125

Extensions de corps. Exemples et applications.

I - Vocabulaire des extensions de corps

<u>Def 1</u> : Soit K un corps. On appelle extension de K tout corps $\mathbb{K}$ tel qu'il existe un morphisme de corps $j : K \to \mathbb{K}$.

On notera $\mathbb{K}/K$.

<u>Rem 2</u> : Tout morphisme de corps est injectif, d'où le terme "extension".

<u>Ex 3</u> : $\mathbb{R}$ est une extension de $\mathbb{Q}$, via l'inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$.

<u>Rem 4</u> : Si $\mathbb{K}/K$ est une extension, $\mathbb{K}$ est muni d'une structure de K-espace vectoriel.

<u>Def 5</u> : Le degré d'une extension $\mathbb{K}/K$ est la dimension $\dim_K \mathbb{K}$ en tant qu'espace vectoriel, notée $[\mathbb{K}:K]$

<u>Ex 6</u> : L'extension $\mathbb{C}/\mathbb{R}$ est de degré 2.

<u>Def 7</u> : Soit K un corps. On appelle sous-corps premier de K le plus petit corps inclus dans K.

<u>Ex 8</u> : Le sous-corps premier de $\mathbb{F}_2(X)$ est $\mathbb{F}_2$.

<u>Prop 9</u> : Soit K un corps. Le morphisme $\varphi : \mathbb{Z} \to K$ a pour noyau $\{0\}$ ou $p\mathbb{Z}$, p premier.

<u>Def 10</u> : Soit K un corps. On dit que K est de caractéristique p lorsque $\operatorname{Ker} \varphi = p\mathbb{Z}$ (ci-dessus).

<u>Prop 11</u> : Soit K un corps. Le sous-corps premier de K est $\mathbb{Q}$ ou $\mathbb{F}_p$, selon la caractéristique de K.

II - Extensions monogènes

<u>Def 12</u> : On dit qu'une extension $\mathbb{K}/K$ est monogène lorsqu'il existe $\alpha \in \mathbb{K}$ tel que $\mathbb{K} = K(\alpha)$ i.e. $\mathbb{K}$ est le plus petit sous-corps de $\mathbb{K}$ contenant α et K.

1) Nombres algébriques, transcendants

<u>Def 13</u> : Soit $\mathbb{K}/K$ une extension, et $\alpha \in \mathbb{K}$. On dit que α est algébrique lorsqu'il existe $P \in K[X]$ tel que $P(\alpha) = 0$. Sinon, on dit que α est transcendant.

<u>Ex 14</u> : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$: $\sqrt{2}^2 - 2 = 0$.
Mais π est transcendant, sur $\mathbb{Q}$.

<u>Prop 15</u> : Soit $\mathbb{K}/K$ une extension, et $\alpha \in \mathbb{K}$.
Le morphisme $ev_\alpha : \begin{array}{ccc} K[X] & \to & K(\alpha) \\ P & \mapsto & P(\alpha) \end{array}$ est un morphisme de K-algèbres, dont le noyau est réduit à $\{0\}$ si et seulement si α est transcendant sur K.
Dans ce cas, le degré de $K(\alpha)/K$ est infini.

<u>Def 16</u> : Soit $\mathbb{K}/K$ une extension et α algébrique.
Le polynôme unitaire générateur de $\operatorname{Ker} ev_\alpha$ est appelé polynôme minimal de α sur K, noté $\pi_{K,\alpha}$.

<u>Ex 17</u> : $\pi_{\mathbb{Q},\sqrt{2}} = X^2 - 2$.

<u>Prop 18</u> : Soit $\mathbb{K}/K$ une extension et α algébrique.
Alors $[\mathbb{K}:K] = d°\pi_{K,\alpha}$.

<u>Ex 19</u> : $[\mathbb{Q}(j):\mathbb{Q}] = 2$ car $\pi_{\mathbb{Q},j} = X^2 + X + 1$.
Pour tout $n \in \mathbb{N}$, $\sqrt[n]{2}$ est algébrique sur $\mathbb{Q}$, et $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = d°(X^n - 2) = n$.

