Chapitre 1

Bibliographie

Voici une liste de livres de théorie de Galois. J'ai mis quelques commentaires pour vous guider.

— Patrice Tauvel, *Corps commutatifs et théorie de Galois : cours et exercices* Calvage & Mounet, 2007, Mathématiques en Devenir ; 102.
(très complet allant des polynômes à la théorie de Galois différentielle, niveau M1.)
— Daniel Guin, Thomas Hausberger ; *Algèbre Tome 1. Groupes, corps et théorie de Galois*, EDP Sciences.
(contenu du livre proche du programme de l'UE, contient une partie exercices sur machine)
— Jean-Pierre Escoffier, *Théorie de Galois : Cours et exercices corrigés*, Dunod
— Joseph Rotman, *Galois theory*, Springer universitext,
(un cours court, mais plus complet que ce poly, clair mais en anglais)
— Julius Brezinski, *Galois Theory through exercices*, Springer undergraduates mathematics series.
(un recueil assez complet d'exercices corrigés)

— je n'ai pas mis les livres édités chez Ellipses (Gozard et Calais) ils sont peut être bien mais le travail d'édition (mise en page etc.) les rend pénibles à lire

Chapitre 2

Extensions de corps — Rappels

Par définition tout corps est commutatif et tout morphisme d'anneau (unitaire) envoie 1 sur 1.

1 Caractéristique

Soit K un corps. Il existe un unique morphisme d'anneau de $\mathbb{Z}$ dans K. Le noyau de ce morphisme est un idéal $p\mathbb{Z}$ ($p \geq 0$), son image est un anneau intègre isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et donc $p = 0$ ou p est premier.

Définition 1.1 *L'entier p premier ou nul ainsi défini s'appelle la caractéristique de K.*

Le sous-corps de K engendré par 1 s'appelle son sous-corps premier. C'est l'intersection de tous les sous-corps de K.

Proposition 1.2 – *Si K est un corps de caractéristique nulle, son sous-corps premier est isomorphe à $\mathbb{Q}$.*
– *Si K est un corps de caractéristique $p > 0$, son sous-corps premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Propriété 1.3 *Si $\sigma : K \to K$ est un morphisme de corps alors σ est injectif et la restriction de σ au sous-corps premier de K est l'identité (ie $\sigma(x) = x$ pour tout x dans le sous-corps premier).*

Proposition 1.4 *Soit K un corps de caractéristique $p > 0$. L'application $\varphi : x \mapsto x^p$ est un isomorphisme de K sur un de ses sous-corps.*

Preuve : On a bien $\varphi(xy) = \varphi(x)\varphi(y)$. Comme p est premier pour tout $0 < k < p$, p divise $\binom{n}{k}$ et (rappel $px = 0$) donc $(x+y)^p = x^p + y^p$ ie $\varphi(x+y) = \varphi(x) + \varphi(y)$. Par ailleurs tout morphisme de corps est injectif (c'est évident mais important) et $\varphi(K)$ est un sous-corps de K.□

2 Critère d'Eisenstein

Théorème 2.1 *Soient A un anneau factoriel*[1] *et K son corps des fractions. Soit $f(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de $A[X]$ de degré $n > 0$. S'il existe un idéal premier*[2] *I de A tel que*

$$a_n \notin I, \quad a_i \in I,\ 0 \leq i < n, \quad a_0 \notin I^2$$

alors f est irréductible dans $K[X]$.

1. ie intègre et tq tout élément s'écrit, de façon unique modulo inversibles, comme produit d'éléments irréductibles
2. ie tel que $a\,b \in I$ implique $a \in I$ ou $b \in I$ ou encore A/I intègre

Preuve : On utilise le lemme de Gauss : *Soient A un anneau factoriel et K son corps de fractions, un polynôme non constant P à coefficients dans A est irréductible dans $A[X]$ si et seulement s'il est primitif*[3] *et irréductible dans $K[X]$.*

On peut supposer f primitif (ie de contenu 1) cela ne change rien à son irréductibilité dans $K[X]$. Si f est réductible dans $K[X]$ il l'est donc dans $A[X]$. On écrit $f = gh$ avec g et h dans $A[X]$ non constants. On note $\bar{f}, \bar{g}, \bar{h}$ les projetés de f, g, h dans $A/I\,[X]$. Comme p ne divise pas a_n, $\deg \bar{f} = \deg f$ et donc $\deg \bar{g} = \deg g$ et $\deg \bar{h} = \deg h$. On a

$$\bar{g}\bar{h} = \bar{a}_n X^n \neq 0$$

L'anneau $A/(p)$ étant intègre, on en déduit que $\bar{f}$ et $\bar{g}$ sont des monômes, en particulier leurs coefficients constants sont nuls (et donc ceux de f et g sont dans I). Mais alors $a_0 \in I^2$ (ie a_0 s'écrit comme le produit de deux éléments de I) ! Contradiction. □

Remarque : Le critère sera surtout utilisé sur Z où les idéaux premiers sont ceux engendrés par les nombres premiers. Si $I = (p)$ la condition $a \in I$ s'écrit $p|a$ et $a \in I^2$ s'écrit $p^2|a$.

Applications :
– $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.
– $T^n - X \in F_p[X][T]$ est irreductible dans $F_p(X)[T]$. On prend $p = X$.
– Si p est premier, $\frac{X^p-1}{X-1} \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ (on pose $X = Y + 1$ et on utilise $\sum_{r \leq i \leq n} \binom{i}{r} = \binom{n+1}{r+1}$).

3 Degré d'une extension

Définition 3.1 *Une extension d'un corps K est la donnée d'un corps L contenant K comme sous-corps. On note L/K.*

Exemples : Tout corps est une extension de son sous-corps premier.
$\mathbb{C}$ est une extension de $\mathbb{R}$.
Si K est un corps et f un polynôme irréductible[4] de $K[X]$ alors $K[X]/(f)$ est un corps qui contient K comme sous-corps. Autrement dit $K[X]/(f)$ est une extension de K.

On voit facilement que si L est une extension de K alors L a une structure de K-espace vectoriel.

Définition 3.2 *Soit L/K une extension. On note $\dim_K L$ la dimension du K-espace vectoriel L. Si $\dim_K L = \infty$, on dit que L est une extension infinie de K ; si $\dim_K L$ est finie, on dit que L est une extension finie de K. On appelle alors degré de L sur K, et on note $[L : K]$, la quantité $\dim_K L$.*

Exemples : — Si K est un corps et f un polynôme irréductible de $K[X]$ alors $(\pi(1), \pi(X), \ldots, \pi(X^{n-1})$ est une base du K-espace vectoriel $K[X]/(f)$ et donc $[K[X]/(f) : K] = \deg f$.
— $\mathbb{R}/\mathbb{Q}$ est infinie.

Proposition 3.3 *Considérons une « tour d'extension » $L/M/K$. Alors $[L : K]$ est fini <u>ssi</u> $[L : M]$ et $[M : K]$ sont finis. Dans ce cas*

$$[L : K] = [L : M][M : K].$$

Preuve : Tout famille génératrice du K-espace vectoriel L est aussi une famille génératrice du M-esp. vect. L (inversement pour les familles libres) et M est un K-sous-espace-vectoriel de L. D'où L/K finie implique L/M et M/K finies.

3. ie le pgcd (qui existe vu que A est factoriel) de ses coefficients est égal à 1
4. ie qui n'est ni inversible ni produit de deux éléments non inversibles

Réciproquement, si L/M et M/K sont finies, on se donne une base $(e_i)_{1\leq i\leq n}$ de L/M et une base $(f_j)_{1\leq j\leq m}$ de M/K. Les e_i engendrent le M-esp vect L donc

$$\exists\ a_1,\dots a_n \in M, x = \sum_{i=1}^{n} a_i e_i,$$

de même pour tout $i \in \{1,\dots,n\}$

$$\forall i \in \{1,\dots,n\}, \exists\ b_{1,i},\dots b_{m,i} \in K, a_i = \sum_j b_{j,i} f_j.$$

Ainsi,

$$x = \sum_{i,j} b_{j,i} f_j e_i.$$

Ce qui montre que la famille $\{f_j e_i\}$ engendre le K-espace vectoriel L.
Enfin, soient $\alpha_{i,j} \in K$ tels que $\sum_{i,j} \alpha_{i,j}(f_j e_i) = 0$. Vu que $\sum_{i,j} \alpha_{i,j}(f_j e_i) = \sum_i \left(\sum_j \alpha_{i,j} f_j\right) e_i$ et que la famille $\{e_i\}$ (vus comme vecteurs du M-esp vect L) est libre, on voit que pour tout $i \in \{1\dots n\}$, on a $\sum_j \alpha_{i,j} f_j = 0$ ce qui implique à son tour $\alpha_{i,j} = 0$ pour tout i, j, vu que $\{e_i\}$ est une famille libre du K-ev M. □

4 Éléments algébriques

Soient L/K une extension et $\alpha \in L$. On note $K[\alpha]$ (resp. $K(\alpha)$) le sous-anneau (resp. le sous-corps) de L engendré par K et α. On considère le morphisme d'anneaux *surjectif* suivant appelé morphisme d'évaluation :

$$\begin{aligned} \mathrm{eval}_\alpha : K[X] &\to K[\alpha] \\ f &\mapsto f(\alpha). \end{aligned}$$

Comme $K[X]$ est principal, il existe $f_\alpha \in K[X]$ tel que $\ker(\mathrm{eval}_\alpha) = (f_\alpha)$, f_α est irréductible et unitaire ou nul.

