Tous les corps seront supposés commutatifs. Soient L, M et K des corps.

I - Notion d'extension de corps

A - Structure d'espace vectoriel : degré d'une extension

[P 65] **Def 1** : On dit que L est une *extension* de K, et on note L/K, si $L \subseteq K$.

[P 65] **Ex 2** : $\mathbb{C}/\mathbb{R}/\mathbb{Q}$ est une tour d'extensions de $\mathbb{Q}$.

Dans la suite, on suppose que $K \subseteq M \subseteq L$.

[P 65] **Prop/Def 3** : L est un K-espace vectoriel dont on note $[L:K]$ la dimension, que l'on appelle *degré* de l'extension L/K.

On dit que L/K est *finie* si $[L:K]$ est fini.

[P 65] **Thm 4** (de la base télescopique) : Si $(e_i)_{i\in I}$ est une K-base de M et si $(f_j)_{j\in J}$ est une M-base de L, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de L.

[P 65] **Cor 5** (multiplicativité des degrés) : $[L:K] = [L:M]\cdot[M:K]$

B - Algébricité d'un élément, d'une extension

[P 66] **Def 5** : • Pour $A \subseteq L$, on note $K(A)$ la plus petite extension de K contenant A. Si $A = \{\alpha_1, \dots, \alpha_n\}$, on note $K(\alpha_1, \dots, \alpha_n)$ plus simplement.

• On dit que L/K est *de type fini* s'il existe $(\alpha_1, \dots, \alpha_n) \in L^n$ tel que $L = K(\alpha_1, \dots, \alpha_n)$.

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

[P 66] **Def 6** : On dit que $\alpha \in L$ est *algébrique sur* K s'il existe $P \in K[X]$ tel que $P(\alpha) = 0$. Sinon, on dit que α est *transcendant*.

[P 66] **Thm/Def 7** : Si $\alpha \in L$ est algébrique sur K, alors $\{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal non nul, qui donc admet un unique générateur unitaire $P_{\alpha,K}$, appelé *polynôme minimal* de α sur K.

[P 66] **Def 8** : Si $\alpha \in L$ est algébrique sur K, alors on appelle *degré* de α sur K le degré de $P_{\alpha,K}$.

[P 66] **Ex 9** : $\sqrt{12}$, j et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, de polynômes minimaux $X^2 - 12$, $X^2 + X + 1$ et $X^3 - 2$.

Notation : $K[\alpha] = \{P(\alpha) : P \in K[X]\}$.

[P 66] **Thm 10** : Soit $\alpha \in L$. Sont équivalentes :

1. α est algébrique sur K
2. $K[\alpha] = K(\alpha)$
3. $K[\alpha]$ est un K-espace vectoriel de dimension finie.

Le cas échéant, $\deg(P_{\alpha,K}) = [K(\alpha):K]$.

Appli 11 : L'ensemble A des éléments de L algébriques sur K est un corps (dénombrable si K l'est)

[P 67] **Def 12** : On dit que L/K est *algébrique* si tout élément de L est algébrique sur K.

Thm 13 : L/K est finie $\Leftrightarrow$ L/K est algébrique de type fini.

Cor 14 : L/K est algébrique $\Leftrightarrow$ L/M et M/K sont algébriques

Ex 15 : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ sont algébriques, donc $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est algébrique

II - Extensions de corps et racines de polynômes

A - Corps de rupture, de décomposition

Dans ce paragraphe, $P \in K[X]$.

[P] 70 **Def 16** : Supposons P irréductible. On dit que L est un corps de rupture de P sur K s'il existe $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

[P] 70 **Thm 17** : Supposons P irréductible. Le corps $\frac{K[X]}{\langle P \rangle}$ est un corps de rupture de P sur K, et c'est le seul à isomorphisme près.

Rq 18 : Si $\alpha \in L$ est algébrique sur K, alors $\left[\frac{K[X]}{\langle P_{\alpha,K} \rangle} : K\right] = \deg(P_{\alpha,K})$, qui est aussi le degré de α sur K. De plus, $K(\alpha) \simeq \frac{K[X]}{\langle P_{\alpha,K} \rangle}$.

