

## Leçon 125 - Extensions de corps. Exemples et applications.

### 1. Corps et extensions de corps. —

#### 1. Définitions et premières propriétés. —

- Def : Un corps  $K$  est un anneau commutatif unitaire pour lequel tout élément non nul est inversible.
- Ex :  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, K(X)$  sont des corps.
- Def+Pro : Pour tout corps  $K$ , le noyau de l'unique morphisme d'anneaux de  $\mathbb{Z}$  vers  $K$  est un idéal de  $\mathbb{Z}$ .  
Si cet idéal est réduit à  $\{0\}$ , on dit que  $K$  est de caractéristique 0. S'il est engendré par  $n \geq 1$ , on dit que  $K$  est de caractéristique  $n$ .
- Pro : Si  $\text{car}(K) \neq 0$ , alors  $\text{car}(K) = p$  pour  $p$  premier.
- Ex :  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sont de caractéristique 0.  $\mathbb{F}_p$  est de caractéristique  $p$ .  $K(X)$  est de caractéristique  $\text{car}(K)$ .
- Rem : Si  $\text{car}(K) = 0$ , alors  $K$  est forcément infini, mais la réciproque est fausse.
- Def+Pro : Un corps  $L$  est une extension de corps sur  $K$  ssi il existe un morphisme d'anneaux  $i$  de  $K$  dans  $L$ . On note en général l'extension  $L/K$ .  
Un morphisme d'anneaux dont l'espace de départ est un corps est forcément injectif. On peut alors identifier  $K$  par son image  $i(K)$  dans  $L$  afin de le voir comme un sous-corps de  $L$ .
- Ex :  $\mathbb{R}$  est une extension de corps de  $\mathbb{Q}$ ,  $\mathbb{Q}(i)$  est une extension de corps de  $\mathbb{Q}$ ,  $K(X)$  est une extension de corps de  $K$ .
- Def : Soit  $L/K$  une extension de corps. On définit  $[L : K] \in \mathbb{N}^* \cup \{+\infty\}$  le degré de l'extension par  $\dim_K(L)$  la dimension de  $L$  comme  $K$ -ev.  
On dit que  $L/K$  est finie si  $[L : K] < +\infty$ .
- Ex :  $[\mathbb{C} : \mathbb{R}] = 2$ ,  $[\mathbb{R} : \mathbb{Q}] = +\infty$ ,  $[K(X) : K] = +\infty$ ,  $\mathbb{Q}(j) : \mathbb{Q} = 2$ .
- Def : Pour  $M/K$  une extension de corps, et  $x_1, \dots, x_n \in M$ , on définit  $K(x_1, \dots, x_n)$  le sous-corps de  $M$  engendré par  $K, x_1, \dots, x_n$ , càd le sous-anneau engendré par les éléments de  $K$ , les  $x_i$ , et les  $x_i^{-1}$ .
- Théorème de la base télescopique : Pour  $L/K$  et  $M/L$  des extensions de corps, on a  $[M : K] = [M : L].[L : K]$ .
- Pro : Soit  $M/K$  une extension de corps et  $L_1, L_2$  deux sous-corps de  $M$  contenant  $K$ , tels que  $L_1/K$  et  $L_2/K$  sont des extensions finies.  
Soit  $L$  le corps engendré par  $L_1$  et  $L_2$ . Alors  $[L : K] = [L_1 : K].[L_2 : K]$  et  $\text{ppcm}([L_1 : K], [L_2 : K]) = [L : K]$ .
- Si  $[L_1 : K]$  et  $[L_2 : K]$  sont premiers entre eux, alors on a  $[L : K] = [L_1 : K].[L_2 : K]$ .
- Ex :  $[\mathbb{Q}(\sqrt[3]{5}, j, \sqrt[3]{2}) : \mathbb{Q}] = 7 * 2 * 3 = 42$ .

#### 2. Eléments algébriques, extensions algébriques. —

- Def : Soit  $L/K$  une extension de corps. Un  $x \in L$  est dit algébrique sur  $K$  s'il existe  $P \in K[X]$  tel que  $P(x) = 0$ . Il est dit transcendant sinon.  
 $L$  est appelée extension algébrique de  $K$  si tous ses éléments sont algébriques sur  $K$ .

