**École Normale Supérieure de Lyon** **Année 2014–2015**

**AGNIEL Vidal** **Stage - Théorie de Galois**

RAPPORT DE STAGE

# Table des matières



# 1 Extensions normales

**1.1 Définition.** — Soit $\mathbb{K}$ un corps et L/$\mathbb{K}$ une extension de corps algébrique. L est **normale** si et seulement si $\forall P \in \mathbb{K}[X]$ irréductible avec une racine dans L, P est scindé sur L.

**1.2 Proposition.** — *On a l'équivalence :*

*i) L/$\mathbb{K}$ est une extension normale*

*ii) L est un corps de décomposition d'une famille de polynômes sur $\mathbb{K}$.*

*iii) $\forall \sigma : \bar{\mathbb{K}} \to \bar{\mathbb{K}}$ morphisme tel que $\sigma_{\mathbb{K}} = id_{\mathbb{K}}$, $\sigma$(L)=L.*

**1.3 Proposition.**

*Pour toute extension L/$\mathbb{K}$ algébrique finie, il existe une extension normale N/$\mathbb{K}$ qui contient L/$\mathbb{K}$.*

*Si L/$\mathbb{K}$ est normale, et si L'/$\mathbb{K}$ est une sous-extension de L/$\mathbb{K}$, alors L/L' est normale.*

*Soient $L_1/\mathbb{K}$ et $L_2/\mathbb{K}$ des sous-extensions de $L/\mathbb{K}$. Si $L_1/\mathbb{K}$ est normale et finie, alors $L_2L_1/L_2$ est normale et finie.*

*Si $L_1/\mathbb{K}$ et $L_2/\mathbb{K}$ sont finies normales, alors $L_1L_2/\mathbb{K}$ et $L_1 \cap L_2/\mathbb{K}$ sont finies normales.*

## 2 Extensions séparables

**2.1 Définition.** — $\alpha \in L$ est **séparable** sur $\mathbb{K}$ si et seulement si le polynôme minimal de $\alpha$ sur $\mathbb{K}$, $Irr(\alpha, \mathbb{K})$, est à racines simples dans une clôture algébrique de L.

L est **séparable** sur $\mathbb{K}$ si et seulement si tous ses éléments sont séparables sur $\mathbb{K}$.

Un polynôme non nul $P \in \mathbb{K}[X]$ est **séparable** sur $\mathbb{K}$ si et seulement s'il est à racines simples sur une clôture algébrique $\bar{\mathbb{K}}$ de $\mathbb{K}$.

**2.2 Proposition.** — *Si L/$\mathbb{K}$ est séparable, pour toute sous-extension L'/$\mathbb{K}$ de L/$\mathbb{K}$, L/L' est une extension séparable.*

**2.3 Lemme.** — *Soient $\alpha_1, \ldots, \alpha_n \in L$ séparables sur $\mathbb{K}$. Alors le nombre d'isomorphismes $\sigma$ de $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ dans une clôture algébrique $\bar{\mathbb{K}}$ de $\mathbb{K}$ tels que $\sigma_{\mathbb{K}} = id_{\mathbb{K}}$ est égal à $[\mathbb{K}(\alpha_1, \ldots, \alpha_n) : \mathbb{K}]$.*

*De tels morphismes sont appelés $\mathbb{K}$-isomorphismes de $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ dans $\bar{\mathbb{K}}$.*

*Démonstration.* On prend $\bar{\mathbb{K}}$ une clôture algébrique de L, et donc de $\mathbb{K}$, pour utiliser le théorème de prolongement des $\mathbb{K}$-isomorphismes de $\mathbb{K}(\alpha_1, \ldots, \alpha_i)$ à $\mathbb{K}(\alpha_1, \ldots, \alpha_{i+1})$ $\forall i \in \{1, .., n-1\}$ : chaque $\mathbb{K}$-isomorphisme de $\mathbb{K}(\alpha_1, \ldots, \alpha_i)$ dans $\bar{\mathbb{K}}$ se prolonge en deg($Irr(\alpha_{i+1}, \mathbb{K})$) $\mathbb{K}$-isomorphismes de $\mathbb{K}(\alpha_1, \ldots, \alpha_{i+1})$ dans $\bar{\mathbb{K}}$. Ce qui en fait un total de $\prod_i (Irr(\alpha_i, \mathbb{K})) = [\mathbb{K}(\alpha_1, \ldots, \alpha_n) : \mathbb{K}]$. □

**2.4 Proposition.** — *Si L/L' et L'/$\mathbb{K}$ sont algébriques séparables finies, L/$\mathbb{K}$ est algébrique séparable.*

*Démonstration.* Soit $\alpha \in L$ et $\bar{\mathbb{K}}$ une clôture algébrique de L. On a $Irr(\alpha, L')$(X) = $\sum_{i=1}^{d} a_i X^i$, $a_i \in L'$. On pose $L_1 = \mathbb{K}a_1, \ldots, a_n$. $L_1(\alpha)/L_1$ et $L_1/\mathbb{K}$ sont séparables, et on a ainsi $[L_1(\alpha) : L_1] \times [L_1 : \mathbb{K}] = [L_1(\alpha) : \mathbb{K}]$ $\mathbb{K}$-isomorphismes de $L_1$ dans $\bar{\mathbb{K}}$, d'où $[\mathbb{K}(\alpha) : \mathbb{K}]$ $\mathbb{K}$-isomorphismes de $\mathbb{K}(\alpha)$ dans $\bar{\mathbb{K}}$ par maximalité du nombre de $\mathbb{K}$-isomorphismes. Ainsi, Irr($\alpha, \mathbb{K}$) a $[\mathbb{K}(\alpha) : \mathbb{K}]$=deg(Irr($\alpha, \mathbb{K}$)) racines distinctes, et est donc à racines simples sur $\bar{\mathbb{K}}$. □

**2.5 Proposition.** — *Si $L_1/\mathbb{K}$ et $L_2/\mathbb{K}$ sont finies et séparables, alors $L_1L_2/\mathbb{K}$ et $L_1 \cap L_2/\mathbb{K}$ sont finies et séparables.*

**2.6 Proposition.** — *$Irr(\alpha, \mathbb{K})$ est à racines simples si et seulement si $Irr(\alpha, \mathbb{K}) \wedge Irr(\alpha, \mathbb{K})' = 1$ dans $\mathbb{K}$.*

*Si car($\mathbb{K}$)=0, tout polynôme P$\in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ est séparable.*

*Si $\mathbb{K}$ est un corps fini de caractéristique p, p premier, tout polynôme P$\in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ est séparable.*

*Ainsi, toute extension algébrique d'un corps de caractéristique nulle ou fini est séparable.*

*Démonstration.* P étant irréductible, P∧P' = 1 ou P. Comme deg(P')<deg(P), P∧P'=P ⇔ P'=0. En caractéristique 0, cela est impossible car les polynômes irréductibles sont de degré au moins 1, et leurs polynômes dérivés de degré au moins 0.

