Théorie de Galois

Marc SAGE

Table des matières

1 Introduction

1.1 Prolongements d'isomorphismes aux corps de décomposition

Définition.
Soit K un corps, $P \in K[X]$.
Un corps de décomposition *de P est une extension L de K telle que*

$$\begin{cases} P \text{ est scindé sur } L \\ L \text{ engendré par les racines de } P \end{cases}.$$

Proposition (rappel).
Un corps de décomposition existe toujours, et est unique à isomorphisme près.

Proposition (prolongement d'isomorphismes aux corps de décomposition).
Soit $\sigma : K_1 \longrightarrow K_2$ un isomorphisme de corps. Soit $P_1 \in K_1[X]$, et $P_2 \in K_2[X]$ le polynôme obtenu via σ, et $\begin{cases} L_1 \text{ le corps de décomposition de } P_1 \text{ sur } K_1 \\ L_2 \text{ le corps de décomposition de } P_2 \text{ sur } K_2 \end{cases}$. Alors il existe un isomorphisme $\widetilde{\sigma} : L_1 \longrightarrow L_2$ qui prolonge σ :

$$\begin{array}{ccc} K_1 & \hookrightarrow & L_1 \\ \downarrow \sigma & & \downarrow \widetilde{\sigma} \\ K_2 & \hookrightarrow & L_2 \end{array},$$

le nombre ν de tels isomorphismes vérifie

$$\nu \leq [L_1 : K_1],$$

et si P_1 est scindé simple dans L_1, on a l'égalité

$$\nu = [L_1 : K_1].$$

Démonstration.
On fait alors une récurrence sur $d = [L_1 : K_1]$.

• Si $d = 1$, *i.e.* si $K_1 = L_1$, ce qui revient à dire que P_1 a toutes ses racines dans K_1, alors $\begin{cases} L_1 = K_1 \\ L_2 = K_2 \end{cases}$, et $\widetilde{\sigma}$ vaut nécessairement σ. On a alors bien $\nu = 1 = [L_1, K_1]$.

• Soit $d > 1$, et supposons la proposition vraie pour tous les extensions (de décomposition) de degré $< d$.
Si P_1 est scindé sur K_1, alors $L_1 = K_1$ et $d = 1$, *absurde*. P_1 peut donc s'écrire dans $K_1[X]$ comme

$$P_1 = Q_1 \Omega_1$$

où Q_1 est un facteur irréductible de P_1 sur K_1 de degré $2 \leq \deg Q_1 < \deg P_1$; notons Q_2 son image dans $K_2[X]$. Dans $L_1[X]$, on a alors

$$\begin{cases} P_1 = \Pi_{i=0}^{r}(X - \lambda_i) \\ Q_1 = \Pi_{i=0}^{s}(X - \lambda_i) \end{cases}, 1 \leq s \leq r,$$

et dans $L_2[X]$ on a

$$\begin{cases} P_2 = \Pi_{i=0}^{r}(X - \mu_i) \\ Q_2 = \Pi_{i=0}^{s}(X - \mu_i) \end{cases}, 1 \leq s \leq r.$$

Le point à remarquer est que tout prolongement $\widetilde{\sigma}$ de σ à L_1 envoie les racines de Q_1 sur celles de Q_2. En effet, on a

$$\Pi_{i=0}^{s}(X - \mu_i) = Q_2 = \sigma(Q_1) = \widetilde{\sigma}(Q_1) = \widetilde{\sigma}(\Pi_{i=0}^{s}(X - \lambda_i)) = \Pi_{i=0}^{s}\widetilde{\sigma}(X - \lambda_i) = \Pi_{i=0}^{s}(X - \widetilde{\sigma}(\lambda_i)),$$

donc nécessairement $\widetilde{\sigma}(\lambda_0)$ est un μ_i où $0 \leq i \leq s$.

Soit donc

$$K_1' = K_1[\lambda_0] \hookrightarrow K_1[\lambda_0, ..., \lambda_r] = L_1,$$

avec $[K_1' : K_1] = \deg \lambda_0$; or Q_1 est un polynôme irréductible sur K_1 qui annule λ_0, donc Q_1 est le polynôme minimal de λ_0 sur K_1. On en déduit $\deg \lambda_0 = \deg Q_1$, d'où

$$[K_1' : K_1] = \deg Q_1 > 1.$$

Pour chaque racine **distincte** μ_i de Q_2, on définit un morphisme

$$\sigma_i : \left\{ \begin{array}{ccc} K_1' = K_1[\lambda_0] & \longrightarrow & L_2 \\ x \in K_1 & \longmapsto & \sigma(x) \\ \lambda_0 & \longmapsto & \mu_i \end{array} \right.$$

par

$$\sigma_i : \left\{ \begin{array}{ccc} K_1' & \longrightarrow & L_2 \\ \sum a_n \lambda_0^n & \longmapsto & \sum \sigma(a_n) \mu_i^n \end{array} \right.$$

(remarquer au passage que σ_i prolonge σ). Soit alors

$$K_2' = \sigma_i(K_1') = \sigma_i(K_1[\lambda_0]) = K_2[\sigma_i(\lambda_0)] = K_2(\mu_i) \hookrightarrow L_2.$$

Résumons la situation :

$$\begin{array}{ccccc} K_1 & \hookrightarrow & K_1' = K_1[\lambda_0] & \hookrightarrow & L_1 = K_1[\lambda_0, ..., \lambda_r] \\ \downarrow \sigma & & \downarrow \sigma_i & & \\ K_2 & \hookrightarrow & K_2' = K_2[\mu_i] & \hookrightarrow & L_2 = K_2[\mu_0, ..., \mu_r] \end{array}.$$

On va appliquer l'hypothèse de récurrence au morphisme $\sigma_i : K_1' \longrightarrow K_2'$ et au polynôme P_1. Il convient de vérifier les hypothèses.

P_1 est scindé sur L_1, et l'engendré de ses racines sur K_1' vaut

$$K_1'[\lambda_0, ..., \lambda_r] = K_1[\lambda_0][\lambda_0, ..., \lambda_r] = K_1[\lambda_0, \lambda_0, ..., \lambda_r] = K_1[\lambda_0, \lambda_1, ..., \lambda_r] = L_1,$$

donc L_1 est bien un corps de décomposition de P_1 sur K_1'. De même, P_2 est scindé sur L_2 et

$$K_2'[\mu_0, ..., \mu_r] = K_2[\mu_i][\mu_0, ..., \mu_r] = K_2[\mu_0, ..., \mu_r] = L_2,$$

donc L_2 est bien un corps de décomposition de P_2 sur K_2'. D'autre part, le degré de l'extension L_1 sur K_1' vaut

$$[L_1 : K_1'] = \frac{[L_1 : K_1]}{[K_1' : K_1]} = \frac{[L_1 : K_1]}{\deg Q_1} < [L_1 : K_1].$$

On peut donc récurrer : il existe un morphisme $\widetilde{\sigma}_i : L_1 \longrightarrow L_2$ qui prolonge σ_i, donc qui prolonge σ :

$$\begin{array}{ccccc} K_1 & \hookrightarrow & K_1' = K_1[\lambda_0] & \hookrightarrow & L_1 = K_1[\lambda_0, ..., \lambda_r] \\ \downarrow \sigma & & \downarrow \sigma_i & & \downarrow \widetilde{\sigma}_i \\ K_2 & \hookrightarrow & K_1' = K_2[\mu_i] & \hookrightarrow & L_2 = K_2[\mu_0, ..., \mu_r] \end{array},$$

et leur nombre ν_i est au plus égal $[L_1 : K_1']$.

Pour l'inégalité : si $\widetilde{\sigma} : L_1 \longrightarrow L_2$ est un prolongement de σ, alors $\widetilde{\sigma}(\lambda_0)$ est nécessairement un μ_i, donc $\widetilde{\sigma}_{|K_1'}$ est nécessairement un σ_i. Par conséquent, en notant

$$N = \#\{\mu_1, ..., \mu_s\} \leq \deg Q_2,$$

i.e. le nombre de racines **distinctes** de Q_2, on a N choix pour σ_i (qui correspondent bien à des morphismes distincts, car $\left\{ \begin{array}{c} \sigma_i(\lambda_0) = \mu_i \\ \sigma_j(\lambda_0) = \mu_j \end{array} \right.$ sont distincts pour $i \neq j$). Par ailleurs, l'hypothèse de récurrence nous fournit au plus $[L_1 : K_1']$ choix pour $\widetilde{\sigma}_i$ à i fixé. On a finalement au plus

$$N \times [L_1 : K_1'] = N \frac{[L_1 : K_1]}{\deg Q_1} \leq \frac{\deg Q_2}{\deg Q_1} [L_1 : K_1] = [L_1 : K_1]$$

choix pour $\widetilde{\sigma}$.

Enfin, si P_1 est scindé simple dans L_1, on a égalité partout. En effet, Q_1 est alors scindé simple, donc on a $N = \deg Q_1$ choix pour i ; comme de plus P_1 est scindé simple sur K_1', on a par hypothèse de récurrence $[L_1 : K_1']$ choix pour.$\widetilde{\sigma}_i$.

1.2 Groupe de Galois

Définition.
Soit $K \subset L$ deux corps. On appelle K-automorphisme *de L tout automorphisme de L qui fixe K. On appelle* groupe de Galois *de L sur K l'ensemble des K-automorphismes de L. On le note*

$$\mathrm{Gal}\left({}^{L}\!/_{K}\right) = \{\sigma \in \mathrm{Aut}\, L \ ; \ \forall a \in K,\, \sigma(a) = a\}.$$

Propriété.
Si L est un corps de décomposition d'un polynome P de $K[X]$, alors

$$\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| \leq [L : K],$$

et si P est scindé simple sur L, il y a égalité.

Démonstration.
Puisqu'un K-automorphisme de L est un prolongement à L de l'identité sur K, on applique la proposition précédente à $K_1 = K_2 = K$ et $\sigma = \mathrm{Id}$.

1.3 Morphisme de Frobenius

Définition.
Soit K un corps de caractéristique p. On appelle morphisme de Frobenius *le morphisme de corps :*

$$\mathrm{Fr} : \left\{ \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^p \end{array} \right. .$$

On note son image

$$K^p = \{x^p \text{ où } x \text{ décrit } K\}.$$

Fr est bien un morphisme additif, étant donné que pour $i \wedge p = n$,

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1} = pi^{-1}\binom{p-1}{i-1} \equiv 0 \ \ [p]$$

et donc que

$$\mathrm{Fr}(x+y) = (x+y)^p = x^p + \underbrace{\sum_{i=1}^{p-1}\binom{p}{i}x^i y^{n-i}}_{=0} + y^p = x^p + y^p.$$

1.4 Polynômes séparables

Définition.
Un polynôme de $K[X]$ est dit séparable *si toutes ses racines sont simples dans toute extension de K.*
Si $K \subset L$ est une extension algébrique, un élément x de L est dit séparable *si son polynôme minimum est séparable.*

Proposition (critère de séparabilité sans sortir du corps de base).
Un polynôme $P \in K[X]$ est séparable ssi il est premier avec sa dérivée :

$$P \text{ séparable} \iff P \wedge P' = 1.$$

Démonstration.

Si P n'est pas séparable, P a une racine double dans une extension L de K, donc $P \wedge P' \neq 1$ dans $L[X]$, a fortiori dans $K[X]$ puisque le pgcd est inchangé par extension de corps.

Réciproquement, si $P \wedge P' \neq 1$, alors P a une racine double dans un de ses corps de décomposition, donc n'est pas séparable.

Proposition (critère de séparabilité pour les polynôme irréductibles).
Soit $P \in K[X]$ irréductible. Alors P est séparable ssi $P' \neq 0$.

Démonstration.
Si P est irréductible sur $K[X]$ et n'est pas séparable, alors P et P' ont (dans une extension de K) un facteur en commun non constant, qui ne peut être que P vu que P est irréductible, d'où $P \mid P'$, ce qui implique $P' = 0$ en prenant les degrés.

Réciproquement, $P' = 0 \implies P \mid P' \implies P \wedge P' = P \neq 1 \implies P$ non scindé simple dans une clôture algébrique de K.

Proposition (factorisation de $X^p - a$).
Soit K de caractéristique $p > 0$, et $a \in K$.
• *Si $a \in K^p$, alors $X^p - a$ se scinde en*

$$X^p - a = \left(X - \sqrt[p]{a}\right)^p.$$

• *Si $a \notin K^p$, alors $X^p - a$ est irréductible.*

Démonstration.
• Évident car on est en caractéristique p.
• Montrons la contraposée. Si $P = X^p - a$ n'est pas irréductible, soit Q un facteur irreductible de P, de sorte que

$$X^p - a = QR$$

avec $1 \leq \deg Q < p$. Soit b une racine de Q dans une extension appropriée de K. Alors

$$0 = QR(b) = P(b) = b^p - a,$$

d'où

$$X^p - a = X^p - b^p = (X - b)^p,$$

donc $Q \mid (X-b)^p$, *i.e.* $Q = (X-b)^r$ pour un $1 \leq r < p$. Puisque $Q \in K[X]$, son terme constant b^r est dans K ; or p est premier, donc Bezout donne $ur + vp = 1$, d'où

$$b = (b^r)^u (b^p)^v \in K \implies a = b^p \in K^p.$$

Corollaire.
Dans $K = \mathbb{F}_p(T)$, le polynôme $P = X^p - T \in K[X]$ n'est pas séparable.

Démonstration.
Montrons déjà que P est irréductible sur $K = \mathbb{F}_p(T)$. D'après la proposition précédente, il suffit pour cela de montrer que $T \in K$ n'est pas une puissance de p dans K. Si c'était le cas, on aurait $T = \left(\frac{A}{B}\right)^p$ avec

$$\begin{cases} A = \sum_i a_i T^i \neq 0 \\ B = \sum_i b_i T^i \end{cases},$$

d'où $\begin{cases} A^p = \sum_i a_i^p T^{pi} \\ B^p = \sum_i b_i^p T^{pi} \end{cases}$ et

$$\sum_i a_i^p T^{pi} = A^p = TB^p = T \sum_i b_i^p T^{pi} = \sum_i b_i^p T^{pi+1},$$

absurde car $p \geq 2$.

Il reste à voir que $P' = 0$, donc, d'après la dernière proposition, P ne peut être séparable.

1.5 Corps parfaits

Définition.
Un corps K est dit parfait *si tout polynôme irréductible de $K[X]$ est séparable.*

Proposition (critère de perfection).
• *Si* $\operatorname{car} K = 0$*, alors K est parfait.*
• *Si* $\operatorname{car} K = p > 0$*, alors K est parfait ssi $K^p = K$,* i.e. *ssi* Fr *est surjectif.*

Demonstration.
• Si $\operatorname{car} K = 0$, alors tout polynôme irréductible y est de degré au moins égal à 1, donc de dérivée non nulle, donc séparable.
• Si $K^p \subsetneq K$, soit $a \in K \setminus K^p$. Le polynôme $X^p - a$ est alors irréductible (car $a \notin K^p$) et de dérivée nulle, donc n'est pas séparable et K ne peut être parfait.

Si $K^p = K$, soit $P \in K[X]$ irréductible. Si P n'était pas séparable, sa dérivée serait nulle. En posant $P = \sum_{k\geq 0} a_k X^k$, on aurait

$$0 = P' = \sum_{k=1}^{n} a_k k X^{k-1},$$

d'où $a_k k = 0$ pour tout k et $a_k = 0$ pour $k \wedge p = 1$.On en déduirait

$$P = \sum_{j\geq 0} a_{pj} X^{jp} = \sum_{j\geq 0} \sqrt[p]{a_{pj}}^{p} X^{jp} = \left(\sum_{j\geq 0} \sqrt[p]{a_{pj}} X^{j} \right)^{p}$$

où l'un des a_{pj} est non nul (sinon $P = 0$), *absurde* car P irréductible.

1.6 Corps finis

1.6.1 Rappels

Soit K un corps fini. Le morphisme $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ n & \longmapsto & n \cdot 1_K \end{array} \right.$ ne saurait être injectif, donc son noyau est du type $a\mathbb{Z}$ avec $a \neq 0$. Alors a est nécessairement premier, puisque pour toute décomposition $a = bc$ on a

$$0 = a \cdot 1_K = bc \cdot 1_K = (b \cdot 1_K)(c \cdot 1_K)$$

d'où $b \cdot 1_K = 0$ (ou $c \cdot 1_K$) par intégrité de K, *i.e.* $b \in a\mathbb{Z}$, ou encore $a \mid b$.
On note alors $a = p$ (comme **p**remier). p est appelée *caractéristique* de K, et est notée

$$\operatorname{car} K = p.$$

D'autre part, K contient les p itérés de 1_K, *i.e.* le corps $\mathbb{F}_p = \{0, 1, ..., p-1\}$ vu dans K (on appelle cette copie de $\mathbb{F}_p$ le *sous-corps premier* de K) Ainsi,

$$\operatorname{car} K = p > 0 \implies \mathbb{F}_p \hookrightarrow K.$$

On peut alors considérer K comme un $\mathbb{F}_p$-espace vectoriel de dimension finie n, d'où $|K| = p^n$.

Proposition (rappel).
Soit p premier. Pour tout $n \geq 1$, il existe (à isomorphisme près) un unique corps fini de cardinal $q = p^n$: c'est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$, et on le note $\mathbb{F}_q$. On a de plus $\mathbb{F}_p \hookrightarrow \mathbb{F}_q$.

