Partie 2 : Extensions de Corps.

I- Quelques définitions.

1. Corps de Fraction d'un anneau intègre A.

$A \rightsquigarrow K = Fr(A)$

ex :

$\mathbb{Z} \rightsquigarrow \mathbb{Q} = \{ \frac{a}{b},\ a,b \in \mathbb{Z},\ b \neq 0 \} / \sim$

on définit une relation d'équivalence sur les couples $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$

déf :

Soit A un anneau intègre,

On définit le corps de fraction K de A de la manière suivante :

$K = Fr(A) = \{ (a,b) \in A \times A \setminus \{0\} \} / \sim$

Rmq :

Si A a des diviseurs de zéro, il y a un souci...

$b \cdot b' = 0$, $b \neq 0$ et $b' \neq 0$

$\frac{a}{b} \sim \frac{ab'}{0}$ n'est pas défini !!

Autre exemple

$A = \mathbb{R}[X] \rightsquigarrow K = Fr(\mathbb{R}[X]) = \{ \frac{P}{Q} \mid P, Q \in \mathbb{R}[X],\ Q \neq 0 \}$

on note aussi $Fr(\mathbb{R}[X]) = \mathbb{R}(X)$ le corps des fonctions rationnelles en une variable X

Rmq 1

$Fr(A)$ est bien un corps

en effet,

si $\frac{a}{b} \neq 0$ alors $a \neq 0$, $b \neq 0$ et l'inverse de $\frac{a}{b}$ est $\frac{b}{a}$

$Fr(A)$ est muni des opérations + et · induite par + et · de A

tq * $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

* $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Rmq 2

On a une inclusion $\begin{array}{l} A \xrightarrow{i} Fr(A) \\ a \longmapsto \frac{a}{1} = i(a) \end{array}$

et i est un homomorphisme d'anneau $i(a+a') = i(a) + i(a')$

$i(aa') = i(a) \cdot i(a')$

Exercice

$Fr(\mathbb{Z}[i]) = ?$

déf

Soit A un anneau.

Une A-algèbre B est à la fois : * un anneau $(B,+,\cdot)$
* un A-module

Autrement dit, l'anneau $(B,+,\cdot)$ a aussi une structure de A-module.

Exemple :

Soit A un anneau

Prenons $B = A[X] = \{$polynôme à coeff dans A en $X\}$

Alors B est une A-algèbre.

2 - Extension de Corps.

Exemple :

$\mathbb{Q} \subset \underbrace{\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}}_{L} \subset \mathbb{R}$ $(\sqrt{2} \notin \mathbb{Q})$

L est un anneau : * $(a+b\sqrt{2}) + (c+d\sqrt{2}) \in L$
* $(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) \in L$

L est une $\mathbb{Q}$-algèbre de dimension 2 et de base $\{1, \sqrt{2}\}$

En fait, L est aussi un corps $(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$

avec $a+b\sqrt{2} = 0 \iff a = b = 0$

On a construit en rajoutant $\sqrt{2}$ une extension de corps L de $\mathbb{Q}$ et $\sqrt{2} \in L$

déf :

Soient K et L deux corps.

On dit que L est une extension de K si $K \subset L$

exemple :

$\mathbb{Q}(\sqrt{2})$ est une extension de $\mathbb{Q}$

rmq :

Si L est une extension de K, L est en particulier une K-algèbre donc aussi K-espace vect.

et on note $[L:K]$ = degré de l'extension

$= \dim_K(L)$ si la dim est finie

ex :

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
- $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = 2$ car $\mathbb{C} = \{a+ib,\ a,b \in \mathbb{R}\}$
- $[\mathbb{R} : \mathbb{Q}] = \infty$

par l'absurde si il existe N nb irrationnel $r_1, r_2, \dots, r_N$ tq $\forall \alpha \in \mathbb{R}$ $\alpha = \sum_i^N \lambda_i r_i \approx \mathbb{Q}^N$

or $\mathbb{Q}^N$ dénombrable alors que $\mathbb{R}$ ne l'est pas.

- $[\mathbb{R}(X), \mathbb{R}] = \infty$

Prop

Si on considère une tour d'extensions finies ($\iff$ de degré fini) $K \subset L_1 \subset L_2$

Alors $[L_2 : K] = [L_2 : L_1][L_1 : K]$

preuve :

L_1 est un K-esp. de dim $n = [L_1 : K]$ où base de $L_1 = \{v_1, \dots, v_n\}$

L_2 est un L_1 - esp de dim $m = [L_1 : L_2]$ où base de $L_2 = \{w_1, \dots, w_m\}$

Alors on va montrer que $\{v_i w_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ est une base du K-esp vect L_2

En effet,

① $v_i w_j \in L_2$ car L_2 est un L_1-e.v.

② $\{v_i w_j\}$ est génératrice

car $\forall x \in L_2$ on peut écrire $x = \sum' \lambda_j w_j$ avec $\lambda_j \in L_1$ car $\{w_j\}$ base de L_2 ĉ L_1-ev

et on sait aussi $\lambda_j = \sum' k_{ij} v_i$ avec $k_{ij} \in K$ car $\{v_i\}$ base de L_1 comme K-ev.