Définition 4.1 *Si $f_\alpha = 0$ on dit que α est transcendant sur K, sinon on dit qu'il est algébrique sur K. Dans ce cas, f_α est appelé le polynôme minimal de α sur K.*

Propriété 4.2 *Soient L/K une extension et $\alpha \in L$ algébrique sur K de polynôme minimal f_α. Alors*

$$K[X]/(f_\alpha) \simeq K[\alpha] = K(\alpha)$$

(l'isomorphisme étant induit par par $eval_\alpha$) et $[K(\alpha) : K] = \deg f_\alpha$ (le degré c'est le degré).

Définition 4.3 *Une extension L/K est dite algébrique si tout $\alpha \in L$ est algébrique sur K.*

Proposition 4.4 *Soit L/K une extension. Alors L/K est finie <u>ssi</u> L/K est algébrique et de type fini (ie $\exists\ \alpha_1,\dots,\alpha_k, L = K(\alpha_1,\dots\alpha_n)$).*

Preuve : Si L/K est finie alors L/K est de type fini. Si $\alpha \in L$, alors $K(\alpha)$ est un K-sous-esp vect de L et donc $K(\alpha)/K$ est finie. Ainsi il existe $n \in \mathbb{N}$ tel que $\{\alpha^i, 0 \leq i \leq n\}$ est "K-liée" ie il existe $f \in K[X]$ non nul tel que $f(\alpha) = 0$.
Supposons $L = K(\alpha_1,\dots\alpha_n)$ algébrique sur K. On définit les corps K_i par $K_i = K_{i-1}(\alpha_i)$. Chaque α_i est algébrique sur K donc sur K_{i-1}. D'où K_i/K_{i-1} est finie et donc par multiplicativité des degrés L/K est finie. □

Exemples :
— $\sqrt[3]{2}$ a pour polynome minimal $X^3 - 2$ car celui-ci est bien irréductible, par Eisenstein. On a donc

$$Q(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3 - 2)$$

Il a pour base (en tant que $\mathbb{Q}$-ev) $(1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$ (ce qui montre au passage que $\sqrt[3]{2}$ n'est pas rationnel).
— $i \in \mathbb{C}$ est algébrique de degré 2 sur $\mathbb{R}$ (ou $\mathbb{Q}$), racine de $X^2 + 1$. D'où

$$\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1) \quad \text{et} \quad \mathbb{Q}(i) \simeq \mathbb{Q}[X]/(X^2 + 1).$$

— e et π sont des nombres transcendants sur $\mathbb{Q}$,

$$\mathbb{Q}(\pi) \simeq \mathbb{Q}(X).$$

Corollaire 4.5 *Soit $L/M/K$ une tour d'extension. Alors L/K est algébrique ssi L/M et M/K le sont.*

Preuve :
Il est clair que si L/K est une extension algébrique, alors M/K et L/M sont des extensions algébriques. On suppose que L/M et M/K sont des extensions algébriques. Soit $\alpha \in L$: il existe des éléments de M : $a_0, \ldots, a_n$ non tous nuls, tels que $\sum a_i \alpha^i = 0$. Considérons $M_0 = K(a_0, \ldots, a_n)$; puisque les a_i sont dans M, ils sont algébriques sur K. Par conséquent M_0/K est finie. De plus $M_0(\alpha)/M_0$ est finie (on a même $[M_0(\alpha) : M_0] \leq n$), par multiplicativité des degrés $M_0(\alpha)/K$ l'est également et donc α est algébrique sur K.□

Exercice : L'ensemble $\overline{\mathbb{Q}}$ des nombres complexes algébriques sur $\mathbb{Q}$ est un corps dénombrable. L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est infinie. Toute extension algébrique de $\overline{\mathbb{Q}}$ est triviale (égale à $\overline{\mathbb{Q}}$) on dit que $\overline{\mathbb{Q}}$ est « algébriquement clos ».

5 Corps de rupture et corps de décomposition

Définition 5.1 *Soient L/K et L'/K deux extensions. On appelle K-morphisme de L dans L', un morphisme de corps qui prolonge l'identité de K (càd dont la restiction à K est l'identité).*

Un K-morphisme est donc aussi un morphisme de K-espace vectoriel, c'est donc un morphisme de K-algèbre.
Remarque : Si $\sigma : L \to L'$ est un K-morphisme et si $f \in K[X]$, alors

$$\forall x \in L, \sigma(f(x)) = f(\sigma(x)).$$

En particulier si x est une racine de f alors $\sigma(x)$ en est une aussi.

Proposition 5.2 *Si L/K est algébrique et si σ est un K-endomorphisme de L alors σ est un K-automorphisme.*

Preuve : On veut montrer que σ est surjective. Soit $\alpha \in L$ et R l'ensemble des racines dans L de son polynome minimal sur K. On a $\sigma(R) \subset R$ et donc $\sigma(R) = R$ (injectif + fini). Ainsi $\alpha \in \sigma(R) \subset \sigma(L)$.□

Définition 5.3 *Soit K un corps et soit $f \in K[X]$* irréductible. *Le quotient $K[X]/(f)$ est un corps appelé* le *corps de rupture de f sur K.*

Remarque : Le corps K se plonge dans $K[X]/(f)$ via la projection canonique et f a au moins une racine dans $K[X]/(f)$ à savoir $\bar{X}$ l'image de X par la projection canonique. En fait $K[X]/(f)$ se plonge dans tout corps ayant cette propriété :

Proposition 5.4 (Propriété universelle des corps de rupture) *Soit K un corps et soit $f \in K[X]$ irréductible. Pour toute extension L/K contenant une racine α de f il existe un unique K-morphisme de corps $\psi : K[X]/(f) \to L$ et tel que $\psi(\bar{X}) = \alpha$. Si $L = K(\alpha)$ le morphisme ψ est un isomorphisme.*

Preuve : Un élément x de $K[X]/(f)$ s'écrit $\sum_i^n a_i \overline{X}^i$, si ψ est un morphisme de corps prolongeant l'identité de K on a donc $\psi(x) = \sum_i^n a_i \psi(\overline{X})^i$. Ce qui prouve l'unicité. Dire que α est une racine de f c'est dire que f appartient à $\ker \mathrm{eval}_\alpha$ ie que f est un multiple de f_α (le polyn min de α). Comme f est irréductible c'est que $f = \lambda f_\alpha$, avec $\lambda \in K$. On a donc $(f) = (f_\alpha)$. Le thm de factorisation, appliqué à eval_α, assure l'existence de ψ et la propriété 4.2 donne le dernier point. □

Définition 5.5 *Étant donné $f \in K[X]$ irréductible, on dira qu'une extension L de K est* un *corps de rupture de f s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$. Tout corps de rupture est isomorphe au corps de rupture :)*

Exemples :
— $X^3 - 2$ irreductible dans $\mathbb{Q}[X]$ a pour racines $\sqrt[3]{2}$ et $j\sqrt[3]{2}$. Ce qui donne deux corps de rupture distincts mais isomorphes.
— $X^4 + X^3 + X^2 + X + 1$ est irréductible (5-Eisenstein) et pour toute paire de racines $\zeta, \zeta' \in \mathbb{C}$ on a $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta')$.

Définition 5.6 *Soient K un corps et f un polynôme non constant de $K[X]$. On appelle corps de décomposition de f sur K, une extension (algébrique) L/K telle que f est scindé dans L, de racines $\alpha_1, \ldots, \alpha_n$ et $L = K(\alpha_1, \ldots, \alpha_n)$.*

On montre facilement

Proposition 5.7 *Tout polynôme $f \in K[X]$ possède un corps de décomposition L et $[L : K] \leq (\deg f)!$.*

Preuve : Récurrence sur le degré de f. Hérédité montrée en considérant le corps de rupture d'un facteur irréductible. □

Exemple : $f \in \mathbb{Q}[X]$ a un unique corps de décomposition contenu dans $\mathbb{C}$, le sous-corps engendré par les racines de f. Si on ne suppose plus l'extension contenue dans $\mathbb{C}$, on a encore un résultat d'unicité à isomorphisme près.

Proposition 5.8 *Soient $f \in K[X]$, L/K et L'/K deux corps de décomposition de f. Alors L et L' sont K-isomorphes.*

On repousse la preuve de la proposition 5.8 à la section suivante où on donnera un résultat plus général.

Unicité des corps finis Si K est un corps fini de caractéristique p alors $|K| = p^r$. Pour tout $x \in K^\times$, $x^{p^r-1} = 1$ (Lagrange) et donc K est le corps de décomposition de $X^{p^r} - X$. Il y a donc au plus un corps de cardinal p^r à isomorphisme près (on notera F_q le corps à q éléments).

6 Prolongement de morphismes

Une des questions clef dans la suite est de savoir si lorsqu'on se donne un morphisme $s : K \to K'$ et deux extensions L/K et L'/K', s'il est possible d'étendre s en un morphisme de K dans K'. On se donne ici des critères en ce sens.

Notation : Pour tout morphisme $s : K \to K'$, on note $\widehat{s} : K[X] \to K'[X]$ le morphisme d'anneau défini par $\widehat{s}(\sum_i a_i X^i) = \sum_i s(a_i) X^i$ (vérifiez qu'il s'agit bien d'un morphisme).

