

Algèbre M1 Cours 1

Extension de corps

14 Septembre 2010

Définition

Définition – Extension de corps. Soit k un corps. Une **extension de k** est une k -algèbre (K, i) où K est un corps c'est-à-dire un couple où K est un corps et $i : k \rightarrow K$ un morphisme d'anneaux unitaires.

Exemples $\mathbb{C}$ (ou plutôt $(\mathbb{C}, i)$ avec $i : x \in \mathbb{R} \mapsto x1_{\mathbb{C}} \in \mathbb{C}$) est une extension de corps de $\mathbb{R}$.

$\mathbb{R}(T)$ est une extension de corps de $\mathbb{R}$.

Remarque Le morphisme i est injectif et permet d'identifier k au sous-corps $i(k)$ de K .

On peut munir K d'une structure de k -espace vectoriel. Comment ? La dimension de K sur k est noté $[K : k]$. D'une manière générale, dans ce cours, si E est un k -espace vectoriel, on note

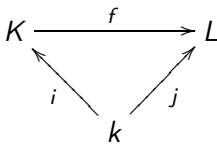
$$[E : k] = \dim_k E$$

Proposition – Base télescopique. Soient K une extension de k et E un K -espace vectoriel. On a alors

$$[E : k] = [E : K][K : k]$$

Remarque Quelle est la dimension de $\mathbb{C}^n$ en tant que $\mathbb{R}$ -espace vectoriel ? En donner une $\mathbb{R}$ -base.

Définition – Morphisme d'extensions. Soient (K, i) et (L, j) deux extensions de k . Un morphisme d'extensions de k de (K, i) dans (L, j) est un morphisme d'anneaux (unitaires) $f : K \rightarrow L$ vérifiant $f \circ i = j$ (ce n'est rien d'autre qu'un morphisme de k -algèbres). Le diagramme suivant est commutatif



Morphisme d'extensions

Exemples Soit (K, i) une extension de k . On vérifie que id_K est un morphisme d'extensions de K dans lui-même.

On considère l'ensemble $\mathbb{C}_1 := \mathbb{R}^2$ muni des lois

$$(x, y) + (x', y') = (x + x', y + y') \text{ et}$$

$$(x, y)(x', y') = (xx' - yy', xy' + yx') \text{ et du morphisme}$$

$i_1 : x \in \mathbb{R} \mapsto (x, 0) \in \mathbb{C}_1$. Vérifier que c'est une extension de corps de $\mathbb{R}$. Vérifier que la structure naturelle d'espace vectoriel sur $\mathbb{R}$ de $\mathbb{C}_1$ coïncide avec la structure d'espace vectoriel donnée par la structure d'extension.

On considère l'extension $\mathbb{C}_2 := \mathbb{R}[X]/(X^2 + 1)$ de $\mathbb{R}$. Quel est le morphisme de $\mathbb{R}$ dans $\mathbb{C}_2$ sous-jacent à l'extension ?

Vérifier que $\mathbb{C}_1$ et $\mathbb{C}_2$ sont deux extensions isomorphes de $\mathbb{R}$.

Remarque Un morphisme d'extensions est nécessairement injectif (pourquoi ?) et est aussi k -linéaire (à vérifier !). En particulier, pour qu'il existe un morphisme d'extensions de K dans L , il faut que $[L : k] \geq [K : k]$. (La condition est-elle suffisante ?)

Sous-extension

Définition — Sous-extension. Soit k un corps et (K, i) une extension de k . Une sous- k -extension de (K, i) est un sous-corps L de K contenant $i(k)$. Le couple (L, i) est alors une extension de k et l'inclusion de L dans K est un morphisme d'extensions.

Remarque Une intersection de sous-extensions est une sous-extension $\implies$ notion de sous-extension engendrée.

Notation Soit k un corps et (K, i) une extension de k . Soit A une partie de K . La sous-extension engendré par A est notée $k(A)$ c'est le plus petit sous-corps contenant k et A .

Exemples Dans $\mathbb{C}$, le sous-corps engendré par i est $\mathbb{Q}(i)$, la sous- $\mathbb{R}$ -algèbre de $\mathbb{C}$ engendré par i est $\mathbb{C} : \mathbb{C} = \mathbb{R}(i)$.