Sur un corps fini de caractéristique p, P'=0 ⇔ ∃ Q $\in \mathbb{K}[X]$ tel que P(X) = $Q(X^p)$= $\sum_{i=1}^{d} a_i X^{p.i}$, $a_i \in \mathbb{K}$. Le corps étant fini, l'endomorphisme de Frobenius est alors un isomorphisme sur $\mathbb{K}$, et $\forall i \in \{1, .., d\}$, $\exists b_i \in \mathbb{K}$ tels que $b_i^p = a_i$. Ainsi, P(X)= $\sum_{i=1}^{d} b_i^p X^{p.i}$ = $(\sum_{i=1}^{d} b_i X^i)^p$ , et est réductible, ce qui est impossible. □

**2.7 Théorème.** *(de l'élément primitif)*

*Soit L/$\mathbb{K}$ finie séparable. Alors $\exists \alpha \in L$ tel que $L = \mathbb{K}(\alpha)$.*

**2.8 Proposition.** — *Si L/$\mathbb{K}$ est séparable finie, alors pour toute clôture normale M de L/$\mathbb{K}$, M/$\mathbb{K}$ est séparable, normale, et finie.*

*Démonstration.* Il existe $\alpha_1, .., \alpha_n \in L$ tels que L= $\mathbb{K}(\alpha_1, .., \alpha_n)$. Ainsi, les Irr($\alpha_i, \mathbb{K}$) sont séparables sur $\mathbb{K}$, et M étant engendré par $\mathbb{K}$ et par les racines de ces polynômes dans une clôture algébrique de $\mathbb{K}$ contenant L, l'extension M/$\mathbb{K}$ est séparable, normale, et finie. □

### 2.1 Critère de séparabilité

**2.9 Définition.** — Soit $\mathbb{K}$ un corps. Soit n$\in \mathbb{N}$. On pose $\delta(X_1, ..X_n) = \prod_{i<j}(X_i - X_j)$.

$\delta(X_1, ..X_n)^2 = (-1)^{n(n-1)/2} \prod_{i\neq j}(X_i - X_j) \in \mathbb{K}[X_1, ..X_n]^{S_n}$.

On note $Q_n$ le polynôme de $\mathbb{K}[X_1, ..X_n]$ tel que $\delta(X_1, ..X_n)^2 = Q_n(\sum_{1,n}, .., \sum_{n,n})$.

Soit P$\in \mathbb{K}[X]$, P(X)=$a_0X^d + ... + a_n$, d=deg(P).

On note **disc(P)**=$a_0^2 Q_d((-1)a_1/a_0, .., (-1)^i a_i/a_0, .., (-1)^n a_n/a_0) \in \mathbb{K}$ le **discriminant** de P.

**2.10 Exemple.** *Pour n=2,* $\delta(X,Y)^2=(X-Y)^2=(X+Y)^2 - 4XY$, $\Rightarrow Q_2(X,Y) = X^2 - 4Y$, $\Rightarrow$ *pour P(X)=*$aX^2 + bX + c$, *disc(P)=*$a^2((b/a)^2 - 4(a/c)) = b^-4ac$.

**2.11 Proposition.** *Critère de séparabilité — P est séparable sur* $\mathbb{K} \Leftrightarrow$ *disc(P)*$\neq 0$.

**2.12 Corollaire.** — *Soit* $P \in \mathbb{Z}[X]$. *S'il existe p premier tel que* $\bar{P}$ *est séparable sur* $\mathbb{F}_p$, *alors P est séparable sur* $\mathbb{Q}$.

**2.13 Proposition.** — *Soient P(X)=*$\prod_{i=1}^n (X - a_i)$ *et P'(X)=*$n\prod_{j=1}^{n-1}(X - b_j)$ *dans* $\bar{\mathbb{K}}[X]$.

*On a : disc(P)=*$\prod_{i<j}(a_i - a_j)^2 = (-1)^{n(n-1)/2}\prod_{i=1}^n P'(a_i) = (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} P(b_j)$.

**2.14 Corollaire.** — *Disc(*$X^n + aX + b$*)=*$(-1)^{n(n-1)/2}((1-n)^{n-1}a^n + n^n b^{n-1})$.

**2.15 Exemple.** *Pour P(X)=*$X^3 + aX + b$, *disc(P)=*$-4a^3 - 27b^2$.

## 3 Extensions galoisiennes

**3.1 Définition.** — Soit L/$\mathbb{K}$ une extension de corps algébrique. L/$\mathbb{K}$ est **galoisienne** si et seulement si elle est normale et séparable.

Le groupe des automorphismes de L préservant $\mathbb{K}$ est alors appelé groupe de Galois de L/$\mathbb{K}$, et est noté Gal(L/$\mathbb{K}$).

**3.2 Définition.** — Soit P$\in \mathbb{K}$[X]. On appelle **groupe de Galois** de P sur $\mathbb{K}$ le groupe Gal(M/$\mathbb{K}$), où M est un corps de décomposition de P sur $\mathbb{K}$.

**3.3 Théorème.** — *Si L/*$\mathbb{K}$ *est galoisienne et finie, alors Gal(L/*$\mathbb{K}$*) est d'ordre [L :*$\mathbb{K}$*].*

*Démonstration.* Soit $\bar{\mathbb{K}}$ une clôture algébrique de L. Il y a [L :$\mathbb{K}$] $\mathbb{K}$-isomorphismes de L dans $\bar{\mathbb{K}}$ d'après le lemme, car L/$\mathbb{K}$ est finie et séparable, et ces $\mathbb{K}$-isomorphismes sont des $\mathbb{K}$-automorphismes car L/$\mathbb{K}$ est normale. □

**3.4 Proposition.** — *Soient* $L_1/\mathbb{K}$ *et* $L_2/\mathbb{K}$ *des sous-extensions de* $L/\mathbb{K}$. *Si* $L_1/\mathbb{K}$ *est galoisienne et finie, alors* $L_2L_1/L_2$ *est galoisienne et finie.*

*Si* $L_1/\mathbb{K}$ *et* $L_2/\mathbb{K}$ *sont finies galoisiennes, alors* $L_1L_2/\mathbb{K}$ *et* $L_1 \cap L_2/\mathbb{K}$ *sont finies galoisiennes.*

*Si* $L_1/\mathbb{K}$ *et* $L_2/\mathbb{K}$ *sont galoisiennes et finies, alors* $L_1L_2/\mathbb{K}$ *et* $L_1 \cap L_2/\mathbb{K}$ *sont galoisiennes et finies*

*Si* $L_1/\mathbb{K}$ *est galoisienne et si* $L_2/\mathbb{K}$ *est une sous-extension de* $L_1/\mathbb{K}$, *alors* $L_1/L_2$ *est galoisienne.*

*Démonstration.* Ces propriétés sont vérifiées pour la normalité et la séparabilité. □

**3.5 Remarque.** — *Si L/*$\mathbb{K}$ *extension galoisienne finie, alors Gal(L/*$\mathbb{K}$*) est isomorphe à un sous-groupe du groupe des permutations des racines d'un polynôme de* $\mathbb{K}$*[X].*

# 4 Corps fixes, correspondance de Galois

**4.1 Définition.** — Soit K un corps et H $\subset$ Aut(K). Alors $\{x \in$ K tels que $\sigma$ (x)=x $\forall \sigma \in H\}$ est un sous-corps de K fixe par H, noté $K^H$.

**4.2 Lemme.** — *Soit L/$\mathbb{K}$ extension galoisienne, et G :=Gal(L/$\mathbb{K}$).*

1. *Soit L' = $L^G$. Alors L'=$\mathbb{K}$.*
2. *Soit L'/$\mathbb{K}$ une sous-extension de L/$\mathbb{K}$. Alors L/L' est une extension galoisienne, et Gal(L/L') = $\{\sigma \in$ G tels que $\sigma(x) = x$, $\forall x \in L'\}$.*

*Démonstration.* 1. On a $\mathbb{K} \subseteq$ L'. De plus, pour tout $\sigma \in$ G, $\sigma_{L'} = id_{L'}$, donc Gal(L/$\mathbb{K}$) $\subseteq$ Gal(L/L'), donc [L :$\mathbb{K}$] $\geq$ [L :L'], d'où l'égalité et $\mathbb{K}$=L'.