Proposition (rappel).
$\mathbb{F}_q^*$ *est cyclique.*

1.6.2 Cyclicité de $\mathrm{Gal}\left(\mathbb{F}_q \diagup \mathbb{F}_p\right)$

Proposition.
$\mathrm{Gal}\left(\mathbb{F}_q \diagup \mathbb{F}_p\right)$ *est cyclique et engendré par* Fr :

$$\mathrm{Gal}\left(\mathbb{F}_q \diagup \mathbb{F}_p\right) = \langle \mathrm{Fr} \rangle .$$

Démonstration.
Soit a engendrant $\mathbb{F}_q^*$, de sorte que $\mathbb{F}_q = \mathbb{F}_p[a]$. Les élément σ de $G = \mathrm{Gal}\left(\mathbb{F}_q \diagup \mathbb{F}_p\right)$ sont entièrement déterminés par les $\sigma(a)$, donc

$$|G| \leq \#\{\sigma(a) \text{ où } \sigma \text{ décrit } G\}.$$

En considèrant le polynôme minimal P de a sur $\mathbb{F}_p$, avec $\deg P = [\mathbb{F}_q : \mathbb{F}_p] = n$, on remarque que les $\sigma(a)$ sont des racines de P car $P \in \mathbb{F}_p$ et σ fixe $\mathbb{F}_p$:

$$P(\sigma(a)) = \sum_k \lambda_k (\sigma(a))^k = \sum_k \sigma(\lambda_k)\sigma\left(a^k\right) = \sum_k \sigma\left(\lambda_k a^k\right) = \sigma\left(\sum_k \lambda_k a^k\right) = \sigma(P(a)) = \sigma(0) = 0.$$

Il y a donc au plus n possibilités pour $\sigma(a)$, d'où $|G| \leq n$.

Pour montrer que Fr engendre G, il suffit de montrer que son ordre ω dans G est $\geq n$. Pour cela, on remarque que $\forall x \in \mathbb{F}_q$, $x = \mathrm{Id}(x) = \mathrm{Fr}^\omega(x) = x^{p^\omega}$, donc le polynôme $X^{p^\omega} - X$ s'annule sur $\mathbb{F}_q$ tout entier, donc est de degré $p^\omega \geq q = p^n$, d'où $\omega \geq n$, *CQFD.*

1.6.3 Extensions intermédiaires

Lemme 0.
Soient a et b des entiers ≥ 1 et p un entier ≥ 2. Alors

$$\begin{cases} (p^a - 1) \wedge \left(p^b - 1\right) = p^{a \wedge b} - 1 \\ (X^a - 1) \wedge \left(X^b - 1\right) = X^{a \wedge b} - 1 \end{cases} .$$

Démonstration.
Clair si $a = b$. On suppose alors $a > b$. On effectue la division euclidienne de a par b : $a = bq + r$. On écrit alors

$$p^a - 1 = p^{bq}p^r - 1 = p^{bq}p^r - p^r + p^r - 1 = p^r\left(p^{bq} - 1\right) + (p^r - 1) = p^r A\left(p^b - 1\right) + (p^r - 1)$$

(où A est entier), ce qui montre que le reste de la division euclidienne de $p^a - 1$ par $p^b - 1$ est $p^r - 1$. Les termes successifs de l'algorithme d'Euclide "passent" donc à la puissance p, et en réitérant le procédé, on trouve que le dernier reste non nul est bien $p^{a \wedge b} - 1$.

La démonstration est identique pour les polynômes, vu que l'on dispose d'une division euclidienne polynomiale.

Lemme.
Les trois énoncés suivants sont équivalents :

$$\begin{array}{rcl} X^{p^m} - X & | & X^{p^n} - X \\ p^m - 1 & | & p^n - 1 \\ m & | & n. \end{array}$$

Démonstration.

Par équivalences, et en utilisant le lemme 0, on a

$$\begin{aligned}
& X^{p^m} - X \mid X^{p^n} - X \\
\iff\quad & X^{p^m-1} - 1 \mid X^{p^n-1} - 1 \\
\iff\quad & \left(X^{p^m-1} - 1\right) \wedge \left(X^{p^n-1} - 1\right) = X^{p^m-1} - 1 \\
\iff\quad & X^{p^{n\wedge m}-1} - 1 = X^{p^m-1} - 1 \\
\iff\quad & n \wedge m = m \\
\iff\quad & m \mid n,
\end{aligned}$$

la même méthode marchant pour $p^m - 1 \mid p^n - 1$.

Proposition (extensions intermédiaires).
Les sous-corps de $\mathbb{F}_{p^n}$ sont exactement les $\mathbb{F}_{p^k}$ où $k \mid n$.
$\mathbb{F}_{p^k}$ peut être également vu comme le corps des racines de $X^{p^k} - X$ sur $\mathbb{F}_p$. On a alors les injections

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^n}.$$

Démonstration.
• Soit E une extension intermédiaire : $\mathbb{F}_p \hookrightarrow E \hookrightarrow \mathbb{F}_q$. E est fini, donc est un $\mathbb{F}_{q'}$ avec $q' = (p')^k$ et $k \geq 1$; E étant par ailleurs un sous-groupe additif de $\mathbb{F}_q$ son cardinal doit diviser le cardinal de $\mathbb{F}_q$, *i.e.* $(p')^k \mid p^n$, d'où $p' = p$ et $q' = p^k$. D'autre part, $\mathbb{F}_q$ peut être vu comme un $\mathbb{F}_{q'}$-espace vectoriel de dimension finie r, d'où $|\mathbb{F}_q| = |\mathbb{F}_{q'}|^r$,*i.e.* $p^n = p^{kr}$,ou encore $k \mid n$.
• Réciproquement, soit $k \mid n$ et considérons

$$E = \left\{\text{racines de } X^{p^k} - X \text{ dans } \mathbb{F}_q\right\}.$$

E^* est clairement un sous-groupe de $\mathbb{F}_q^*$, et est de plus stable par $+$: en effet, si x et y sont dans E, on a

$$(x+y)^{p^k} = \mathrm{Fr}^k(x+y) = \mathrm{Fr}^{k-1}\left(x^p + y^p\right) = \mathrm{Fr}^{k-2}\left(x^{p^2} + y^{p^2}\right) = ... = x^{p^k} + y^{p^k} = 0.$$

E est donc un corps pour les lois induites, *i.e.* un sous-corps de $\mathbb{F}_q$. Comme de plus $k \mid n$, on a (par le lemme)

$$X^{p^k} - X \mid X^{p^n} - X = \prod_{a \in \mathbb{F}_q} (X - a)$$

scindé simple, donc $X^{p^k} - X$ a exactement p^k racines, d'où $|E| = p^k$. On a ainsi construit un sous-corps de $\mathbb{F}_q$ de cardinal p^k, qui est donc isomorphe à $\mathbb{F}_k$, *CFQD.*

Corollaire (correspondance de Galois).
On a une correspondance bijective entre les sous-groupes de $G = \mathrm{Gal}\left(\mathbb{F}_q \diagup \mathbb{F}_p\right)$ et les extensions intermédiaires $\mathbb{F}_p \subset \mathbb{F}_{p^k} \subset \mathbb{F}_q$, qui à un sous-groupe H associe le sous-corps $\mathbb{F}_q^H$ des éléments de $\mathbb{F}_q$ stables par H.

Démonstration.
Le point central est de remarquer que si $k \mid n$, alors $\mathbb{F}_{p^k} = \mathbb{F}_q^{\left\langle \mathrm{Fr}^k \right\rangle}$. En effet, les racines du polynôme $X^{p^k} - X$ de $\mathbb{F}_q[X]$ sont exactement les éléments de $\mathbb{F}_q$ stables par Fr^k, *i.e.* par $\left\langle \mathrm{Fr}^k \right\rangle$, donc $\mathbb{F}_q^{\left\langle \mathrm{Fr}^k \right\rangle}$ est l'ensemble $\mathbb{F}_{p^k}$ de ces telles racines.
• Soit H un sous-groupe de G, et $E = \mathbb{F}_q^H$. Puisque G est engendré par Fr, H est de la forme $\left\langle \mathrm{Fr}^k \right\rangle$ où $k \mid n$ (pour $H = \{\mathrm{Id}\}$, prendre $k = n$). Donc $E = \mathbb{F}_q^{\left\langle \mathrm{Fr}^k \right\rangle} = \mathbb{F}_{p^k}$, qui est bien une extension intermédiaire d'après la proposition précédente.
• La correspondance établie est injective : si $\begin{cases} H = \left\langle \mathrm{Fr}^k \right\rangle \\ H' = \left\langle \mathrm{Fr}^{k'} \right\rangle \end{cases}$ sont deux sous-groupes de G tels que $\mathbb{F}_q^H = \mathbb{F}_q^{H'}$, alors les polynômes $X^{p^k} - X$ et $X^{p^{k'}} - X$ ont même ensemble de racines, *i.e.* $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k'}}$, d'où $k = k'$ et $H = H'$.
• Elle est en outre surjective : si E est une extension intermédiaire, E est un $\mathbb{F}_{p^k}$ d'après la proposition précédente, donc un $\mathbb{F}_q^{\left\langle \mathrm{Fr}^k \right\rangle}$ où $\left\langle \mathrm{Fr}^k \right\rangle$ est un sous-groupe de G.

1.7 Clôture algébrique de $\mathbb{F}_q$

Définition.
Soit $(K_n)_{n\in\mathbb{N}}$ une suite croissante de corps, au sens où $\forall n \leq m$, il existe un morphisme $\iota_{n\to m} : K_n \hookrightarrow K_m$.
On appelle limite inductive *de la suite (K_n) le corps $K = \bigcup_{n\in\mathbb{N}} K_n$ formé de la réunion "croissante" des K_n, dont les lois $*$ entre deux éléments sont définis par :*

$$\text{si } \begin{cases} a \in K_n \\ b \in K_{m\geq n} \end{cases} \text{, alors } a * b = \iota_{n\to m}(a) * b.$$

Proposition.
Soit p premier, $q = p^k$ où $k \geq 1$. La limite inductive des $\mathbb{F}_{p^{n!}}$ est une clôture algébrique de $\mathbb{F}_q$.

Démonstration.
Posons $\Omega = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$.
• Pour $x \in \Omega$, mettons $x \in \mathbb{F}_{p^{n!}}$, x est annulé par le polynôme $X^{p^{n!}} - X$ de $\mathbb{F}_q$, donc est algébrique sur $\mathbb{F}_q$.
• Soit par ailleurs P un polynôme de $\Omega[X]$. Les coefficients de P sont en nombre fini, donc sont tous dans un même $\mathbb{F}_{p^{n!}}$.
On considère alors D un corps de décomposition de P sur $\mathbb{F}_{p^{n!}}$, mettons $D = \mathbb{F}_{p^{n!}}[\xi_1, .., \xi_r]$ où $\xi_1, .., \xi_r$ sont les racines de P dans D. Alors les éléments de D sont les polynômes en les $\xi_1, .., \xi_r$ dont le degré total est majoré par $(\deg P)^r$ (le degré de chaque puissance d'un ξ_i pouvant être majoré par $\deg P$), à coefficients dans un corps fini, donc sont en nombre fini. Par conséquent, D est un $\mathbb{F}_{(p')^{k'}}$, admettant $\mathbb{F}_{p^{n!}}$ comme sous-corps, donc D est un $\mathbb{F}_{p^m}$ où $n! \mid m$. On a alors les extensions

$$\mathbb{F}_{p^{n!}} \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^{m!}},$$

donc D est contenu dans $\mathbb{F}_{p^{m!}} \subset \Omega$. Par conséquent, P se scinde sur Ω.

1.8 Théorème de Lüroth

Soit K un corps. On s'intéresse à $\mathrm{Gal}\left({}^{K(X)}\!/_{K}\right)$ ainsi qu'aux extensions intermédiaires

$$K \subset E \subset K(X).$$

Lemme.
Soit $u \in K(X)\setminus K$, mettons $u = \frac{P}{Q}$ où $P \wedge Q = 1$. Alors :
• *u est transcendant sur K ;*
• *L'extension $K(u) \subset K(X)$ est algébrique finie, de degré $\delta(u) := \max(\deg P, \deg Q)$;*
• *Le polynôme minimal de X sur $K(u)$ est le normalisé de $P(T) - uQ(T) \in K(u)[T]$.*

Démonstration.
Soit $R(T) = P(T) - uQ(T) \in K(X)[T]$. On a $R(X) = 0$, donc X est algébrique sur $K(u)$ de degré $\leq \deg R \leq \delta(u)$, donc $K(X)$ est une extension algébrique finie de $K(u)$. Nécessairement, u ne peut être algébrique sur K, car alors X le serait (pas possible).
On peut considérer $R(T) = P(T) - uQ(T)$ comme un polynôme en u de degré 1, irréductible car $P \wedge Q = 1$, donc irréductible dans $K[u][T]$, a fortiori dans $K(u)[T]$
Donc R est le polynôme minimal de X.

Théorème.
Les K-automorphismes de $K(X)$ sont donnés par les $\varphi : X \longmapsto \frac{aX+b}{cX+d}$ où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$. On a de plus

$$\mathrm{Gal}\left({}^{K(X)}\!/_{K}\right) \simeq PGL_2(K).$$

Démonstration.
Soit φ un K-automorphisme de $K(X)$. Puisque X génère $K(X)$, la donnée de $u=\varphi(X)$ détermine entièrement φ. De plus, φ est surjective, donc $K(u)=\operatorname{Im}\varphi=K(X)$; en particulier $u\notin K$, et le lemme s'applique :

$$\delta(u)=[K(X):K(u)]=[K(X):K(X)]=1.$$

On en déduit la forme de u :

$$u=\frac{aX+b}{cX+d}$$

où a ou $c\neq 0$ et $ad-bc\neq 0$, *i.e.* $ad-bc\neq 0$, ou encore $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in GL_2(K)$. On considère ensuite le morphisme surjectif

$$\Phi:\left\{\begin{array}{ccc} GL_2(K) & \longrightarrow & \operatorname{Gal}\left({}^{K(X)}\!/_{K}\right)\\ \begin{pmatrix} a & b\\ c & d\end{pmatrix} & \longmapsto & X\longmapsto\frac{aX+b}{cX+d}\end{array}\right.,$$

dont le noyau est $K\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$, d'où

$$\operatorname{Gal}\left({}^{K(X)}\!/_{K}\right)\simeq {}^{GL_2(K)}\!/_{\operatorname{Ker}\Phi}=PGL_2(K).$$

Théorème de Lüroth (sous-corps de $K(X)$).
Les sous-corps de $K(X)$ sont monogènes, en cela que

$$K\subset E\subset K(X)\implies\exists u\in K(X)\ \textit{tel que}\ E=K(u).$$

Démonstration.
Si $E=K$, $u=1$ convient.
Si $K\subsetneq E$, soit $v\in E\setminus K$, d'où des extensions $K(v)\subset E\subset K(X)$. Le lemme nous dit alors que $K(X)$ est une extension algébrique de $K(v)$ de degré $\delta(v)$. A fortiori, X est algébrique sur E, et l'on dispose de son polynôme minimal sur $E[T]$

$$\mu=T^n+a_1T^{n-1}+...+a_n$$

où chaque $a_i\in E$. Puisque X n'est pas algébrique sur K, un des a_i n'habite pas chez K, mettons $a_{i_0}=\frac{P}{Q}\in E\setminus K$ où $P\wedge Q=1$, avec $d=\delta(a_{i_0})$. Nous allons montrer que $E=K(a_{i_0})$, ce qui concluera.
Le lemme nous donne des extension finies $K(a_{i_0})\subset E\subset K(X)$ avec

$$[E:K(a_{i_0})]=\frac{[K(X):K(a_{i_0})]}{[K(X):E]}=\frac{\delta(a_{i_0})}{n}=\frac{d}{n}.$$

Montrons que $d=n$, ce qui donnera $[E:K(a_{i_0})]=1$ et $E=K(a_{i_0})$ monogène comme voulu.
Le polynôme $P(T)-a_{i_0}Q(T)$ annule X et est à coefficients dans $K(a_{i_0})\subset E$, donc est un multiple de μ, mettons

$$P(T)-a_{i_0}Q(T)=\mu(T)\nu(T)$$

dans $K(X)[T]$, ce que l'on réécrit sous la forme

$$P(T)Q(X)-P(X)Q(T)=\mu(T)\nu(T)Q(X).$$

Par ailleurs, les $a_i\in E\subset K(X)$ s'écrivent $a_i=\frac{P_i(X)}{Q_i(X)}$, donc en multipliant μ par le ppcm des dénominateurs $\lambda=\bigvee_{i=1,...n}Q_i$, on retombe dans $K[X]$ (plutôt que dans $K(X)$), mettons

$$\lambda(X)\mu(T)=A_0(X)T^n+A_1(X)T^{n-1}+...+A_n(X),$$

et on a même les A_i premiers entre eux (on dit que le terme de droite est *primitif* en X).
Puisque $A_{i_0}(X)=\lambda(X)a_{i_0}=\lambda(X)\frac{P(X)}{Q(X)}$ avec $P\wedge Q=1$, on a $\left\{\begin{array}{l} P\mid A_{i_0}\\ Q\mid\lambda\end{array}\right.$. On en déduit une réécriture

$$\begin{aligned} P(T)Q(X)-P(X)Q(T) &= \lambda(X)\mu(T)\nu(T)\frac{Q(X)}{\lambda(X)}\\ &= \nu(T)\frac{Q(X)}{\lambda(X)}\left[A_0(X)T^n+A_1(X)T^{n-1}+...+A_n(X)\right].\end{aligned}$$

À gauche, le degré en X est $\leq \max\{\deg Q, \deg P\} = d$, à droite le degré en X est $\geq \deg A_{i_0} \geq d$ car $P \mid A_{i_0}$, donc le degré en X est d partout et par conséquent le terme $\frac{Q(X)}{\lambda(X)}$ est une constante $\alpha \in K$. Réécrivons encore une fois :

$$P(T)Q(X) - P(X)Q(T) = \alpha\nu(T)\left[A_0(X)T^n + A_1(X)T^{n-1} + ... + A_n(X)\right].$$

Le terme de droite est primitif en X, donc le terme de gauche aussi, et ce dernier étant symétrique (en X et T) il est aussi primitif en T, donc le terme de droite est primitif en T, ce qui impose $\nu(T)$ constante, disons $\nu(T) = \beta \in K$. On a finalement

$$P(T)Q(X) - P(X)Q(T) = \alpha\beta\left[A_0(X)T^n + A_1(X)T^{n-1} + ... + A_n(X)\right].$$

En prenant le degré en T, on obtient d à gauche et n à droite, d'où $d = n$ comme voulu.