Exemples Ne pas confondre la sous-algèbre de K engendrée par A notée $k[A]$ et la sous-extension de K engendrée par A notée $k(A)$. Dans $\mathbb{R}(T)$, si $A = \{T^2\}$, on distingue $\mathbb{R}[T^2]$ et $\mathbb{R}(T^2)$.

Exercice Soient k un corps, (K, i) une extension de k et A une partie de K . Montrer que

$$k[A] = \{P(a_1, \dots, a_n), n \in \mathbb{N}, a_1, \dots, a_n \in A, P \in k[X_1, \dots, X_n]\}$$

$$k(A) = \{P(a_1, \dots, a_n)/Q(a_1, \dots, a_n), n \in \mathbb{N}, a_1, \dots, a_n \in A, \\ P, Q \in k[X_1, \dots, X_n], Q(a_1, \dots, a_n) \neq 0\}$$

Exercice Comparer

- (i) $\mathbb{R}[i]$ et $\mathbb{R}(i)$
- (ii) $\mathbb{Q}[i]$ et $\mathbb{Q}(i)$
- (iii) $\mathbb{R}[T^2]$ et $\mathbb{R}(T^2)$
- (iv) $\mathbb{Q}[\pi]$ et $\mathbb{Q}(\pi)$
- (v) $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}(\sqrt{2})$
- (vi) $\mathbb{Q}[e]$ et $\mathbb{Q}(e)$

Élément algébrique

Soit (K, i) une extension de k . Pour $x \in K$, on désigne par $\varphi_x : k[X] \rightarrow K$ l'unique morphisme de k -algèbres tel que $\varphi_x(P) = P(x)$. Son image est $k[x] \subset K$.

Proposition Soit (K, i) une extension de k et $x \in K$. Les propriétés suivantes sont équivalentes

- (i) La famille $(x^k, k \in \mathbb{N})$ est liée sur k
- (ii) Il existe $P \in k[X] \setminus \{0\}$ tel que $P(x) = 0$
- (iii) φ_x n'est pas injectif
- (iv) $k[x] = k(x)$
- (v) $[k[x] : k] < +\infty$
- (vi) $[k(x) : k] < +\infty$
- (vii) Il existe une sous-algèbre L de K contenant x telle que $[L : k] < +\infty$
- (viii) Il existe une sous-extension L de K contenant x telle que $[L : k] < +\infty$

Un tel x est dit **algébrique sur k** .

Élément transcendant

Définition – Élément transcendant. Soit (K, i) une extension de k et $x \in K$. Les propriétés suivantes sont équivalentes

- (i) La famille $(x^k, k \in \mathbb{N})$ est libre sur k
- (ii) Si $P(x) = 0$ avec $P \in k[X]$ alors $P = 0$
- (iii) φ_x est injectif
- (iv) $k[X] \stackrel{k\text{-alg.}}{\simeq} k[x]$
- (v) $k(X) \stackrel{k\text{-alg.}}{\simeq} k(x)$
- (vi) $[k[x] : k] = +\infty$
- (vii) $[k(x) : k] = +\infty$

Un tel x est dit **transcendant** sur k .

Élément algébrique : le retour

Proposition — Élément algébrique (suite). Soit (K, i) une extension de k et $x \in K$ un élément algébrique.

Il existe un unique polynôme unitaire $P_x \in k[X]$ tel que $\text{Ker } \varphi_x = (P_x)$. Le polynôme P_x est appelé **polynôme minimal de x** . Le polynôme P_x est irréductible. Les éléments de $\text{Ker } \varphi_x$ sont appelés **polynômes annulateurs de x** .

Inversement, soit $P \in k[X]$ un polynôme irréductible qui est un polynôme annulateur de x . Alors, il existe $\lambda \in k^\times$ tel que $P = \lambda P_x$.

On a $[k[x] : k] = \deg P_x$. Cet entier est noté **$\deg_k(x)$** et appelé **degré de x sur k** .

Proposition — Ensemble des éléments algébriques. Soit (K, i) une extension de k . L'ensemble des éléments de K algébriques sur k est une sous-extension de k appelée **fermeture algébrique de k dans K** .