- Def+Pro : Pour  $x$  algébrique sur  $K$ , il existe un unique polynôme unitaire générateur de l'idéal des polynômes annulateurs de  $x$ . On le note  $\text{Irr}(x, K)$  et on l'appelle polynôme minimal de  $x$  sur  $K$ .
- Pro : Pour tout  $P \in K[X]$  tel que  $P(x) = 0$ , on a  $\text{Irr}(x, K) | P$ . Ainsi,  $\text{Irr}(x, K)$  est irréductible sur  $K$ .
- Ex :  $\sqrt[n]{n}$  est algébrique sur  $\mathbb{Q}$ ,  $\exp^{i\pi \frac{k}{n}}$  est algébrique sur  $\mathbb{Q}$ ,  $i$  est algébrique sur  $\mathbb{R}$ .  
 $K \in K(X)$  est transcendant sur  $K$ .
- Pro :  $e, \pi$  sont transcendants sur  $\mathbb{Q}$ .
- Pro : Les extensions finies sont algébriques.
- Ex : Pour  $p_n$  le  $n$ -ième nombre premier et  $F_n := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ ,  $F = \cup_n F_n$  est une extension algébrique de  $\mathbb{Q}$ , avec  $[F : \mathbb{Q}] = +\infty$ .
- Pro : Pour  $M/L/K$ , et  $x \in M$  algébrique sur  $K$ , on a  $\text{Irr}(x, L) | \text{Irr}(x, K)$  dans  $L[X]$ .
- Thm : Un élément  $x \in L$  est algébrique sur  $K$  ssi le corps  $K(x)$  est une extension algébrique de  $K$ , ssi  $K(x)$  est une extension finie de  $K$ .  
On a alors  $[K(x) : K] = \deg(\text{Irr}(x, K))$ , et  $\{1, x, x^2, \dots, x^{\deg(\text{Irr}(x, K)-1)}\}$  est un  $K$ -base de  $K(x)$ .
- Ex :  $\mathbb{C}$  est une extension algébrique de  $\mathbb{R}$ .  $\mathbb{R}$  n'est pas une extension algébrique de  $\mathbb{Q}$ .  $K(T)$  n'est pas une extension algébrique de  $K$ .
- Thm : Si  $x_1, \dots, x_n$  sont algébriques sur  $K$ , alors  $K(x_1, \dots, x_n)$  est une extension algébrique finie de  $K$ , avec  $[K(x_1, \dots, x_n) : K] \leq \prod_i [K(x_i) : K]$ .
- Cor :  $L/\mathbb{K}$  est finie ssi l'extension est algébrique et engendrée par  $K$  et par un nombre fini d'éléments.
- App : L'ensemble des éléments de  $L$  algébriques sur  $K$  est un sous-corps de  $L$ .
- Ex :  $\sqrt{2} + \sqrt[3]{5}$  est algébrique sur  $\mathbb{Q}$ .
- Ex : L'ensemble  $\overline{\mathbb{Q}}$  des éléments de  $\mathbb{C}$  algébriques sur  $\mathbb{Q}$  est un sous-corps de  $\mathbb{C}$ .

### 2. Adjonction de racines. —

#### 1. Corps de Rupture. —

- Def : Soit  $P \in K[X]$  irréductible sur  $K$ . Un corps de rupture de  $P$  sur  $K$  est une extension de corps  $L$  sur  $K$  telle que  $P$  admet une racine  $\lambda$  dans  $L$ , et telle que  $L$  est engendré par  $K$  et  $\lambda$ .
- Pro : Pour tout  $P \in K[X]$  irréductible, le corps  $K[X]/(P)$  est un corps de rupture de  $P$  sur  $K$ .  
De plus, le corps de rupture de  $P$  sur  $K$  est une extension finie de degré  $\deg(P)$  sur  $K$  et est unique à isomorphisme de  $K$ -algèbre près.
- Cor : Pour  $L/K$  et  $x \in L$  algébrique sur  $K$ ,  $K(x)$  est le corps de rupture de  $\text{Irr}(x, K)$  sur  $K$ .
- Ex :  $\mathbb{C}$  est le corps de rupture de  $X^2 + 1$  sur  $\mathbb{R}$ . Les polynômes  $X^p + X + 1$  sont irréductibles sur  $\mathbb{F}_p$ . Cela permet de construire des corps à  $p^p$  éléments comme  $\mathbb{F}_4$  pour  $p = 2$ .
- Pro : Soit  $P \in K[X]$  de degré  $n \geq 2$ .  $P$  est irréductible sur  $K$  ssi  $P$  n'admet aucune racine dans toute extension de corps finie de degré  $\leq \lfloor \frac{n}{2} \rfloor$ .

