Leçon 125 Extensions de corps, exemples et applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Extensions de corps Théorie de Galois de Josette Calais
2. Cours d'algèbre de Daniel Perrin
3. Algèbre de Xavier Gourdon
4. Algèbre et géométrie de Jean-Etienne Rombaldi
5. Théorie des nombres de Daniel Duverney

Développements.

1. Théorème de l'élément primitif
2. Irréductibilité des polynômes cyclotomiques

Table des matières

1 Des corps plus grands que d'autres

1.1 Degrés et extensions simples

(Chapitres 1.2 et 1.3 de Extensions de corps de Josette Calais)
On considère K un corps.

1. Définition : On dit que L est une extension du corps K si L est un corps contenant un sous-corps isomorphe à K
2. Exemple : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
3. Remarque : Soit L une extension de K, alors L est un K-espace vectoriel avec $\forall(\lambda, x) \in K \times L, \lambda.x = f(\lambda)x$ avec $f : K \longrightarrow L$ le morphisme de corps
4. Définition : Soit $L : K$ tel que $dim_K(L) < +\infty$ alors $[L : K] = dim_K(L)$ est le degré de l'extenstion L sur K
5. Exemple : $[\mathbb{C} : \mathbb{R}] = 2, [K, K] = 1$
6. Remarque : Si K est fini et L un extension de degré fini de K alors $|L| = |K|^{[L:K]}$
7. Théorème de la base télescopique : Soit $M : L$ et $L : K$ de degrés finis avec $(e_i)_{i\in I}$ base de L sur K et $(f_j)_{j\in J}$ base de M sur L alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K
8. Corollaire : Multiplicativité du degré : Dans ce cas $[M : K] = [M : L][L : K]$
9. Exemple : $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \times 3 = 6$
10. Définition : Soit $L : K$ et $A \subset L$, alors l'extension engendré par A sur K est le plus petit sous-corps de L contenant K et A, on le note $K(A)$ ou $K(a_1, ..., a_n)$ si $A = \{a_1, ..., a_n\}$
11. Définition : On dit que L est une extension monogène ou simple de K s'il existe $a \in L$ tel que $L = K(a)$
12. Exemple : $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ est simple
13. Proposition : Soit $L : K$ et $a \in L$, alors $K(a) = \{P(a), P \in K(X)\}$

1.2 Eléments algébriques et extensions algébriques

(Chapitres 2.1, 2.3, 2.4 et 5.5 de Extensions de corps de Josette Calais et III.1.a du Cours d'algèbre de Daniel Perrin)
On considère une extension de corps $L : K$.

1. Définition : Soit $a \in L$, alors on dit que a est algébrique sur K s'il existe $P \in K[x]\backslash K$ tel que $P(a) = 0$, sinon on dit que a est transcendant sur K, on dit alors que $K(a)$ est une extension simple algébrique ou transcendante
2. Exemple : e et π sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$
3. Théorème : Soit $\varphi : f \in K[X] \longrightarrow f(a) \in L$, alors :
   — φ est non injectif si et seulement si a est algébrique sur K
   — φ est injectif si et seulement si a est transcendant sur K
4. Théorème : Soit $a \in L$, alors les assertions suivantes sont équialentes :
   (a) Il existe un unique polynôme $P \in K[X]$ unitaire irréductible tel que $f(a) = 0 \Longleftrightarrow P \mid f$ dans $K[X]$

(b) $K[a] = K(a)$

(c) $[K(a) : K] = deg(p)$

5. Remarque : Dans ce cas a est algébrique et P est appelé polynôme minimal de a
6. Exemple : i et $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux $X^2 - 1$ et $X^2 - 2$
7. Proposition : Si $a \in L$ est transcendant sur K alors $K[a] \simeq K[X]$ et $K(a) \simeq K(X)$
8. Remarque : Si a est algébrique sur K alors $dim_K(K(a)) = deg(P)$ appelé degré de a avec P polynôme minimal de a sur K
9. Définition : On dit que L est une extension algébrique de K si pour tout $a \in L$, a est algébrique sur K
10. Proposition : Soit L extension algébrique de K et M extension algébrique de L, alors M est une extension algébrique de K
11. Théorème : Soit $L : K$ de degré fini L est une extension algébrique de K
12. Exemple : Les extensions simples $K(a)$ avec a algébrique sur K sont des extensions algébriques de K
13. Théorème : L'ensemble M des $x \in L$ tel que x soit algébrique sur K est un sous-corps de L
14. Exemple : Dans le cas $L = \mathbb{C}$ et $K = \mathbb{Q}$ alors $M =: \overline{\mathbb{Q}}$ est un extension algébrique de $\mathbb{Q}$ mais n'est pas de degré fini car $dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{2})) = n$
15. Lemme (admis) : Théorème de Lindemann-Weierstrass : Soit $z_1, ..., z_n \in \overline{Q}$ algébriquement indépendants sur $\mathbb{Q}$, ie $\forall P \in K[X_1, ..., X_n] \backslash K, P(z_1, ..., z_n) \neq 0$, alors $e^{z_1}, ..., e^{z_n} \in \mathbb{C}$ sont algébriquement indépendants sur $\overline{\mathbb{Q}}$
16. Application : e et π sont transcendants sur $\mathbb{Q}$

