Extensions $K > k$

de type fini : $\exists\, x_1, \dots, x_m \in K$ tels que $K = k(x_1, \dots, x_m)$

finie : K est de dimension finie $[K:k]$ comme k-espace vectoriel

$\alpha \in K$ est algébrique sur k s'il existe $P \in k[X]$, $P \neq 0$, $P(\alpha) = 0$

transcendant sinon

Quand $K = \mathbb{C}$ et $k = \mathbb{Q}$ on dit simplement algébrique ou transcendant.

Extension algébrique K/k :

tout élément de K est algébrique sur k.

extension transcendante : qui n'est pas algébrique : $\exists\, \gamma \in K$ transcendant sur k.

Extension finie $\Rightarrow$ de type fini

$\Downarrow$

algébrique

Exemple d'extension algébrique pas de type fini

$k = \mathbb{Q}$ $\quad K = \mathbb{Q}\left(\left\{e^{2i\pi r} ;\, r \in \mathbb{Q}\right\}\right)$

$e^{2i\pi/p}$ p premier $\quad \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1$ irréd. / $\mathbb{Q}$.

Exemples d'extensions transcendantes.

$\mathbb{C}/\mathbb{Q}$. Liouville .

$\mathbb{R}/\mathbb{Q}$

k $\quad K = k(X_1, \dots, X_m)$ fractions rationnelles en $X_1, \dots, X_m$

$$\begin{array}{ccc} k & \subset & K \\ \uparrow & & \uparrow \\ \alpha & & \end{array} \qquad \begin{array}{ccc} k[X] & \longrightarrow & K \\ \downarrow & \psi_\alpha & \downarrow \\ P & & P(\alpha) \end{array}$$

ψ_α homomorphisme d'anneaux.

α alg $/k \iff \psi_\alpha$ pas injectif.

$\ker \psi_\alpha =$ idéal de $k[X]$ engendré par un polynôme unitaire

$$\operatorname{Im} \psi_\alpha = k[\alpha] \simeq \frac{k[X]}{\ker \psi_\alpha}$$

$\cap$ K intègre.

$\ker \psi_\alpha$ idéal premier

générateur = polynôme irréductible sur k.

= le seul polynôme unitaire irréductible de $k[X]$ nul en α

= le polyn. irréd. de α sur k.

degré : $[k(\alpha) : k]$

et $k(\alpha) = k[\alpha]$.

$P_\alpha = \mathrm{Irr}(\alpha, k) \in k[X]$.

unitaire, irréd/k, $P_\alpha(\alpha) = 0$.

$fg - P_\alpha h = 1$

$(f, P_\alpha) = k[X]$

$P_\alpha \nmid f$

P_α irréductible

division euclidienne.

$k = \mathbb{Q}$	$\alpha = i$	$P_i(X) = X^2 + 1$
$K = \mathbb{C}$	$\alpha = \sqrt{2}$	$P_{\sqrt{2}}(X) = X^2 - 2$
	$\alpha = e^{2i\pi/3}$	$P_\alpha(X) = X^2 + X + 1$

$k(\alpha) = k[\alpha]$

$f \in k[X]$ $\quad f(\alpha) \neq 0$ $\quad \exists\, g \in k[X]$,

$\frac{1}{f(\alpha)} = g(\alpha)$ $\quad$? $g \in k[X]$? $h \in k[X]$ $\quad f(\alpha)g(\alpha) - 1$ $\quad fg - 1 = P_\alpha \cdot h$

$\alpha \in K$ transcendant sur k

$\Leftrightarrow \Psi_\alpha : k[X] \longrightarrow K$ injectif.

$P \mapsto P(\alpha)$

image $= k[\alpha]$ est isomorphe à $k[X]$

$\frac{1}{\alpha} \notin k[\alpha]$ $\quad k[\alpha]$ n'est pas un corps.

— o —

Lemme $F \supset L \supset K$ Alors F/K est finie $\Leftrightarrow F/L$ et L/K finies. Dans ce cas $[F:K] = [F:L]\,[L:K]$

$[F:K]$ (F | L)$[F:L]$ (L | K)$[L:K]$

F) base $\{\beta_j\}_{j \in J}$

L

K) base $\{\alpha_i\}_{i \in I}$

$\Rightarrow \{\alpha_i \beta_j ;\ i \in I,\ j \in J\}$ base de F sur K

$I \times J$ fini $\Leftrightarrow I$ et J finis.

$[L:K] = 1 \Leftrightarrow L = K$.

