Extensions de corps. Exemples et applications.

125

K, L et M sont des corps commutatifs. K[α] (K(α)) désigne le plus petit anneau (corps) contenant K et α.

I - Premières définitions [LAN], [PER], [GOB]

Déf 1: (Extension)
On appelle extension d'un corps K, notée K ⊂ L, tout corps L muni d'un morphisme de K dans L.

Ex 2: $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.

Déf 3: (Degré)
Soit K ⊂ L, alors L est un K-espace vectoriel. On appelle degré de l'extension : $\dim_K L = [L:K] \in \mathbb{N}^* \cup \{\infty\}$.
- Si $[L:K] < \infty$, K ⊂ L est finie.
- Si $[L:K] = \infty$, K ⊂ L est infinie.

Ex 4: $[\mathbb{R}:\mathbb{Q}] = \infty$, $[\mathbb{Q}\sqrt{2}:\mathbb{Q}] = 2$.

Th 5: (Base télescopique).
Soit K ⊂ L, L ⊂ M, deux extensions. $\{x_i\}_{i\in I}$ base de L sur K, $\{y_j\}_{j\in J}$ base de M sur L, alors $\{x_i y_j\}_{i,j\in I\times J}$ est une base de M sur K.
On en déduit : $[M:K] = [M:L][L:K]$.

Ex 6: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{2})] = 2$
donc $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

Déf 7: (éléments algébriques).
Soit K ⊂ L, α ∈ L. On considère le morphisme $\varphi : K[T] \to L$, $P \longmapsto P(\alpha)$.
- α est transcendant si φ est injectif, i.e. : Aucun polynôme de K[T] ne s'annule en α.
- α est algébrique sinon. Alors $\ker(\varphi) = (P)$, P irréductible et unitaire, on l'appelle polynôme minimal de α, noté P_α.

Déf 8: (Extension algébrique).
- K ⊂ L est algébrique si tous les éléments de L sont algébriques.
- K ⊂ L est transcendante sinon.

Ex 9: i est algébrique sur $\mathbb{Q}$ car racine de T^2+1, donc $\mathbb{Q}(i)$ est algébrique. π est transcendant sur $\mathbb{Q}$ donc $\mathbb{Q}(\pi)$ est transcendant.

Prop 10: (Degré et polynôme minimal).
α ∈ L. Si α est algébrique sur K, alors $[K(\alpha):K] = d^\circ P_\alpha$.

Ex 11: $T^2 - 2$ polynôme minimal de $\sqrt{2}$ dans $\mathbb{Q}$, donc $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$.

Prop 12: Toute extension finie est algébrique.

Ex 13: $[\mathbb{C}:\mathbb{R}] = 2 \Rightarrow \mathbb{R} \subset \mathbb{C}$ est algébrique.

⚠ Réciproque fausse : $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique sur } \mathbb{Q}\}$.
A est algébrique sur $\mathbb{Q}$, pas finie sur $\mathbb{Q}$.

Déf 14: (Norme et Trace).
Soit K ⊂ L, α ∈ L. On définit : $L_\alpha : L \longrightarrow L$, K linéaire, $s \longmapsto s\alpha$.

- On appelle polynôme caractéristique de x sur K :
$P_{L/K,x}(T) = \det_K(xI_L - TI_L)$.
- on appelle trace et norme de x sur K la trace $(\mathrm{Tr}_{L/K}(x))$ de L_x et le déterminant $(N_{L/K}(x))$ de L_x.

Ex 15 : $z = x + iy \in \mathbb{C}$,

$\mathrm{Mat}(\mathbb{C}_z) = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$ $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2x \cdot N_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2 = |z|^2$

$P_{\mathbb{C}/\mathbb{R};z}(T) = T^2 - 2xT + x^2 + y^2$

II - Types d'extensions [PER], [ERA], [OCR], [LAN]

Déf 16 : (Corps de ruptures).
Soit $P \in K[T]$ irréductible. $K \subset L$ est appelé corps de rupture de P sur K si $L = K(\alpha)$, avec $P(\alpha) = 0$.