$\Rightarrow x = \sum'_{i,j} k_{ij} v_i w_j$

③ $\{v_i w_j\}$ est K - libre

En effet,

on suppose qu'il existe $k_{ij} \in K$ vérifiant $\sum_{j=1}^{m} \left(\sum_{i=1}^{n}{}' k_{ij} v_i \right) w_j = 0$

comme $\{w_j\}$ base de L_2 sur L_1 on obtient $\forall j \ \sum_{i=1}^{n}{}' k_{ij} v_i = 0$

comme $\{v_i\}$ ——— L_1 — L_2 ——— $\forall i \ k_{ij} = 0$

$\boxtimes$

Exemple

$L_2 = \{a + b\sqrt{2} + c\sqrt{6}, \ a,b,c \in \mathbb{Q}\}$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\mathbb{Q} = K$, $\mathbb{Q}(\sqrt{2}) = L_2 = \{a + b\sqrt{2}, \ a,b \in \mathbb{Q}\}$

déf

On se donne une extension de corps $K \subset L$ et $\alpha \in L$.

On dit que α est algébrique sur K s'il existe un P non-nul $P \in K[X]$ tq $P(\alpha) = 0$.

En d'autres mots le morphisme d'évolution $\text{évl}_\alpha : K[X] \longrightarrow L$, $P \longmapsto P(\alpha)$ n'est pas injectif.

Si évl_α n'est pas injectif ($\Leftrightarrow \alpha$ algébrique)

Alors l'idéal $\ker(\text{évl}_\alpha) \neq (0)$

et comme $K[X]$ est principal, cet idéal a un générateur (unique si on le suppose unitaire) appelé le polynôme minimal de α, noté $P_{min,\alpha,K} \in K[X]$ et dépendant de α et de K

Exemples

① $\alpha = \sqrt{2}$, $K = \mathbb{Q}$

on considère $\text{évl}_{\sqrt{2}} : \mathbb{Q}[X] \longrightarrow \mathbb{R}$, $P \longmapsto P(\sqrt{2})$

$\ker(\text{évl}_{\sqrt{2}}) = (X^2 - 2)$

si $P(\sqrt{2}) = 0$ alors $X - \sqrt{2} \mid P$ dans $\mathbb{R}[X]$ mais $X - \sqrt{2} \notin \mathbb{Q}[X]$

donc le poly minimal annulant $\sqrt{2}$ est $X^2 - 2$

② $\alpha = i$, $K = \mathbb{Q}$

$\text{évl}_i : \mathbb{Q}[X] \longrightarrow \mathbb{C}$, $P \longmapsto P(i)$

$X - i \notin \mathbb{Q}[X]$

dc $\ker(\text{évl}_i) = (X^2 + 1)$

③ $\alpha = \frac{9}{4}$, $K = \mathbb{Q}$

$\ker(\text{évl}_{9/4}) = (X - \frac{9}{4})$

Rmq :
Dans le cas contraire, ie $\ker(ev_\alpha) = (0)$ $\Leftrightarrow$ $ev_\alpha : K[x] \longrightarrow L$ est injective,
On dit que α est transcendant

ex :
nb d'Euler $e = 2,718\ldots$, $\pi = 3,1415\ldots$ sont transcendants sur $\mathbb{Q}$

déf :
Une extension L de K est algébrique si tout $\alpha \in L$ est algébrique

Ex
$\mathbb{Q}(\sqrt{2})$ est une extension algébrique
Mais $\mathbb{R}(X)$ n'est pas une extension algébrique sur $\mathbb{R}$. car $X \in \mathbb{R}(X)$ n'est pas algébrique sur $\mathbb{R}$

Prop :
Si L est une extension finie de K,
Alors L est algébrique sur K
preuve :
L est finie de K $\Leftrightarrow$ L est un Kev de dim finie $= n$
si on se donne $\alpha \in L$, il faut mq α vérifie une équation polynomiale
on considère la suite des puissances de α : $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^k, \ldots$ $k \in \mathbb{N}$, $\alpha^k \in L$
mais L est de dim $= n$ sur K, toute famille ayant str. plus de n élts est nécessairement lin. dépendante (liée)
Donc $1, \alpha, \alpha^2, \ldots, \alpha^n$ ($n+1$ vecteurs) est une famille liée.
Donc il existe $\lambda_0, \ldots, \lambda_n \in K$ non tous nuls tq $\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \ldots + \lambda_n\alpha^n = 0$
Donc le polynôme $P(X) = \lambda_0 + \lambda_1 X + \ldots + \lambda_n X^n \neq 0$ vérifie $P(\alpha) = 0$
Donc α est algébrique sur K
$\square$

Rmq :
Si $\alpha \in L$ est algébrique sur K,
son polynôme minimal $P = P_{min,\alpha,K}$ est irréductible.
en effet,
$P(\alpha) = P_1(\alpha)P_2(\alpha) = 0$ $\Rightarrow$ $P_1(\alpha) = 0$ ou $P_2(\alpha) = 0$ $\Rightarrow$ P_1 ou $P_2 \in \ker(ev_\alpha)$ ABSURDE car P minimal