2 Théorie de Galois

2.1 Étude préliminaires des K-morphismes

Soit K un corps, $K \subset L$ une extension **finie** (donc algébrique) et $\overline{K}$ une clôture algébrique de K. On dispose d'une inclusion canonique $\iota : K \hookrightarrow \overline{K}$ que l'on cherche à prolonger à L. On recherche donc les morphismes de L dans $\overline{K}$ qui fixent K, *i.e.* les K-morphismes de L dans $\overline{K}$, ensemble que l'on notera $\mathrm{Hom}_K\left(L, \overline{K}\right)$.

Noter que $\overline{K}$ n'a aucune raison de contenir L.

Le problème consiste donc à chercher les morphismes $\bar{\iota}$ faisant commuter le diagramme :

$$\begin{array}{ccc} K & \longrightarrow & L \\ & \iota \searrow & \downarrow \bar{\iota} \\ & & \overline{K} \end{array} .$$

2.1.1 Théorème d'existence

Théorème (existence de prolongements).
Soit $\iota : K \hookrightarrow \overline{K}$ un morphisme de corps – par exemple l'inclusion canonique – et $K \subset L$ une extension finie. Le nombre N de prolongements de ι à L vérifie

$$1 \leq N \leq [L : K] .$$

Démonstration.
On fait un récurrence sur $d = [L : K]$.
• Si $[L : K] = 1$, *i.e.* si $L = K$, alors ι est l'unique prolongement de ι.
• Si $[L : K] > 1$, on écrit

$$L = K[x_0, ..., x_r] = K[x_1, ..., x_r][x_0] = L'[x_0]$$

où $L' = K[x_1, ...x_r]$ et $r \geq 0$ est minimal, de sorte que $x_0 \notin L'$, donc $\deg_{L'} x_0 \geq 2$, d'où

$$[L' : K] < [L : K] .$$

Par récurrence, il existe un prolongement $\iota' : L' \longrightarrow K$, que l'on prolonge à L en posant

$$\overline{\iota'} : \left\{ \begin{array}{ccc} L = L'[x_0] & \longrightarrow & \overline{K} \\ \sum \lambda_n x_0^n & \longmapsto & \sum \iota'(\lambda_n) x_0^n \end{array} \right. ,$$

d'où l'existence d'un prolongement de ι à L.

Pour la majoration, on considére le diagramme

$$\begin{array}{ccccc} K & \hookrightarrow & L' & \hookrightarrow & L = L'[x_0] \\ & & & \searrow \sigma_{|L'} & \downarrow \sigma \\ & & & & \overline{K} \end{array}$$

afin de récurrer, ce qui amène naturellement l'application

$$\Phi : \left\{ \begin{array}{ccc} \{\text{prolongements à } L\} & \longrightarrow & \{\text{prolongements à } L'\} \\ \sigma & \longmapsto & \sigma_{|L'} \end{array} \right. .$$

Le cardinal de l'image est inférieur au nombre de prolongements à L', lequel est (par hypothèse de récurrence) $\leq [L' : K]$. On a par ailleurs au plus $\deg_{L'} x_0$ antécédents σ possibles à $\sigma_{|L'}$ fixé : en effet, deux antécédents d'un même prolongement σ' à L' ne peuvent être distingués que par l'image qu'ils ont de x_0 (puisqu'ils coïncident déjà sur L'), laquelle image doit être une racine du polynôme minimal P de x_0 sur L' (car $P(\sigma(x_0)) = \sigma(P(x_0)) = 0$).

Par conséquent, le nombre de prolongements à L vaut au plus

$$\deg_{L'} x_0 \times [L' : K] = [L'[x_0] : L'] \times [L' : K] = [L'[x_0] : K] = [L : K] .$$

Corollaire (existence de K-morphismes).
Le nombre $N = \left|\mathrm{Hom}_K\left(L, \overline{K}\right)\right|$ *de* K*-morphismes de* $L \longrightarrow \overline{K}$ *vérifie*

$$1 \leq N \leq [L : K]\,.$$

Démonstration.
On applique le théorème à l'inclusion canonique $\iota : K \hookrightarrow \overline{K}$, en remarquant que les K-morphismes de $L \longrightarrow \overline{K}$ sont exactement les prolongements de ι.

On s'intéresse maintenant au cas d'égalité $N = [L : K]$.

2.1.2 Extensions séparables

Définition.
Une extension ***finie*** $K \subset L$ *est dite* séparable *si le nombre* $N = \left|\mathrm{Hom}_K\left(L, \overline{K}\right)\right|$ *de* K*-morphismes de* $L \longrightarrow \overline{K}$ *vaut exactement*

$$N = [L : K]\,.$$

Proposition.
Soit $K \subset L$ *une extension* ***finie****. On a équivalence entre :*
• $K \subset L$ *est séparable.*
• $\forall x \in L$*,* x *est séparable.*
• L *s'écrit* $K[x_1, ..., x_n]$ *où les* x_i *sont séparables.*

Démonstration.
On récurre sur $d = [L : K]$.
• Pour $d = 1$, N vaut 1, tous les éléments λ de $L = K$ sont séparables car leurs polynômes minimaux $X - \lambda$ sont de degré 1 et on peut toujours écrire $L = K = K[1]$ où 1 séparable. Donc l'équivalence $(i) \iff (ii) \iff (iii)$ est vérifiée, les trois propriétés étant vraies.
• On suppose désormais $d > 1$.
$(i) \implies (ii)$ Par contraposée. Supposons qu'il y a un x_0 dans L dont le polynôme minimal P sur K ne soit pas séparable, on écrit

$$L = K[x_0, ..., x_r] = L'[x_0] \quad \text{où } L' = K[x_1, ...x_r]$$

et $r \geq 0$ est minimal, de sorte que $x_0 \in L \setminus L'$ est de degré ≥ 2 sur L'.

Puisque P n'est pas séparable, il admet au plus $\deg P - 1$ racines dans $\overline{K}$. Or, l'image de x_0 par un K-morphisme $\sigma : L \longrightarrow \overline{K}$ est une racine de P dans $\overline{K}$, donc ne peut prendre qu'au plus $\deg P - 1$ valeurs distinctes. En remarquant que $2 \leq \deg_{L'} x \leq \deg P = \deg_K x_0$, on en déduit au plus $\deg_{L'} x_0 - 1 \geq 1$ choix pour les antécédent par $\Phi : \left\{ \begin{array}{ccc} \mathrm{Hom}_K\left(L, \overline{K}\right) & \longrightarrow & \mathrm{Hom}_K\left(L', \overline{K}\right) \\ \sigma & \longmapsto & \sigma_{|L'} \end{array} \right.$ d'un $\Phi(\sigma)$ donné.

Ainsi, le nombre de K-morphismes de $L \longrightarrow \overline{K}$ vaut au plus

$$(\deg_{L'} x_0 - 1) \times [L' : K] < \deg_{L'} x_0 \times [L' : K] = [L'[x_0] : L'] \times [L' : K] = [L : K]\,,$$

d'où $N < [L : K]$.
$(ii) \implies (iii)$ Trivial vu que L est finie sur K.
$(iii) \implies (i)$ Supposons que $L = K[x_0, ..., x_r]$ où chaque x_i est séparable. On peu t toujours supposer $r \geq 0$ minimal, et donc écrire $L = L'[x_0]$ où $L' = K[x_1, ..., x_r]$ vérifie $[L' : K] < [L : K]$, donc l'hypothèse de récurrence nous dit que le nombre de K-morphismes de $L' \longrightarrow \overline{K}$ vaut exactement $[L' : K]$. Puisque x_0 est séparable, on a exactement $\deg_{L'} x_0$ antécédents par $\Phi : \left\{ \begin{array}{ccc} \mathrm{Hom}_K\left(L, \overline{K}\right) & \longrightarrow & \mathrm{Hom}_K\left(L', \overline{K}\right) \\ \sigma & \longmapsto & \sigma_{|L'} \end{array} \right.$ d'un σ' donné, d'où exactement

$$[L' : K] \times \deg_{L'} x_0 = [L : K]$$

K-morphismes de $L \longrightarrow \overline{K}$.

Corollaire.
Toute extension finie $K \subset L$ de caractéristique nulle est séparable.

Démonstration.
En effet, L étant alors parfait, tous les éléments de L ont leur polynôme minimal séparable, donc sont séparables.

2.1.3 Extensions normales

Proposition.
On a la majoration $\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| \leq N$.

Démonstration.
Donnons-nous un K-morphisme $\sigma_0 : L \longrightarrow \overline{K}$. Si $g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)$, alors $\sigma_0 \circ g$ est encore un K-morphisme ; puisque σ_0 est injectif, tous les $\sigma_0 \circ g$ sont distincts quand g décrit $\mathrm{Gal}\left({}^{L}\!/_{K}\right)$. On a donc

$$\left\{\sigma_0 \circ g\,;\, g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)\right\} \subset \underset{K}{\mathrm{Hom}}\left(L, \overline{K}\right),$$

d'où $\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| \leq N$ en prenant les cardinaux.

On s'intéresse, de même que pour les extensions séparables, au cas d'égalité.

Définition.
Une extension ***finie*** $K \subset L$ *est dite* normale *si le nombre* $N = \left|\mathrm{Hom}_K\left(L, \overline{K}\right)\right|$ *de K-morphismes de* $L \longrightarrow \overline{K}$ *vaut exactement*

$$\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| = N.$$

On dispose de caractérisations des extensions normales en termes de morphismes.

Proposition.
Soit $K \subset L$ une extension ***finie*** *et $\overline{L}$ une clôture algébrique de L. On a les équivalences :*
(i) $K \subset L$ *est normale.*
(ii) *Tous les K-morphismes de* $L \longrightarrow \overline{K}$ *ont même image.*
(iii) $\mathrm{Hom}_K\left(L, \overline{K}\right)$ *est l'orbite d'un σ_0 quelconque de* $\mathrm{Hom}_K\left(L, \overline{K}\right)$ *pour l'action à droite de* $\mathrm{Gal}\left({}^{L}\!/_{K}\right)$, i.e.

$$\underset{K}{\mathrm{Hom}}\left(L, \overline{K}\right) = \left\{\sigma_0 \circ g\ ;\ g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)\right\}\ ;$$

(iv) *Tous les K-morphismes $\sigma : L \longrightarrow \overline{L}$ ont même image $\sigma(L) = L$.*
(v) *À une injection canonique $L \hookrightarrow \overline{L}$, près,* $\mathrm{Hom}_K\left(L, \overline{L}\right) = \mathrm{Gal}\left({}^{L}\!/_{K}\right)$.

Démonstration.
On utilisera l'inclusion $\left\{\sigma_0 \circ g\,;\, g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)\right\} \subset \mathrm{Hom}_K\left(L, \overline{K}\right)$ établie lors de la proposition précédente.
(i) $\Longrightarrow$ *(ii)* Si on a égalité des cardinaux, on a l'égalité ensembliste

$$\left\{\sigma_0 \circ g\,;\, g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)\right\} = \underset{K}{\mathrm{Hom}}\left(L, \overline{K}\right),$$

donc tous les K-morphismes de $L \longrightarrow \overline{K}$ sont de la forme $\sigma_0 \circ g$ où g est surjectif, donc ont même image $\mathrm{Im}\,\sigma_0$.
(ii) $\Longrightarrow$ *(iii)* Supposons que tous les K-morphismes de $L \longrightarrow \overline{K}$ ont même image. Soit $\sigma : L \longrightarrow \overline{K}$ un tel K-morphisme. Puisque $\mathrm{Im}\,\sigma = \mathrm{Im}\,\sigma_0$, on peut écrire $\sigma = \sigma_0 \circ g$ où g est une application de $L \longrightarrow L$. Puisque σ est un K-morphisme de corps et σ_0 injectif, g est aussi un K-morphisme de corps, *i.e.* $g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)$. On a donc $\mathrm{Hom}_K\left(L, \overline{K}\right) \subset \left\{\sigma_0 \circ g\,;\, g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)\right\}$ et égalité.
(iii) $\Longrightarrow$ *(i)* Il suffit de prendre les cardinaux.

$(i) \iff (iv) \iff (v)$ $K \subset L \subset \overline{L}$ est une clôture algébrique de K, donc on dispose de l'équivalence $(i) \iff (ii) \iff (iii)$ en prenant pour σ_0 l'injection canonique ι de L dans $\overline{L}$, qui vérifie $\sigma_0(L) = L$

On peut également caractériser les extensions normales en termes de polynômes.

Proposition
*Soit $K \subset L$ une extension **finie**. On a les équivalences :*
(i) $K \subset L$ est normale.
(ii) Pour tout poynôme $P \in K[X]$ irréductible, si P possède une racine sur L, alors P se scinde sur L.
(iii) L est un corps de décomposition d'un polynôme de $K[X]$.

Démonstration.
$(i) \implies (ii)$ Soit P irréductible dans $K[X]$ et ξ une racine de P dans L. Soit $\overline{L}$ une clôture algébrique de L (qui est une clôture algébrique de K). On a $K \subset K[\xi] \subset L \subset \overline{L}$. Dans $\overline{L}[X]$, P est scindé. Soit ζ une autre racine de P dans $\overline{L}$; on veut $\zeta \in L$.

Puisque L est finie, on peut écrire $L = K[\xi, x_1, ..., x_r]$ où $r \geq 0$ est minimal. Puisque $K \subset L$ est normale, le K-morphisme $\varphi : \begin{cases} L = K[\xi, x_1, ..., x_r] & \longrightarrow & \overline{L} \\ A(\xi, x_1, ..., x_r) & \longmapsto & A(\zeta, x_1, ..., x_r) \end{cases}$ (? ? ? ? ? unicité de $A(\xi, x_1, ..., x_r)$? ? ? ? ?) doit avoir pour image L, d'où $\zeta = \varphi(\xi) \in \operatorname{Im}\varphi = L$, *CQFD.*

$(ii) \implies (iii)$ Supposons $L = K[x_1, ..., x_n]$ où chaque x_i est séparable. Soit μ_i le polynôme minimal de x_i et notons $P = \bigvee_{i=1}^{n} \mu_i$ leur ppcm. Notons $\xi_1, ..., \xi_k$ les racines des μ_i dans L. Puisque L est normale et que chaque μ_i a une racine x_i dans L, les μ_i se scindent dans L sous la forme $\mu_i = \prod_{j=1}^{k} (X - \xi_j)^{\alpha_i(j)}$ où $\alpha_i(j) \geq 0$, et donc $P = \prod_{j=1}^{k} (X - \xi_j)^{\max_i \alpha_i(j)}$ est scindé dans L. Puisqu'en outre

$$L = K[x_1, ..., x_n] \subset K[\xi_1, ..., \xi_k] \subset L,$$

on en déduit que L est un corps de décomposition de P.

$(iii) \implies (i)$ Si L est un corps de décomposition de $P \in K[X]$, mettons $P = \prod_{i=1}^{r} (X - x_i)^{\alpha_i}$, alors $L = K[x_1, ..., x_r]$. Pour tout K-morphisme $\varphi : L \longrightarrow \overline{K}$, on a ainsi

$$\operatorname{Im}\varphi = \varphi(L) = \varphi(K[x_1, ..., x_r]) = K[\varphi(x_1), ..., \varphi(x_r)].$$

Or $P^{(n)}(\varphi(x_i)) = \varphi\left(P^{(n)}(x_i)\right)$ pour tout $n \geq 0$, donc $\varphi(x_i)$ est une racine de $P \in K[X]$ d'ordre α_i exactement, d'où $\prod_{i=1}^{r} (X - \varphi(x_i))^{\alpha_i} \mid P$ et on a égalité en comparant les degrés. Ainsi, φ permute les racines de P, d'où

$$\operatorname{Im}\varphi = K[\varphi(x_1), ..., \varphi(x_r)] = K[x_1, ..., x_r]$$

qui ne dépend pas de φ, donc tous les K-morphismes de $L \longrightarrow \overline{K}$ ont même image, *i.e.* $K \subset L$ séparable

Remarque. Si $K \subset L$ est normale et séparable, alors tout polynôme irréductible de $K[X]$ qui possède une racine dans L se scinde simplement dans L.

2.2 Extensions galoisiennes

Il ressort de l'étude précédente la conclusion suivante.

Conclusion.
*Soit $K \subset L$ une extension **finie**. On a toujours*

$$\left|\operatorname{Gal}\left(L/K\right)\right| \leq [L : K]$$

avec égalité

$$\left|\operatorname{Gal}\left(L/K\right)\right| = [L : K]$$

ssi $K \subset L$ est normale et séparable.

On s'intéresse maintenant au double cas d'égalité

$$\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| = N = [L:K].$$

Définition.
Une extension ***finie*** $K \subset L$ *est dite* galoisienne *si*

$$\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| = [L:K].$$

Par exemple, si L est un corps de décomposition d'un polynôme séparable, alors L est galoisienne (cf théorème de prolongements). On montre que la réciproque est vraie.

Théorème (caractérisation des extensions galoisiennes).
Soit $K \subset L$ une extension ***finie*** *et $\overline{L}$ une clôture algébrique de L. On a équivalences entre :*
(i) $K \subset L$ *est galoisienne.*
(ii) $K \subset L$ *est normale et séparable.*
(iii) $K \subset L$ *est séparable et tous les K-morphismes $\sigma : L \longrightarrow \overline{L}$ ont même image $\sigma(L) = L$.*
(iv) L *est un corps de décomposition d'un polynôme* ***séparable*** *de $K[X]$.*

Démonstration.
$(i) \iff (ii) \iff (iii)$ Immédiat par définition.
$(iv) \implies (i)$ Déjà vu.
$(i) \implies (iv)$ Supposons $K \subset L$ galoisienne. Par séparabilité, $L = K[x_1, ..., x_n]$ où les polynômes minimaux μ_i des x_i sont séparables. Par normalité, les μ_i se scindent dans L puisqu'ils y ont déjà une racine x_i. Il en résulte que les μ_i sont scindés simples dans L. En notant $P = \bigvee_{i=1}^{n} \mu_i$ le ppcm des μ_i et $\xi_1, ..., \xi_k$ les racines des P_i dans L, chaque μ_i s'écrit alors sous la forme $\mu_i = \prod_{j=1}^{k} (X - \xi_j)^{\varepsilon_i(j)}$ où $\varepsilon_i(j) = 0$ ou 1, donc $P = \prod_{j=1}^{k} (X - \xi_j)$ est scindé simple L. Comme on a en outre

$$L = K[x_1, ..., x_n] \subset K[\xi_1, ..., \xi_k] \subset L,$$

L est bien un corps de décomposition de P, qui est séparable car scindé simple dans L.