2. L/L' est normale et séparable, donc galoisienne, et Gal(L/L') $\subseteq$ Gal(L/$\mathbb{K}$) avec une restriction sur L' étant l'identité.

□

**4.3 Lemme.** *(d'Artin) — Soit $\mathbb{K}$ un corps, et H un sous-groupe fini de Aut($\mathbb{K}$). Alors l'extension $\mathbb{K}/\mathbb{K}^H$ est finie galoisienne et Gal($\mathbb{K}/\mathbb{K}^H$)=H.*

*Démonstration.* Soit $\alpha \in \mathbb{K}$. Soit $\{\sigma_1, .., \sigma_r\}$ un ensemble dans H de taille maximale vérifiant : $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, $\forall i \neq j$. Soit P(X)=$\prod_{i=1}^{r}(X - \sigma_i(\alpha)$. $\forall \tau \in H$, $\tau$(P(X))=P(X) par maximalité de $\{\sigma_1, .., \sigma_r\}$. Donc $\alpha$ est algébrique et séparable sur $\mathbb{K}^H$. De plus, toutes les racines de P(X) sont dans $\mathbb{K}$, donc $\mathbb{K}/\mathbb{K}^H$ est normale, donc galoisienne.

Si [$\mathbb{K} : \mathbb{K}^H$]>|H|, on a $\alpha_1, .., \alpha_n \in \mathbb{K}$ tels que |H| < [$\mathbb{K}^H(\alpha_1, .., \alpha_n) : \mathbb{K}^H$] < $\infty$. L'extension étant finie et séparable, elle est simple. Mais $\forall \alpha \in \mathbb{K}$, [$\mathbb{K}^H(\alpha) : \mathbb{K}^H$]$\leq$ |H|, contradiction.

Donc [$\mathbb{K} : \mathbb{K}^H$]$\leq$|H|. De plus, H$\subseteq$Gal($\mathbb{K} : \mathbb{K}^H$), donc |Gal($\mathbb{K} : \mathbb{K}^H$)|$\geq$|H|, d'où l'égalité. □

**4.4 Théorème.** *(Correspondance de Galois) — Soit L/$\mathbb{K}$ une extension finie galoisienne, et soit G :=Gal(L/$\mathbb{K}$). Il existe une bijection entre l'ensemble des sous-extensions L'/$\mathbb{K}$ de L/$\mathbb{K}$ et l'ensemble des sous-groupes H de G donnée par :*

*H $\mapsto$ $L^H$*

*et la bijection réciproque est donnée par :*

*L' $\mapsto$ Gal(L/L')*

*Démonstration.* On étudie L' $\mapsto$ Gal(L'/$\mathbb{K}$). L'application est bien définie car L/L' est galoisienne, et Gal(L/L')$\subseteq$Gal(L/$\mathbb{K}$).

Injectivité. Soient $L_1/\mathbb{K}$ et $L_2/\mathbb{K}$ des sous-extensions telles que Gal(L/$L_1$)=Gal(L/$L_2$). Soit $\sigma \in$Gal(L/$L_1$). La restriction de $\sigma$ à $L_1L_2$ est l'identité, donc $\sigma \in$ Gal(L/$L_1L_2$), d'où [L :$L_1L_2$]=[L :$L_1$]=[L :$L_2$], d'où $L_1$=$L_2$.

Surjectivité. Soit H un sous-groupe de G. En prenant L'=$L^H$, on a le sous-corps voulu d'après le lemme d'Artin.

Application réciproque. Soit L'/$\mathbb{K}$ une sous-extension de L/$\mathbb{K}$. On lui associe Gal(L/L'). D'après un lemme précédent, $L^{Gal(L/L')}$=L' car L/L' est galoisienne. □

**4.5 Corollaire.** — *La correspondance de Galois intervertit l'ordre des inclusions entre les sous-extensions de L/$\mathbb{K}$ et les sous-groupes de Gal(L/$\mathbb{K}$) et vérifie :*

1. *$\mathbb{K} \subseteq L_1 \subseteq L_2 \subseteq$L $\Longleftrightarrow$ Gal(L/$L_1$)$\supseteq$Gal(L/$L_2$) ;*
2. *Gal(L/$L_1L_2$) = Gal(L/$L_1$)$\cap$Gal(L/$L_2$) ;*
3. *Gal(L/$L_1 \cap L_2$) = <Gal(L/$L_1$),Gal(L/$L_2$)>.*

**4.6 Théorème.** — *Soient $L_1/\mathbb{K}$ et $L_2/\mathbb{K}$ des extensions finies galoisiennes. Alors $L_1 \cap L_2/\mathbb{K}$ est finie galoisienne, et Gal($L_1 \cap L_2/\mathbb{K}$)≃Gal($L_1L_2/\mathbb{K}$)/Gal($L_1L_2/L_1 \cap L_2$).*

**4.7 Théorème.** — *Soit L/$\mathbb{K}$ une extension finie galoisienne. Soit L'/$\mathbb{K}$ une sous-extension, et soit H :=Gal(L/L'). Soit G :=Gal(L/$\mathbb{K}$). L'/$\mathbb{K}$ est alors galoisienne si et seulement si H est distingué dans G. Lorsque cela est vrai, Gal(L'/$\mathbb{K}$)≃G/H, l'isomorphisme résultant de la factorisation du morphisme de restriction $\sigma \in G \mapsto \sigma_{L'} \in$ Gal(L'/$\mathbb{K}$) de noyau H.*

**4.8 Lemme.** *Soit $\sigma \in G$ et soit $H_\sigma := \sigma H \sigma^{-1}$. Alors $H_\sigma$=Gal(L/$\sigma$(L')).*

*Démonstration.* On a $\sigma$(L')$\subseteq$ $\sigma$(L)=L et $\sigma(L')/\mathbb{K}$ est une sous-extension de L/$\mathbb{K}$ avec [L :$\sigma$(L')]=[L :$\sigma$(L')] car L'≃ $\sigma$(L'). Soit $\sigma\tau\sigma^{-1} \in H_\sigma$, $\tau \in H$, et soit x ∈ L'. On a $\sigma\tau\sigma^{-1}(\sigma(x))=\sigma\tau(x) = \sigma(x)$ car $\tau \in H$. D'où $H_\sigma \subseteq$Gal(L/$\sigma$(L')), et l'égalité des degrés donne l'égalité. □

*Démonstration.* Démonstration du théorème Si L'/$\mathbb{K}$ est galoisienne, $\forall\sigma \in G$, $\sigma(L') = L'$, d'où $\sigma H\sigma^{-1}$=Gal(L/L')=H.

Réciproquement, si H est distingué dans G, $\sigma H\sigma^{-1}$=H $\forall\sigma \in G$. Ainsi, Gal(L/$\sigma(L')$) = Gal(L/L'), d'où $\sigma$(L')=L' $\forall\sigma \in G$ par injection de la correspondance de Galois. Soit $\tau$ un $\mathbb{K}$-isomorphisme de L' dans une clôture algébrique de L. On le prolonge en un $\mathbb{K}$-isomorphisme $\sigma$ de L, donc en un élément de Gal(L/$\mathbb{K}$), et on a $\tau(L') = \sigma$(L')=L', donc L"/$\mathbb{K}$ est normale. Elle est séparable et donc galoisienne car L/$\mathbb{K}$ est galoisienne.

