Introduction à la théorie de Galois

Cédric Astier-David

2014

Table des matières

La théorie de Galois a pour objet l'étude des extensions de corps **commutatifs**. Dans toute la suite, les corps considérés seront donc toujours commutatifs.

1 Rappels

1.1 Extensions de corps

On rappelle sans démonstration quelques définitions et résultats de base sur les extensions de corps, qui serviront à de multiples reprises dans la suite.

Définition 1.1.1.
Soit K un corps (commutatif).

1. *Une extension de K est un corps E contenant K comme sous-corps. On la note E/K.*
2. *On appelle **degré** de E/K la dimension de E comme K-espace vectoriel. On le note $[E : K]$. Lorsque celui-ci est fini, l'extension est dite **finie**.*
3. *Une **sous-extension** L de E/K est un sous-corps de E contenant K.*
4. *Si S est une partie de E, l'extension de K engendrée par S, notée $K(S)$, est le plus petit sous-corps de E contenant K et S.*
5. *Un élément α de E est dit **algébrique** sur K s'il est racine d'un polynôme non nul de $K[X]$. Il est dit transcendant dans le cas contraire.*
6. *On dit que E/K est une extension algébrique si tout élément de E est algébrique sur K.*
7. *Soient E/K une extension algébrique et $\alpha \in E$. Le **polynôme minimal** de α sur K, noté $Irr(\alpha, K)$ est l'unique générateur irréductible unitaire de l'idéal annulateur $\{P \in K[X] \ ; \ P(\alpha) = 0\}$.*

Remarque :
Toute extension finie est algébrique (l'implication inverse est fausse : l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est une extension algébrique de degré infini).

Proposition 1.1.2.
Soient K un corps et α un élément d'une extension de K.
Alors α est algébrique sur K si et seulement si $K(\alpha)/K$ est de degré finie.
Dans ce cas, $(1, \alpha, \ldots, \alpha^{m-1})$ est une K-base de $K(\alpha)$, où m est le degré du polynôme minimal de α sur K.

Proposition 1.1.3.
Soient K un corps et $\alpha_1, \ldots, \alpha_n$ des éléments d'une extension de K.
Alors $K(\alpha_1, \ldots, \alpha_n)$ est l'ensemble des fractions rationnelles sur K en les α_i $(1 \leq i \leq n)$.
*Si tous les α_i sont algébriques, alors $K(\alpha_1, \ldots, \alpha_n)$ est l'ensemble des **polynômes** sur K en les α_i : $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$*

Définition 1.1.4.
Soit K un corps et P un polynôme non constant de $K[X]$.

- *Un **corps de rupture** de P sur K est une extension L/K telle que L contient une racine α de P et L est engendré par α. ($L = K(\alpha)$)*
- *Un **corps de décomposition** (ou corps des racines) de P sur K est une extension E/K telle que E contient toutes les racines $\alpha_1, \ldots, \alpha_n$ de P et E est engendré par ces racines. ($E = K(\alpha_1, \ldots, \alpha_n)$)*

Remarques : Un corps de rupture et un corps de décomposition existent toujours. Attention, il n'y a pas unicité du corps de décomposition, à moins de se placer dans une clôture algébrique de K (par exemple $\mathbb{C}$ pour $K = \mathbb{Q}$). En revanche (*cf.* 1.1.9), tous les corps de décomposition sont isomorphes, il y a donc unicité **à isomorphisme près**.
On notera donc $D_K(P)$ **un** corps de décomposition de P sur K choisi arbitrairement, à moins que les racines $\alpha_1, \ldots, \alpha_n$ soient déterminées, auquel cas on posera

$$D_K(P) := K(\alpha_1, \ldots, \alpha_n)$$

Proposition 1.1.5 (formule de multiplicativité des degrés)**.**
Soient L/K et M/L deux extensions de corps.
Alors M/K est de degré fini si et seulement si L/K et M/L sont de degrés finis.
Dans ce cas, $[M : K] = [M : L][L : K]$

Corollaire 1.1.6.

- *Une extension finie de K est de la forme $K(\alpha_1, \ldots, \alpha_n)$, avec α_i algébrique $\forall i$;*
- *Un corps de décomposition est de degré fini (et donc algébrique).*

Proposition 1.1.7.
Soient K et L deux corps et P dans $K[X]$ tels que $K \subset L \subset D_K(P)$. Alors $D_K(P)$ est aussi un corps de décomposition de P sur L.

Notation : Si $i : K \to K'$ est un morphisme de corps (*ie* un morphisme d'anneaux entre deux corps), on notera $\bar{i} : K[X] \to K'[X]$ son extension naturelle aux anneaux de polynômes.

Proposition 1.1.8.
Soient K un corps, soit $i : K \to K$ un isomorphisme d'anneaux et soit $P \in K[X]$ un polynôme irréductible.
Soient $K(\alpha)$ un corps de rupture de P et $K(\beta)$ un corps de rupture de $\bar{i}(P)$.
Alors il existe un isomorphisme d'anneaux $\widetilde{i} : K(\alpha) \to K(\beta)$ qui prolonge i et envoie α sur β.
En particulier, deux corps de rupture d'un même polynôme irréductible sont isomorphes (prendre $i = id_K$).

Proposition 1.1.9.
Soient K_1, K_2 deux corps, soit $f : K_1 \to K_2$ un isomorphisme d'anneaux et soit P un polynôme de $K_1[X]$.
Soient L_1/K_1 un corps de décomposition de P et L_2/K_2 un corps de décomposition de $\overline{f}(P)$.
Alors il existe un isomorphisme d'anneaux $\widetilde{f} : L_1 \to L_2$ qui prolonge f.
En particulier, deux corps de décomposition d'un même polynôme sont isomorphes.

On pourra appliquer ce résultat à la suite du précédent pour obtenir un automorphisme d'un corps de décomposition $D_K(P)$ qui relie deux racines α et β d'un même polynôme irréductible P de $K[X]$ et qui fixe K ($i = id_K$).

1.2 Le groupe symétrique $\mathfrak{S}_n$

On note ε le morphisme signature.

Proposition 1.2.1.
a) $\forall n \geq 2$, $\mathfrak{S}_n$ *est engendré par les transpositions de la forme* $(i\ i+1)$, $i \in \{1, \ldots, n-1\}$
b) $\forall n \geq 3$, *le groupe alterné* $\mathfrak{A}_n$ *est engendré par les 3-cycles*

Proposition 1.2.2.
Si p est un nombre premier, alors $\mathfrak{S}_p$ est engendré par toute partie $\{\sigma, \tau\}$ formée d'un p-cycle et d'une transposition.

Démonstration.

τ est de la forme $(i\ j)$ avec $i, j \in \{1, \ldots, p\}$ distincts. σ étant un p-cycle, il existe un entier k tel que $\sigma^k(i) = j$. Comme $\sigma^k \in < \sigma >$ et $\sigma^k \neq id$, σ est d'ordre p (car p est premier) donc est encore un p-cycle. Quitte à renuméroter l'ensemble $\{1, \ldots, p\}$, on peut se ramener au cas où $\tau = (1\ 2)$ et $\sigma^k = (1\ 2 \ldots p)$ (par la permutation $\phi \in \mathfrak{S}_p$ définie par $\phi^{-1}(s) = (\sigma^k)^{s-1}(i)$, $s \in \{1, \ldots, p\}$).
Montrons donc que $\mathfrak{S}_p = < (1\ 2), (1\ 2 \ldots p) > := G$. (vrai même si p n'est pas premier)
Il suffit d'après la proposition 1.2.1 *a)* de voir que G contient les transpositions de la forme $(i\ i+1)$. Or $\sigma^k \tau (\sigma^k)^{-1} = (2\ 3)$, et $\sigma^k (i\ i+1)(\sigma^k)^{-1} = (i+1\ i+2)$ pour tout i dans $\{1, \ldots, p-2\}$, donc on trouve par récurrence que $(i\ i+1) \in G$ pour tout i dans $\{1, \ldots, p-1\}$, donc $G = \mathfrak{S}_p$.

□

Proposition 1.2.3.
Soit $\sigma \in \mathfrak{S}_n$. Alors

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

2 Extensions galoisiennes

Nous allons ici nous intéresser à la théorie de Galois dite "classique" (à distinguer des théories "inverse" ou "infinie" développées par la suite), qui ne traite que le cas des extensions finies. Passées les premières définitions, et sauf exception, nous ne considèrerons donc que des extensions E/K **finies**. A ces extensions, nous allons associer un groupe

$$Gal(E|K) := \{\sigma \in Aut(E) \ ; \ \sigma_{|K} = id_K\} := Aut_K(E)$$

Les éléments de $Gal(E|K)$ sont ainsi les K-automorphismes de corps de E, *ie* les automorphismes de E qui fixent K. $Gal(E|K)$ est bien un groupe : $Gal(E|K) = \cap_{x \in K} Stab(x)$, où $Stab(x)$ est le stabilisateur (ou sous-groupe d'isotropie) de x pour l'action de $Aut(E)$ sur E.

Définition 2.0.1.
*$Gal(E|K)$ est appelé le **groupe de Galois** de E sur K.*
Si P est un polynôme de $K[X]$, on note $Gal(P|K) := Gal(D_K(P)|K)$ le groupe de Galois "du" corps de décomposition de P sur K (bien défini à isomorphisme près, cf. 1.1.9 et remarque page 3).

2.1 Définition et caractérisations

Définition 2.1.1.
Soit K un corps et E/K une extension algébrique.

1. *On dit que E/K est une extension **séparable** si le polynôme minimal sur K de tout élément de E n'admet que des racines simples (dans une clôture algébrique de K).*
2. *On dit que E/K est une extension **normale** si tout élément de E est racine d'un polynôme non nul de $K[X]$ scindé sur E.*

Proposition 2.1.2.
Les extensions algébriques d'un corps K fini ou de caractéristique nulle sont toutes séparables.
Plus précisément, tout polynôme irréductible P de $K[X]$ a ses racines simples dans $D_K(P)$.

Démonstration.

Supposons K fini ou de caractéristique nulle. Soit $P \in K[X]$ irréductible.
Par l'absurde, supposons que P possède une racine a au moins double ($deg(P) \geq 2$) : $P = (X-a)^\alpha Q$ avec $\alpha \geq 2$ et $Q(a) \neq 0$.

$$\text{On a : } P' = \alpha(X-a)^{\alpha-1}Q + (X-a)^\alpha Q', \text{ donc } P'(a) = P(a) = 0$$

Premier cas : P' n'est pas le polynôme nul ($P' \neq 0$). C'est vrai en particulier si K est de caractéristique nulle. Alors comme P est irréductible et s'annule en a, P est à une constante multiplicative près le polynôme minimal de a sur K, et divise donc tout

polynôme annulateur de a. En particulier P divise P' qui est non nul, donc $deg(P) \leq deg(P')$, ce qui est absurde.