Ex 17 : $\mathbb{C}$ est un corps de rupture de T^2+1 sur $\mathbb{R}$.

Th 18 : $P \in K[T]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.
Δ Un corps de rupture de P ne contient pas toutes les racines de P.

C - Ex 19 : $T^3 - 2 \in \mathbb{Q}[T]$ est irréductible sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de P, mais ne contient pas $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$

Déf 20 : (Corps de décomposition)
Soit $P \in K[T]$ irréductible. On appelle corps de décomposition de P sur K une extension L de K telle que :
1) Dans $L[T]$, P est produit de facteurs de degré 1.
2) L est minimal pour cette propriété.

Ex 21 : $P(T) = T^3 - 2$ irréductible sur $\mathbb{Q}$,
$\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de P sur $\mathbb{Q}$.

Th 22 : $P \in K[T]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.

Déf 23 : (Algébriquement clos)
K est algébriquement clos si tout polynôme de $K[X]$ de degré supérieur ou égal à 1 admet une racine dans K.

Déf 24 : (Clôture algébrique).
L est la clôture algébrique de K si L est algébriquement clos et algébrique sur K,

Ex 25 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Th 26 : Tout corps K admet une clôture algébrique, unique à isomorphisme près.

Déf 27 : (Normale)
Une extension $K \subset L$ est normale si elle est algébrique et, $\forall a \in L$, P_a a toutes ses racines dans L.

Prop 28 : Si L est un corps de décomposition de $P \in K[T]$ sur K, alors $K \subset L$ est normale.

Déf 30 : - $P \in K[T]$ irréductible, P est séparable sur K si ses racines dans un corps de décomposition sont distinctes
- $a \in K$ est séparable sur K si P_a l'est.
- $K \subset L$ est séparable si $\forall \lambda \in L$, λ est séparable sur K.

Prop 31 : K de caractéristique 0 ou corps fini, alors tout $P \in K[T]$ irréductible est séparable sur K.

Ex 32 : (Inséparabilité).
$p \in \mathbb{N}$ premier, $K = \mathbb{F}_p(T)$, $\bar{K}$ clôture algébrique de K, $P(X) = X^p - T$ est irréductible et inséparable.

Déf 33 : (Primitif).
$\gamma \in L$ est primitif de L sur K si $L = K(\gamma)$.

Th 34 : Toute extension finie L d'un corps K de caractéristique nulle admet un élément primitif. DEV 1 [FRA]

Ex 35 : $\mathbb{Q}(i, j, \sqrt{2}) = \mathbb{Q}(i + j + \sqrt{2})$.

Déf 36 : $K \subset L$ normale et séparable est dite galoisienne.
On appelle groupe de Galois de L sur K : $G = \mathrm{Aut}_K(L)$.

Prop 37 : $|G| = [L : K]$.

Prop 38 : $K \subset K' \subset L$, L galoisien sur K, alors L est galoisien sur K'.

Th 39 : $K \subset L$ galoisien de groupe de Galois G.
- Il y a bijection entre : $\{K'$ sous-corps de K contenant $L\}$ et $\{G'$ sous-groupe de $G\}$.
- K' sous-corps de L contenant K est galoisien sur K si et seulement si G' groupe de Galois de $K' \subset L$ vérifie : $G' \lhd G$.

II - Constructibilité à la règle et au compas. [PER], [GOB].

