

Retour sur l'énoncé:
 L/K $\alpha, \beta \in L$ Existe-t-il un K -isomorphisme
 $K(\alpha) \rightarrow K(\beta)$
 $\alpha \mapsto \beta$.

Réponse: α transcendant: oui ssi β transcendant
 α algébrique polyn. irred $f \in K[X]$,
 oui $\Leftrightarrow f(\beta) = 0$.

$L \supset K$ α algébrique $\overline{K} \supset K$ $f \in K[X]$
 $\Rightarrow K(\alpha) = K[\alpha] \cdot \overline{K} \cong \overline{K}[X]/(f)$ (irréductible)

$\alpha \in L$ L/K
 $f \in K[X]$ irréductible unitaire
 $f(\alpha) = 0$. $\psi: K[X] \rightarrow K[\alpha] \subset L$
 \downarrow
 $g \mapsto g(\alpha)$
 ψ homomorphisme d'anneaux.
 $\ker \psi \ni f$ $\ker \psi$ idéal de $K[X]$
 $\frac{K[X]}{\ker \psi} \cong K[\alpha]$ maximal (= premier)
 $\ker \psi = (f)$
 \cong corps $K(\alpha)$

Corps de rupture. K corps $f \in K[X]$
 f irréductible. \exists existe un corps L
 (corps de rupture de f sur K) (ce que
 $\exists \alpha \in L, f(\alpha) = 0$ et $L = K(\alpha)$.)
 Unicité à K -isomorphisme unique près
 $\psi: K(\alpha) \rightarrow K(\alpha')$ $\psi|_K = \text{id}$.
 $\alpha \mapsto \alpha'$ $K(X) = X \forall X \in K$

Un peu plus général: K_1, K_2 deux corps
 isomorphes $f_1 \in K_1[X]$ irréductible
 $\varphi: K_1 \xrightarrow{\sim} K_2$ $f_2 = \varphi(f_1) \in K_2[X]$ irred.
 $K_1(\alpha_1)$ corps de rupture de f_1 sur K_1 $\varphi: K_1(\alpha_1) \rightarrow K_2(\alpha_2)$
 $K_2(\alpha_2)$ corps de rupture de f_2 sur K_2 $\varphi = \text{id}|_K$

\exists existe un unique isomorphisme
 $\psi: K_1(\alpha_1) \rightarrow K_2(\alpha_2)$
 tel que $\psi(\alpha_1) = \alpha_2$ et $\psi|_K = \text{id}$

Unicité à isomorphisme (non unique) près
 du corps de décomposition d'un polynôme.

K corps $f \in K[X]$
 L est un corps de décomposition de f sur K
 si $\exists \alpha_1, \dots, \alpha_n \in L$ tels que
 $f(x) = a_0(x - \alpha_1) \dots (x - \alpha_n)$ $a_0 \in K$
 et $L = K(\alpha_1, \dots, \alpha_n)$.
 $L \supset K(\alpha_i) \cong \text{id}$. $d=0 \Rightarrow L=K$
 f constant

$X^3 - 2$ corps de rupture / \mathbb{Q} $\mathbb{Q}(\sqrt[3]{2})$
 $\mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$
 Corps de décomposition $\mathbb{Q}(j, \sqrt[3]{2})$
 Dans un corps algébriquement clos Ω
 contenant K , ^{existence et} unicité du corps de décomposition
Proposition. (Lemme 2.13) $\varphi: K \rightarrow K'$ isomorphisme
 $f \in K[X], \varphi f \in K'[X]$.
 L un corps de décomposition de f sur K
 $L' \xrightarrow{\varphi|_L} K'$
 Il existe un isomorphisme ψ de L sur L'
 dont la restriction à K est φ
 $\psi|_K = \varphi$

Démonstration.
 récurrence sur $d = \deg f$.
 $d = 0 \} L = K \quad L' = K' \quad \psi = \varphi$
 $d = 1 \} \quad \quad \quad d = 1 \quad f(x) = a_0x + a_1 = a_0(x - \alpha)$
 $a_0, a_1 \in K \quad a_0 \neq 0$
 $d \geq 2$
 Supp. l'énoncé vrai $L = K(\alpha) = K$
 sous la restriction $\deg < d$.
 $K \xrightarrow{\varphi} K' \quad f$ degré d .
 $L \subset K' \xrightarrow{\varphi} L' \subset K'$
 $L = K(\alpha_1, \dots, \alpha_d)$
 $f(\alpha_i) = 0 \quad 1 \leq i \leq d$
 $L' = K(\alpha'_1, \dots, \alpha'_d) \quad \varphi f(\alpha'_i) = 0$