Prop
Soit $P \in K[X]$
$L = K[X]/(P)$ corps $\Leftrightarrow$ P irréductible ($\Leftrightarrow$ (P) maximal)

si L est un corps, c'est une extension finie de K de deg $[L:K] = \deg(P) = d$
et $1, \bar{X}, \ldots, \bar{X}^{d-1}$ est une K-base de L

II _ Construction d'extensions de corps

Construction

On se donne un corps K et un polynôme $P \in K[X]$ de degré $d = \deg(P)$

① Alors le quotient $K[X]/(P)$ est une K-algèbre de dim finie ayant comme base $\{\bar{1}, \bar{X}, \bar{X}^2, \dots, \bar{X}^{d-1}\}$ où $\bar{X}$ est la classe de $X \bmod (P)$, $\bar{X} \in K[X]/(P)$

② si $d \geq 1$ $K \subset L := K[X]/(P)$ est un corps (= extension de corps de K) $\Leftrightarrow$ P irreductible.

rmq

si $P = k \in K$ (ie $\deg P = 0$)

$(P) = K[X]$

$L := K[X]/K[X] = (0)$

preuve :

① déjà fait !

②

$\Rightarrow$] supposons que P est réductible

alors on peut écrire $P = R \cdot S$ avec $R \cdot S \in K[X]$ et $1 \leq \deg R < d$, $1 \leq \deg S < d$

alors on a des diviseurs de zéro dans L : $\bar{R} \cdot \bar{S} = \bar{P} = \bar{0}$ dans $L = K[X]/P$

comme $1 \leq \deg R < d$ alors $\bar{R} \neq \bar{0}$ car $\bar{R} = \sum_{i=0}^{d'} \lambda_i \bar{X}^i$ où $d' < d$

——— $1 \leq \deg S < d$ ——— $\bar{S} \neq \bar{0}$

Donc L n'est pas un corps car L a des div de zéros.

$\Leftarrow$] supposons P irreductible

on veut mq L est un corps ie mq $\forall l \in L$ $l \neq 0$ est inversible

soit $l \in L = K[X]/(P)$

on peut représenter $l \in L$ par un polynôme $Q \in K[X]$ avec $\deg Q < \deg P = d$

on peut appliquer l'identité de Bézout à $P, Q \in K[X]$

comme P est irréductible $(Q \nmid P)$ dc $PGCD(P,Q) = 1$ ou P mais $P \nmid Q$ car $\deg Q < \deg P$

$PGCD(P,Q) = 1$ à inversible près

ensuite, on écrit l'identité de Bézout dans $K[X]$ sur P, Q :

il existe $AP + BQ = PGCD(P,Q) = 1$

mtn, on repasse au quotient $K[X]/(P)$

$\underset{\bar{0}}{\bar{A} \cdot \bar{P}} + \underset{m}{\bar{B}} \cdot \underset{l}{\bar{Q}} = \bar{1}$

Si on note $m = \bar{B}$, on a $m \cdot l = 1$

Donc l est inversible ie L est un corps.

$\square$

Application 1 :

Soient K et $p \in K[X]$

Alors il existe une extension de corps finie $K \subset L$ qui contient toutes les racines de P

ie $\exists\, \alpha_1, \dots, \alpha_d \in L$ tq $P = \lambda(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_d)$ avec $\lambda \in K$

Ex :

si $K = \mathbb{Q}$

$P := X^3 - 2 \in \mathbb{Q}[X]$

P a des racines dans $\mathbb{C}$:
- il y a une racine réelle
- il y a deux racines complexes $\sqrt[3]{2}\, e^{2i\pi/3}$ et $\sqrt[3]{2}\, e^{4i\pi/3}$

Rmq :

$\mathbb{C}$ contient toutes les racines de $P = X^3 - 2$ et $\mathbb{Q} \subset \mathbb{C}$

Mais $[\mathbb{C} : \mathbb{Q}] = \infty$

donc on ne peut pas prendre $L = \mathbb{C}$ car ce n'est pas une extension finie

on fait alors la construction précédente $\mathbb{Q} \subset L = \mathbb{Q}[X]/(X^3-2)$ corps car X^3-2 est irréduct. dans $\mathbb{Q}[X]$

$[L:\mathbb{Q}] = 3$

$L = \mathrm{Vect}_{\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{4}) \subset \mathbb{R}$

application 1 :

$P \in K[X]$

Il existe une extension finie $K \subset L$ dans laquelle P a toutes ses racines $\alpha_1, \dots, \alpha_d \in L$

$P = \prod_{i=1}^{d} (X - \alpha_i)$

preuve

on suppose P irréductible dans $K[X]$

on fait la preuve de manière itérativative

* on commence par construire $K \subset L_1 = K[X]/(P)$ où L_1 contient déjà une racine $\alpha_1 = \bar{X} = X \bmod (P)$