$[F:K] = [L:K] \Leftrightarrow [F:L] = 1 \Leftrightarrow F = L$

$[F:L]$ divise $[F:K]$

$[L:K]$ divise $[F:K]$

Exemple. Si $[F:K] = p$ p premier, $\alpha \in F$, $\alpha \notin K$ alors $F = K(\alpha)$

Lemme. K/k extension.

$\alpha_1, \dots, \alpha_m \in K$ algébriques sur k.

$\Rightarrow k(\alpha_1, \dots, \alpha_m)$ est une extension finie de k.

Une extension algébrique de type fini est finie.

Dém. $m = 1$. $\quad K \supset k$, $\alpha \in K$ $\quad \alpha$ alg. sur k. $\quad P \in k[X]$ son polyn. irréd.

$\deg P = [k(\alpha) : k] = d$

Une base de $k(\alpha)/k$ est $1, \alpha, \dots, \alpha^{d-1}$

Récurrence sur m. $\quad [k(\alpha_1, \dots, \alpha_{m-1}) : k] < \infty$ (par hypothèse de récurrence)

α_m alg. sur k.

$\Rightarrow \alpha_m$ est alg sur L

$[L(\alpha_m) : L] < \infty$.

$L(\alpha_m) = k(\alpha_1, \dots, \alpha_{m-1}, \alpha_m)$

$L = k(\alpha_1, \dots, \alpha_{m-1})$.

k

$k \subset L$

$K(a_1, \dots, a_d)/k$ finie

$=$

E $\quad P \in E[X]$

α alg. sur E

$E(\alpha)/E$ finie.

$\Rightarrow E(\alpha)/k$ finie donc

$\Rightarrow \alpha$ alg. sur k (alg)

Conséquence $F \supset L \supset K$. Alors F/K est algébrique $\Longleftrightarrow$ F/L et L/K sont algébriques

$\Rightarrow$ banal.

$\Leftarrow$ $\alpha \in F$ $\quad P \in L[X]$ $\quad P(\alpha) = 0$. d degré

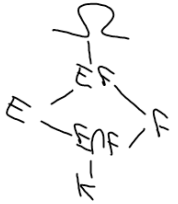
$P \neq 0$. $\quad a_1, \dots, a_d$ coeff. de P.

$\in L$

Lemme. L/K extension. A partie de L formée d'éléments algébriques sur K. Alors $K(A)$ est une ext. alg. de K et $K(A) = K[A]$.

Définition. Ω corps K s/corps, E, F sous-corps de Ω contenant K ; on note EF le corps $E(F) = F(E)$ le sous corps de Ω engendré par E et F. (compositum de E et F).

Lemme



Si F/K est algébrique alors EF/E est algébrique et $EF = E[F]$.

$\{\alpha \in \mathbb{C}, \text{algébriques}\} = \text{corps} = \overline{\mathbb{Q}}$

corps des nombres algébriques

$\alpha = \sqrt[5]{7} + \sqrt[11]{13} \in \mathbb{Q}(\sqrt[5]{7}, \sqrt[11]{13})$ | finie.) $\subset$

$\mathbb{Q}(\sqrt[5]{7})$ $\quad$ $\mathbb{Q}(\sqrt[11]{13})$ $\quad$ $\mathbb{Q}$

5 | $\quad$ 11 | $\quad$

$\mathbb{Q}$ $\quad$ $\mathbb{Q}$

$X^5 - 7$ irréd./$\mathbb{Q}$.

$K \subset L$ $\quad$ L l'ensemble des éléments de L alg $/K$ est un sous-corps de L = fermeture algébrique de K dans L.

$\mathbb{C}$ est algébriquement clos.

Corps algébriquement clos Ω

= qui satisfait les propriétés équivalentes

(i) Tout polynôme non constant $\in \Omega[X]$ admet une racine dans Ω.

(ii) Tout polynôme non constant se décompose totalement dans $\Omega[X]$

$a_0(X - \alpha_1) \dots (X - \alpha_d)$ $\quad a_0 \in \Omega$, $a_0 \neq 0$. $\alpha_i \in \Omega$

(iii) Tout élément algébrique sur Ω appartient à Ω.

(iv) Les polynômes irréductibles de $\Omega[X]$ sont ceux de degré 1

* $\overline{\mathbb{Q}}$ est algébriquement clos.
* Ω algébriquement clos
  $\cup$
  K
  la fermeture algébrique de K dans Ω est un corps algébriquement clos c'est une extension alg. de K

Déf. clôture algébrique de K = extension algébrique de K qui est algébriquement clos.

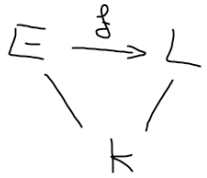
Admis : Pour tout corps K il existe un corps algébriquement clos contenant K.

