Leçon 125 : Extension de corps - Applications

Cadre :

1. Généralités. — On suppose connus les notions et résultats simples sur les groupes, anneaux, corps et espaces vectoriels. .
Hypothèse : Sauf dans la dernière partie, on considère uniquement des corps commutatifs.

1. *Quelques rappels utiles.* — :

- Pro :Un sur-corps m de k est un k-espace vectoriel. On note $[m : k]$ sa k-dimension.
- The : théorème des bases télescopiques.
- Pro : $k[X]/f(X)$ où $f(X) \in k[X]$ est un k-e.v.
- Pro : tout morphisme de corps est injectif.

2. *Définitions et propriétés.* — On considère deux corps emboîtés $k \subseteq K$.

- Def : *Anneaux engendré par une partie* $A \subseteq K$. C'est un sur-anneau de k et un sous-anneau de K. On le note $k[A]$.
  Il se définit "par le haut" comme l'intersection de tous les anneaux de K contenant A et k, dont par exemple K.
  Il se définit "par le bas" comme l'ensemble des éléments construits en un nombre fini d'opérations de multiplications et d'additions faisant intervenir des éléments de $A \cup k$.
- Def : *Corps engendré par une partie* $A \subseteq K$. Il correspond au corps des fractions de $k[A]$.
  Il se définit "par le haut" comme l'intersection de tous les corps de K contenant A et k, dont par exemple K.
  Il se définit "par le bas" comme l'ensemble des éléments construits en un nombre fini d'opérations de multiplications et d'additions faisant intervenir des éléments de $A \cup k \cup A^{-1}$, où A^{-1} désigne l'ensemble des inverses des éléments non nuls de A.
  C'est un sur-corps de k et un sous-corps de K. On le note $k(A)$.
- Pro : Nous avons $Vect(A) \subseteq Vect(\{a^n \, tq \, a \in A \, , n \in N\}) \subseteq k[A] \subseteq k(A) \subseteq K$.
- Pro : Pour toutes parties S et T de K, nous avons $k[S \cup T] = k[S][T]$ et $k(S \cup T) = k(S)(T)$.

2. Cas de la dimension finie $[m : k]$ **- Extension algébrique finie.** —

1. *Extension algébrique m de k à l'intérieur d'un sur-corps global K.* — On a vu comment engendrer un corps intermédiaire à partir d'une partie d'un sur-corps. A contrario, nous pouvons partir d'un corps intermédiaire comme ci-après.

Pour toute extension m/k de k-dimension finie n nous avons :

- Pro : m est de la forme $k(A)$ avec $A \subseteq K$ finie : il suffit de prendre pour A une k-base de l'e.v. m/k pour avoir alors l'inclusion $k(A) \subseteq Vect(A)$ qui complète l'égalité.
- Pro : chaque élément de $k[A] - k$ a un inverse dans $k[A]$ de sorte que $k(A) = k[A]$. En effet, la famille $(1, a, a^2, \cdots, a^n)$ est forcément liée, ce qui permet de construire un inverse de a qui est un polynôme en a.
- Pro : tout élément de m est racine d'un polynôme à coefficient dans k : on dit que cet élément est "algébrique sur k". Il y a donc une équivalence entre la dimension finie de m/k et le caractère algébrique sur k des éléments de m.
- Rem : Cas particulier de l'extension simple : $k(\{a\})$ où $a \notin k$ mais $a \in K$. On la note $k(a)$.

Exe : $k = Q$, $K = C$ et $m = Q + \sqrt{2}Q = Q(\sqrt{2}) = Q[\sqrt{2}]$
On a toujours $Vect(a) \subseteq k(a)$ donc $Q + \sqrt{2}Q = Q(\sqrt{2}) \subseteq Q[\sqrt{2}]$. Par ailleurs $(\sqrt{(2)})^{-1} = 1/2\frac{\sqrt{(2)}}{2} \in Vect(\sqrt{(2)})$, ce qui donne l'inclusion inverse.