Deuxième cas : P' est le polynôme nul. Alors K est un corps fini, de caractéristique un nombre premier p.

$$\text{Notons } P := \sum_{k\geq 0} a_k X^k \text{ ; alors } P' = \sum_{k\geq 1} k a_k X^{k-1} = 0$$

Donc $ka_k = 0$ pour tout k. En particulier si $a_k \neq 0$, k est un multiple de p. Ainsi $P = \sum_{i\geq 0} a_{ip} X^{ip}$. De plus il existe un entier $n \geq 1$ tel que $K = \mathbb{F}_{p^n}$ (corps à p^n éléments), donc $x = x^{p^n} = \left(x^{p^{n-1}}\right)^p$ pour tout x dans K. On peut donc noter les $a_{ip} \in K$ sous la forme b_i^p. Ainsi $P = \sum_{i\geq 0} b_i^p (X^i)^p = \left(\sum_{i\geq 0} b_i X^i\right)^p$ (car p divise $\binom{p}{k}$ pour tout $k \in \{1, \ldots, p-1\}$). Or $p \geq 2$ donc P n'est pas irréductible, contradiction.

Dans tous les cas, P n'a donc que des racines simples.

□

Définition 2.1.3 (extension galoisienne)**.**
Soit K un corps. Une extension E/K est dite ***galoisienne*** *(ou de Galois) si elle est de degré fini (donc algébrique), normale et séparable.*

Remarque : La définition "classique" d'extension galoisienne, également utilisée pour la théorie de Galois infinie, ne demande pas que l'extension soit finie mais seulement algébrique. Le choix fait ici permettra de simplifier significativement la rédaction.

L'un des objectifs de cette section sera de montrer que si K est de caractéristique nulle ou est un corps fini, une extension E/K est galoisienne si et seulement si c'est un corps de décomposition sur K d'un polynôme de $K[X]$.
Dans le cas où E/K est galoisienne, nous pourrons ensuite établir la **correspondance de Galois**, qui nous assurera entre autres que les applications Γ et Φ définies ci-dessous sont des bijections réciproques entre l'ensemble des sous-extensions de E contenant K et l'ensemble des sous-groupes du groupe $Gal(E|K)$ (qui est fini car E est un corps de décomposition, *cf.* 2.1.5) :

$$\begin{aligned} \mathcal{K}_K^E := \{\text{sous-extensions de } E/K\} &\longleftrightarrow \{\text{sous-groupes de } Gal(E|K)\} := \mathcal{H}_K^E \\ F &\overset{\Gamma}{\longmapsto} Gal(E|F) \\ E^H := \{x \in E \ ; \ \forall h \in H, \ h(x) = x\} &\overset{\Phi}{\longmapsfrom} H \end{aligned}$$

On peut vérifier que ces deux applications sont bien définies et vérifient toujours les propriétés suivantes :

Propriétés 2.1.4. *Soient $F, F' \in \mathcal{K}_K^E$ et $H, H' \in \mathcal{H}_K^E$.*

a) Γ *et* Φ *renversent les inclusions :* $\begin{cases} F \subset F' \Rightarrow \Gamma(F') \subset \Gamma(F) \\ H \subset H' \Rightarrow \Phi(H') \subset \Phi(H) \end{cases}$

b) $F \subset \Phi \circ \Gamma(F)$

c) $H \subset \Gamma \circ \Phi(H)$

d) $\Phi \circ \Gamma \circ \Phi = \Phi$

e) $\Gamma \circ \Phi \circ \Gamma = \Gamma$

Proposition 2.1.5.
Soient P un polynôme de $K[X]$ et E un corps de décomposition de P sur K.
Soit $R := \{\alpha_1, \ldots, \alpha_n\}$ l'ensemble des racines distinctes de P dans E.

a) Pour tout $g \in Gal(P|K)$, la restriction de g à R est une permutation de R. Cette restriction induit un isomorphisme de $Gal(P|K)$ sur un sous-groupe de $\mathfrak{S}_R \simeq \mathfrak{S}_n$

b) Soit $\prod_{i=1}^{s} P_i^{k_i}$ la décomposition de P en irréductibles de $K[X]$ ($i \neq j \Rightarrow P_i \neq P_j$), et soit R_i l'ensemble des racines de P_i dans E. Alors les R_i sont exactement les orbites de $R = \bigcup_{i=1}^{s} R_i$ sous l'action de $Gal(P|K)$. (autrement dit $Gal(P|K)$ agit transitivement sur les racines de chaque composante irréductible de P)

c) Si P est à racines simples, P est irréductible si et seulement si $Gal(P|K)$ agit transitivement sur R.

Remarque : Si K est de caractéristique nulle ou est un corps fini, on a alors (2.1.2) :

$P \in K[X]$ irréductible $\Rightarrow Gal(P|K)$ agit transitivement sur ses racines (toutes distinctes)

Démonstration de la Proposition 2.1.5.

a) Soient $g \in Gal(P|K)$ et $\alpha_i \in R$. g fixe les éléments de K donc il fixe les coefficients de P. Ainsi $P(g(\alpha_i)) = g(P(\alpha_i)) = 0$. Donc $g(\alpha_i) \in R$ et $g(R) \subset R$. Or g est injectif et R est fini, donc $g(R) = R$, et en notant $g_{|R}$ la restriction de g à R au départ et à l'arrivée, $g_{|R} \in \mathfrak{S}_R$.
Notons $\rho : Gal(P|K) \to \mathfrak{S}_R$ la restriction à R au départ et à l'arrivée.
$\forall g, g' \in Gal(P|K)$, $(g \circ g')_{|R} = g_{|R} \circ g'_{|R}$, donc ρ est un morphisme de groupes. De plus, ρ est injectif.
En effet si $\rho(g) = id_R$, alors g, qui fixe les éléments de K, fixe aussi chaque α_i, donc tout polynôme sur K en les α_i, *ie* (1.1.3) tous les éléments de $K(\alpha_1, \ldots, \alpha_n) = D_K(P)$. Donc $g = id_{D_k(P)}$, et ρ est injectif. Ainsi $Gal(P|K)$ s'identifie au sous-groupe $Im(\rho)$ de $\mathfrak{S}_R \simeq \mathfrak{S}_n$.

b) Avec les notations de l'énoncé, soient α et β deux racines de P_i (donc de P) dans E. D'après 1.1.8, il existe un K-isomorphisme $g : K(\alpha) \to K(\beta)$ tel que $g(\alpha) = \beta$.

Or (1.1.7) $E := D_K(P)$ est à la fois un corps de décomposition de P sur $K(\alpha)$ et $K(\beta)$, donc d'après 1.1.9, g se prolonge en un K-automorphisme $\widetilde{g} : E \to E$.
En particulier $\widetilde{g}(\alpha) = \beta$, donc les racines de P_i sont toutes dans la même orbite sous l'action de $Gal(P|K)$.
Par ailleurs si $\alpha \in R_i$ et $\beta \in R_j$ sont tels qu'il existe $g \in Gal(P|K)$ vérifiant $g(\alpha) = \beta$, alors $0 = g(P_i(\alpha)) = P_i(g(\alpha)) = P_i(\beta)$, donc β est racine de P_i, et donc $i = j$ car P a toutes ses racines simples par hypothèse.
Les R_i sont donc exactement les orbites de R sous l'action de $Gal(P|K)$.

c) immédiat d'après b).

□

Exemple 2.1.6. On considère le polynôme $P := X^3 - 2 \in \mathbb{Q}[X]$.
Soit $R := \{\alpha_k := \sqrt[3]{2}j^k \ ; \ 0 \leq k \leq 2\}$ l'ensemble des trois racines (distinctes) de P.
P est irréductible (de degré 3 sans racine rationnelle). Son corps de décomposition est : $E := \mathbb{Q}(\sqrt[3]{2}, j)$. D'après la proposition précédente, $Gal(P|\mathbb{Q})$ s'identifie à un sous-groupe de $\mathfrak{S}_3$, que l'on va déterminer en prolongeant à E les $\mathbb{Q}$-automorphismes de la sous-extension $\mathbb{Q}(j)/\mathbb{Q}$ de $E/\mathbb{Q}$:

On a $Irr(j, \mathbb{Q}) = X^2 + X + 1$, et ses racines sont j et $j^2 = \overline{j}$. Un élément g de $Gal(\mathbb{Q}(j)|\mathbb{Q})$ est déterminé par $g(j)$ et envoie une racine sur une racine (deux choix possibles), donc

$$Gal(\mathbb{Q}(j)|\mathbb{Q}) = \{id_{\mathbb{Q}(j)}, \overbrace{(a + bj \mapsto a + bj^2}^{\text{conjugaison complexe}}, \ a, b \in \mathbb{Q})\}$$

Par la proposition 1.1.8, **chacun** de ces deux automorphismes peut se prolonger en un automorphisme de E (vu comme corps de rupture de P sur $\mathbb{Q}(j)$: $E = \mathbb{Q}(j)(\alpha_k)$) de trois façons différentes :

$$\alpha_0 \longmapsto \alpha_k, \ 0 \leq k \leq 2$$

Ainsi $Gal(P|\mathbb{Q})$ contient au moins $2 \times 3 = 6$ éléments. Or $Gal(P|\mathbb{Q})$ s'injecte dans $\mathfrak{S}_3$ qui est de cardinal 6, donc $Gal(P|\mathbb{Q}) \simeq \mathfrak{S}_3$.

Exemple 2.1.7. Soit $n \geq 2$. On considère Φ_n le n-ième polynôme cyclotomique sur $\mathbb{Q}$. On note ξ la racine primitive n-ième de l'unité $e^{2i\pi/n}$. On peut montrer (admis ici) que Φ_n appartient à $\mathbb{Q}[X]$ (et même à $\mathbb{Z}[X]$) et est irréductible sur $\mathbb{Q}$. ξ engendre le groupe des racines n-ièmes de l'unité donc :

$$\mathbb{Q}(\xi) = D_{\mathbb{Q}}(X^n - 1) = D_{\mathbb{Q}}(\Phi_n) := E, \text{ et } [E : \mathbb{Q}] = deg(\Phi_n) = \varphi(n),$$

où φ est l'indicatrice d'Euler.

On note R l'ensemble des racines (toutes distinctes) de Φ_n. Pour k dans $\mathbb{Z}$, $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si k est premier avec n, donc $R = \{\xi^k \ ; \ 1 \leq k \leq n, \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times\}$.

$$\begin{aligned} \text{Soit } \psi : (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow Gal(\Phi_n|\mathbb{Q}) = Aut(\mathbb{Q}(\xi)) \\ \overline{k} &\longmapsto (\xi \mapsto \xi^k) \end{aligned}$$

On peut facilement vérifier que l'application ψ est bien définie et est un isomorphisme de groupes. En particulier $Gal(\Phi_n|\mathbb{Q})$ est abélien, de cardinal $\varphi(n)$.
Enfin si n est premier, alors $Gal(\Phi_n|\mathbb{Q})$ est **cyclique** (c'est un résultat sur les corps finis : tout sous-groupe fini du groupe des inversibles d'un corps (ici $\mathbb{Z}/n\mathbb{Z}$) est cyclique).
Par exemple :

- $(\xi \mapsto \xi^3)$ engendre $Gal(\Phi_{17}|\mathbb{Q})$ (on vérifie que $\overline{3}$ engendre $(\mathbb{Z}/17\mathbb{Z})^\times$) ;
- $(\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^2$, donc $Gal(\Phi_8|\mathbb{Q})$ est d'ordre 4, abélien non cyclique.