- App :  $X^4 + 1$  est irréductible dans  $\mathbb{Q}[X]$  mais est pourtant réductible dans tous les  $\mathbb{F}_p[X]$ .
- Thm : Soit P un polynôme irréductible sur  $K$  de degré  $n$ . Soit L une extension algébrique finie de  $K$  de degré  $m$ . Si  $m \wedge n = 1$ , alors P est irréductible sur L.
- Ex :  $X^3 + X + 1$  est irréductible sur  $\mathbb{Q}(i)$ .
- Contre-ex :  $X^4 + 1$  n'est pas irréductible sur  $\mathbb{Q}(i)$ .

## 2. Corps de décomposition. —

- Def : Soit L une extension de corps sur  $\mathbb{K}$ ,  $P \in K[X]$  de degré  $n$ . L est un corps de décomposition de P sur  $K$  si P est scindé dans L et si L est engendré par  $K$  et par les racines de P.
- Pro : Pour tout polynôme P de degré  $\geq 1$ , il existe un corps de décomposition de P sur  $K$ . Ce corps de décomposition est une extension finie de degré  $\leq n!$ , et est unique à isomorphisme de  $K$  – algèbre près.
- Ex :  $\mathbb{Q}(\sqrt{2})$  est le corps de décomposition de  $X^2 - 2$  sur  $\mathbb{Q}$ .  $\mathbb{Q}(\sqrt{2}, i)$  est le corps de décomposition de  $X^4 - 1$  sur  $\mathbb{Q}$ .
- Ex :  $\mathbb{Q}(\sqrt[3]{2})$  n'est qu'un corps de rupture de  $X^3 - 2$  sur  $\mathbb{Q}$ . Son corps de décomposition est  $\mathbb{Q}(\sqrt[3]{2}, j)$ , qui est une extension de degré  $3! = 6$  sur  $\mathbb{Q}$ .
- App : Pour tout p premier et pour tout  $q = p^r$ , il existe un corps fini à  $q$  éléments. Il est à isomorphisme près le corps de décomposition de  $X^q - X$  sur  $\mathbb{F}_p$ . On le note  $\mathbb{F}_q$ .
- Cor : Pour  $q = p^r$ ,  $F = \cup_n \mathbb{F}_{q^n}$  peut ainsi être bien défini, et est une extension algébrique de  $\mathbb{F}_q$  de degré infini.
- Def : On note  $I(n, q)$  l'ensemble des polynômes irréductibles de degré  $n$  sur  $\mathbb{F}_q$ .
- Pro :  $\forall n \geq 1, X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d, q)} P$
- Def : On définit la fonction de Moëbius  $\mu : \mathbb{N}^* \rightarrow \{-1, 0, 1\}$  par :
 
$$\begin{cases} 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = p_1 \dots p_r \text{ avec } p_i \text{ premiers distincts} \end{cases}$$
- Dev : Pour tout  $n \geq 1$ , on a :  $n \cdot |I(n, q)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d$ .  
On a ainsi  $I(n, q) \sim \frac{q^n}{n}$  pour  $n \rightarrow +\infty$ .
- App : Test de Rabin :  $P \in \mathbb{F}_q[X]$  est irréductible sur  $\mathbb{F}_q$  ssi P divise  $X^{q^n} - X$  et si  $P \wedge X^{q^d} - X = 1$  pour tout  $d$  diviseur strict de  $n$ .
- Application des corps de décomposition : Théorème de Hamilton-Cayley : Pour tous  $K, n$ , pour tout  $A \in M_n(K)$ ,  $\chi_A(A) = 0$ .
- Def : Soit  $K$  un corps,  $n \geq 1$  et  $A \in M_n(\mathbb{K})$ . On note  $C(A) := \{M \in M_n(\mathbb{K}) \text{ tq } AM = MA\}$  le commutant de A.
- Dev Dimension du commutant : On a  $C(A) = K[A]$  ssi  $\mu_A = \chi_A$ .

## 3. Clôture algébrique. —

- Def : Un corps  $K$  est dit algébriquement clos ssi tout polynôme de degré  $\geq 1$  est scindé sur  $K$ , ssi tout polynôme de degré  $\geq 1$  admet une racine sur  $K$ , ssi les seuls

irréductibles de  $K[X]$  sont les polynômes de degré 1, ssi toute extension algébrique sur  $K$  est triviale.