2 Des extensions de corps utiles aux polynômes

2.1 Polynômes irréductibles et corps de rupture

(Chapitre III.1.c du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $P \in K[X]$, alors on dit que P est irréductible si ses seuls diviseurs sont les inversibles K^* ou les polynômes associés à P
2. Exemple : $X^2 + 1$ est irréductible sur $\mathbb{R}$
3. Définition : Soit $P \in K[X]$ irréductible, alors un corps de rupture de P sur K est une extension monogène $L = K(a)$ de K avec $a \in L$ tel que $P(a) = 0$
4. Proposition : Soit $P \in K[X]$ irréductible, alors $K[X]/(P)$ est un corps dans lequel K s'injecte et x image de $X \in K[X]$ par $Q \in K[X] \longmapsto \overline{Q} \in K[X]/(P)$ vérifie $P(x) = 0$ et $K[X]/(P) = K(x)$
5. Exemple : $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$ car $i \in \mathbb{C}$ et $(X^2 + 1)(i) = 0$
6. Théorème : Il existe un corps de rupture de P sur K unique à isomorphisme près

7. Lemme : Soit $i : K \longrightarrow K'$ un isomorphisme de corps que l'on étend un isomorphisme $\tilde{i} : K[X] \longrightarrow K'[X]$, $P' = \tilde{i}(P)$, L corps de rupture de $P \in K[X]$ irréductible engendré par une racine x de P et L' de $P' := \bar{i}(P)$ engendré par une racine x' de P', alors il existe un unique isomorphisme $\varphi : L \longrightarrow L'$ prolongeant i et tel que $\varphi(x) = x'$
8. Remarque : Dans un corps de rupture, un polynôme n'est en général pas scindé
9. Exemple : $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ mais $X^3 - 2$ n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$ car $j^3\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$ et $(X^3 - 2)(j^3\sqrt{2}) = 0$

2.2 Corps de décomposition

(Chapitre III.1.c du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $P \in K[X]$, alors on dit que L est un corps de décomposition de P si L est une extension de K telle que :
   — P soit scindé dans $L[X]$, ie P a toutes ses racines dans L
   — L soit minimal pour cette propriété, ie les racines de P engendrent L
2. Théorème : Il existe un corps de décomposition de P sur K unique à isomorphisme près
3. Lemme : Soit $i : K \longrightarrow K'$ un isomorphisme de corps que l'on étend un isomorphisme $\tilde{i} : K[X] \longrightarrow K'[X]$, $P' = \tilde{i}(P)$, L corps de décomposition de $P \in K[X]$ et L' de $P' := \bar{i}(P)$, alors il existe un isomorphisme $\varphi : L \longrightarrow L'$ prolongeant i
4. Exemple : Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$ et celui de $X^4 - 2$ est $\mathbb{Q}(\sqrt[4]{2}, i)$
5. Application : Théorème de l'élément primitif : Soit L une extension de degré fini de K, si K est de caractéristique 0 alors L est monogonèe, ie il existe $a \in L$ tel que $L = K(a)$ (Problème 2.5.8 d'Algèbre de Xavier Gourdon)
6. Lemme : Soit $P, Q \in K[X]$ et $L : K$, alors $PGCD_{K[X]}(P, Q) = PGCD_{L[X]}(P, Q)$
7. Remarque : Ce théorème est également vérifié si K est fini

2.3 Corps algébriquement clos et cloture algébrique

(Chapitres 3.1.A, 5.0, 5.2 et 5.3 de Extensions de corps de Josette Calais)

