125 — Extensions de corps. Exemples et applications.

On considère $\mathbb{K}$, $\mathbb{L}$ et k des corps.

I. Généralités sur les extensions de corps.

1. Définitions, exemples et premiers résultats.

Définition 1 : On dit que $\mathbb{K}$ est une extension de k s'il existe un morphisme de corps $j : k \to \mathbb{K}$. On note dans ce cas $\mathbb{K}/k$.

Remarque 2 :
- Soit k un sous-corps de $\mathbb{K}$. Par le morphisme d'inclusion, $\mathbb{K}$ est une extension de k.
- Réciproquement, tout morphisme de corps est injectif. Si $\mathbb{K}/k$ est une extension, k peut être vu comme sous-corps de $\mathbb{K}$.
- Si $\mathbb{L}/\mathbb{K}$ et $\mathbb{K}/k$ sont des extensions, alors $\mathbb{L}/k$ aussi.

Exemple 3 :
- $\mathbb{C}$ est une extension de $\mathbb{R}$. • $\mathbb{R}$ est une extension de $\mathbb{Q}$.
- Tout corps est une extension de son sous-corps premier. Ainsi, tout corps de caractéristique 0 est une extension de $\mathbb{Q}$, et tout corps de caractéristique p est une extension de $\mathbb{F}_p$ (p premier).
- $k(T)$ est une extension de k.

Proposition 4 : Soit $\mathbb{K}/k$ une extension et $j : k \to \mathbb{K}$ morphisme de corps. En munissant $\mathbb{K}$ du "produit par un scalaire" $\lambda x = j(\lambda)x$ pour tous $\lambda \in k$ et $x \in \mathbb{K}$, $\mathbb{K}$ est une k-algèbre.

Définition 5 : On appelle degré de l'extension $\mathbb{K}/k$ et on note $[\mathbb{K}:k]$ la dimension de $\mathbb{K}$ comme k-espace vectoriel.

Remarque 6 : Le degré d'une extension peut être fini ou infini. On dit que l'extension est de degré fini ou infinie.

Exemple 7 :
- $[\mathbb{K}:k] = 1$ ssi $\mathbb{K} = k$.
- $[\mathbb{R}:\mathbb{Q}] = +\infty$
- $[\mathbb{C}:\mathbb{R}] = 2$
- $[k(X):k] = +\infty$.

Théorème 8 (de la base télescopique) **:** Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{K}/k$ des extensions de corps. Soient $(e_i)_{i \in I}$ une base du $\mathbb{K}$-ev $\mathbb{L}$ et $(\alpha_j)_{j \in J}$ une base du k-ev $\mathbb{K}$. Alors $(\alpha_j e_i)_{(i,j) \in I \times J}$ est une base de $\mathbb{L}$ comme k-ev.

Corollaire 9 : Sous les notations du th. 8, $\mathbb{L}$ est une extension de degré fini de k si et seulement si [$\mathbb{L}/\mathbb{K}$ est de degré fini et $\mathbb{K}/k$ est de degré fini]. Dans ce cas, $[\mathbb{L}:k] = [\mathbb{L}:\mathbb{K}][\mathbb{K}:k]$.

Définition 10 : Soit $\mathbb{L}/k$ une extension. On appelle sous-extension de $\mathbb{L}/k$ tout corps $\mathbb{K}$ tel que $k \subset \mathbb{K} \subset \mathbb{L}$.

Proposition / Définition 11 : Soit $\mathbb{L}/k$ une extension, soit P une partie de $\mathbb{L}$. L'ensemble des sous-corps de $\mathbb{L}$ qui contiennent k et P admet au sens de l'inclusion un plus petit élément. Ce élément est noté $k(P)$ et est appelé la sous-extension de $\mathbb{L}/k$ engendrée par P.

Exemple 12 :
- Si $P = \{\alpha_1, \dots, \alpha_n\} \subset \mathbb{L}$, on note $k(\alpha_1, \dots, \alpha_n)$ au lieu de $k(\{\alpha_1, \dots, \alpha_n\})$.
- Si $\alpha \in k$, alors $k(\alpha) = k$.
- Si $\alpha \in \mathbb{L}$, alors $k(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} \text{ où } P \in k[X], Q \in k[X] \text{ avec } Q(\alpha) \neq 0 \right\}$.

