125 : Extensions de corps. Exemples et applications.

Pandou

10 mars 2022

1 Corps et extensions

1.1 Définitions

Définition 1. *Soit K et L deux corps. On dit que L est une extension de K si K est isomorphe à un sous-corps de L. On note L/K cette extension.*

Définition 2. *Soit L/K une extension de corps, on appelle degré de L sur K, et on note $[L : K]$, la dimension de L en tant que K-espace vectoriel.*

Exemples 3 :
- $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré 2.
- $\mathbb{R}$ est une extension de $\mathbb{Q}$ de degré infini.
- Si K est un corps, $K(X)$ est une extension de K de degré infini.

Théorème 4 (Base téléscopique)**.** *Soit L/K et M/L deux extensions de corps. Alors, M/K est finie si, et seulement si, L/K et M/L sont finies et dans ce cas,*

$$[M : K] = [M : L] \times [L : K]$$

Exemple 5 : Soit p un nombre premier et L/K, M/L deux extensions de corps. Si M/L est finie de degré p, alors $M = L$ ou $L = K$.

Définition 7. *Soit L/K une extension de corps et A une partie de L, on note $K(A)$ le plus petit sous-corps de L contenant K et A et $K[A]$ le plus petit sous-anneau contenant K et A.*

Exemple 8 : Si $\alpha \in L$, alors

$$K(\alpha) = \{R(\alpha), R \in K(X)\} \qquad \text{et} \qquad K[\alpha] = \{P(\alpha), P \in K[X]\}$$

1.2 Algébricité

Définition 9. *Soit L/K une extension, $\alpha \in L$ et $\mathrm{ev}_\alpha : K[X] \longrightarrow K[\alpha]$ tel que $\mathrm{ev}_{\alpha|K} = \mathrm{Id}_K$ et $\mathrm{ev}_\alpha(X) = \alpha$. Alors,*
- *Si ev_α n'est pas injectif, on dit que α est algébrique sur K. Le générateur unitaire de $\mathrm{Ker}(\mathrm{ev}_\alpha)$ est appelé polynôme minimal de α.*
- *Si ev_α est injectif, on dit que α est transcendant sur K.*

Exemples 10 :
- $\sqrt{2}$, i sont algébriques sur $\mathbb{Q}$, de polynômes minimaux respectifs $X^2 - 2$ et $X^2 + 1$.
- $X \in K(X)$ est transcendant sur K.
- e et π sont transcendants sur $\mathbb{Q}$.

Remarque 11 : Si α est transcendant sur K, alors

$$K[\alpha] \simeq K[X] \qquad \text{et} \qquad K(\alpha) \simeq K(X)$$

Théorème 12. *Soit L/K une extension et $\alpha \in L$. Alors, on a équivalence entre :*
1. *α est algébrique sur K.*
2. *$K[\alpha] = K(\alpha)$.*
3. *$K(\alpha)/K$ est finie.*

Dans ces cas, $\big[K(\alpha) : K\big]$ est le degré du polynôme minimal de α, appelé degré de α.

Définition 13. *On dit que L/K est algébrique si tout élément $\alpha \in L$ est algébrique sur K.*

Remarque 14 : Toute extension finie est algébrique. La réciproque est fausse, nous le verrons en remarque sur théorème suivant.

Théorème 15. *Soit L/K une extension, alors*

$$\{x \in L, x \text{ est algébrique sur } K\}$$

est un sous-corps de L.

Remarque 16 : $\overline{\mathbb{Q}} = \{x \in \mathbb{C}, x \text{ est algébrique sur } \mathbb{Q}\}$ est algébrique, mais n'est pas fini sur $\mathbb{Q}$.

1.3 Extension quadratique

Proposition 17. *Soit $d \in \mathbb{N}$, alors*

$$\big[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}\big] \leqslant 2$$

et on a égalité si, et seulement si, $\sqrt{d} \notin \mathbb{N}$.

Remarque 18 : Il existe d'autres extensions de degré 2, par exemple $\mathbb{Q}(i)$, mais on est pas loin du vrai compte.

