Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

B. Le Stum

Le théorème fondamental de la théorie de Galois

Bernard Le Stum*
Université de Rennes 1

Version du 26 janvier 2001

1 Extensions algébriques

1.1 Définition

Si K est un corps, une *extension* L/K est une K-algèbre L qui est un corps. Un *morphisme* d'extensions est un morphisme de K-algèbres. On définit une *sous-extension* ou *extension intermédiaire* de manière évidente. On dispose aussi de la notion de *composée* M/K d'extensions L/K et M/L. Enfin, on note $[L : K] := \dim_K L$ et on dit que L/K est *finie* si $[L : K] < \infty$ et *triviale* si $[L : K] = 1$.

1.2 Proposition

Si L/K est une extension de corps et E un espace vectoriel sur L, on a $\dim_K E = [L : K] \dim_L E$. En particulier, on a toujours $[M : L][L : K] = [M : K]$. Il suit que la composée de deux extensions finies est finie.

1.3 Remarque

Toute intersection de sous-extensions de K dans L est une extension de K. Si $E \subset L$, on note $K(E)$ la plus petite sous-extension de L contenant E. On a bien sûr toujours $K(E)(F) = K(E \cup F)$. Enfin, on note $\deg_K(E) := [K(E) : K]$.

1.4 Proposition

Soient $\alpha \in L$, $d := \deg_K(\alpha)$ et Φ_α le morphisme de K-algèbres $K[T] \to L, T \mapsto \alpha$. Alors

Si $d = \infty$, Φ_α est injective et se prolonge de manière unique en un isomorphisme $K(T) \tilde{\to} K(\alpha)$.

Si $d < \infty$, Φ_α est induit un isomorphisme

$$K[T]/P_\alpha \tilde{\to} K(\alpha)$$

et P_α est l'unique polynôme unitaire irréductible de degré d tel que $P_\alpha(\alpha) = 0$.

*lestum@univ-rennes1.fr

1.5 Définition

Dans le premier cas, on dit que α est *transcendant*. Dans le second, on dit qu'il est *algébrique* et que P_α est son *polynôme minimal*. Enfin, on dit que $\alpha, \beta \in L$ sont *conjugués* si $P_\beta = P_\alpha$.

On dit que L/K est *algébrique* si tous les éléments de L sont algébriques sur K.

1.6 Remarque

Soit $\sigma : L \to M$ un morphisme de K-extensions, $\alpha \in L$ et $\beta = \sigma(\alpha)$. Alors σ induit un isomorphisme $K(\alpha) \simeq K(\beta)$. En particulier, α est algébrique ssi β est algébrique et on a alors $P_\beta = P_\alpha$.

1.7 Proposition

i) Toute extension finie est algébrique.

ii) Une extension L/K est finie ssi il existe $\alpha_1, \ldots, \alpha_n$ algébriques sur K tels que $L = K(\alpha_1, \ldots, \alpha_n)$.

iii) La composée de deux extensions algébriques est algébrique.

iv) Si L/K est une extension algébrique, tout K-morphisme $\sigma : L \to L$ est bijectif.

2 Corps de rupture

2.1 Définition

Un *corps de rupture* pour $P \in K[T]$ est une extension L/K telle qu'il existe $\alpha \in L$ avec $P(\alpha) = 0$ et $L = K(\alpha)$.

2.2 Proposition

Si $P \notin K$, il existe un corps de rupture L pour P sur K.

Supposons P irréductible. Soit L'/K une extension et $\alpha \in L, \alpha' \in L'$ tels que $P(\alpha) = P(\alpha') = 0$. Alors, il existe un unique K-morphisme $\sigma : L \to L'$ tel que $\sigma(\alpha) = \alpha'$. Si L' est aussi un corps de rupture de P sur K, σ est un isomorphisme.

2.3 Remarque

Si L/K une extension et $\alpha \in L$, alors $K(\alpha)$ est un corps de rupture pour P_α sur K.

2.4 Définition

On dit que $P \in K[T]$ se décompose sur une extension L/K en produit de facteurs linéaires s'il existe $\alpha_1, \ldots, \alpha_d \in L$ avec $P = c(T - \alpha_1) \cdots (T - \alpha_d)$.

On dit que L est un *corps de décomposition* pour P si, en plus, $L = K(\alpha_1, \ldots, \alpha_d)$.