Définition 13 : Soit $\mathbb{L}/k$ une extension. On dit que $\mathbb{L}$ est une extension de type fini de k s'il existe une partie finie $\{\alpha_1, \dots, \alpha_n\} \subset \mathbb{L}$ telle que $\mathbb{L} = k(\alpha_1, \dots, \alpha_n)$.

Proposition 14 : Toute extension de degré fini est de type fini.

Remarque 15 : La réciproque est fausse : on considère $k(X)/k$.

Définition 16 : Soit $\mathbb{L}/k$ une extension. On dit que $\mathbb{L}$ est une extension monogène de k s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = k(\alpha)$. On dit alors que $\alpha \in \mathbb{L}$ est un élément primitif de $\mathbb{L}/k$.

Remarque 17 : Il n'y a pas unicité d'élément primitif. Par exemple, $k = k(\alpha)$ pour tout $\alpha \in k$.

Proposition 18 : Soit $\mathbb{L}/k$ une extension avec $[\mathbb{L}:k]$ premier. Alors $\mathbb{L}$ est une extension monogène de k.

2. Éléments et extensions algébriques.

a. Éléments algébriques et transcendants.

On considère $\mathbb{K}/k$ une extension de corps et $a \in \mathbb{K}$.

Définition 19 : On considère le morphisme de k-algèbres $ev_a : k[X] \to \mathbb{K}$, $P \mapsto P(a)$.
- Si ev_a est injectif i.e. $\{P \in k[X] \mid P(a) = 0\} = \{0\}$, on dit que a est transcendant sur k.
- Si ev_a n'est pas injectif, i.e. il existe $P \in k[X] \setminus \{0\}$ tel que $P(a) = 0$, on dit que a est algébrique sur k.

Remarque 20 : La notion d'algébricité / transcendance dépend des corps considérés.

Exemple 21 :
- $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car annulé par $X^2 - 2 \in \mathbb{Q}[X]$.
- $i \in \mathbb{C}$ est algébrique sur $\mathbb{R}$ car annulé par $X^2 + 1 \in \mathbb{R}[X]$.
- $\pi \in \mathbb{R}$ est algébrique sur $\mathbb{R}$ mais transcendant sur $\mathbb{Q}$.

Théorème 22 : Si $a \in \mathbb{K}$ est transcendant sur k, alors $k(a)$ et $k(X)$ sont isomorphes.

Corollaire 23 : $[k(a):k] = +\infty$ si $a \in \mathbb{K}$ est transcendant sur k.

Proposition / Définition 24 : Supposons dans la suite que $a \in \mathbb{K}$ est algébrique sur k. Il existe un unique polynôme unitaire $M_a \in k[X]$ tel que $\ker(ev_a) = (M_a)$. M_a est appelé polynôme minimal de a sur k et son degré est appelé degré de a sur k.

Exemple 25 : $a \in k$ ssi $\deg(M_a) = 1$. Dans ce cas, $M_a = X - a$.

Proposition 26 : Soit $P \in k[X]$ unitaire. P est le polynôme minimal de a ssi [$P(a) = 0$ et P est irréductible sur k].

Exemple 27 : Le polynôme minimal de i sur $\mathbb{C}$ est $X - i$, celui sur $\mathbb{R}$ est $X^2 + 1$.

Proposition 28 : Soit $m := \deg(M_a)$. Alors la famille $(1, a, a^2, \dots, a^{m-1})$ est une base de $k[a]$ en tant que k-ev.

Proposition 29 : $k[a] = k(a)$ et $[k(a):k] = m$.

Corollaire 30 : Si $a \in \mathbb{K}^*$ est algébrique, alors $a^{-1} \in k[a]$.

Proposition 31 : L'application $ev_a : k[X] \to \mathbb{K}$ induit un isomorphisme de k-algèbres $k[X]/(M_a) \simeq k(a)$.

Corollaire 32 : $k[X]/(M_a)$ est un corps.

Exemple 33 : $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$.

Proposition 33,5 : Soit $x \in \mathbb{K}$. x est algébrique sur k ssi $\dim_k(k[x]) < +\infty$.

b. Extensions algébriques.

Définition 34 : Soit $\mathbb{K}/k$ une extension de corps. On dit que $\mathbb{K}$ est une extension algébrique de k si tous les éléments de $\mathbb{K}$ sont algébriques sur k. Dans le cas contraire, on dit que $\mathbb{K}$ est une extension transcendante de k.

Exemple 35 : $\mathbb{C}/\mathbb{R}$ est algébrique, $\mathbb{R}/\mathbb{Q}$ est transcendante.