Théorème 19. *Soit $L/\mathbb{Q}$ une extension quadratique (ie de degré 2), alors il existe $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteurs carrés tel que*

$$L \simeq \mathbb{Q}(\sqrt{d})$$

Proposition 20. *Soit L/K une extension de corps de caractéristique $\neq 2$. Alors, $[L : K] = 2$ si, et seulement si, il existe un élément Δ de K qui admet une racine carrée δ dans L et $L = K(\delta)$.*

2 Extensions et polynômes

On fixe un polynôme $P \in K[X]$.

2.1 Corps de rupture et de décomposition

Théorème 21 (Définition)**.** *Si P est irréductible, il existe une extension L/K engendrée par une racine de P. De plus, cette extension est unique à isomorphisme près.*
Un tel corps est appelé corps de rupture de P sur K.

Remarque 22 : P n'est pas toujours scindé dans son corps de rupture : $P = X^3 - 2$ dans $\mathbb{Q}$: $L = \mathbb{Q}(\sqrt[3]{2})$.

Remarque 23 : P est irréductible sur K si, et seulement si, K n'a pas d'extension de degré au plus $\frac{d}{2}$ dans lequel P a une racine.

Théorème 24 (Définition)**.** *P n'est plus nécessairement irréductible, alors il existe une extension L/K, unique à isomorphisme près, telle que :*

- *P est scindé dans $L[X]$.*
- *$L = K(\alpha_1, ..., \alpha_n)$ où $\alpha_1, ..., \alpha_n$ sont les racines de P.*

L est appelé corps de décomposition de P sur K.

Exemple 25 : Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$.

Proposition 26. *Si P est de degré n et si L/K est le corps de décomposition de P sur K, alors $[L : K]$ divise $n!$.*

2.2 Clôture algébrique

Définition 27. *On dit que K est algébriquement clos si tout polynôme non constant de $K[X]$ admet une racine dans K.*

Théorème 28 (D'Alembert-Gauss)**.** *$\mathbb{C}$ est algébriquement clos.*

Définition 29. *L/K est une clôture algébrique de K si on a*

- *L est algébriquement clos.*
- *L/K est algébrique.*

Exemple 30 : $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$.

Théorème 31 (Admis)**.** *Tout corps admet une clôture algébrique. De plus, deux clôtures algébriques de K sont K-isomorphes.*

Proposition 32. *Soit L un corps algébriquement clos et K un sous-corps de L, alors*

$$\overline{K} = \{x \in L, x \text{ est algébrique sur } K\}$$

est la clôture algébrique de K.

2.3 Application : Corps finis

Définition 33. *Soit K un corps, le générateur positif de $\mathrm{Ker}(\mathbb{Z} \longrightarrow K)$ est appelée caractéristique de K, notée $\mathrm{car}(K)$.*

Proposition 34. *Si K est un corps, alors $\mathrm{car}(K)$ est soit nul, soit un nombre premier.*

Proposition 35. *Si K est un corps fini, alors K est de caractéristique p non nulle et le cardinal de K est une puissance de p.*

Proposition 36. *Soit p un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments, noté $\mathbb{F}_p$.*

Théorème 37. *Soit p un nombre premier et $n \geqslant 1$, on note $q = p^n$.*
Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$, alors dans $\overline{\mathbb{F}_p}$, il y a un unique corps à q éléments.

Proposition 38. *Dans $\overline{\mathbb{F}_p}$, on a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si, et seulement si, n divise m.*

3 Problèmes impossibles

3.1 Constructibilité

On munit $\mathbb{R}^2$ de sa structure d'espace affine orienté canonique.

Définition 39. *Soit $X \subset \mathbb{R}^2$ de cardinal au moins 2. On distingue deux constructions à la règle et au compas :*

1. *Les droites affines (AB) pour $A \neq B$ des points de X.*
2. *Les cercles centrés en un point $A \in X$ et passant par un point $B \neq A \in X$.*

On dit que M est constructible en un pas à partir de X si, et seulement si, M est un point d'intersection de $1. \cap 1.$, $2. \cap 2.$ ou $1. \cap 2.$.