Ex 19 : $\mathbb{C}$ peut être défini comme $\frac{\mathbb{R}[X]}{\langle X^2+1 \rangle}$.

Appli 20 : Si P est irréductible et si $\deg(P) \wedge [L:K]$, alors P est irréductible sur L.

[P] 71 **Def 21** : On dit que L est un *corps de décomposition* de P sur K si P est scindé sur L et si $L = K(\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ les racines de P.

[P] 71 **Thm 22** : Il existe un corps de décomposition de P sur K, unique à isomorphisme près.

[P] 72 **Ex 23** : $\mathbb{Q}(j, \sqrt[3]{2})$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$.

[P] 87 **Thm 24 (de l'élément primitif)** : Toute extension finie d'un corps de caractéristique nulle est monogène.

B - Clôture algébrique

Def 25 : On dit que K est *algébriquement clos* si tout polynôme non nul de $K[X]$ est scindé, et si K n'admet pas d'extension algébrique non triviale. [P] 67

Def 26 : On dit que L est une *clôture algébrique* de K si c'est une extension de K algébrique et algébriquement close. [P] 72

Ex 27 : [P] 68 72
- $\mathbb{C}$ est algébriquement clos (d'Alembert, Gauss)
- $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Ex 28 : Si L est algébriquement clos, alors A de Appli 11 aussi. [Go] 94

Thm 29 : K admet une unique clôture algébrique à isomorphisme près.

C - Application : construction des corps finis

Soient p un nombre premier, $r \in \mathbb{N}^*$ et $q = p^r$.

Lemme 30 : Si $\mathrm{car}(K) = p$, alors K admet un sous-corps $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. [P] 72

Cor 31 : Si K est fini, alors $\#K$ est une puissance de p. [P] 72

Thm 32 : Il existe un corps à q éléments, unique à isomorphisme près. Sa classe d'isomorphisme est représentée par un corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. On note $\mathbb{F}_q$ "le" corps fini à q éléments. [P] 73

Ex 33 : $\mathbb{F}_4 \simeq \frac{\mathbb{Z}/2\mathbb{Z}}{\langle X^2+X+1 \rangle} = \{0, 1, \bar{X}, 1+\bar{X}\}$ et $\bar{X}^2 = 1 + \bar{X}$.

Prop 34 : $\forall (n,m) \in (\mathbb{N}^*)^2$, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$ FIGURE

Def 35 : La fonction de Moebius est : [Rb] 331

$\mu : \mathbb{N}^* \longrightarrow \{-1,0,1\}$

$$n \longmapsto \begin{cases} 1 & \text{si } n=1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ facteurs premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

[Rb] 333 **Thm 36** (formule d'inversion de Moebius) : Soient $(u_n)_{n\in\mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$.
Si $\forall n \in \mathbb{N}^*,\ u_n = \sum_{d|n} v_d$, alors $\forall n \in \mathbb{N}^*,\ v_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) u_d$.

[Rb] 423 **Thm 37** : $P_n := X^{p^n} - X = \prod_{d|n} \prod_{P\in U_d(p)} P$ où $U_d(p)$ est l'ensemble des polynômes irréductibles unitaires de degré d de $\mathbb{F}_p[X]$.

[Rb] 424 **Cor 38** : $\#U_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$

DEV 1

III - Polynômes cyclotomiques

On note $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ le groupe des racines complexes n-ièmes de l'unité, et μ_n^* l'ensemble de ses générateurs (que l'on appelle racines primitives n-ièmes de l'unité).