Et la restriction $\sigma \in$ G $\mapsto \sigma_{L'} \in$ Gal(L'/$\mathbb{K}$) a pour noyau les isomorphismes qui laissent fixe L', donc qui appartiennent à Gal(L/L')=H. □

**4.9 Remarque.** — *Le treillis des sous-extensions d'une extension galoisienne peut se déterminer entièrement à partir du treillis des sous-groupes de son groupe de Galois, ce qui se ramène à de la théorie des groupes.*

*De plus, le groupe de Galois est en bijection avec un sous-groupe d'un $S_n$ car il permute les racines de polynômes irréductibles pour lesquels l'extension est le corps de décomposition.*

*Le groupe de Galois sur $\mathbb{K}$ d'un polynôme P∈ \$KK[X] irréductible sur $\mathbb{K}$ est transitif : pour $\alpha$ et $\beta$ racines de P, il existe $\sigma$ dans le groupe de Galois de P sur $\mathbb{K}$ tel que $\sigma(\alpha) = \beta$. Il y a en effet autant d'isomorphismes de $\mathbb{K}(\alpha)$ dans $\bar{\mathbb{K}}$ que de racines distinctes de P sur $\mathbb{K}$, et ceux-ci sont déterminés par l'image de $\alpha$ dans $\bar{\mathbb{K}}$.*

**4.10 Exemple.** *Ici, $\mathbb{K}=\mathbb{Q}$, P(X)=$X^4 - 2$, et L est le corps de décomposition de P sur $\mathbb{Q}$. L/$\mathbb{Q}$ est ainsi galoisienne finie.*

*On pose $\zeta := 2^{1/4}$. Les racines de P sont $\zeta$, -$\zeta$, i$\zeta$, -i$\zeta$. Ainsi, L contient i et $\zeta$, donc $\mathbb{Q}$(i,$\zeta$), et $\mathbb{Q}$(i,$\zeta$) contient les racines de P, donc L=$\mathbb{Q}$(i,$\zeta$).*

*Or, [$\mathbb{Q}$($\zeta$) :$\mathbb{Q}$]=4 comme corps de rupture, et [$\mathbb{Q}$(i,$\zeta$) :$\mathbb{Q}$($\zeta$)]=2 car i$\notin \mathbb{Q}(\zeta) \subset \mathbb{R}$. D'où [L :$\mathbb{Q}$]=8. Gal(L$\mathbb{Q}$) a ainsi 8 éléments, et est un sous-groupe de $S_4$.*

*Comme L=$\mathbb{Q}$(i,$\zeta$), ces éléments sont fixés par les images de i et $\zeta$, qui sont : i$\mapsto \pm i$ et $\zeta \mapsto \pm\zeta$ ou $\pm i\zeta$, qui sont les autres racines des polynômes minimaux de i et $\zeta$ sur $\mathbb{Q}$. Il y a 8 combinaisons d'images pour 8 éléments, ce qui fait que chaque combinaison d'images est réalisée par un élément de Gal(L/$\mathbb{Q}$). Il reste à déterminer la structure de groupe de Gal(L/$\mathbb{Q}$).*

*Posons s : i$\mapsto$-i et $\zeta \mapsto \zeta$ et r : i$\mapsto$i et $\zeta \mapsto i\zeta$. Gal(L/$\mathbb{Q}$) est engendré par r et s, avec pour relations $r^4$=id, $s^2$=id, srs=$r^{-1} = r^3$. Donc Gal(L/$\mathbb{Q}$)= <r,s tq $r^4 = s^2$=id, sr=$r^3$s> = $D_8$, le groupe des isométries du carré.*

*Liste des sous-groupes : Ordre 8 : Gal(L/$\mathbb{Q}$)≃ $D_8$*

*Ordre 4 : S :=$\{id, r, r^2, r^3\} \simeq \mathbb{Z}/4\mathbb{Z}$ ; T :=$\{id, r^2, s, r^2s\} \simeq \mathbb{Z}_2x\mathbb{Z}_2$ ; U :=$\{id, rs, r^2, r^3s\} \simeq \mathbb{Z}_2x\mathbb{Z}_2$.*

*Ordre 2 : B :=$\{id, s\} \simeq \mathbb{Z}_2$ ; A :=$\{id, r^2\} \simeq \mathbb{Z}_2$ ; C :=$\{id, rs\} \simeq \mathbb{Z}_2$ ; D :=$\{id, r^2s\} \simeq \mathbb{Z}_2$ ; E :=$\{id, r^3s\} \simeq \mathbb{Z}_2$.*

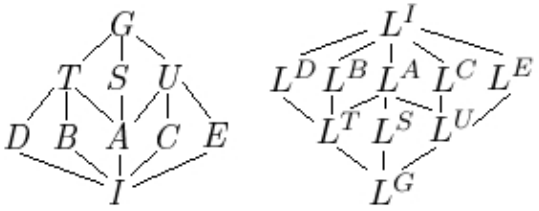


FIGURE 1 – Treillis des sous-groupes et des sous-extensions de $X^4 - 2$ sur $\mathbb{Q}$.

*Ordre 1 : I :=*$\{id\}$.

*Cela donne le treillis de groupe et le treillis de sous-extensions suivant :*

*Le calcul des sous-corps stables donne :* $L^I$*=L,* $L^D = \mathbb{Q}(i\zeta)$*,* $L^B = \mathbb{Q}(\zeta)$*,* $L^C = \mathbb{Q}(\zeta(1+i))$*,* $L^A = \mathbb{Q}(i, 2^{1/2})$*,* $L^E = \mathbb{Q}(\zeta(1-i))$*,* $L^S = \mathbb{Q}(i)$*,* $L^T = \mathbb{Q}(2^{1/2})$*,* $L^U = \mathbb{Q}(i2^{1/2})$*,* $L^G = \mathbb{Q}$*. Les sous-groupes distingués de G sont A,S,T,U, et leurs sous-corps associés sont bien normaux sur* $\mathbb{Q}$*.*

**4.11 Exemple.** *Soit p premier, n* $\geq$ *1, q=*$p^n$*. L'extension* $\mathbb{F}_q/\mathbb{F}_p$ *est galoisienne finie en tant que corps de décomposition de* $X^{p^n} - X$ *sur* $\mathbb{F}_p$*, et Gal(*$\mathbb{F}_q/\mathbb{F}_p$*) est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius sur* $\mathbb{F}_q$*.*

*Ainsi, Gal(*$\mathbb{F}_q/\mathbb{F}_p$*)*$\simeq \mathbb{Z}/n\mathbb{Z}$*, ses sous-groupes sont isomorphes aux* $\mathbb{Z}/d\mathbb{Z}$*, d|n, et la correspondance de Galois les envoie sur les* $\mathbb{F}_{p^{n/d}}$

# 5 Résolubilité et simplicité

**5.1 Définition.** — Un groupe G est **résoluble** si et seulement s'il existe une chaîne de sous-groupes $\{1\} = G_0 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n = G$ telle que $G_{i+1}/G_i$ est abélien et non trivial $\forall 0 \leq i \leq n-1$.