$P(\alpha) = 0$

$\bar{P} = \overline{\sum_{i=0}^{d} \lambda_i X^i} = \bar{0} = \sum \lambda_i \bar{X}^i = \bar{0}$

donc $P = (X-\alpha) P_1$ dans $L_1[X] \supset K[X]$ avec $P_1 \in L_1[X]$

* ensuite, on choisit un facteur irréductible de P_1 et on recommence :

$L_2 = L_2[X]/(P_1)$

⋮

* on finira par trouver une extension finie qui contient toutes les racines de P

$\square$

Exemple :

$K = \mathbb{Q}$ $P = X^3 - 2$

$\mathbb{Q} \subset L_1 = \mathbb{Q}[X]/(X^3-2) \subset L_2 = L_1[X]/(P_1)$ (deg 2)

deg 3

$\mathbb{Q}[X]/(X^3-2) = \mathbb{Q}(\sqrt[3]{2})$

$X^3 - 2 = (X - \sqrt[3]{2}) P_2$ et $P_2 \in \mathbb{Q}(\sqrt[3]{2})[X]$

Application 2 : Construction des corps finis.

on veut décrire les K corps et ens. fini

on sait que $K = \mathbb{Z}/p\mathbb{Z}$, pour p premier, est un corps.

si on se donne un polynôme $P \in \mathbb{Z}/p\mathbb{Z}[X]$ irréductible de degré d.

on a vu que $L = \mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un corps

ce corps est fini de card p^d car $L = \mathrm{vect}_{\mathbb{Z}/p\mathbb{Z}}(1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{d-1}) \cong ((\mathbb{Z}/p\mathbb{Z})^d, +)$ (en tant que grpe abélien)

un elt de L correspond à un d-uplet $(\lambda_0, \lambda_1, \dots, \lambda_{d-1})$ avec $\lambda_i \in \mathbb{Z}/p\mathbb{Z}$

Exemple :

$P = X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$

P irréductible

$L = \mathbb{Z}/2\mathbb{Z}[X]/(P)$ corps fini de card $2^2 = 4$

Thm :

1)

Pour tout p premier et $d \geq 1$, il existe un polynome irréductible de degré d dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Rightarrow$ il existe un corps fini de card p^d

2)

Tout corps fini est isomorphe à un corps fini du type $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ avec P irréductibles ds $\mathbb{Z}/p\mathbb{Z}[X]$

Prop :

Si K est un corps fini,

Alors il existe p premier tq $\mathbb{Z}/p\mathbb{Z} \subset K$ et K est de card p^d pour $d \in \mathbb{N}^*$

preuve :

si K corps, on regarde l'application (= homomorphisme d'anneaux)

$\mathbb{Z} \xrightarrow{i} K$

$n \longmapsto 1 + 1 + \dots + 1$

unité de K

$\ker(i) \subsetneq \mathbb{Z}$ car i n'est pas inj car K fini

$\ker(i)$ est un ideal non nul de $\mathbb{Z}$

donc de la forme $p\mathbb{Z}$ et p est necessairement un nb premier car si $p = ab$ est composé ($a \neq 1$ et $b \neq 1$)

$$p \cdot 1 = \overbrace{1_K + \dots + 1_K}^{p \text{ fois}} = 0$$

$$\underset{i(a)\cdot i(b)}{\overset{i(p)}{\shortparallel}} \Leftrightarrow \underbrace{(1_K + \dots + 1_K)}_{a \text{ fois}}\underbrace{(1_K + \dots + 1_K)}_{b \text{ fois}} = 0$$

on a $i(p) = i(a) \cdot i(b) = 0$ donc $i(a)$ est un diviseur de zero ce qui contredit K corps.

déf

On dit qu'un corps est algébriquement clos si pour tout $P \in \mathbb{K}[X]$, P se factorise en facteurs linéaires dans $\mathbb{K}[X]$ ie il existe $\alpha_1, \dots, \alpha_d \in \mathbb{K}$ tq $P = \lambda \prod_{i=1}^{d} (X - \alpha_i)$

Rmq:

En fait il suffit de demander que tout polynôme P admet au moins une racine dans $\mathbb{K}$

Thm:

Le corps $\mathbb{C}$ (= nombres complexes) est algébriquement clos (ex. TD)

Thm (admis)

Soit K un corps quelconque

Alors il existe un corps $\overline{K}$ algébriquement clos qui contient K, $K \subset \overline{K}$, avec la prop universelle suivante

$\forall K \subset L$ avec L alg. clos, il existe un unique homomorphisme de corps

$$\begin{tikzcd} K \arrow[r, hook] \arrow[dr] & \overline{K} \arrow[d, "i"] \\ & L \end{tikzcd}$$

Exemple

Prenons $K = \mathbb{Q}$

$\overline{K} = \overline{\mathbb{Q}}$ = une clôture algebrique de $\mathbb{Q}$ $= \{\alpha \mid \alpha$ algébrique sur $\mathbb{Q}\}$

Si on prend une extension de $\mathbb{Q}$ alg. clos (p. ex $\mathbb{C}$) on a :

$$\begin{tikzcd} \mathbb{Q} \arrow[r, hook] \arrow[dr, hook] & \overline{\mathbb{Q}} \arrow[d, hook] \\ & \mathbb{C} \end{tikzcd}$$

Donc on peut représenter la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ comme un sous-corps de $\mathbb{C}$.

