier}$ ($= \overline{\mathbb{F}_p}$) im(con)
||

$$\text{Dem: } x \in k^F \Leftrightarrow x^p = x \Leftrightarrow (X-x) \mid (X^p - X) \quad \text{dans } k[X]$$

$$\text{Or } \forall a \in \overline{\mathbb{F}_p} \subset k, a^p = a \Rightarrow (X-a) \mid (X^p - X)$$

$$\Rightarrow \underline{X^p - X} = \prod_{a \in \overline{\mathbb{F}_p}} (X-a)$$

$$\Rightarrow x \in \overline{\mathbb{F}_p}$$

$$\text{Plus g n ralment: } k^{\overline{\mathbb{F}_p}} = \{x \in k, \overline{\mathbb{F}_p}(x) = x\} = \{x \in k, x^{p^r} = x\}$$

Th: Soit $\overline{\mathbb{F}_p}$ une cl t. alg. de $\mathbb{F}_p$.

Alors: $\overline{\mathbb{F}_p}^{\overline{\mathbb{F}_p}}$ est un corps de d composition de $X^{p^r} - X$

| ii) toute ext. finie K de $\mathbb{F}_p$ est corps de d composition de $X^{p^r} - X$
avec $r = [K: \mathbb{F}_p]$

Dem: Si $x \in \overline{\mathbb{F}_p}$, $\overline{\mathbb{F}_p}(x) = x \Leftrightarrow x$ racine de $X^r - X$

$$\Rightarrow \overline{\mathbb{F}_p}^{\overline{\mathbb{F}_p}} = \{ \text{racines de } X^{p^r} - X \} \Rightarrow \text{Corps de}$$

= corps

/ ou décomp !

ii) K est fini et $|K| = p^r$ car $K \cong \mathbb{F}_{p^r}$

$$|K^*| = p^r - 1 \Rightarrow \forall x \in K^* \text{ on a } x^{p^r-1} = 1 \Rightarrow x^{p^r} = x$$

$$0^{p^r-0} = 0$$

$$\Rightarrow K = \{ \text{racines de } X^{p^r} - X \text{ dans } K \}$$

Rq: pour finir la classification des corps finis.

il reste à prouver $X^{p^r} - X$ possède p^r racines distinctes de $\mathbb{F}_p$

$\Rightarrow \forall r, \exists$ corps fini à p^r elt
unique à isom près

(notation $\mathbb{F}_{p^r}$)

$$\triangle \quad \mathbb{Z} \xrightarrow{\text{can}} \mathbb{F}_{p^r}^* \xrightarrow{\sim} \mathbb{F}_p^*$$

$$\mathbb{F}_{p^r} \hookrightarrow \mathbb{F}_{p^{r'}}$$

$$\Rightarrow \mathbb{F}_{p^{r'}} = \mathbb{F}_{p^r} \text{ ev.}$$

$$\Rightarrow \mathbb{F}_{p^{r'}} \cong (\mathbb{F}_{p^r})^d \text{ comme } \mathbb{F}_{p^r} \text{ ev.}$$

$$p^{r'} = (p^r)^d = p^{rd}$$

en fait: $\mathbb{F}_{p^r}^* \cong$ grp cyclique à p^r-1 elt (que des p^r-1 racines de 1)
 $\cong \mu_{p^r-1}$

$$p^r-1 \mid p^{rd}-1$$

$\mathbb{F}_{p^{rd}}$ contient les racines (p^r-1) -èmes de 1

donc contient les racines de $X^{p^r} - X$

$$= 1 \quad \text{''} \quad \overline{H_p}$$

$$\overline{H_p} \hookrightarrow \overline{H_{p^2}} \xrightarrow{(\text{der})} \overline{H_{p^3}} \xrightarrow{\text{der}} \overline{H_{p^4}} \dots \hookrightarrow \overline{H_{p^i}} \dots$$

$$\cancel{\bigcup \overline{H_{p^i}} \sim}$$

$$\xrightarrow{\text{lim}}$$

$$\bigcup \overline{H_{p^i}} \sim$$

$$\cancel{\bigcup}$$

$$r_i \sim 2^i$$

$$(r_i) \nearrow$$

$$r_i \mid r_{i+1}$$

$$\forall n \in \mathbb{N}, \exists i \mid n \mid r_i$$