I Corps, extensions de corps et degré d'une extension

1) Définition et premiers résultats.

Définition 1. Soit K et L deux corps tels qu'il existe un morphisme de corps $j: K \to L$. On dit que L est une extension (de corps) de K et on note L/K.

Remarque 2. On considèrera dans la suite que $K \subset L$ et j est l'inclusion.

Exemple 3.
- $\mathbb{R}$ est une extension de $\mathbb{Q}$
- $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$
- $\mathbb{Q}(X)$ est une extension de $\mathbb{Q}$.
- Pour p premier, tout corps de caractéristique p est une extension de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition 4. Soit L/K. L est donc muni d'une structure de K-espace vectoriel. On définit $[L:K] = \dim_K(L)$ le degré de L sur K.

Exemple 5.
- $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = [\mathbb{Q}(X):\mathbb{Q}] = +\infty$.
- Si K et L sont des corps finis et $\operatorname{card} L = \operatorname{card} K^n$, on a $[L:K] = n$.

Théorème 6 (de la base téléscopique)
Soit $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de M sur L. Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K.

Corollaire 7 : Si les degrés des extensions sont finis, alors :

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

Définition 8. Soit L/K et $A \subset L$. On dit que A engendre L sur K et on écrit $L = K(A)$ si L est le plus petit sous-corps de L contenant K et A.

- Si $A = \{\alpha_1, \dots, \alpha_n\}$ est fini, on note $L = K(\alpha_1, \dots, \alpha_n)$ et on a :

$$L = \left\{ \frac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)} \mid P, Q \in K[X], Q(\alpha_1, \dots, \alpha_n) \neq 0 \right\}.$$

- On dit que L/K est monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Exemple 9 :
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est monogène de degré 3.
- $\mathbb{Q}(j)/\mathbb{Q}$ est monogène de degré 2.
- $\{j, \sqrt[3]{2}\}$ engendre $\mathbb{Q}(j, \sqrt[3]{2})$ sur $\mathbb{Q}$ et

$$[\mathbb{Q}(j, \sqrt[3]{2}):\mathbb{Q}] = [\mathbb{Q}(j, \sqrt[3]{2}):\mathbb{Q}(j)][\mathbb{Q}(j):\mathbb{Q}] = 3 \times 2 = 6.$$

Définition 10. Soit L/K et L'/K. $\sigma: L \to L'$ est un K-morphisme si σ est un morphisme de corps dont la restriction à K est l'identité.

Exemple 11 : $\mathbb{C} \to \mathbb{C}$, $j \mapsto \bar{j}$ est un $\mathbb{R}$-automorphisme.

2) Extensions algébriques

Définition 12. Soit L/K et $\alpha \in L$. Soit $\varphi: K[X] \to L$ le morphisme d'anneaux défini par $\varphi_{|K} = \mathrm{Id}_K$ et $\varphi(X) = \alpha$. On note $K(\alpha) = \operatorname{Im} \varphi$.
- (i) Si φ est injectif, on dit que α est transcendant sur K.
- (ii) Sinon il existe un unique $P \in K[X] \setminus \{0\}$ tel que $\ker \varphi = (P)$ et P soit unitaire.

On dit que α est algébrique sur K et que P est son polynôme minimal sur K.

Exemple 13.
- $X \in K(X)$ est transcendant sur K.
- [admis] e et π sont transcendants sur $\mathbb{Q}$.
- $\sqrt{2}, \dots, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, de polynôme minimal respectif $X^2 - 2$, $X^2 + 1$, $X^3 - 2$.

Proposition 14. Si α est transcendant sur K, alors $K[\alpha] \simeq K(X)$ et $K(\alpha) \simeq K(X)$.
En particulier $K(\alpha) \neq K[\alpha]$.

Théorème 15. Soit L/K, $\alpha \in L$. Les propriétés suivantes sont équivalentes :
(i) α est algébrique sur K
(ii) $K[\alpha] = K(\alpha)$
(iii) $\dim_K K[\alpha] < +\infty$.
Dans ce cas si P est le polynôme minimal de α, P est irréductible dans $K[X]$ et on a : $\dim_K K[\alpha] = [K[\alpha] : K] = \deg P$. $\deg P$ est le degré de α.