Donc on a les inclusions $\underset{\substack{\sqrt{2} \in \overline{\mathbb{Q}} \\ \sqrt{2} \notin \mathbb{Q}}}{\mathbb{Q} \subsetneq \overline{\mathbb{Q}}} \underset{\substack{e, \pi \in \overline{\mathbb{Q}} \\ i \in \overline{\mathbb{Q}}}}{\subsetneq} \mathbb{C}$

Prop

Tout homomorphisme d'anneaux non-nul $f : K \to A$ d'un corps K vers un anneau A est injectif

preuve:

$\ker(f) \subset K$

ideal car ker d'un homo d'anneaux.

or comme K est un corps, K n'a que 2 idéaux (0) et K

mais $\ker(f) \neq K$ car on a supposé $f \neq 0$

Rmq

①

En particulier si A est un autre corps, tout homomorphisme de corps non-nul est injectif.

②

Autre cas particulier, si on prend une extension finie $K \subset L$.

Alors tout homomorphisme de corps-K-linéaire $\varphi : L \to L$ non-nul est un isomorphisme

En effet,

Par la remarque précédente φ est injectif
mais comme φ est K-linéaire entre deux K-ev de même dim
on conclut que φ est un isomorphisme. (thm du rg)

<u>déf</u>
Un isomorphisme d'un corps dans lui-même est appelé un automorphisme.
Si L extension de K, un automorphisme est un iso K-linéaire de L dans L.
<u>déf</u>
Pour une extension de corps fini $K \subset L$, on note $\mathrm{Aut}_K(L) = \{ \varphi : L \to L,\ \varphi$ homo d'anneaux K-linéaire$\}$

<u>Rmq</u>:
$\mathrm{Aut}_K(L)$ est un groupe pour la compositions des homomorphismes $\varphi_1 \cdot \varphi_2 = \varphi_1 \circ \varphi_2$

$$\begin{tikzcd} L \arrow[r, "\varphi_2"] \arrow[rr, bend right, "\varphi_1 \circ \varphi_2"'] & L \arrow[r, "\varphi_1"] & L \end{tikzcd}$$

En effet, la rmq précédente montre que tout $\varphi \in \mathrm{Aut}(L)$ est inversible

<u>Rmq</u>
$(\mathrm{End}(V), \circ)$ n'est pas un groupe car il y a des elts non inversibles.
ev.

<u>Exemple</u>
$K = \mathbb{Q}$
$L = \mathbb{Q}(\sqrt{2})$
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ tq $\mathbb{Q}(\sqrt{2}) = \mathrm{Vect}_{\mathbb{Q}}(1, \sqrt{2})$

$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{ \varphi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ $\mathbb{Q}$-linéaire, $\varphi(ab) = \varphi(a) + \varphi(b)$ $\forall a, b \in \mathbb{Q}(\sqrt{2}) \}$

$\mathrm{mat}_{\{1,\sqrt{2}\}}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ $\varphi(\sqrt{2}) \cdot \varphi(\sqrt{2}) = \varphi((\sqrt{2})^2) = \varphi(2) = 2\varphi(1) = 2$

Donc on a trouvé deux automorphismes $\varphi_1, \varphi_2 \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$

$\mathrm{Id} = \mathrm{mat}_{\{1,\sqrt{2}\}}(\varphi_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\mathrm{mat}_{\{1,\sqrt{2}\}}(\varphi_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Donc $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = (\mathbb{Z}/2\mathbb{Z}, +) = (\{\mathrm{Id}, \varphi_2\}, \circ)$

<u>Prop</u>
Si on se donne deux extensions de K, $K \subset L$ et $K \subset L'$
et $\alpha \in L$, $P \in K[X]$ tq $P(\alpha) = 0$ et $\varphi : L \to L'$ homom. de K-algèbre ($\Leftrightarrow$ K-lin et hom. d'anneaux)
$0 \mapsto 0$, $1_K = 1_L \mapsto 1_K = 1_{L'}$
Alors $P(\varphi(\alpha)) = 0$
<u>preuve</u>:
si on écrit $P = \sum_{i=0}^{d} \lambda_i X^i$ avec $\lambda_i \in K$
$P(\alpha) = 0 \iff \sum_{i=0}^{d} \lambda_i \alpha^i = 0$ (dans L)
si on applique φ, on obtient $0 = \varphi(0) = \varphi\left(\sum_{i=0}^{d} \lambda_i \alpha^i\right)$
$= \sum_{i=0}^{d} \lambda_i \varphi(\alpha^i)$ par K-linéarité de φ
$= \sum_{i=0}^{d} \lambda_i (\varphi(\alpha))^i$ par φ homo d'anneaux

$\iff P(\varphi(\alpha)) = 0$

$\boxtimes$

Cas particulier:

$L' = L$, $\alpha \in L$

$\varphi \in Aut_K(L)$ et si $P(\alpha) = 0$ alors $P(\varphi(\alpha)) = 0$

Si P est le polynôme minimal de α, alors φ envoie α sur une autre racine de son poly min.