**5.2 Définition.** — Un groupe G est **simple** si et seulement si ses seuls sous-groupes distingués sont $\{e\}$ et G.

**5.3 Remarque.**

*Si G est abélien, alors G est résoluble.*

*Un groupe résoluble est simple si et seulement s'il est cyclique d'ordre premier.*

*Les groupes symétriques* $S_n$ *ne sont pas résolubles pour n*$\geq$*5 car* $A_n$ *est alors simple et non abélien.*

**5.4 Théorème.** — *Soit G un groupe, soient N et H des sous-groupes de G tels que* $N \triangleleft G$*.*

1. *Si G est résoluble, alors H et N sont résolubles.*
2. *Si G est résoluble, alors G/N est résoluble.*
3. *Si N et G/N sont résolubles, alors G est résoluble.*

**5.5 Définition.** — Soit L/$\mathbb{K}$ une extension de corps. Elle est **radicale** si et seulement s'il existe $\alpha_1, .., \alpha_n \in \bar{\mathbb{K}}$ et $p_1, .., p_n \in \mathbb{N}$ tels que L=$\mathbb{K}(\alpha_1, .., \alpha_n)$ avec $\alpha_1^{p_1} \in \mathbb{K}$ et $\alpha_i^{p_i} \in \mathbb{K}(\alpha_1, .., \alpha_{i-1})$ $\forall i \in \{2, ..n\}$.

**5.6 Définition.** — Un polynôme P$\in \mathbb{K}$[X] est **résoluble par radicaux** si et seulement si un corps de décomposition M de P sur $\mathbb{K}$ est contenu dans une extension radicale L/$\mathbb{K}$ : $\mathbb{K} \subseteq M \subseteq L$.

**5.7 Lemme.** — *Si L/*$\mathbb{K}$ *est radicale est séparable, alors pour toute clôture normale M de L sur* $\mathbb{K}$*, l'extension M/*$\mathbb{K}$ *est radicale et normale.*

*Démonstration.* L=$\mathbb{K}(\alpha_1, .., \alpha_n)$, et M est engendré par $\mathbb{K}$ et par les $\sigma(\alpha_i)$, $\forall i \in \{1, ..n\}$,$\forall \sigma \in$ Gal(M/$\mathbb{K}$) qui forment une tour d'extensions radicales, qui est une extension radicale, car les $\sigma$ sont des $\mathbb{K}$-automorphismes de M. □

**5.8 Lemme.** — *Soit L le corps de décomposition de $X^p - 1$ sur $\mathbb{K}$, p premier. Si L/$\mathbb{K}$ est séparable, alors Gal(L/$\mathbb{K}$) est cyclique d'ordre p-1.*

*Démonstration.* L'ensemble des racines de $X^p - 1$ forme un groupe d'ordre p cyclique, et pour une racine $\zeta$ fixée, chaque élément de Gal(L/$\mathbb{K}$) l'envoie $\zeta$ sur $\zeta^j$, $j \in \{0, .., p-1\}$, et la valeur de j détermine l'image de toutes les autres racines par cet automorphisme. □

**5.9 Lemme.** — *Soit n≥1 et soit $\mathbb{K}$ un corps sur lequel $X^n-1$ est scindé. Soit a∈ $\mathbb{K}$ et soit L un corps de décomposition de $X^n-a$ sur $\mathbb{K}$. Alors Gal(L/$\mathbb{K}$) est abélien.*

*Démonstration.* Les racines de $X^n-a$ sont les $\alpha\zeta^j$, $\alpha,\zeta\in\bar{\mathbb{K}}$ tel que $\alpha^n=a$, et $\zeta^n=1$. Les éléments de Gal(L/$\mathbb{K}$) sont alors fixés par l'image de $\alpha$, c'est-à-dire par le choix de j $\in\{0,..,n-1\}$ tel que $\alpha\mapsto\alpha\zeta^j$. Ainsi, Gal(L/$\mathbb{K}$) est abélien. □

**5.10 Lemme.** — *Si L/$\mathbb{K}$ est galoisienne et radicale, alors Gal(L/$\mathbb{K}$) est résoluble.*

*Démonstration.* Ici, L=$\mathbb{K}(\alpha_1,..,\alpha_n)$ avec $\alpha_1^{p_1}\in\mathbb{K}$ et $\alpha_i^{p_i}\in\mathbb{K}(\alpha_1,..,\alpha_{i-1})\ \forall i\in\{2,..n\}$. On démontre le lemme par récurrence sur n.

Si $\alpha_1\in\mathbb{K}$, L=$\mathbb{K}(\alpha_2,..,\alpha_n)$ et $HR_{n-1}$ s'applique. Si $\alpha_1\notin\mathbb{K}$, son polynôme minimal sur $\mathbb{K}$ est scindé sur L et admet une autre racine, $\beta_1$. Soit $\zeta=\alpha_1/\beta_1$. On a $\zeta^{p_1}$=1 Donc $X^{p_1}-1$ est scindé sur L car L/$\mathbb{K}$ galoisienne.

Soit M le corps de décomposition de $X^{p_1}-1$ sur $\mathbb{K}$. On a $\mathbb{K}\subseteq M\subseteq M(\alpha_1)\subseteq L$ avec Gal(M/$\mathbb{K}$) abélien, Gal(M($\alpha_1$)/M) abélien, et Gal(L/M($\alpha_1$)) résoluble par $HR_{n-1}$. De plus, L/M($\alpha_1$) est galoisienne et M($\alpha_1$)/M aussi comme corps de décomposition de $X^{p_1}-\alpha_1^{p_1}$ sur M. Ainsi, Gal(M($\alpha_1$)/M)≃ Gal(L/M)/Gal(L/M($\alpha_1$)), donc Gal(L/M) est résoluble, et comme M/$\mathbb{K}$ est galoisienne,

Gal(M/$\mathbb{K}$)≃Gal(L/$\mathbb{K}$)/Gal(L/M), donc Gal(L/$\mathbb{K}$) est résoluble. □

**5.11 Théorème.** — *Soit $\mathbb{K}\subseteq L\subseteq M$ telle que M/$\mathbb{K}$ est finie, radicale et séparable. Soit $\mathbb{K}_0$=$L^{Gal(L/\mathbb{K})}$ Alors Gal(L :$\mathbb{K}_0$) est résoluble.*

*Démonstration.* Soit N la clôture normale de M/$\mathbb{K}_0$. On a $\mathbb{K}\subseteq\mathbb{K}_0\subseteq L\subseteq M\subseteq N$.

Comme M/$\mathbb{K}$ est radicale, M/$\mathbb{K}_0$ est radicale, donc N/$\mathbb{K}_0$ est normale, séparable, et radicale, donc Gal(N/$\mathbb{K}_0$) est résoluble. De plus, Gal(L/$\mathbb{K}$)=Gal(L/$\mathbb{K}_0$), donc L/$\mathbb{K}_0$ est normale car $L^{Gal(L/\mathbb{K}_0)}$=$\mathbb{K}_0$. Donc Gal(L/$\mathbb{K}_0$)≃Gal(N/$\mathbb{K}_0$)/Gal(N/L). Ainsi, Gal(L/$\mathbb{K}_0$) est résoluble. □

**5.12 Théorème.** — *Soit P∈ $\mathbb{K}$[X]. Si P est séparable et résoluble par radicaux, alors le groupe de Galois de P sur $\mathbb{K}$ est résoluble.*

## 5.1 Expression des racines d'un polynôme par radicaux

**5.13 Proposition.** — *Soit $\mathbb{K}$ un corps et n≥1.*

*Pour n≥5, il n'existe aucune formule générale à base d'addition, de multiplication, et d'extraction de racines q-ièmes, $q\in\mathbb{N}$.permettant d'exprimer les racines de tout polynôme de degré n en fonction de ses coefficients*

*Démonstration.* L'existence d'une telle formule est équivalente au fait que l'extension

$\mathbb{K}(X_1,..,X_n)/\mathbb{K}(X_1,..,X_n)^{S_n}$ soit radicale, car pour P(X)= $a_nX^n+...+a_0=a_n\prod_{k=1}^n(X-\alpha_k)$, ses coefficients vérifient $a_i=(-1)^{n-i}a_n\sum_{(n-i),n}(\alpha_1,..,\alpha_n)$, où $\sum_{(n-i),n}$ est le (n-i)-ième polynôme symétrique élémentaire d'ordre n en les racines de P.