Dans toute la suite, on supposera désormais que K est de caractéristique nulle ou est un corps fini. On note $(*K)$ cette hypothèse.

Remarques : Sous cette nouvelle hypothèse, une extension galoisienne est donc une extension finie et normale, puisque le caractère séparable est automatique d'après 2.1.2.
De plus si $P \in K[X]$ est irréductible de degré n, on a alors : $\begin{cases} n \text{ divise } |Gal(P|K)| \\ |Gal(P|K)| \text{ divise } n! \end{cases}$,
où $|X|$ désigne le cardinal d'un ensemble X.
La première relation provient du point c) de la proposition 2.1.5 et du fait que le cardinal d'une orbite divise le cardinal du groupe. La seconde relation provient du point a) de la proposition 2.1.5.
La proposition qui suit montre que le groupe de Galois de toute extension finie est un groupe fini, et borne son cardinal :

Proposition 2.1.8.
*Soit E/K une extension **finie**.*
On a $|Gal(E|K)| \leq [E : K]$.

Démonstration. Par récurrence forte sur le degré $[E : K]$ de l'extension :
· Si $[E : K] = 1$, $E = K$ et $Gal(E|K) = \{id_K\}$.
· On suppose que la propriété est vraie pour toute extension E'/K' de degré strictement inférieur à n pour un certain $n \geq 2$. Soit E/K une extension de degré n. On a $E \neq K$,

donc il existe $x \in E \backslash K$. Alors $[E : K] = [E : K(x)][K(x) : K] = n$, donc $[E : K(x)] < n$, et l'hypothèse de récurrence donne donc :

$$|Gal(E|K(x))| \leq [E : K(x)] = \frac{[E : K]}{[K(x) : K]} = \frac{n}{d}, \text{ où } d := [K(x) : K] \geq 2.$$

On note $G := Gal(E|K)$. On veut montrer que $|G| \leq [E : K]$. D'après le corollaire 1.1.6, E est de la forme $K(\alpha_1, \ldots, \alpha_s)$. Un élément g de G envoie chacun des α_i sur une racine de son polynôme minimal sur K (nombre fini de possibilités), et les $g(\alpha_i)$ déterminent entièrement g, donc G est un groupe fini.
$Gal(E|K(x)) = \{g \in G \ ; \ g(x) = x\} := Stab_G(x)$ est le stabilisateur de x pour l'action de G sur E. En notant $Orb(x)$ l'orbite de x pour l'action de G sur E, on a la relation

$$|G| = |Stab_G(x)| \times |Orb(x)|, \text{ et } |Stab_G(x)| \leq \frac{n}{d}, \text{ donc } |G| \leq \frac{n}{d} \times |Orb(x)|$$

On considère $Q := Irr(x, K)$. $Q \in K[X]$ est de degré d $(= [K(x) : K])$ et annule x, donc

$$\forall g \in G, \ 0 = g(Q(x)) = Q(g(x)), \text{ et } g(x) \text{ est une racine de } Q$$

Donc il y a au plus $deg(Q)$ valeurs possibles pour $g(x)$, c'est à dire $|Orb(x)| \leq d$.
Ainsi $|G| \leq \frac{n}{d} \times d = n = [E : K]$, ce qu'on voulait démontrer.

□

Nous allons maintenant voir plusieurs caractérisations de la notion d'extension galoisienne, que nous utiliserons en fonction de nos besoins :

Théorème 2.1.9.
Soit E/K une extension algébrique. On suppose $(*K)$. On note $G := Gal(E|K)$ et $E^G := \{x \in E; \forall g \in G, g(x) = x\}$ (cf. page 6). Les propriétés suivantes sont équivalentes :

A) L'extension E/K est galoisienne ;

B) L'extension E/K est un corps de décomposition ;

C) On a $[E : K] < \infty$ et $K = E^G$;

D) On a $|Gal(E|K)| = [E : K] < \infty$.

Proposition 2.1.10.
La notion d'extension normale admet elle-même plusieurs caractérisations :
Les propriétés suivantes sont équivalentes (E/K extension algébrique) :

a) E/K est une extension normale, ie tout élément de E est racine d'un polynôme non nul de $K[X]$ scindé sur E ;

b) Pour tout x dans E, $Irr(x, K)$ est scindé sur E ;

c) Tout polynôme irréductible de $K[X]$ qui admet une racine dans E est scindé sur E.

Démonstration du Théorème 2.1.9.

On va prouver la suite d'implication : $B) \Longrightarrow D) \Longrightarrow C) \Longrightarrow A) \Longrightarrow B)$

· $B) \Longrightarrow D)$ **:** On a $[E : K] < \infty$ par le corollaire 1.1.6, et $|Gal(E|K)| \leq [E : K]$ par la proposition 2.1.8. Reste à voir que sous l'hypothèse $(*K)$ et si E est un corps de décomposition sur K ($E = D_K(P)$), alors l'inégalité inverse est vraie. Pour cela on reprend la preuve de la proposition 2.1.8 en remplaçant l'inégalité de l'hypothèse de récurrence par une égalité et en ne considérant que des extensions E'/K' qui sont des corps de décomposition :
Si $[E : K] = n \geq 2$, on peut maintenant prendre pour le choix du $x \in E\backslash K$ une des racines de P qui n'est pas dans K. $Irr(x, K)$ divise P, donc par la proposition 2.1.5, $Gal(E|K)$ agit transitivement sur les racines de $Irr(x, K)$, c'est à dire l'orbite $Orb(x)$ est exactement l'ensemble des d racines (toutes distinctes) de $Irr(x, K)$.
Comme $|Gal(E|K(x)| = [E : K(x)] = \dfrac{n}{d}$ par hypothèse de récurrence (et par 1.1.7),

$$\text{on a } |Gal(E|K)| = |Stab_G(x)| \times |Orb(x)| = \frac{n}{d} \times d = n, \text{ ce qui conclut.}$$

· $D) \Longrightarrow C)$ **:** On veut montrer que $K = E^G$, c'est à dire que K est exactement l'ensemble des éléments de E fixés par tout élément de $G := Gal(E|K)$. On utilise les applications Γ et Φ définies page 6 :

$$Gal(E|E^G) = \Gamma(E^G) = \Gamma \circ \Phi(G) = \overbrace{\Gamma \circ \Phi \circ \Gamma(K) = \Gamma(K)}^{\text{d'après 2.1.4 e)}} = G$$

Donc (proposition 2.1.8) $|G| = |Gal(E|E^G)| \leq [E : E^G] \leq [E : K] < \infty$
Mais par hypothèse (D), $|G| = [E : K]$, donc $[E : E^G] = [E : K] = [E : E^G][E^G : K]$, donc $[E^G : K] = 1$, *ie* $E^G = K$.

· $C) \Longrightarrow A)$ **:** On a $[E : K] < \infty$. Il reste à voir que l'extension E/K est normale, *ie* (proposition 2.1.10) que le polynôme minimal sur K de tout élément de E est scindé sur E. Soit $\alpha \in E$. On va montrer que :

$$P := Irr(\alpha, K) = \prod_{\beta \in Orb(\alpha)} (X - \beta) := Q \ ,$$

où $Orb(\alpha)$ est l'orbite de α sous l'action de $G := Gal(E|K)$. Il suffit pour cela de montrer que $Q \in K[X]$ car alors :

- P divise Q dans $K[X]$ (donc dans $E[X]$) par définition de P ;
- Q divise P dans $E[X]$ car $Orb(\alpha) \subset E \cap \{\text{racines de } Irr(\alpha, K)\}$;
- P et Q sont unitaires, d'où il suit que $P = Q$.

Montrons que $Q \in K[X]$: on note $\beta_1, \ldots, \beta_d$ les éléments de l'orbite (finie) $Orb(\alpha)$.
Si $j \in \{0, \ldots, d-1\}$, le coefficient de degré j de Q est $a_j := (-1)^{d-j}\sigma_{d-j}(\beta_1, \ldots, \beta_d)$, où σ_k est le polynôme symétrique élémentaire de degré k. Un élément g de G induit une permutation de $Orb(\alpha)$, notée s. On a :

$$\begin{aligned}(-1)^{d-j}g(a_j) = \sigma_{d-j}(g(\beta_1), \ldots, g(\beta_d)) &= \sigma_{d-j} \circ s(\beta_1, \ldots, \beta_d) \ (\sigma_{d-j} \text{ vu comme fonction}) \\ &= \sigma_{d-j}(\beta_1, \ldots, \beta_d) \ (\sigma_{d-j} \text{ symétrique}) \\ &= (-1)^{d-j}a_j\end{aligned}$$

Donc pour tout j dans $\{0, \ldots, d\}$, $a_j \in E^G = K$ ($a_d = 1$ car Q est unitaire), et $Q \in K[X]$.

$\cdot$ $A) \Longrightarrow B)$ **:** L'extension E/K étant finie, il existe un entier $s \geq 1$ et des éléments $\alpha_1, \ldots, \alpha_s$ de E tels que $E = K(\alpha_1, \ldots, \alpha_s)$. Par hypothèse $Irr(\alpha_i, K)$ est scindé dans E pour tout $i \in \{1, \ldots, s\}$. On pose $P := \prod_{i=1}^{s} Irr(\alpha_i, K)$.
Ainsi $P \in K[X]$, P est scindé sur E, et son corps de décomposition sur K (plus petit corps contenant K est les racines de P) est $K(\alpha_1, \ldots, \alpha_s) = E$. Donc E est un corps de décomposition sur K.

□

Corollaire 2.1.11.
Soit $P \in K[X]$ un polynôme irréductible et F une sous-extension de $D_K(P)$ contenant une racine de P. Alors F est galoisienne si et seulement si $F = D_K(P)$.

Démonstration.

Si F est galoisienne et contient une racine α de P, alors d'après la proposition 2.1.10 $Irr(\alpha, K)$ est scindé sur F. Or P est irréductible, donc P et $Irr(\alpha, K)$ sont égaux à une constante multiplicative près, et F contient donc toutes les racines de P, donc $F = D_K(P)$.
L'autre implication est immédiate.

□

Enonçons maintenant un lemme qui sera utile pour la preuve de la correspondance de Galois.