Proposition 6.1 *Soient $s : K \to K'$ un morphisme de corps et f un polynôme irréductible de $K[X]$. Soient $\alpha \in L/K$ une racine de f et $\alpha' \in L'/K'$ une racine de $\widehat{s}(f)$. Il existe un unique morphisme de corps $\sigma : K(\alpha) \to L'$ prolongeant s et tel que $\sigma(\alpha) = \alpha'$. De plus si s est un isomorphisme alors σ induit un isomorphisme entre $K(\alpha)$ et $K'(\alpha')$.*

Preuve : Soit $K'' = s(K) \subset K'$. La "corestriction" de s à K'' est un isomorphisme, donc $\widehat{s}(f)$ est un polynôme irréductible de $K''[X]$. Soit $\pi'' : K''[X] \to K''[X]/(\widehat{s}(f))$ la projection canonique. Le théorème de factorisation appliqué à $\pi'' \circ \widehat{s}$ nous dit que $\widehat{s}$ induit un isomorphisme entre $K[X]/(f)$ dans $K''[X]/(\widehat{s}(f))$. La proposition 5.4 nous permet d'en déduire un isomorphisme entre $K(\alpha)$ et $K''(\alpha)$. Comme $K''(\alpha)$ est un sous-corps de L', on a montré l'existence. L'unicité est évidente. □

Remarque : Si σ est un morphisme de corps qui prolonge s alors $\sigma(\alpha)$ est une racine de $\widehat{s}(f)$. On voit donc qu'il existe autant de prolongement de s à $K(\alpha)$ que de racines de $\widehat{s}(f)$ dans L'.

Proposition 6.2 *Soient $s : K \to K'$ un morphisme de corps, $f \in K[X]$, L une extension de K engendrée par <u>des</u> racines de f et L' une extension de K' sur laquelle $\widehat{s}(f)$ est scindé. Alors, il existe un morphisme de corps $\sigma : L \to L'$ qui prolonge s. Il en existe au plus $[L : K]$ avec égalité si $\widehat{s}(f)$ est à racines simples.*

De plus si s est un isomorphisme et si L et L' sont des corps de décomposition respectivement de f et de $\widehat{s}(f)$, alors σ est un isomorphisme.

Preuve : Par réccurence sur $[L : K]$ (qui est bien fini). Si $[L : K] = 1$ c'est évident.

Si $[L : K] > 1$, il existe une racine $\alpha \in L$ de f telle que $[K(\alpha) : K] > 1$. On note g son polynôme minimal sur K, g divise f. Le polynôme $\widehat{s}(g)$ divise $\widehat{s}(f)$ qui est scindé. Il est donc scindé. On *choisit* β une racine de $\widehat{s}(g)$ dans L'. D'après la prop. 6.1, il existe un (unique) morphisme s_1 de $K(\alpha)$ dans L' prolongeant s et vérifiant $s_1(\alpha) = \beta$.
On a $[K : k(\alpha)] < [K : k]$. D'après l'hyphotèse de récurrence (certes non formulée mais claire). il existe un morphisme σ de L (vu comme extension de $K(\alpha)$) dans L' (vu comme extension de $K'(\beta)$) prolongeant s_1. Ce qui montre l'existence.

Si s est un isomorphisme et L est un corps de décomposition de f alors $\sigma(L)$ contient K' et toutes les racines de $\widehat{s}(f)$ dans L'. Si L' est un corps de décomposition de $\widehat{s}(f)$, on a donc $\sigma(L) = L'$ et σ est un isomorphisme.

Si $L = K(\alpha_1, \dots \alpha_n)$ avec les α_i racines de f. On note $f_1 \in K[X]$ le polynôme minimal de α_1. Il existe autant de prolongements s_1 de s à $K(\alpha_1)$ que de racines de $\widehat{s}(f_1)$ dans L' (cf. remarque ci-dessus). Le nombre de racines de $\widehat{s}(f_1)$ est majoré par $\deg(f_1) = [K(\alpha_1) : K]$ avec égalité si $\widehat{s}(f_1)$ est à racines simples. De même, le nombre de prolongement de s_1 de $K(\alpha_1)$ à $K(\alpha_1, \alpha_2)$ est égal au nombres de racines distinctes de $\widehat{s}_1(f_2) \in K(\alpha_1)[X]$, avec f_2 polyn. minimal de α_2 sur $K(\alpha_1)$, avec égalité si $\widehat{s}_1(f_2)$ est à racines simples (il est scindé vu que $\widehat{s}_1(f_2)$ divise $\widehat{s}_1(f) = \widehat{s}(f)$ qui est scindé). Ainsi de suite, [5] on voit que le nombre de prolongements de s à L est majoré par $[K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots \alpha_{n-1})] \dots [K(\alpha_1) : K] = [L : K]$ avec égalité <u>ssi</u> tous les $\widehat{s}_i(f_{i+1})$ sont à racines simples en particulier si $\widehat{s}(f)$ est à racines simples. □

Corollaire 6.3 *Soit $f \in K[X]$. Deux corps de décomposition de f sur K sont K-isomorphes.*

Preuve : On applique la proposition ci-dessus avec $s = \mathrm{id}$.

On utilisera parfois la proposition 6.2 sous la forme si L est une extension finie de K alors tout morphisme de corps de K dans K' s'étend en un morphisme de L dans une extension de K'.

5. le lecteur pointilleux rerédigera ce paragraphe sous forme d'une récurrence

Chapitre 3

Séparabilité

1 Séparabilité d'un polynôme

Définition 1.1 *Soit $f \in K[X]$ de degré n. On dit que f est séparable (sur K) s'il existe une extension L/K tq f admet n racines* distinctes *dans L. Un polynôme non séparable est dit inséparable.*

Exemples :
— Tout polynôme de degré 2 de $\mathbb{Q}[X]$ de discriminant non nul. Par exemple X^2+1.
— Sur F_3, X^3-2 est inséparable car égal à $(X+1)^3$. Vu comme polyn̂ de $\mathbb{Q}[X]$ il est séparable.
— $X^p - T \in F_p(T)[X]$ n'est pas séparable (si α est une racine elle est de multiplicité p). Il est aussi irréductible (Eisenstein).

Définition 1.2 *Soit L/K une extension. Un élément $\alpha \in L$ algébrique sur K est dit séparable sur K si son polynôme minimal $f_\alpha \in K[X]$ l'est (sinon on dit qu'il est inséparable).*
L'extension algébrique L/K est dite séparable sur K si tous ses éléments le sont.

Exemples :
— $\sqrt[3]{2}$ est séparable sur $\mathbb{Q}$.
— Le corps de rupture de $X^p - T \in F_p(T)[X]$ n'est pas séparable. Il contient une racine α de multiplicité p.

On caractérise la séparabilité en utilisant le polynôme dérivé. On rappelle que le polynôme dérivé de $\sum_{i\geq 0} a_i X^i \in K[X]$ est $\sum_{i\geq 0}(i+1)a_{i+1}X^i$ ($i+1$ désigne l'image de l'entier $i+1$ par l'unique morphisme de $\mathbb{Z}$ dans K et peut-être nul). On vérifie que $(fg)' = f'g + fg'$ et que $\deg f' < \deg f$.

Proposition 1.3 *f est séparable sur K ssi $f \wedge f' = 1$.*

Preuve : Premièrement on remarque que deux polynômes f et g ont un facteur commun non trivial ssi il existe une extension dans laquelle ils ont une racine commune (prendre le corps de rupture d'un facteur irréductible commun).
Supposons f séparable et non constant et considérons un corps de décomposition L/K. On a donc

$$f(X) = c\prod_i (X-\alpha_i)$$

dans $L[X]$ avec les α_i 2 à 2 distincts. Alors

$$f'(X) = c\sum_i \prod_{j\neq i}(X-\alpha_j)$$

et donc

$$f'(\alpha_k) = c\prod_{j\neq k}(\alpha_k - \alpha_j) \neq 0.$$

Ainsi f et f' n'ont aucune racine commune et donc $f \wedge f' = 1$.

Récipt. si f est inséparable il existe L/K et $\alpha \in L$ tels que $(X-\alpha)^2$ divise f dans $L[X]$ ie il existe $h \in L[X]$ tel que $f(X) = (X-\alpha)^2 h(X)$. On a alors $f'(\alpha) = 0$.□

Exemple : Si $f(X) = X^n - a$, $a \neq 0$, alors $f'(X) = nX^{n-1}$.
Si $n \neq 0$ dans K (ie si $\mathrm{car}(K)$ ne divise pas n) alors $f \wedge f' = 1$ et f est séparable (tout élément non nul a n racine n-ième).
Si $n = 0$ (ie si $\mathrm{car}(K)$ divise n) alors $f' = 0$ et f est inséparable (a a moins de n racine n-ième).
Sur $\mathbb{F}_2$, les polynômes $X^3 - 1$ et $X^9 - 1$ sont séparables mais $(X^6 - 1) = (X^3 - 1)^2$. Il n'existe que 3 racines 6-ième de l'unité en caractéristique 2 (parce qu'il n'existe qu'une racine carrée de 1).

Exercice (existence des corps finis) Montrer que $X^{p^r} - X \in F_p[X]$ est séparable et l'ensemble de ses racines forment un corps à p^r éléments.