$f(\alpha_i) = 0$
 g polynôme irréductible de α_i sur K .
 $f \in (g) \quad g$ divise f dans $K[X]$.
 $\varphi g \in K'[X] \quad \varphi g$ est irréductible dans $K'[X]$
 L' est un corps de décom / K' de φf
 on numérote les racines de φf de sorte que
 $\varphi g(\alpha'_i) = 0$
 $K(\alpha_i)$ est un corps de rupture de g sur K
 $K'(\alpha'_i) \xrightarrow{\varphi} K'$

$L \xrightarrow{\varphi} L' \quad \psi|_K = \varphi$
 unicité du corps de rupture $\Rightarrow \exists \varphi_1$
 $K_i = K(\alpha_i) \xrightarrow{\varphi} K'(\alpha'_i) = K'$
 φg
 $\exists \varphi_1: K_i \xrightarrow{\sim} K'_i \quad \varphi_1|_K = \varphi \quad \varphi_1(\alpha_i) = \alpha'_i$
 $f_i(x) = \frac{f(x)}{x - \alpha_i} = a_0(x - \alpha_2) \dots (x - \alpha_d) \in K_i[X]$
 degré $d-1$.
 $\varphi_1 f_i = \frac{\varphi f(x)}{x - \alpha'_i} = \varphi(a_0)(x - \alpha'_2) \dots (x - \alpha'_d)$
 L est le corps de décomposition de f sur K
 $K_i(\alpha_2, \dots, \alpha_d)$ et L' celui de $\varphi_1 f_i$ sur K'_i (HR)

$K \subset \mathbb{C}$

$$f \in L[X] \cap K_1(X) = K_1[X]$$

$$f = \frac{a}{b} \quad a, b \in K_1[X]$$

$$a = bq + r \quad \deg r < \deg b$$

$$q, r \in K_1[X]$$

dans $L[X]$

$$a = bf_1$$

unicité
division eucl. $\Rightarrow f_1 = q \quad r = 0$
quotient $f_1 \in L[X]$
reste 0

Absence d'unicité

$$K = \mathbb{Q} \quad f(x) = x^3 - 2 \quad L = \mathbb{Q}(j, \sqrt[3]{2})$$

$$K' = \mathbb{Q} \quad \psi = \text{id}$$

$$L = \mathbb{Q}(j, \sqrt[3]{2}) \xrightarrow{\sim} L' = \mathbb{Q}(j, \sqrt[3]{2}) \quad L = L'$$

$$\exists \psi \quad \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(j\sqrt[3]{2})$$

$$\sqrt[3]{2} \mapsto j\sqrt[3]{2}$$

L est le corps de rupture sur $\mathbb{Q}(\sqrt[3]{2})$ de $x^2 + x + 1$

L' ————— $\mathbb{Q}(j\sqrt[3]{2})$
de $x^2 + x + 1$

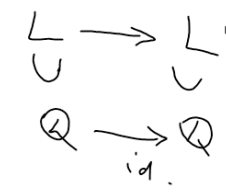
$$\exists \psi \text{ automorphisme de } L$$

$$\psi(\sqrt[3]{2}) = j\sqrt[3]{2}$$

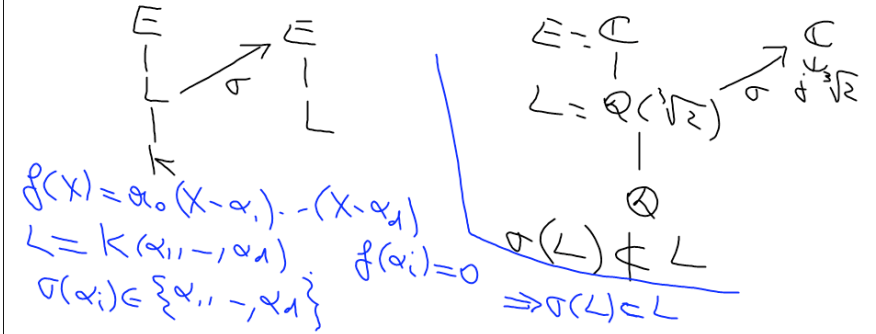
Si on écrit

$$L = K(\alpha_1, \dots, \alpha_n)$$

$$L' = K'(\alpha'_1, \dots, \alpha'_n)$$



Conséquence - L un corps de décomposition sur K de $f \in K[X]$, E extension de L
 $\sigma: L \rightarrow E$ un K -isomorphisme, alors $\sigma(L) = L$



$$\{\sigma \alpha_i, 1 \leq i \leq d\} = \{\alpha_i, 1 \leq i \leq d\}$$

$$\sigma L = K(\sigma \alpha_1, \dots, \sigma \alpha_n) = K(\alpha_1, \dots, \alpha_n) = L$$

Lemme et définition. L/K est normale.

