125

Extensions de corps. Exemples et applications

K désignera ici un corps.

I - Généralités.

Déf 1 : Une extension du corps K est la donnée d'un couple (L, j), avec L un corps, et $j : K \to L$, un morphisme. On note $L | K$.

Rem 2 : Si L est une extension de K, on dit que K est un sous-corps de L.

Ex 3 : • $\mathbb{C}$ est une extension de $\mathbb{R}$.
• $\mathbb{R}$ est une extension de $\mathbb{Q}$.

Prop 4 : Si L est une extension de K, alors L est un K-espace vectoriel.

Déf 5 : On appelle tour d'extensions une suite finie de corps croissante pour l'inclusion : si $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r$ est une tour d'extensions, alors $\forall (i,j) \in [\![1, r]\!]^2$, $i \leq j$ implique $K_j | K_i$.

Ex 6 : $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ est une tour d'extensions.

Déf 7 : Pour L une extension de K, on appelle degré de l'extension $L|K$ la dimension de L vu comme K-espace vectoriel. On note ce nombre $[L:K]$.

Rem 8 : • $[L:K] = 1 \iff L \cong K$.
• Si $[L:K] = 2$, l'extension $L|K$ est dite quadratique.
• $[\mathbb{C}:\mathbb{R}] = 2$, $\mathbb{C}|\mathbb{R}$ est quadratique.
• $[\mathbb{R}:\mathbb{Q}] = +\infty$, le degré d'une extension peut être infini.

Th 9 (base télescopique) : Soit L une extension de K, et E une extension de L. On pose $(e_i)_{i\in I}$ une base du L-espace vectoriel E, et $(f_j)_{j\in J}$ une base du K-espace vectoriel L. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de E vu comme K-espace vectoriel.

Cor 10 : Soit $K \subseteq L \subseteq E$ une tour d'extensions. Alors $[E:K]$ est fini ssi $[E:L]$ et $[L:K]$ sont finis. En particulier, $[E:K] = [E:L] \times [L:K]$.

Déf 11 : Soit $L|K$. On appelle corps intermédiaire de l'extension $L|K$ tout sous-corps de L contenant K.

Prop 12 : Soit $L|K$, P une partie de L. L'ensemble des corps intermédiaires de $L|K$ contenant P admet un plus petit élément, au sens de l'inclusion. Cet élément est noté $K(P)$ et est appelé sous-extension de $L|K$ engendrée par P.

Rem 13 : • Si $P = \{\alpha_1, \dots, \alpha_n\}$ est finie, l'extension $K(P)|K$ est dite de type finie, et on note $K(P) := K(\alpha_1, \dots, \alpha_n)$.
• Si $P = \{\alpha\}$, $K(P) := K(\alpha)$, et l'extension $K(\alpha)|K$ est dite monogène.

Déf 14 : Soit $L|K$ une extension. Un élément α de L est dit algébrique s'il existe P dans $K[X]$ tel que $P(\alpha) = 0$. Il est dit transcendant sinon.

Déf 15 : Un polynôme P de $K[X]$ est dit séparable s'il n'admet que des racines simples dans toute extension L de K.

Déf 16 : Soit $L|K$. On dit que $\alpha \in L$ est séparable s'il est algébrique sur K et si son polynôme minimal sur K est séparable.

Def 17 : une extension $L|K$ est dite séparable si tout élément de L est séparable sur K.

II - Corps de rupture, corps de décomposition

Def 18 : Soit K un corps, $P \in K[X]$ irréductible. Une extension $L|K$ est un corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$, avec $P(\alpha) = 0$.

Th 19 : Soit $P \in K[X]$, irréductible. Alors il existe, unique à isomorphisme près, un corps de rupture de P sur K.

Ex 20 : $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$. On peut montrer qu'il est isomorphe à $\mathbb{R}[X]/_{(X^2+1)}$.