1. Définition : On dit que K est algébriquement clos si tout polynôme non constant de $K[X]$ admet au moins une racine dans K
2. Exemple : $\mathbb{C}$ est algébriquement clos et $\overline{Q}$ défini précédemment également
3. Proposition : Si K est algébriquement clos alors tout $P \in K[X] \backslash K$ est scindé
4. Remarque : Un corps fini n'est jamais algébriquement clos et un corps algébriquement clos n'admet aucune extension algébrique propre
5. Théorème (admis) : Tout corps K admet une extension algébriquement close
6. Définition : L est une cloture algébrique de K si :
   — L est algébriquement clos
   — L est une extension algébrique de K

7. Exemple : $\mathbb{C}$ est une cloture algébrique de $\mathbb{R}$ et $\overline{Q}$ en est une de $\mathbb{Q}$
8. Théorème : Tout corps K admet une cloture algébrique, plus précisément si L est une extension de K alors l'ensemble $\overline{K}$ des $a \in L$ tels que a est algébrique sur K est une cloture algébrique de K
9. Lemme : Si L extension algébrique de K, L' extension algébriquement close de K alors :
   — Il existe un monomorphisme $\sigma : L \longrightarrow L'$ tel que $\sigma \circ i = i'$ avec $i : K \longrightarrow L$ et $i' : K \longrightarrow L'$ les morphismes de corps sous-jacents
   — Si de plus L est algébriquement clos et L' algébrique sur $i'(K)$ alors σ est un isomorphisme
10. Théorème : Tout corps admet une cloture algébrique unique à isomorphisme près

3 Etude d'extensions particulières

3.1 Existence et unicité des corps finis

(Chapitres 13.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.b du Cours d'algèbre de Daniel Perrin et 4.3 et 5.4 de Extensions de corps de Josette Calais)

On considère $q = p^n$ avec $p \in \mathbb{N}$ premier.

1. Définition : On note $U_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = |U_n(p)|$
2. Proposition : Soit $P \in U_n(p)$, alors $\mathbb{F}_p[X]/(P)$ est un $\mathbb{F}_p$-espace vectoriel de dimension n et est un corps de cardinale $q = p^n$
3. Exemple : $\forall \lambda \in \mathbb{F}_p, X - \lambda \in U_1(p)$ donc $I_1(p) = p$ et tous ces corps $\mathbb{F}_p[X]/(X - \lambda)$ sont isomorphes à $\mathbb{F}_p$
4. Exemple : Comme $P = X^2 + \lambda X + \mu$ est irréductible si et seulement si sans racines, $I_2(p) = \frac{p(p-1)}{2}$
5. Lemme : En notant $P_n = X^{p^n} - X = X^q - X$, 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 $P \in U_n(d)$ divise P_n
6. Théorème : P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en irréductibles $P_n = \prod_{d|n} \prod_{P \in U_d(p)} P$
7. Théorème : A isomorphisme près, il existe un unique corps à $q = p^n$ éléments, on le note $\mathbb{F}_p$, il s'agit de $\mathbb{F}_p[X]/(P)$ avec $P \in U_n(p)$, et du corps de décomposition de P_n sur $\mathbb{F}_p$
8. Exemple : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}, \mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + 1)$
9. Remarque : Un corps fini n'est jamais algébriquement clos
10. Théorème : $E = \bigcup_{k \in \mathbb{N}^*} \mathbb{F}_{p^{k!}}$ est une cloture algébrique de $\mathbb{F}_{p^n}$

3.2 Polynômes et extensions cyclotomiques

(Chapitres 6.2 et 6.3 de Extensions de corps de Josette Calais)
On note $\Omega_n \subset \overline{K}$ l'ensemble des racines n-ièmes primitives de l'unité dans K.