On peut maintenant décrire plus précisement les éléments de $G = \mathrm{Gal}\left({}^{L}\!/_{G}\right)$.

Corollaire.
Soit $K \subset L$ galoisienne et P un polynôme de décomposition de $K \subset L$ séparable de degré n. Alors

$$\mathrm{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow \mathfrak{S}_n$$

par permutation des racines de P.
On a par ailleurs la majoration

$$[L:K] \leq n!.$$

Démonstration.
Si $P = \prod_{i=1}^{n} (X - \xi_i)$, alors $\forall g \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)$, $P(g(\xi_i)) = g(P(\xi_i)) = g(0) = 0$, d'où $g(\xi_i) = \xi_{\sigma_g(i)}$ avec $\sigma_g \in \mathfrak{S}_n$ par injectivité de g. On a donc un morphisme de groupes

$$\begin{cases} \mathrm{Gal}\left({}^{L}\!/_{K}\right) & \longrightarrow & \mathfrak{S}_n \\ g & \longmapsto & \sigma_g \end{cases}$$

qui est injectif : si $\sigma_g = \mathrm{Id}$, alors $g(\xi_i) = \xi_i$ pour tout i, et comme $L = K[\xi_1, ..., \xi_n]$, on en déduit $g = \mathrm{Id}$ puisque g stabilise K.
La majoration est immédiate : $[L:K] = \left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right| \leq |\mathfrak{S}_n| = n!$.

Cette interprétation de l'action du groupe de Galois comme permutant les racines est importante. On en reparlera pour calculer explicitement le groupe de Galois d'un polynôme.

2.3 Lemme d'Artin

Si H est un sous-groupe de $\operatorname{Aut} L$, on note L^H le sous-corps de L formé des éléments laissés fixes par H. Le lemme d'Artin donne un classe d'extensions galoisiennes.

Lemme (Artin).
Soit $K \subset L$ une extension finie, H un sous-groupe de $\operatorname{Gal}\left(L/K\right)$. Alors l'extension $L^H \subset L$ est galoisienne de groupe de Galois

$$\operatorname{Gal}\left(L/L^H\right) = H.$$

Ainsi :

$$\left[L : L^H\right] = \left|\operatorname{Gal}\left(L/L^H\right)\right| = |H|.$$

Démonstration.
On a déjà trivialement que $H \subset \operatorname{Gal}\left(L/L^H\right)$, donc $|H| \leq \left|\operatorname{Gal}\left(L/L^H\right)\right|$; comme de plus L est finie sur K, L est finie sur $L^H \supset K$, donc $\operatorname{Gal}\left(L/L^H\right) \leq \left[L : L^H\right]$. On a ainsi $|H| \leq \left|\operatorname{Gal}\left(L/L^H\right)\right| \leq \left[L : L^H\right]$. Il suffit donc de montrer que $\left[L : L^H\right] \leq |H|$. Notons $E = L^H$ (comme **e**xtension intermédiaire).

Soient $n = |H| \geq 1$, $p > n$ et $x_1, ..., x_p$ dans L. Il suffit de montrer qu'ils sont liés sur E, *i.e.* qu'il exite $a_1, ..., a_p$ non tous nuls dans K tels que $\sum_{i=1}^{p} a_i x_i = 0$. Si de tels a_i existent, on aurait pour tout η de H $\sum_{i=1}^{p} a_i \eta(x_i) = 0$. En écrivant $H = \{\mathrm{Id}, \eta_2, ..., \eta_n\}$, les p scalaires a_i devraient vérifier les n équations

$$\begin{cases} \sum_{i=1}^{p} a_i \eta_1(x_i) = 0 \\ \cdots \\ \sum_{i=1}^{p} a_i \eta_n(x_i) = 0 \end{cases},$$

i.e.

$$\begin{pmatrix} \eta_1(x_1) & \cdots & \eta_1(x_p) \\ \vdots & & \vdots \\ \eta_n(x_1) & \cdots & \eta_n(x_p) \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix} = 0.$$

Puisque $n < p$, on a toujours une solution $(a_1, ..., a_p)$ non nulle à ce système dans L^p. On en choisit une qui minimise le nombres de termes a_i non nuls. Quitte à normaliser par un terme a_i non nul, on peut supposer qu'un des a_i vaut 1, mettons $a_1 = 1$, d'où une solution

$$(a_1, ..., a_p) = (1, a_2, ..., a_p).$$

Alors cette dernière est dans E^p. En effet, il existerait sinon un $a_{i_0>1}$ qui n'habite pas chez $E = L^H$, *i.e.* on pourrait trouver un $\eta_{j_0>1}$ dans H tel que $\eta_{j_0}(a_{i_0}) \neq a_{i_0}$. On reprend alors le système

$$\begin{pmatrix} \eta_1(x_i)_{i=1,...,p} \\ \vdots \\ \eta_n(x_i)_{i=1,...,p} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix} = 0,$$

on l'évalue en η_{j_0}, d'où

$$\begin{pmatrix} \eta_{j_0}\eta_1(x_i)_{i=1,...,p} \\ \vdots \\ \eta_{j_0}\eta_n(x_i)_{i=1,...,p} \end{pmatrix} \begin{pmatrix} \eta_{j_0}(a_1) \\ \vdots \\ \eta_{j_0}(a_p) \end{pmatrix} = 0.$$

Or $H = \left\{\eta_{j_0}\eta_k \text{ où } k = 1, ..., n\right\}$, donc après une permutation adéquate des lignes, le système devient

$$\begin{pmatrix} \eta_1(x_i)_{i=1,...,p} \\ \vdots \\ \eta_n(x_i)_{i=1,...,p} \end{pmatrix} \begin{pmatrix} \eta_{j_0}(a_1) \\ \vdots \\ \eta_{j_0}(a_p) \end{pmatrix} = 0,$$

d'où une autre solution $\left(\eta_{j_0}(a_1) = 1, \eta_{j_0}(a_2), ..., \eta_{j_0}(a_p)\right)$. Alors la différence $\left(1, \eta_{j_0}(a_2), ..., \eta_{j_0}(a_p)\right) - (1, a_2, ..., a_p)$ est encore solution, mais elle a un zéro de plus, donc elle est nulle par minimalité. On en déduit $\eta_{j_0}(a_{i_0}) = a_{i_0}$, *absurde.*

Corollaire (Artin faible).

Soit K un corps et G un sous-groupe de $\operatorname{Aut} K$. Alors l'extension $K^G \subset K$ est galoisienne de groupe de Galois

$$\operatorname{Gal}\left({}^{K}\!/_{K^G}\right) = G.$$

Démonstration.
On applique ce qui précède à l'extension triviale $\{0\} \subset K$.

2.4 Correspondance de Galois

Généralisons la correspondance de Galois établie pour les corps finis, qui à un sous-groupe H du groupe de Galois associait l'extension stable par H.

On considère

$$\begin{array}{c} \mathcal{G} = \left\{\text{sous-groupes de } \operatorname{Gal}\left({}^{L}\!/_{K}\right)\right\} \\ \mathcal{E} = \{\text{extensions intermédiaires}\} \end{array}.$$

On a des applications

$$\alpha : \left\{ \begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathcal{E} \\ H & \longmapsto & L^H \end{array} \right. \text{ et } \beta : \left\{ \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{G} \\ E & \longmapsto & \operatorname{Gal}\left({}^{L}\!/_{E}\right) \end{array} \right. .$$

Le théorème suivant montre que α et β sont réciproques l'une de l'autre. Ainsi, pour comprendre les extensions intermédiaires, problème de théorie des corps, on se ramène à étudier le groupe de Galois, problème de théorie des groupes.

Théorème (fondamental).
Soit $K \subset L$ galoisienne et H un sous-groupe de $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$.

- *Pour toute extension intermédiaire E, on a $L^{\operatorname{Gal}\left({}^{L}\!/_{E}\right)} = E$.*
- *L'extension $L^H \subset L$ est galoisienne avec $\operatorname{Gal}\left({}^{L}\!/_{L^H}\right) = H$.*
- *Pour $g \in G = \operatorname{Gal}\left({}^{L}\!/_{K}\right)$, on a $g\left(L^H\right) = L^{gHg^{-1}}$ et $\operatorname{Gal}\left({}^{L^H}\!/_{K}\right) \simeq {}^{N_G(H)}\!/_{H}$.*
- *L'extension $K \subset L^H$ est galoisienne ssi $H \lhd \operatorname{Gal}\left({}^{L}\!/_{K}\right)$, et alors*

$$\operatorname{Gal}\left({}^{L^H}\!/_{K}\right) \simeq {}^{G}\!/_{H} = {}^{\operatorname{Gal}\left({}^{L}\!/_{K}\right)}\!/_{H}.$$

Démonstration.
• Soit $E \in \mathcal{E}$. Par définition, on a toujours $E \subset L^{\operatorname{Gal}\left({}^{L}\!/_{E}\right)}$. Montrons l'égalité des dimensions sur K pour conclure à l'égalité.

Comme $K \subset L$ est galoisienne, L est un corps de décomposition d'un polynôme $P \in K[X]$ séparable. Alors $P \in E[X]$, et L est aussi corps de décomposition d'un polynôme séparable de $E[X]$, *i.e.* $E \subset L$ est galoisienne, d'où $[L : E] = \left|\operatorname{Gal}\left({}^{L}\!/_{E}\right)\right| \overset{\text{Artin}}{=} \left[L : L^{\operatorname{Gal}\left({}^{L}\!/_{E}\right)}\right]$, *CQFD.*

• Déjà fait (Artin faible).

• Soit $H \in \mathcal{G}$, et $g \in \operatorname{Gal}\left({}^{L}\!/_{K}\right)$. On veut $g\left(L^H\right) = L^{gHg^{-1}}$. D'une part, pour $x \in L^H$, on a $\forall h \in H$, $\left[ghg^{-1}\right](g(x)) = gh(x) = g(x)$, d'où $g(x) \in L^{gHg^{-1}}$ et $g\left(L^H\right) \subset L^{gHg^{-1}}$. D'autre part, pour $y \in L^{gHg^{-1}}$, soit $x = g^{-1}(y)$; pour $h \in H$, $h(x) = hg^{-1}(y) = g^{-1}\left[ghg^{-1}\right](y) = g^{-1}(y) = x$, d'où $x \in L^H$, $y = g(x) \in g\left(L^H\right)$, puis $L^{gHg^{-1}} \subset g\left(L^H\right)$.

Considérons maintenant le morphisme de groupe $\Phi : \left\{ \begin{array}{ccc} N_G(H) & \longrightarrow & \operatorname{Gal}\left({}^{L^H}\!/_{K}\right) \\ g & \longmapsto & g_{|L^H} \end{array} \right.$. Φ est bien défini car pour $g \in N_G(H)$, on a $g\left(L^H\right) = L^{gHg^{-1}} = L^H$, donc g_{L^H} est surjective ; comme $g_{|L^H}$ est clairement injective et fixant K, $g_{|L^H}$ est bien un K-automorphisme de L^H.

Calculons le noyau $\operatorname{Ker}\Phi$:

$$g \in \operatorname{Ker}\Phi \iff g_{|L^H} = \operatorname{Id} \iff g \in \operatorname{Gal}\left({}^{L}\!/_{L^H}\right) \overset{\text{Artin}}{=} H.$$

Montrons ensuite que Φ est surjectif. Soit $\sigma \in \operatorname{Gal}\left({}^{L^H}\!/_{K}\right)$. Puisque $K \subset L$ est normale, L est un corps de décomposition d'un polynôme $P \in K[X]$. Mais alors $L^H \subset L$ est aussi une extension de décomposition de

$P \in L^H[X]$, donc on peut prolonger l'isomorphime $\sigma : L^H \longrightarrow L^H$ en un isomorphisme $\widetilde{\sigma} : L \longrightarrow L$. Puisque σ fixe K, $\widetilde{\sigma}$ aussi, donc $\widetilde{\sigma} \in \mathrm{Gal}\left({}^{L}\!/_{K}\right) = G$, et comme $\widetilde{\sigma}$ prolonge σ, on a $\Phi(\sigma) = \widetilde{\sigma}_{|L^H} = \sigma$. Φ est donc bien surjectif.

On conclut en disant que $\mathrm{Im}\,\Phi \simeq {}^{N_G(H)}\!/_{\mathrm{Ker}\,\Phi}$, ce qui donne $\mathrm{Gal}\left({}^{L^H}\!/_{K}\right) \simeq {}^{N_G(H)}\!/_{H}$.

• $K \subset L^H$ est une extension galoisienne ssi

$$\begin{aligned}
& \left|\mathrm{Gal}\left({}^{L^H}\!/_{K}\right)\right| = [L^H : K] \\
\Longleftrightarrow \quad & \left|{}^{N_G(H)}\!/_{H}\right| = \frac{[L:K]}{[L:L^H]} \\
\Longleftrightarrow \quad & \frac{|N_G(H)|}{|H|} = \frac{\left|\mathrm{Gal}\left({}^{L}\!/_{K}\right)\right|}{\left|\mathrm{Gal}\left({}^{L}\!/_{L^H}\right)\right|} = \frac{|G|}{|H|} \\
\Longleftrightarrow \quad & N_G(H) = G \\
\Longleftrightarrow \quad & H \lhd G,
\end{aligned}$$

et le troisième point donne alors $\mathrm{Gal}\left({}^{L^H}\!/_{K}\right) \simeq {}^{N_G(H)}\!/_{H} = {}^{G}\!/_{H}$.

2.5 Clôture galoisienne d'une extension séparable finie – Théorème de l'élément primitif

Proposition.
*Soit $K \subset L$ une extension finie **séparable**, $\overline{L}$ une clôture algébrique de L. Alors il existe une plus petite extension galoisienne $K \subset L^g$ dans $\overline{L}$, qui vérifie donc $K \subset L \subset L^g \subset \overline{L}$. On l'appelle la* clôture galoisienne *de L.*

Démonstration.

Construction 1 : utilise le critère $K \subset L$ galoisienne ssi L décompose un polynôme séparable de $K[X]$).

$K \subset L$ est séparable, donc $L = K[x_1, ..., x_n]$ où les x_i sont séparables. Notant μ_i leurs polynômes minimaux. Si L^g répond au problème, alors L^g est normale, donc les μ_i (qui ont une racine x_i sur K) se scindent sur L^g, donc L^g contient l'engendré des racines de tous les μ_i, ou plus précisément l'engendré des racines du ppcm $P = \bigvee \mu_i$.

Réciproquement, si l'on appelle D un corps de décomposition de P sur K, on a déjà vu que P est séparable puisque les x_i le sont, donc $K \subset D$ est galoisienne. Ainsi, l'extension D répond au problème et est la plus petite d'après l'analyse.

Construction 2 : utilise le critère $K \subset L$ normale ssi tous les K-morphismes $L \longrightarrow \overline{L}$ ont même image L.

Supposons qu'une telle extension $K \subset L \subset L^g \subset \overline{L}$ existe. En remarquant que $\overline{L}$ est une clôture algébrique de L^g, on doit avoir $\sigma(L^g) = L^g$ pour tout K-morphisme $\sigma : L^g \longrightarrow \overline{L}$. En particulier, si $\sigma_0 : L \longrightarrow \overline{L}$ désigne un K-morphisme, on peut prolonger σ_0 à L^g (cf théorème de prolongements), et alors $\sigma_0(L) \subset \sigma_0(L^g) = L^g$. Ainsi, en appelant $\sigma_1, ..., \sigma_n$ les K-morphismes de $L \longrightarrow \overline{L}$, L^g doit donc contenir tous les $\sigma_i(L)$, donc doit contenir l'*extension composée* des $\sigma_i(L)$:

$$E := K(\sigma_1(L), ..., \sigma_n(L)).$$

Montrons réciproquement que E convient – ce qui précède prouvant qu'elle sera la plus petite extension répondant au problème.

Soit φ un K-morphisme de $E \longrightarrow \overline{L}$. Les σ_i étant d'image $\sigma_i(L) \subset K(\sigma_1(L), ..., \sigma_n(L)) = E$, on peut parler de la composée $\varphi\sigma_i$, laquelle est un K-morphisme de $L \longrightarrow \overline{L}$, *i.e.* est un $\sigma_{\sigma(i)}$, σ étant une permutation de $\mathfrak{S}_n$ par injectivité de φ. On en déduit

$$\begin{aligned}
\varphi(E) &= \varphi(K(\sigma_1(L), ..., \sigma_n(L))) \\
&= K(\varphi\sigma_1(L), ..., \varphi\sigma_n(L)) \\
&= K\left(\sigma_{\sigma(1)}(L), ..., \sigma_{\sigma(n)}(L)\right) \\
&= K(\sigma_1(L), ..., \sigma_n(L)) \\
&= E,
\end{aligned}$$

donc $K \subset E$ est normale. D'autre part, $K \subset L$ étant séparable, on peut écrire $L = K[x_1, ..., x_r]$ où les x_i sont séparables. On en déduit $\sigma_i(L) = \sigma_i(K[x_1, ..., x_r]) = K[\sigma_i(x_1), ..., \sigma_i(x_r)]$, et chaque $\sigma_i(x_j)$ est séparable car de même polynôme minimal que x_j (σ_i fixe K...). Ainsi, $E = K(\sigma_i(L)) = K(K[\sigma_i(x_j)]) = K(\sigma_i(x_j))$ est séparable. $K \subset E$ est par conséquent galoisienne, *CQFD*.

Conséquence. On peut décrire les extensions intermédiaires $K \subset E \subset L$ d'une extension séparable à l'aide de $\mathrm{Gal}\left(L^g/K\right)$. En particulier, *il n'y a qu'un nombre fini d'extensions intermédiaires.*

On en déduit le théorème de l'élément primitif.

Théorème de l'élément primitif.
*Soit $K \subset L$ extension finie **séparable**. Alors il exite un $a \in L$ tel que $L = K[x]$.*

Lemme.
Soit E un K-espace vectoriel et $F_1, ..., F_n$ des sous-espaces vectoriels stricts de E. Si K est infini, alors $\bigcup_{i=1}^n F_i \subsetneq E$.