Prop 20 : Soit $\mathbb{K}/K$ une extension et $\alpha \in \mathbb{K}$ algébrique. Alors $(1, \alpha, \dots, \alpha^{d-1})$, avec $d := d^\circ \pi_{K,\alpha}$ est une base de $K(\alpha)$.

Ex 21 : Une base de $\mathbb{Q}(j)$ sur $\mathbb{Q}$ est $(1, j)$.

2) Adjonction de racines : corps de rupture

Def 22 : Soit K un corps, et $P \in K[X]$ irréductible. Un corps de rupture de P sur K est une extension $\mathbb{K}/K$ monogène, avec $\mathbb{K} = K(\alpha)$ et $P(\alpha) = 0$.

Prop 23 : Soit K un corps et $P \in K[X]$ irréductible. Il existe un unique corps de rupture de P sur K, à isomorphisme près.

Ex 24 : $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.

Prop 25 : Soit K un corps et $P \in K[X]$ irréductible, unitaire. Soit $K(\alpha)$ le corps de rupture de P. Alors $P = \pi_{K,\alpha}$.

Prop 26 : Soit K un corps et $P \in K[X]$ de degré n. P est irréductible sur K ssi P n'a pas de racine dans les extensions L de K telles que $[L:K] \leq \frac{n}{2}$.

3) Application : corps cyclotomiques

Def 27 : Soit $n \in \mathbb{N}^*$. Soit $\xi \in \mu_n^\times(\mathbb{C})$. Le corps $\mathbb{Q}(\xi)$ est appelé corps cyclotomique.

Prop 28 : $\mathbb{Q}(\xi)$ ne dépend pas de la racine primitive nième choisie, et $[\mathbb{Q}(\xi) : \mathbb{Q}] \leq n$.

Def 29 : Soit $n \in \mathbb{N}^*$. On pose $\Phi_n := \prod_{\xi \in \mu_n^\times(\mathbb{C})} (X - \xi)$

Lemme 30 : Soient $P, A, B \in \mathbb{Q}[X] \setminus \{0\}$, avec P, A unitaires et $P \in \mathbb{Z}[X]$. Alors A, B sont aussi dans $\mathbb{Z}[X]$.

Prop 31 : Soit $\xi \in \mu_n^\times(\mathbb{C})$, $n \in \mathbb{N}^*$. Alors Φ_n est le polynôme minimal de ξ sur $\mathbb{Q}$. En particulier, Φ_n est irréductible sur $\mathbb{Q}$, et $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$. DEV 1

Ex 32 : $\Phi_8 = X^4 + 1$ est irréductible.

Rem 33 : Attention, Φ_n n'est pas forcément irréductible sur les corps finis. Par exemple, Φ_8 n'est jamais irréductible sur $\mathbb{F}_p$, pour p premier. DEV 1

III - Chaînes d'extensions

Thm 34 (base télescopique) : Soit $\mathbb{K}/K$ et $\mathbb{L}/\mathbb{K}$ deux extensions. Soit $(e_i)_{i \in I}$ une base de $\mathbb{K}$ sur K et $(f_j)_{j \in J}$ une base de $\mathbb{L}$ sur $\mathbb{K}$. Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{L}$ sur K. En particulier, $[\mathbb{L} : K] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : K]$.

1) Extensions de type fini

Def 35 : Soit $\mathbb{K}/K$ une extension. On dit qu'elle est de type fini lorsqu'il existe $\{\alpha_1, \dots, \alpha_n\} \subset \mathbb{K}$ telle que $\mathbb{K} = K(\alpha_1, \dots, \alpha_n)$, i.e. $\mathbb{K}$ est le plus petit sous-corps de $\mathbb{K}$ contenant $\alpha_1, \dots, \alpha_n$ et K.

Ex 36 : Les extensions monogènes sont de type fini.

Ex 37 : $\mathbb{Q}(i, \sqrt{3})$ est une extension de $\mathbb{Q}$ de type fini. Et $[\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$.

Ex 38 : $\mathbb{Q}(X)$ est de type fini, mais de degré infini.

Thm 39 (de l'élément primitif) : Soit $\mathbb{K}/k$ une extension de degré fini.
On suppose que $\mathbb{K}$ est fini ou de caractéristique nulle.
Alors $\mathbb{K}/k$ est monogène.