Exemple

$\varphi \in Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$

$P_{min}(\sqrt{2}) = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ dans $\mathbb{Q}(\sqrt{2})[X]$

$\Rightarrow \varphi(\sqrt{2}) = \pm\sqrt{2}$

Autre cas particulier:

si $L = K(\alpha)$ où P = poly min de α, $\deg(P) = d$

$\varphi \in Aut_K(K(\alpha))$

φ est en fait déterminé par l'image $\varphi(\alpha)$ car si $\alpha \mapsto \varphi(\alpha)$ alors $\alpha^i \mapsto \varphi(\alpha^i) = \varphi(\alpha)^i$

mais $\varphi(\alpha)$ doit être une racine de P (par la prop. précédente)

Donc $\# Aut_K(K(\alpha)) \leq d = [K(\alpha) : K]$ car φ est déterminé par le choix d'une racine de P.

et P a au plus $\deg(P) = d$ racines distinctes dans $K(\alpha)$

Prop

$K \subset K(\alpha)$ et $K \subset L$ une extension et $\beta \in L$

On note P le polynôme minimal de α sur K, $P \in K[X]$

On suppose que β est une racine de P $\Leftrightarrow P(\beta) = 0$

Alors il existe un unique homom. (de K-algèbres) $\varphi : K(\alpha) \longrightarrow L$

$\alpha \longmapsto \beta = \varphi(\alpha)$

preuve:

on sait que $K(\alpha) = K[X]/(P)$

on définit $\tilde{\varphi} : K[X] \longrightarrow L$

$Q \longmapsto Q = \tilde{\varphi}(Q)$

comme β vérifie $P(\beta) = 0$, $P \in \ker(\tilde{\varphi}) \Rightarrow (P) \subset \ker(\tilde{\varphi})$

Donc l'application $\tilde{\varphi}$ se factorise à travers $K[X]/(P)$

$$\begin{tikzcd}
X \in K[X] \arrow[r, "\tilde{\varphi}", "Q \mapsto Q(\beta)"'] \arrow[d, mapsto] & L \\
\bar{X} = \alpha \in K[X]/(P) \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

$\tilde{\varphi}(X) = \beta$ donc $\varphi(\alpha) = \beta$.

L'unicité vient du fait que φ est déterminé par $\varphi(\alpha)$ qui est donné $\varphi(\alpha) = \beta$

$\square$

Corollaire

$\# Hom_K(K(\alpha), L) \leq \deg P = [K(\alpha) : K]$

Prop

Soit $K \subset L$ une extension finie

Alors, 1. $|Aut_K(L)| \leq [L : K]$

2. Si M est une autre extension de K alors $\# Hom(L, M) \leq [L : K]$

pas necessairement finie

preuve:

- si $L = K(\alpha)$ ok avec le corollaire
- soit L une extension finie qcq de K, on peut trouver $\alpha_1, \dots, \alpha_n \in L$ tq $K(\alpha_1, \dots, \alpha_n) = L$

idée: faire une recurrence sur n = le nb de générateurs

$n = 1$ ok

$K \subset K(\alpha_1, \dots, \alpha_{n-1}) \subset L = K(\alpha_1, \dots, \alpha_n)$

L est une extension finie de K

Il existent $\alpha_1, \dots, \alpha_n \in L$ tq $L = K(\alpha_1, \dots, \alpha_n)$

On va démontrer l'inégalité par récurrence sur n.

. Si $n = 1$,

$L = K(\alpha_1)$ avec α_1 algébrique et $P = P_{min, \alpha_1, K} \in K[X]$ et $\deg P = [L:K]$

si $\phi \in \mathrm{Hom}_K(L,M)$, $\phi(\alpha_1)$ est une racine de $P \in K[X]$

$$\phi : \begin{array}{l} L \to M \\ \alpha_1 \mapsto \phi(\alpha_1) \end{array}$$

ϕ est determinée par $\phi(\alpha_1)$

et P a au plus $\deg P = [L:K]$ racines distinctes

Donc $\# \mathrm{Hom}_K(L,M) \leq \#\{\text{racines distinctes de } P\} \leq \deg P = [L:K]$

. on suppose que l'inégalité est vraie pour une extension ayant $n-1$ générateurs

$K \subset K(\alpha_1, \dots, \alpha_{n-1}) = L' \subset L = K(\alpha_1, \dots, \alpha_n) = L'(\alpha_n)$

Si $\phi \in \mathrm{Hom}_K(L,M)$ et si on note ϕ' la restriction de ϕ à L'

par hypothèse de récurrence $\# \mathrm{Hom}_K(L',M) \leq [L':K]$

De plus, α_n est algébrique sur L'

$$L'(\alpha_n) = \begin{array}{ccc} L & \xrightarrow{\phi} & M \\ \cup & \nearrow_{\phi'} & \\ L' & & \\ \cup & & \\ K & & \end{array}$$