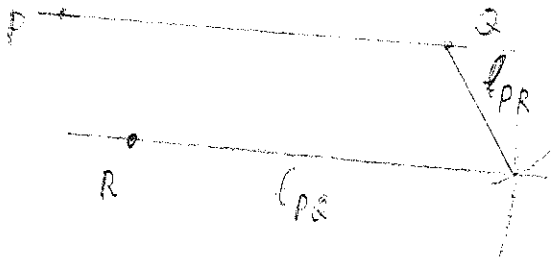
Déf 95 : Soit $A \subset \mathbb{R}^2$, $M \in \mathbb{R}^2$ est constructible en un pas si c'est l'intersection de droite ou de cercle à partir de A.
- M est constructible s'il existe $A_0 \subset \dots \subset A_n$ parties de $\mathbb{R}^2$, avec : - $A_0 = \{0, I\}$, - $M \in A_n$.
- $A_i = A_{i-1} \cup \{M_i\}$, où M_i est constructible en un pas à partir de M_{i-1}.

Th 41 : Soit α un réel constructible, alors $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$, $n \in \mathbb{N}$.

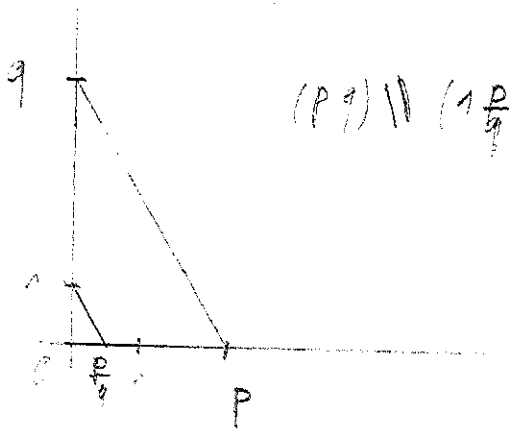
Appl 42 : Les 3 problèmes grecs, la duplication du cube, la trisection de l'angle et la quadrature du cercle sont impossibles. DEV 2 [PER]

Appl 43 : Un polygône régulier à n côtés est constructible si et seulement si n est de la forme : $n = 2^m p_1 \dots p_k$, $p_i = 2^{2^l} + 1$, $m, l \in \mathbb{N}$

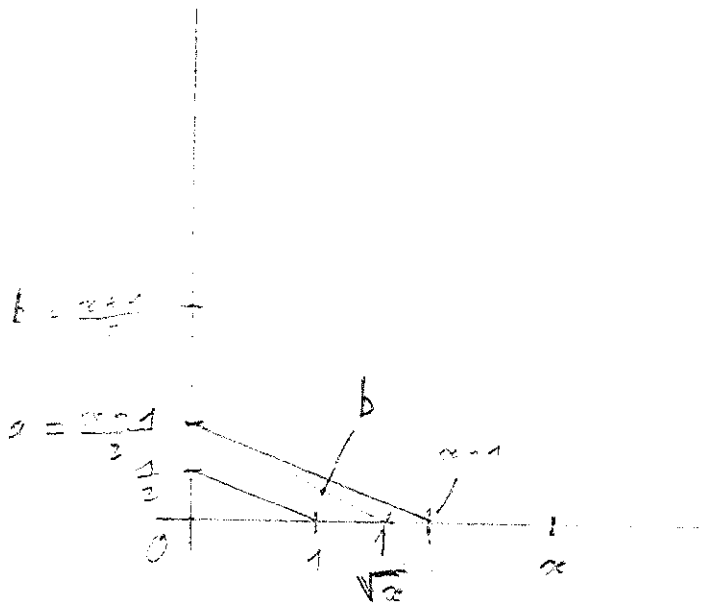
- Parallèle à une droite passant par un point.



- Construire $\frac{p}{q}$:



- Construire $\sqrt{x}$



Références : "Cours d'algèbre", Daniel Perrin [PER]

"Algèbre commutative", Rémi Goblot [GOB].

"Exercices de mathématiques pour l'agrégation", Francinou [FR

"Algebra", Lang [LAN]

Premier développement : Théorème de l'élément primitif

1er février 2016

Théorème 1 *Toute extension finie de caractéristique nulle admet un élément primitif.*

Démonstration

Soit $K \subset L$ une extension finie de caractéristique nulle.
Dans un premier temps on suppose qu'il existe $x, y \in L$ tels que : $L = K[x, y]$.
On note P_x et P_y les polynômes minimaux de x et y, de degrés respectifs m et n.
On considère M un corps de décomposition de P_x et P_y, et on note $x_2, \ldots, x_m$ les conjugués de x et $y_2, \ldots, y_n$ les conjugués de y dans M.