Définition 16. • L/K est finie si $[L:K] < +\infty$.
• L/K est algébrique si pour tout $\alpha \in L$, α est algébrique sur K.

Corollaire 17. Toute extension finie est algébrique. De plus, si L/K est de degré n, $\alpha \in L$ et est de degré d, alors $d \mid n$.

Corollaire 18. Si α est algébrique sur K de polynôme minimal P, alors $K[\alpha] \simeq K[X]/(P)$ et $(1, \alpha, \dots, \alpha^{\deg P - 1})$ est une base de $K[\alpha]$.

Théorème 19. Soit L/K et $M = \{x \in L \mid x \text{ est algébrique sur } K\}$.
Alors M est un sous-corps de L.

Exemple 20. Soit $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$. A est un corps et une extension de $\mathbb{Q}$ qui n'est pas finie.

II - Extensions et polynômes

1) Corps de rupture

Définition 21. Soit K un corps, $P \in K[X]$ irréductible. L/K est un corps de rupture de P sur K s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.

Exemple 22. • $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.
• Un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$ est $\mathbb{C} = \mathbb{R}(i)$.
• $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ est un corps de rupture de $X^2 + X + 1$.

Théorème 23. Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K et il est unique à isomorphisme près et isomorphe à $K[X]/(P)$.

Application 24. $\forall \xi$ racine primitive n-ième de l'unité, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$

2) Corps de décomposition

Définition 25. Soit K un corps, $P \in K[X]$ de degré n. On appelle corps de décomposition de P sur K une extension L de degré n telle que
(i) P est scindé sur L.
(ii) Si $\alpha_1, \dots, \alpha_n \in L$ sont les racines de P dans L, $L = K(\alpha_1, \dots, \alpha_n)$

Théorème 26. $\forall P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.

Application 27. Soit p premier, $n \in \mathbb{N}^*$, $q = p^n$.
(i) Il existe un corps fini $\mathbb{F}_q$ à q éléments : c'est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$.
(ii) Si F et F' sont deux corps à q éléments, ils sont $\mathbb{F}_p$-isomorphes.
(iii) $\mathbb{F}_q^*$ est un groupe cyclique.

3) Clôture algébrique d'un corps

Définition 28. Soit K un corps, $\overline{K}/K$ une extension. $\overline{K}$ est une clôture algébrique de K si :
(i) $\forall P \in K[X]$, P est scindé sur $\overline{K}$
(ii) $\overline{K}/K$ est algébrique.

Exemple 29 : $\mathbb{Q}$ n'est pas algébriquement clos car X^2+1 n'a pas de racine dans $\mathbb{Q}$.

Théorème 30 [D'Alembert - Gauss] : $\mathbb{C}$ est algébriquement clos. (DVP)

Corollaire 31 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 32 (admis) : Tout corps K possède une clôture algébrique.

4) Extensions séparables.

Soit p un nombre premier.

Définition 33 : Soit K un corps de caractéristique p. $\tilde{F} : K \to K$, $x \mapsto x^p$ est un morphisme appelé morphisme de Frobenius.

Si K est fini, $\tilde{F}$ est un F_p-automorphisme.

Proposition 34 : Soit $L = K[x]/K$ une extension monogène, P le polynôme minimal de x, soit $\bar{K}$ une clôture algébrique de K. Alors

$$\varphi : \mathrm{Hom}_K(L, \bar{K}) \to \{y \in \bar{K} \mid P(y) = 0\}, \quad f \longmapsto f(x)$$

est bijective.

En particulier il y a entre 1 et $[L:K]$ K-morphismes de L dans $\bar{K}$.

Définition 35 : Soit L/K une extension algébrique. $x \in L$ est séparable sur K si son polynôme minimal est séparable.

Théorème 36 : Soit L/K et $\bar{K}$ une clôture algébrique de K. Alors

$$1 \leq n = \#\mathrm{Hom}_K(L, \bar{K}) \leq [L:K]$$

et les propriétés suivantes sont équivalentes :

(i) $n = \#\mathrm{Hom}_K(L, \bar{K}) = [L:K]$.

(ii) $\exists x_1, \dots, x_m \in L$ séparables sur K tels que $L = K[x_1, \dots, x_m]$.

