I. Extensions de corps: algébricité:

1°- Sous-corps et extension de corps, morphismes.

Définition: Soit $K \subset L$, deux corps: On dit que L est un sous-corps de K! Plus généralement, si K et L sont deux corps et ϕ est un morphisme ~~de~~ K vers L, on dit que L est une extension de K. L est naturellement muni d'une structure de k-algèbre avec ϕ pour morphisme structural.

Définition: Si $k \hookrightarrow L$ et $k \hookrightarrow L'$ sont deux extensions, un k-morphisme de L vers L' est un morphisme de corps k-linéaire.

Dans la suite toutes les extensions de k sont des sous-corps, avec pour morphisme ϕ l'inclusion.

Définition: Si $k \hookrightarrow L$ est une extension. Si $S \subset L$, un ensemble, on note: $k(S)$ le plus petit sous corps de L contenant S et k. $k[S]$ le plus petit sous anneau de L contenant k et S.

En général $k[S] \subsetneq k(S)$

Exemple: On considère $\mathbb{Q} \hookrightarrow \mathbb{C}$. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2}, a,b \in \mathbb{Q}\}$. On a $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$.

2°- Éléments algébriques, extensions algébriques.

On fixe une extension $k \hookrightarrow L$!

Définition: Un élément $\xi \in L$ est dit algébrique sur k s'il est racine d'un polynôme à coefficient dans k. Dans le cas contraire, il est dit transcendant.

Ex: $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, i est algébrique sur $\mathbb{Q}$. π est transcendant sur $\mathbb{Q}$ (Lindemann, 1882)

Définition: Le polynôme annulateur d'un élément algébrique ξ est défini par: 1- $\Pi_\xi(\xi)=0$ 2- Π_ξ est unitaire 3- Si $P(\xi)=0$ alors $\Pi_\xi | P$.

Rmq: Sa définition relève de la principalité de $k[X]$.

Proposition: Π_ξ est un polynôme irréductible de $k[X]$.

EX: $\Pi_{\sqrt{2}} = X^2-2$, $\Pi_j = X^2+X+1$.

Proposition: (Caractérisation des éléments algébriques)

1. ξ est algébrique
2- $k[\xi] = k(\xi)$
3- $\dim k[\xi] < +\infty$. L'extension est dite finie.

Si ξ est algébrique, $k[\xi] \simeq k[X]/(\Pi_\xi)$ et $(1, \xi, \dots, \xi^{d-1})$ est une base de $k[\xi]$.

Définition: Une extension algébrique est une extension où tous les éléments sont algébriques.

Une extension séparable est une extension algébrique où tous les polynômes Π_ξ, $\xi \in k$ sont séparables.

Proposition: Une extension de dimension finie séparable est monogène ie il existe $\theta \in L$ tel que $k[\theta] = L$. θ est un élément primitif.

Proposition: Une extension de degré fini $k \hookrightarrow L$. Elle est monogène ssi le nombre de sous extensions $k \hookrightarrow L' \subset L$ est fini.

Rmq: Lorsque l'extension est monogène, on peut décrire ces sous extensions! Ce sont les extensions de k engendrées par les coefficients des diviseurs dans $L[X]$ du polynôme minimal d'un élément θ primitif de $k \hookrightarrow L$.

3°- Algèbre linéaire

La dimension L en tant que k-ev est appelé degré de l'extension, noté $[L:k]$

Théorème: (Base télescopique) Si $k \hookrightarrow L^1 \hookrightarrow L^2$, alors:

$$[L^2:k] = [L^2:L^1][L^1:k]$$

Corollaire: Si ξ_1 et ξ_2 sont algébriques alors $[k[\xi_1,\xi_2]:k] < +\infty$.
$\forall P \in k[X,Y]$ $P(\xi_1,\xi_2)$ est algébrique!

Ex: $1+\sqrt{2}$ est algébrique, $\sqrt{j} + e^{\frac{2i\pi}{5}} - 7$ est algébrique.

Définition: On note m_ξ l'endomorphisme k-linéaire de multiplication par ξ. La norme de ξ, $N_k(\xi)$ est le déterminant de m_ξ. La trace de ξ est la trace de cet endomorphisme.

Proposition: Pour $k = \mathbb{Q}$, et $k \hookrightarrow L \subset \mathbb{C}$. Si $x_1, \dots, x_r$ sont les racines de Π_ξ dans $\mathbb{C}$ alors: $N(\xi) = (x_1 \cdots x_r)^{[L:k(\xi)]}$ et $Tr(\xi) = [L:k(\xi)] \sum_{i=1}^{r} x_i$

Exemples: Dans $\mathbb{Q}(\sqrt{2})$ on a $N(a+b\sqrt{2}) = a^2-2b^2$, $tr(a+b\sqrt{2}) = 2a$.
Dans $\mathbb{Q}(i)$ on a $N(a+bi) = a^2+b^2$ et $tr(a+bi) = 2a$.

II- Extensions de corps remarquables

1° des extensions cyclotomiques: Soit K un corps (de caractéristique finie ou non) soit $n \geq 0$ (premier avec la caractéristique ou non) Soit D_n un corps de décomposition de $X^n - 1$ sur k.

