

Chapitre 6

Extensions de corps : généralités

Tous les corps considérés dans ce chapitre et le suivant sont commutatifs.

6.1 Théorie de base

Rappel : La caractéristique d'un corps est soit zéro, soit un nombre premier.

Définition 6.1.1. Si K et L sont des corps, on appelle morphisme de corps tout morphisme d'anneau $f : K \rightarrow L$. Un tel morphisme est injectif et aussi appelé extension de K . Le degré de l'extension, noté $[L : K]$ est la dimension de L comme espace vectoriel sur K .

Proposition 6.1.2. a) Si K est un corps de caractéristique nulle, alors il existe une unique extension $f : \mathbb{Q} \rightarrow K$.

b) Si K est un corps de caractéristique $p > 0$, alors il existe une unique extension $f : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \rightarrow K$.

Définition 6.1.3. L'image de l'homomorphisme précédent s'appelle le sous-corps premier de $\mathbb{K}$: c'est le plus petit sous-corps de $\mathbb{K}$.

Proposition 6.1.4 (Tour d'extensions). Soit $f : K \rightarrow L$, $g : L \rightarrow L'$ une tour d'extension, alors :

$$[L' : K] = [L' : L][L : K] .$$

6.2 Construction d'extensions

6.2.1 Corps de rupture d'un polynôme irréductible

Soit $P \in K[X]$ un polynôme irréductible, alors $K[X]/(P)$ est un corps.

Proposition 6.2.1. *L'extension $K \rightarrow K[X]/(P)$, avec $P \in K[X]$ polynôme irréductible, est une extension de degré $\deg(P)$.*

6.2.2 Adjonction d'éléments

Soit $f : K \rightarrow L$ une extension de corps, et $\alpha \in L$. On note $K(\alpha)$ le plus petit sous-corps de L qui contient $f(K)$ et α ; on l'appelle extension de K engendrée par α . On définit de même l'extension $K \rightarrow K(A)$ engendrée par une partie $A \subset L$.

Définition 6.2.2. Une extension est de type finie si et seulement si elle est engendrée par une partie finie. Une extension est simple si et seulement si elle est engendrée par un élément (appelé élément primitif).

6.3 Algébricité

Proposition 6.3.1. *Soit $f : K \rightarrow L = K(\alpha)$ une extension simple, alors il y a équivalence entre :*

- a) *l'extension est de degré finie ;*
- b) *l'anneau $K[\alpha]$ est égal au corps $K(\alpha)$;*
- c) *l'idéal annulateur de $\alpha : I_\alpha = \{P \in K[X], P(\alpha) = 0\}$ est non trivial.*

22/11/2010

Remarques 6.3.2. 1. Lorsque l'idéal annulateur de α est non trivial, il est engendré par un polynôme irréductible P_α appelé le polynôme minimal de α et $K[X]/(P_\alpha)$ est isomorphe à $K(\alpha)$.

2. Si α et β ont le même polynôme minimal, alors les extensions $K \rightarrow K(\alpha)$ et $K \rightarrow K(\beta)$ sont isomorphes.

Définition 6.3.3. a) Avec les hypothèses précédentes, l'élément α est algébrique sur K si et seulement s'il satisfait les conditions équivalentes de la proposition ; dans le cas contraire, α est dit transcendant.

b) Une extension $f : K \rightarrow L$ est algébrique si et seulement si tous les éléments de L sont algébriques sur K .

Théorème 6.3.4. *Les éléments de L algébriques sur K forment un sous-corps de L .*

6.4 Corps de décomposition

Définition 6.4.1. Soit $Q \in K[X]$ un polynôme unitaire, et $f : K \rightarrow L$ une extension. On dit que L est un corps de décomposition de Q si et seulement si :

- a) $f(Q)$ est scindé dans L et
- b) l'extension L est engendrée par les racines de Q .

Théorème 6.4.2. Soit $Q \in K[X]$ un polynôme unitaire, alors il existe une extension qui est un corps de décomposition de K , et deux telles extensions sont isomorphes.

6.5 Corps cyclotomiques

On note $\zeta_n = e^{\frac{i2\pi}{n}} \in \mathbb{C}$.

Proposition 6.5.1. Le corps $\mathbb{Q}(\zeta_n)$ est le corps de décomposition du polynôme $X^n - 1$.