Def 21 : Soit $P \in K[X]$, non constant. L'extension $L|K$ est un corps de décomposition de P sur K si les conditions suivantes sont vérifiés :
- dans $L[X]$, P est produit de polynômes de degré 1 ;
- les racines de P engendrent L.

Rem 22 : On peut montrer qu'un polynôme est séparable ssi il est scindé à racines simples sur son corps de décomposition.

Th 23 : Soit $P \in K[X]$, un polynôme non constant. Alors il existe un corps de décomposition de P sur K, unique à isomorphisme près.

III - Corps finis

Def 24 : On dit qu'un corps est fini s'il possède un nombre fini d'éléments. On note $\mathbb{F}_q$ un corps à q éléments.

Th 25 : $\mathbb{F}_q$ existe ssi $q = p^n$, avec p un nombre premier et n un entier naturel non nul. De plus, ce corps est unique à isomorphisme près.

Rem 26 : $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Ex 27 :
- Si $q = p$ premier, $\mathbb{F}_p \simeq \mathbb{Z}/_{p\mathbb{Z}}$.
- X^2+X+1 étant irréductible $\mathbb{F}_2$, $\mathbb{F}_2[X]/_{(X^2+X+1)}$ est un corps, de plus fini, à 4 éléments. Il est donc isomorphe à $\mathbb{F}_4$.

Th 28 : Pour q une puissance d'un nombre premier, $\mathbb{F}_q^*$ ($= \mathbb{F}_q \setminus \{0\}$) est cyclique.

Cor 29 : Soit $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. Alors le corps $\mathbb{F}_{p^m}$ s'identifie à une extension du corps $\mathbb{F}_{p^n}$ ssi $n | m$.

DEV

Cor 30 (théorème de l'élément primitif) : Soit q une puissance d'un nombre premier, $m \in \mathbb{N}^*$. On pose $K = \mathbb{F}_q$ et $L = \mathbb{F}_{q^m}$. Alors L est une extension monogène de K.

Rem 31 : Plus généralement, toute extension séparable de type fini est monogène.

IV - Points et nombres constructibles

Soit X une partie de P, le plan affine euclidien orienté, muni du repère orthonormé direct $R = (O, \vec{i}, \vec{j})$, telle que $\#X \geq 2$. On considérera dans cette partie :

(1) • les droites affines (AB), avec $(A,B) \in X^2$, $A \neq B$, les droites passant par deux points de X ;

(2) • les cercles $\mathcal{C}(A, \|AB\|)$, $(A,B) \in X^2$, $A \neq B$, cercles centrés en un point de X passant par un autre point de X.

Def 32 : On dit que $M \in P$ est constructible en un pas à partir de X si M est l'intersection :
- de deux droites affines de type (1).
- ou • de deux cercles de type (2)
- ou • d'une droite de type (1) et d'un cercle de type (2).

Rem 33 : Chaque point de X est constructible à partir de X, en un pas.

Def 34 : Soit B_0 une partie de X, $\#B_0 \geq 2$. On définit, par récurrence sur $i \in \mathbb{N}$, B_i, l'ensemble des points constructibles en un pas à partir de B_{i-1}.

Rem 35 : $(B_n)_{n \in \mathbb{N}}$ est une suite croissante au sens de l'inclusion.

Prop 36 : Pour $M \in P$, $M \in \bigcup_{n \in \mathbb{N}} B_n$ ssi il existe une suite finie $M_1, \dots, M_n$ de points de P telle que, avec $A_0 = B_0$, et $A_i = A_{i-1} \cup \{M_i\}$, $\forall i \in [\![1;n]\!]$, on ait $M_n = M$ et, $\forall i \in [\![1;n]\!]$, M_i constructible en un pas à partir de A_{i-1}.

Rem 37 : Dans la suite, $B_0 = \{(0,0), (1,0)\}$.

