Retour sur l'énoncé :

L/K $\alpha, \beta \in L$ Existe-t-il un K-isomorphisme

$K(\alpha) \to K(\beta)$

$\alpha \longmapsto \beta$.

Rép. α transcendant : oui ssi β transcendant

α algébrique polyn. irréd $f \in K[X]$,

oui $\iff f(\beta) = 0$.

$L \supset K$ α algébrique $/K$ $f \in K[X]$ irréductible

φ

$\Rightarrow K(\alpha) = K[\alpha] \simeq K[X]/(f)$

$\alpha \in L$ L/K

$f \in K[X]$ irréductible unitaire

$f(\alpha) = 0$. $\psi_\alpha : K[X] \to K[\alpha] \subset L$

$g \longmapsto g(\alpha)$

ψ homomorphisme d'anneaux.

$\ker \psi \ni f$ $\ker \psi$ idéal de $K[X]$ maximal ($=$ premier)

$\dfrac{K[X]}{\ker \psi} \simeq K[\alpha]$ $\ker \psi = (f)$

$\|$

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) tel que

$\exists\, \alpha \in L,\ f(\alpha) = 0$ et $L = K(\alpha)$.

Unicité à K-isomorphisme unique près

$\psi : K(\alpha) \to K(\alpha')$ $\psi|_K = id$.

$\alpha \longmapsto \alpha'$ $\psi(x) = x\ \forall x \in K$

Un peu plus général : K_1, K_2 deux corps isomorphes $f_1 \in K_1[X]$ irréductible

$\varphi : K_1 \xrightarrow{\sim} K_2$ $f_2 = \varphi(f_1) \in K_2[X]$ irréd.

$K_1(\alpha_1)$ corps de rupture de f_1 sur K_1 $\psi : K_1(\alpha_1) \to K_2(\alpha_2)$

$K_2(\alpha_2)$ f_2 — K_2. $\psi = \varphi|_{K_1}$ $\alpha_1 \mapsto \alpha_2$

$\exists$ existe un unique isomorphisme

$\psi : K_1(\alpha_1) \to K_2(\alpha_2)$

tel que $\psi(\alpha_1) = \alpha_2$ et $\psi|_{K_1} = \varphi$

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 $\exists\, \alpha_1, \dots, \alpha_d \in L$ tels que

$f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_d)$ $a_0 \in K$

et $L = K(\alpha_1, \dots, \alpha_d)$. $d = 0$ $L = K$ f constant

$L \supset K(\alpha_i)$ $1 \leq i \leq d$.

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) $\varphi : K \to K'$ isomorphisme

$f \in K[X]$, $\varphi f \in K'[X]$.

L un corps de décomposition de f sur K

L' ——————— φf — K'

Il existe un isomorphisme ψ de L sur L' dont la restriction à K est φ

$\psi|_K = \varphi$

Démonstration.

récurrence sur $d = \deg f$.

$\left.\begin{array}{l} d=0 \\ d=1 \end{array}\right\}$ $L=K$ $L'=K'$ $\psi=\varphi$

$d=1$ $f(X)=a_0X+a_1=a_0(X-\alpha)$

$a_0, a_1 \in K$ $a_0 \neq 0$

$\alpha = -\frac{a_1}{a_0} \in K$

$L = K(\alpha) = K$

$d \geq 2$

Supp. l'énoncé vrai sous la restriction $\deg < d$.

$K \xrightarrow{\varphi} K'$ f degré d.

$$\begin{tikzcd} f \quad L \arrow[r, "\varphi ?"] & L' \\ K \arrow[u, hook] \arrow[r, "\varphi"] & K' \arrow[u, hook] \quad \varphi f \end{tikzcd}$$

$L = K(\alpha_1, \dots, \alpha_d)$.

$f(\alpha_i)=0$ $1 \leq i \leq d$

$L' = K(\alpha'_1, \dots, \alpha'_d)$ $\varphi f(\alpha'_i)=0$

$f(\alpha_1)=0$

g polynôme irréductible de α_1 sur K.

$f \in (g)$ g divise f dans $K[X]$.

$\varphi g \in K'[X]$ φg est irréductible dans $K'[X]$ divise φf.

L' est un corps de décom $/K'$ de φf

On numérote les racines de φf de sorte que

$\varphi g(\alpha'_1)=0$

$K(\alpha_1)$ est un corps de rupture de g sur K

$K'(\alpha'_1)$ ——————— φg sur K'

$$\begin{tikzcd} L \arrow[r, "\psi"] & L' \\ K_1 = K(\alpha_1) \arrow[u, hook] \arrow[r, "\varphi_1"] & K'(\alpha'_1) = K'_1 \arrow[u, hook] \\ g \quad K \arrow[u, hook] \arrow[r, "\varphi"] & K' \arrow[u, hook] \quad \varphi g \end{tikzcd}$$

$\psi|_{K_1} = \varphi_1$

Unicité du corps de rupture $\Longrightarrow \exists\, \varphi_1$

$\psi|_K = \varphi_1|_K = \varphi$

$\exists\, \varphi_1 : K_1 \xrightarrow{\sim} K'_1$ $\varphi_1|_K = \varphi$ $\varphi_1(\alpha_1) = \alpha'_1$

$f_1(X) = \frac{f(X)}{X-\alpha_1} = a_0(X-\alpha_2)\dots(X-\alpha_d) \in K_1[X]$

degré $d-1$.