(iii) Tout élément de L est séparable sur K.

L est alors dite séparable.

Corollaire 37 : Soit L/K. Alors l'ensemble des K-automorphismes de L $\mathrm{Aut}(L/K)$ est un groupe de cardinal au plus égal à $[L:K]$.

S'il y a égalité, L est séparable.

III. Constructions à la règle et au compas

Dans le plan euclidien $\mathbb{R}^2$ muni des points $O = (0,0)$, $I = (1,0)$, soit $A \subset \mathbb{R}^2$. On s'intéresse aux figures suivantes obtenues à partir de A :

(i) Les droites affines (PQ), $P, Q \in A$, $P \neq Q$.

(ii) Les cercles centrés en $P \in A$, passant par $Q \neq P \in A$.

(iii) Les cercles centrés en $P \in A$ de rayon $\|QR\|$ avec $Q, R \in A$, $R \neq Q$.

Définition 38 : Soit $A \subset \mathbb{R}^2$, $M \in \mathbb{R}^2$. On dit que M est constructible en un pas à partir de A s'il existe deux droites ou cercles distincts de type (i), (ii) ou (iii) dont M soit un point d'intersection.

- $M \in \mathbb{R}^2$ est constructible s'il existe $n \in \mathbb{N}$, $A_0 \subset \cdots \subset A_n \subset \mathbb{R}^2$ tels que :
  - (1) $A_0 = \{0, I\}$ (2) $M \in A_n$
  - (3) $A_i = A_{i-1} \cup \{M_i\}$ où M_i est constructible en un pas à partir de A_{i-1}.
- $x \in \mathbb{R}$ est constructible si $(x, 0)$ l'est.

Proposition 39 : Pour $n \in \mathbb{N}$, $x \in \mathbb{Q}$, les $(n, 0)$, $(0, n)$, $(x, 0)$ sont constructibles.

- Si $x > 0$ est constructible, $\sqrt{x}$ également.

Théorème 40 [Wantzel] : Soit x un réel constructible. Alors x est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}[x] : \mathbb{Q}]$ est une puissance de 2. (DVP)

Applications 41 et 42 : Impossibilité de dupliquer le cube et de trisecter un angle de $\frac{\pi}{3}$.

Références

Perrin, Cours d'algèbre

Chambert-Loir, Algèbre corporelle

Escofier, Théorie de Galois

Théorème de Wantzel et applications

Références:
Perrin, Cours d'Algèbre : III.1 Théorème 1.21 et les applications qui suivent

Théorème de Wantzel

Théorème de Wantzel. *Soit x un réel constructible, alors x est algébrique dans $\mathbb{Q}$ et son degré $[\mathbb{Q}[x] : \mathbb{Q}]$ est une puissance de 2*

Démonstration. Comme x est constructible, d'après la définition, on a une suite

$$A_0 \subset A_1 \subset ... \subset A_n$$

avec $(x, 0) \in A_n$. Soit K_i le sous corps de $\mathbb{R}$ engendré sur $\mathbb{Q}$ par les coordonnées des points de A_i. On a donc

$$K_0 = \mathbb{Q} \quad et \quad x \in K_n$$

On va alors avoir besoin du lemme suivant:

Lemme.

$$[K_i : K_{i-1}] = 1, 2 \text{ ou } 4$$

Démonstration. 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 l'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 ≤ 2 sur K_{i-1}. On a donc

$$[K_{i-1}(x_i) : K_{i-1}] \leq 2 \text{ et } [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] \leq 2$$

Donc, on a $[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}]$. Comme $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] = 1 \text{ ou } 2$ et $[K_{i-1}(x_i) : K_{i-1}] = 1 \text{ ou } 2$ on a le résultat attendu. □

Par une récurrence immédiate, le lemme donne $[K_n : K_0] = [K_n : \mathbb{Q}]$ est une puissance de 2. Or comme $w \in K_n$, on a $\mathbb{Q}[x]$ est un sous corps de K_n et donc $[\mathbb{Q}[x] : \mathbb{Q}]$ divise $[K_n : \mathbb{Q}]$ ce qui termine la démonstration. □

Applications

Duplication du cube unité

Ce problème date des grecs, on cherche à construire à la règle et au compas un nombre a tel que le cube d'arrête a ait une aire égale au double de l'aire du cube unité. On cherche donc à construire a tel que $a^3 = 2$, soit $a = 2^{1/3}$.