Corollaire 1.4 *Un polynôme $f \in K[X]$ irréductible est inséparable ssi $f' = 0$. Ce qui est équivalent à dire que K est de caractéristique $p > 0$ et que $f \in K[X^p]$.*

Preuve : Si $f' \neq 0$ alors $f \wedge f' = 1$ (par irréductibilité de f) et f est séparable. Si $f' = 0$, $f \wedge f' = f \neq 1$ et f est inséparable.
Si $f = \sum_i a_i X^i$ et $f' = 0$ alors $\forall i, i a_i = 0$. Or il existe $i > 0$ tel que $a_i \neq 0$ (par définition un polynôme irreductible n'est pas inversible) et donc K est de caractéristique $p > 0$ et p divise tous les i tels que $a_i \neq 0$ ie $f \in K[X^p]$. □

Pour le moment nous n'avons qu'un exemple de polynôme irreductible et inseparable, en voici la raison :

Proposition 1.5 *Soit K un corps fini ou de caractéristique 0, alors toute extension algébrique de K est séparable sur K.*

Plus généralement, si $\mathrm{car}(K) = p > 0$,

$$L/K \text{algebrique} \Rightarrow L/K \text{separable}$$

si et seulement si le Frobenius $\mathrm{Fr} : K \to K, x \mapsto x^p$ *est surjectif.*

Preuve : Si K est de caract. 0 tout polynôme irréductible est séparable et donc tout polyn. minimal l'est et toute extension algébrique est séparable.

Si $|K| < \infty$ alors Fr est une application injective (un morph de corps) entre ensembles finis il est donc surjectif.

Montrons le dernier cas. Soit $g \in K[X]$. Si $g' \neq 0$ il est séparable, si $g' = 0$ alors $g(X) = \sum_i a_i X^{p\,i}$. Si Fr est surjectif alors pour tout i il existe b_i tel que $b_i^p = a_i$, donc

$$g = \sum_i b_i^p (X^i)^p = (\sum_i b_i X^i)^p$$

et g est donc reductible.

La réciproque sera vue en TD. □

Les corps vérifiant les conclusions de la proposition ci-dessus sont dit **parfaits.**

Proposition 1.6 *Soient des extensions $M/L/K$. Si M/K est séparable alors M/L et L/K sont aussi séparables.*

Preuve : Il est évident que L/K est séparable. Soit $x \in M$. Le polynome minimal de x sur L divise celui de x sur K. Il est séparable. □

Théorème 1.7 (de l'élément primitif) *Soit L/K une extension finie et séparable alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Preuve : Si K est fini alors L est fini et donc $L^\times$, son groupe multiplicatif, est cyclique[1]. Si $L^\times = \langle \alpha \rangle$ alors $K(\alpha) = L$.

On suppose donc K infini. L/K finie implique algébrique de type fini. On écrit $L = K(\alpha_1, \ldots, \alpha_k)$. Traitons le cas $k = 2$, le cas général s'en déduit par récurrence immédiate (en utilisant la proposition 1.6). On suppose donc que $L = K(\alpha, \beta)$ avec α, β alg. sur K. On note f et g les pol. min. de α et β sur K et on considère M/K un corps de décomposition de fg.

On cherche un élément primitif parmi les combinaisons K-linéaires de α et β. On pose

$$\gamma = \alpha + \lambda\beta, \quad \lambda \in K.$$

On va montrer que seul un nombre fini de λ ne donne pas un élément primitif (en essayant au hasard ça doit marcher). Bien sûr $\beta \in K(\gamma)$ implique $K(\alpha, \beta) = K(\gamma)$. On regarde donc le degré du polynôme minimal de β sur $K(\gamma)$.

On considère $h \in K(\gamma)[X]$ défini par $h(X) = f(\gamma - \lambda X)$. On a $h(\beta) = f(\alpha) = 0$. Par conséquent, le polynôme minimal de β dans $K(\gamma)$ divise g et h et donc $g \wedge h$. On montre qu'il existe λ tel que $\deg(g \wedge h) < 2$.

Supposons que $\deg(g \wedge h) \geq 2$. Comme $g \wedge h$ est séparable (en tant que diviseur d'un polynôme séparable), il existe $\beta' \neq \beta$ dans M racine commune de g et h. On pose $\alpha' = \gamma - \lambda\beta' \in M$, c'est une racine de f. Alors $\gamma = \alpha' + \lambda\beta' = \alpha + \lambda\beta$ donc $\lambda = \frac{\alpha - \alpha'}{\beta' - \beta}$. Par conséquent, si

$$\lambda \notin \left\{ \frac{\alpha - \alpha'}{\beta' - \beta} \,|\, \alpha, \alpha' \text{ racines de } f,\ \beta \neq \beta' \text{ racines de } g \right\} \quad \text{(qui est un ensemble fini)}$$

alors $\deg(g \wedge h) = 1$, le degré du polyn minimal de β sur $K(\gamma)$ est aussi égal à 1 et $K(\alpha, \beta) = K(\gamma)$.□

Citons un autre résultat classique caractérisant les extensions monogènes, sa preuve sera vue en TD.

Théorème 1.8 (Steinitz) *Une extension finie est monogène (ie engendrée par un élément) si et seulement si elle ne contient qu'un nombre fini de corps intermédiaires.*

1. soit n le ppcm des ordres des éléments de $L^\times$. Tous les éléments de $L^\times$ sont des racines de $X^n - 1$ donc $n = |L| - 1$. Le groupe $L^\times$ est abelien donc il contient un élément d'ordre n (c'est le point délicat).

Chapitre 4

Normalité

Définition 0.1 *Une extension algébrique L/K est dite normale si tout polynôme irréductible à coefficients dans K, ayant au moins une racine dans L, a toutes ses racines dans L (ie est scindé sur L).*

Exemples : – Toute extension quadratique (de degré 2) est normale : Soit L/K telle que $[L : K] = 2$. Soit $f \in K[X]$ irréductible. Si f a une racine α dans L alors L contient un corps de rupture de f et donc f est de degré 1 ou 2. Il est divisible dans $L[X]$ par $X - \alpha$ et donc scindé.

– $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale. En effet, $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ et possède une racine dans $\mathbb{Q}(\sqrt[3]{2})$. Mais $j\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$ est une autre racine de $X^3 - 2$. On va voir que $\mathbb{Q}(j, \sqrt[3]{2})$ est normale.

Proposition 0.2 *Une extension finie L/K est normale ssi toute extension Ω/L et tout K-morphisme $\sigma : L \to \Omega$ vérifient $\sigma(L) \subset L$.*

Preuve : Soit $\sigma : L \to \Omega$ un K-morphisme. Soient $\alpha \in L$ et f_α sont polyn. minimal sur K. Comme L/K est normale f_α est scindé sur L. Clairement $\sigma(\alpha)$ est une racine de f_α et donc $\sigma(\alpha) \in L$.

Réciproquement, si L/K n'est pas normale, il existe $f \in K[X]$ irreductible ayant une racine $\alpha \in L$ et une racine $\beta \notin L$. D'après la proposition 6.2, il existe un K-morphisme de $K(\alpha)$ dans $K(\beta)$ qu'on peut étendre en un K-morphisme σ de L dans une extension Ω qui vérifie $\sigma(L) \not\subset L$. □

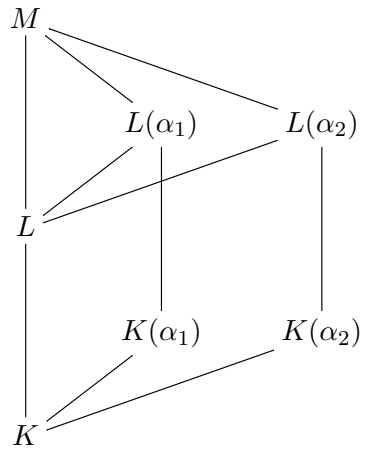
Corollaire 0.3 *Soient $L/K/k$ une tour d'extensions telle que L/k est finie et normale et $s : K \to K$ un k-automorphisme. Alors il existe un (k-)automorphisme $\sigma : L \to L$ qui prolonge s.*

Preuve : L'extension L/K étant finie, la proposition 6.2 implique que s s'étend en un morphisme σ de L dans une extension Ω/K. Comme L/k est normale et σ est un k-morphisme, la proposition 0.2 implique que $\sigma(L) \subset L$ et donc $\sigma(L) = L$ par proposition 5.2. □

Théorème 0.4 *Soit L/K une extension. Il existe $f \in k[X]$ tel que L/K soit un corps de décomposition de f ssi L/K est finie et normale.*

Preuve : Si L/K est finie et normale, alors il existe $b_1, \ldots, b_n$ tels que $L = K(b_1, \ldots, b_n)$ On note g_i le pol. min. de b_i. Chaque g_i a une racine dans L et comme L/K est normale chaque g_i est scindé sur L. Par conséquent L est un corps de décomposition sur K de $g = \prod_i g_i$.