Définition 40. *On note $\mathcal{C}_0 = \{(0,0), (0,1)\}$, puis $\mathcal{C}_i$ l'ensemble des points constructibles en un point à partir de $\mathcal{C}_{i-1}$.*
On dit qu'un point $M \in \mathbb{R}^2$ est constructible lorsque $\exists n \in \mathbb{N}, M \in \mathcal{C}_n$.

Proposition 41. *Soit M, A et B des points constructibles. Alors,*

1. *Le symétrique de M par rapport à O est constructible.*
2. *Le milieu de $[A,B]$ est constructible. Plus généralement, la médiatrice de $[A,B]$ est constructible.*
3. *La perpendiculaire à (AB) passant par M est constructible.*
4. *La parallèle à (AB) passant par M est constructible.*

Définition 42. *On dit que $x \in \mathbb{R}$ est constructible lorsque $(0,x)$ est constructible. On note E l'ensemble des nombres constructibles.*

Proposition 43. *E est une extension de $\mathbb{Q}$ stable par la racine carrée.*

Lemme 44. *Soit F un sous-corps de $\mathbb{R}$, on note $\mathcal{D}$ l'ensemble des droites passant par deux points de F^2 et $\mathcal{C}$ l'ensemble des cercles centrés en un point de F^2 et de rayon égal à la distance entre deux points de F^2. Alors,*

1. *Si $d \in \mathcal{D}$, alors d a une équation cartésienne à coefficients dans F.*
2. *Si $c \in \mathcal{C}$, alors c a une équation cartésienne à coefficients dans F.*

DEVELOPPEMENT 1

Proposition 45. *On reprend les notations du lemme précédent. Soit $d_1, d_2 \in \mathcal{D}$ deux droites et $\gamma_1, \gamma_2 \in \mathcal{C}$. Alors,*

1. *Si d_1 et d_2 sont sécantes, alors leur point d'intersection est dans F^2.*
2. *Si $M \in d_1 \cap \gamma$, alors $M \in F^2$, ou il existe une extension quadratique K/G telle que $M \in K^2$.*
3. *Si $M \in \gamma_1 \cap \gamma_2$, alors $M \in F^2$, ou il existe une extension quadratique K/G telle que $M \in K^2$.*

Théorème 46. *Soit $t \in \mathbb{R}$, alors t est constructible si, et seulement s'il existe une tour finie d'extensions quadratiques $\mathbb{Q} < F_1 < ... < F_p$ (ie F_{i+1}/F_i est quadratique) tel que $t \in F_p$.*

Applications 47 :

- On ne peut pas dupliquer le cube.
- On ne peut pas trissecter l'angle.

Remarque 48 : La quadrature du cercle est aussi impossible.

Remarque 49 : Une extension de $\mathbb{Q}$ de degré 4 n'est pas nécessairement issue d'une tour d'extensions quadratiques. Par exemple, examiner $X^4 - 4X + 2$.

3.2 Intégration formelle

Définition 50. *Soit K un corps. Une dérivation de K est une application $\partial : K \longrightarrow K$ telle que*

$$\partial(x+y) = \partial x + \partial y \qquad et \qquad \partial(xy) = \partial(x)y + x\partial(y)$$

On dit que (K, ∂) est un corps différentiel.

Proposition 51. *$\mathrm{Ker}(\partial)$ est un sous-corps de K, noté K_0 et appelé corps des constantes de K.*

Exemple 52 : $\mathbb{Q}(X)$ est un corps différentiel, muni de la dérivation usuelle, dont le corps des constantes est $\mathbb{Q}$. Plus généralement, le corps des constantes de K contient le sous-corps premier de K.

Proposition 53. *On a les résultats suivants, pour $x \in K$ et $y \neq 0$:*

1. $0, 1 \in K_0$.
2. $\partial(-x) = -\partial x$.
3. $\partial\left(\dfrac{x}{y}\right) = \dfrac{y\partial x - x\partial y}{y^2}$.
4. $\partial(x^n) = nx^{n-1}\partial x$, $n \in \mathbb{Z}$.