L'extension $\mathbb{K}(X_1,..,X_n)/\mathbb{K}(X_1,..,X_n)^{S_n}$ est le corps de décomposition de Q(T)=$\prod_{k=1}^n(T-X_k)$ sur $\mathbb{K}(X_1,..,X_n)^{S_n}$, et est ainsi galoisienne et finie. De plus, $S_n$ agit sur $\mathbb{K}(X_1,..,X_n)$ par isomorphismes permutant les indices des indéterminées, et ces isomorphismes laissent $\mathbb{K}(X_1,..,X_n)^{S_n}$ stable. Réciproquement, tout élément du groupe de Galois de l'extension préserve Q(T), et permute ainsi les indices des indéterminées.

Le groupe de Galois de l'extension est ainsi $S_n$. Comme $S_n$ n'est pas résoluble pour n≥5, l'extension n'est alors pas radicale. Pour n=2,3,4, la résolubilité de $S_n$ permet de trouver une tour d'extension radicale pour $\mathbb{K}(X_1,..,X_n)/\mathbb{K}(X_1,..,X_n)^{S_n}$ et ainsi d'obtenir des formules générales d'expression des racines d'un polynôme de degré n en fonction de ses coefficients. □

**5.14 Remarque.** — *Cela n'implique toutefois pas qu'il n'existe pas pour un polynôme de degré n donné une formule permettant de déterminer ses racines via ses coefficients par radicaux. Seule la non-existence d'une formule générale a été démontrée.*

**5.15 Lemme.** — *Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$, p premier et P $\in \mathbb{K}$[X] irréductible sur $\mathbb{K}$ et de degré p. Si P a exactement deux racines complexes, alors le groupe de Galois de P sur $\mathbb{K}$ est isomorphe à $S_p$.*

*Si p≥5, un tel polynôme P n'est alors pas résoluble par radicaux, ce qui donne l'existence de polynômes dont les racines ne sont pas exprimables par radicaux en fonction de leurs coefficients.*

*Démonstration.* Soit M un corps de décomposition de P sur $\mathbb{K}$. Comme M contient au moins un corps de rupture de P sur $\mathbb{K}$, p|[M :$\mathbb{K}$] = |Gal(M/$\mathbb{K}$)|. Donc il existe un élément $\tau$ de Gal(M/$\mathbb{K}$) d'ordre p.

Gal(M/$\mathbb{K}$) étant isomorphe à un sous-groupe de $S_p$, $\tau$ est alors isomorphe à un p-cycle. De plus, la conjugaison complexe $\sigma$ est dans Gal(M/$\mathbb{K}$) et intervertit deux racines, elle est alors isomorphe à une transposition dans $S_p$.

On associe alors $\sigma$ à (12). L'une des puissances de $\tau$ envoie alors 1 sur 2, et on associe cet isomorphisme à (123...p). On forme alors aisément (23),(34),..(p-1 p) par conjugaison, ce qui permet d'engendrer $S_p$ tout entier. Ainsi, Gal(M/$\mathbb{K}$)$\simeq S_p$. □

**5.16 Exemple.** $\mathbb{K} = \mathbb{Q}$, *P(X)=*$X^5 - 6X + 3$. *P est irréductible sur $\mathbb{Q}$, et possède 3 racines réelles. $S_5$ n'étant pas résoluble, P n'est pas résoluble par radicaux sur $\mathbb{Q}$.*

*Il existe ainsi des éléments algébriques sur $\mathbb{Q}$ qui ne s'écrivent pas qu'à partir de l'addition, la multiplication, et l'extraction de racines q-ièmes de nombres rationnels.*

*Il y en a de plus une infinité : Pour n≥2 et p premier, p≥5, Q(X)=*$X^5 - npX + p$ *est irréductible, possède deux racines complexes, et n'est ainsi pas résoluble par radicaux sur $\mathbb{Q}$.*

**5.17 Remarque.** — *Si P$\in \mathbb{K}$[X] irréductible a au moins une racine exprimable par radicaux sur $\mathbb{K}$, alors toutes ses racines le sont, car pour $\alpha$ et $\beta$ racines de P, $\mathbb{K}(\alpha/)\mathbb{K}$ et $\mathbb{K}(\beta)\mathbb{K}$ sont isomorphes.*

# 6 Constructions à la règle et au compas

**6.1 Théorème.** — *Soit $\mathbb{K}$ un corps de caractéristique nulle, et $\alpha \in \bar{\mathbb{K}}$, $\bar{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$. On a l'équivalence :*

1. *$\alpha$ est constructible à la règle et au compas à partir de $\mathbb{K}$.*
2. *Il existe une tour d'extensions $\mathbb{K} = C_0 \subseteq C_2 \subseteq \cdots \subseteq C_m$ telle que $[C_i : C_{i-1}] = 2$ $\forall 1 \leq i \leq m$ et $\alpha \in C_m$.*
3. *Il existe une extension $L : \mathbb{K}$ galoisienne telle que $[L : \mathbb{K}] = 2^n$ , $n \in \mathbb{N}$ et $\alpha \in L$.*

*Démonstration.*

$1) \Leftrightarrow 2)$ a été démontré en cours.

$3) \Rightarrow 2)$

$L : \mathbb{K}$ étant galoisienne, son groupe de Galois G vérifie $|G| = [L : \mathbb{K}] = 2^n$. G est donc un 2-groupe. Ainsi, il existe ainsi une chaîne $\{1\} = G_0 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n = G$ telle que $G_{i+1}/G_i$ est d'ordre 2 $\forall 0 \leq i \leq n-1$.

$L : \mathbb{Q}$ étant galoisienne, la correspondance de Galois entre les sous-extensions de $L : \mathbb{Q}$ et les sous-groupes de G nous donne alors la tour d'extensions recherchée. $2) \Rightarrow 3)$

Démonstration par récurrence sur $m \in \mathbb{N}^*$ que toute clôture normale de $C_m : K$ est une extension sur K ayant pour degré une puissance de 2.

Pour m=1, $C_1 : \mathbb{K}$ est normale car de degré 2, et tout est séparable car $car(\mathbb{K}) = 0$. Un lemme est ensuite nécessaire :

**6.2 Lemme.**

*Soit $L_1 \subseteq L \subseteq K$ une extension de corps avec $car(K) = 0$, L/K galoisienne de degré $2^l$, $l \in \mathbb{N}$, et $[L_1 : L]$ =1 ou 2.*

*Alors, pour M une clôture normale de $L_1 : K$, on a $[M : K] = 2^r,\ r \in \mathbb{N}$.*

*Démonstration.*

Si $[L_1 : L] = 1,\ L_1 = L$. Sinon, $[L_1 : L] = 2$, et il existe ainsi $\beta_1 \in \mathbf{K}$ tel que $L_1 = L(\beta_1)$. Soient $\alpha_1 \dots \alpha_m \in \mathbf{K}$ tels que $L = K(\alpha_1, \dots, \alpha_m)$.