2. *Extension algébrique de k par création et adjonction de racines.* — *Adjonction d'une racine*

- si $f(X) \in k[X]$ est irréductible (et donc en particulier est sans racine dans k), alors (f) est maximal et $k[X]/f(X)$ est un corps.
- Il vérifie que, si on note $\alpha = [X]$ alors $f(\alpha) = 0$.
- $[m : k] = deg(f)$
- on a $k \subseteq m$ via l'injection canonique d'un anneau dans son anneau des polynômes.
- *Nota :* on a donc "fabriqué" un nouvel élément α et un nouveau corps m de la forme $k(\alpha)$. Dans ce nouveau corps, f a une racine et n'est donc plus irréductible : on parle de "corps de rupture de f".

Corps de rupture Le degré de $m = k(a)$, noté $[m : k]]$, est $n = degré(f)$ et $(1, a, a^2, \cdots, a^{n-1})$ est une base canonique de m en tant que k-e.v On peut tout autant réaliser cette rupture pour un polynôme quelconque dont un des facteurs irréductible ne serait pas de degré 1.

Pro : adjonctions successives On peut retrouver en le construisant le cas général de $k(A)$ de dimension finie vu dans le cas particulier d'une extension au sein d'un sur-corps préexistant. Construire ou fabriquer un élément revient à identifier un polynôme irréductible et à en réaliser sa rupture. Ceci peut être fait en partant de $k(a_1)$ au lieu de k, puis de $k(a_1)(a_2)$ et ainsi de suite. En gardant au contraire le même polynôme de départ on arrive à le scinder entièrement. Le dernier des sur-corps obtenu par la dernière rupture à faire est alors appelé 'corps de factorisation de f' ou 'corps des racines de f'. *Nota :* si a et b ont été construits en dehors de k par des polynômes sur $k[X]$ on a : $k(a, b) = k(a)(b) = k[a][b] = k[b][a]$

Pro : Les extensions par rupture ou factorisation sont algébriques

Pro : Unicité et dimension du corps de factorisation d'un polynôme La dimension du corps de factorisation est inférieure ou égale à $n!$.

The : Théorème d'extension des isomorphismes Etant donnés des corps k_1 et k_2, un isomorphisme ϕ entre eux et un polynôme $f(X) \in k_1[X]$, on associe naturellement ϕf à f. Etant alors donnés des corps de factorisation Σ_1 et Σ_2 de f et de ϕf, on a un isomorphisme entre Σ_1 et Σ_2 selon le carré commutatif suivant :

Exemples :

- Exe : $f(X) = (X^2 + X + 1)$ sa rupture donne sa décomposition. On ne peut pas distinguer j de $j2$ par ce procédé de création de racine.
- Exe : $f(X) = X^3 - 2$ La première rupture est d'ordre 3 et permet de créer un élément parmi $\{\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2\}$ sans que l'on puisse dire laquelle vu du procédé qui ne les distingue pas. La deuxième et dernière rupture est d'ordre deux et crée les deux conjugués manquants. Au total la dimension est de 6.

Pro Lien avec les polynômes :

Nous avons vu que :

- tout polynôme de $k[X]$ irréductible sur k donne lieu à la création d'un "corps de rupture" contenant au moins une racine. Ces corps ont pour dimension le degré du polynôme et sont isomorphes entre eux.
- la construction peut aller jusqu'à la décomposition totale de ce polynôme et on parle de "corps des racines" qui est unique à un isomorphisme près. Ce corps a une dimension finie majorée par $n!$.
- A l'inverse, toute extension finie peut être associée à l'adjonction de racines d'un polynôme. Nous verrons que, sous certaines conditions, l'adjonction d'une racine unique, dite élément primitif, suffit.
- Un élément est dit algébrique sur k s'il est solution d'un polynôme de $k[X]$. Une extension est dite algébrique si tous les éléments de celle-ci sont algébrique. On a donc que tout élément d'une extension finie est algébrique.
- L'inverse est faux car on peut établir une chaîne infinie d'adjonctions, par exemple basé sur $\sqrt{p}$ où p parcours les nombres premiers.

3. Clôture algébrique. — *Définitions 10 :*

- Un élément de M sur-corps de k est dit "algébrique sur k" s'il est racine d'un polynôme à coefficients dans k.
- Une extension est dite "extension algébrique de k" dès lors que tous ses éléments sont algébriques sur k. On peut alors la construire par une série d'adjonctions de racines.
- Un corps est dit "algébriquement clos" si tout polynôme y est scindé. Dès lors il coïncide avec toute extension algébrique de lui-même.
- Si on considère le corps minimal par inclusion parmi les corps clos contenant le corps k, on a affaire à une (la) "Clôture algébrique de k".