Définition 54. *Soit L/K une extension de corps. On dit que L/K est une extension de corps diférentiels si leurs dérivations coincident sur K.*

Définition 55. *Soit L/K une extension de corps différentiels et $u \in L$. On dit que*

1. *u est exponentiel sur K lorsqu'il existe $x \in K$ tel que $\partial u = u\partial x$. Une extension de la forme $K(u)$ est une extension exponentielle de K si u est transcendant sur K.*
2. *u est logarithmique sur K lorsqu'il existe $x \in K$ tel que $\partial u = \dfrac{\partial x}{x}$. Une extension de la forme $K(u)$ est une extension logarithmique de K si u est transcendant sur K.*

Une extension élémentaire est une extension de la forme $K(u_1, ..., u_n)$ tel que u_{i+1} est soit exponentielle, soit logarithmique, soit algébrique sur $K(u_1, ..., u_i)$.

Remarque 56 : Un élément exponentiel n'est pas nécessairement transcendant. Par exemple, si $h \in \exp\big(\log(x)/2\big) \in \mathbb{Q}(x, u_1, u_2)$ avec $u_1 = \log(x)$ et $u_2 = \exp\big(u_1/2\big)$, alors,

- u_1 est logarithmique sur $\mathbb{Q}(x)$.
- u_2 est exponentiel sur $\mathbb{Q}(x, u_1)$.
- Mais, u_2 est algébrique sur $\mathbb{Q}(x)$.

Proposition 57. *Soit F un corps différentiel et $F(u)$ une extension logarithmique qui a même sous-corps des constantes. Soit $P(u) \in F[u]$ de degré > 0. Alors, on a*

1. *$\partial\big(P(u)\big) \in F[u]$.*
2. *Soit a_n le coefficient dominant de $P(u)$:*

$$\deg \partial\big(P(u)\big) = \begin{cases} \deg\big(P(u)\big) - 1 & si\ a_n \in F_0 \\ \deg\big(P(u)\big) & sinon \end{cases}$$

Proposition 58. *Soit F un corps différentiel et $F(u)$ une extension exponentielle qui a même sous-corps des constantes. Soit $P(u) \in F[u]$ de degré > 0. Alors, on a*

1. $\partial\big(P(u)\big) \in F[u]$.
2. $\deg \partial\big(P(u)\big) = \deg\big(P(u)\big)$.
3. *$P(u)$ divise $\partial\big(P(u)\big)$ si, et seulement si, $P(u)$ est un monôme.*

Proposition 59. *Soit F un corps différentiel et $F(u)$ une extension algébrique de F, alors il existe un unique prolongement de la dérivation de F en une dérivation de $F(u)$.*

DEVELOPPEMENT 2

Théorème 60. *Soit K un corps différentiel et $f \in K$. On suppose qu'il existe y dans une extension élémentaire de K avec même sous-corps des constantes tel que $\partial y = f$, alors il existe $v_0, v_1, ..., v_m \in K$ et des constantes $\lambda_1, ..., \lambda_m \in K_0$ tels que*

$$f = \partial v_0 + \sum_{i=1}^{m} \lambda_i \frac{\partial v_i}{v_i}$$

Autrement dit, on a formellement,

$$\int f = v_0 + \sum_{i=1}^{m} \lambda_i \log(v_i)$$

Application 61 : Soit $f, g \in \mathbb{C}(x)$, alors une primitive élémentaire de $f\exp(g)$ est de la forme $h\exp(g)$ avec $h \in \mathbb{C}(x)$. On travaille pour cela dans le corps différentiel $\mathbb{C}(x)(t)$ avec $t = \exp(g)$.

Conséquence 62 : $\exp(x^2)$ n'a pas de primitive élémentaire.

4 Annexe

Ajout des dessins de constructions à la règle et au compas.

Références :

- Geddes, Czapor, Labahn, Algorithms for Computer Algebra.
- Gourdon, Algèbre.
- Gozard, Théorie de Galois.
- Perrin, Cours d'algèbre.
- Tauvel, Algèbre pour l'agrégation.
- Tauvel, Corps commutatifs et théorie de Galois.