Démonstration.
Par récurrence sur n.
• $n = 1$ est trivial.
• Pour $n > 1$, supposons $\bigcup_{i=1}^n F_i = E$. Par hypothèse de récurrence, $\bigcup_{i=1}^{n-1} F_i \subsetneq E$, donc on peut trouver un u dans $E \setminus \bigcup_{i=1}^{n-1} F_i$; noter qu'un tel u est dans $F_n \setminus \bigcup_{i=1}^{n-1} F_i$. Puisque $F_n \subsetneq E$, on peut trouver un a dans $E \setminus F_n$. On pose alors $D = a + Ku$.
D'une part, on a $D \cap F_n = \emptyset$, sinon

$$a + \lambda u = f_n \implies a = f_n - \lambda u \in F_n,$$

d'autre part, on a $\forall i \neq n$, $|D \cap F_i| \leq 1$ car

$$\begin{cases} a + \lambda u = x_i \\ a + \mu u = y_i \end{cases} \implies (\lambda - \mu) u = x_i - y_i \in F_i \cap Ku = \{0\} \implies x_i = y_i.$$

Ainsi, $|D| \leq n - 1$, ce qui *absurde* car D et K ont même cardinal.

Démonstration de la proposition.
Si K est de cardinal fini, alors L est également fini, donc L est un $\mathbb{F}_q$ qui est monogène (car $\mathbb{F}_q^*$ cyclique). On peut donc supposer K infini.
On écrit alors $L = \bigcup_{x \in L} K[x]$ où $K \subset K[x] \subset L$ est un extension intermédiaire. Or ces dernières sont en nombres fini, donc on peut extraire un recouvrement fini $L = \bigcup_{i=1}^n K[x_i]$. Or L est un K-espace vectoriel de dimension finie avec K infini, donc le lemme s'applique, d'où un x_i tel que $L = K[x_i]$.

2.6 Exemples

2.6.1 Racines de l'unités – Extensions cyclotomiques

Soit K un corps de caractéristique p et $n \geq 1$. On note $\mu_n(K)$ l'ensemble des racines n-ièmes de l'unité, *i.e.*

$$\mu_n(K) = \{x \in K \ ; \ x^n = 1\}.$$

Proposition.
On suppose $p \nmid n$. Alors $\mu_n(K)$ est un groupe cyclique dont l'ordre ω vérifie

$$p \nmid \omega \mid n.$$

Démonstration.
• $\mu_n(K)$ est un sous-groupe fini de K^*, donc est cyclique.

$X^n - 1$ est premier avec sa dérivée $nX^{n-1} \neq 0$, donc est séparable. Si L est un corps de décomposition de $X^n - 1$ sur K, on en déduit que $|\mu_n(L)| = n$, donc l'ordre ω de $\mu_n(K)$ vu en tant que sous-groupe de $\mu_n(L)$ doit diviser l'ordre de $\mu_n(L)$, *i.e.* $\omega \mid n$.

• Soit $p = \operatorname{car} K$. Si $p = 0$, p ne peut diviser $\omega \neq 0$. Supposons donc p premier.

On écrit $n = p^\alpha m$ où $p \wedge m = 1$ et $\alpha \geq 0$. En remarquant que $(-1)^{p^\alpha} = -1$ car

$$\begin{cases} \text{pour } \alpha = 0,\ (-1)^{p^\alpha} = (-1)^1 = -1 \\ \text{pour } p = 2,\ (-1)^{p^\alpha} = (-1)^2 = 1 = -1 \\ \text{pour } p \text{ impair},\ (-1)^{p^\alpha} = (-1)^p = -1 \end{cases},$$

on obtient $X^n - 1 = X^{p^\alpha m} - 1 = (X^m - 1)^{p^\alpha}$, d'où $\mu_n(K) = \mu_m(K)$. Puisque $p \nmid m$ (sinon $p \mid m \mid n$), on peut appliquer le premier point : $\omega = |\mu_m(K)|$ divise m, d'où $p \nmid \omega$ (sinon $p \mid \omega \mid m \mid n$, *absurde*).

Définition.
On appelle extension cyclotomique *de niveau n de K un corps de décomposition L de $X^n - 1$.*

Proposition.
Soit L une extension cyclotomique de niveau n sur K. Alors
• *Il y a exactement n racines n-ièmes de l'unité dans L.*
• *$K \subset L$ est galoisienne de groupe de Galois* $\operatorname{Gal}\left(L/K\right) \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.
• *Le degré de l'extension cyclotomique vérifie $[L : K] \leq \varphi(n)$.*

Démonstration.
• $X^n - 1$ est séparable et scindé sur L, donc scindé simple sur L, d'où $|\mu_n(L)| = n$.
• L est un corps de décomposition d'un polynôme séparable, donc l'extension $K \subset L$ est galoisienne.

Soit $G = \operatorname{Gal}\left(L/K\right)$ et $g \in G$. g induit sur $\mu_n(L)$ un automorphisme de $\mu_n(L)$. En effet, si $\xi \in \mu_n(L)$, alors $g(\xi)^n = g(\xi^n) = g(1) = 1$, donc la restriction de g à $\mu_n(L)$ est un endomorphisme du groupe $\mu_n(L)$, injectif (car g injectif) donc bijectif (car $\mu_n(L)$ fini) ; c'est donc un automorphisme de $\mu_n(L)$. On a ainsi un morphisme de groupes $\begin{cases} G & \longrightarrow & \operatorname{Aut}(\mu_n(L)) \\ g & \longmapsto & g_{|\mu_n(L)} \end{cases}$. L'injectivité s'obtient en remarquant que, puisque L est engendré par $\mu_n(L)$, un K-morphisme g est entièrement déterminé par les valeurs qu'il prend sur $\mu_n(L)$. Comme $\mu_n(L)$ est cyclique d'ordre n, on a $\operatorname{Aut}(\mu_n(L)) \simeq \operatorname{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ et G s'injecte bien dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. En prenant les cardinax, on obtient la majoration voulue :

$$[L : K] = |G| \leq \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right| \leq \varphi(n).$$

On regarde le cas particulier de $K = \mathbb{Q}$.

Proposition (extensions cyclotomiques de $\mathbb{Q}$).
Soit L une extension cyclotomique de niveau n de $\mathbb{Q}$. Alors $\operatorname{Gal}\left(L/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Démonstration.
On peut écrire $L = \mathbb{Q}[\xi]$ où ξ est une racine primitive de l'unité. Son polynôme minimal est $\Phi_n \in \mathbb{Z}[X]$, avec $\deg \Phi_n = \varphi(n)$, d'où

$$\varphi(n) = \deg \Phi_n = \deg_K \xi = [L : K] = |G| \leq \varphi(n).$$

On obtient donc une égalité, et le morphisme injectif $G \hookrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ devient un isomorphisme.

2.6.2 Polynômes symétriques – Discriminant

Soit A un anneau commutatif. On considère les polynômes symétriques de $A[X_1, ..., X_n]$. On dispose en particulier des polynômes symétriques élémentaires

$$\begin{cases} \sigma_1 = X_1 + ... + X_n \\ \sigma_k = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k} \\ \sigma_n = X_1 ... X_n \end{cases} .$$

On précisera si besoin le nombre de variables des σ_k par un exposant :

$$\sigma_k^{(n)} := \sigma_k (X_1, ..., X_n) .$$

Proposition.
Soit $P \in A[X_1, ..., X_n]$ symétrique. Alors il existe un unique polynôme $S \in A[Y_1, ..., Y_n]$ tel que

$$P(X_1, ..., X_n) = S(\sigma_1, ..., \sigma_n) .$$

Démonstration.
• Pour l'existence, on fait une récurrence sur le nombre de variables plus le degré total.
Pour $n = 1$, $X = \sigma_1$, donc $P = P(X) = P(\sigma_1)$.
Pour $\deg P = 0$, *i.e.* $P = a$ constant, on a $P(X_1, ..., X_n) = a = a(\sigma_1, ..., \sigma_n)$.
Soit P à $n \geq 2$ variables et de degré ≥ 1. On considère le polynôme à $n-1$ variables

$$P_n(X_1, ..., X_{n-1}) = P(X_1, ..., X_{n-1}, 0)$$

symétrique (car P l'est), donc on peut récurrer :

$$\begin{aligned} P_n(X_1, ..., X_{n-1}) &= Q\left(\sigma_1^{(n-1)}(X_1, ..., X_{n-1}), ..., \sigma_{n-1}^{(n-1)}(X_1, ..., X_{n-1})\right) \\ &= Q\left(\sigma_1^{(n)}(X_1, ..., X_{n-1}, 0), ..., \sigma_{n-1}^{(n)}(X_1, ..., X_{n-1}, 0)\right) . \end{aligned}$$

On en déduit que $P(X_1, ..., X_n) - Q\left(\sigma_1^{(n)}, ..., \sigma_{n-1}^{(n)}\right)$ s'annule en $X_n = 0$, donc en tous les X_i par symétrie, donc est divisible par $X_1 ... X_n = \sigma_n$, d'où

$$P(X_1, ..., X_n) - Q\left(\sigma_1^{(n)}, ..., \sigma_{n-1}^{(n)}\right) = \sigma_n P^*$$

où P^* est un polynôme à n variables symétrique de degré $< \deg P$, et on peut alors récurrer sur le degré de P^*.
• Pour l'unicité, on récurre sur n.
Pour $n = 1$, $S(\sigma_1) = S(X) = S$, d'où l'unicité.
Pour $n \geq 2$, supposons $S(\sigma_1, ..., \sigma_n) = T(\sigma_1, ..., \sigma_n)$. On fait $X_n = 0$, d'où

$$S\left(\sigma_1^{(n-1)}, ..., \sigma_{n-1}^{(n-1)}, 0\right) = T\left(\sigma_1^{(n-1)}, ..., \sigma_{n-1}^{(n-1)}, 0\right) .$$

En posant $\begin{cases} S_n(X_1, ..., X_{n-1}) = S(X_1, .., X_{n-1}, 0) \\ T_n(X_1, ..., X_{n-1}) = T(X_1, .., X_{n-1}, 0) \end{cases}$, on a alors

$$S_n\left(\sigma_1^{(n-1)}, ..., \sigma_{n-1}^{(n-1)}\right) = T_n\left(\sigma_1^{(n-1)}, .., \sigma_{n-1}^{(n-1)}\right)$$

d'où $T_n = S_n$ par récurrence. ? ? ? ? ?

Corollaire.
L'extension $K(\sigma_1, ..., \sigma_n) \subset K(X_1, ..., X_n)$ est galoisienne de groupe de Galois

$$\mathrm{Gal}\left({}^{K(X_1,...,X_n)}\!\!\diagup_{K(\sigma_1,...,\sigma_n)}\right) \simeq \mathfrak{S}_n$$

qui permute les indéterminées.

Démonstration.
• Soit $P(T) = \prod_{i=1}^{n}(T - X_i)$ élément de $K(X_1, ..., X_n)[T]$. En développant, on trouve

$$P(T) = T^n - \sigma_1 T^{n-1} + ... + (-1)^n \sigma_n,$$

donc $P(T) \in K(\sigma_1, ..., \sigma_n)[T]$. P est de plus séparable (car scindé simple), et $K(X_1, ..., X_n)$ en est un corps de décomposition, donc $K(\sigma_1, ..., \sigma_n) \subset K(X_1, ..., X_n)$ est une extension galoisienne.
• Soit $G = \mathrm{Gal}\left({}^{K(X_1,...,X_n)}\!/_{K(\sigma_1,...,\sigma_n)}\right)$. On sait déjà que G s'injecte dans $\mathfrak{S}_n$ par permutation des racines d'un polynômes de décomposition, en particulier P, donc G agit en permutant les indéterminées X_i. D'autre part, il est clair que toute permutation des X_i laisse stable $K(\sigma_1, ..., \sigma_n)$, d'où l'égalité.

Introduisons maintenant un outil issu des symétries de $K(X_1, ..., X_n)$: le discriminant.

Définition.
Le polynôme $\prod_{i<j}(X_i - X_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(X_i - X_j)$ *est invariant sous* $\mathfrak{S}_n$*, donc s'écrit comme un polynôme* $S(\sigma_1, ..., \sigma_n)$ *à coefficients entiers en les* σ_i*.*
Pour $P = X_1 - a_1 X^{n-1} + ... + (-1)^n a_n$ *polynôme unitaire de degré* $n \geq 1$*, on pose*

$$\operatorname{disc} P = S(a_1, ..., a_n) \in K$$

et on l'appelle le discriminant *de* P*.*
Si P *n'est pas unitaire,* P *s'écrit* λQ *où* Q *est unitaire, et on pose*

$$\operatorname{disc} P = \lambda^2 \operatorname{disc} Q$$

Par exemple, pour $n = 2$, on a

$$\prod_{i<j}(X_i - X_j)^2 = (X - Y)^2 = (X + Y)^2 - 4XY = \sigma_1^2 - 4\sigma_2,$$

d'où

$$S(X, Y) = X^2 - 4Y.$$

Aini, le discriminant d'un polynôme $P = aX^2 + bX + c$ vaut

$$\Delta = a^2\left(\left(\frac{b}{a}\right)^2 - 4\left(\frac{a}{c}\right)\right) = b^2 - 4ac$$

bien connu...

L'intérêt du discriminant (entre autres) est de donner un critère pratique de séparabilité.
En effet, soient $\alpha_1, ..., \alpha_n$ les racines d'un polynôme P dans un corps de décomposition : $P = \lambda \prod (X - \alpha_i)$. Alors

$$\operatorname{disc} P = \lambda^2 S(\sigma_1(\alpha_1, ..., \alpha_n), ..., \sigma_n(\alpha_1, ..., \alpha_n)) = \lambda^2 \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Proposition (critère de séparabilité).
P *est séparable ssi* $\operatorname{disc} P \neq 0$*.*

Proposition (calcul du discriminant).
Soit P *unitaire de degré* n *et* $\begin{cases} \alpha_1, ..., \alpha_n \text{ les racines de } P \\ \beta_1, ..., \beta_{n-1} \text{ les racines de } P' \end{cases}$ *dans une extension de décomposition. On a alors*

$$\operatorname{disc} P = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{i=1}^{n-1} P(\beta_i).$$

Démonstration.
On a $P' = \sum_{i=1}^{n} \prod_{j\neq i} (X - \alpha_j)$, donc $P'(\alpha_i) = \prod_{j\neq i} (\alpha_i - \alpha_j)$, d'où

$$\prod_{i=1}^{n} P'(\alpha_i) = \prod_{i=1}^{n} \prod_{j\neq i} (\alpha_i - \alpha_j) = \operatorname{disc} P.$$

D'autre part, P' s'écrit $n\prod_{j=1}^{n-1}(X - \beta_j)$,donc

$$\begin{aligned} \operatorname{disc} P &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} n \prod_{j=1}^{n-1} (\alpha_i - \beta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} n^n \prod_{j=1}^{n-1} \prod_{i=1}^{n} (\alpha_i - \beta_j) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_{j=1}^{n-1} P(\beta_j). \end{aligned}$$

Par exemple, pour $P = X^n + aX + b$, on peut montrer que

$$\operatorname{disc}(X^n + aX + b) = (-1)^{\frac{n(n-1)}{2}} \left[(1-n)^{n-1} a^n + n^n b^{n-1}\right].$$

Pour un polynôme de degré 3 réduit, mettons $P = X^3 + pX + q$, on va montrer que

$$\operatorname{disc} P = -4p^3 - 27q^2.$$

En effet, $\prod_{i<j}(X_i - X_j)^2 = (X-Y)^2(Y-Z)^2(Z-X)^2 = S(\sigma_1, \sigma_2, \sigma_3)$ est homogène de degré 6, et $\operatorname{disc} P = S(0, p, -q)$, donc seul les termes sans σ_1 nous intéressent. Il n'y en a que deux sortes : $\sigma_2\sigma_2\sigma_2$ et $\sigma_3\sigma_3$. Ainsi,

$$S(\sigma_1, \sigma_2, \sigma_3) = A(\sigma_1) + \lambda\sigma_2^3 + \mu\sigma_3^2.$$

Pour trouver les constantes λ et μ, on regarde des valeurs particulières.

Pour $P = X(X-1)(X+1) = X^3 - X$, on a $\operatorname{disc} P = (1-(-1))^2(1-0)^2(0-(-1))^2 = 4$, qui doit aussi valoir λ, d'où $\lambda = 4$

Pour $P = X^3 - 1$, la formule avec les racines de la dérivée $3X^2$ donne $\operatorname{disc} P = -3^3\left(0^3-1\right)\left(0^3-1\right) = -27$, qui doit aussi valoir μ, d'où $\mu = -27$.

Finalement :

$$\operatorname{disc}\left(X^3 + pX + q\right) = -4p^3 - 27q^2$$

Proposition (un critère pour que $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \subset \mathfrak{A}_n$**).**
Soit $K \subset L$ galoisienne, P un polynôme de décomposition de degré n et $\xi_1, ..., \xi_n$, les racines de P dans L.
Soit $\operatorname{disc} P = \prod_{i<j}\left(\xi_j - \xi_i\right)^2$ *et posons* $\delta = \prod_{i<j}\left(\xi_j - \xi_i\right) \in L$. *On dispose d'une signature* ε sur $G = \operatorname{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow \mathfrak{S}_n$ *(qui dépend de l'indexation des racines choisie).*
Alors les deux conditions suivantes sont équivalentes :
- $\operatorname{disc} P$ *est un carré dans* K, i.e. $\delta \in K$;
- ε *est trivial sur* G, i.e. $G \hookrightarrow \mathfrak{A}_n$.

Démonstration.
$\forall \sigma \in G$, on a

$$\varepsilon(\sigma) = \frac{\prod_{i<j}\left(\xi_{\sigma(j)} - \xi_{\sigma(i)}\right)}{\prod_{i<j}\left(\xi_j - \xi_i\right)} = \frac{\prod_{i<j}\left(\sigma\left(\xi_j\right) - \sigma\left(\xi_i\right)\right)}{\delta} = \frac{\sigma\left(\prod_{i<j}\left(\xi_j - \xi_i\right)\right)}{\delta} = \frac{\sigma(\delta)}{\delta}.$$

Ainsi, si $\delta \in K$, alors G fixe δ, d'où $\varepsilon(G) = \{1\}$.
Réciproquement, si $G \subset \mathfrak{A}_n$, alors G fixe δ, donc $\delta \in L^G = K$.