2.5 Proposition

Si $P \notin K$, il existe un corps de décomposition L pour P sur K. Soient L'/K une extension sur laquelle P se décompose en produit de facteurs linéaires. Alors, il existe un K-morphisme $\sigma : L \to L'$. Si L' est aussi un corps de décomposition de P sur K, σ est un isomorphisme.

2.6 Définition

Un corps K est *algébriquement clos* s'il n'existe pas d'extension algébrique non-triviale de K. Une *clôture algébrique* d'un corps K est une extension algébrique $\bar{K}/K$ qui est un corps algébriquement clos.

2.7 Théorème

Tout corps K possède une clôture algébrique $\bar{K}$. Si L/K est une extension algébrique, il existe un K-morphisme $\sigma : L \to \bar{K}$. Si L est algébriquement clos, σ est un isomorphisme.

3 Extensions galoisiennes

3.1 Définition

Une extension algébrique L/K est *normale* si pour toute extension M/K contenant L et tout K-morphisme $\sigma : L \to M$, on a $\sigma(L) \subset L$.

3.2 Remarques

Il suffit de considérer le cas ou M est une clôture algébrique de L.

3.3 Proposition

i) Une extension algébrique L/K est normale ssi tout $P \in K[T]$ irréductible avec une racine dans L se décompose en produit de facteurs linéaires.

ii) Une extension finie est normale ssi c'est le corps de décomposition d'un polynôme.

3.4 Définition

On dit que $\alpha \in L$ est *séparable* sur K si $P'_\alpha(\alpha) \neq 0$. Une extension algébrique L/K est *séparable* si tout $\alpha \in L$ est séparable sur K.

3.5 Remarque

On dit aussi qu'un polynôme non-constant $P \in K[T]$ est *séparable* s'il se décompose sur un corps de décomposition en produit de facteurs linéaires *distincts*. On voit alors que $\alpha \in L$ est séparable sur K ssi P_α est séparable.

3.6 Proposition

Soit L/K une extension finie de degré d et M/K une extension quelconque. Alors, il existe au plus d K-morphisme distincts $L \to M$. En fait, si M est algébriquement clos, alors L/K est séparable ssi il existe exactement d K-morphisme distincts $L \to M$.

3.7 Théorème (de l'élément primitif)

Si L/K est une extension séparable finie, il existe $\alpha \in L$ tel que $L = K(\alpha)$.

3.8 Définition

Une extension algébrique L/K est *galoisienne* ssi elle est normale et séparable.

3.9 Remarque

Une extension algébrique L/K est galoisienne si pour tout $\alpha \in L$, P_α se décompose sur L en produit de facteurs linéaires distincts.

4 Théorie de Galois

4.1 Définition

Si L/K une extension algébrique, le groupe $G := Gal(L/K)$ des K-automorphismes de L est le *groupe de Galois* de L/K.

4.2 Proposition

Une extension finie L/K de degré d et de groupe de Galois G est galoisienne ssi $|G| = d$.

4.3 Remarque

Soit L/K une extension algébrique et G son groupe de Galois.

Si M est une extension intermédiaire, alors $H := Gal(L/M)$ est le sous-groupe de G composé des σ tels que $\sigma_{|M} = \mathrm{Id}_M$.

Réciproquement, si $H \subset G$ est un sous-groupe, alors $M := L^H := \{\alpha \in L, \forall \sigma \in H, \sigma(\alpha) = \alpha\}$ est une extension de corps intermédiaire.

4.4 Théorème

Soit L/K une extension algébrique de groupe de galois G. Alors,

i) L/K est galoisienne ssi $K \tilde{\to} L^G$.

ii) L/K est galoisienne finie ssi il existe un sous-groupe fini $H \subset G$ tel que $K \tilde{\to} L^H$. Et alors, $H = G$.

4.5 Corollaire (Théorème de Galois)

Soit L/K une extension galoisienne finie et $G := Gal(L/K)$. Alors, les applications $M \mapsto H := Gal(L/M)$ et $H \mapsto M := L^H$ établissent une bijection décroissante entre les extensions intermédiaires M et les sous-groupes H de G.

4.6 Proposition

Avec les notations du théorème de Galois, M/K est galoisienne ssi H est distingué dans G et on a alors un isomorphisme canonique $Gal(M/K) \cong G/H$.

Références

[1] J.-P. Lafon, *algèbre commutative, Langages géométriques et algébriques*. Collection Enseignement des sciences, 24. Hermann (1977)

[2] S. Lang, *Algebra*. Addison-Wesley, Reading, Massachusets (1965)