Lemme 2.1.12.
Soit E un corps et G un sous-groupe fini de $Aut(E)$. Alors $[E : E^G] \leq |G|$.
En particulier l'extension E/E^G est galoisienne, et $Gal(E|E^G) = G$.

Remarque :
Ce lemme fournit en particulier une preuve directe de l'implication $C) \Longrightarrow D)$ du théorème 2.1.9 (prendre $G := Gal(E|K)$).

Démonstration du Lemme.

— Posons $G := \{g_1, \ldots, g_n\}$. Montrons que toute famille $\{\alpha_1, \ldots, \alpha_{n+1}\}$ de $n+1$ éléments de E est liée sur E^G (ce qui donnera $[E : E^G] \leq |G|$) :

$$\text{Posons } A := \begin{pmatrix} g_1(\alpha_1) & \ldots & g_1(\alpha_{n+1}) \\ \vdots & & \vdots \\ g_n(\alpha_1) & \ldots & g_n(\alpha_{n+1}) \end{pmatrix} \in \mathcal{M}_{n,n+1}(E), \text{ et } r := rang(A).$$

Quitte à renuméroter les α_j, on peut supposer que les r premières colonnes de A sont linéairement indépendantes (sur E). La $(r+1)$-ième colonne de A est donc combinaison linéaires de ces colonnes, avec des coefficients $\lambda_j \in E$ $(1 \leq j \leq r)$ uniques. On veut montrer que $\lambda_j \in E^G$ pour tout j. On a :

$$g(\alpha_{r+1}) = \lambda_1 \cdot g(\alpha_1) + \ldots + \lambda_r \cdot g(\alpha_r) \ \forall g \in G \tag{1}$$

On applique $g' \in G$ à cette égalité pour obtenir :

$$(g' \circ g)(\alpha_{r+1}) = \underbrace{g'(\lambda_1)}_{:=\lambda'_1} \cdot (g' \circ g)(\alpha_1) + \ldots + \underbrace{g'(\lambda_r)}_{:=\lambda'_r} \cdot (g' \circ g)(\alpha_r) \ \forall g, g' \in G \tag{2}$$

En appliquant d'une part l'égalité (1) pour $g = id_E$ et d'autre part l'égalité (2) pour $g' = g^{-1}$, on obtient :

$$\alpha_{r+1} = \lambda_1 \cdot \alpha_1 + \ldots + \lambda_r \cdot \alpha_r = g^{-1}(\lambda_1) \cdot \alpha_1 + \ldots + g^{-1}(\lambda_r) \cdot \alpha_r \tag{3}$$

Or g^{-1} parcourt G quand g parcourt G (car G est un groupe), donc par unicité de la famille $(\lambda_j)_j$, $\lambda_j = g(\lambda_j)$ pour tout j dans $\{1, \ldots, n\}$ et tout g dans G, *ie* $\lambda_j \in E^G$ pour tout j.
D'après l'égalité (3), α_{r+1} est donc une combinaison linéaire à coefficients dans E^G, donc la famille $\{\alpha_1, \ldots, \alpha_{n+1}\}$ est liée sur E^G, et $[E : E^G] \leq n = |G|$.

— Par la proposition 2.1.8, $|Gal(E|E^G)| \leq [E : E^G]$. Par 2.1.4 *c*), on a donc :

$$|G| \leq |\Gamma \circ \Phi(G)| = |Gal(E|E^G)| \leq [E : E^G] \leq |G|$$

Il y a donc égalité partout. Par la caractérisation *D*) du théorème 2.1.9, E/E^G est donc galoisienne, et $G = Gal(E|E^G)$. □

2.2 Correspondance de Galois

On rappelle les définitions des applications Γ et Φ de la page 6 :

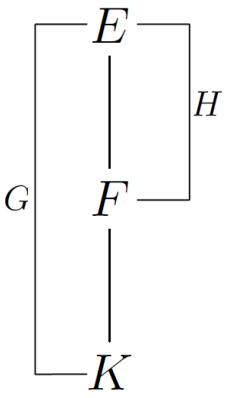
$$\mathcal{K}_K^E := \{\text{sous-extensions de } E/K\} \longleftrightarrow \{\text{sous-groupes de } Gal(E|K)\} := \mathcal{H}_K^E$$
$$F \overset{\Gamma}{\longmapsto} Gal(E|F)$$
$$E^H := \{x \in E \ ; \ \forall h \in H, \ h(x) = x\} \overset{\Phi}{\longmapsto} H$$

Théorème 2.2.1 (Correspondance de Galois)**.**
Soit E/K une extension galoisienne. On suppose $(*K)$. On note $G := Gal(E|K)$.

a) Les applications Γ et Φ sont des bijections, réciproques l'une de l'autre.

b) Pour chaque extension intermédiaire F/K, on a, en notant $H := Gal(E|F)$:

- *L'extension "du haut" E/F est galoisienne (et donc $|H| = [E : F]$ et $[F : K] = \dfrac{|G|}{|H|}$).*
- *L'extension "du bas" F/K est galoisienne* ***si et seulement si*** *H est distingué dans G* ***si et seulement si*** *$\forall g \in G$, $g(F) = F$*
  Dans ce cas on a alors $Gal(F|K) \simeq G/H$ (isomorphisme induit par la restriction à F des automorphismes de E)



Démonstration. On note $\mathcal{K}$ (resp. $\mathcal{H}$) au lieu de $\mathcal{K}_K^E$ (resp. $\mathcal{H}_K^E$) pour alléger l'écriture.
Si F/K est une sous-extension de E/K, et si $E := D_K(P)$ avec $P \in K[X]$, alors (1.1.7) : $E = D_F(P)$, donc E/F est galoisienne (première partie de b)).
Si $H := \Gamma(F) = Gal(E|F)$, alors (2.1.9 caractérisation C) $F = E^H = \Phi \circ \Gamma(F)$, donc $\Phi \circ \Gamma = id_{\mathcal{K}}$. De plus par la caractérisation D du théorème 2.1.9,

$$[F : K] = \frac{[E : K]}{[E : F]} = \frac{|G|}{|H|} = [G : H] \text{ (indice de } H \text{ dans } G)$$

Pour terminer la preuve de a), montrons que $\Gamma \circ \Phi = id_{\mathcal{H}}$:
Soit $H \in \mathcal{H}$. H est un sous-groupe fini de G (donc de $Aut(E)$), donc par le lemme 2.1.12, $[E : E^H] \leq |H|$. Or (2.1.4,c) $H \subset \Gamma \circ \Phi(H) = Gal(E|E^H)$, donc (2.1.8) : $|H| \leq |Gal(E|E^H)| \leq [E : E^H] \leq |H|$. Ainsi $|H| = [E : E^H]$ et $H = \Gamma \circ \Phi(H)$.
Finalement $\Gamma \circ \Phi = id_{\mathcal{H}}$.

Reste à étudier l'extension "du bas" F/K. On aura besoin du lemme suivant :

Lemme 2.2.2.
Si F/K est une sous-extension d'un corps de décomposition E sur K,
alors tout K-morphisme de F dans E se prolonge en un K-automorphisme de E.
De plus il y a exactement $[F : K]$ K-morphismes de F dans E.

(pour $F := E$, cela montre l'implication $B) \Longrightarrow D)$ du théorème 2.1.9)

Démonstration du Lemme.

Notons $\rho : G := Gal(E|K) \longrightarrow Morph_K(F, E)$ la restriction à F. Pour montrer le premier point, il suffit de voir que ρ est surjectif :
Si $f : F \longrightarrow E$ est un K-morphisme, f est injectif donc c'est un K-isomorphisme de F sur $f(F) \subset E$.
Par hypothèse, il existe $P \in K[X]$ tel que $E = D_K(P)$.
Si on note $\overline{f} : F[X] \longrightarrow f(F)[X]$ l'extension naturelle de f aux anneaux de polynômes, $\overline{f}(P) = P$, et $E = \underbrace{D_F(P)}_{:=L_1} = \underbrace{D_{f(F)}(\overline{f}(P))}_{:=L_2}$. Ainsi par la proposition 1.1.9, l'isomorphisme f se prolonge en un isomorphisme $\widetilde{f} : E \longrightarrow E$, qui est donc un élément de $Gal(E|K)$. On a ainsi $f = \rho(\widetilde{f})$, donc ρ est surjective.

Montrons maintenant le deuxième point du lemme, *ie* $|\rho(G)| = [F : K]$:
On définit sur G une relation d'équivalence par :

$$g \mathcal{R} g' \Longleftrightarrow g_{|F} = g'_{|F} \Longleftrightarrow \rho(g) = \rho(g')$$

Il y $|\rho(G)|$ classes d'équivalence pour cette relation. Déterminons le cardinal d'une classe :
On a vu dans la première partie de la preuve de la correspondance de Galois que E/F est galoisienne, donc $[E : F] = |H|$, où $H := Gal(E|F)$.
Soient $g, g' \in G$. Notons $f_{|R} : R \longrightarrow f(R)$ l'application induite par la restriction d'une application f à un sous-ensemble R. Alors :

$$\rho(g) = \rho(g') \Longleftrightarrow g_{|F} = g'_{|F} \Longleftrightarrow {g'}^{-1}_{|F} \circ g_{|F} = id_F \Longleftrightarrow g' \circ g \in H \Longleftrightarrow g \in g'H$$

Et $|g'H| = |H| = [E : F]$, donc la classe d'équivalence de $g \in G$ est de cardinal $[E : F]$.
Ainsi $|G| = |\rho(G)| \times [E : F]$ (les $|\rho(G)|$ classes ont même cardinal), donc :

$$|\rho(G)| = \frac{|G|}{[E : F]} = \frac{[E : K]}{[E : F]} = [F : K]$$

Il y a donc $|\rho(G)| = [F : K]$ morphismes de F dans E.

□

Terminons maintenant la preuve de la correspondance de Galois :
· On se sert de l'application ρ définie au début de la preuve du lemme 2.2.2. La propriété $(\forall g \in G, g(F) = F)$ est équivalente à $\rho(G) = Gal(F|K)$, c'est à dire $Morph_K(F, E) = Gal(F|K)$ car ρ est surjective. Or $Gal(F|K)$ s'injecte dans $Morph_K(F, E)$ qui est un ensemble fini, donc la propriété équivaut à l'égalité des cardinaux : $|Gal(F|K)| = [F : K]$. Cette égalité est elle-même équivalente (2.1.9) à F/K galoisienne.

· On remarque que pour tout g dans G, $Gal(E|g(F)) = g \circ Gal(E|F) \circ g^{-1}$
(l'inclusion $\supset$ est évidente ; conjuguer par g^{-1} pour montrer l'inclusion $\subset$)
Cette égalité nous donne immédiatement que H est distingué dans G si et seulement si $\forall g \in G,\ Gal(E|g(F)) = Gal(E|F)$, *ie* $\forall g \in G,\ \Gamma(g(F)) = \Gamma(F)$, *ie* $(\forall g \in G,\ g(F) = F)$ car Γ est injective (c'est une bijection d'après a)).
Finalement $H \triangleleft G \iff (\forall g \in G, g(F) = F)$.