On a alors deux extensions $K(\alpha_1, \dots, \alpha_m, \beta_1) = L_1 \subseteq K(\beta_1) \subseteq K$ et $L_1 \subseteq L \subseteq K$. Ainsi, $[K(\beta_1) : K] \mid 2^{l+1}$, donc $[K(\beta_1) : K] = 2^s$, $1 \leq s \leq l+1$, et $2^s = deg(Irr(\beta_1, K))$. De plus, $deg(Irr(\beta_1, L)) = 2$.

Notons G le groupe de Galois de L :K. Ainsi, $P(X) = \prod_{\varphi \in G} \varphi(Irr(\beta_1, L)) \in K[X]$ car L :K est galoisienne, $deg(P) = 2^{l+1}$, et $P(\beta_1) = 0$. Donc $Irr(\beta_1, K) \mid P(X)$. Ainsi, il existe $H \subseteq G$ tel que $Irr(\beta_1, K) = \prod_{\varphi \in H} \varphi(Irr(\beta_1, L))$ dans L[X].

Soient $\beta_1 \dots \beta_p$ les racines de $Irr(\beta_1, K)$. Elles ont ainsi toutes un polynôme minimal de degré 2 sur L. Donc $[L(\beta_1, \dots, \beta_p) : L] = 2^{l_2}$, donc $[L(\beta_1, \dots, \beta_p) : K] = 2^{l_3}$, $l_2, l_3 \in \mathbb{N}$. Soit N la clôture normale de $L_1$ sur K. On a $K \subseteq N \subseteq L(\beta_1, \dots, \beta_p)$, donc $[N : K] \mid 2^{l_3}$, donc $[N : K] = 2^{l_4}$, $l_4 \in \mathbb{N}$. □

Soit $\mathbb{K} = C_0 \subseteq C_2 \subseteq \dots \subseteq C_m$ tour d'extensions telle que $[C_i : C_{i-1}] = 2\ \forall 1 \leq i \leq m$ et $\alpha \in C_m$. Par $HR_{m-1}$, pour L clôture normale de $C_{m-1} : K$, on a $[L : K] = 2^l,\ l \in \mathbb{N}$. Comme $C_{m-1} \subseteq L$, soit $C_m \subseteq L$, soit $[C_m : L] = 2$.

Si $C_m \subseteq L$, c'est bon. Sinon, le lemme précédent appliqué à $C_m : L : K$ donne pour M clôture normale de $C_m : K$ : $[M : K] = 2^{l_2},\ l_2 \in \mathbb{N}$. □

## 6.1 Polygones réguliers

**6.3 Définition.** — Soit n$\in \mathbb{N}$.

n est **constructible à la règle et au compas** (constructible) si et seulement si le n-gone régulier est CRC à partir de $\mathbb{Q}$.

**6.4 Lemme.** — *Soient m,n* $\in \mathbb{N}$

1. *n est constructible si et seulement si $\zeta = e^{2i\pi/p^n}$ est CRC à partir de $\mathbb{Q}$.*
2. *Si m|n et n est constructible, alors m est constructible.*
3. *Si m et n sont constructibles, et si m∧n=1, alors mn est constructible.*

On s'intéresse ainsi à la constructibilité des nombres premiers et de leurs puissances.

**6.5 Corollaire.**

1. *n=$p_1^{a_1}..p_r^{a_r}$ est constructible $\leftrightarrow$ $p_1^{a_1}, \dots, p_r^{a_r}$ sont constructibles.*
2. *$2^n$ est constructible.*

**6.6 Lemme.** — *Soit p premier.*

1. *S'il existe n$\in \mathbb{N}$ tel que $p^n$ est constructible, alors pour $\zeta = e^{2i\pi/p^n}$, Irr($\zeta, \mathbb{Q}$) a pour degré une puissance de 2.*
2. *Irr($e^{2i\pi/p}, \mathbb{Q}$)=$1 + X + .. + X^{p-1}$.*
3. *Irr($e^{2i\pi/p^2}, \mathbb{Q}$)=$1 + X + .. + X^{p(p-1)}$.*

*Démonstration.*

1. Si $\zeta$ est CRC à partir de $\mathbb{Q}$, alors il est dans une tour d'extensions de degré une puissance de 2.
2. $P_1(X) = 1 + X + .. + X^{p-1} = (X^p - 1)/(X - 1)$ est annulé par $e^{2i\pi/p}$ est est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein car $P_1(X + 1) = X^{p-1} + \sum_{k=1}^{p-1} \binom{n}{k} X^{k-1}$.
3. $P_2(X) = 1 + X + .. + X^{p(p-1)} = (X^{p^2} - 1)/(X - 1)$ est annulé par $e^{2i\pi/p^2}$ est est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein car $P_2(X + 1) \equiv X^{p(p-1)}$(mod p) et car le terme devant 1 de $P_2(X + 1)$ est p(p-1).

□

**6.7 Théorème.** *Théorème (Gauss) — Le n-gone régulier est CRC à partir de $\mathbb{Q}$ si et seulement si n=$2^r p_1..p_s$, r,s$\in \mathbb{N}$ avec les $p_i$ des nombres premiers de la forme $2^{2^{r_i}} + 1$, $r_i \in \mathbb{N}$.*

*Démonstration.*

$\Rightarrow$ Soit n=$2^r p_1^{a_1}..p_s^{a_s}$ constructible. Tous les $p_i^{a_i}$ sont alors constructibles. Si $a_i \geq$2, alors $p_i^2$ est constructible. Or, deg(Irr($e^{2i\pi/p_i^2}, \mathbb{Q}$))=$p_i(p_i - 1)$, qui n'est pas une puissance de 2. Donc $a_i$=1 $\forall i \in \{1, .., s\}$.

De plus, deg(Irr($e^{2i\pi/p_i}, \mathbb{Q}$))=$p_i - 1 = 2^{\lambda_i}$, $\lambda_i \in \mathbb{N}$ $\forall i \in \{1, .., s\}$. Si $\lambda_i$=ab, a,b $\in \mathbb{N}$ avec a impair, alors $p_i$=$(2^b)^a - (-1)^a$, et est divisible par $2^b + 1$, contradiction. Donc $\lambda_i$=$2^{r_i}$, $r_i \in \mathbb{N}$.

$\Leftarrow$ Pour $p_i$=$2^{2^{r_i}} + 1$, deg(Irr($e^{2i\pi/p_i}, \mathbb{Q}$))=$p_i - 1 = 2^{2^{r_i}}$, et $\mathbb{Q}(e^{2i\pi/p_i})/\mathbb{Q}$ est galoisienne, donc $e^{2i\pi/p_i}$ est CRC à partir de $\mathbb{Q}$. □

**6.8 Remarque.** — *Les nombres premiers de la forme $2^{2^n} + 1$ connus sont 2,3,5,17,257,65537.*

*La détermination de sous-extensions de $\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}$ permet d'avoir une tour d'extensions quadratiques qui donne une expression sous forme de radicaux quadratiques de $\cos(2\pi/n)$ et $\sin(2\pi/n)$ qui pourra être construite à la règle et au compas.*

# 7 Corps cyclotomiques

**7.1 Proposition.** — *Soit $\mathbb{K}$ un corps. Soit $\mu_n$ l'ensemble des racines de $X^n - 1$ dans $\bar{\mathbb{K}}$.*

*Si car($\mathbb{K}$)=0, $|\mu_n|$=n, car $X^n - 1$ est séparable.*

*Si car($\mathbb{K}$)=p, p premier, et n=$p^\lambda$d, p$\wedge$d=1, $|\mu_n|$=d, car $X^n - 1$=$(X^d - 1)^{p^\lambda}$ et car $X^d - 1$ est séparable.*