Si on note $P = P_{min, \alpha, L}$

On a : $\phi : L = L'(\alpha_n) \longrightarrow M$, $\phi(\alpha_n) \in M$ est une racine du polynôme $\phi(P)$

$$\begin{array}{ccc} L'(\alpha_n) & \longrightarrow & M \\ \cup & \nearrow_{\phi'} & \\ L' & & \end{array}$$

$\phi(P) \in \overset{M}{\overset{\cup}{\phi(L')}}[X]$

Mais $\phi(P)$ a le même degré que P car ϕ est injectif

Donc comme ϕ est déterminé par $\phi' = \phi|_{L'}$ et par $\phi(\alpha_n)$

et $\phi(\alpha_n)$ est une racine d'un polynome de degré $\deg P$.

D'où $\# \mathrm{Hom}_K(L,M) \leq \underbrace{\# \mathrm{Hom}_K(L',M)}_{\overset{H.R}{\leq} [L':K]} \cdot \underbrace{\#\{\text{racine de } \phi(P)\}}_{\leq \deg P = [L:L']}$

et comme $[L':K][L:L'] = [L:K]$

<u>déf</u>: (corps de décomposition d'un polynôme)

K corps, $P \in K[X]$

Le corps de décomposition de P sur K est l'extension finie L engendrée dans une clôture algébrique $\bar{K}$ par les racines de P.

C'est-à-dire, si on choisit une clôture algébrique $\bar{K}$, P a toutes ses racines $\alpha_1, \dots, \alpha_n$ dans $\bar{K}$ et $L = K(\alpha_1, \dots, \alpha_n)$

<u>Rmq</u>:

Si on fixe une clôture alg. $\bar{K}$, L est le plus petit corps contenant toutes les racines de P.

<u>Exemple</u>:

$K = \mathbb{Q}$, $P = X^3 - 2 \in \mathbb{Q}[X]$

racines de P dans $\bar{\mathbb{Q}} \subset \mathbb{C}$ $\sqrt[3]{2}$, $\sqrt[3]{2} \cdot \omega$, $\sqrt[3]{2}\, \omega^2$ où $\omega = e^{2i\pi/3}$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2} \cdot \omega)$

corps de décomposition de P $= \mathbb{Q}(\sqrt[3]{2}, \omega)$

<u>Rmq</u>:

Soit $P \in K[X]$ et L son corps de décomposition

si $\deg P = n$ et P a m ($\leq n$) racines distinctes dans $\bar{K}$

Alors on a un homomorphisme de groupes - injectif

$$\begin{array}{ccc} \mathrm{Aut}_K(L) & \hookrightarrow & \mathfrak{S}_n \\ \phi & \longmapsto & \sigma_\phi : \{\alpha_1, \dots, \alpha_m\} \mapsto \{\phi(\alpha_1), \dots, \phi(\alpha_m)\} \end{array}$$

groupe symétrique = groupe des permut

déf

K corps quelconque et $P \in K[X]$

On dit que P est séparable si $PGCD(P, \underset{\text{dérivée}}{P'}) = 1$

Prop

P séparable $\iff$ les racines de P dans une clôture algébrique $\overline{K}$ sont simples

ie P n'a pas de racine double

preuve:

$\Rightarrow$)

si $PGCD(P, P') = 1$

on a la relation de Bezout $AP + BP' = 1$

Obs: P a une racine double $\alpha \in \overline{K} \iff P(\alpha) = 0$ et $P'(\alpha) = 0$

Si on a $AP + BP' = 1$, P ne peut pas avoir de racine double $A(\alpha)\overset{=0}{P(\alpha)} + B(\alpha)\overset{=0}{P'(\alpha)} \neq 1$

$\Leftarrow$)

Inversement, si $PGCD(P, P') = \Delta$ non cst $\in K[X]$

on a $\deg \Delta \geq 1$ dc Δ admet une racine $\alpha \in \overline{K}$

et comme $\Delta | P$ et $\Delta | P'$ on obtient $P(\alpha) = 0$ et $P'(\alpha) = 0$

Donc α racine double

Prop

si $car(K) = 0$ (ie $\begin{array}{l} \mathbb{Z} \longrightarrow K \\ n \longmapsto n \cdot 1_K \end{array}$ est injectif)

alors tout polynôme irreductible est séparable.

preuve

supposons $car(K) = 0$

prenons P un polynôme irreductible

alors $PGCD(P, \underset{\neq 0}{P'}) = \begin{cases} 1 \\ \text{ou} \\ P \end{cases}$

or $\deg(P') < \deg P$ dc P ne peut pas diviser P'