· On a vu que $(\forall g \in G, g(F) = F) \iff \rho(G) = Gal(F|K)$.
L'hypothèse $(\forall g \in G, g(F) = F)$ assure également que ρ est un morphisme de groupes, et en prenant $g' = id_E$ dans la preuve du lemme 2.2.2, on a $\rho(g) = id_F \iff g \in H$, *ie* $Ker(\rho) = H$. La factorisation de ρ fournit donc l'isomorphisme $G/H \simeq Gal(F|K)$.

□

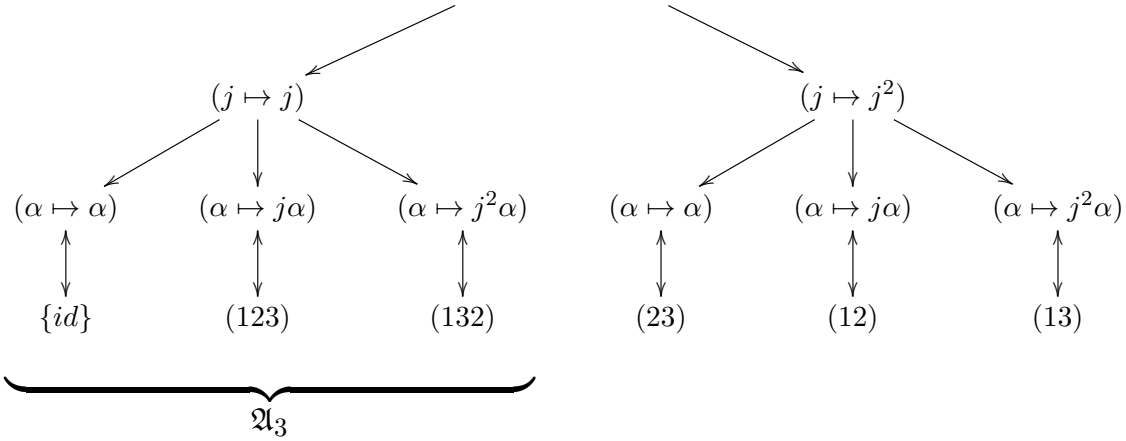
2.3 Exemples

Exemple 2.3.1. $P = X^3 - 2$, $K = \mathbb{Q}$

On a vu (exemple 2.1.6) que le corps de décomposition de P sur $\mathbb{Q}$ est $E := \mathbb{Q}(\alpha, j)$ ($\alpha := \sqrt[3]{2}$), et que $G := Gal(P|\mathbb{Q})$ est isomorphe à $\mathfrak{S}_3$. On va expliciter cet isomorphisme, en commençant par choisir une bijection entre l'ensemble $R := \{\alpha, j\alpha, j^2\alpha\}$ des racines de P (sur lequel agit G) et l'ensemble $\{1, 2, 3\}$ (sur lequel agit $\mathfrak{S}_3$) :

$$\alpha \mapsto 1 \ , \ j\alpha \mapsto 2 \ , \ j^2\alpha \mapsto 3$$

Le schéma ci-dessous résume le procédé de construction des éléments de G utilisé dans l'exemple 2.1.6. La dernière ligne donne l'isomorphisme entre G et $\mathfrak{S}_3$:



En utilisant la proposition 1.2.2, on peut déterminer l'ensemble des sous-groupes de $\mathfrak{S}_3$, isomorphes aux éléments de $\mathcal{H}^E_{\mathbb{Q}}$. Ce dernier étant en bijection avec $\mathcal{K}^E_{\mathbb{Q}}$ d'après la correspondance de Galois, on peut donc également déterminer l'ensemble des sous-corps de $\mathbb{Q}(\alpha, j)$ contenant $\mathbb{Q}$:

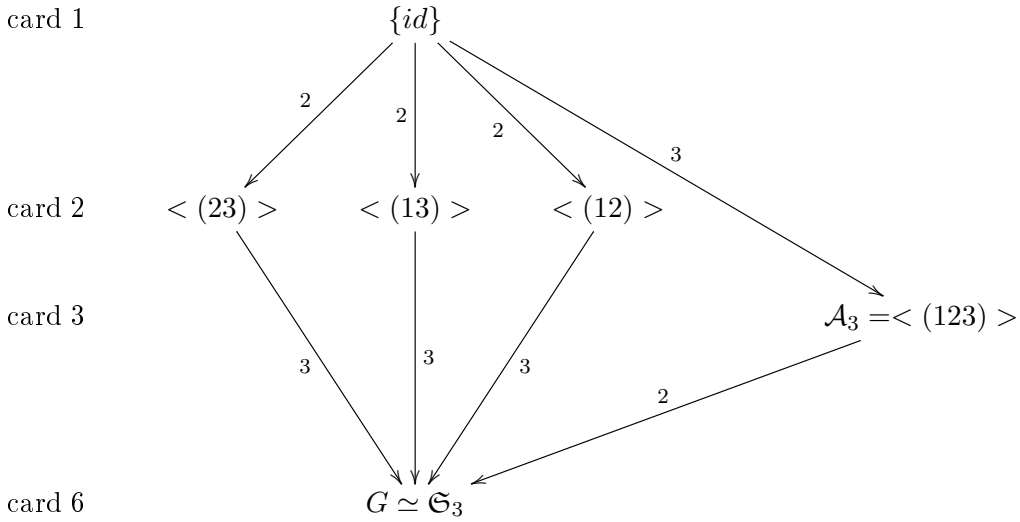


Schéma de $\mathcal{H}_{\mathbb{Q}}^{E}$ (à isomorphisme près) avec les cardinaux et indices

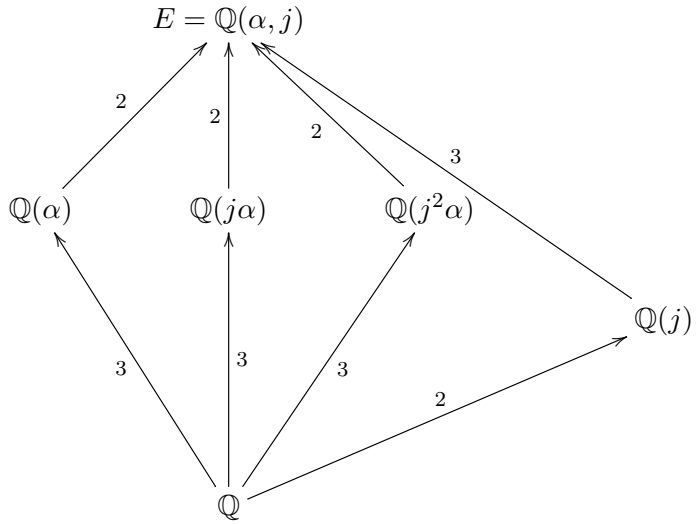


Schéma de $\mathcal{K}_{\mathbb{Q}}^{E}$ avec les degrés des extensions

D'après la correspondance de Galois, on sait que les extensions "du haut" sont toutes galoisiennes. En revanche, $\mathbb{Q}(j)/\mathbb{Q}$ est la seule extension "du bas" galoisienne :

- $Gal(E|\mathbb{Q}(j)) \simeq \mathfrak{A}_3$ (*cf.* arbre page 17) et $|Gal(\mathbb{Q}(j)|\mathbb{Q})| = 2$ (*cf.* exemple 2.1.6),

  donc $Gal(\mathbb{Q}(j)|\mathbb{Q}) \simeq Gal(E|\mathbb{Q})/Gal(E|\mathbb{Q}(j)) \simeq \mathfrak{S}_3/\mathfrak{A}_3$ (d'ordre 2).

- en notant g l'automorphisme de E qui envoie $j^k\alpha$ sur $j^{k+1}\alpha$ (g s'identifie à la permutation (123)), on a $g(\mathbb{Q}(j^k\alpha)) \neq \mathbb{Q}(j^k\alpha)$, donc les trois extensions de la forme $\mathbb{Q}(j^k\alpha)/\mathbb{Q}$ ne sont pas galoisiennes.

Remarque : Dans cet exemple, il n'était bien sûr pas nécessaire d'utiliser les arguments de la correspondance de Galois pour déterminer quelles extensions "du bas" sont galoisiennes :

- $\mathbb{Q}(j)/\mathbb{Q}$ est le corps de décomposition sur $\mathbb{Q}$ de X^2+X+1 donc est galoisienne ;
- α, $j\alpha$ et $j^2\alpha$ ont le même polynôme minimal X^3-2 dont le corps de décomposition $\mathbb{Q}(j,\alpha)$ contient strictement $\mathbb{Q}(\alpha)$, $\mathbb{Q}(j\alpha)$ et $\mathbb{Q}(j^2\alpha)$ (tous 3 distincts), qui ne sont donc pas des corps de décomposition sur $\mathbb{Q}$ (corollaire 2.1.11).

Exemple 2.3.2. $P := X^4-5X^2+6 = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$

Notons $E := D_{\mathbb{Q}}(P)$ et $G := Gal(E|K)$.
Les racines de P sont $\pm\sqrt{2}$ et $\pm\sqrt{3}$, et $E = \mathbb{Q}(\sqrt{2},\sqrt{3})$. On a :

$$[E:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\times 2 = 4 \text{ car } \sqrt{3}\notin\mathbb{Q}(\sqrt{2}),$$

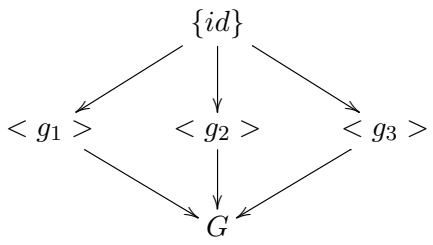
donc $|G|=4$. $(X^2-2)(X^2-3)$ est la décomposition de P en produit d'irréductibles dans $\mathbb{Q}[X]$, donc d'après la proposition 2.1.5, G agit transitivement sur chacune des orbites $\{-\sqrt{2},\sqrt{2}\}$ et $\{-\sqrt{3},\sqrt{3}\}$ de l'ensemble des racines de P. En particulier pour tout $g\in G$, $g(\sqrt{2}) = \pm\sqrt{2}$ et $g(\sqrt{3}) = \pm\sqrt{3}$. Les éléments de G sont donc tous d'ordre au plus 2, et G est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. En notant :

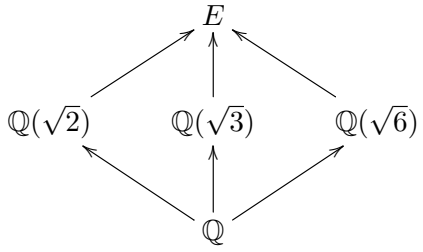
$$\begin{cases} g_1(\sqrt{2}) = \sqrt{2} \\ g_1(\sqrt{3}) = -\sqrt{3} \end{cases} \text{ et } \begin{cases} g_2(\sqrt{2}) = -\sqrt{2} \\ g_2(\sqrt{3}) = \sqrt{3} \end{cases}, \text{ on a } G = \{id_E,\ g_1,\ g_2,\ \overbrace{(g_1\circ g_2)}^{:=g_3}\}$$

Par la correspondance de Galois, les sous-extensions de E contenant $\mathbb{Q}$ sont donc :

$$\Phi(<g_1>) = \mathbb{Q}(\sqrt{2}),\ \Phi(<g_2>) = \mathbb{Q}(\sqrt{3}) \text{ et } \Phi(<g_3>) = \mathbb{Q}(\sqrt{6})$$

On obtient les schémas de $\mathcal{H}_{\mathbb{Q}}^E$ et de $\mathcal{K}_{\mathbb{Q}}^E$:





Pour $k=2,3,6$, l'extension $\mathbb{Q}(\sqrt{k})/\mathbb{Q}$ est galoisienne si et seulement si $Gal(E|\mathbb{Q}(\sqrt{k}))$ est distingué dans G (point b) de la correspondance de Galois), ce qui est ici trivialement vérifié car G est abélien (d'ordre 4).
Ainsi toutes les extensions intermédiaires sont galoisiennes.