Propriété. $2^{1/3}$ *n'est pas constructible*

Démonstration. Le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$. Car il n'admet pas de racine dans $\mathbb{Q}$. Donc c'est le polynôme minimal de $2^{1/3}$ et donc

$$\left[\mathbb{Q}\left(2^{1/3}\right) : \mathbb{Q}\right] = 3$$

qui n'est pas une puissance de 2, ce qui donne que ce nombre n'est pas constructible d'après le théorème. □

On ne peut donc pas construire le nombre a, et la duplication du cube unité à la règle et au compas est impossible.

Trisection de l'angle

On cherche à "trisecter" un angle, par exemple $\pi/3$, ce qui revient à essayer de construire $x = cos(\pi/9)$. Grâce aux polynômes de Chebychev, on a

$$cos(3\theta) = 4cos^3(\theta) - 3cos(\theta)$$

et x vérifie l'équation $8x^3 - 6x - 1 = 0$, ce polynôme étant irreductible dans $\mathbb{Q}$, on a

$$[\mathbb{Q}(x) : \mathbb{Q}] = 3$$

On ne peut donc pas trisecter l'angle $\pi/3$, d'après le théorème.

$\mathbb{C}$ est algébriquement clos

Références:
Inspiré de Guin, Algèbre I : XII.2 Théorème XII.2.1

Théorème. $\mathbb{C}$ *est algébriquement clos*

Démonstration. Pour cette démonstration on aura besoin de s'appuyer sur plusieurs propriétés des polynômes dont on admettra certaines:

Polynômes de degré impair dans $\mathbb{R}$. *Tout polynôme à coefficients dans $\mathbb{R}$ de degré impair admet une racine dans $\mathbb{R}$*

Proof. Soit $P \in \mathbb{R}[X]$ et $f : \mathbb{R} \to \mathbb{R}$ sa fonction polynômiale associée. Comme P est de degré impair, on a bien

$$\lim_{x \to +\infty} f(x) = +\infty \quad et \quad \lim_{x \to -\infty} f(x) = -\infty$$

Donc d'après le TVI, $f(\mathbb{R}) = \mathbb{R}$ et donc il existe $x_0 \in \mathbb{R}$ tel que $f(x_0) = 0$ □

Polynômes de degré 2 dans $\mathbb{C}$. *Tout nombre dans $\mathbb{C}$ admet une racine carrée dans $\mathbb{C}$. Tout polynôme à coefficients dans $\mathbb{C}$ de degré 2, admet 2 racines dans $\mathbb{C}$*

Démonstration. On sait que tout nombre réel positif admet une racine carrée dans $\mathbb{R}$. En effet, soit $x > 0 \in \mathbb{R}$, et $P = \{a \in \mathbb{R} \, tel \, que \, a^2 \leq x\}$, P est non vide et bornée (par $sup(1, x)$ par exemple). Il est évident que $sup(P)$ est atteint et donc qu'il existe s tel que $s^2 = x$. Soit maintenant $z \in \mathbb{C}$, z est de la forme $a+ib$ avec a et b des réels. Un calcul simple permet de déterminer que si $z' = \alpha + i\beta$ avec

$$\alpha = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \, et \, \beta = \frac{b}{\sqrt{a + \sqrt{a^2 + b^2}}}$$

alors $z'^2 = z$. Avec la méthode du discriminant on trouve donc que les deux racines d'un polynomes de degré 2 à coefficients dans $\mathbb{C}$ sont dans $\mathbb{C}$. □

On admettra que tout corps admet un corps de décomposition, et que tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.