$\Rightarrow$ Tout corps admet une clôture algébrique.

Isomorphismes de corps.

Tout homomorphisme d'un corps dans un anneau est injectif $\psi : K \longrightarrow A$ $\psi(1)=1$

ψ est un isomorphisme de K sur $\psi(K)$



E, L deux extensions de K

Un homomorphisme de E dans L dont la restriction à K est l'identité est un K-isomorphisme de E dans L

$E = K(\alpha)$
$L = K(\beta)$

$\exists$? f K-isom. de E dans L
$f(\alpha) = \beta$

Définition Ω / K extension;

$\alpha, \beta \in \Omega$. sont conjugués sur K s'il existe un K-isomorphisme

$f : K(\alpha) \longrightarrow K(\beta)$ $f(\alpha) = \beta$.

1er cas α est transcendant / K

Si f existe alors β est transcendant sur K.

Un ranscement β transcendant

$K(\alpha) \simeq K(X) \simeq K(\beta)$.

2e cas. α alg. sur K. $P \in K[X]$ $P(\alpha) = 0$.

Si f existe $f(P(\alpha)) = P(f(\alpha)) = 0$ donc $P(\beta) = 0$

$P(\beta) = 0$

β est une des racines dans Ω de $P(X)$

Résultat - α alg. sur K de polynôme irréductible $P \in K[X]$

$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ les racines de P dans Ω. Les conjugués de α sur K sont $\alpha_1, \alpha_2, \ldots, \alpha_m$.

En particulier si P se décompose totalement dans $\Omega[X]$ $P(X) = (X-\alpha_1)\ldots(X-\alpha_m)$

$m = [K(\alpha) : K]$ alors α a m conjugués dans Ω.

Exemple. $\sqrt[3]{2} = \alpha \in \Omega = \mathbb{C}$

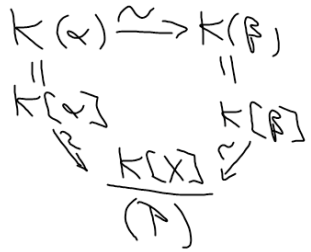
$K = \mathbb{Q}$

$$X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$$

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

Dém. $P \in K[X]$ irréductible

$P(\alpha) = P(\beta) = 0$

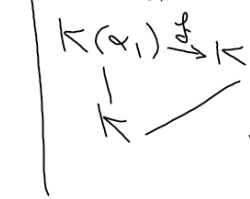


Corps de rupture d'un polynôme irréductible

$f \in K[X]$ irréductible.

Déf extension L de K dans laquelle f a une racine α. et telle que $L = K(\alpha)$.

Prop. Il existe un corps de rupture de f sur K unique à isomorphisme unique près.



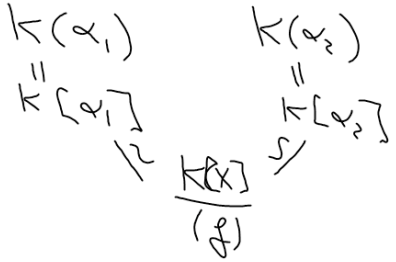
Si $K(\alpha_1)$ et $K(\alpha_2)$ sont deux corps de rupture de f sur K alors il existe un K-isom. unique $K(\alpha_1) \to K(\alpha_2)$ qui envoie α_1 sur α_2.

$f \in K[X]$ irréductible $\qquad \dfrac{K[X]}{(f)} = L$

$K \longrightarrow L$ homomorphisme injectif.

α classe de X

$L = K(\alpha)$ corps de rupture de f sur K.



Corps de décomposition d'un polynôme sur K.

$K[X] \ni f$ quelconque.

E ext. de K dans laquelle f se factorise complètement (facteurs de degré 1)

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

$a_0 \in K \qquad \alpha_i \in E$.

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

Proposition Il existe un corps de décomposition de f sur K. Unique à isomorphisme non unique près K.

Si L est le corps de décomposition sur K d'un polynôme $f \in K[X]$, les K-automorphismes de L forment un groupe $G(L|K)$ le groupe de Galois de L sur K.

Dém. de l'existence d'un corps de décomposition.

$K[X] \ni f$. $f = f_1 \dots f_k$ f_i irréd. sur K.

récurrence sur $\deg f$.

$\deg f = 0$ $L = K$

$\deg f = 1$ $L = K$

- Si $\deg f_i = 1$ $\forall i$ OK.
- $\deg f_i > 1$. E corps de rupture de f_i sur K, α_i racine de f_i dans E.