Prop 38 :
- Si M est constructible son symétrique par rapport à l'origine l'est ;
- Si A et B sont constructibles, le milieu du segment $[AB]$ l'est ;
- $(0, 1)$ est constructible.

Prop 38 : Pour $x \in \mathbb{R}$, les conditions suivantes sont équivalents :
- le point $(x, 0)$ est constructible ;
- le point $(0, x)$ est constructible.

Dans ce cas, on dit que x est un nombre constructible.

Not 39 : On note $\mathbb{E}$ l'ensemble des nombres réels constructibles.

Prop 40 : $\mathbb{Q} \subset \mathbb{E}$.

Prop 41 : $M = (x, y)$ est constructible ssi x et y sont constructibles.

Th 42 : $\mathbb{E}$ est un sous-corps de $\mathbb{R}$, stable par la racine carrée.

DEV 2

Th 43 (Wantzel) : Soit $t \in \mathbb{R}$. t est constructible ssi il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ telle que :
- $L_0 = \mathbb{Q}$
- $\forall i \in [\![0, p-1]\!]$, L_{i+1} est une extension quadratique de L_i
- $t \in L_p$.

App 44 : $\sqrt[3]{2}$ n'est pas constructible

Rem 45 : Ce théorème a un équivalent sur $\mathbb{C}$.

Théorème de Wantzel

Enoncé dans $\mathbb{R}$

Soit $t \in \mathbb{R}$. t est constructible si et seulement si il existe une suite finie $(L_0, \dots L_p)$ de sous-corps de $\mathbb{R}$ vérifiant : $\begin{cases} L_0 = \mathbb{Q} \\ [L_{i+1} : L_i] = 2 \quad \forall i \in [\![0, p-1]\!] \\ t \in L_p \end{cases}$

Preuve

On notera P le plan euclidien $\mathbb{R}^2$ muni de son repère orthonormé (O, I, J)

- Supposons $t \in \mathbb{R}$ constructible, càd $M = (t, 0)$ constructible.
Autrement dit, il existe une suite finie $(M_1, \dots M_n)$ de points de P tels que avec $\begin{cases} A_0 = \{O, I\} \\ A_i = A_{i-1} \cup \{M_i\}, \ i \in [\![1, n]\!] \end{cases}$ on ait $M_n = M$

et $\forall i \in [\![1, n]\!]$ M_i est constructible en un pas à partir de A_{i-1}.
Notons pour chaque $i \in [\![1, n]\!]$, $M_i = (x_i, y_i)$.
Posons $K_0 = \mathbb{Q}$ et $\forall i \in [\![1, n]\!]$, $K_i = K_{i-1}(x_i, y_i)$
On remarque que, ainsi construit $K_i = \mathbb{Q}(x_1, y_1, \dots, x_i, y_i)$; que $(K_0, \dots K_n)$ est une suite croissante de sous-corps de $\mathbb{R}$ (au sens de l'inclusion) et que $t = x_n \in K_n$.
Soit $i \in [\![1, n]\!]$, M_i est constructible en un pas à partir de A_{i-1}, alors :
  - ou bien $x_i, y_i \in K_{i-1}$ et alors $K_i = K_{i-1}$
  - ou bien il existe une extension G quadratique de K_{i-1} telle que $x_i, y_i \in G$. Alors $K_i = G$ et $[K_i : K_{i-1}] = 2$.

La suite $(K_0, \dots K_n)$ de sous corps de $\mathbb{R}$ est croissante et vérifie :
$K_0 = \mathbb{Q}$; $\forall i \in [\![1, n]\!]$ $[K_i : K_{i-1}] = 2$ ou 1 ; $t = x_n \in K_n$.
Enfin, on extrait une sous suite $(L_0, \dots, L_p)$ strictement croissante, en ne conservant de la suite initiale $(K_0, \dots K_n)$ que les corps extension quadratique du précédent. (On conserve $L_0 = K_0$ et $L_p = K_n$).
On a ainsi obtenu la tour d'extension quadratique réelle recherchée.

