Le théorème fondamental de la théorie de Galois

Bernard Le Stum[1]

Université de Rennes 1

Version du 27 février 2007

[1] bernard.lestum@univ-rennes1.fr

Définition

- *Une extension de corps L/K est un homomorphisme de corps (nécéssairement injectif) $K \hookrightarrow L$.*
- *Un morphisme d'extensions de K est un homorphisme de corps $\sigma : L \to M$ compatible avec les extensions.*
- *Lorsque σ est l'inclusion d'un sous-corps, on dit que L/K est une sous-extension ou extension intermédiaire de M/K.*
- *Le degré d'une extension L/K est $[L : K] := \dim_K L$.*
- *Une extension L/K est finie si $[L : K] < \infty$ et triviale si $[L : K] = 1$.*

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, si M/L est une autre extension, on a

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

Il suit que la composée de deux extensions finies est finie.

Si L/K est une extension, 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, si $F \subset L$,

$$K(E)(F) = K(E \cup F).$$

Enfin, on note

$$\deg_K(E) := [K(E) : K].$$

Définition

Lorsque E est réduit à un élément α, on écrit $K(\alpha)$ et $\deg_K \alpha$. On dit que $\deg_K \alpha$ est le degré de α sur K.

Proposition

Soient L/K une extension de corps, $\alpha \in L$ de degré d et

$$\begin{array}{rcl} K[T] & \xrightarrow{\Phi_\alpha} & L \\ P & \longmapsto & P(\alpha). \end{array}$$

1. *Si $d = \infty$, Φ_α est injective et se prolonge de manière unique en un isomorphisme $K(T) \tilde{\to} K(\alpha)$.*
2. *Si $d < \infty$, Φ_α induit un isomorphisme $K[T]/P_\alpha \tilde{\to} K(\alpha)$ où P_α est l'unique polynôme unitaire (irréductible) de degré d tel que $P_\alpha(\alpha) = 0$.*

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.*
- *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.*

Proposition

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

Proposition

1. *Toute extension finie est algébrique.*
2. *Une extension L/K est finie si et seulement si il existe $\alpha_1, \ldots, \alpha_n$ algébriques sur K tels que $L = K(\alpha_1, \ldots, \alpha_n)$.*
3. *La composée de deux extensions algébriques est algébrique.*
4. *Si L/K est une extension algébrique, tout morphisme $\sigma : L \to L$ sur K est bijectif.*
5. *Si L/K est une extension quelconque, l'ensemble L' des élémetnts de L algébriques sur K est un sous-corps de L.*

On fixe un corps de base K.

Définition

Un corps de rupture pour $P \in K[T]$ est une extension L/K munie d'un $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

Proposition

Si $P \notin K$, il existe un corps de rupture L pour P sur K.
Supposons P irréductible. Soit L'/K une autre extension et $\alpha' \in L'$ tel que $P(\alpha') = 0$. 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.

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

Définition

- *Un polynôme $P \in K[T]$ se décompose sur une extension L/K en produit de facteurs linéaires s'il existe $\alpha_1, \ldots, \alpha_d \in L$ et $c \in K$ avec*

$$P = c(T - \alpha_1) \cdots (T - \alpha_d).$$

- *L'extension L/K est un corps de décomposition pour P si, en plus, $L = K(\alpha_1, \ldots, \alpha_d)$.*

Proposition

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

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.*

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.

Définition

Une extension algébrique L/K est normale si pour corps M contenant L et tout morphisme d'extensions $\sigma : L \longrightarrow M$, on a $\sigma(L) \subset L$.

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

Proposition

1. *Une extension algébrique L/K est normale si et seulement si tout $P \in K[T]$ irréductible avec une racine dans L se décompose en produit de facteurs linéaires.*
2. *Une extension finie est normale si et seulement si c'est le corps de décomposition d'un polynôme.*

Définition

Soit L/K une extension algébrique.

- *$\alpha \in L$ est séparable sur K si $P'_\alpha(\alpha) \neq 0$.*
- *L/K est séparable si tout $\alpha \in L$ est séparable sur K.*

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 si et seulement si P_α est séparable.

Proposition

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

Dans le second cas, on dit parfois que le nombre de morphismes distincts $L \to M$ est le **degré de séparabilité** de L sur K et on le note $[L:K]_s$. On écrit aussi $\deg_s(\alpha) = [K(\alpha):K]_s$.

Théorème (de l'élément primitif)

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

En fait, il existe toujours $\alpha \in L$ tel que $[L : K]_s = \deg_s(\alpha)$.

Remarquons aussi que si K est de caractéristique nulle ou fini, toute extension algébrique est séparable.

Définition

Une extension algébrique L/K est galoisienne si et seulement si elle est normale et séparable.

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.

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.

Attention : certains auteurs donnent une définition différente du groupe de Galois dans le cas d'extension non-galoisienne.

Proposition

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

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.

Théorème

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

1. *L/K est galoisienne si et seulement si $K \tilde{\to} L^G$.*
2. *L/K est galoisienne finie si et seulement si il existe un sous-groupe fini $H \subset G$ tel que $K \tilde{\to} L^H$. Et alors, $H = G$.*

Corollaire (Théorème de Galois)

Soit L/K une extension galoisienne finie et $G := Gal(L/K)$. Alors, les applications

$$M \mapsto H := Gal(L/M) \quad \text{et} \quad H \mapsto M := L^H$$

établissent une bijection décroissante entre les extensions intermédiaires M et les sous-groupes H de G.

Proposition

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

- J.-P. Lafon, *algèbre commutative, Langages géométriques et algébriques*. Collection Enseignement des sciences, 24. Hermann (1977)
- S. Lang, *Algebra*. Addison-Wesley, Reading, Massachusets (1965)