2) Corps de décomposition et corps finis

Def 40 : Soit K un corps, $P \in K[X]$. Un corps de décomposition de P sur K est une extension L/K minimale telle que P soit scindé sur L.

Thm 41 : Soit $P \in K[X]$, K un corps. Il existe un unique corps de décomposition de P, à isomorphisme près

Ex 42 : Si P est de degré 2 sur K, de caractéristique différente de 2, tout corps de rupture de P est un corps de décomposition.

Prop 43 : Soit p premier et $n \in \mathbb{N}^*$. Il existe un unique corps, à isomorphisme près, de cardinal p^n.
Il est noté $\mathbb{F}_{p^n}$, et c'est "le" corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

Coro 44 : Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

Prop 46 : Soient p premier, $n \in \mathbb{N}^*$, $d \in [\![1, n]\!]$.
Alors $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_{p^n}$ ssi $d \mid n$.

Ex 47 : $\mathbb{F}_4 \subset \mathbb{F}_{16}$ mais $\mathbb{F}_8 \not\subset \mathbb{F}_{16}$.

3) Constructions à la règle et au compas

Def 48 : Soit $n \in \mathbb{N}^*$. On dit que le polygone régulier $\mathcal{P}_n$ à n côtés est constructible lorsque $\cos(\frac{2\pi}{n})$ l'est.

Thm 49 (Wantzel) : Un réel x est constructible si et seulement si il existe une suite finie $L_0 \subset \dots \subset L_p \subset \mathbb{R}$ d'extensions telles que
(i) $L_0 = \mathbb{Q}$
(ii) $\forall i \in [\![0, p-1]\!]$, $[L_{i+1} : L_i] = 2$
(iii) $x \in L_p$.

Lemme 50 : Soient $n, m \in \mathbb{N}^*$ premiers entre eux.
Alors $\mathcal{P}_{nm}$ est constructible ssi $\mathcal{P}_n$ et $\mathcal{P}_m$ le sont.

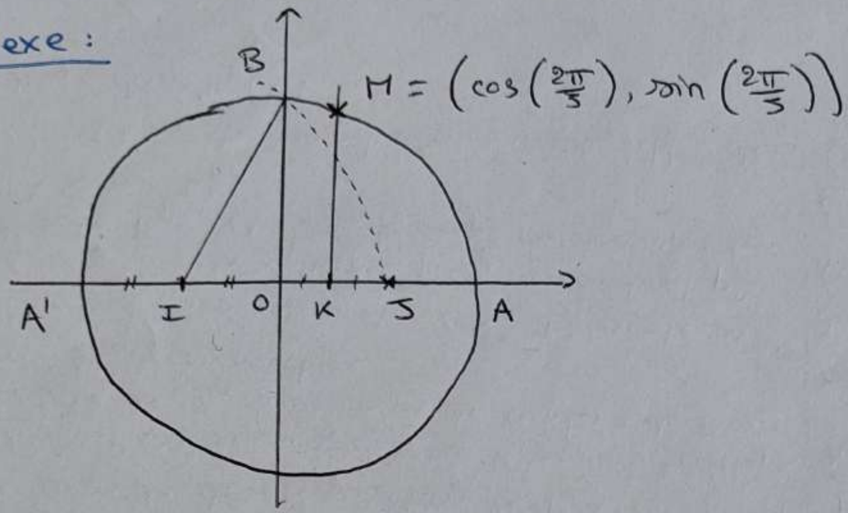
Thm 51 : Soit $n \in \mathbb{N}$, $n \geq 2$.
Alors $\mathcal{P}_n$ est constructible ssi
- ou bien $n = 2^\alpha$ avec $\alpha \in \mathbb{N}^*$
- ou bien $n = 2^\alpha p_1 \cdots p_r$ avec $\alpha \in \mathbb{N}$ et $p_1, \dots, p_r$ des nombres premiers de Fermat distincts.

(on admettra la réciproque du deuxième point).

DEV 2

Ex 52 : Le pentagone régulier est constructible, (voir annexe) car $5 = 2^2 + 1$ est de Fermat.

Annexe :


B
$M = \left(\cos\left(\frac{2\pi}{3}\right), \sin\left(\frac{2\pi}{3}\right)\right)$
A'
I
O
K
J
A