Soit L/K une extension finie. Les deux propriétés suivantes sont équivalentes.

- (1) L est un corps de décomposition sur K d'un polynôme de $K[X]$.
- (2) Tout polynôme ~~irréductible~~ de $K[X]$ ayant une racine dans L est complètement décomposé dans $L[X]$.

Démonstration.

(1) \Rightarrow (2) Supp. L est le corps de décomposition de f sur K . ; $g \in K[x]$ irréductible

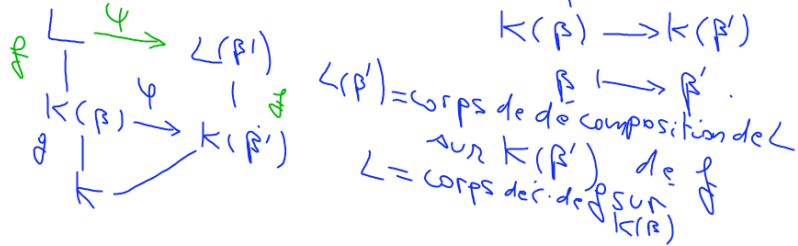
$\beta \in L \quad g(\beta) = 0.$

E un corps de décomposition de g sur K

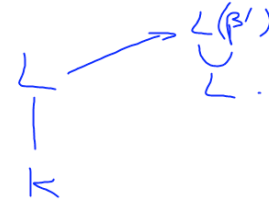
But: $E \subset L \quad \beta' \in E \quad g(\beta') = 0$

But: $\beta' \in L \quad \exists \psi: K\text{-isomorph.}$

$K(\beta) \rightarrow K(\beta')$



Il existe un isomorphisme $\psi: L \rightarrow L(\beta')$
 $\psi(L) = L(\beta'), \quad \psi(\beta) = \beta', \quad \psi|_K = id.$



Corollaire \Rightarrow

$\psi(L) = L = L(\beta')$

Donc $\beta' \in L.$

Réciproque. L/K finie \Rightarrow de type fini

(2) \Rightarrow (1) $K(\alpha_1, \dots, \alpha_m) = L$

$f_i =$ polyn. irréductible de α_i sur K . $f_i(\alpha_i) = 0$

(2) \Rightarrow toutes les racines de f_i sont dans L
 $f = f_1 \dots f_m \in K[X]$ compl. décom. dans L

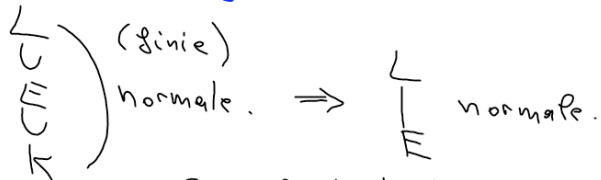
$f \in K[X]$

a toutes ses racines dans L

$\alpha_1, \dots, \alpha_m$ sont des racines de f

$L = K(\alpha_1, \dots, \alpha_m)$

$\Rightarrow L$ est le corps de décomposition sur K de $f.$



Exemple où E/K pas normale:

$K = \mathbb{Q}$
 $L = \mathbb{Q}(\sqrt[3]{2})$
 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$

s/s groupes:
 Distingué = normal

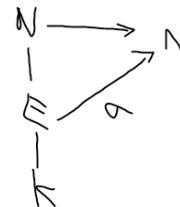
Proposition 2.16



$\sigma: E \rightarrow N$

un K -isomorphisme de E dans N

Mais il existe un K -automorphisme de N dont la restriction à E est σ



Dém. $f \in K[X]$ $N =$ corps de décom. de f sur K
 N est aussi le corps de décom. de f sur E . De plus $\sigma f = f$

$$\begin{array}{ccc}
 N & \xrightarrow{\psi} & N \\
 | & & | \\
 E & \xrightarrow{\sigma} & \sigma(E)
 \end{array}$$

$\exists \psi$ isom. $N \rightarrow N$
 (automorphisme)
 $\psi|_E = \sigma$

$f \in E[X] \quad \sigma f \in \sigma(E)[X]$

Corollaire 2.17.

L/K finie.

L/K normale \Leftrightarrow pour toute extension

F de L et tout K -isom. $\sigma: L \rightarrow F$

on a $\sigma(L) = L$.