

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 de K engendrée par une partie $A \subset L$: $K(A)$.

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 α : $I_\alpha = \{P \in K[X], P(\alpha) = 0\}$ est non trivial.*

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.

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 $m = [\mathbb{F} : \mathbb{F}_p]$.

Proposition 6.4.3. Un corps fini (commutatif) de cardinal $q = p^m$ est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.

Remarque 6.4.4. On montrera que tout corps fini est commutatif. A isomorphisme près, il existe un unique corps à $q = p^m$ éléments, noté $\mathbb{F}_q$.

Proposition 6.4.5. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

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.

Théorème 6.5.3. Le degré de l'extension $\mathbb{Q} \rightarrow \mathbb{Q}(\zeta)$ est l'indicateur d'Euler $\phi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

Polynômes cyclotomiques

Définition 6.5.4. 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 6.5.5. 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 6.5.6. *Le polynôme cyclotomique Φ_n est à coefficients entiers et il est irréductible sur $\mathbb{Q}$.*

Fin du
cours
du
20 no-
vembre

6.6 Extension normale, extension séparable

Définition 6.6.1. Une extension $f : K \rightarrow L$ est normale si et seulement si tout polynôme irréductible de $K[X]$ qui admet une racine dans L est scindé dans L .

Théorème 6.6.2. *Soit $f : K \rightarrow L$ une extension. Il y a équivalence entre :*
a) *l'extension est normale et de degré fini ;*
b) *L est corps de décomposition d'un polynôme unitaire de $K[X]$.*

Définition 6.6.3. Une clôture normale d'une extension de degré fini : $f : K \rightarrow L$ est une extension $g : L \rightarrow L'$ telle que
a) l'extension $g \circ f : K \rightarrow L'$ est normale, et
b) l'extension $g : L \rightarrow L'$ est minimale pour la propriété a).

Proposition 6.6.4. *Toute extension admet une clôture normale, unique à isomorphisme près.*

Définition 6.6.5. Soit K un corps commutatif. Un polynôme irréductible $P \in K[X]$ est séparable sur K si et seulement s'il n'a pas de racine multiple dans son corps de décomposition. Dans le cas contraire, on dit que P est inséparable.

Proposition 6.6.6. a) *Si k est de caractéristique nulle, un polynôme irréductible de $K[X]$ est toujours séparable.*
b) *Si K est de caractéristique $p > 0$, un polynôme irréductible de $K[X]$ est inséparable si et seulement s'il appartient à $K[X^p]$.*

Définition 6.6.7. Soit $f : K \rightarrow L$ une extension algébrique (tout élément de L est algébrique sur K).

a) Un élément $\alpha \in L$ est séparable si et seulement si son polynôme minimal est séparable.

b) L'extension est séparable si et seulement si tous les éléments de L sont séparables.

Définition 6.6.8. Un corps K est parfait si et seulement si toute extension algébrique est séparable.

Remarque 6.6.9. Tout corps de caractéristique zéro est parfait.

Corps parfaits de caractéristique non nulle

On rappelle que sur un corps K de caractéristique $p > 0$, l'application :

$$\begin{array}{ccc} K & \rightarrow & K \\ x & \mapsto & x^p \end{array}$$

est un homomorphisme, appelé homomorphisme de Frobenius. Comme homomorphisme de corps, il est toujours injectif. Pour un corps fini, cet homomorphisme est surjectif.

Théorème 6.6.10. *Un corps de caractéristique non nulle est parfait si et seulement si son homomorphisme de Frobenius est surjectif.*

Démonstration. Soit K un corps de caractéristique non nulle p , et $K^p = \{x^p, x \in K\}$ le sous-corps image de l'homomorphisme de Frobenius. Supposons que b soit un élément de $K - K^p$. Soit α une racine de $X^p - b$ (dans le corps de décomposition de $X^p - b$). On a : $X^p - b = X^p - \alpha^p = (X - \alpha)^p$. Il en résulte que le polynôme minimal de α sur K est non séparable. Donc si K est parfait, alors $K = K^p$.

Supposons que $K = K^p$, et soit P un polynôme inséparable :

$$P = \sum_i a_i X^{pi} = \sum_i b_i^p X^{pi} = \left(\sum_i b_i X^i \right)^p .$$

Il n'existe aucun polynôme irréductible inséparable : K est parfait. □

Exercice 6.6.11. Soit K un corps de caractéristique non nulle p .

1. Montrer que si b n'a pas de racine p -ième dans K , alors $X^p - b$ est irréductible sur K .
2. Montrer que si b n'a pas de racine p -ième dans K , alors pour tout $k > 0$ $X^{p^k} - b$ est irréductible sur K .

3. Montrer que si le sous-corps K^p est distinct de K , alors l'extension $(K : K^p)$ n'est pas de degré fini.
4. Montrer que si $(F : K)$ est une extension de degré fini avec F corps parfait, alors K est parfait.

On montrera dans le prochain chapitre le théorème suivant.

Théorème 6.6.12. *Une extension de degré fini $K \rightarrow L$ est séparable si et seulement si elle est engendrée par des éléments séparables.*

6.7 Corps algébriquement clôs, clôture algébrique

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

b) Une clôture algébrique d'un corps commutatif K est une extension algébrique L dans laquelle tout polynôme de $K[X]$ est scindé.

Proposition 6.7.2. *Toute clôture algébrique est algébriquement close.*

Théorème 6.7.3. *Tout corps commutatif admet une clôture algébrique unique à isomorphisme près.*

Fin du
cours
du
21 no-
vembre