Propriétés :

- Pro : Toute extension de dimension finie est algébrique.
- The : *Théorème de l'élément primitif :* Si k est de caractéristique 0, toute extension finie est en fait isomorphe à une extension $k[\alpha]$.
- Pro : Une extension algébrique peut ne pas être de dimension finie mais la dimension reste dénombrable.
  - Exe : pour p_n le n-ième nombre premier et $Fn = Q[\sqrt{(p_1)}, \cdots, \sqrt{(p_n)}]$,si $F = \cup Fn$, F est algébrique de dimension infinie.
  - Rem : R étant non dénombrable, il existe donc des éléments non algébriques sur Q.
- Il y a équivalence entre :
  - M est algébriquement clos
  - Tout polynôme de $M[X]$ admet une racine.
  - M n'admet pas d'extension propre de dimension finie.
- Le sous-ensemble d'un sur-corps K de k qui contient ceux des éléments de K qui sont algébriques sur k est un corps extension de k. On le note K_{k-Alg}.
- The : *Théorème de Steinitz* Tout corps peut être plongé dans un sur-corps algébriquement clos, noté Ω.
- *Existence d'une clôture algébrique* Le corps Ω_{k-Alg} est algébriquement clos. Il est algébrique sur k. C'est sa clôture.

Exemple : $k = Q$, $\Omega = C$ et $\Omega_{k-Alg} = Q_{Alg}$ le corps des entiers algébriques.
Pro : La clôture algébrique de Q est infinie dénombrable.
Développement : *Proposition 13 : théorème dit fondamental de l'algèbre :* C est algébriquement clos.

Cor : Les polynômes irréductibles de $R[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine réelle.

App : Toute matrice de $Mn(C)$ est trigonalisable.
Rem : Q et F_q admettent des polynômes irréductibles de degré aussi grand que l'on veut. (On pourra considérer $X^n - 2$ pour Q et YYYY).

4. Extension transcendante. — *Définition et propriétés :*

- Def : Un élément a d'un sur-corps K est dit transcendant s'il n'existe aucun polynôme de $k[X]$ dont il est racine.
- Rem : Par définition donc, cet élément n'a pas pu être fabriqué par des procédés algébriques et doit être fourni par un autre moyen (comme par exemple la topologie dans le cas de R).
- Pro : a est transcendant ssi $[k(a) : k]$ est infini.
- Rem : Il existe alors un morphisme entre $k[X]$ et $k[a]$: on obtient une interprétation très éclairante de l'anneau des polynômes (notamment du mystérieux "X") et de son corps des fractions ! On obtient $k(a)$ comme corps des fractions de l'anneau intègre $k[a]$.

Proposition : Il existe des réels transcendants. L'ensemble de ceux-là est non dénombrable. Développement e est transcendant.

Exemples : $Q(\}\sqrt{2}, 2\sqrt{2}+4\})$ et $Q(\}\sqrt{2}, 2\sqrt{3}\})$

Enfin $m = k(a_1, \cdots a_n) = k(a_1)\cdots(a_n)$ et $[m : k] \leq \prod deg(\Pi_{a_k})$
x. Exercice : construire un polynôme minimal de $Q[\sqrt{2}, \sqrt{3}]$

5. Eléments de la théorie de Galois. — x. Extension normale. Extension galoisienne.

x. k-automorphismes. Groupes de Galois. Montrer que les racines dansent.

14. Th. $Gal(L/K) <= [L : K]$

doutes : extension monogène (p premier) ? caracteristique ? corps parfaits ?

Développement 1 : ***e est transcendant***

Développement 2 : ***constructions à l règle et au compas. Trois grands problèmes de l'Antiquité***

Développement 3 : ***Polygones à n côtés*** **Développement 4 :** ***th. de d'Alembert / Gauss démontré par la théorie de Galois***

.

Sources :

- *D. Perrin "Algèbre Générale"*
- *Dany-Jack Mercier "Corps Finis"*
- *J. Calais "Extension des corps - Théorie de Galois"*
- *Jeanneret - Lines "Invitation à l'Algèbre"*

November 20, 2017

Bruno Nitrosso, EPP et indépendant