Réciproquement, si L est un corps de décomposition de $f \in K[X]$, on a vu $[L : K] \leq (\deg f)! < \infty$. Pour montrer que L/K est normale, on considère $g \in K[X]$ irréductible ayant une racine dans L. Soit M un corps de décomposition de g sur L. Soient α_1 et α_2 deux racines de g, montrons que $\alpha_1 \in L \Leftrightarrow \alpha_2 \in L$.
C'est vrai si $\deg g = 1$. On suppose donc $\deg g \geq 2$. On a la situation suivante :



— Comme $K(\alpha_1)$ et $K(\alpha_2)$ sont deux corps de ruptures de g sur K, il existe un isomorphisme σ entre eux tel que $\sigma(\alpha_1) = \alpha_2$.
— Chaque $L(\alpha_i)$ est un corps de décomposition de f sur $K(\alpha_i)$. D'après la prop. 6.2, il existe un isomorphisme $\varphi : L(\alpha_1) \to L(\alpha_2)$ qui prolonge σ et donc $[L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)]$ (exercice).
— Ainsi

$$[L(\alpha_1) : K] = \underbrace{[L(\alpha_1) : K(\alpha_1)]}_{=[L(\alpha_2):K(\alpha_2)]} \underbrace{[K(\alpha_1) : K]}_{=[K(\alpha_2):K]} = [L(\alpha_2) : K]$$

En écrivant $[L(\alpha_i) : K] = [L(\alpha_i) : L][L : K]$ on voit que $[L(\alpha_1) : L] = [L(\alpha_2) : L]$. On a donc bien $\alpha_1 \in L \Leftrightarrow \alpha_2 \in L$ et donc L/K est normale.□

Exemples : – On peut retrouver le fait que toute extension quadratique est normale. Si K/k est quadratique et si $\alpha \in K \setminus k$ alors f_α le polynôme minimal de α est scindé sur K et $K = k(\alpha)$ et donc K/k est normale en tant que que corps de décomposition de f_α.
– $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est une extension normale, c'est un corps de décomposition de $X^3 - 2$.
– Soit ζ une racine $n$ieme primitive de l'unité (par exemple $e^{2i\pi/n}$). L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ (de degré $\varphi(n)$) est normale. En effet $\mathbb{Q}(\zeta)$ est le corps de décomposition de $X^n - 1$ (ou de son polynôme minimal (le $n$ieme polynome cyclotomique) si on veut de l'irréductible) sur $\mathbb{Q}$.
– Toute extension finie d'un corps fini k'/k est normale. En effet, si $|k| = q$ alors $|k'| = q^r$ et k' est le corps de décomposition de $X^{q^r} - X$ sur k.

Chapitre 5

Correspondance de Galois

1 Groupes d'automorphismes d'un corps et théorème d'Artin

On rappelle :

Définition 1.1 *Soient L/K et M/K deux extensions. Un K-morphisme de L dans M est un morphisme de corps qui prolonge l'identité de K (ie qui fixe K point par point).*
Un K-isomorphisme de L dans M est un K-morphisme bijectif, si $M = L$ on parle de K-automorphisme.
$\mathrm{Aut}(L) = \{\sigma : L \to L,\ \text{automorphisme}\}$ *et* $\mathrm{Aut}(L/K) = \{\sigma : L \to L,\ K-\text{automorphisme}\}$ *sont des groupes.*

Exemples : — Les automorphismes de $\mathbb{Q}(\sqrt{2})$ sont l'identité et $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (exercice).
— Le seul automorphisme de $\mathbb{Q}(\sqrt[3]{2})$ est l'identité (l'extension ne contient qu'une racine de X^3-2).
— Les $\mathbb{R}$-automorphismes de $\mathbb{C}$ sont id et la conjugaison complexe ($i \mapsto \pm i$), ainsi $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$ (montrer qu'il en est de même pour toute extension quadratique *séparable*).
— $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$! En effet, soit σ un $\mathbb{Q}$-autom. de $\mathbb{R}$. Comme tout nombre positif est un carré et que tout carré est positif $\sigma(\mathbb{R}_+) = \mathbb{R}_+$ et donc σ est monotone. Comme σ laisse fixe $\mathbb{Q}$ et que que $\mathbb{Q}$ est dense dans $\mathbb{R}$ on conclut par le thm des gendarmes.

Dans la suite on ne considèrera que des extensions finies (contrairement au dernier cas ci-dessus). Dans ce cas on n'a affaire qu'à des groupes finis, en effet :

Proposition 1.2 *Si K/k est une extension finie alors $|\mathrm{Aut}(K/k)| \leq [K : k]$. Si K est un corps de décomposition d'un polynôme à racines simples alors cette inégalité est une égalité.*

Preuve : $K = k(a_1, \ldots, a_k)$ et L un corps de décomposition de $\prod_{i=1}^{k} f_i$ contenant K, où f_i est le pol min de a_i. Tout k-automorphisme de K est un k-morphisme de K dans L. D'apres la prop 6.2, il y en a au plus $[K : k]$.
Le cas d'égalité est directement donné par la prop. 6.2. □

Exemples : — Le groupe $G = \mathrm{Aut}(\mathbb{Q}(j, \sqrt[3]{2}))$ est donc d'ordre 6. Si $s \in G$ alors $s(j) = j^a$ avec $a \in \{1, 2\}$ et $s(\sqrt[3]{2}) = j^b\sqrt[3]{2}, b \in \{0, 1, 2\}$. Ce qui donne les 6 possibilités (en fait $G \simeq S_3$). Il est facile de donner la matrice de s (vu comme un automorphisme d'un $\mathbb{Q}$-espace vectoriel de dimension 6) dans la $\mathbb{Q}$-base de $\mathbb{Q}(j, \sqrt[3]{2})$ de son choix, par exemple $\mathcal{B} = (1, j, 2^{1/3}, 2^{2/3}, j2^{1/3}, j2^{2/3})$. Ainsi si s est l'automorphisme obtenu en prenan $a = 2$ et $b = 0$ et s' avec $a = 1$ et $b = 1$, on a

$$M_{\mathcal{B}}(s) = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \qquad M_{\mathcal{B}}(s') = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}.$$

— Si K est un corps fini de cardinal $q = p^r$, alors son groupe d'automorphisme est cyclique engendré par ϕ l'automorphisme de Frobenius. Il suffit de voir que ϕ est d'ordre r. Si k désigne l'ordre de ϕ alors K est contenu dans l'ensemble des racines de $X^{p^k} - X$ et donc $k \geq r$. La proposition 1.2 donne l'autre inégalité.

Définition 1.3 *Pour tout G un sous groupe de $Aut(L)$, on note L^G le sous-corps de L défini par $L^G = \{x \in L \,|\, \sigma(x) = x, \forall \sigma \in G\}$, appelé corps des invariants de G dans L.*

Exemples : — Le corps des invariants du groupe $< s >$ ci-dessus est $\mathbb{Q}(2^{1/3})$ (l'inclusion est claire et son degré est un diviseur propre de 6). De même, le corps des invariants de $< s' >$ est $\mathbb{Q}(j)$.

— Si K est le coprs fini de cardinal $q = p^r$ alors le corps invariant par l'automorphisme de Frobenius ϕ est $\{x \in K \,|\, x^p = x\} = F_p$. Les sous-groupes de $\mathrm{Aut}(K)$ sont de la forme $G =< \phi^k >$ avec k divisant r alors $K^G = \{x \in K \,|\, x^{p^k} = x\} \simeq F_{p^k}$.

Théorème 1.4 (Artin) *Soit G un sous groupe fini de $Aut(L)$ et L^G son sous-corps fixe associé. Alors $[L : L^G] = |G|$.*

Preuve : On a déjà vu que $[L : L^G] \geq |G|$.

Autre sens : Soit $n = |G|$, on va montrer que toute famille à $n + 1$ éléments de L est L^H-liée. On note $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$.
Soit $(\alpha_1, \ldots, \alpha_{n+1}) \in L^{n+1}$. On lui associe le système suivant, d'inconnues $x_1, \ldots, x_{n+1}$

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \cdots \\ \sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_{n+1})x_{n+1} = 0 \\ \cdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0. \end{cases}$$

Il existe des solutions non nulles à ce sytème (thm. du rang). Soit $(c_1, \ldots, c_{n+1}) \in L^{n+1}$ une solution non nulle avec un nombre maximal de termes nuls. On peut supposer $c_1 \neq 0$ et même $c_1 = 1$.
On remarque que pour tout $\sigma \in G$ et tout i (en notant $\sigma_k = \sigma\sigma_i$)

$$0 = \sigma(\sigma_i(\alpha_1)c_1) + \cdots + \sigma(\sigma_i(\alpha_{n+1})x_{n+1})) = \sigma_k(\alpha_1)\sigma(c_1) + \cdots + \sigma_k(\alpha_{n+1})\sigma(c_{n+1})$$

et donc $(\sigma(c_1), \ldots, \sigma(c_{n+1})$ est encore une solution du système. Or $\sigma(c_1) = c_1$ et donc $(0, c_2 - \sigma(c_2), \ldots, c_{n+1} - \sigma(c_{n+1}))$ est aussi solution. Par maximalité du nombre de termes nuls de $(c_1, \ldots, c_{n+1})$ on voit que $c_i = \sigma(c_i)$ pout tout i et tout σ. Par conséquent, $c_i \in L^G$. La première ligne du système est donc $\sum_i \alpha_i c_i = 0$ avec les c_i dans L^G non tous nuls. Ce qui montre que toute famille de $n + 1$ vecteurs du L^G-espace vectoriel L est liée. Ainsi $[L : L^G] \leq n$.□

Corollaire 1.5 *Soit L un corps et G un groupe fini d'automorphismes de L. Alors*

$$G = \mathrm{Aut}(L/L^G).$$

Preuve : Bien-sûr $G \leq \mathrm{Aut}(L/L^G)$. Ainsi $|G| \leq |\mathrm{Aut}(L/L^G)| \leq [L : L^G] = |G|$ (Artin).□

2 Extensions galoisiennes

Définition 2.1 *Une extension L/K est dite galoisienne si elle est séparable et normale.*

Exemples : — En caractéristique différente de 2, toute extension quadratique est galoisienne.
— Rappelons que si K est fini ou de caractéristique nulle (ie parfait) alors la condition de séparabilité est automatique. Ce sera le cas principalement étudié.
— $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale et donc pas galoisienne. — Une extension finie d'un corps fini est toujours galoisienne.