$\varphi_1 f_1 = \frac{\varphi f(X)}{X-\alpha'_1} = \varphi(a_0).(X-\alpha'_2)\dots(X-\alpha'_d)$

L est le corps de décomposition de de f_1 sur K_1

$\|$

$K_1(\alpha_2, \dots, \alpha_d)$. et L' celui de $\varphi_1 f_1$ sur K'_1 HR

$$\begin{array}{c} L \\ \cup \\ K_1 \\ \cup \\ K \end{array}$$

$f_1 \in L[X] \cap K_1(X) = K_1[X]$

$f_1 = \frac{a}{b}$ $a, b \in K_1[X]$.

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

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

dans $L[X]$ $a = b f_1$

quotient $f \in L[X]$

reste 0

unicité division eucl. $\Rightarrow f_1 = q$ $r = 0$

Absence d'unicité :

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

$K' = \mathbb{Q}$ $\varphi = id$.

$$\begin{tikzcd} L = \mathbb{Q}(j, \sqrt[3]{2}) \arrow[r, "\sim"] \arrow[d, dash, "2"] & L' = \mathbb{Q}(j, \sqrt[3]{2}) \arrow[d, dash, "2"] \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[r] & \mathbb{Q}(j\sqrt[3]{2}) \end{tikzcd}$$

$L = L'$

$\exists \varphi$ $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(j\sqrt[3]{2})$.

$\sqrt[3]{2} \longmapsto j\sqrt[3]{2}$.

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.

$\exists \psi$ automorphisme de L

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

Si on écrit

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

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

$$\begin{tikzcd} L \arrow[r] & L' \\ \mathbb{Q} \arrow[u, phantom, "\cup"] \arrow[r, "id"'] & \mathbb{Q} \arrow[u, phantom, "\cup"] \end{tikzcd}$$

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

$$\begin{tikzcd} E \arrow[d, dash] & E \arrow[d, dash] \\ L \arrow[d, dash] \arrow[ur, "\sigma"] & L \\ K & \end{tikzcd}$$

$$\begin{tikzcd} E = \mathbb{C} \arrow[d, dash] & \mathbb{C} \\ L = \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] \arrow[ur, "\sigma"] & j\sqrt[3]{2} \\ \mathbb{Q} & \end{tikzcd}$$

$\sigma(L) \not\subset L$

$f(X) = a_0(X - \alpha_1) \dots (X - \alpha_d)$

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

$\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_d\}$

$f(\alpha_i) = 0$

$\Rightarrow \sigma(L) \subset L$

$\{\sigma \alpha_i, 1 \le i \le d\} = \{\alpha_i, 1 \le i \le d\}$.

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

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

$\Uparrow$ But : $\beta' \in L$

$\exists \varphi$: K-isomorph.

$K(\beta) \longrightarrow K(\beta')$

$\beta \longmapsto \beta'$.

$$\begin{tikzcd} L \arrow[r, "\psi"] \arrow[d, dash, "f"'] & L(\beta') \arrow[d, dash, "f"] \\ K(\beta) \arrow[r, "\varphi"] \arrow[d, dash, "g"'] & K(\beta') \\ K \arrow[ur] & \end{tikzcd}$$

$L(\beta')$ = corps de décomposition de L sur $K(\beta')$ de f

L = corps déc. de f sur $K(\beta)$

Il existe un isomorphisme $\psi : L \longrightarrow L(\beta')$

$\psi(L) = L(\beta')$, $\quad \psi(\beta) = \beta'$, $\quad \psi|_K = id$.

$$\begin{tikzcd} & L(\beta') \arrow[d, phantom, "\cup"] \\ L \arrow[ur] \arrow[d, dash] & L. \\ K & \end{tikzcd}$$

Corollaire $\Rightarrow$

$\psi(L) = L$

$= L(\beta')$

Donc $\beta' \in L$.

Réciproque. L/K finie $\Rightarrow$ de type fini

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

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

(2) $\Rightarrow$ toutes les racines de f_i sont dans L

$f = f_1 \cdots f_m \in K[X]$ compl. déc. dans L

$f \in K[X]$

a toutes ses racines dans L

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

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

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

$L \supset E \supset K$ (finie) normale. $\Longrightarrow$ L / E normale.

Exemple où E/K pas normale :

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ $\qquad K = \mathbb{Q}$

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

$E = \mathbb{Q}(\sqrt[3]{2})$

s/s groupes :

Distingué = normal

Proposition 2.16

$N \supset E \supset K$ finie normale

$\sigma : E \longrightarrow N$ un K-isomorphisme de E dans N

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

$$\begin{tikzcd} N \arrow[r] \arrow[d, dash] & N \\ E \arrow[ur, "\sigma"'] \arrow[d, dash] & \\ K & \end{tikzcd}$$

Dém. $f \in K[X]$ $\qquad N$ = corps déc. de f sur K

N est aussi le corps de déc. 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. $N \to N$
(automorphisme)
$\Psi|_E = \sigma$

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

<u>Corollaire</u> 2.17.

L/K finie.

L/K normale $\Leftrightarrow$ pour toute extension F de L et tout K-isom. $\sigma : L \to F$ on a $\sigma(L) = L$.