Remarque. Bien que la proposition $G \hookrightarrow \mathfrak{A}_n$ dépende de l'indexation des racines choisie, la condition $\operatorname{disc} P \in K^2$, elle, n'en dépend pas.

2.6.3 Extension cycliques

Définition.
Une extension est dite cyclique *si elle est galoisienne de groupe de Galois* ***cyclique****.*

Lemme de Dedekind.
Soit $n \geq 2$, G un monoïde et $\sigma_1, ..., \sigma_n : G \longrightarrow K^*$ des morphismes multiplicatifs deux à deux distincts. Alors les σ_i (vus dans le K-espace vectoriel K^G) sont linéairement K-indépendants.

Démonstration.
Par l'absurde. On suppose $\sum_i \lambda_i \sigma_i = 0$ où le support des λ_i est non vide et minimal. Alors, pour tous x, y dans G, on a

$$0 = \left[\sum_i \lambda_i \sigma_i\right](xy) = \left[\sum_i \lambda_i \sigma_i(x)\,\sigma_i\right](y),$$

d'où pour tout j :

$$\sum_i \lambda_i \left(\sigma_i(x) - \sigma_j(x)\right)\sigma_i = \sum_i \lambda_i \sigma_i(x)\,\sigma_i - \sigma_j(x)\sum_i \lambda_i \sigma_i = 0 - 0 = 0,$$

donc par minimalité du cardinal des (λ_i) on a $\lambda_i\left(\sigma_i(x) - \sigma_j(x)\right) = 0$ pour tous i, j, en particulier pour un i_0 tel que $\lambda_{i_0} \neq 0$ et pour $j \neq i_0$ (possible car $n \geq 2$), d'où $\sigma_{i_0}(x) - \sigma_j(x) = 0$, et ce pour tout x de G, *i.e.* $\sigma_{i_0} = \sigma_j$, *absurde* car les σ_i sont deux à deux distintcs.

Remarque. On aura besoin par la suite de l'hypothèse

"K contient déjà toutes les racines n-ièmes de l'unité",

ce qu'on peut reformuler de manière équivalente en :
- $|\mu_n(K)| = n$;
- $X^n - 1$ est scindé simple sur K ;
- $X^n - 1$ scindé sur K (par séparabilité) ;
- K est une extension cyclotomique de niveau n de lui-même ;
- K contient une racine n-ième de l'unité non triviale (par cyclicité de $\mu_n(K)$) ;

Proposition.
Supposons $|\mu_n(K)| = n$, et soit a qui n'est pas une puissance (non triviale) de K divisant n, i.e.

$$\begin{cases} a \in K^d \\ d \mid n \end{cases} \implies d = 1.$$

Alors
- *$X^n - a$ est irréductible sur K ;*
- *Toute extension L de décompostion de $X^n - a$ est cyclique ; plus précisément*

$$\mathrm{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow \mu_n(K).$$

Démonstration.
Soit L un corps de rupture de $X^n - a$ sur K, et $x \in L$ tel que $x^n = a$. Soit ξ une racine n-ième de l'unité dans K. Alors les $x\xi^k$ pour $0 \leq k < n$ sont les racines de $X^n - a$ dans L, d'où $X^n - a = \prod_{k=0}^{n-1}\left(X - x\xi^k\right)$ (ce qui montre au passage que $X^n - a$ est séparable).

Soit maintenant une décomposition $X^n - a = QR$ dans $K[X]$ où Q non constant. Dans $L[X]$, on a $Q = \prod_{k\in A}\left(X - x\xi^k\right)$ pour une certaine partie $A \subset \{0, ..., n-1\}$ de cardinal ≥ 1, mettons q (comme Q).

Le terme constant de Q est $(-1)^q x^q \xi^? \in K$, donc $x^q \in K$; en outre, $x^n = a \in K$. Soit $\delta = n \wedge q$. Bezout donne $\delta = \alpha n + \beta q$, d'où $x^\delta = (x^n)^\alpha (x^q)^\beta \in K$, donc

$$a = x^n = \left(x^\delta\right)^{\frac{n}{\delta}} \in K^{\frac{n}{\delta}},$$

d'où par hypothèse sur a

$$\frac{n}{\delta} = 1 \iff n = \delta \iff q = n \iff Q = X^n - a.$$

Par conséquent, $X^n - a$ est irréductible.

Ainsi, si L est un corps de décomposition de $X^n - a$ sur K, alors $X^n - a$ est irréductible séparable, donc $K \subset L$ est galoisienne. Or, $L = K\left[x, x\xi, ..., x\xi^{n-1}\right] = K[x]$, donc un $\sigma \in \mathrm{Gal}\left(L/K\right)$ est déterminé par $\sigma(x)$, qui vaut une certaine racine $\sigma(x) = x\xi^k$ de P puisque

$$P(\sigma(x)) = \sigma(x)^n - a = \sigma(x^n) - a = \sigma(a) - a = a - a = 0.$$

On a donc un morphisme de groupe injectif $\left\{ \begin{array}{ccc} \mathrm{Gal}\left(L/K\right) & \longrightarrow & \mu_n(K) \\ \sigma & \longmapsto & \frac{\sigma(x)}{x} \end{array} \right.$, d'où $\mathrm{Gal}\left(L/K\right)$ cyclique.

Proposition (réciproque).
Soit $K \subset L$ cyclique, $n = [L : K]$, et supposons que $|\mu_n(K)| = n$. Alors on peut trouver un a dans K tel que L soit un corps de décomposition de $X^n - a$.

Démonstration.
Soit σ un générateur de $\mathrm{Gal}\left(L/K\right)$. D'après la démonstration qui précède, il est judicieux de chercher un $x \in L$ tel que $\frac{\sigma(x)}{x}$ soit une racine primitive n-ième de l'unité.

Soit ξ une racine primitive n-ième de l'unité (qui est dans K par hypothèse). On veut un $x \in L$ tel que

$$\frac{\sigma(x)}{x} = \xi \iff \xi^{-1}\sigma(x) = x \iff \sigma\left(\xi^{-1}x\right) = x \iff x \in \mathrm{Fix}\left(\xi^{-1}\sigma\right).$$

Un bon candidat serait $x = \sum_{g \in \left\langle \xi^{-1}\sigma \right\rangle} g$, à condition de lui donner du sens. Or, $\left\langle \xi^{-1}\sigma \right\rangle$ est fini car

$$\left(\xi^{-1}\sigma\right)^n = \xi^{-n}\sigma^n = \mathrm{Id},$$

donc on peut regarder l'application K-linéaire

$$\varphi : \left\{ \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & \sum_{g \in \left\langle \xi^{-1}\sigma \right\rangle} g(x) = \\ & & x + \xi^{-1}\sigma(x) + ... + \xi^{-(n-1)}\sigma^{n-1}(x) \end{array} \right. .$$

Tout point de l'image de φ est fixe par $\xi^{-1}\sigma$ par construction, et φ est non identiquement nulle, sinon $\mathrm{Id}, \sigma, ..., \sigma^{n-1}$ seraient K-liés, *absurde* par Dedekind. D'où l'existence d'un $x_0 \neq 0$ dans L tel que $\sigma(x_0) = \xi x_0$.

Il reste à remonter la démonstration précédente, en posant $a = x_0^n$. Tout d'abord, $a \in K$ puisque

$$\sigma(a) = \sigma(x_0^n) = \sigma(x_0)^n = (\xi x_0)^n = x_0^n = a \implies a \in L^{\mathrm{Gal}\left(L/K\right)} = K$$

($K \subset L$ est galoisienne). Par ailleurs, $X^n - a$ se scinde en $\prod_{k=1}^n \left(X - \xi^k x_0\right)$, et pour conclure que L est un corps de décomposition de $X^n - a$, il suffit de montrer que L est engendré par les racines de $X^n - a$. Comme on sait déjà que

$$K \subset K[x_0] \subset K\left[x_0, x_0\xi, x_0\xi^2, ..., x_0\xi^{n-1}\right] \subset L$$

avec $[L : K] = n$, il suffit de montrer que x_0 est de degré n sur K, ce qui forcera l'égalité $K\left[x_0, x_0\xi, x_0\xi^2, ..., x_0\xi^{n-1}\right] = L$ comme souhaité.

Soit donc $\mu = \sum_{i=0}^d \lambda_i X^i$ polynôme minimal de x_0 sur K avec $\lambda_d \neq 0$. On a $d = [K[x_0] : K] \leq [L : K] = n$, et on veut $d = n$. En appliquant σ à l'égalité $\sum_{i=0}^d \lambda_i x_0^i = 0$, on obtient $0 = \sum \lambda_i \sigma\left(x_0^i\right) = \sum \lambda_i \sigma(x_0)^i = \sum \lambda_i \xi^i x_0^i$, d'où $0 = \sum_{i=1}^d \lambda_i \left(1 - \xi^i\right) x_0^i$ et $0 = \sum_{i=0}^{d-1} \lambda_{i+1}\left(1 - \xi^{i+1}\right) x_0^i$, ce qui impose par minimalité $\lambda_d\left(1 - \xi^d\right) = 0$ (coefficient dominant), d'où $\xi^d = 1$, $n \mid d$, $n \leq d$, et $n = d$ comme voulu.

3 Résolubilité par radicaux

Soit K un corps, $P \in K[X]$, $K \subset L$ une extension de décomposition d'un polynôme P. On aimerait pouvoir expliciter les racines de P à l'aide d'opérations algébriques rationnelles et de racines n-ièmes.

Définition.
Une extension $K \subset L$ est dite radicale élémentaire *si* $\left\{ \begin{array}{l} \exists x \in L \\ \exists n \geq 1 \end{array} \right.$ *tel que* $\left\{ \begin{array}{c} x^n \in K \\ L = K[x] \end{array} \right.$ (on rajoute une racine n-ième).

Une extension $K \subset L$ est dite radicale *si il y a une tour*

$$K = K_0 \subset K_1 \subset ... \subset K_n = L$$

où $K_i \subset K_{i+1}$ est radicale élémentaire. Ainsi $L = K[x_1, ..., x_n]$ où x_i est une racine n_i-ième d'un élément de $K[x_1, ..., x_{i-1}]$.

Une extension $K \subset L$ est dite résoluble (par radicaux) *si L est contenue dans une extension radicale de K finie sur L.*

On dit que $P \in K[X]$ est résoluble par radicaux *si le corps de décomposition de P est une extension résoluble de K.*

Remarques.
• Si $K \subset L$ est radicale et $K \subset L' \subset L$, alors $K \subset L'$ est radicale. Ainsi, pour montrer qu'une extension est radicale, il suffit de l'inclure dans un extension radicale.
• Si $K \subset L$ est résoluble et $K \subset L' \subset L$, alors $K \subset L'$ et $L' \subset L$ sont résolubles ;
• Si $K \subset L$ est radicale (resp. résoluble) et $K \subset L_1$ K-isomorphe à L, alors $K \subset L_1$ est radicale (resp. résoluble).

3.1 Extensions composées

Définition.
Soient $\left\{ \begin{array}{l} K \subset L_1 \\ K \subset L_2 \end{array} \right.$ *deux extensions contenues dans un même sur-corps L de K.*
On appelle extension composée *de L_1 et L_2 le sous-corps de L engendré par L_1 et L_2 :*

$$L_1 L_2 = K(L_1 \cup L_2) = L_1(L_2) = L_2(L_1).$$

On suppose désormais que L est une clôture algébrique $\overline{K}$ de K.

Lemme.
Soit A une K-algèbre intègre de dimension finie. Alors A est un corps.

Démonstration.
Soit $a \neq 0$ dans A ; alors la multiplication par a est un endomorphisme injectif donc surjectif, ainsi 1 est atteint.

Proposition.
Soit $K \subset L_1$ finie. Alors $L_2 \subset L_1 L_2$ est finie et

$$[L_1 L_2 : L_2] \leq [L_1 : K].$$

De plus, si on a égalité $[L_1 L_2 : L_2] = [L_1 : K]$, alors $L_1 \cap L_2 = K$.

Démonstration.
$L_2[L_1]$ est une L_2-algèbre intègre de dimension finie sur L_2, donc un corps. Une partie génératrice de $L_2[L_1]$ vu comme L_2-espace vectoriel est une base de L_1 comme K-espace vectoriel, d'où $[L_1 L_2 : L_2] \leq [L_1 : K]$.

D'autre part, on peut faire la même chose en prenant comme sous-corps commun $L_1 \cap L_2$: $[L_1L_2 : L_2] \leq [L_1 : L_1 \cap L_2] \leq [L_1 : K]$. Donc si on a égalité, $[L_1L_2 : L_2] = [L_1 : K]$, alors on a égalité partout et $K = L_1 \cap L_2$.

Corollaire.
Si L_1 et L_2 sont des extensions finies, alors

$$[L_1L_2 : K] \leq [L_1 : K]\,[L_2 : K]\,.$$

De plus, si on a égalité, alors $K = L_1 \cap L_2$.

Proposition.
• *Si $K \subset L_1$ est galoisienne, alors $L_2 \subset L_1L_2$ est galosienne.*
• *Si $\begin{cases} K \subset L_1 \\ K \subset L_2 \end{cases}$ sont galoisiennes, alors $\begin{cases} K \subset L_1L_2 \\ K \subset L_1 \cap L_2 \end{cases}$ sont galosiennes.*

Démonstration.
• L_1 est un corps de décomposition d'un P séparable de $K[X]$, donc P séparable dans $L_2[X]$, et alors L_1L_2 est un corps de décomposition de P sur L_2.
• $L_1L_2 = K(L_1 \cup L_2)$; L_i est un corps de décomposition d'un P_i séparable de $K[X]$, donc $P = P_1 \vee P_2$ séparable dans $L_1L_2[X]$, et alors L_1L_2 est un corps de décomposition de P sur K. De plus, $L_1 \cap L_2$ est séparable car L_1 ou L_2 l'est, et $\overline{K}$ est une clôture algèbrique de $L_1 \cap L_2$. Soit alors $\eta : L_1 \cap L_2 \longrightarrow \overline{K}$; a-t-on $\eta(L_1 \cap L_2) = L_1 \cap L_2$? On écrit $K \subset L_1 \cap L_2 \subset L_1L_2$, on peut prolonger η en $\widetilde{\eta}$ à L_1L_2 ; alors $\widetilde{\eta}(L_1) \subset L_1$ car $K \subset L_1$ est galoisienne, d'où $\eta(L_1 \cap L_2) = \widetilde{\eta}(L_1 \cap L_2) \subset \widetilde{\eta}(L_1) \cap \widetilde{\eta}(L_2) \subset \widetilde{\eta}(L_1 \cap L_2)$.

3.2 Calcul de $\mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right)$ en fonction de $\mathrm{Gal}\left({}^{L_1}\!/_{K}\right)$ et $\mathrm{Gal}\left({}^{L_2}\!/_{K}\right)$

Proposition.
Si $K \subset L_1$ est galoisienne, alors $L_2 \subset L_1L_2$ est galosienne, et

$$\mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right) \simeq \mathrm{Gal}\left({}^{L_1}\!/_{L_1\cap L_2}\right).$$

Démonstration.
On construit un morphisme injectif $\mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right) \longrightarrow \mathrm{Gal}\left({}^{L_1}\!/_{K}\right)$, puis on identifiera les images. On a clairement un morphisme $\mathrm{Gal}\left({}^{L_1L_2}\!/_{L_2}\right) \longrightarrow \mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right)$, et comme $\underbrace{K \subset L_1}_{\text{galoisienne}} \subset L_1L_2$, tout σ de $\mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right)$ stabilise L_1 (car L_1 normale). On a donc un morphisme $\mathrm{Gal}\left({}^{L_1L_2}\!/_{K}\right) \longrightarrow \mathrm{Gal}\left({}^{L_1}\!/_{K}\right)$, d'où par composition un morphisme $\varphi : \mathrm{Gal}\left({}^{L_1L_2}\!/_{L_2}\right) \longrightarrow \mathrm{Gal}\left({}^{L_1}\!/_{K}\right)$.

φ est injectif, car si $\sigma \in \mathrm{Gal}\left({}^{L_1L_2}\!/_{L_2}\right)$ s'envoie sur l'indentité, alors $\sigma_{|L_1} = \mathrm{Id}$, et comme $\sigma_{|L_2} = \mathrm{Id}$, $\sigma_{|L_1L_2} = \mathrm{Id}$.

Image de φ ? C'est un sous-groupe H de $\mathrm{Gal}\left({}^{L_1}\!/_{K}\right)$, déterminé par son sous-corps des points fixe L_1^H. On a déjà que $L_1 \cap L_2 \subset L_1^H$. D'autre part, si $x \in L_1^H$, $\forall \sigma \in \mathrm{Gal}\left({}^{L_1L_2}\!/_{L_2}\right)$, $\sigma(x) = x$, *i.e.* $x \in L_1 \cap L_2$.

Corollaire.
Si $K \subset L_1$ galoisienne, alors

$$[L_1L_2 : K] = [L_1L_2 : K]\,[L_2 : K] = [L_1 : L_1 \cap L_2]\,[L_2 : K]\,.$$

Démonstration.
la première égalité est triviale, la seconde vient de ce que $L_1 \cap L_2 \subset L_1$ est galoisienne.

3.3 Construction de la théorie des groupes : produit fibré

Soit G_1, G_2, H des groupes, $\varphi_i : G_i \longrightarrow H$ des morphismes. Le *produit fibré* $G_1 \times_H G_2$ est le sous-groupe de $G_1 \times G_2$ des (x, y) tels que $\varphi_1(x) = \varphi_2(y)$, *i.e.* tel que

$$\begin{array}{ccc} G_1 \times_H G_2 & \xrightarrow{pr_1} & G_1 \\ \downarrow pr_2 & & \downarrow \varphi_1 \\ G_2 & \xrightarrow{\varphi_2} & H \end{array}$$

commute.