Théorème 2.2 *Soit L/K une extension finie. Les propositions suivantes sont équivalentes :*

1) L/K est galoisienne,

2) L est le corps de décomposition d'un polynôme à racines simples $f \in K[X]$,

3) K est le corps invariant de $\mathrm{Aut}(L/K)$, le groupe des K-automorphisme de L, ie. $K = L^{\mathrm{Aut}(L/K)}$

4) Kest le corps invariant d'un sous-groupe fini G de $\mathrm{Aut}(L)$, ie $K = L^G$.

Preuve : 1) $\Rightarrow$ 2) : Il existe $a_1, \dots a_n$ tels que $L = K(a_1, \dots, a_n)$. On note f_i le pol.min. de a_i sur K. Chaque f_i est scindé et à racines simples sur L. Pour tout i, j, $f_i \wedge f_j = 1$, si $f_i \neq f_j$. Soit $J \in \{1, \dots, n\}$ le plus grand sous-ensemble tel que $\forall i \neq j \in J, f_i \neq f_j$. Le polynôme $f = \prod_{i \in J} f_i$ est à racines simples et L est un corps de décomposition de f.

2)$\Rightarrow$ 3) : Si L est le corps de décomposition d'un polynôme à racines simples $f \in K[X]$, alors $|\mathrm{Aut}(L/K)| = [L : K]$ d'après la proposition 1.2. Et donc $[L : K] = [L : L^{\mathrm{Aut}(L/K)}]$, nous dit le thm d'Artin. Ce qui entraine $K = L^{\mathrm{Aut}(L/K)}$ vu que $K \subset L^{\mathrm{Aut}(L/K)}$.

3)$\Rightarrow$ 4) évident

4) $\Rightarrow$ 1) On suppose $K = L^G$, $G \leq \mathrm{Aut}(L)$ fini. Le théorème d'Artin dit que $|G| = [L : K]$. Soient $\alpha \in L$ et f son polynôme minimal. On note $G.\alpha = \{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m\}$ l'orbite de α sous G (m divise $|G|$ c'est inutile ici). On définit

$$g(X) = \prod_{i=1}^{m} (X - \alpha_i) = X^m + \sum_{i=0}^{m-1} a_i X^i.$$

Les a_i sont des polynômes symétriques en les α_i. Comme G permute les α_i, chaque $a_i \in L^G = K$ et donc $g \in K[X]$. Par conséquent f divise g (α est racine de g). Mais tout α_i est racine de f (pour tout $h \in K[X]$, $\sigma(h(\alpha)) = h(\sigma(\alpha))$). Ainsi $g = f$ (ils sont tout deux unitaires) et donc f est scindé sur L et séparable. Ce qui montre que L/K est normale et séparable. □

Corollaire 2.3 *1) Toute extension finie et séparable de K est contenue dans une extension galoisienne.*
2) Soient L/M et M/K des extensions. Si L est galoisienne sur K alors L est galoisienne sur M.

Preuve : 1) $M = K(\alpha_1, \dots, \alpha_n)$. On prend pour L un corps de décomposition de "$\prod_{i \in J} f_i$" (cf. preuve du théorème 2.2)

2) Si L est un corps de décomposition de f sur K c'est aussi un corps de décomposition de f sur M (et f est toujours à racines simples).□

Contre-exemples :
— $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est galoisienne donc $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}(j)$ et $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ le sont aussi. MAIS on a vu (et revu) que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ne l'est pas.

— Les extensions $\mathbb{Q}(\sqrt{(}2)/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sont galoisiennes (car quadratiques) mais $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas ($X^4 - 2$ n'est scindé).

Remarques :

1) On a montré notamment que le corps de décomposition d'un polynôme séparable est séparable. Ce qui implique que *le corps de rupture d'un polynome séparable est séparable* ou plus généralement *une extension finie est séparable ssi elle est engendrée par des éléments séparables.*

2) La preuve de 4)$\Rightarrow$ 1) est à connaitre. Elle permet, une fois $\mathrm{Gal}(L/K)$ déterminé, de trouver le polynôme minimal de tout élément α de L. Elle donne en particulier le degré du polynôme minimal de α (le m de la preuve) et donc $[K(\alpha) : K]$.

Définition 2.4 *Si L/K est galoisienne, le groupe des K-automorphismes de L est appelé le* groupe de Galois *de l'extension L/K. Il est noté* $\mathrm{Gal}(L/K)$. *On a toujours* $|\mathrm{Gal}(L/K)| = [L : K]$.
Si L est le corps de décomposition de $f \in K[X]$ séparable, $\mathrm{Gal}(L/K)$ *est aussi appelé le groupe de Galois de f.*
Si L/K est galoisienne et $\alpha \in L$, l'orbite de α sous Gal(L/K), $\{\sigma(\alpha) \,|\, \sigma \in \mathrm{Gal}(L/K)\}$, est appelé l'ensemble des conjugués (de Galois) de α.

Soit $f \in K[X]$ et L/K un corps de décomposition de f. Le groupe de Galois de $f \in K[X]$ agit fidèlement sur l'ensemble des racines de f dans L (vu que les racines de f engendrent L, un K-automorphisme de L qui laisse fixe les racines de f est l'identité). On peut donc voir $\mathrm{Gal}(L/K)$ comme un sous-groupe du groupe des permutations de l'ensemble des racines de f (ce qui redémontre $|\mathrm{Gal}(L/K)|$ divise $(\deg f)!$).

Soit L/K galoisienne et $\alpha \in L$. On a vu que *l'ensemble des conjugués de α est aussi l'ensemble des racines du polynôme minimal de α. Le nombre de conjugués de α est donc égal à $[K(\alpha) : K]$. Ainsi $L = K(\alpha)$ si et seulement si le nombre de conjugués de α est égal à $[L : K]$.*

Notation : Pour tout groupe G on notera $\mathcal{G}$ l'ensemble des sous-groupes de G. Pour toute extension L/K, on note $\mathcal{K}(L/K)$ l'ensemble des corps intémédiaires entre L et K, ie l'ensemble des extensions de K contenue dans L.

Théorème 2.5 (Correspondance de Galois) *Soient L/K une extension galoisienne finie et $G = \mathrm{Gal}(L/K)$. Les applications :*

$$\begin{array}{ll} \mathcal{G} \to \mathcal{K}(L/K) & \textit{et} \quad \mathcal{K}(L/K) \to \mathcal{G} \\ H \mapsto L^H & \qquad\quad M \mapsto \mathrm{Gal}(L/M) \end{array}$$

sont des bijections réciproques l'une de l'autre. De plus :

1) *$G \supset H_1 \supset H_2 \Rightarrow (H_1 : H_2) = [L^{H_2} : L^{H_1}]$ (en particulier on a inclusion des extensions) ;*
2) *pour tout $\sigma \in G$ et tout $H \leq G$, au sous-groupe $\sigma H \sigma^{-1}$ correspond $\sigma(L^H)$;*
3) *$H \triangleleft G$ <u>ssi</u> L^H/K est galoisienne. On a alors Gal$(L^H/K) \simeq G/H$.*

Remarque : Les applications ci-dessus sont clairement décroissantes (pour l'inclusion)

Preuve : Si on a une tour d'extension $L/M/K$, on a vu que L/M galoisienne et donc $M = L^{\mathrm{Gal}(L/M)}$ d'après le théorème 2.2. Réciproquement, si $H \leq G$, L/L^H est galoisienne (toujours par le théorème 2.2), $H \leq \mathrm{Gal}(L/L^H)$, $|H| = [L : L^H]$ (Artin) et donc $H = \mathrm{Gal}(L/L^H)$.
1) On a vu $|\mathrm{Gal}(L/L^H)| = |H|$. Si $G \supset H_1 \supset H_2$ alors $L^{H_2} \supset L^{H_1} \supset K$ et

$$\underbrace{[L : L^{H_1}]}_{=|H_1|} = \underbrace{[L : L^{H_2}]}_{=|H_2|}[L^{H_2} : L^{H_1}].$$

et donc $(H_1 : H_2) = [L^{H_2} : L^{H_1}]$.
2) Tout $\tau \in G$ et tout $\alpha \in L$ vérifient :

$$\tau\alpha = \alpha \Leftrightarrow \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma(\alpha).$$

D'où $\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ et conclut en utilisant la correspondance.
3) Soit $H \triangleleft G$. On vient de montrer que pour tout $\sigma \in G$, $\sigma(L^H) = L^H$. Autrement dit tout élément de G se restreint en un K-automorphisme de L^H. On a donc un morphisme : $G \to \mathrm{Aut}(L^H/K)$, $\sigma \mapsto \sigma|_{L^H}$. Son noyau est H. On a donc $|\mathrm{Aut}(L^H/K)| \geq (G : H) = [L^H : K]$ et donc (par la proposition 1.2) L^H/K est galoisienne. Le premier thm d'isomorphisme (pour les groupes) donne l'isomorphisme entre $\mathrm{Gal}(L^H/K)$ et G/H (le morphisme donné plus haut est bien surjectif).
Réciproquement, soit $L/M/K$ avec M/K galoisienne. On applique la proposition 0.2 du chapitre 4 qui dit $\forall \sigma \in G, \sigma(M) = M$. D'après le point précédent, on a donc $\mathrm{Gal}(M/K) \triangleleft G$. □