Pour montrer que $\mathbb{C}$ est algébriquement clos, on va montrer que tout polynôme non constant à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. Soit $P \in \mathbb{C}[X]$ et $\bar{P}$ le polynôme dont les coefficients sont les conjugués de ceux de $P(X)$. Le polynôme $F(X) = P(X)\bar{P}(X)$ appartient à $\mathbb{R}[X]$. Si $F(X)$ a une racine $\alpha \in \mathbb{C}$, alors soit $P(\alpha) = 0$ et on a le résultat, soit $\bar{P}(\alpha) = 0$ et dans ce cas $P(\bar{\alpha}) = 0$ et on a le résultat. Il suffit donc de montrer que tout polynôme non constant $f(X) \in \mathbb{R}[X] \subset \mathbb{C}[X]$ admet une racine dans $\mathbb{C}$. Posons $d = degré(f)$, on peut écrire $d = 2^n q$, avec q impair et $n \in \mathbb{N}$. On va faire un raisonnement de récurrence sur n. Si $n = 0$, le degré de f est impair d'où le résultat, d'après la première propriété.
Supposons le résultat vrai pour $d = 2^{n-1}q$ (et $f(X)$ unitaire). Soit un corps K de décomposition sur $\mathbb{C}$ de $f(X)$ dont on a admis l'existence. On a :

$$f(X) = \prod_{i=1}^{d}(X - \alpha_i), \quad \alpha_1, ..., \alpha_d \in K$$

Soit $c \in \mathbb{R}$, on pose

$$y_{ij} = \alpha_i + \alpha_j + c\alpha_i\alpha_j, \quad i \leq j$$

On considère le polynôme

$$G(X) = \prod_{1 \leq i \leq j \leq d} (X - y_{ij})$$

On a alors le lemme suivant

Lemme. *Les coefficients de G sont réels*

Démonstration. On considère le polynôme en les Y_{ij} où les Y_{ij} sont vus commes des indéterminées

$$H(Y_{ij}) = \prod_{1 \leq i \leq j \leq d} (X - Y_{ij}) \in (\mathbb{R}[X])[Y_{ij}]$$

qui est symétrique en les Y_{ij} en temps que polynôme à plusieurs indéterminées à coeficients dans l'anneau $\mathbb{R}[X]$. D'après ce qu'on a admis précedemment:

$$H(Y_{ij}) = Q(\Sigma_1, ..., \Sigma_m), \quad Q \in \mathbb{R}[X][X_1, ..., X_m]$$

avec Σ_i polynômes symétriques élementaires. On peut donc écrire

$$H(y_{ij} = Q\left(\Sigma_1(y_{ij}), ..., \Sigma_m(y_{ij})\right)$$

et les $\Sigma_i(y_{ij})$ sont les coefficients de $f(X)$ et sont donc réels. Donc

$$H(y_{ij}) = G(X) \in \mathbb{R}[X]$$

□

Le degré de G est le nombre de y_{ij}, or il est très simple de voir qu'il y en a $\frac{d(d+1)}{2}$. Donc $degré(G) = \frac{d(d+1)}{2} = 2^{n-1}q(d+1) = 2^{n-1}q'$ avec q' impauir car q et $d+1$ sont impairs. Par hypothèse de récurrence, il admet donc une racine $z_c \in \mathbb{C}$. Cette racine est nécessairement un des y_{ij}. Donc il existe $i(c)$ et $j(c)$ tels que :

$$\alpha_{i(c)} + \alpha_{j(c)} + c\alpha_{i(c)}\alpha_{j(c)} = z_c$$

C'est vrai pour tout $c \in \mathbb{R}$. Or $\mathbb{R}$ est infini et l'ensemble des couples $(i,j), i \leq j$, est fini. Donc il existe un $c' \neq c$ tel que $i(c) = i(c') = r$ et $j(c) = j(c') = s$. On a

$$\alpha_r + \alpha_s + c\alpha_r\alpha_s = z_c \in \mathbb{C}$$

$$\alpha_r + \alpha_s + c'\alpha_r\alpha_s = z'_c \in \mathbb{C}$$

D'où on déduit que $\alpha_r + \alpha_s$ et $\alpha_r\alpha_s$ appartiennent à $\mathbb{C}$. Et donc α_r et α_s sont racines d'une même équation du second degré à coefficients dans $\mathbb{C}$. Donc d'après la deuxième propriété, α_r etα_s appartiennent à $\mathbb{C}$. Et donc $f(X)$ admet une racine dans $\mathbb{C}$ ce qui permet de conclure la démonstration. □