On sait que K est de caractéristique nulle, donc séparable.
Donc les racines de P_y sont deux à deux distinctes.
On pose alors $E := \{ \dfrac{x - x_i}{y - y_j} \ ; \ 1 \leqslant i \leqslant m, \ 2 \leqslant j \leqslant n \}$.
E est fini, de cardinal inférieur ou égal à $(m-1)(n-1)$, et comme K est de caractéristique nulle il contient une infinité d'éléments.
On peut donc prendre un t dans K^* tel qu'il ne soit pas dans E, et on pose : $z := x + ty$.

On pose $K' := K[z]$, et $F(X) := P_x(z - tX)$. On va montrer que $K' = L$.

D'abord, on remarque que $P_y \in K[X] \subset K'[X]$, et que F est la composée de deux polynômes de $K'[X]$.
P_y et F sont donc dans $K'[X]$, donc leur pgcd l'est également.

Calculons ce pgcd. Dans $M[X]$, F se décompose ainsi :

$$\begin{aligned} F(X) &= ((z - tX) - x) \prod_{i=2}^{m} ((z - tX) - x_i) \\ &= (x + ty - tX - x) \prod_{i=2}^{m} (x + ty - tX - x_i) \\ &= t(y - X) \prod_{i=2}^{m} (x - x_i + t(y - X)) \end{aligned}$$

et P_y ainsi :

$$P_y(X) = (X - y) \prod_{j=2}^{n} (X - y_j)$$

Donc $X - y$ divise F et P_y.

Par ailleurs, par choix de t, on a :

$$\forall\, 2 \leqslant i \leqslant m,\ \forall\, 2 \leqslant j \leqslant n, \quad x - x_i + t(y - y_j) \neq 0$$
$$\Longrightarrow\ \forall\, 2 \leqslant j \leqslant n, \quad F(y_j) \neq 0$$

Donc y est l'unique racine commune de F et P_y dans $M[X]$.
Donc $X - y = \gcd(F, P_y)$.
Donc $y \in K'$.

De même, $x \in K'$.
Donc $K' = L$, ie L admet z comme élément primitif.

On a ainsi démontré le cas où L est engendré par deux éléments.
Montrons par récurrence que : $\forall n \geqslant 2$, $L := K(x_1, \ldots, x_n)$ est monogène.

- Pour $n = 2$, cette proposition est vraie d'après ce qui précède.

- Soit $n \geqslant 2$, tel que la proposition soit vraie au rang n.
  On pose : $L := K(x_1, \ldots, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$.
  D'après l'hypothèse de récurrence, il existe $y \in L$ tel que $K(x_1, \ldots, x_n) = K(y)$.
  On a donc : $L = K(y)(x_{n+1}) = K(y, x_{n+1})$.
  D'après ce qui précède, il existe donc $z \in L$ tel que $K(y, x_{n+1}) = K(z)$.
  L est monogène, la propriété est donc vérifiée au rang n+1.

On a ainsi démontré le théorème.

Application : En appliquant la méthode utilisée dans la démonstration, on peut trouver $\alpha \in \mathbb{C}$ tel que $\mathbb{Q}(\alpha) = \mathbb{Q}(i, j, \sqrt{2})$:

Commençons par trouver z tel que $\mathbb{Q}(z) = \mathbb{Q}(i, \sqrt{2})$.
Le polynôme minimal de i est $P(X) = X^2 + 1$ de racines i et $-i$, et le polynôme minimal de $\sqrt{2}$ est $Q(X) = X^2 - 2$, de racines $\sqrt{2}$ et $-\sqrt{2}$.
Il faut donc trouver $t \in \mathbb{Q}^*$ tel que $i + t\sqrt{2} \neq -i - t\sqrt{2}$.
$t = 1$ convient. En posant $z = i + \sqrt{2}$, on a donc : $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(z)$.