- Ex :  $\mathbb{Q}, \mathbb{R}, \mathbb{F}_q$  ne sont pas algébriquement clos.
- Théorème de d'Alembert-Gauss :  $\mathbb{C}$  est algébriquement clos.
- Cor : Les polynômes irréductibles de  $\mathbb{R}[X]$  sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine réelle.
- App : Toute matrice de  $M_n(\mathbb{C})$  est trigonalisable.
- Rem :  $\mathbb{Q}$  et  $\mathbb{F}_q$  admettent des polynômes irréductibles de degré aussi grand que l'on veut.
- Ex :  $\cup_n \mathbb{F}_{p^n}$  est algébriquement clos.
- Def : Une extension L de  $K$  qui est algébriquement close est appelée clôture algébrique de  $K$ .
- Thm : Tout corps  $K$  admet une clôture algébrique. De plus, les clôtures algébriques de  $K$  sont isomorphes entre elles par des isomorphismes de  $K$ -algèbres.
- Ex : La clôture algébrique de  $\mathbb{R}$  est  $\mathbb{C}$ .
- Ex : La clôture algébrique de  $\mathbb{Q}$  est  $\overline{\mathbb{Q}}$ , l'ensemble des nombre complexes algébriques sur  $\mathbb{Q}$ .
- Ex : La clôture algébrique de  $\mathbb{F}_p$  est  $\cup_n \mathbb{F}_{p^n}$ .

## 3. Extensions normales, séparables, primitives, galosiennes. —

### 1. Extensions normales, séparables. —

- Def : Pour  $M/K$  extension de corps et  $L_1, L_2$  sous-corps de M contenant K, un  $K$ -morphisme de corps entre  $L_1$  et  $L_2$  est un morphisme d'anneaux  $L_1 \rightarrow L_2$  qui laisse K stable.
- Def : Une extension algébrique de corps  $L/K$  est dite séparable ssi pour tout  $x \in L$ ,  $Irr(x, K)$  est à racines simples dans son corps de décomposition.
- Ex :  $\mathbb{C}/\mathbb{R}$  est séparable,  $\mathbb{F}_q/\mathbb{F}_p$  est séparable.
- Thm : Si  $car(K) = 0$ , toute extension algébrique  $L/K$  est séparable.  
Si  $car(K) = p$ , une extension algébrique  $L/K$  est séparable ssi le morphisme de Frobenius  $x \mapsto x^p$  est surjectif sur  $K$ .
- Thm : Soit  $\overline{L}$  une extension algébrique de L. Une extension algébrique  $L/K$  est séparable ssi pour tout  $x \in L$ , il y a exactement  $[K(x) : L] = deg(Irr(x, K))$   $K$ -morphisms de corps distincts de  $K(x)$  dans  $\overline{L}$ .
- Ainsi, les extensions algébriques sur  $\mathbb{R}, \mathbb{Q}, \mathbb{F}_q$  sont toujours séparables.
- Contre-ex : Pour  $K = \mathbb{F}_p(X)$ , et L le corps de décomposition de  $T - X^p$  sur K,  $L/K$  est algébrique de degré  $p$  mais pas séparable.
- Def : Une extension algébrique de corps  $L/K$  est dite normale ssi tout  $P \in K[X]$  irréductible qui admet une racine dans L est scindé sur L.
- Thm : Une extension algébrique de corps  $L/K$  est normale ssi elle L est le corps de décomposition d'une famille de polynômes de  $K[X]$  ssi tout  $K$ -morphisme de corps de L vers une clôture algébrique  $\overline{L}$  laisse L sable.

- $\mathbb{C}/\mathbb{R}$  est normale.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  n'est pas normale.  $\mathbb{F}_q/\mathbb{F}_p$  est normale.  $\overline{K}/K$  est normale.

## 2. Extensions primitives. —

- Def : Une extension algébrique de corps  $L/K$  est primitive ssi il existe  $x \in L$  tq  $L = K(x)$ .
- Rem : Une extension primitive est forcément finie.
- Ex :  $\mathbb{C}/\mathbb{R}$  est primitive.  $\mathbb{Q}(\sqrt[3]{2} + \sqrt[5]{7})/\mathbb{Q}$  est primitive.  $\mathbb{F}_q/\mathbb{F}_p$  est primitive.  $\overline{\mathbb{Q}}/\mathbb{Q}$  et  $\overline{\mathbb{F}_q}/\mathbb{F}_q$  ne sont pas primitives car non finies.
- Théorème de l'élément primitif : Toute extension algébrique finie séparable est primitive.
- Contre-ex : Pour  $K = \mathbb{F}_p(X, Y)$  et  $L$  le corps de décomposition de  $(T - X^p)(T - Y^p)$  sur  $K$ ,  $L/K$  n'est pas primitive car pour tout  $x \in L - K$ ,  $\deg(\text{Irr}(x, K)) = p < p^2 = [L : K]$ .