3 Résolubilité par radicaux

Dans la suite, tous les corps considérés seront de caractéristique nulle.

On donne toute de suite la définition d'une extension résoluble par radicaux. Des exemples suivront pour se familiariser avec cette notion.

Définition 3.0.1.
Soit K un corps de caractéristique nulle.

*a) Une extension L/K est **radicale** si L est de la forme $L = K(a_1, \dots, a_r)$, où pour tout $i \in \{1, \dots, r\}$,*

$$\text{il existe } n_i \geq 1 \text{ tel que } a_1^{n_1} \in K, \text{ et si } i \geq 2,\ a_i^{n_i} \in K(a_1, \dots, a_{i-1}).$$

*b) Une extension E/K est **résoluble par radicaux** si E peut être inclus dans une extension radicale L/K.*

c) Un polynôme P de $K[X]$ est dit résoluble par radicaux si l'extension $D_K(P)/K$ est résoluble par radicaux.

Autrement dit, une extension est radicale si elle s'obtient en un nombre fini d'extensions monogènes successives, où à chaque étape "le" générateur de l'extension est un radical, *ie* une racine n-ième d'un élément de l'extension précédente. A chaque étape, les éléments de l'extension s'expriment donc en terme des opérations usuelles de l'extension précédente et de ce radical.

Remarque : Choisir $K = \mathbb{R}$ comme corps de base n'a que peu d'intérêt : toute extension intermédiaire entre $\mathbb{R}$ et $\mathbb{C}$ est résoluble par radicaux en une étape ($\mathbb{C} = \mathbb{R}(i)$, $i^2 \in \mathbb{R}$).

Exemple 3.0.2.
$K = \mathbb{Q}$, $\alpha := \sqrt{3 + \sqrt[3]{2}}$. L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est-elle résoluble par radicaux ?

$$\text{En prenant } \begin{matrix} a_1 := \sqrt[3]{2} & a_2 := \alpha \\ n_1 := 3 & n_2 := 2 \end{matrix},$$

on obtient la "tour d'extensions" : $\boxed{\mathbb{Q} \underset{(\sqrt[3]{2})^3 \in \mathbb{Q}}{\subset} \mathbb{Q}(\sqrt[3]{2}) \underset{\alpha^2 \in Q(\sqrt[3]{2})}{\subset} \mathbb{Q}(\sqrt[3]{2}, \alpha) = \mathbb{Q}(\alpha)}$

Donc $\mathbb{Q}(\alpha)/\mathbb{Q}$ est résoluble par radicaux, et même **radicale** (en au plus 2 étapes).

Exemple 3.0.3.
$K = \mathbb{Q}, P := (X^2 - 3)^3 - 2 \in \mathbb{Q}[X]$. Le polynôme P est-il résoluble par radicaux ? Les racines de P sont $\pm\sqrt{3 + j^k \sqrt[3]{2}}$. On note α_k une racine carrée de $3 + j^k \sqrt[3]{2}$, $0 \leq k \leq 2$. (on peut prendre $\alpha_0 = \alpha$, *cf.* exemple 3.0.2)

$$\text{En prenant } \begin{array}{ccccc} a_1 := \sqrt[3]{2} & a_2 := j & a_3 = \alpha & a_4 = \alpha_1 & a_5 = \alpha_2 \\ n_1 := 3 & n_2 := 3 & n_3 = 2 & n_4 = 2 & n_5 = 2 \end{array},$$

On obtient la "tour d'extensions" :

$$\boxed{\begin{array}{ccccc} \mathbb{Q} & \underset{(\sqrt[3]{2})^3 \in \mathbb{Q}}{\subset} & \mathbb{Q}(\sqrt[3]{2}) & \underset{j^3 \in \mathbb{Q}(\sqrt[3]{2})}{\subset} & \mathbb{Q}(\sqrt[3]{2}, j) \\ \underset{\alpha^2 \in \mathbb{Q}(\sqrt[3]{2}, j)}{\subset} & \mathbb{Q}(\sqrt[3]{2}, j, \alpha) & \underset{(\alpha_1)^2 \in \mathbb{Q}(\sqrt[3]{2}, j, \alpha)}{\subset} & \mathbb{Q}(\sqrt[3]{2}, j, \alpha, \alpha_1) & \underset{(\alpha_2)^2 \in \mathbb{Q}(\sqrt[3]{2}, j, \alpha, \alpha_1)}{\subset} \underbrace{\mathbb{Q}(\sqrt[3]{2}, j, \alpha, \alpha_1, \alpha_2)}_{\text{contient } D_{\mathbb{Q}}(P)} \end{array}}$$

Donc P est résoluble par radicaux (en au plus 5 étapes).

3.1 Sur l'équation $X^n - a = 0$

Comme on vient de le voir, chacune des extensions successives d'une extension radicale est monogène, engendrée par une racine d'un polynôme de la forme $X^n - a$, où a est un élément de l'extension précédente. Les résultats des paragraphes précédents n'étant en général valables que pour des extensions galoisiennes, nous allons voir comment rendre galoisienne chacune de ces extensions successives.

L'idée importante (ce sera la proposition 3.1.3) est qu'une extension de la forme $K(\xi, b)/K$ (où $b \in K$ est une racine du polynôme $X^n - a := P$ et ξ est une racine **primitive** n-ième de l'unité) contient **toutes** les racines de P, et est même un corps de décomposition de P sur K, *ie* une extension galoisienne.
Cette démarche sera décisive pour la preuve du théorème d'Abel-Galois.

On commence par le cas particulier où $a = 1$ (polynôme $X^n - 1$) :

Proposition 3.1.1.
Soit K un corps (de caractéristique nulle), soit n un entier ≥ 2 et soit $E := D_K(X^n - 1)$. Pour toute racine primitive n-ième de l'unité ξ dans E, on a $K(\xi) = E$, et $Gal(E|K)$ est abélien.
(K doit ici être vu comme un corps intermédiaire entre $\mathbb{Q}$ et E)

Démonstration.
On plonge E dans $\mathbb{C}$. Ainsi les racines de $X^n - 1$ dans E sont exactement les racines n-ième de l'unité dans $\mathbb{C}$. Soit ξ une racine primitive n-ième de 1. Toute racine du polynôme $X^n - 1$ peut s'écrire comme une puissance de ξ, donc $K(\xi) = E$, et tout élément g de $G := Gal(E|K)$ est entièrement déterminé par l'image de ξ. De plus l'image par g d'une racine de $X^n - 1$ est encore une racine, donc $g(\xi) = \xi^k$ pour un k dans $\mathbb{N}$.
Si $g, g' \in G$ sont tels que $g(\xi) = \xi^k$ et $g'(\xi) = \xi^{k'}$, alors :

$(g \circ g')(\xi) = g(\xi^{k'}) = (\xi^k)^{k'} = (\xi^{k'})^k = (g' \circ g)(\xi)$, donc $g \circ g' = g' \circ g$ et G est abélien. □

Définition 3.1.2.
Une extension E/K est dite abélienne (resp. cyclique) si elle est galoisienne et si son groupe de Galois est abélien (resp. cyclique).

La proposition suivante servira pour la preuve de la première implication du théorème d'Abel-Galois.

Proposition 3.1.3 (Kummer)**.**
Soit K un corps (de caractéristique nulle), soit n un entier ≥ 2, soit $a \in K\backslash\{0\}$. On suppose que K contient une racine primitive n-ième de l'unité notée ξ. Alors :

a) Les corps de décomposition de $X^n - a$ sur K sont exactement les corps de la forme $K(b)$ tels que $b^n = a$.

b) Si $b^n = a$, l'extension $K(b)/K$ est cyclique de degré d un diviseur de n tel que $b^d \in K$, et on a $Irr(b, K) = X^d - b^d$.

c) En particulier si $X^n - a$ est irréductible sur K, alors $Gal(K(b)|K) \simeq \mathbb{Z}/n\mathbb{Z}$.

Démonstration.
Notons $E := D_K(X^n - a)$. Soit b tel que $b^n = a$.

a) Les racines de $X^n - a$ sont les b' tels que $(b')^n = a$, *ie* les b' tels que $\left(\frac{b'}{b}\right)^n = 1$.
L'ensemble des $\frac{b'}{b}$ est donc l'ensemble $\mathbb{U}_n(K)$ des racines n-ième de 1, qui est de cardinal n car K est de caractéristique nulle (contre-exemple : si $carac(K) = n$, $X^n - 1 = (X-1)^n$, donc $\mathbb{U}_n(K) = \{1\}$).
Les racines de $X^n - a$ sont donc les $b\xi^k$ avec $0 \leq k \leq n-1$. Or $\xi \in K$ par hypothèse, donc $b\xi^k \in K(b)$ pour tout k, et donc $K(b) = D_K(X^n - a)$ (et $K(b)/K$ est galoisienne).

b) Notons $G := Gal(K(b)|K)$. Tout $g \in G$ est entièrement déterminé par l'image de b, de la forme $g(b) = b\xi^k$ pour un $k \in \{0, \ldots, n-1\}$.

$$\text{Soit } \phi : G \longrightarrow \mathbb{U}_n(K(b)) = \mathbb{U}_n(K) = <\xi>$$
$$g \longmapsto \frac{g(b)}{b} = \xi^k$$

· ϕ est un morphisme de groupes : si $g, g' \in G$ sont tels que $g(b) = b\xi^k$ et $g'(b) = b\xi^{k'}$,

$$(g \circ g')(b) = g(b\xi^{k'}) = g(b)g(\underbrace{\xi^{k'}}_{\in K}) = b\xi^k\xi^{k'}, \text{ donc } \phi(g \circ g') = \frac{b\xi^k\xi^{k'}}{b} = \phi(g)\phi(g')$$

· $g \in Ker(\phi) \Longleftrightarrow g(b) = b \Longleftrightarrow g = id_{K(b)}$, donc ϕ est injectif.
Or $(\mathbb{U}_n(K), \times)$ est cyclique d'ordre n (engendré par ξ) donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ainsi G s'identifie à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$, forcément cyclique (engendré par le plus petit entier naturel non nul h tel que $\overline{h}$ soit dans le sous-groupe). $|G| := d$ divise donc n. Pour tout g dans G tel que $g(b) = b\xi^k$, on a :

$$1 = \phi(id_{K(b)}) = \phi(g^d) = \phi(g)^d = (\xi^k)^d, \text{ donc } \xi^{kd} = 1.$$

Par ailleurs $K(b)/K$ est galoisienne donc $b^d \in K \iff b^d \in K(b)^G \iff g(b^d) = b^d \, \forall g \in G$. Soit $g \in G$ tel que $g(b) = b\xi^k$. On a $g(b^d) = g(b)^d = (b\xi^k)^d = b^d(\xi^k)^d = b^d$, donc $b^d \in K$.

