Leçon 125 : Extensions de corps. Exemples et application.

RM
2022-2023

Les corps introduit sont supposés commutatif sauf mention particulière.

1 Extensions de corps

1.1 Définition

Définition 1 : Soient $\mathbb{K}, \mathbb{L}$ des corps. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$, si il existe un morphisme de corps non nul (nécessairement injectif) $i : \mathbb{K} \to \mathbb{L}$. On note $\mathbb{L}/\mathbb{K}$ pour dire que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$.

Remarque 2 : • Comme i est injectif, on a $i(\mathbb{K})$ est isomorphe à $\mathbb{K}$ et comme $i(\mathbb{K})$ est un sous-corps de $\mathbb{L}$, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ à isomorphisme près.

• Réciproquement, si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors $\mathbb{L}$ est une extension de corps de $\mathbb{K}$ en considérant l'injection canonique.

Exemple 3 : $\mathbb{C}$ est une extension de $\mathbb{R}$ qui est lui même une extension de $\mathbb{Q}$. $\mathbb{R}[X]$ est une extension de $\mathbb{R}$.

Proposition 4 : Si $\mathbb{L}/\mathbb{K}$ une extension de corps, alors L est un $\mathbb{K}$-espace vectoriel.

Définition 5 : Si $dim_{\mathbb{K}}\mathbb{L}$ est finie, on pose $[\mathbb{L} : \mathbb{K}] = dim_{\mathbb{K}}\mathbb{L}$ et l'entier $[\mathbb{L} : \mathbb{K}]$ s'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$, ou degré de l'extension. On parle alors d'extension finie.

Exemple 6 : • Si $\mathbb{K}$ et $\mathbb{L}$ sont des corps finis, on a $|\mathbb{L}| = |\mathbb{K}|^n$ avec $n = [\mathbb{L} : \mathbb{K}]$.

• Comme $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2, on a que le degré de l'extension $\mathbb{C}/\mathbb{R}$ est 2.

Théorème (de la base télescopique) 7 : Soient deux extension de corps $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

Corollaire 8 : Si les extensions sont finies, alors on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 9 : 1) Soit $\mathbb{L}/\mathbb{K}$ une extension et A une partie de $\mathbb{L}$. On dit que A engendre $\mathbb{L}$ sur $\mathbb{K}$ et on écrit alors $\mathbb{L} = \mathbb{K}(A)$ si $\mathbb{L}$ est le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\mathbb{A}$. Si A est fini, $A = \{\alpha_1, ..., \alpha_n\}$, on note $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_n)$.

2) L'extension $\mathbb{L}/\mathbb{K}$ est dite monogène s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

Remarque 10 : On a pas $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ mais $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$, car $\mathbb{K}[\alpha]$ est le sous-anneau de $\mathbb{L}$ engendré par $\mathbb{K}$ et α.

1.2 Extensions et éléments algébriques

Définition 11 : Soit $\mathbb{L}/\mathbb{K}$ une extension et soit $\alpha \in \mathbb{L}$. Soit $\varphi : \mathbb{K}[T] \to \mathbb{L}$ le morphisme défini par $\varphi_{|\mathbb{K}} = id_{\mathbb{K}}$ et $\varphi(T) = \alpha$.

1) Si φ est injectif, alors on dit que α est transcendant sur $\mathbb{K}$.

2) Sinon, on dit que α est algébrique sur $\mathbb{K}$. Cela signifie qu'il existe un polynôme non nul $P \in \mathbb{K}[T]$ tel que $P(\alpha) = 0$.

Exemple 12 : i et $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Proposition 13 : Si α est algébrique sur $\mathbb{K}$, alors $Ker\varphi$ est un idéal principal non nul. Donc il existe P unitaire telle que $Ker\varphi = (P)$. On appelle P le polynôme minimal de α sur $\mathbb{K}$.

Exemple 14 : Les polynômes minimaux de $\sqrt{2}$ et i sont $X^2 - 2$ et $X^2 + 1$.

Proposition 15 : Si α est transcendant, on a $\mathbb{K}[\alpha] \cong \mathbb{K}[T]$ et $\mathbb{K}(\alpha) \cong \mathbb{K}(T)$.