- Réciproquement, supposons l'existence d'une telle tour d'extension quadratique $(L_0, \dots L_p)$. On note $\mathbb{E}$ l'ensemble des nombres réels constructibles.
Montrons par récurrence sur $j \in [\![0, p]\!]$ la propriété "$L_j \subseteq \mathbb{E}$".
Initialisation. $L_0 = \mathbb{Q} \subseteq \mathbb{E}$
Hérédité Supposons $L_j \subseteq \mathbb{E}$.
Soit $x \in L_{j+1}$, comme $[L_{j+1} : L_j] = 2$, il existe $(a, b, c) \in L_j^3 \setminus \{(0,0,0)\}$ tel que $ax^2 + bx + c = 0$.

- si $a=0$, $x = -\frac{c}{b} \in L_j$ donc $x \in \mathbb{E}$
- si $a \neq 0$, $x \in \left\{ \frac{1}{2a} \left(-b \pm \sqrt{b^2-4ac}\right) \right\}$ donc $x \in \mathbb{E}$ car $\mathbb{E}$ est un sous corps de $\mathbb{R}$ stable par racine carrée.

Ainsi $L_{j+1} \subseteq \mathbb{E}$

Par conséquent $L_p \subseteq \mathbb{E}$ et t est constructible. $\square$

Enoncé dans $\mathbb{C}$

Soit $z \in \mathbb{C}$, z est constructible si et seulement si il existe une tour d'extension quadratique complexe $(L_0, \dots, L_q)$ de $\mathbb{Q}$ telle que $z \in L_q$.

Preuve

- Soit $z \in \mathbb{C}$ constructible, càd $M = (\mathrm{Re}(z), \mathrm{Im}(z)) \in \mathbb{R}^2$ constructible.
Par le théorème de Wantzel dans $\mathbb{R}$, on construit la suite $(L_0, \dots, L_p)$ telle que
$$\begin{cases} L_0 = \mathbb{Q} \\ \forall i \in [\![0, p-1]\!] \ [L_{i+1} : L_i] = 2 \\ (\mathrm{Re}(z), \mathrm{Im}(z)) \in L_p^2 \end{cases}$$
Alors $z \in L_p(i)$. Or le polynôme minimal de i dans L_p est X^2+1.
Ainsi $[L_p(i) : L_p] = 2$.
En posant $q = p+1$ et $L_q = L_p(i)$ on obtient alors bien la tour d'extension quadratique complexe recherchée.
- Réciproquement, on procède comme pour la preuve de Wantzel dans $\mathbb{R}$. Le même raisonnement est possible car l'ensemble des complexes constructibles $\mathbb{E}(i)$ est un sous corps de $\mathbb{C}$ stable par racine carrée (càd $\forall x \in \mathbb{E}(i)$, les racines de $X^2 - x$ sont dans $\mathbb{E}(i)$) $\square$

Reference Théorie de Galois, Gozard.

Théorème de l'élément primitif

Enoncé

Toute extension séparable de type fini est monogène.
ie si L est une extension de K tq $L = K(a_1, \dots a_n)$ avec les a_i séparables sur K, alors il existe $a \in L$ tq $L = K(a)$.

Preuve

- Pour K un corps fini de caractéristique p.

On note $[L:K] = m \in \mathbb{N}^*$.
L est un K-espace vectoriel de dimension m, et est alors isomorphe en tant que K-espace vectoriel à K^m. Ainsi $\text{card}(L) = (\text{card}(K))^m$ et L est un corps fini. Alors le groupe multiplicatif $L^\times$ est cyclique.
Soit ξ un générateur de $L^\times$.
La caractéristique p de K est aussi celle de L, alors $L = \mathbb{F}_p(\xi)$.
On a la tour d'extension $\mathbb{F}_p \subset K \subseteq L$.
or $\mathbb{F}_p \subset K \Rightarrow \mathbb{F}_p(\xi) \subset K(\xi)$ Alors $L \subset K(\xi)$
On a par ailleurs l'inclusion $K(\xi) \subset L$. En conclusion $L = K(\xi)$.