Proposition 36 : Toute extension de degré fini de k est algébrique sur k.

Remarque 37 : La réciproque est fausse.

Proposition 38 : Soit $\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_s)$ une extension de $\mathbb{K}$ de type fini. Si les α_i sont algébriques sur $\mathbb{K}$, alors $\mathbb{L}$ est de degré fini sur $\mathbb{K}$ et $\mathbb{L}=\mathbb{K}[\alpha_1,\dots,\alpha_s]$.

Remarque 39 : On a [$\mathbb{L}/\mathbb{K}$ algébrique de type fini] ssi [$\mathbb{L}/\mathbb{K}$ est de degré fini].

Théorème 40 (de l'élément primitif, car 0). Soit $\mathbb{L}/\mathbb{K}$ une extension de degré fini en caractéristique 0. Alors $\mathbb{L}/\mathbb{K}$ a un élément primitif, ie. l'extension est monogène.

II. Extensions de corps et polynômes.

1. Corps de rupture.

Définition 41 : Soit $f\in\mathbb{K}[X]$ irréductible dans $\mathbb{K}[X]$. On dit que le corps $\mathbb{L}$ est un corps de rupture de f sur $\mathbb{K}$ si $\mathbb{L}$ est une extension monogène de $\mathbb{K}$, engendrée par $\mathbb{K}$ et une racine de f notée α, ie. $\mathbb{L}=\mathbb{K}(\alpha)$.

Exemple 42 : Si $\deg f=1$, alors $\mathbb{K}$ est un corps de rupture de f sur $\mathbb{K}$.

Théorème 43 : Soit $f\in\mathbb{K}[X]$ un polynôme irréductible dans $\mathbb{K}[X]$. Alors :
- il existe un corps de rupture de f.
- Si $\mathbb{L}=\mathbb{K}(\alpha)$ et $\mathbb{L}'=\mathbb{K}(\beta)$ sont deux corps de rupture de f sur $\mathbb{K}$, alors $\mathbb{L}$ et $\mathbb{L}'$ sont $\mathbb{K}$-isomorphes.

Remarque 44 : En reprenant les notations précédentes, $(1,\alpha,\dots,\alpha^{n-1})$ où $n=\deg f$ est une base du $\mathbb{K}$-ev $\mathbb{L}$.

Exemple 45 : $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de X^3-2 sur $\mathbb{Q}$.

Corollaire 46 : Soit $P\in\mathbb{K}[X]$ de degré supérieur ou égal à 1. Il existe une extension monogène algébrique $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P possède (au moins) une racine.

Proposition 47 : Soit $P\in\mathbb{K}[X]$, $\deg P=n$. Alors P est irréductible dans $\mathbb{K}[X]$ ssi P n'a pas de racine dans les extensions $\mathbb{L}$ de $\mathbb{K}$ telles que $[\mathbb{L}:\mathbb{K}]\le\frac{n}{2}$.

Proposition 48 : Soit $P\in\mathbb{K}[X]$ irréductible sur $\mathbb{K}$ de degré n. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ telle que $[\mathbb{L}:\mathbb{K}]=m$ soit premier avec n. Alors P est irréductible dans $\mathbb{L}[X]$.

Exemple 49 : X^3+X+1 est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.

2. Corps de décomposition.

Définition 50 : Soit $\mathbb{L}/\mathbb{K}$ une extension. Soit $P\in\mathbb{K}[X]$ avec $\deg P=n\in\mathbb{N}^*$. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si :
- il existe $a\in\mathbb{L}$ et $\alpha_1,\dots,\alpha_n\in\mathbb{L}$ tels que dans $\mathbb{L}[X]$, $P=a(X-\alpha_1)\cdots(X-\alpha_n)$
- $\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_n)$.

Remarque 51 : $\mathbb{L}$ est alors une extension algébrique de degré fini de $\mathbb{K}$.

Exemple 52 :
- $\mathbb{K}$ est un corps de décomposition sur $\mathbb{K}$ de tout polynôme de degré 1.
- Soit $\mathbb{K}$ de caractéristique différente de 2. Soit $P=X^2+bX+c\in\mathbb{K}[X]$ irréductible dans $\mathbb{K}[X]$. Soit $\mathbb{K}(\alpha)$ un corps de rupture de P sur $\mathbb{K}$. Alors $\mathbb{K}(\alpha)$ est un corps de décomposition de P sur $\mathbb{K}$.
- $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$.
- $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.
- $\mathbb{Q}(\sqrt[3]{2})$ n'est pas un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

Théorème 53 : Soit $P\in\mathbb{K}[X]$ un polynôme de degré $n\ge1$. Alors :
- il existe un corps de décomposition $\mathbb{L}$ de P sur $\mathbb{K}$ avec $[\mathbb{L}:\mathbb{K}]\le n!$
- Si $\mathbb{L}$ et $\mathbb{L}'$ sont deux corps de décomposition de P sur $\mathbb{K}$, alors $\mathbb{L}$ et $\mathbb{L}'$ sont $\mathbb{K}$-isomorphes.