Théorème 16 : Soit $\mathbb{K}/\mathbb{L}$ une extension et $\alpha \in \mathbb{L}$. Les propriétés suivantes sont équivalentes : *i*) α est algébrique sur $\mathbb{K}$.

ii) on a $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

iii) on a $dim_{\mathbb{K}}\mathbb{K}[\alpha] < +\infty$. Plus précisément, on a $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = [\mathbb{K}[\alpha] : \mathbb{K}] = deg(P)$ ou P est le polynôme minimal de α.

Exemple 17 : Comme le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$ de degré 2, on a que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Définition 18 : Une extension $\mathbb{L}/\mathbb{K}$ est dite algébrique si pour tout $\alpha \in L$, α est algébrique sur $\mathbb{K}$.

Exemple 19 : $\mathbb{C}$ est donc une extension algébrique de $\mathbb{R}$ car tout élément z de $\mathbb{C}$, il existe un polynôme $P \in \mathbb{R}[X]$ tel que $P(z) = 0$.

Théorème 20 : Soit $\mathbb{L}/\mathbb{K}$ une extension et posons $M = \{x \in \mathbb{L} | x \text{ est algébrique sur } \mathbb{K}\}$. Alors M est un sous-corps de $\mathbb{L}$.

Remarque 21 : On déduit du théorème 16 que toute extension finie est algébrique, mais la réciproque est fausse.
Par exemple, $A = \{\alpha \in \mathbb{C} | \alpha \text{ algébrique sur } \mathbb{Q}\}$ est une extension algébrique de $\mathbb{Q}$,

mais pas finie car on a que $\sqrt[n]{2}$ est dans A pour n aussi grand que l'on veut, et donc le polynôme minimal $X^n - 2$ est de degré aussi grand que l'on veut.

2 Extension de corps et polynômes

2.1 Corps de décomposition et corps de rupture

Théorème 22 : Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. On a que $\mathbb{K}[X]/(P)$ est un corps si et seulement si le polynôme P est irréductible.

Définition 23 : Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}/\mathbb{K}$ est appelée un corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L}$ est une extension monogène $L = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$.

Théorème 24 : Soit $P \in \mathbb{K}[X]$, irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.

Remarque 25 : Il suffit de considérer $\mathbb{K}[X]/(P)$ qui fonctionne bien d'après le théorème 22.

Remarque 26 : P n'est pas forcément factorisé sur un corps de rupture $\mathbb{L}$. Par exemple, si $P = x^3 - 2 \in \mathbb{Q}[X]$, on a que $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$ qui ne contient pas $j\sqrt[3]{2}$.

Exemple 27 : $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$, $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3 - 2)$ est un corps de rupture de $X^3 - 2$.

Théorème 28 : Soit $P \in \mathbb{K}[X]$ de degré n. Alors, P est irréductible sur $\mathbb{K}$ si et seulement si P n'a pas de racines dans les extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie $[\mathbb{L} : \mathbb{K}] \leq n/2$.

Exemple 29 : Comme $X^4 + X + 1$ est n'a pas de racine dans $\mathbb{F}_2$ et $\mathbb{F}_4$, alors il est irréductible dans $\mathbb{F}_2$.

Théorème 30 : Soit $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n et soit $\mathbb{L}$ une extension de degré m avec $m \wedge n = 1$. Alors P est encore irréductible sur $\mathbb{K}$.

Exemple 31 : Comme $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$, alors il est aussi irréductible sur $\mathbb{Q}(i)$.

Définition 32 : Soit $P \in \mathbb{K}[X]$ un polynôme, irréductible ou non, de degré n. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension de $\mathbb{L}$ sur $\mathbb{K}$ qui est telle que :

1) Dans $\mathbb{L}[X]$, P est produit de facteurs de degré 1 (ou encore P a toutes sas racines dans $\mathbb{L}$).

2) Le corps $\mathbb{L}$ est minimal pour cette propriété (ou encore, les racines de P engendrent $\mathbb{L}$).

Théorème 33 : Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Exemple 34 : Pour $\mathbb{K} = \mathbb{Q}$, on a pour $P(X) = X^3 - 2$ que $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, j)$ et $P(X) = X^4 - 2$ que $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[4]{2}, i)$.

2.2 Clôture algébrique

Définition 35 : Un corps $\mathbb{K}$ est dit algébriquement clos s'il vérifie l'une des conditions équivalentes suivantes :

- Tout polynôme $P \in \mathbb{K}[X]$ de degré ≥ 1 admet une racine dans $\mathbb{K}$.
- Tout polynôme $P \in \mathbb{K}[X]$ est produit de polynôme de degré 1.
- Les éléments irréductible de $\mathbb{K}[X]$ sont les $X - a$, $a \in \mathbb{K}$.