Ainsi $X^d - b^d \in K[X]$. C'est le polynôme minimal de b sur K car b annule $X^d - b^d$, donc $Irr(b,K)$ divise $X^d - b^d$ et tout deux sont de degré $d = |G| = [K(b) : K]$, donc ils sont égaux car unitaires.

c) Si $X^n - a$ est irréductible sur K, alors $X^n - a = Irr(b,K)$, donc $[K(b) : K] = n$ $= |Gal(K(b)|K)|$, donc $Gal(K(b)|K)$ est cyclique d'ordre n par le point précédent.

□

Reprenons maintenant l'exemple 2.3.1. On avait obtenu la tour d'extension :

$$\boxed{\mathbb{Q} \underset{(\sqrt[3]{2})^3 \in \mathbb{Q}}{\subset} \mathbb{Q}(\sqrt[3]{2}) \underset{\alpha^2 \in Q(\sqrt[3]{2})}{\subset} \mathbb{Q}(\sqrt[3]{2}, \alpha) = \mathbb{Q}(\alpha)}, \text{ où } \alpha := \sqrt{3 + \sqrt[3]{2}}$$

$\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension radicale. On veut rendre ses extensions intermédiaires galoisiennes. $\mathbb{Q}(\sqrt[3]{2}, \alpha)/\mathbb{Q}(\sqrt[3]{2})$ étant déjà galoisienne, il n'y a qu'à s'occuper de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ (non galoisienne, cf. remarque page 19). D'après la proposition précédente, il suffit d'ajouter une racine 3-ième primitive de 1 dans une première extension :

$$\boxed{\mathbb{Q} \underset{j^3 \in \mathbb{Q}}{\subset} \mathbb{Q}(j) \underset{(\sqrt[3]{2})^3 \in \mathbb{Q}(j)}{\subset} \mathbb{Q}(j, \sqrt[3]{2}) \underset{\alpha^2 \in Q(j, \sqrt[3]{2})}{\subset} \mathbb{Q}(j, \sqrt[3]{2}, \alpha) \supset \mathbb{Q}(\alpha)}$$

Les extensions successives sont maintenant toutes galoisiennes (remarque : cette tour d'extensions ne nous dit pas que $\mathbb{Q}(\alpha)/\mathbb{Q}$ est radicale).

Plus généralement, pour rendre galoisiennes les extensions successives d'une l'extension radicale $K(a_1, \ldots, a_r)$ (où $a_i^{n_i} \in K(a_1, \ldots, a_{i-1})$), on ajoute une racine n_i-ième primitive de 1 pour tout $i \in \{1, \ldots, r\}$. On peut en réalité faire plus simple : il suffit d'après la proposition suivante d'ajouter une racine m-ième primitive de 1 au début de la suite d'extensions, où m est le PPCM des n_i.

Proposition 3.1.4.
Soit $m \in \mathbb{N}^*$. Si $\xi \in K$ est une racine primitive m-ième de l'unité, alors K possède une racine primitive n-ième de l'unité pour tout diviseur n de m.

Démonstration.
Soit n un diviseur de m. Il existe λ tel que $m = \lambda n$. $\xi^\lambda \in K$ et est d'ordre n, c'est une racine primitive n-ième de l'unité. □

Remarque :
Le fait que les extensions successives d'une extension radicale $K(a_1, \ldots, a_r)/K$ soient galoisiennes ne nous dit pas que la "grande" extension $K(a_1, \ldots, a_r)/K$ est galoisienne ! On verra dans la preuve du théorème d'Abel-Galois qu'une manière de s'en assurer est d'ajouter les racines des polynômes minimaux des a_i.

Voici pour terminer une réciproque à la proposition 3.1.3, qui servira pour la preuve de la seconde implication du théorème d'Abel-Galois.

Proposition 3.1.5.
Soient K un corps de caractéristique nulle et E/K une extension cyclique de degré n. On suppose que K contient une racine primitive n-ième de l'unité notée ξ.
Alors il existe $b \in E$ tel que $b^n := a \in K$ et $E = K(b)$.
En particulier, $Gal(E|K) = Gal(X^n - a|K)$, et $X^n - a$ est irréductible dans $K[X]$.

Démonstration.
· Si $n = 1$, $E = K$ et tout est trivial.
· Supposons $n \geq 2$. Soit g un générateur de $G := Gal(E|K)$. g est un K-endomorphisme de E d'ordre n, donc il annule le polynôme $X^n - 1$ qui est scindé sur K ($\mathbb{U}_n(K) = \{\xi^k,\ 0 \leq k \leq n-1\}$). Donc g est diagonalisable, et ses valeurs propres sont dans $\mathbb{U}_n(K)$.

Pour montrer la proposition, il suffit en fait de montrer qu'une racine primitive n-ième de 1 est valeur propre de g. En effet si ξ est une racine primitive n-ième de 1 valeur propre de g et $b \in E\backslash\{0\}$ un vecteur propre pour ξ ($g(b) = \xi b$), on a $g^k(b) = \xi^k b$ si $0 \leq k \leq n-1$, donc l'orbite de b sous $G =< G >$ a n éléments.
Notons $P := Irr(b, K)$. Les éléments de l'orbite de b sont tous racines de P, donc $[K(b) : K] = deg(P) \geq n$. Par ailleurs $K(b) \subset E$, donc $[K(b) : K] \leq [E : K] = n$. Donc $K(b) = E$.
De plus on a :

$$g^k(b^n) = (g^k(b))^n = (\xi^k b)^n = b^n \text{ pour tout } k, \text{ donc } b^n := a \in E^G = K$$

$X^n - a \in K[X]$ est de degré n et annule b, donc c'est $Irr(b, K)$, irréductible dans $K[X]$.

Montrons donc qu'une racine primitive n-ième de 1 est valeur propre de g, et même que le sous-ensemble Λ des valeurs propres de g est exactement $\mathbb{U}_n(K)$:

- Λ est un sous-groupe de $\mathbb{U}_n(K)$: $1 \in \Lambda$ car $g_{|K} = id$. Si $g(b) = \lambda b$ et $g(b') = \lambda' b'$ (où b, b' vecteurs non nuls de E), alors $g(bb') = g(b)g(b') = \lambda\lambda' bb'$. Comme $bb' \neq 0$, c'est un vecteur propre pour $\lambda\lambda'$, et $\lambda\lambda' \in \Lambda$. Enfin, $\lambda^n = 1$ donc $\lambda^{-1} = \lambda^{n-1} \in \Lambda$.
- $\mathbb{U}_n(K)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, donc $|\Lambda| := d$ divise n. Comme g est diagonalisable, il existe une base composée de vecteur propres de g, et comme $g^d(v) = v$ pour tout vecteur propre v, $g^d = id_E$. Mais g est d'ordre n, donc $d = n$, et $\Lambda = \mathbb{U}_n(K)$. □

3.2 Résolubilité par radicaux des polynômes de degré 2 ou 3

Soit K un corps de caractéristique nulle : on suppose que $\mathbb{Q} \subset K \subset \mathbb{C}$.
Dans toute la suite, pour $z \in \mathbb{C}$, $\sqrt[n]{z}$ désignera **une** racine n-ième de z dans $\mathbb{C}$, fixée une fois pour toutes.

Cas des polynômes de degré 2 : $P := X^2 + aX + b \in K[X]$

Le discriminant est $\Delta = a^2 - 4b \in K$ et les racines sont $\dfrac{-a \pm \sqrt{\Delta}}{2}$
On a $D_K(P) = K(\sqrt{\Delta})$, donc $D_K(P)/K$ est une extension radicale, obtenue en une étape (et P est résoluble par radicaux).

Cas des polynômes de degré 3 : $Q := X^3 + aX^2 + bX + c \in K[X]$

On effectue le changement de variable $X' = X + \dfrac{a}{3}$ pour obtenir Q de la forme
$X'^3 + pX' + q := \widetilde{Q}$. z est une racine de $\widetilde{Q}$ si et seulement si $z - \dfrac{a}{3}$ est une racine de Q.
On pose

$$P := X^3 + pX + q \in K[X]$$

Si P n'est pas irréductible dans $K[X]$, alors P possède une racine $z \in K$ et P est de la forme $(X - z)S$ avec $S \in K[X]$ de degré 2.
On a alors $D_K(P) = D_K(S)$ et on est ramené au cas des polynômes de degré 2 (P est résoluble par radicaux, en une étape).

On suppose donc P irréductible dans $K[X]$, et on note z_1, z_2, z_3 ses trois racines distinctes (proposition 2.1.2).

— Si $p = 0$, $P = X^3 + q$ et ses racines sont les $j^k \sqrt[3]{-q}$ avec $k \in \{0, 1, 2\}$. On a alors $D_K(P) = K(\sqrt[3]{-q}, j\sqrt[3]{-q}, j^2\sqrt[3]{-q}) = K(j, \sqrt[3]{-q})$, et $D_K(P)$ est une extension radicale obtenue en deux étapes (au plus).

— On suppose donc $p \neq 0$. Notons $E := D_K(P)$.
Ajoutons j à E pour la première étape de notre tour d'extensions et notons
$G_1 := Gal(E(j)|K(j))$. P est de degré 3 sans racine dans $K(j)$ (si z est une racine de P dans $K(j)$, $K(z) \subset K(j)$ donc $\underbrace{[K(z) : K]}_{=d^\circ Irr(z,K)=3} \leq \underbrace{[K(j) : K]}_{\leq 2}$, absurde), donc P est irréductible dans $K(j)[X]$.