Exemple. Soit n_1, n_2 des entiers, $\left\{ \begin{array}{l} \delta = n_1 \wedge n_2 \\ \mu = n_1 \vee n_2 \end{array} \right.$. Alors

$$\mathbb{Z}/n_1\mathbb{Z} \times_{\mathbb{Z}/\delta\mathbb{Z}} \mathbb{Z}/n_1\mathbb{Z} \simeq \mathbb{Z}/\mu\mathbb{Z}.$$

en effet, cela revient à dire que le système de congrunces $\left\{ \begin{array}{l} x \equiv x_1 \,[n_1] \\ x \equiv x_2 \,[n_2] \end{array} \right.$ possède une solution ssi $x_1 \equiv x_2 \,[\delta]$.

Théorème.
Soient $\left\{ \begin{array}{l} K \subset L_1 \\ K \subset L_2 \end{array} \right.$ *galoisiennes. Alors* $\left\{ \begin{array}{l} K \subset L_1 L_2 \\ K \subset L_1 \cap L_2 \end{array} \right.$ *sont galoisiennes, et*

$$\mathrm{Gal}\left(L_1L_2/K\right) \simeq \mathrm{Gal}\left(L_1/K\right) \times_{\mathrm{Gal}\left(L_1\cap L_2/K\right)} \mathrm{Gal}\left(L_2/K\right).$$

Démonstration.
$K \subset L_1 \subset L_1L_2$. Soit $j_k : \mathrm{Gal}\left(L_1L_2/K\right) \longrightarrow \mathrm{Gal}\left(L_k/K\right)$ obtenu par restriction. Alors

$$(j_1, j_2) : \mathrm{Gal}\left(L_1L_2/K\right) \longrightarrow \mathrm{Gal}\left(L_1/K\right) \times \mathrm{Gal}\left(L_2/K\right)$$

est un morphisme de groupe injectif.

Or, en composant j_k avec la restriction $r_k : \mathrm{Gal}\left(L_k/K\right) \longrightarrow \mathrm{Gal}\left(L_1\cap L_2/K\right)$, on obtient le même morphisme $\mathrm{Gal}\left(L_1L_2/K\right) \longrightarrow \mathrm{Gal}\left(L_1\cap L_2/K\right)$. Donc l'image est contenue dans le produit fibré $\mathrm{Gal}\left(L_1/K\right) \times_{\mathrm{Gal}\left(L_1\cap L_2/K\right)} \mathrm{Gal}\left(L_2/K\right)$. Montrons qu'ils ont même cardinal. On considère

$$(r_1, r_2) : \mathrm{Gal}\left(L_1/K\right) \times \mathrm{Gal}\left(L_2/K\right) \longrightarrow \mathrm{Gal}\left(L_1\cap L_2/K\right) \times \mathrm{Gal}\left(L_1\cap L_2/K\right)$$

dont l'image contient le sous-groupe diagonal. L'image réciproque de ce sous-groupe diagonal, modulo le noyau, est isomorphe à ce sous-groupe diagonal. Donc

$$\begin{array}{rcl} |\text{image réciproque}| & = & \left|\mathrm{Gal}\left(L_1\cap L_2/K\right)\right| |\mathrm{Ker}\,(r_1, r_2)| \\ & = & \left|\mathrm{Gal}\left(L_1\cap L_2/K\right)\right| |\mathrm{Ker}\, r_1|\, |\mathrm{Ker}\, r_2| \\ & = & \left|\mathrm{Gal}\left(L_1\cap L_2/K\right)\right| \left|\mathrm{Gal}\left(L_1/L_1\cap L_2\right)\right| \left|\mathrm{Gal}\left(L_2/L_1\cap L_2\right)\right| \\ & = & \underbrace{[L_1 \cap L_2 : K]\,[L_1 : L_1 \cap L_2]}\,[L_2 : L_1 \cap L_2] \\ & = & [L_1 : K]\,[L_2 : L_1 \cap L_2] \\ & = & [L_1L_2 : K] \\ & = & \left|\mathrm{Gal}\left(L_1L_2/K\right)\right|. \end{array}$$

Théorème.
• *Soient* $\left\{ \begin{array}{l} K \subset L_1 \\ K \subset L_2 \end{array} \right. \subset \overline{K}$. *Si elles sont radicales (resp. résolubles), alors* $K \subset L_1L_2$ *l'est aussi.*
• *Soit* $K \subset L$ *extension finie séparable. Si elle est radicale (resp. résoluble), alors la clôture galoisienne* $K \subset L^g$ *l'est aussi.*

Démonstration.

• (extensions radicales) Soient $\begin{matrix} K \subset E_1 \subset E_2 ... \subset E_n = L_1 \\ K \subset F_1 \subset F_2 ... \subset F_m = L_2 \end{matrix}$ des tours d'extensions élémentaires. Alors

$$L_1 = L_1K \subset L_1F_1 \subset L_1F_2 \subset ...L_1F_m = L_1L_2,$$

avec $F_{j+1} = F_j\left[y_{j+1}\right]$ où y_{j+1} est une racine n_{j+1}-ième de F_j, d'où $L_1F_{j+1} = L_1F_j\left[y_{j+1}\right]$.

(extensions résolubles) On est $K \subset L_i \subset F_i \subset \overline{K}$ où $K \subset F_j$ radicale. Quitte à remplacer F_1 et F_2 par des extensions isomorphes, on peut suppoeser qu'ils sont dans une même clôture algébrique de K.

• Le second point résulte du premier, car L^g est construite comme extension composée de tous les $\eta\left(L\right)$ où $\eta : L \longrightarrow \overline{K}$ morphisme dans une clôture algébrique de L.

Théorème.
Soit $K \subset L$ galoisienne, où $\operatorname{car} K = 0$. Alors $K \subset L$ est résoluble ssi $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$ est résoluble.

Rappel. Un groupe G est dit *résoluble* si on peut trouver une tour finie de sous-groupes

$$\{0\} = G_0 \subset G_1 \subset ... \subset G_n = G$$

avec $G_i \lhd G_{i+1}$ et ${}^{G_{i+1}}\!/_{G_i}$ abélien. Il revient au même de dire que la suite des sous-groupes dérivés stationne à $\{e\}$.

Proposition. Si G est résoluble, alors tout sous-groupe et tout quotient de G est résoluble.

Proposition. Soit G un groupe, $H \lhd G$. Si H et ${}^{G}\!/_{H}$ sont résolubles, alors G est résoluble.

Proposition. Si G est un groupe fini, alors G est résoluble ssi il exite une tour

$$\{0\} = G_0 \subset G_1 \subset ... \subset G_n = G$$

avec $G_i \lhd G_{i+1}$ et ${}^{G_{i+1}}\!/_{G_i}$ cyclique.

Proposition.
Si K contient toutes les racines n-ième de l'unité, si $K \subset L$ est radicale élémentaire de niveau n (i.e. $L = K\left[\alpha\right]$ avec $\alpha^n \in K$), alors elle est galoisienne de groupe de Galois cyclique. Et inversement.

Démonstration du théorème.
• On suppose que $K \subset L$ est radicale et que $[L : K] = n = \left|\mu_n\left(K\right)\right|$. Alors $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$ est résoluble. On dispose d'une tour

$$K \subset E_1 \subset ... \subset E_k \subset L.$$

On a déjà vu le cas $k = 1$ (extension cyclique), donc on peur supposer $k \geq 2$. On fait alors une récurrence sur le degré n de l'extension. On sait que $E_1 \subset L$ est radicale galoisienne, $[L : E_1] \mid [L : K] = n$ et E_1 contient toutes les racines $[L : E_1]$-ième de l'unité. Par récurrence, $\operatorname{Gal}\left({}^{L}\!/_{E_1}\right)$ est résoluble. $K \subset E_1$ est rédicale élémentaire, $[E_1 : K] \mid n$ et $n = \left|\mu_n\left(K\right)\right|$, donc on toutes les racines n-ièmes de l'unité. Donc l'extension est galoisienne, de groupe de Galois cyclique. $K \subset E_1$ galoisienne implique $\operatorname{Gal}\left({}^{L}\!/_{E_1}\right) \lhd \operatorname{Gal}\left({}^{L}\!/_{K}\right)$ et ${}^{\operatorname{Gal}\left({}^{L}\!/_{E_1}\right)}\!/_{\operatorname{Gal}\left({}^{L}\!/_{E_1}\right)} \simeq \operatorname{Gal}\left({}^{E_1}\!/_{K}\right)$, d'où $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$ résoluble.

• Cas général, $K \subset L$ galoisienne, résoluble. Soit $K \subset L \subset F$ avec $K \subset F$ radicale. On prend une clôture galoisienne E

$$\underbrace{K \subset L}_{\text{galoisienne}} \subset E$$

radicale galoisienne. $\operatorname{Gal}\left({}^{L}\!/_{K}\right)$ est un quotient de $\operatorname{Gal}\left({}^{E}\!/_{K}\right)$. Soit $n = [E : K]$, et $K \subset L'$ une extension de décomposition de $X^n - 1$ contenue dans Ω une clôture algébrique de E. $K \subset L$ est galoisienne radicale élémentaire. On considère ensuite $K \subset EL'$ radicale galoisienne. $L' \subset EL'$ est galoisienne ($K \subset E$ l'est) radicale. De plus, $[EL' : L'] \mid [E : K]$ donc on a les racines de l'unités qu'on veut. On applique le premier point à $L' \mid EL'$, d'où $\operatorname{Gal}\left({}^{EL'}\!/_{L'}\right)$ résoluble. D'autre part, $\operatorname{Gal}\left({}^{EL'}\!/_{L'}\right) \simeq \operatorname{Gal}\left({}^{E}\!/_{E\cap L'}\right) \subset \operatorname{Gal}\left({}^{E}\!/_{K}\right)$.

$$\overbrace{\underbrace{K \subset E \cap L'}_{\text{galoisienne}} \subset E}^{\text{gaoisienne}}$$

donc $\mathrm{Gal}\left({}^{E}\!/_{E\cap L'}\right) \lhd \mathrm{Gal}\left({}^{E}\!/_{K}\right)$ est résoluble.

$$\overbrace{\underbrace{K \subset E \cap L'}_{\text{galoisienne}} \subset E}^{\text{gaoisienne cyclique}}$$

donc le quotient $\mathrm{Gal}\left({}^{E\cap L'}\!/_{K}\right)$ est cyclique, donc $\mathrm{Gal}\left({}^{E}\!/_{K}\right)$ résoluble, donc $\mathrm{Gal}\left({}^{L}\!/_{K}\right)$ est résoluble.

Réciproque!!!!

• On suppose $\mathrm{Gal}\left({}^{L}\!/_{K}\right)$ résoluble, $[L:K] = n = |\mu_n(K)|$. Alors $K \subset L$ est radicale.
On a un groupe fini résoluble, donc on a un sous-groupe $H \lhd \mathrm{Gal}\left({}^{L}\!/_{K}\right)$ à quotient cyclique.

$$\underbrace{K \subset L^H}_{\text{galoisienne cyclique avec toutes les racines de 1}} \subset L$$

donc radicale élémentaire. Par récurrence sur le degré de l'extension, on montre que $L^H \subset L$ est radicale.

$\mathrm{Gal}\left({}^{L}\!/_{L^H}\right)$ résoluble comme sous-groupe cyclique de $\mathrm{Gal}\left({}^{L}\!/_{H}\right)$ résoluble, $\left[L:L^H\right] \mid n$, $K \subset L^H$ et donc toutes les racines n-ièmes qu'on veut. $L^H \subset L$ galoisienne car $K \subset L$ l'est, cqfd.

• Cas général. $K \subset L$, $[L:K] = n$, $K \subset L'$ corps de décomposition de $X^n - 1$ dans Ω, est galoisienne. Alors $K \subset LL'$ est galoisienne car L et L' le sont. $L' \subset LL'$ galoisienne, on a toutes les racines $[LL':L']$-ièmes de l'unité de L', $\mathrm{Gal}\left({}^{LL'}\!/_{L'}\right) \simeq \mathrm{Gal}\left({}^{L}\!/_{L\cap L'}\right) \subset \mathrm{Gal}\left({}^{L}\!/_{K}\right)$ résoluble, donc $\mathrm{Gal}\left({}^{LL'}\!/_{L'}\right)$ résoluble. $L' \subset LL'$ radicale, $K \subset L'$ radicla eémélentaire, donc$K \subset LL'$ radicale ($K \subset L \subset LL'$ implique L résoluble).

4 Calcul du groupe de Galois d'un polynôme $P \in \mathbb{Z}[X]$ via la réduction modulo p

Définition.
Soit $P \in \mathbb{Z}[X]$ unitaire séparable de degré n. On dispose d'un extension $\mathbb{Q} \subset L$ de décomposition de P (qui est galoisienne). On appelle groupe de Galois *de P sur $\mathbb{Q}$*

$$\underset{\mathbb{Q}}{\mathrm{Gal}}\, P = \mathrm{Gal}\left(L/\mathbb{Q}\right).$$

On rappelle que $\mathrm{Gal}_{\mathbb{Q}} P$ agit par permutation sur les racines de P, d'où $\mathrm{Gal}_{\mathbb{Q}} P \hookrightarrow \mathfrak{S}_n$.

4.1 Lecture de $\mathrm{Gal}_{\mathbb{Q}} P$ dans la décomposition de P en facteurs irréductibles

Proposition (calcul du polynôme minimal par action du groupe de Galois).
Soit $K \subset L$ galoisienne de groupe de Galois G. Le polynôme minimal d'un $\alpha \in L$ sur K est donné par

$$\mu_\alpha = \prod_{\sigma \in G} \left(X - \sigma(\alpha)\right).$$

Démonstration.
$\prod_{\sigma\in G}(X-\sigma(\alpha))$ est à coefficients dans $L^G = K$. De plus, tous les $\sigma(\alpha)$ sont des racines de μ_α, donc $\prod_{\sigma\in G}(X-\sigma(\alpha)) \mid \mu_\alpha$. Comme μ_α est irréductible, on a égalité.

Proposition.
Soit $K \subset L$ galoisienne et $P \in K[X]$ unitaire scindé simple dans L. Soit Ω l'ensemble des racines de P. On partitionne Ω en orbites sous l'action de $G = \mathrm{Gal}\left(L/K\right)$, mettons $\Omega = \coprod_{i=1}^{k} \Omega_i$, et on pose $F_i = \prod_{\alpha\in\Omega_i}(x-\alpha)$. Alors $F_i \in K[X]$, est irréductible, et $P = \prod_{i=1}^{k} F_i$.

Démonstration.
Pour $\alpha \in \Omega_i$, on a $G(\alpha) = \Omega_i$, donc les coefficients de F_i sont stables par G et sont donc dans K. D'après la proposition précédente, F_i est le polynôme minimal de l'un quelconque des $\alpha \in \Omega_i$, a fortiori est irréductible.

Intérêt.
Si G est cyclique engendré par g_0, on peut décrire les orbites Ω_i en regardant la décomposition de g_0 (vu dans $\mathfrak{S}_n$) en cycles à support disjoints. Les longueurs des cycles sont données par les degrés des facteurs irréductibles de P. Ainsi, si ces degrés sont $n_1, ..., n_k$, G est engendré par un élément conjugué à

$$(1, ..., n_1)(n_1+1, ..., n_1+n_2)...(n_1+...+n_{k-1}, ..., n).$$

On connait déjà une classe de groupes de Galois cycliques, les $\mathrm{Gal}\left(\mathbb{F}_q/\mathbb{F}_p\right)$, qui sont engendrés par Fr. On va donc ramener l'étude du groupe de Galois du polynôme P aux $\mathrm{Gal}\left(\mathbb{F}_q/\mathbb{F}_p\right)$ en réduisant modulo p (où p premier à choisir opportunément...).

En notant $\overline{P}$ le réduit de P modulo p et L un corps de décomposition de $\overline{P}$ sur $\mathbb{F}_p$, un bon candidat pour $\mathrm{Gal}\left(\mathbb{F}_q/\mathbb{F}_p\right)$ est $\mathrm{Gal}_{\mathbb{F}_p}\overline{P} = \mathrm{Gal}\left(L/\mathbb{F}_p\right)$, d'où l'attention particulière qu'on lui porte.

4.2 Réduction modulo p

Soit $P \in \mathbb{Z}[X]$ unitaire. Pour p premier, on note $\overline{P} \in \mathbb{F}_p[X]$ obtenu en réduisant P modulo p. On pose alors

$$\begin{cases} \mathbb{Q} \subset E \text{ un corps de décomposition de } P \\ \mathbb{F}_p \subset L \text{ un corps de décomposition de } \overline{P} \end{cases}.$$

On veut "comparer" l'étude de E et $\mathrm{Gal}_{\mathbb{Q}} P$ à celle de L et $\mathrm{Gal}_{\mathbb{F}_p}\overline{P}$.

4.2.1 Construction d'un corps de décomposition de P

Soient $\xi_1, ..., \xi_n$ les racines de P dans E. On a donc

$$E = \mathbb{Q}[\xi_1, ..., \xi_n] \simeq \mathbb{Z}[\xi_1, ..., \xi_n] \otimes \mathbb{Q} = A \otimes \mathbb{Q}$$

en posant $A = \mathbb{Z}[\xi_1, ..., \xi_n]$.

Proposition.
A est un $\mathbb{Z}$-module libre de type fini de rang $[E : \mathbb{Q}]$ (on dit que c'est est un réseau *dans E).*

Démonstration.
A est de type fini car engendré par les $\xi_1^{\alpha_1}...\xi_k^{\alpha_k}$ où $\alpha_i < n$, et est sans torsion car E est sans torsion. Puisque $\mathbb{Z}$ est principal, A est libre, mettons $A = \mathbb{Z}u_1 + ... + \mathbb{Z}u_r$ où $(u_1, ..., u_r)$ est un $\mathbb{Z}$-base de A. Montrons que c'est une $\mathbb{Q}$-base de E, ce qui nous donnera $r = [E : \mathbb{Q}]$.