- Pour K un corps infini

On procède par récurrence sur le nombre de générateurs $n \in \mathbb{N}^*$:
$S(n)$: "Si $L = K(a_1, \dots a_n)$ est une extension algébrique de K avec au moins $(n-1)$ des a_i séparables alors $L|K$ est monogène"

initialisation

$S(1)$ est vraie.
$S(2)$: Soit $K(a,b) = L$ une extension algébrique, avec b séparable.
Soit P le polynôme minimal de a sur K et $p = \deg(P)$
et Q le polynôme minimal de b sur K, $q = \deg(Q)$.
Soit M le corps de décomposition PQ.
On note $(a_1, \dots a_p)$ les racines de P dans M, $a_1 = a$.
et $(b_1, \dots b_q)$ les racines de Q dans M, $b_1 = b$.
Comme b est séparable, les b_i sont distincts deux à deux.
On cherche $c \in K$ pour que $\gamma = a + cb \neq a_i + cb_j$ $\forall i \in [\![1,p]\!]$ $\forall j \in [\![1,q]\!]$
(sauf évidemment $i = 1$ et $j = 1$)
Un tel $c \in K$ existe car ceux qui ne conviennent pas sont de la forme $c = \dfrac{a - a_i}{b_j - b}$ et sont en nombre fini alors que K est infini.

Reste à montrer que $\gamma = a + cb$ (c choisi correctement) est un élément primitif de L.

- Tout d'abord, comme $\gamma = a + cb$ $K(\gamma) \subset K(a,b) = L$
- Ensuite, $Q(b) = 0$, $Q \in K[X]$ et $K \subset K(\gamma)$ alors $Q \in K(\gamma)[X]$

mais b est aussi racine de $R(X) = P(\gamma - cX) \in K(\gamma)[X]$.

Soit $S = \mathrm{pgcd}(Q,R)$ sur $K(\gamma)[X]$.

$*$ Si $\deg S = 1$ alors $b \in K(\gamma)$.

$*$ Si $\deg S > 1$. $S \mid Q(X) = \prod_{j=1}^{q} (X - b_j)$

Alors il existe $j \geq 2$ tel que b_j est racine de S donc aussi racine de R.

Alors il existe $i \in [\![1,p]\!]$, $a_i = \gamma - cb_j$

(car les racines de P sont les a_i)

Or $a_i = \gamma - cb_j \Leftrightarrow \gamma = a_i + cb_j$ ce qui est impossible par choix de c.

Par conséquent $\deg S \leq 1$ et $b \in K(\gamma)$.

Ces deux points montrent que $b \in K(\gamma)$

- Enfin $a = \gamma - cb \in K(\gamma)$ donc $K(a,b) \subset K(\gamma)$.

Par double inclusion $K(a,b) = K(\gamma)$ et L est monogène.

<u>Hérédité</u>

On suppose $S(n)$ vraie pour $n \geq 2$.

Soit $L = K(a_1, \dots a_n, a_{n+1})$ algébrique sur K.

Quitte à permuter supposons $a_2, \dots a_{n+1}$ séparables.

L'extension $L_1 = K(a_1, \dots a_n)$ est monogène par hypothèse de récurrence. Soit $a \in L_1$ tel que $L_1 = K(a)$.

On peut écrire $L = L_1(a_{n+1}) = K(a, a_{n+1})$. L'élément a_{n+1} est séparable alors d'après $S(2)$, il existe $\gamma \in L$ tel que $L = K(\gamma)$ donc L est bien monogène.

$\square$

<u>Références</u> : Théorie de Galois, Gozard.

Basic Algebra I, Jacobson