[P] 80 **Def 39** : Pour $n \in \mathbb{N}^*$, on définit le n-ième polynôme cyclotomique :

$$\Phi_n = \prod_{\zeta \in \mu_n^*} X - \zeta$$

[P] 80-83 **Prop 40** :
- $\Phi_n = \prod_{\substack{k=1 \\ k\wedge n = 1}}^{n} X - \zeta_n^k$ avec $\zeta_n \in \mu_n^*$.
- $X^n - 1 = \prod_{d|n} \Phi_d$
- $\Phi_n \in \mathbb{Z}[X]$

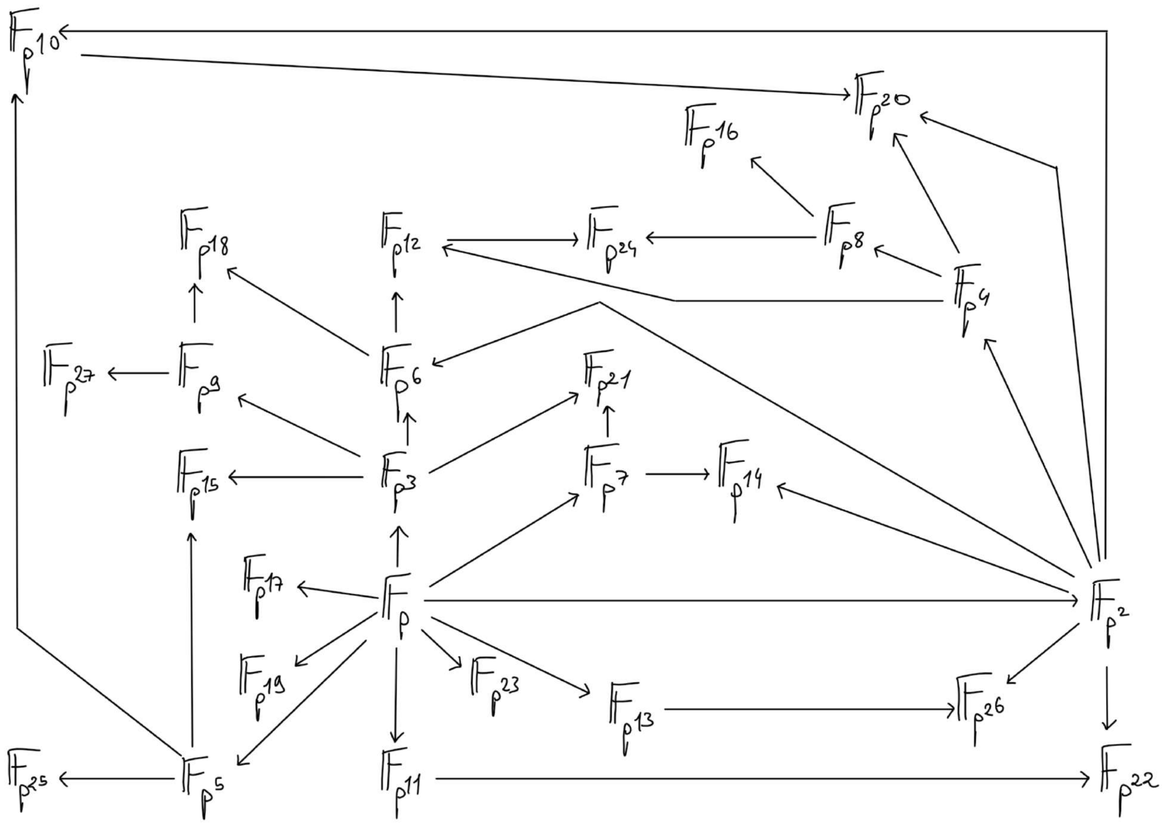
[P] 81 **Ex 41** :
- Pour p premier, $\Phi_p = X^{p-1} + \cdots + X + 1$
- $\Phi_1 = X-1$, $\Phi_4 = X^2+1$, $\Phi_6 = X^2 - X + 1$, $\Phi_8 = X^4+1$

[P] 82-83 **Thm 42** : Soit $\zeta_n \in \mu_n^*$. Le polynôme minimal de ζ_n sur $\mathbb{Q}$ est Φ_n.

Cor 43 : Φ_n est irréductible sur $\mathbb{Q}$ et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

DEV 2

FIGURE



RÉFÉRENCES

[P] Perrin

[Go] Gourdon

[Rb] Rombaldi