Extension algébrique

Définition Soit (K, i) une extension de k . On dit que K est une **extension finie de k** si $[K : k] < +\infty$. On dit que K est une **extension algébrique de k** si tout élément de K est algébrique sur k (ou encore si K est la fermeture algébrique de k dans K). Une extension finie est toujours algébrique. La réciproque est fausse.

Exercice Montrer que la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est une extension algébrique de $\mathbb{Q}$ qui n'est pas une extension finie. Déterminer la fermeture algébrique de $\mathbb{R}$ dans $\mathbb{R}(T)$.

Proposition – Transitivité de l'algébricité. Soit (K, i) une extension algébrique de k et (L, j) une extension de K . Un élément $x \in L$ de L est algébrique sur k si et seulement si x est algébrique sur K .

L est une extension algébrique de k si et seulement si L est une extension algébrique de K .

Exercice Soit (K, i) une extension de k et $x_1, \dots, x_n \in K$. Les propositions suivantes sont équivalentes :

- (i) x_{i+1} algébrique sur $k(x_1, \dots, x_i)$ pour tout $i \in \{0, \dots, n-1\}$
- (ii) x_i algébrique sur k pour tout $i \in \{1, \dots, n\}$
- (iii) $[k(x_1, \dots, x_n) : k] < +\infty$
- (iv) $k(x_1, \dots, x_n)$ algébrique sur k .

Exercice – Endomorphisme et automorphisme. Soit k un corps et (K, i) une extension **algébrique** de k et σ un endomorphisme de (K, i) . Montrer que σ est un automorphisme de (K, i) .

Montrer que σ peut ne pas être un automorphisme si K n'est pas algébrique.

Caractéristique

Proposition La caractéristique d'un corps (comme d'ailleurs celle d'un anneau intègre) est zéro ou un nombre premier.

Tout corps de caractéristique nulle est une extension de $\mathbb{Q}$ et ceci de façon unique. Tout corps de caractéristique p (avec p premier) est extension de façon unique de $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Soit k un corps. L'intersection des sous-corps de k est le plus petit sous-corps de k . Il est appelé **sous-corps premier de k** . C'est l'image de l'unique morphisme de $\mathbb{Q}$ ou $\mathbb{F}_p$ dans k .

Exercice Soient K et K' deux corps de caractéristique différentes. Montrer qu'il n'existe pas de morphismes d'anneaux unitaires de K dans K' .

Corps de rupture : problématique

Le polynôme $X^2 + 1 \in \mathbb{R}[X]$ n'a pas de racine dans $\mathbb{R}$. Pour remédier à ce problème, on crée le corps $\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$. Dans $\mathbb{C}$, le polynôme $T^2 + 1$ a une racine qui est la classe de X .

Soit $P \in k[X]$ un polynôme. Peut-on trouver un corps (une extension de k) dans lequel P a une racine ? Dans quelle mesure, une telle extension est-elle unique ?

Si P n'est pas irréductible, on écrit $P = P_1 P_2$ avec P_1, P_2 non inversible. Il suffit de trouver une racine de P_1 ou de P_2 . Ainsi, en continuant la factorisation, il suffit de trouver des racines aux polynômes irréductibles sur k . Cette même factorisation en irréductibles montre que si P n'est pas irréductible, il n'y a aucune chance d'obtenir une quelconque propriété d'unicité du corps dans lequel P a une racine. Par exemple, sur $\mathbb{R}$, avec $P = X(X^2 + 1)$, $\mathbb{R}$ et $\mathbb{C}$ sont deux corps dans lesquels P admet une racine. De même, si on n'impose pas une propriété de minimalité de l'extension cherchée, aucune chance d'avoir unicité : les extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{C}$ contiennent des racines de $P = X^2 - 2$.

Corps de rupture : solution

Définition — Corps de rupture. Soit $P \in k[X]$ un polynôme **irréductible**. Un **corps de rupture sur k** pour P est un triplet (K, i, a) où (K, i) est une extension de k et $a \in K$ vérifiant $P(a) = 0$ et $K = k(a)$.

Proposition — Existence, unicité et propriété universelle.

Soit $P \in k[X]$ un polynôme **irréductible**. Il existe un corps de rupture pour P : $k[X]/P$ en est un.