Si une extension $\mathbb{L}/\mathbb{K}$ est algébrique, on a $\mathbb{L} = \mathbb{K}$.

Exemple/Théorème 36 : Le corps $\mathbb{C}$ est algébriquement clos.

Définition 37 : Une extension $\overline{\mathbb{K}}$ est appelée clôture algébrique de $\mathbb{K}$ si $\overline{\mathbb{K}}$ est algébriquement clos et $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$.

Exemple 38 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, A est une clôture algébrique de $\mathbb{Q}$.

Théorème (de Steinitz) 39 : Tout corps admet une clôture algébrique, à isomorphisme près.

3 Applications

3.1 Construction des corps finis

Définition 40 : On note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p)$ le cardinal de $\mathcal{U}_n(p)$. On pose le polynôme $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$.

Exemple 41 : Comme tous les polynômes $P(X) = X - \lambda$ sont irréductible pour $\lambda \in \mathbb{F}_p$, on a $I_1(p) = p$.

Remarque 42 : Si $P \in \mathcal{U}_n(p)$, on a donc que $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal p^n. On peut le voir comme une extension de corps de $\mathbb{F}_p$ de degré n avec comme base

$(\overline{X}^k)_{0\leq k\leq n-1}$.
De cette manière, on peut associer l'existence de corps finis à l'existence de polynômes irréductibles.

Lemme 43 : Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, pour tout diviseur d de n, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

Théorème 44 : Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteur irréductible, $P_n(X) = X^{p^n} - X = \prod_{d|n} \prod P \in \mathcal{U}_d(p) P$.

Remarque 45 : On peut alors compter le nombre de polynôme irréductible dans $\mathbb{F}_p[X]$. Par exemple, le nombre de polynômes irréductible de degré 2 dans $\mathbb{F}_2[X]$ est de 1, et c'est $X^2 + X + 1$.

Développement 46 : Pour tout entier naturel non nul n, on a $nI_n(p) = \sum_{d|n} \mu(d) p^{n/d}$. **Dev 1**

Corollaire 47 : Il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$.

Théorème 48 : A un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est le corps $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_n(p)$.

Remarque 49 : L'avantage est ici que en plus de l'existence des corps finis, on a une construction. On peut avoir l'existence et l'unicité sans méthode constructive, par exemple :

Théorème 50 : Il existe un corps $\mathbb{K}$ à $q = p^n$ élément ou p premier et $n \in \mathbb{N}^*$, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. Il est unique à isomorphisme près.

3.2 Polynôme cyclotomique

Définition 51 : Soit $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} | \zeta^n = 1\}$ l'ensemble des racines n-èmes de l'unité et $K_n = D_{\mathbb{K}}(X^n - 1)$. On pose de plus $\mu_n^*(\mathbb{K}_n) = \{\zeta \in \mathbb{K}_n | \zeta^n = 1 \text{ et } \zeta^d \neq 1 \text{ pour } d < n\}$ l'ensemble des racines primitives n-èmes de l'unité.

Proposition 52 : On a $|\mu_n^*(\mathbb{K}_n)| = \varphi(n)$ et si $\zeta \in \mu_n^*(\mathbb{K}_n)$, alors ζ^m l'est aussi si et seulement si $m \wedge n = 1$.

Définition 53 : On définit le n-ème polynôme cyclotomique $\Phi_{n,\mathbb{K}} \in \mathbb{K}_n[X]$ est donné par la formule :

$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K}_n)} (X - \zeta).$$

Remarque 54 : Sur $\mathbb{Q}$, comme le corps de décomposition de $X^n - 1$ est $\mathbb{C}$, on a les racines n-èmes de l'unité "classiques".

Proposition 55 : On a que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Exemple 56 : On a $\Phi_1(X) = X - 1$, $Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_p(X) = X^{p-1} + ... + X + 1$ pour p premier.

Proposition 57 : On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Développement 58 : $\Phi_n(X)$ est irréductible sur $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$). **Dev 2**

Application 59 : Soit K une extension finie de $\mathbb{Q}$. Il y a alors un nombre fini de racines de l'unité dans $\mathbb{K}$.

Corollaire 60 : Si ζ est une racine primitive n-ème de l'unité dans un corps de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est Φ_n, et donc on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Références :

1. Cours d'algèbre Perrin
2. Algèbre et géométrie Rombaldi