1. Définition : $\phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$ est appelé le n-ième cyclotomique et $K(\omega)$ la n-ième extension cyclotomique de K (indépendant du choix de $\omega \in \Omega_n$)
2. Exemple : Si $K = \mathbb{Q}$ alors $\phi_1 = X-1, \phi_2 = X+1, \phi_3 = (X-e^{\frac{2i\pi}{3}}(X-e^{-\frac{2i\pi}{3}}) = X^2+X+1$
3. Remarque : ϕ_n est unitaire dans $K(\omega)[X]$ et $deg(\phi_n) = \varphi(n)$ avec φ la fonction d'Euler
4. Proposition : $X^n - 1 = \prod_{d|n} \phi_d$
5. Théorème : Si $car(K) = 0$ alors ϕ_n est unitaire dans $\mathbb{Z}[X]$ et si $car(K) = p$ tel que p ne divise pas n alors ϕ_n unitaire dans $\mathbb{Z}/p\mathbb{Z}[X]$
6. Application : Théorème de Wedderburn : Tout anneau intègre fini dont tous les éléments non nuls sont inversibles (corps gauche) est un corps
7. Théorème : Si $K = \mathbb{Q}$, soit $\omega \in \Omega_n$, alors le polynôme irréductible de ω sur $\mathbb{Q}$ est ϕ_n
8. Corollaire : Si $K = \mathbb{Q}$ alors ϕ_n est irréductible et $[\mathbb{Q}(\omega), \mathbb{Q}] = \varphi(n)$

3.3 Les entiers d'un corps quadratique

(Chapitres 5.1, 5.2, 5.3 et 5.7 de Théorie des nombres de Daniel Duverney, 8.4.A de Extensions de corps de Josette Calais et II.6 du Cours d'algèbre de Daniel Perrin)
On considère K un corps quadratique.

1. Définition : On dit que K est un corps quadratique si K est une extension de degré 2 de $\mathbb{Q}$
2. Théorème : Il existe $d \in \mathbb{Z}$ sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$ avec $\sqrt{d}$ désignant la racine carré de d si $d > 0$ et $i\sqrt{-d}$ si $d < 0$
3. Définition : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors on dit que z est un entier de $\mathbb{Q}(\delta)$ (ou entier quadratique) si z est racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbb{Z}$, et on note A_d l'ensemble des entiers de $\mathbb{Q}(\sqrt{d})$
4. Exemple : Le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ est un entier de $\mathbb{Q}(\sqrt{5})$, i est un entier de $\mathbb{Q}(i)$ et $j = e^{i\frac{2\pi}{3}}$ est un entier de $\mathbb{Q}(i\sqrt{3})$
5. Définition : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors, comme $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ et $(1, \delta)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{d})$, il existe $(x, y) \in \mathbb{Q}^2$ tel que $z = x + \delta y$, ainsi on appelle :
   — Conjugué de z : $\overline{z} = x - \delta y$
   — Norme de z : $N(z) = z\overline{z} = x^2 - dy^2$
   — Trace de z : $tr(z) = z + \overline{z} = 2x$
6. Remarque : Si $d < 0$ alors $\overline{z}$ est également le conjugué complexe de $z \in \mathbb{C}$
7. Lemme : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors $z \in A_d \iff tr(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}$
8. Lemme : Soit $z = \frac{a}{b} + \frac{\alpha}{\beta}\delta \in A_d \subset Q(\sqrt{d})$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux et (α, β) dans $\mathbb{Z} \times \mathbb{N}^*$ premiers entre eux, alors $b \in \{1, 2\}$, puis :

— Si $b = 1$ alors $z = a + \alpha\delta$
— Si $b = 2$ alors a, α impairs, $\beta = 2$ et $d \equiv 1[4]$.

9. Théorème : On a les deux cas suivants :
— Si $d \equiv 2[4]$ ou $d \equiv 3[4]$ alors $A_d = \mathbb{Z} + \mathbb{Z}\delta = \mathbb{Z}[\delta]$
— Sinon $d \equiv 1[4]$ alors $A_d = \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2} = \mathbb{Z}\left[\frac{1+\delta}{2}\right]$
10. Corollaire : L'ensemble A_d est un sous-anneau de $\mathbb{Q}(\delta)$
11. Théorème : Soit $z \in A_d$, alors $z \in A_d^\times \iff |N(z)| = 1$
12. Théorème : L'anneau $A_{-1} = \mathbb{Z}[i]$ (car $-1 \equiv 3[4]$) est euclidien avec N comme stathme
13. Remarque : Plus généralement l'application norme sur A_d est un stathme sur A_d si $d \in \{2, 3, 5, 13, -1, -2, -3, -7, -11\}$, en particulier les anneaux correspondants A_d sont euclidiens donc principaux
14. Application : L'équation de Mordell (pour $k = 2$) $y^2 = x^3 - 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour uniques solutions $(3, 5)$ et $(3, -5)$ (Exercice 5.17 de Théorie des nombres de Daniel Duverney)
15. Application : Soit $n \in \mathbb{N}$, alors n s'écrit comme somme de deux carrés si et seulement si $\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$