Par ailleurs, soit (K, i, a) un corps de rupture pour P et considérons (L, j) une extension de k et $b \in L$ vérifiant $P(b) = 0$. Il existe un unique morphisme d'extensions σ de (K, i) dans (L, j) vérifiant $\sigma(a) = b$.

Soit (K, i, a) et (L, j, b) deux corps de rupture pour P . Il existe un unique isomorphisme d'extensions σ de (K, i) dans (L, j) vérifiant $\sigma(a) = b$.

Le degré d'un corps de rupture est donc bien défini et c'est le degré du polynôme. Un corps de rupture de P est isomorphe à $k[X]/P$.

Corps de rupture : exercices

Exercice Soient k un corps et K une extension de k de la forme $K = k(a)$ avec a algébrique sur K .

Montrer que K est un corps de rupture pour le polynôme minimal de a .

Soit L une extension de k . Montrer que l'application

$$\begin{cases} \text{Hom}_{k\text{-alg.}}(K, L) \longrightarrow \{x \in L, \quad P(x) = 0\} \\ \sigma \qquad \qquad \qquad \longmapsto \sigma(a) \end{cases}$$

est une bijection.

Exercice Quel est « le » corps de rupture de $X^2 + 1$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$? Les questions posées ont-elles un sens?

Montrer que le polynôme $P = X^3 - 2$ est irréductible sur $\mathbb{Q}$.

Montrer qu'il existe trois sous-corps de $\mathbb{C}$ qui sont des corps de rupture pour P sur $\mathbb{Q}$.

Corps de décomposition : problématique

Étant donné un polynôme P à coefficients dans k , on sait construire une extension de k dans lequel P a une racine.

On cherche maintenant à agrandir encore le corps pour scinder le polynôme P : existe-t-il une extension de k dans laquelle P est scindée. Dans quelle mesure une telle extension est-elle unique ?

Bien entendu, une extension d'une extension dans laquelle P est scindé est encore une extension dans laquelle P est scindé. Ainsi, on ne peut espérer de résultats d'unicité qu'en demandant des propriétés de minimalité sur l'extension dans laquelle P est scindé.

Corps de décomposition : solution

Définition — Corps de décomposition. Soit $P \in k[X]$ un polynôme. Un **corps de décomposition de P sur k** est une extension (K, i) dans laquelle P est scindé (P est produit de polynômes de degré 1) et $K = k(x_1, \dots, x_n)$ où $x_1, \dots, x_n$ sont les racines de P dans K .

Proposition — Existence et unicité. Pour tout $P \in k[X]$, il existe un corps de décomposition de P sur k .

Si (K, i) et (K', j) sont deux corps de décomposition de P sur k , il existe $\sigma : K \rightarrow K'$ un isomorphisme d'extensions de (K, i) dans (K', j) .

Il n'y a pas de propriété universelle du corps de décomposition, sinon il n'y aurait pas de théorie de Galois !

Corps de décomposition : exercices

Exercice Déterminer dans $\mathbb{C}$ un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. Le comparer à son corps de rupture.
Soient $P \in k[X]$ un polynôme irréductible de degré 2. Montrer qu'un corps de rupture de P est un corps de décomposition de P .

Exercice – Une autre propriété d'unicité pour les corps de décomposition. Soit $P \in k[X]$ et K une extension de k dans laquelle P est scindé. Montrer qu'il existe un unique sous-corps de K qui est un corps de décomposition de P sur k .
A-t-on un résultat analogue pour les corps de rupture ?

Corps algébriquement clos

Proposition Soit k un corps. Les propositions suivantes sont équivalentes

- (i) Tout polynôme non constant à coefficients dans k admet une racine dans k
- (ii) Les éléments irréductibles de $k[X]$ sont les polynômes de degré 1
- (iii) Tout polynôme non constant est produit de polynômes de degré 1
- (iv) Si (K, i) est une extension algébrique de k alors i est un isomorphisme.

Un corps vérifiant ces propriétés est dit **algébriquement clos**. Par exemple, $\mathbb{C}$ est algébriquement clos.

Définition Soit k un corps. Une **clôture algébrique de k** est une extension (K, i) de k où K est algébriquement clos et (K, i) est algébrique sur k . $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$.