Définition 6.5.2. Le corps $\mathbb{Q}(\zeta_n)$ est appelé corps cyclotomique des racines n -ièmes de l'unité.

Polynômes cyclotomiques

Définition 6.5.3. On appelle racine primitive n -ième de l'unité tout générateur du groupe $U_n \subset \mathbb{C}$ des racines n -ièmes de 1. Ce sont les éléments d'ordre n de $\mathbb{C}^*$.

Définition 6.5.4. Le polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est le polynôme unitaire dont les racines sont les racines primitives n -ièmes de 1 :

$$\Phi_n = \prod_{\substack{0 \leq k < n \\ \text{PGCD}(k,n)=1}} (X - \zeta_n^k) .$$

Théorème 6.5.5. Le polynôme cyclotomique Φ_n est à coefficients entiers et il est irréductible sur $\mathbb{Q}$.

Corollaire 6.5.6. Le degré de l'extension $\mathbb{Q} \rightarrow \mathbb{Q}(\zeta)$ est l'indicateur d'Euler $\phi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times) = \deg(\Phi_n)$.

6.6 Corps finis

Soit $\mathbb{F}$ un corps fini de caractéristique p , et de cardinal q , alors $\mathbb{F}$ est une extension de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On a $q = p^m$, où $m = [\mathbb{F} : \mathbb{F}_p]$.

Théorème 6.6.1. *Un corps fini de cardinal $q = p^m$ est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.*

Corollaire 6.6.2. *Deux corps finis de cardinal $q = p^m$ sont isomorphes.*

Remarque 6.6.3. L'isomorphisme précédent n'est pas canonique.

L'hypothèse de commutativité n'est pas nécessaire :

Théorème 6.6.4 (Wedderburn). *Tout corps fini est commutatif.*

Exercice 6.6.5. a) Montrer que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

b) Montrer que toute extension entre corps finis est primitive.

Exercice 6.6.6. a) Montrer que s'il existe une extension $F \rightarrow F'$ entre deux corps finis de caractéristique p , de cardinaux respectifs $q = p^d$ et $q' = p^n$, alors d divise n .

c) Soit $\mathbb{F}_q$ est un corps de caractéristique p à $q = p^n$ éléments. Montrer que si d divise n , alors $\mathbb{F}_q$ contient un unique sous-corps à p^d éléments.

Polynômes irréductibles sur $\mathbb{F}_p$

Proposition 6.6.7. *Tout polynôme irréductible de degré d à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ divise $X^{p^d} - X$.*

Proposition 6.6.8. *Pour p premier et $d > 0$, soit $n_p(d)$ le nombre de polynômes irréductibles unitaires de degré d sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors :*

$$p^n = \sum_{d|n} d n_p(d) .$$

6.7 Corps algébriquement clos, clôture algébrique

Définition 6.7.1. a) Un corps commutatif L est algébriquement clos si et seulement si tout polynôme à coefficients dans L a au moins une racine dans L .

b) Une clôture algébrique d'un corps commutatif K est une extension algébrique qui est algébriquement close.

Etant donné une extension $K \rightarrow L$, la fermeture algébrique de K dans L est l'ensemble $K_{\text{alg},L}$ des éléments de L algébriques sur K . C'est un sous-corps de L .

Proposition 6.7.2. *Si L est algébriquement clos, alors la fermeture algébrique de K dans L est une clôture algébrique de K .*

Corollaire 6.7.3. *Le corps des nombres algébriques $\overline{\mathbb{Q}} = \mathbb{Q}_{\text{alg},L}$ est une clôture algébrique de $\mathbb{Q}$.*

Clôture algébrique de $\mathbb{F}_p$

Pour p premier on pose $K_1 = \mathbb{F}_p$, et pour $n \geq 2$ on définit l'extension $K_{n-1} \subset K_n$ comme corps de décomposition de $X^{p^{n!}} - X$; K_n est un corps à $p^{n!}$ éléments.

Proposition 6.7.4. *La réunion $\overline{\mathbb{F}_p} = \cup_n K_n$ est une clôture algébrique de $\mathbb{F}_p$.*

Existence d'une clôture algébrique

Théorème 6.7.5. *Tout corps commutatif K admet une clôture algébrique, et deux telles clôtures sont (non canoniquement) isomorphes (comme K -algèbre).*

28/11/2010