Définition : Le polynôme cyclotomique $\Phi_n^k(X)$ est égal à :
$\Phi_n(X) = \prod_{i \in \mathbb{Z}/N\mathbb{Z}^\times} (X - \zeta^i)^{\varphi(p^{v_p(n)})}$ où $\mu_n \cong \mathbb{Z}/N\mathbb{Z}^\times = (\mathbb{Z}/\frac{n}{p^{v_p(n)}}\mathbb{Z})^\times$ avec la convention $v_0(n) = 0$ $= \Phi_N(X)^{\varphi(p^{v_p(n)})}$

Rmq : $\Phi_n(X) \in D_n = D(X^n - 1)$.

Proposition : (Polynôme cyclotomique sur $\mathbb{Q}$). 1. $\Phi_n^{\mathbb{Q}}(X) = \prod_{ord(\zeta)=n} (X - \zeta)$
2. $\deg \Phi_n(X) = \varphi(n)$ (Ind. d'Euler) 3. $\Phi_n(X) \in \mathbb{Z}[X]$
4. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Rmq 4 est vraie pour tout corps.

Proposition : $\Phi_n(X) \in \mathbb{Z}[X]$ $\forall n \geq 1$. Si K est un corps et $\tau : \mathbb{Z} \to K$ le morphisme canonique alors $\Phi_n^k(X) = \tau \cdot \Phi_n^{\mathbb{Q}}(X)$.
En particulier, $\Phi_n^k(X)$ appartient au corps primitif de k ($\mathbb{Q}$ ou $\mathbb{F}_p$)

Proposition : Les polynômes cyclotomiques $\Phi_n^{\mathbb{Q}}(X)$ sont irréductibles sur $\mathbb{Q}[X]$. Si ζ est une racine $n^{\text{ème}}$ de l'unité, $\mathbb{Q}(\zeta)$ est une extension cyclotomique d'ordre n et est de degré $\varphi(n)$

Application : Constructibilité des polygones réguliers

Proposition (Gauss-Wantzel) : Soit $z \in \mathbb{C}$, il est constructible à la règle et au compas ssi $\mathbb{Q}[\zeta]$ est une tour d'extension quadratique, i.e s'il existe $L_0 = \mathbb{Q} \subset L_1 \dots \subset L_n = \mathbb{Q}(\zeta)$ tel que $[L_{i+1} : L_i] = 2$.
On s'intéresse à la constructibilité du polygone à n côtés, ou au découpage du cercle en n arcs égaux.

Proposition : Le problème précédent est équivalent à la constructibilité de $\zeta = e^{\frac{2i\pi}{n}}$.

$\zeta = e^{\frac{2i\pi}{n}}$. On sait que si le polygone à n côtés est constructible, celui à $2n$ côtés l'est également : il suffit de construire des bissectrices.

Proposition : Le polygone à n côtés est constructible ss. $n = 2^k F_{i_1} \dots F_{i_r}$ avec F_i des nombres de Fermat.

Remarque : La démonstration repose sur la correspondance de Galois et une condition nécessaire et suffisante pour que l'extension $\mathbb{Q}(\zeta)$ soit de degré une puissance de 2.
On a la même condition pour le découpage de la lemniscate en arcs égaux.

Application 2 : Le critère de Frobenius de Burnside-Schur : Si $G \subset GL_n(\mathbb{C})$ est de torsion et de type fini, alors il est fini. DEVPT 1

2° - Corps finis :

Proposition : Soit $m \geq 0$. 1 Il existe un corps fini à m éléments ss. m est une puissance d'un nombre premier.
2. Si $m = p^r$ et si deux corps finis à p^r éléments sont toujours isomorphes. On note le corps fini $\mathbb{F}_{p^r}$
3. $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$ ssi $r | n$. 4. $\mathbb{F}_{p^r}$ est une extension de degré r de $\mathbb{F}_p$ et c'est le corps de décomposition de $X^{p^r} - 1$ sur $\mathbb{F}_p$.
4. $X^{p^r} - 1 = \prod Q$ où Q parcourt les irréductibles unitaires de $\mathbb{F}_p[X]$

Exemple : $\mathbb{F}_2[X]/_{X^2+X+1}$ est une présentation du corps fini à 4 éléments.

Proposition et définition : l'application $Fr : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$, $x \mapsto x^p$ est un isomorphisme de corps $\mathbb{F}_p$ linéaire d'ordre r.

3° - Fermeture algébrique - Clôture algébrique

Soit $k \hookrightarrow L$ une extension.

Définition : On appelle clôture algébrique de k dans L l'ensemble des éléments de L qui sont algébriques sur k.

Proposition : $\bar{k}^{(L)}$ est un sous-corps de L. Si $P \in \bar{k}^{(L)}[X]$ et $x \in L$ est une racine de P alors $x \in \bar{k}^{(L)}$.

Ex : $\mathbb{C}$ est algébriquement clos. $\bar{\mathbb{Q}}^{(\mathbb{C})}$ est une clôture algébrique de $\mathbb{Q}$.