Exemples de degré 6 : À isomorphisme près, il existe deux groupes d'ordre 6 ($\mathbb{Z}/6\mathbb{Z}$ et S_3) et donc deux types d'extension galoisienne de degré 6.
1) On a vu que $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est galoisienne (c'est un corps de décomposition de X^3-2) et de degré 6. On sait que son groupe de Galois peut être vu comme un sous-groupe du groupe des permutations des racines X^3-2 c'est-à-dire de S_3. Étant d'ordre 6 il est forcément isomorphe à S_3 (on peut aussi montrer que les éléments s et s' vus au début du chapitre ne commutent pas). Ainsi le groupe de Galois est en bijection avec le groupe des permutations de $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$ l'ensemble des racines de X^3-2 (voir l'exemple en début de chapitre pour plus de détails).
Le groupe S_3 a 6 sous-groupes : 3 d'ordre 2, 1 d'ordre 3 et les deux triviaux. Le seul sous-groupe propre distingué est celui d'indice 2. Il existe donc 4 corps intermédiaires propres :

- $\mathbb{Q}(\sqrt[3]{2})$ qui correspond au sous-groupe engendré par la transposition $(j\sqrt[3]{2}, j^2\sqrt[3]{2})$ (qui correspond au morphisme s' de début de chapitre),
- $\mathbb{Q}(j\sqrt[3]{2})$ qui correspond au sous-groupe engendré par la transposition $(\sqrt[3]{2}, j^2\sqrt[3]{2})$,
- $\mathbb{Q}(j^2\sqrt[3]{2})$ qui correspond au sous-groupe engendré par la transposition $(\sqrt[3]{2}, j\sqrt[3]{2})$,
- $\mathbb{Q}(j)$ qui correspond au sous-groupe d'ordre 3 (engendré par un 3-cycle qui correspond au morphisme s). C'est la seule extension galoisienne : elle est en correspondance avec un sous-groupe normal.

Les trois premiers sous-groupes sont conjugués et donc d'après le point 2) du théorème de correspondance de Galois les corps intermédiaires correspondants sont isomorphes (l'isomorphisme étant s ou s^2).

2) Soit ζ une racine primitive 7-eme de l'unité. Son polynome minimal est $\Phi_7(X) = 1+X+\cdots+X^6$. Il est clair que $\mathbb{Q}(\zeta)$ est le corps de décomposition (contenu dans $\mathbb{C}$) de Φ_7 et donc $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne, son groupe de Galois (qu'on notera G) est d'ordre 6. Pour tout $\sigma \in G$, il existe $1 \leq i \leq 6$ tel que $\sigma(\zeta) = \zeta^i$ et ce i détermine σ. On a en fait (vérifiez !) un isomorphisme de groupe :

$$G \to (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$$
$$\sigma \mapsto i \text{ (tq } \sigma(\zeta) = \zeta^i)$$

On sait donc que G a 4 sous-groupes (mais seulement 2 non triviaux), un par diviseur de 6, tous distingués (G est abélien). Les extensions correspondantes sont toutes galoisiennes.

On note σ_0 l'élément de G qui envoie ζ sur ζ^3, $\langle\sigma_0\rangle = G$ (vu que $3^2 \not\equiv 1 \mod 7$ et $3^3 \not\equiv 1 \mod 7$). L'autre générateur est donc σ_0^5 qui envoie ζ sur $\zeta^{3^5} = \zeta^5$. Le sous-groupe $H_2 = \langle\sigma_0^2\rangle$ est d'ordre 3 et H_1 celui engendré par σ_0^3 est d'ordre 2.

Pour trouver le corps invariant par H_1 il suffit de trouver un nombre invariant par σ_0^3 mais n'appartenant pas à $\mathbb{Q}$ (vu qu'on a affaire à une extension de degré premier). On remarque que $\sigma_0^3(\zeta) = \zeta^{27} = \zeta^6 = \overline{\zeta} = \zeta^{-1}$ et donc $\sigma_0^3(\zeta^6) = \zeta$. Ainsi $\sigma_0^3(\zeta+\overline{\zeta}) = \zeta+\overline{\zeta}$. C'est bien un irrationnel vu qu'il est envoyé par σ_0 sur $\zeta^3+\overline{\zeta}^3 \neq \zeta+\overline{\zeta}$ (la droite verticale $z+\overline{z} = \zeta+\overline{\zeta}$ coupe le cercle unité en 2 points) et sur $\zeta^2+\overline{\zeta}^2$ par σ_0^2. Son polynôme minimal est donc $(X-(\zeta+\overline{\zeta}))(X-(\zeta^2+\overline{\zeta}^2))(X-(\zeta^3+\overline{\zeta}^3)) \in \mathbb{Q}[X]$, qu'on pourrait développer si besoin. On a donc $\mathbb{Q}(\zeta)^{H_1} = \mathbb{Q}(\zeta+\overline{\zeta})$.

L'orbite de ζ par H_2 est $\{\zeta, \zeta^2, \zeta^4\}$ et donc l'orbite de $\zeta+\zeta^2+\zeta^4$ sous G est $\{\zeta+\zeta^2+\zeta^4, \zeta^3+\zeta^5+\zeta^6\}$. On développe donc (même si on ne sait pas encore que ces 2 nombres sont distints) le polynôme $(X-(\zeta+\zeta^2+\zeta^4))(X-(\zeta^3+\zeta^5+\zeta^6))$, on trouve X^2+X+2 [1] de discriminant -7 ce qui montre que les 2 nombres sont bien distincts (et donc $\zeta+\zeta^2+\zeta^4 \notin \mathbb{Q}$) et que $\mathbb{Q}(\zeta+\zeta^2+\zeta^4) = \mathbb{Q}(i\sqrt{7}) = \mathbb{Q}(\zeta)^{H_2}$.

En raison du lien entre les propriétés du groupe de Galois et celles de l'extension correspondante on pose :

Définition 2.6 *Une extension L/K est dite cyclique (resp. abélienne, résoluble, nilpotente (!),...) si L/K est galoisienne et si son groupe de Galois est cyclique (resp. abélien, résoluble, nilpotent (!),...).*

1. $(\zeta+\zeta^2+\zeta^4))(\zeta^3+\zeta^5+\zeta^6) = 3+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 = 2$

3 Résolubilité par radicaux

On suppose maintenant tous les corps de caractéristique nulle.

Définition 3.1 *Soit $f \in K[X]$. L'équation $f(x) = 0$ est dite résoluble par radicaux s'il existe une tour d'extension*

$$K_0 \subset K_1 \subset \cdots \subset K_m$$

telle que
a) pour tout $1 \leq i \leq m$ il existe $n_i \in \mathbb{N}$, $\alpha_i \in K_i$ tels que $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$,
b) K_m contient un corps de décomposition de f

Autrement dit, une équation est résoluble par radicaux si on sait exprimer ses racines grâce à une suite d'additions, multiplications et extractions de racines.

Théorème 3.2 (Tartaglia, Cardan(o), Ferrari) *Si $f \in K[X]$ est de degré inférieur ou égal à 4 alors l'équation $f(x) = 0$ est résoluble par radicaux.*

Abel a montré l'existence de polyn de degré 5 non résolubles par radicaux. Galois a fait mieux :

Théorème 3.3 (Galois) *L'équation $f(x) = 0$ est résoluble par radicaux ssi le groupe de Galois de f est résoluble.*

On a vu en TD qu'il existe des polynômes de degré 5 dans $\mathbb{Q}[X]$ dont le groupe de Galois est S_5 et qui sont donc non résolubles par radicaux. Comme S_4 est résoluble tous ses sous-groupes le sont et le théorème 3.2 est donc un corollaire du théoème 3.3

Avant de commencer la preuve, voici quelques propositions qui nous seront utiles.

Proposition 3.4 *Soit D_n un corps de décomposition de $X^n - 1 \in \mathbb{Q}[X]$. L'extension $D_n/\mathbb{Q}$ est abelienne, plus précisément* $\mathrm{Gal}(D_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Preuve : Comme $X^n - 1$ est à racines simple l'extension est galoisienne. Soit ζ une racine primitive n-ieme. Clairement $D_n = \mathbb{Q}(\zeta)$. Le polynôme minimal de ζ est $\prod_{1 \leq k \leq n | k \wedge n = 1}(X - \zeta^k)$ (cf TD). On a donc $[D_n : \mathbb{Q}] = \varphi(n)$ (indicatrice d'Euler). Le morphisme de groupes (vu plus haut) :

$$\begin{aligned} \mathrm{Gal}(D_n/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto i \ (\text{tq } \sigma(\zeta) = \zeta^i) \end{aligned}$$

est clairement injectif et donc bijectif pour des raisons de cardinal.□

Lemme 3.5 *Soit p un nombre premier et K un corps ($car(K) = 0$) contenant les racines p-ieme de 1. Soit $a \in K$ tel que le polynôme $f = X^p - a$ n'a pas de racines dans K. Alors le groupe de Galois de f est cyclique d'ordre p.*

Preuve On a vu en TD que f est irreductible. Comme K contient les racines p-ieme de 1 il est clair que le corps de décomposition de f est égal à son corps de rupture. Il est donc de degré p et son groupe de Galois est cyclique car d'ordre premier.□

Lemme 3.6 *Si M est une extension radicale de K (ie de la forme décrite dans la définition 3.1) alors il existe une extension N/M telle que N/M et N/K soient radicales et galoisiennes.*

Preuve : On est toujours en caracteristique nulle. On doit juste trouver une extension normale. On part de la suite

$$K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_m) = M,$$

telle que pour tout $1 \leq i \leq m$ il existe $n_i \in \mathbb{N}$, $\alpha_i \in K_i$ tels que $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$.