D'où $PGCD(P, P') = 1$

P est séparable

$\boxtimes$

Rmq:

si $car(K) = p > 0$, il existe des polynômes non-séparables

par ex: $K = \mathbb{F}_p(T) = \{ \frac{A}{B}, A, B \in \mathbb{F}_p[X] \}$

$P \in K[X]$

$P = X^p - T$

$P' = 0$

Prop

Soit α algébrique sur K

Le polynôme minimal de α sur K, $P = P_{min, \alpha, K}$ est irreductible

preuve:

si $P = A \cdot B$ est réductible

$0 = P(\alpha) = A(\alpha) \cdot B(\alpha) \in \overline{K} \Rightarrow A(\alpha) = 0$ ou $B(\alpha) = 0$ ce qui contredit la minimalité de P

$\boxtimes$

Cor

si $car(K) = 0$, tout élément α algébrique possède un poly minimal séparable.

donc il y en a au plus (= exactement) $p^k < p^n$

comme $p^k < p^n$ on voit qu'il existe $x \in \mathrm{Dec}(X^{p^n} - X)$ tq $x^{p^k} \neq x$ dc $\phi^k \neq Id$ pour $k \leq p-1$

mais $\phi^n : x \mapsto x^n$ et $\forall x \in K$ $x^{p^n} = x$ dc $\phi^n = Id$

déf

α séparable si le polynome minimal de α est séparable

déf

Une extension $K \subset L$ est séparable si tout élément α de L est séparable

Thm

Soit K un corps fini

Alors :
1) il existe un nombre premier p $(= car(K))$ tq $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subset K$
et K est un $\mathbb{F}_p$ = esp. vectoriel de dim $n \in \mathbb{N}^*$
dc $|K| = p^n$
2) Si on choisit une clôture algébrique $\overline{\mathbb{F}_p}$
K est isomorphe au corps de décomposition du polynôme $X^{p^n} - X \in \mathbb{F}_p[X]$
3) L'application $\Phi : K \to K$, $\Phi(x) = x^p$ est un automorphisme de l'extension $\mathbb{F}_p \subset K$
il est appelé le morphisme de Frobenius et $Aut_{\mathbb{F}_p}(K) = \{Id, \phi, \phi^2, \dots, \phi^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$
c'est le grp cyclique d'ordre $n = [K : \mathbb{F}_p]$

preuve:

1) soit $i : \mathbb{Z} \longrightarrow K$
$n \longmapsto n 1_K$

comme K fini, i n'est pas injectif
donc il existe un entier $p > 0$ tq $i(p) = 0$
de plus p est premier car K corps donc K n'a pas de div de zéros
donc $\mathbb{F}_p = \mathbb{Z}/_{ker(i)} \subset K$
si on note $n = \dim_{\mathbb{F}_p}(K)$ on obtient $|K| = p^n$ et $K \cong \mathbb{F}_p^{\,n}$ comme groupe abélien (pour +)

2) on choisit une clôture algébrique $\overline{\mathbb{F}_p}$
comme K est un corps, $K^* = K \setminus \{0\}$ est un groupe (pour $\times$) d'ordre $p^n - 1$
d'après le thm de Lagrange $\forall x \in K^*$ $ord_{K^*}(x) \mid p^n - 1 \Rightarrow x^{p^n-1} = 1 \Rightarrow x^{p^n-1} = x$
Donc $\forall x \in K$, x est racine du polynome $X^{p^n} - X \in \mathbb{F}_p[X]$
si on choisit un morphisme de K dans $\overline{\mathbb{F}_p}$ $j : K \hookrightarrow \overline{\mathbb{F}_p} \supset \mathbb{F}_p$
on voit que $j(K) \subset$ corps de décomposition de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$
Et $P = X^{p^n} - X \in \mathbb{F}_p[X]$, $P' = p^n X^{p^n-1} - 1 = -1$
Donc $PGCD(P, P') = 1$ ie P séparable
D'où P a exactement p^n racines simples dans $\overline{\mathbb{F}_p}$
On sait que $j : K \longrightarrow Déc(P)$ injectif
dc j est un isomorphisme

3) $\phi : K \to K$, $x \mapsto x^p$ c'est un homomorphisme d'extension de corps

$\forall x, y \in K$ $\forall \lambda \in \overline{\mathbb{F}_p}$
1) $(x+y)^p = x^p + y^p$
2) $(xy)^p = x^p y^p$
3) $\lambda^p x^p = \lambda x^p$ (fermat)

Obs: si $1 \leq k \leq p-1$ $\binom{k}{p} = \dfrac{p(p-1)\cdots(p-k+1)}{k!}$ est divisible par p.
$k!\binom{k}{p} = p(p-1)\cdots(p-k+1)$
Comme $PGCD(p, k!) = 1$ par le lemme de Gauss on déduit que $p \mid \binom{k}{p}$
Donc $\phi \in Aut_{\mathbb{F}_p}(K)$ et $\phi^k(x) = (((x^p)^p)^p)^{\cdots p} = x^{p^k}$
D'après un résultat précédent $|Aut_{\mathbb{F}_p}(K)| \leq [K : \mathbb{F}_p] = n$
on regarde l'ensemble des points fixes par ϕ^k
le $x \in \overline{\mathbb{F}_p}$ vérifiant $\phi^k(x) = x \iff x^{p^k} - x = 0$
$\Rightarrow x$ est une racine du poly $X^{p^k} - X$