Application : Théorème de Rothstein-Trager : Si $F = \frac{P}{Q} \in \mathbb{Q}(X)$, Q est sans facteurs carrés. Si $Res_x(P - YQ', Q)$ a pour racines x_i et si $v_i = pgcd(P - x_iQ', Q)$ alors : $\int \frac{P}{Q} = \sum_{R(x_i)=0} x_i \ln(v_i)$ DEVPT 2.

Rmq : Une clôture algébrique est une extension algébrique maximale au sens où si $k \hookrightarrow L$ est une autre extension algébrique, alors elle s'injecte k-linéairement dans une clôture algébrique.

Théorème (Steinitz) : Une clôture algébrique existe toujours et est unique à isomorphisme près.

Ex : Si Ω est une clôture algébrique de $\mathbb{F}_p$, si (n_i) est une suite d'entiers telle que $n_i | n_{i+1}$ et $i | n_i$ alors $\bigcup \mathbb{F}_{p^{n_i}} \subset \Omega$ est une clôture algébrique de $\mathbb{F}_p$.

4° - Extension d'Artin-Schreier :

Définition : Soit k un corps. Une extension d'Artin-Schreier de k est une extension de k engendrée par une racine ζ du polynôme

$f(X) = X^p - X - a$ avec $p = car(k)$.

Proposition: Le polynôme $f(X)$ précédent vérifie: Si il admet une racine α dans k, alors toutes ses racines sont dans k, Rac $f = \{\alpha + i, i = 1..p\}$.

S'il n'admet aucune racine dans k, il est irréductible.

III - Groupe d'automorphismes.

Soit $k \hookrightarrow L$ une extension de degré fini.

1° - Degré et cardinalité

Proposition: Soit $k \hookrightarrow E$ une extension algébrique de k degré fini. alors on a toujours $\# Hom_{k\text{-}al}(E, L) \leq [E : k]$

Rmq: En dimension finie, l'étude du groupe $Hom_k(E, L)$ est donc affaire de théorie des groupes finis.

Proposition: Si $k \hookrightarrow E$ est l'extension de décomposition d'un polynôme P alors pour tout surcorps $E \subset L$, algébriquement clos, on a $Hom_{k\text{-}alg}(E, L) = Aut_k(E)$

Proposition: (Caractérisation de la séparabilité). Soit $k \hookrightarrow L$ une extension algébriquement close. Soit $k \hookrightarrow E$ une seconde extension de degré fini. Alors $k \hookrightarrow E$ est séparable ssi $[E : k] = \# Hom_k(E, L)$

Rmq: En particulier, pour une extension de degré fini séparable qui est le corps de décomposition d'un polynôme P alors $\# Aut_k(E) = [E : k]$

. Un automorphisme $\sigma : E \to E$, k linéaire permute les racines d'un polynôme $P \in k[X]$. Plus précisément les racines d'un même facteur irréductible de P.

. On note $Gal(E, k) = Aut_k(E)$.

2° - Groupe d'automorphismes des extensions du II.

. Extensions cyclotomiques sur $\mathbb{Q}$: Si ζ est une racine primitive $n$ième de l'unité alors $Aut_{\mathbb{Q}}[\mathbb{Q}[\zeta]] \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

. Extensions cyclotomiques en caractéristique finie: Si $p = car(k)$. Si n est premier à p. Si ζ est une racine du $n$ième polynôme cyclotomique et si w est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$ alors $\dim_k k[\zeta] = w$, On a $\# Aut_k k[\zeta] = w$ isomorphe à $\mathbb{Z}/w\mathbb{Z}$.

. Les corps finis: Le groupe de galois de l'extension de degré n, $\mathbb{F}_{p^n}$ est cyclique et engendré par le Frobenius.

Les derniers groupes étaient cycliques... :

. Le groupe d'Automorphismes de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ est le groupe de Klein.

3° - Caractérisation des extensions cycliques:

On appelle extension cyclique une extension séparable, de degré fini, étant le corps de décomposition d'un polynôme dont le groupe d'Automorphisme est cyclique.

Proposition: Soit k un corps de caractéristique p. Soit $\mathbb{K}$ une extension cyclique de k de degré n.

1. Si k possède une racine primitive $n$ième de l'unité, $n \wedge p = 1$ alors $\mathbb{K} = k(\alpha)$ avec α une racine de $X^n - a$, $a \in k$.
2. Si $n = p$ alors $\mathbb{K} = k(\alpha)$ avec α une racine de $X^p - X - a$.

Proposition: (Réciproque).

1. Avec les mêmes hypothèses que dans 1 pré. si α est une racine de $X^n - a$ alors $k(\alpha)$ est cyclique de degré d et $\alpha^d \in k$.
2. Si $f(X) = X^p - X + a$ est irréductible alors $k(\alpha)$ est une extension cyclique de degré p.

Autres choses: a - Résolubilité par Radicaux. b - Extensions transcendantes.

Ref: . bib : + Tauvel: Galois. + Lang: Algebra + Artin: Algebra + Escoffier: Galois. Ian Stewart: Galois