3. Clôture algébrique

Proposition (Définition) 54 : Les conditions suivantes sont équivalentes :

(i). Tout polynôme de degré ≥1 de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$.
(ii). Tout polynôme de degré ≥1 de $\mathbb{K}[X]$ admet au moins une racine dans $\mathbb{K}$.
(iii). Les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.

Si ces conditions sont vérifiées, on dit que $\mathbb{K}$ est algébriquement clos.

Exemple 55 :
- $\mathbb{Q}$ n'est pas algébriquement clos car X^2-2 n'y admet pas de racine.
- $\mathbb{R}$ n'est pas algébriquement clos car X^2+1 n'y admet pas de racine.

Proposition 56 : Tout corps algébriquement clos est infini.

Théorème 57 (de d'Alembert-Gauss). $\mathbb{C}$ est algébriquement clos.

Corollaire 58 :
- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racine réelle.

Définition 59 : Soit $\mathbb{L}/\mathbb{K}$ une extension. On dit que $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et $\mathbb{L}$ est algébriquement clos.

Exemple 60 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$.

Proposition 61 : L'ensemble $\{x\in\mathbb{C}\mid x \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$. — Dév 1

Théorème 62 (Steinitz) : Tout corps $\mathbb{K}$ admet une clôture algébrique. Si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont deux clôtures algébriques de $\mathbb{K}$, alors $\mathbb{K}_1$ et $\mathbb{K}_2$ sont $\mathbb{K}$-isomorphes.

III. Quelques exemples fondamentaux d'extensions de corps.

1. Extensions quadratiques.

Proposition 63 : Soit $d \in \mathbb{N}$, $d \geq 2$. Les conditions suivantes sont équivalentes :
(i). $\sqrt{d} \notin \mathbb{Q}$
(ii). $\sqrt{d} \notin \mathbb{N}$
(iii) il existe p premier tel que $v_p(d)$ impair.
(iv). $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.

Exemple 64 : Soit $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{Q}$. Alors $\mathbb{Q}(\sqrt{2})$ est une extension de degré 2 sur $\mathbb{Q}$ et $(1, \sqrt{2})$ est une base du $\mathbb{Q}$-ev $\mathbb{Q}(\sqrt{2})$.
Soit $\alpha \in \mathbb{Q}(\sqrt{d})$. $\exists! (x,y) \in \mathbb{Q}^2$ / $\alpha = x + y\sqrt{2}$. Le polynôme minimal de α sur $\mathbb{Q}$ est soit $X - \alpha$, ou $X^2 - 2xX + x^2 - dy^2$.

Définition 65 : On appelle corps quadratique toute extension de degré 2 de $\mathbb{Q}$ dans $\mathbb{C}$.

Exemple 66 : $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{Q}$. Alors $\mathbb{Q}(\sqrt{d})$ est un corps quadratique.

Théorème 67 : Soit $\mathbb{L}$ un corps quadratique. Il existe $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré tel que $\mathbb{L} = \mathbb{Q}(\sqrt{d})$.

2. Corps finis.

Proposition 68 : Soit $p \geq 2$ un entier. $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier. Dans ce cas, on le note $\mathbb{F}_p$.

Théorème 69 : Soit F un corps fini. Alors :
- Sa caractéristique est un nombre premier p.
- Son sous-corps premier est isomorphe à $\mathbb{F}_p$.
- Il existe $n \in \mathbb{N}^*$ tel que $|F| = p^n$.

Proposition / Définition 70 : Soit $\mathbb{K}$ un corps de caractéristique p premier. L'application $\mathcal{F}_r : \begin{array}{l} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto x^p \end{array}$ est un $\mathbb{F}_p$-endomorphisme de $\mathbb{K}$, appelé endomorphisme de Frobenius de $\mathbb{K}$.
- Si $\mathbb{K}$ est fini, alors $\mathcal{F}_r$ est un automorphisme.
- Si $\mathbb{K} = \mathbb{F}_p$, alors $\mathcal{F}_r$ est l'identité.