**7.2 Théorème.** — *Si car($\mathbb{K}$)$\wedge$n=1, $\mathbb{K}(\mu_n)/\mathbb{K}$ est galoisienne, de groupe de Galois isomorphe à un sous-groupe de $\mathbb{Z}/n\mathbb{Z}^*$.*

*Démonstration.* Soit $\zeta$ une racine primitive n-ième de l'unité dans $\mu_n$. On a $\mathbb{K}(\mu_n) = \mathbb{K}(\zeta)$, et $\forall \sigma \in$ Gal($\mathbb{K}(\mu_n)/\mathbb{K}$), $\sigma(\zeta)$ est encore une racine primitive n-ième de l'unité, ce qui revient à dire que $\sigma$ préserve l'ordre de $\zeta$ dans $\mu_n$=<$\zeta$>$\simeq \mathbb{Z}/n\mathbb{Z}$, d'où $\sigma(\zeta)$=$\zeta^{\bar{a}}$, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}^*$. Cela donne une application de Gal($\mathbb{K}(\mu_n)/\mathbb{K}$) dans $\mathbb{Z}/n\mathbb{Z}^*$ qui est injective et est un morphisme de groupes. □

**7.3 Corollaire.** — *[$\mathbb{K}(\mu_n)/\mathbb{K}$]|$\varphi$(n).*

**7.4 Théorème.** — *Soit p premier, q=$p^d$, et n tel que p$\wedge$n=1.*

*L'image de Gal($\mathbb{F}_q(\mu_n)/\mathbb{F}_q$) dans $\mathbb{Z}/n\mathbb{Z}^*$ est le sous-groupe <$\bar{q}$> engendré par la classe de q modulo n.*

*Démonstration.* $\mathbb{F}_q(\mu_n) \simeq \mathbb{F}_{q^t}$ pour un certain t, et Gal($\mathbb{F}_{q^t}/\mathbb{F}_q$) est engendré par $Frob_q$ : x$\mapsto x^q$. De plus, $Frob_q(\zeta) = \zeta^q$ d'où le résultat. □

**7.5 Corollaire.** — *Le degré de l'extension est égal à l'ordre de $\bar{q}$ dans $\mathbb{Z}/n\mathbb{Z}^*$.*

**7.6 Théorème.** — *[$\mathbb{Q}(\mu_n) : \mathbb{Q}$]=$\varphi(n)$, $\forall n \geq$1.*

*Ainsi, Gal($\mathbb{Q}(\mu_n)/\mathbb{Q}$)$\simeq \mathbb{Z}/n\mathbb{Z}^*$.*

*Démonstration.* Prendre $\zeta$ racine primitive de $\mu_n$, et montrer que $\forall m$ tels que m$\wedge$n=1, $\zeta^m$ est une racine de Irr($\zeta, \mathbb{Q}$). □

**7.7 Proposition.** — *Toute extension quadratique de $\mathbb{Q}$ est dans un $\mathbb{Q}(\mu_n)$.*

*Soit m$\in \mathbb{Z}^\times$ sans facteurs carrés. Si m est impair, $m^{1/2} \in \mathbb{Q}(\mu_{|m|})$. Si m est pair, $m^{1/2} \in \mathbb{Q}(\mu_{|4m|})$.*

*Démonstration.* i $\in \mathbb{Q}(\mu_4)$, et pour p premier, et $\zeta$ racine primitive p-ième de l'unité,

$(-1)^{(p-1)/2}p=\prod_{k=1}^{(p-1)/2}(\zeta^k - \zeta^{-k})^2$ et est ainsi un carré dans $\mathbb{Q}(\mu_p)$. □

**7.8 Remarque.** — *Cependant, $\mathbb{Q}(\mu_n)$ a un treillis qui se complique rapidement car pour tout p premier divisant n, $\varphi(p)$ est divisible par une puissance de 2 non nulle, ce qui implique un important 2-Sylow.*

## 7.1 Théorie de Kummer

**7.9 Définition.** — Soit L/$\mathbb{K}$ une extension finie galoisienne. Soit x$\in$L.

On définit la **norme** de x : $N_{L/\mathbb{K}}(x)=\prod_{\sigma\in Gal(L/\mathbb{K})}\sigma(x)$, et la **trace** de x : $Tr_{L/\mathbb{K}}(x)=\sum_{\sigma\in Gal(L/\mathbb{K})}\sigma(x)$.

$\forall x \in L$, $N_{L/\mathbb{K}}(x)$ et $Tr_{L/\mathbb{K}}(x) \in \mathbb{K}$.

**7.10 Théorème.** *Théorème (Hilbert 90) — Soit L/$\mathbb{K}$ une extension galoisienne cyclique de degré n, et soir $\sigma$ un générateur de Gal(L/$\mathbb{K}$).*

*$\forall x \in L$, $N_{L/\mathbb{K}}(x)$=1 si et seulement si $\exists y \in L$ tel que x=$y/\sigma(y)$.*

*$\forall x \in L$, $Tr_{L/\mathbb{K}}(x)$=0 si et seulement si $\exists y \in L$ tel que x=$y - \sigma(y)$.*

**7.11 Théorème.** *Théorème de Kummer — Soit $\mathbb{K}$ un corps, et soit n tel que k$\wedge$n=1. On suppose que $\mu_n \in \mathbb{K}$. ($|\mu_n| = n$). Alors on a :*

1. *L/$\mathbb{K}$ est une extension galoisienne cyclique de degré divisant n $\Leftrightarrow \exists a \in \mathbb{K}$ tel que L=$\mathbb{K}(a^{1/n})$.*
2. *$\mathbb{K}(a^{1/n}) = \mathbb{K}(b^{1/n}) \Leftrightarrow$ b=$a^\lambda u$, $\lambda\wedge$n=1 et u$\in \mathbb{K}$.*

*Démonstration.* Soit L/$\mathbb{K}$ une extension galoisienne cyclique de degré d, $d|n$. Soit $\sigma$ un générateur de Gal(L/$\mathbb{K}$). Soit $\zeta$ une racine primitive d-ième de l'unité dans $\mathbb{K}$. On a $N_{L/\mathbb{K}}(\zeta^{-1})=\zeta^{-d}$=1, donc d'après Hilbert 90, $\exists y \in L$ tel que $\zeta^{-1}=y/\sigma(y) \Rightarrow \zeta=\sigma(y)/y$.

Ainsi, $\sigma(y)=\zeta y \Rightarrow \sigma^i=\zeta^i y$ $\forall$i, donc [$\mathbb{K}(y) : \mathbb{K}$]$\geq$d, mais $\mathbb{K}(y) \subseteq$L, donc $\mathbb{K}(y) = L$. On pose a=$y^n$ pour avoir L=$\mathbb{K}(a^{1/n})$. □

**7.12 Corollaire.** — *Sous les mêmes hypothèses, $X^n - a$ est irréductible sur $\mathbb{K}$ si et seulement si a$\notin \mathbb{K}^{\times l}$ pour tout l diviseur premier de n.*

**7.13 Exemple.** *Sur $\mathbb{Q}((1+i)/\sqrt{2})=\mathbb{Q}(i, \sqrt{2})$, $X^8 - 3$ est irréductible, car 3 n'est pas un carré.*

# Références


[1] GRAS Marie-Nicole GRAS Georges. *Algébre fondamentale - Arithmétique*. Ellipses, 2004.

[2] STEWART Ian. *Galois Theory, Third Edition*. Chapman & Hall/Crc Mathematics, 2003.