Passons à α.
Le polynôme minimal de j est $R(X) = X^2 + X + 1$, de racines j et j^2, et le polynôme minimal de z est $(X^2 - 1)^2 + 8$ (admis), de racines z, $-z$, $\overline{z}$ et $-\overline{z}$.
Il faut donc trouver $t' \in \mathbb{Q}^*$ tel que $i + \sqrt{2} + t'j \neq \pm i \pm \sqrt{2} + t'j$, les signes devant i et $\sqrt{2}$ n'étant pas simultanément positifs.
Ici encore, $t' = 1$ convient. D'où finalement : $\mathbb{Q}(i, j, \sqrt{2}) = \mathbb{Q}(i + j + \sqrt{2})$.

Deuxième développement : Condition de constructibilité

1er février 2016

Théorème 1 *Soit x un réel constructible.*
Alors x est algébrique sur $\mathbb{Q}$ et son degré $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.

Démonstration : On suppose x constructible. Par hypothèse, il existe une suite $A_0 \subset \cdots \subset A_n$ de parties de $\mathbb{R}^2$ avec $(x, 0) \in A_n$ et, $\forall\, 0 \leqslant i \leqslant n-1$, $A_{i+1} = A_i \cup \{M_i\}$ où M_i est un point de $\mathbb{R}^2$ constructible en un pas à partir de A_i.
Pour $1 \leqslant i \leqslant n$, on note K_i le sous-corps de $\mathbb{R}$ engendré sur $\mathbb{Q}$ par les coordonnées des points de A_i.
On a donc $K_0 = \mathbb{Q}$ et $x \in K_n$.

On va utiliser le lemme suivant :

Lemme 1 $[K_i : K_{i-1}] = 1$, *2 ou 4.*

Démonstration 1 *On a $A_i = A_{i-1} \cup \{M_i\}$ avec $M_i = (x_i, y_i)$. Donc $K_i = K_{i-1}(x_i, y_i)$. Par définition, M_i est intersection de droites ou de cercles dont les équations sont dans $K_{i-1}[X, Y]$, de sorte que x_i et y_i vérifient des équations de degré $\leqslant 2$ sur K_{i-1}.*
En effet :

- *Si M_i est l'intersection de deux droites, alors x_i et y_i vérifient :*

$$\begin{cases} ax_i + by_i + c &= 0 \\ a'x_i + b'y_i + c' &= 0 \end{cases}$$

Ce qui équivaut à :

$$\begin{cases} (ab' - a'b)x_i + b'c - bc' &= 0 \\ (a'b - ab')y_i + a'c - ac' &= 0 \end{cases}$$

- *Si M_i est l'intersection d'une droite et d'un cercle, alors x_i et y_i vérifient :*

$$\begin{cases} ax_i + by_i + c &= 0 \\ (x_i - a')^2 + (y_i - b')^2 - r^2 &= 0 \end{cases}$$

Si $a \neq 0$, la première équation nous permet de remplacer x_i par $-\dfrac{by_i + c}{a}$ dans la seconde. Sinon, elle donne directement la valeur de y_i, qu'on peut utiliser dans la seconde égalité.
Dans les deux cas, ce système permet d'obtenir x_i et y_i en résolvant une équation de degré 2 et une équation de degré 1.

- *Si M_i est l'intersection de deux cercles, alors x_i et y_i vérifient :*

$$\begin{cases} (x_i - a)^2 + (y_i - b)^2 - r^2 &= 0 \\ (x_i - a')^2 + (y_i - b')^2 - r'^2 &= 0 \end{cases}$$

On admettra que cela revient à résoudre deux équations de degré 2, l'une en x_i l'autre en y_i.