## 3. Extensions galoisiennes. —

- Def : Pour  $L/K$  algébrique, on définit  $\text{Gal}(L : K)$  le groupe des  $K$ -morphisms de corps  $L \rightarrow L$  (ce sont automatiquement des automorphismes), appelé groupe de Galois de  $L/K$ .
- Ex :  $\text{Gal}(\mathbb{C} : \mathbb{R}) = \{id, z \mapsto \bar{z}\}$ .  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{id\}$ .
- Pro : Pour tout polynôme  $P \in K[X]$  qui admet des racines dans  $L$ , les éléments de  $\text{Gal}(L : K)$  vont permuter les racines de  $P$  dans  $L$ .  
Ainsi, pour  $L = K(x)$ , un élément de  $\text{Gal}(L : K)$  est défini par l'image de  $x$  parmi les racines de  $\text{Irr}(x, K)$  dans  $L$ .  
De fait,  $\text{Gal}(L : K)$  est isomorphe à un sous-groupe de  $\Sigma_{\deg(\text{Irr}(x:K))}$ .
- Pro : Pour  $L/K$  algébrique finie,  $\text{Card}(\text{Gal}(L : K)) \leq [L : K]$ .
- Pro : Le groupe de Galois d'une extension algébrique est transitif : Pour tout  $x \in L$ , et pour toute racine  $\lambda$  de  $\text{Irr}(x, K)$  dans  $L$ , il existe  $\phi \in \text{Gal}(L : K)$  tel que  $\phi(x) = \lambda$ .
- Rem :
- Def : Une extension de corps  $L/K$  est galoisienne ssi elle est normale et séparable.
- Rem : Une extension finie séparable étant toujours primitive, si  $L/K$  est finie alors  $\text{Gal}(L : K)$  est isomorphe à un sous-groupe de  $\Sigma_{[L:K]}$ .
- Thm :  $L/K$  est galoisienne et finie ssi  $\text{Card}(\text{Gal}(L : K)) = [L : K]$ .
- Ex :  $\mathbb{C}/\mathbb{R}$  est galoisienne.  $\mathbb{F}_q/\mathbb{F}_p$  est galoisienne.  $\mathbb{Q}(\exp^{i\pi/n})/\mathbb{Q}$  est galoisienne.  $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$  n'est pas galoisienne.
- Pro : Soit  $L/K$  galoisienne. Pour  $x \in L$  tel que  $L$  est le corps de décomposition de  $\text{Irr}(x, K)$  sur  $K$ ,  $\text{Gal}(L : K)$  est isomorphe à un sous-groupe de  $\Sigma_{\deg(\text{Irr}(x:K))}$ .
- Ex :  $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$  est une extension galoisienne de degré 6. Comme  $\mathbb{Q}(\sqrt[3]{2}, j)$  est le corps de décomposition de  $X^3 - 2$  sur  $\mathbb{Q}$ ,  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q})$  est donc isomorphe à un sous-groupe de  $\Sigma_3$ .  
Comme l'extension est de degré 6, le groupe de Galois de l'extension est donc isomorphe à  $\Sigma_3$ .

- Pro : Soit  $M/K$  galoisienne et  $L$  sous-corps de  $M$  contenant  $K$ . Alors  $M/L$  est galoisienne.
- Thm : Correspondance de Galois : Soit  $M/K$  une extension galoisienne finie. L'application qui à  $H$  sous-groupe de  $\text{Gal}(M : K)$  envoie  $M^H$  l'ensemble des points fixes de  $M$  par l'action de  $H$  est une bijection de l'ensemble des sous-groupes de  $\text{Gal}(M : K)$  vers l'ensemble des sous-corps de  $M$  contenant  $K$ , qui est décroissante pour l'inclusion.  
Son application inverse est l'application qui à  $L$  sous-corps de  $M$  contenant  $K$  envoie  $\text{Gal}(M : L)$ . De plus, la restriction de cette application aux sous-groupes distingués de  $\text{Gal}(M : L)$  est d'image l'ensemble des sous-corps  $L$  de  $M$  contenant  $K$  tels que  $L/K$  est galoisienne.
- Exemple de Groupe de Galois d'un corps de décomposition d'un polynôme sur  $\mathbb{Q}$ . (genre  $X^4 - 3$ )

## Références

- Perrin : Eléments algébriques. Irréductibilité via les extensions, exemples, contre-ex, corps finis. Ex de clôtures algébriques.
- Gozard : Eléments algébriques/transcendants, exemples. Corps de rupture, corps de décomposition, clôtures algébriques, exemples.
- Gras : Extensions normales, séparables, primitives, galoisiennes.
- FGN (Algèbre 1) : Polynômes irréductibles de degré  $n$  sur  $\mathbb{F}_q$ .(Dev)
- FGN (Algèbre 2) : Dimension du commutant.(Dev)

---

January 23, 2018

Vidal Agniel, École normale supérieure de Rennes