En effet, $(u_1, ..., u_r)$ est $\mathbb{Z}$-libre, donc $\mathbb{Q}$-libre (en tuant les dénominateurs d'une relation de liaison), et génère $\mathbb{Q}$-linéairement E puisque

$$\begin{aligned} & x \in E = \mathbb{Q}[r_1, ..., r_n] \\ \Longrightarrow \quad & \exists k \in \mathbb{N} \text{ tel que } kx \in \mathbb{Z}[r_1, ..., r_n] = A \\ \Longrightarrow \quad & \exists k \in \mathbb{N} \text{ tel que } kx = \sum_{i=1}^{r} \lambda_i u_i \text{ où } \lambda_i \in \mathbb{Z} \\ \Longrightarrow \quad & x = \sum_{i=1}^{r} \left(\frac{\lambda_i}{k}\right) u_i \text{ où } \frac{\lambda_i}{k} \in \mathbb{Q}. \end{aligned}$$

Contruisons à présent une extension de décompositon L de $\overline{P}$ sur $\mathbb{F}_p$ à l'aide de A.

Proposition.
Soit $\mathfrak{M}$ un idéal maximal de A contenant pA. Alors $L = {}^{A}\!/_{\mathfrak{M}}$ est un corps de décomposition de $\overline{P}$ sur $\mathbb{F}_p$.

Démonstration.
Un bon candidat pour un $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$-espace vectoriel de dimension finie est l'anneau quotient ${}^{A}\!/_{pA}$, mais il peut très bien ne pas être un corps. D'où l'idée de considérer $pA \subset \mathfrak{M} \subset A$.

Notons $\pi : A \longrightarrow L$ la projection canonique modulo $\mathfrak{M}$. On munit $L = \pi(A)$ de la loi externe issue de la multiplication $\overline{\lambda} \cdot \pi(a) = \pi(\lambda a)$, ce qui transforme en quelque sorte π en un morphisme d'algèbres de la $\mathbb{Z}$-algèbre A dans la $\mathbb{F}_p$-algèbre L.

L est alors une extension finie de $\mathbb{F}_p$. En effet, L est clairement un corps, et si $(u_1, ..., u_r)$ est une $\mathbb{Z}$-base de A, alors $(\pi(u_1), ..., \pi(u_r))$ est une famille $\mathbb{F}_p$-génératrice de $\pi(A) = L$, donc L est finiment généré (linéairement), donc de dimension finie sur $\mathbb{F}_p$.

Enfin, en remarquant que π envoie les scalaires de $\mathbb{Z}$ sur ceux de $\mathbb{F}_p$, on peut dire que L est un corps de décomposition de $\overline{P}$ puisque

$$\overline{P} = \pi(P) = \pi\left(\prod_{i=1}^{n}(X - \xi_i)\right) = \prod_{i=1}^{n}(X - \pi(\xi_i))$$

est scindé sur L et que

$$L = \pi(A) = \pi(\mathbb{Z}[\xi_1, ..., \xi_n]) = \mathbb{F}_p[\pi(\xi_1), ..., \pi(\xi_n)]$$

est algébriquement engendré par les $\pi(\xi_i)$.

La construction effectuée est naturelle, au sens suivant :

Proposition.
Soit $\mathbb{F}_p \subset K$ une extension finie. On équivalence entre :
- *K est un corps de décomposition de $\overline{P}$;*
- *Il existe un morphisme d'anneaux surjectif $\mathbb{Z}[\xi_1, ..., \xi_n] \longrightarrow K$.*

Démonstration.
$(i) \implies (ii)$ On a déjà construit un corps de décomposition L. Par unicité à isomorphisme φ près, $\varphi \circ \pi$ est un morphisme d'anneaux surjectif.
$(ii) \implies (i)$ Soit $\theta : A \longrightarrow K$ un morphisme d'anneaux surjectif. Comme pour la projection π, on a $\theta(\mathbb{Z}) = \mathbb{F}_p$, donc K est algébriquement $\mathbb{F}_p$-engendré par les $\theta(\xi_i)$, et $\overline{P} = \theta(P) = \prod (X - \theta(r_i))$ est scindé sur K.

Ainsi, si K est un corps de décomposition de $\overline{P}$, il existe un morphisme d'anneaux de A dans K qui envoie surjectivement les racines de P sur celles de $\overline{P}$. De plus, la démonstration qui précède montre que c'est le cas de tous les morphismes d'anneaux de A dans K.

Remarque. Tout morphisme d'anneaux φ de A dans L est nécessairement surjectif. En effet,

$$\operatorname{Im}\varphi = \varphi(A) = \varphi(\mathbb{Z}[\xi_1, ..., \xi_n]) = \mathbb{F}_p[\varphi(\xi_1), ..., \varphi(\xi_n)] = L$$

4.2.2 Injection de $\mathrm{Gal}_{\mathbb{F}_p}\overline{P}$ dans $\mathrm{Gal}_{\mathbb{Q}} P$

Propriété.
Soit $P \in \mathbb{Z}[X]$ unitaire, p premier, $\overline{P} \in \mathbb{F}_p[X]$ son réduit modulo p. Alors

$$\overline{P} \text{ séparable} \implies P \text{ séparable.}$$

Démonstration.
$\operatorname{disc}\overline{P} \in \mathbb{F}_p$ est la réduction modulo p de $\operatorname{disc} P \in \mathbb{Z}$.

Lemme.
Si P est séparable, l'action à droite de $\mathrm{Gal}_{\mathbb{Q}} P$ sur $\mathrm{Hom}(A, L)$ définie par $\sigma \cdot \varphi = \varphi \circ \sigma$ est libre et transitive.

Démonstration.
• *Liberté.*
Si $\sigma \cdot \varphi = \varphi$, *i.e.* $\varphi \circ \sigma = \varphi$, on se restreint à Ω (ensemble des racines de P) : $\varphi \circ \sigma_{|\Omega} = \varphi_{|\Omega}$; comme σ stabilise Ω, on a même $\varphi_{|\Omega} \circ \sigma_{|\Omega} = \varphi_{|\Omega}$. Or, on sait que φ envoie surjectivement les racines de P sur celles de P', donc $\varphi_{|\Omega} : \Omega \longrightarrow \overline{\Omega}$ est surjectif, et P étant séparable, on a $|\Omega| = \left|\overline{\Omega}\right| = \deg P$, d'où $\varphi_{|\Omega}$ injective. On en déduit $\sigma_{|\Omega} = \mathrm{Id}$, d'où $\sigma = \mathrm{Id}$ (car Ω engendre E).
• *Transitivité.*
Fixons φ dans $\mathrm{Hom}(A, L)$. Posons $N = |\mathrm{Gal}_{\mathbb{Q}} P|$, et soit $\{\varphi_1, ..., \varphi_N\} = \{\varphi \circ \sigma\,;\, \sigma \in \mathrm{Gal}_{\mathbb{Q}} P\}$ l'orbite de φ sous l'action de $\mathrm{Gal}_{\mathbb{Q}} P$. Puisque l'action est libre, l'orbite est de cardinal N exactement.
Soit ensuite $\psi \in \mathrm{Hom}(A, L)$. S'il n'est pas parmi les φ_i, on aurait $N+1$ morphismes d'anneaux deux à deux distincts, donc linéairement indépendants d'après Dedekind (dans le monoïde multiplicatif A). Il suffit donc de montrer qu'ils sont liés pour conclure.
Cherchons $\lambda_i \in L$ tel que $\sum_{i=1}^{N+1} \lambda_i \varphi_i = 0$ (on a posé $\varphi_{N+1} = \psi$). Puisque $N = |\mathrm{Gal}_{\mathbb{Q}} P| = [E : \mathbb{Q}] = \mathrm{rg}\, A$, on dispose d'une base $(u_1, ..., u_N)$ de A de cardinal N, donc nécessairement $(\lambda_1, ..., \lambda_{N+1})$ est solution du système

$$\begin{cases} \sum_{i=1}^{N+1} \lambda_i \varphi_i(u_1) = 0 \\ \qquad\qquad ... \\ \sum_{i=1}^{N+1} \lambda_i \varphi_i(u_N) = 0 \end{cases}$$

qui a N équations et $N+1$ inconnues, donc qui a au moins une solution $\left(\mu_1, ..., \mu_{N+1}\right)$ non nulle dans L^{N+1}. Montrons réciproquement qu'une telle solution convient.
Soit $a \in A$, que l'on décompose en $a = \sum_{j=1}^{N} a_j u_j$. Alors

$$\sum_{i=1}^{N+1} \mu_i \varphi_i(a) = \sum_{i=1}^{N+1} \mu_i \varphi_i \left(\sum_{j=1}^{N} a_j u_j \right) = \sum_{i=1}^{N+1} \mu_i \sum_{j=1}^{N} \overline{a_j} \varphi_i(u_j) = \sum_{j=1}^{N} \overline{a_j} \underbrace{\sum_{i=1}^{N+1} \mu_i \varphi_i(u_j)}_{=0} = 0,$$

d'où $\sum_{i=1}^{N+1} \mu_i \varphi_i = 0$, *CQFD.*

Remarque. Soit G agissant librement et transitivement sur un ensemble E. Alors G est en bijection avec E via n'importe quelle application $\left\{ \begin{array}{ccc} G & \longrightarrow & E \\ g & \longmapsto & ge \end{array} \right.$ où $e \in E$.

Théorème.
Soit $P \in \mathbb{Z}[X]$ *unitaire,* p *premier,* $\left\{ \begin{array}{l} \mathbb{Q} \subset E \text{ un corps de décomposition de } P \\ \mathbb{F}_p \subset L \text{ un corps de décomposition de } \overline{P} \end{array} \right.$ *. On suppose que* $\overline{P}$ *est séparable. On dispose alors d'un morphisme de groupes injectif* $g : \left\{ \begin{array}{ccc} \mathrm{Gal}_{\mathbb{F}_p} \overline{P} & \longrightarrow & \mathrm{Gal}_{\mathbb{Q}} P \\ \sigma & \longmapsto & g(\sigma) \end{array} \right.$ *vérifiant*

$$\rho \circ g(\sigma) = \sigma \circ \rho.$$

où $\rho \in \mathrm{Hom}(A, L)$ *et* $h = \rho_{|\Omega}^{-1}$ *est une bijection de* $\overline{\Omega} \longrightarrow \Omega$.
En particulier, l'action de $\mathrm{Gal}_{\mathbb{F}_p} \overline{P}$ *sur* Ω *se ramène à l'action de* $\mathrm{Gal}_{\mathbb{Q}} P$ *sur* Ω *modulo la conjugaison*

$$g(\sigma) = h \circ \sigma \circ h^{-1}$$

ou le diagramme commutatif

$$\begin{array}{ccc} \overline{\Omega} & \stackrel{h}{\longrightarrow} & \Omega \\ \sigma \downarrow & & \downarrow g(\sigma) \\ \overline{\Omega} & \stackrel{h}{\longrightarrow} & \Omega \end{array} .$$

Démonstration.
Donnons-nous un $\psi \in \mathrm{Hom}(A, L)$. Alors $\forall \sigma \in \mathrm{Gal}_{\mathbb{F}_p} \overline{P}$, $\sigma \circ \psi \in \mathrm{Hom}(A, L)$, donc par transitivité/liberté de l'action à droite de $\mathrm{Gal}_{\mathbb{Q}} P$ sur $\mathrm{Hom}(A, L)$ (cf lemme),

$$\exists ! \tau \in \underset{\mathbb{Q}}{\mathrm{Gal}}\, P \text{ tel que } \sigma \circ \psi = \psi \circ \tau.$$

Ceci détermine une application $g : \left\{ \begin{array}{ccc} \mathrm{Gal}_{\mathbb{F}_p} \overline{P} & \longrightarrow & \mathrm{Gal}_{\mathbb{Q}} P \\ \sigma & \longmapsto & \tau \end{array} \right.$ vérifiant $\sigma \circ \psi = \psi \circ g(\sigma)$ et qui est un morphisme de groupes injectif. En effet, d'une part on a

$$\begin{array}{rcl} \psi \circ g(\sigma_1 \sigma_2) & = & (\sigma_1 \sigma_2) \circ \psi = \sigma_1 \circ (\sigma_2 \circ \psi) \\ & = & \sigma_1 \circ (\psi \circ g(\sigma_2)) = (\sigma_1 \circ \psi) \circ g(\sigma_2) \\ & = & \psi \circ g(\sigma_1) \circ g(\sigma_2) = \psi \circ (g(\sigma_1)\, g(\sigma_2)) \end{array}$$

et ψ est par ailleurs injective ? ? ? ? ? ; d'autre part,

$$g(\sigma) = \mathrm{Id} \implies \sigma \circ \psi = \psi \implies \sigma = \mathrm{Id}$$

par liberté de l'action à droite (cf lemme), d'où l'injectivité de g.
De plus, ψ induit une bijection $\Omega \longrightarrow \overline{\Omega}$; on prend alors $h = \psi_{|\Omega}^{-1}$, et toutes les vérification tombent.

Le principal résultat est l'injection de $\mathrm{Gal}_{\mathbb{F}_p} \overline{P}$ dans $\mathrm{Gal}_{\mathbb{Q}} P$, injection qui est une conjugaison quand on ne regarde que l'action sur les racines (la plus facile à lire).
Ainsi, en réduisant $\overline{P}$ modulo différents p et en factorisant $\overline{P}$ selon ses facteurs irréductibles, on obtient des éléments de $\mathrm{Gal}_{\mathbb{F}_p} \overline{P}$ (des produits de cycles dont les longueurs sont les degrés des facteurs irréductibles de $\overline{P}$) qui s'injectent par conjugaison dans $\mathrm{Gal}_{\mathbb{Q}} P \hookrightarrow \mathfrak{S}_\Omega$. Si on obtient ainsi des générateurs de $\mathfrak{S}_\Omega$ à travers différents p, on aura directement $\mathrm{Gal}_{\mathbb{Q}} P \simeq \mathfrak{S}_\Omega$.
On est donc amené à chercher les degrés des facteurs irréductibles d'un polynôme unitaire $\overline{P} \in \mathbb{F}_p[X]$.

4.2.3 Recherche de facteurs irréductibles

Soit Q un polynôme de $\mathbb{F}_p[X]$. La proposition suivante montre que la recherche des facteurs irréductibles de degré d de Q doit passer par le calcul du pgcd $Q \wedge \left(X^{p^d} - X\right)$.

Proposition.
Si Q admet un facteur irréductible de degré d, ce facteur divise nécessairement $Q \wedge \left(X^{p^d} - X\right)$.

Démonstration.
Soit A un facteur irréductible de Q de degré d. Considérons un corps K de décomposition de A sur $\mathbb{F}_p$, par exemple $K = {}^{\mathbb{F}_p[X]}\!/_{(A)}$. K est de cardinal $p^{\deg A} = p^d$, donc $K \simeq \mathbb{F}_{p^d}$. Ainsi, tous les éléments de K sont racines de $X^{p^d} - X$, et en regardant le degré on peut écrire $X^{p^d} - X = \prod_{\lambda \in K}(X - \lambda)$, de sorte que A divise $X^{p^d} - X$ dans $K[X]$. Or, A et $X^{p^d} - X$ sont déjà dans $\mathbb{F}_p[X]$, donc le quotient $\frac{X^{p^d} - X}{A}$ est en fait dans $\mathbb{F}_p[X]$, *CQFD.*

Proposition.
Si Q admet une racine dans $\mathbb{F}_{p^d}$ qui n'est dans aucun des $\mathbb{F}_{p^{d'}}$ pour d' divisant strictement d, alors Q admet un facteur irréductible de degré d.

Démonstration.
Soit ξ une racine de Q dans $\mathbb{F}_{p^d}$ comme dans l'énoncé et μ le polynôme minimal de ξ sur $\mathbb{F}_p$. Un corps de rupture de μ est un sous-corps de $\mathbb{F}_{p^d}$, donc un certain $\mathbb{F}_{p^{d'}}$ où d' divise d. Comme de plus un tel corps est de degré $\deg \mu$ sur $\mathbb{F}_p$, on en déduit que $\deg \mu$ divise d. Or, $\deg \mu$ ne peut diviser strictement d, sinon ξ serait racine de Q dans $\mathbb{F}_{p^{\deg \mu}}$, ce qui est exclu par hypothèse. Finalement, μ est irréductible et de degré d, d'où la conclusion.

Corollaire.
Q admet un facteur irréductible de degré d ssi $Q \wedge \left(X^{p^d} - X\right)$ a une racine dans $\mathbb{F}_{p^d}$ qui n'est dans aucun des $\mathbb{F}_{p^{d'}}$ pour d' divisant strictement d.

Démonstration.
Le sens direct fait l'objet de la première proposition, l'autre sens découle de la seconde.

Exemple : calcul du groupe de Galois de $P = X^5 - X - 1$.
Modulo 2, $\overline{P} = X^5 + X + 1$. On cherche les degrés des facteurs irréductibles de $\overline{P}$. Aucun ne peut être de degré 1, car $\overline{P}$ n'a pas de racines dans $\mathbb{F}_2$. Pour les facteurs de degré deux, on calcule $\left(X^5 + X + 1\right) \wedge \left(X^4 - X\right) = X^2 + X + 1$, qui a une racine dans $\mathbb{F}_4$ (rappelons incidemment que $\mathbb{F}_4 \simeq {}^{\mathbb{F}_2[X]}\!/_{X^2+X+1}$...) et aucune dans $\mathbb{F}_2$, donc P admet un facteur irréductible d'ordre deux. P se factorise par conséquent sous la forme $(\deg 2)(\deg 3)$; il y a donc dans Gal vu comme sous-groupe des permutations des racines un élément σ qui se factorise en un produit d'une transposition et d'un cycle de longueur 3. En particulier, Gal contient σ^3 qui est une transposition.

Modulo 3, $\overline{P} = X^5 - X - 1$. Même topo : on cherche les degrés des facteurs irréductibles de $\overline{P}$. Aucun de degré 1 car pas de racines dans $\mathbb{F}_3$. On regarde alors $\left(X^5 + X + 1\right) \wedge \left(X^9 - X\right) = 1$, d'où pas de facteur de degré 3. Donc P est irréductible sur $\mathbb{F}_3$ et Gal contient un 5-cycle.

Gal contient une transposition et un 5-cycle, donc vaut $\mathfrak{S}_5$ tout entier.

Ainsi $P = X^5 - X - 1$ n'est pas résoluble par radicaux, car la suite des dérivés de $\mathfrak{S}_5$ stationne à $\mathfrak{A}_5$, donc $\mathfrak{S}_5$ n'est pas résoluble.