On a donc $[K_{i-1}(x_i) : K_{i-1}] \leqslant 2$ *et* $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] \leqslant 2$.
D'où le résultat.

Par une récurrence immédiate, on montre que $[K_n : \mathbb{Q}]$ est une puissance de 2, en vertu du théorème de la base télescopique.
Comme $\mathbb{Q}(x)$ est un sous-corps de K_n, le degré de l'extension $[\mathbb{Q}(x) : \mathbb{Q}]$ divise $[K_n : \mathbb{Q}]$.
$[\mathbb{Q}(x) : \mathbb{Q}]$ est donc une puissance de 2.

Exemple 1 *On peut construire, pour* $x \in \mathbb{Q}$, $(x, 0)$ *et* $(\sqrt{x}, 0)$.

- *Pour montrer que* $(x, 0)$ *est constructible, il faut d'abord montrer que si on a trois points* $P, Q, R \in \mathbb{R}^2$ *on sait construire la parallèle à* (PQ) *passant par* R.
  Pour cela, il suffit de construire, au compas, le point S *situé à distance* PR *de* Q *et à distance* PQ *de* R *: le quadrilatère* $PQSR$ *ainsi obtenu est un parallèlogramme, donc* (RS) *est la droite recherchée.*
  Ensuite, on construit $\frac{p}{q} \in \mathbb{Q}$ *en menant la parallèle au segment* $< (p, 0); (0; q) >$ *passant par* $(0, 1)$.

- *Pour montrer que* $(\sqrt{x}, 0)$ *est constructible, on pose* $a := \frac{x-1}{2}$ *et* $b := a + 1 = \frac{x+1}{2}$.
  On a : $(b - a)(b + a) = b + a = b^2 - a^2 = x$ *donc* $b^2 = a^2 + c^2$ *avec* $c^2 = x$.
  On construit alors à partir de x *les points* $(0, a)$ *et* $(b, 0)$ *et on construit* $(c, 0)$ *comme troisième sommet d'un triangle rectangle de sommets* O *et* $(0, a)$ *dont l'hypoténuse* a *pour longueur* b.

Corollaire 1 *Les problèmes grecs sont insolvables.*

Les trois grands problèmes grecs sont : la duplication du cube, la trisection de l'angle, et la quadrature du cercle.

Duplication du cube :
Considérons un cube de côté 1. Pour le dupliquer, il faudrait construire un cube de volume 2, donc de côté $\sqrt[3]{2}$.
Or $\sqrt[3]{2}$ n'est pas constructible.
En effet, le polynôme $X^3 - 2$, est irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein, donc est le polynôme minimal de $\sqrt[3]{2}$.
Donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ qui n'est pas une puissance de 2.
Donc $\sqrt[3]{2}$ n'est pas constructible.

Trisection de l'angle :
S'il est possible de trisecter n'importe quel angle constructible, il doit être notamment possible de trisecter $\frac{\pi}{3}$. Cela impliquerait de construire les instersections de droites d'angle $\frac{\pi}{9}$ et du cercle unité, ainsi que les coordonnées de ces intersections.
Cela impliquerait donc de construire $x := \cos\left(\frac{\pi}{9}\right)$.
Or, pour tout $\theta \in \mathbb{R}$, on a : $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$.
D'où :

$$\cos\left(3 \times \frac{\pi}{9}\right) = 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right) \tag{1a}$$

$$\frac{1}{2} = 4x^3 - 3x \tag{1b}$$

Donc x est racine du polynôme $8X^3 - 6X - 1$, qui est irréductible sur $\mathbb{Q}$.
Donc $[\mathbb{Q}(x) : \mathbb{Q}] = 3$.

Quadrature du cercle :
On cherche un carré de côté a tel que son aire soit celle du cercle unité.
Cela signifie qu'on cherche a tel que $a^2 = \pi$.
Or $\sqrt{\pi}$ est transcendant sur $\mathbb{Q}$ (admis), donc non constructible.