Théorème 71 : Soient p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$. Alors :
- il existe un corps fini à q éléments. Il est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.
- Si F et F' sont deux corps à q éléments, alors ils sont $\mathbb{F}_p$-isomorphes.

Définition 72 : On note $\mathbb{F}_q$ "le" corps (à isomorphisme près) à q éléments.

Théorème 73 : Soient p premier, $n \in \mathbb{N}^*$. On note $q = p^n$. Alors $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Corollaire 74 :
- Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.
- Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors π divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$. Son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(\pi)$ est aussi son corps de décomposition.

Exemple 75 : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ $\quad \mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$ $\quad \mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+X-1)$

Remarque 76 : $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$.

Théorème 77 : Soient p premier, $n \in \mathbb{N}^*$ et $q := p^n$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{F}_q$, il existe d diviseur de n tel que $|\mathbb{K}| = p^d$.
- pour chaque diviseur d de n, $\mathbb{F}_q$ possède un unique sous-corps de cardinal p^d, isomorphe à $\mathbb{F}_{p^d}$.

Corollaire 78 : $\mathbb{F}_q$ est un sous corps de $\mathbb{F}_{q'}$ ssi q' est une puissance de q.

Théorème 79 (de l'élément primitif, corps finis) : Soit $\mathbb{K}$ un corps fini. Soit $\mathbb{L}/\mathbb{K}$ une extension de degré fini. Alors $\mathbb{L}/\mathbb{K}$ est une extension monogène.

3. Corps cyclotomiques. Soit $n \in \mathbb{N}^*$.

Proposition / Définition 80 :
- Soit $\mathbb{U}_n := \{z \in \mathbb{C} \,/\, z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$. Alors $\mathbb{U}_n$ est un groupe cyclique d'ordre n pour la multiplication.
- On appelle racine primitive n-ième de l'unité tout générateur de $\mathbb{U}_n$.
- On notera $\mathcal{P}_n$ l'ensemble des racines primitives n-ièmes de l'unité.

Proposition 81 : $\mathcal{P}_n$ est de cardinal $\varphi(n)$.

Proposition 82 : Soit $\xi \in \mathbb{C}$ une racine primitive n-ième de l'unité. On a alors $\mathcal{P}_n = \{\xi^k,\ k \in [\![1,n]\!],\ k \wedge n = 1\}$.

Proposition / Définition 83 : Soit ξ une racine primitive $n$ième de l'unité. Le sous-corps $\mathbb{Q}(\mathbb{U}_n)$ de $\mathbb{C}$ est égal à $\mathbb{Q}(\xi)$ et est appelé corps cyclotomique d'indice n.

Définition 84 : On appelle n-ième polynôme cyclotomique le polynôme
$$\Phi_n(X) = \prod_{\xi \in \mathcal{P}_n} (X - \xi).$$

Remarque 85 :
- Φ_n est un polynôme unitaire de degré $\varphi(n)$ de $\mathbb{C}[X]$.
- Φ_n est à racines simples sur $\mathbb{C}$.

Exemple 86 : $\Phi_1 = X - 1$ $\quad \Phi_2 = X + 1$ $\quad \Phi_3 = X^2 + X + 1$

Proposition 87 : $X^n - 1 = \prod_{d \mid n} \Phi_d$.

Exemple 88 : $\Phi_4 = \dfrac{X^4 - 1}{\Phi_2 \Phi_1} = \dfrac{(X^2-1)(X^2+1)}{(X-1)(X+1)} = X^2 + 1$.

Lemme 89 : Soient $P, A, B \in \mathbb{Q}[X] \setminus \{0\}$. On suppose $P \in \mathbb{Z}[X]$, $P = AB$ et P et A unitaires. Alors $A, B \in \mathbb{Z}[X]$.

Proposition 90 : $\Phi_n \in \mathbb{Z}[X]$.

Lemme 91 : Soit p premier, $p \nmid n$. Alors Φ_n n'a que des racines simples dans tout corps de caractéristique p.

Théorème 92 : Φ_n est irréductible dans $\mathbb{Q}[X]$.] Dév 2.

Corollaire 93 : Soit $\xi \in \mathbb{C}$ une racine primitive n-ième de l'unité. Son polynôme minimal sur $\mathbb{Q}$ est Φ_n.
On a donc $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.