Clôture algébrique

Proposition Soient K un corps algébriquement clos et k un sous-corps de K . La fermeture algébrique de k dans K est une clôture algébrique de k .

Par exemple, $\overline{\mathbb{Q}} = \{x \in \mathbb{C}, \quad x \text{ algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$ et $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$.

Proposition – Théorème de Steinitz. Tout corps admet une clôture algébrique. Soient (K, i) et (K', j) deux clôtures algébriques de k . Alors les extensions (K, i) et (K', j) sont isomorphes.

Lemme – Théorème de prolongement. Soient (K, i) une extension **algébrique** de k et (K', j) une extension algébriquement close. Alors il existe un morphisme de (K, i) dans (K', j) .

Exercice Soient k un corps et (K, i) une extension algébrique de k . Montrer que k et K ont même clôture algébrique.

Applications : Corps finis

Soit k un corps fini (c'est-à-dire de cardinal fini). Sa caractéristique est nécessairement un nombre premier p . Ainsi k est une extension de $\mathbb{F}_p$. Comme les éléments de k forment une famille génératrice de k sur $\mathbb{F}_p$, $1 \leq n = [k : \mathbb{F}_p] < +\infty$. On en déduit que k est un espace vectoriel de dimension finie sur $\mathbb{F}_p$. Ainsi $|k| = p^n$.

Pour tout p et tout $n \in \mathbb{N}^*$, existe-t-il un corps de cardinal p^n ?
peut-on décrire à isomorphisme près tous les corps de cardinal p^n ?

Proposition — Existence et unicité des corps finis. Soit p un nombre premier et $n \in \mathbb{N}^*$.

Il existe un corps de cardinal p^n , c'est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. Deux corps de cardinal p^n sont isomorphes.

Pour désigner « le » corps à p^n éléments, on utilise la notation $\mathbb{F}_{p^n}$.

Attention, $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

Cyclicité – Carré

Lemme Soient k un corps (commutatif) et G un sous-groupe fini de $k^\times$ alors G est cyclique.

Corollaire Si k est un corps fini alors $k^\times$ est cyclique.

Proposition – Carré dans un corps fini. Soit k un corps à p^n éléments (avec p premier et $n \in \mathbb{N}^*$). On note

$$k^{\times 2} = \{x \in k^\times, \exists y \in k, x = y^2\}$$

Si $p = 2$ alors $k^{\times 2} = k^\times$.

Si $p \neq 2$ alors $k^{\times 2}$ est un sous-groupe d'indice 2 de $k^\times$ et $x \in k^{\times 2}$ si et seulement si $x^{(p^n-1)/2} = 1$.

Exercices

Exercice Soient p un nombre premier impair, $n \in \mathbb{N}^*$ et $k = \mathbb{F}_{p^n}$. On considère $a, b \in k^\times$. Montrer que, pour tout $c \in k$, l'équation $ax^2 + by^2 = c$ d'inconnues (x, y) admet au moins une solution.

Exercice Soient p un nombre premier et $n \in \mathbb{N}^*$ et $k = \mathbb{F}_{p^n}$. Montrer la factorisation

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mu_d(p)} P$$

où $\mu_d(p)$ désigne l'ensemble des polynômes unitaires de degré d irréductibles sur $\mathbb{F}_p$.

Exercice Montrer que $\mathbb{F}_2[X]/\langle X^3 + X + 1 \rangle$ et $\mathbb{F}_2[X]/\langle X^3 + X^2 + 1 \rangle$ sont des corps, qu'ils sont isomorphes et donner un isomorphisme explicite entre ces deux corps.

Sous-corps d'un corps fini

Proposition — Sous-corps d'un corps fini. Soient p un nombre premier, $n \in \mathbb{N}^*$ et $k = \mathbb{F}_{p^n}$.
Soit k' un sous-corps de k alors $|k'| = p^m$ avec $m \mid n$. Inversement, pour tout $m \mid n$, k admet un unique sous-corps de cardinal $\mathbb{F}_{p^m}$.
De façon précise, le corps à p^m éléments contenu dans k est $k' = \{x \in k, x^{p^m} = x\}$.

Exemple $\mathbb{F}_4$ n'est pas un sous-corps de $\mathbb{F}_8$ mais c'est un sous-corps de $\mathbb{F}_{16}$.