Soit f_i le polynôme minimal de α_i sur K et $f = f_1 \cdots f_m$. Soit N un corps de décomposition de f sur M. On remarque N est aussi un corps de décomposition sur K (vu que M est engendré par des racines de f). Les extensions N/M et N/K sont donc galoisiennes.

Remarquons que $\mathrm{Gal}(N/K) = \{\tau_1 = \mathrm{id}, \ldots, \tau_\ell\}$ agit transitivement sur les racines de chaque f_i (cf. preuve Théorème 2.2). Ainsi toutes les racines de f sont de la forme $\tau_i(\alpha_j)$. En mettant ces éléments dans le bon ordre on voit que N/K est bien radicale :

$$\begin{array}{c} K = L_0 \subset L_0(\tau_1(\alpha_1)) \subset L_0(\tau_1(\alpha_1), \tau_1(\alpha_2)) \cdots \subset L_0(\tau_1(\alpha_1), \tau_1(\alpha_2), \ldots \tau_1(\alpha_m)) = \\ M = L_1 \subset L_1(\tau_2(\alpha_1)) \subset L_1(\tau_2(\alpha_1), \tau_2(\alpha_2)) \cdots \subset L_1(\tau_2(\alpha_1), \tau_2(\alpha_2), \ldots \tau_2(\alpha_m)) = \\ \vdots \\ L_{\ell-1} \subset L_{\ell-1}(\tau_\ell(\alpha_1)) \subset L_{\ell-1}(\tau_\ell(\alpha_1), \tau_\ell(\alpha_2)) \cdots \subset L_{\ell-1}(\tau_\ell(\alpha_1), \tau_\ell(\alpha_2), \ldots \tau_\ell(\alpha_m)) = N \end{array}$$

Pour conclure, on remarque que

$$\tau_i(\alpha_j)^{n_j} = \tau_i(\alpha_j^{n_j}) \in \tau_i(K(\alpha_1, \ldots, \alpha_{j-1})) = K(\tau_i(\alpha_1), \ldots, \tau_i(\alpha_{j-1})) \subset L_{i-1}(\tau_i(\alpha_1), \ldots, \tau_i(\alpha_{j-1}))$$

ce qui montre bien que N/K est radicale. □

On peut maintenant montrer un sens du théorème de Galois ! !

Preuve ($\Rightarrow$)

On suppose $f \in K[X]$ résoluble par radicaux, ie il existe une extension radicale $M = K(\alpha_1, \ldots, \alpha_m)$ qui contient un corps de décomposition L de f. D'après le lemme 3.6, on peut supposer M/K galoisienne. Quitte à rajouter des extensions intermédiaires on peut supposer aussi que les n_i sont des nombres premiers. Soit n le produits de tous les n_i et ξ une racine primitive n-ieme de 1.

L'extension $L(\xi)/K$ est galoisienne vu que $L(\xi)$ est le corps de décomposition de $(X^n - 1)f(X)$. De même l'extension $M(\xi)/K$ est galoisienne. Le groupe de Galois de $L(\xi)/K$ est donc un quotient de celui de $M(\xi)/K$. Il suffit donc de montrer que $\mathrm{Gal}(M(\xi)/K)$ est résoluble (tout quotient d'un groupe résoluble est résoluble).

On regarde maintenant la tour d'extensions : $K \subset K(\xi) \subset K(\xi, \alpha_1) \subset \cdots \subset K(\xi, \alpha_1, \ldots, \alpha_m) = M(\xi)$. On note H_i le groupe $\mathrm{Gal}(M(\xi)/K(\xi, \alpha_1, \ldots, \alpha_i)$ (celui donné par le théorème de correspondance 2.5) et H celui de $N(\xi)/K$. D'après la proposition 3.4, l'extension $K(\xi)/K$ est abélienne et donc, par le théorème de correspondance, le groupe H_0 est distingué dans H et H/H_0, étant isomorphe au groupe de Galois de $K(\xi)/K$, est abelien.

Pour tout $i > 1$, le lemme 3.5 affirme que l'extension $K(\xi, \alpha_1, \ldots, \alpha_i)/K(\xi, \alpha_1, \ldots, \alpha_{i-1})$ est cyclique. En appliquant le théorème de correspondance à $M(\xi)/K(\xi, \alpha_1, \ldots, \alpha_i)/K(\xi, \alpha_1, \ldots, \alpha_{i-1})$, on obtient $H_i \triangleleft H_{i-1}$ et H_i/H_{i-1} est cyclique.

En fin de compte on a une suite de sous-groupes

$$\{1\} = H_\ell \leq H_{\ell-1} \leq \cdots \leq H_0 \leq H = \mathrm{Gal}(M(\xi)/K),$$

telle que $H_i \triangleleft H_{i-1}$, $H_0 \triangleleft H$, les H_i/H_{i-1} et H/H_0 sont abeliens. Le groupe H est donc résoluble. □

Pour montrer la réciproque on a besoin d'une proposition supplémentaire.

Proposition 3.7 *Soit L/K est une extension abélienne de degré n. Si K contient les racines n-ieme de l'unité alors il existe une base du K-espace vectoriel L constitué d'éléments radicaux sur K (ie dont une certaine puissance est dans K).*

Preuve On note $G = \{\sigma_1, \ldots, \sigma_n\}$ le groupe de Galois de G/K. On fait de l'algèbre linéaire, ie on voit les éléments comme des isomorphismes du K-espace vectoriel L. Tout élément de G est d'ordre n (Lagrange) autrement dit tout élément de G est annulé par $X^n - 1$. Ce polynôme est scindé (K contient les racines n-ieme de 1) et à racines simples (on est toujours en caractéristique nulle) donc tout élément de G est diagonalisable et ses valeurs propres sont des racines n-ieme de 1. Comme G est abélien les élements de G sont simultanément diagonalisables [2], autrement dit il existe une base $(v_1, \ldots, v_n)$ du K-espace vectoriel L telle que

$$\forall\, 1 \leq i, j \leq n, \exists \lambda_{i,j} \in K, \sigma_i(v_j) = \lambda_{i,j} v_j.$$

2. montrez le !

Dès lors

$$\forall\, 1 \leq i, j \leq n, \sigma_i(v_j^n) = (\sigma_i(v_j))^n = (\lambda_{i,j} v_j)^n = v_j^n,$$

et donc $v_j^n \in L^G = K$ ie v_j est radical. $\square$

Fin de la preuve ($\Leftarrow$)

On part de $f \in K[X]$ ayant un corps de décomposition L tel que $\mathrm{Gal}(L/K)$ est résoluble.

On veut pouvoir appliquer la proposition 3.7 pour produire des éléments radicaux. On voit qu'il faut ajouter des racines de l'unité à L . Ce n'est pas un problème vu qu'il s'agit d'éléments radicaux, mais il faut s'assurer que le groupe de Galois reste résoluble.

On note n le degré de L sur K. Soit ξ une racine primitive n-ieme de 1. On a vu que l'extension $L(\xi)/K$ est galoisienne (c'est le corps de décomposition d'un polynôme) il en est de même de $L(\xi)/K(\xi)$. On considère le morphisme suivant (bien défini d'après la prop. 0.2 chap 4) :

$$\begin{aligned} \mathrm{Gal}(L(\xi)/K(\xi)) &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

Il est clairement injectif. Par conséquent $\mathrm{Gal}(L(\xi)/K(\xi))$ est isomorphe à un sous-groupe de $\mathrm{Gal}(L/K)$, il est donc lui aussi résoluble et son ordre divise n. Il existe donc des sous-groupes

$$\{\mathrm{id}\} = H_k \lhd H_{k-1} \lhd \cdots \lhd H_0 = \mathrm{Gal}(L(\xi)/K(\xi))$$

tels que les H_i/H_{i+1} sont abéliens. D'après le théorème de correspondance 2.5, $H_i \lhd H_{i+1}$ implique que l'extension $L^{H_{i+1}}/L^{H_i}$ est galoisienne de groupe de Galois H_i/H_{i+1} qui est abélien d'ordre n_i un diviseur de n. Comme L^{H_i} contient ξ il contient les racines n_i-ieme de 1. Les hypothèses de la proposition 3.7 sont donc satisfaites, il existe donc $\alpha_{i+1,1}, \ldots, \alpha_{i+1,\ell_{i+1}} \in L^{H_{i+1}}$ tels que $L^{H_i}(\alpha_{i+1,1}, \ldots, \alpha_{i+1,\ell_{i+1}}) = L^{H_{i+1}}$ et $\alpha_{i+1,j}^{n_i} \in L^{H_i}$ pour tout $1 \leq j \leq \ell_{i+1}$. On voit donc que l'extension $L(\xi)/K$ est radicale et contient L, autrement dit l'équation $f(x) = 0$ est résoluble par radicaux. $\square$