On a $E(j) = D_{K(j)}(P)$, donc $G_1 = Gal(P|K(j))$ et d'après la proposition 2.1.5, G_1 s'identifie donc à un sous-groupe de $\mathcal{S}_3$ qui agit transitivement sur l'ensemble des racines z_i (une seule orbite à trois éléments). Or le cardinal de l'orbite divise le cardinal du groupe, donc $3 \mid \#G_1 \mid \#\mathcal{S}_3 = 6$ et G_1 s'identifie soit à $\mathcal{A}_3$ soit à $\mathcal{S}_3$. Il sera nécessaire de séparer les deux cas un peu plus loin.

Dans tous les cas, il existe $\sigma \in G_1$ agissant comme le 3-cycle (1 2 3) sur les z_i.

$$\text{Posons } \begin{cases} S' := \sum_{k=0}^{2} j^k \sigma^k = \sum_{g \in <j\sigma>} g \quad , ((j\sigma)^3 = (j\sigma)^0) \\ S'' := \sum_{k=0}^{2} j^{2k} \sigma^k = \sum_{g \in <j^2\sigma>} g \end{cases}$$

S' et S'' sont des $K(j)$-endomorphismes de $E(j)$.

$$\text{Posons } \begin{cases} Z' := S'(z_1) = z_1 + jz_2 + j^2 z_3 \quad (1) \\ Z'' := S''(z_1) = z_1 + j^2 z_2 + jz_3 \quad (2) \end{cases}$$

. *Effectuons quelques calculs concernant Z' et Z'' qui seront utiles pour la suite :*

a) Relations coefficients/racines : $\begin{cases} z_1 + z_2 + z_3 = 0 \\ z_1 z_2 + z_1 z_3 + z_2 z_3 = p \end{cases}$

b) $Z' + Z'' = 3z_1$

c) $Z'Z'' = -3p$ *(en particulier* $Z' \neq 0$, $Z'' \neq 0$, $Z'' = \dfrac{-3p}{Z'}$*)*

d) $K(Z', Z'') = K(Z')$

e) Expression des z_i en fonction de Z' et Z'' :

$$z_1 = \frac{Z' + Z''}{3}, \; z_2 = \frac{j^2 Z' + jZ''}{3}, \; z_3 = \frac{jZ' + j^2 Z''}{3}$$

(donc $z_i \in K(j, Z', Z'') = K(j, Z')$, mais Z' n'est pas à priori une racine n-ième d'un élément de $K(j)$!)

Démonstration.

b) On a $Z' + Z'' = 2z_1 - z_2 - z_3 = -(z_1 + z_2 + z_3) + 3z_1 = 3z_1$

c) On a $Z'Z'' = z_1^2 + z_2^2 + z_3^2 + \underbrace{(j + j^2)}_{=-1}(z_1 z_2 + z_1 z_3 + z_2 z_3)$

$$= (z_1 + z_2 + z_3)^2 - 2(z_1 z_2 + z_1 z_3 + z_2 z_3) - (z_1 z_2 + z_1 z_3 + z_2 z_3)$$
$$= -3(z_1 z_2 + z_1 z_3 + z_2 z_3) = -3p$$

e) On calcule (1)+(2) puis $j^2(1)+j(2)$ et $j(1)+j^2(2)$ et on utilise dans chacun des cas l'égalité $z_1+z_2+z_3=0$.

□

On remarque que $Im(S')$ est fixe par $j\sigma$ et $Im(S'')$ est fixe par $j^2\sigma$. En particulier,

$$\begin{cases} j\sigma(Z')=Z' \\ j^2\sigma(Z'')=Z'' \end{cases}, \; ie \begin{cases} \sigma(Z')=j^2Z'\neq Z' \text{ (car } Z'\neq 0) \\ \sigma(Z'')=jZ''\neq Z'' \text{ (car } Z''\neq 0) \end{cases}$$

Donc Z' et Z'' ne sont pas fixes par $\sigma\in G_1$ et $Z',Z''\notin E(j)^{G_1}=K(j)$.

Deux cas se présentent :

— Soit $G_1\simeq\mathcal{A}_3 : <\sigma>=G_1$, donc comme $\begin{cases} \sigma(Z'^3)=Z'^3 \\ \sigma(Z''^3)=Z''^3 \end{cases}$, Z'^3 et Z''^3 sont fixes par tout élément de G_1, *ie* $Z'^3,Z''^3\in K(j)$. On peut donc ajouter Z' comme seconde étape de notre tour d'extensions, et on obtient :

$$\boxed{K \underset{j^3\in K}{\subset} K(j) \underset{Z'^3\in K(j)}{\subset} \underbrace{K(j,Z')}_{\supset D_K(P)}}$$

Donc P est résoluble par radicaux (en au plus deux étapes).

— Soit $G_1\simeq\mathcal{S}_3 : <\sigma>\neq G_1=<\sigma,\tau>$, où τ est l'élément de G_1 agissant comme la transposition (2 3) sur les z_i. On a

$$\tau^2=id_{E(j)} \text{ et } \tau(Z')=Z'', \text{ donc } \begin{cases} \tau(Z'^3)=Z''^3 \\ \tau(Z''^3)=Z'^3 \end{cases},$$

et Z'^3 et Z''^3 ne sont pas égaux à priori, donc on ne sait pas si Z'^3,Z''^3 sont dans $K(j)$ et on ne peut pas conclure comme dans le premier cas.
En revanche, τ fixe $Z'^3+Z''^3$, donc $Z'^3+Z''^3\in K(j)$ (c'est bien sûr encore vrai si $G_1\simeq\mathcal{A}_3$, donc la suite du raisonnement est également valable dans le premier cas, elle est seulement moins "optimisée").

On a $Z'^3+Z''^3\in K(j)$ et $Z'^3Z''^3\in K(j)$, donc Z'^3 et Z''^3 sont les racines du polynôme $R:=X^2-X(Z'^3+Z''^3)+\underbrace{Z'^3Z''^3}_{=-27p^3}\in K(j)[X]$

Calculons $Z'^3+Z''^3$:

$$(Z'+Z'')^3=Z'^3+Z''^3+3Z'Z''(Z'+Z'')=Z'^3+Z''^3-9p(Z'+Z'')$$

Par ailleurs, $z_1 = \dfrac{Z' + Z''}{3}$, donc $P(z_1) = 0 = \left(\dfrac{Z' + Z''}{3}\right)^3 + p\dfrac{Z' + Z''}{3} + q$,

$$ie\ (Z' + Z'')^3 = -27q - 9p(Z' + Z''), \text{ donc } Z'^3 + Z''^3 = -27q$$

et $R = X^2 + 27qX - 27p^3$. Son discriminant est $\Delta = 27^2\left(\dfrac{27q^2 + 4p^3}{27}\right)$,
et on a vu dans l'exemple précédent que R est résoluble par radicaux, avec

$$D_{K(j)}(R) = K(j)(\sqrt{\Delta})$$

On a ainsi la tour d'extensions :

$$\boxed{K \underset{j^3 \in K}{\subset} K(j) \underset{(\sqrt{\Delta})^2 \in K(j)}{\subset} K(j, \sqrt{\Delta}) \underset{Z'^3 \in K(j,\sqrt{\Delta})}{\subset} \underbrace{K(j, \sqrt{\Delta}, Z')}_{\supset D_K(P)}}$$

Ainsi P est résoluble par radicaux (en au plus trois étapes).
On peut pour terminer calculer explicitement les racines de P :

Z'^3 et Z''^3 sont racines de Q, donc $\begin{cases} Z'^3 = \dfrac{-27q + \sqrt{\Delta}}{2} = 27\left(\dfrac{-q}{2} + \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}\right) \\ Z''^3 = \dfrac{-27q - \sqrt{\Delta}}{2} = 27\left(\dfrac{-q}{2} - \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}\right) \end{cases}$

De l'expression des z_i en fonction de Z' et Z'' (e), on retrouve les formules de Cardan

$$\begin{cases} z_1 = \sqrt[3]{\dfrac{-q}{2} + \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} + \sqrt[3]{\dfrac{-q}{2} - \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} \\ z_2 = j^2\sqrt[3]{\dfrac{-q}{2} + \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} + j\sqrt[3]{\dfrac{-q}{2} - \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} \\ z_3 = j\sqrt[3]{\dfrac{-q}{2} + \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} + j^2\sqrt[3]{\dfrac{-q}{2} - \dfrac{1}{2}\sqrt{\dfrac{(4p^3 + 27q^2)}{27}}} \end{cases}$$

(à partir de ces formules, il est bien sûr facile de retrouver la tour d'extensions ci-dessus)
Ceci termine le paragraphe sur la résolubilité par radicaux des polynômes de degré 2 ou 3.

Comme on vient de le voir, il est important dans l'étude de la résolubilité par radicaux d'un polynôme P de faire des cas sur la façon dont $Gal(P|K)$ s'injecte dans $\mathfrak{S}_R$, où R est l'ensemble des racines de P.
Le résultat suivant donne une condition nécessaire et suffisante pour savoir si $Gal(P|K)$ s'injecte ou non dans $\mathfrak{A}_R$:

Proposition 3.2.1.
Sous l'hypothèse (∗K), soient $P \in K[X]$ et $R := \{\alpha_1, \ldots, \alpha_n\}$ l'ensemble des racines de P. On a :

$$\begin{gathered} \textit{Gal}(P|K) \textit{ est isomorphe à un sous-groupe de } \mathfrak{A}_R \\ \textit{si et seulement si} \\ \textit{le discriminant } \Delta(P) := \prod_{i<j}(\alpha_i - \alpha_j)^2 \textit{ est un carré dans } K \end{gathered}$$

Démonstration.

Notons $G := Gal(P|K)$, $E := D_K(P)$ et $\delta := \prod_{i<j}(\alpha_i - \alpha_j) \in E$. On identifie un élément σ de G à la permutation des racines α_i qui lui est associée par restriction. Pour tout $\sigma \in G$, on a par la proposition 1.2.3 : $\sigma(\delta) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \varepsilon(\sigma)\delta$.

Donc $\delta \in E^G = K \iff \forall \sigma \in G,\ \varepsilon(\sigma) = 1 \iff G \subset \mathfrak{A}_R$. □

Remarque : $G \not\subset \mathfrak{A}_R$ n'implique pas que $G \simeq \mathfrak{S}_R$:
2.3.2 fourni un premier exemple, un autre est donné par le polynôme cyclotomique Φ_7, irréductible de degré $\varphi(7) = 6 = |Gal(\Phi_7|\mathbb{Q})|$. $Gal(\Phi_7|\mathbb{Q})$ n'est pas isomorphe à $\mathfrak{S}_R \simeq \mathfrak{S}_6$ et contient (par un théorème de Sylow) un groupe d'ordre 2, donc une permutation.

3.3 Groupes résolubles

Définition 3.3.1 (Groupe résoluble)**.**
Soit G un groupe. On dit que G est résoluble s'il existe n dans $\mathbb{N}$ et une suite de sous-groupes (dite "suite de résolubilité" de G)

$$G_0 = G \supset G_1 \supset \ldots \supset G_{n-1} \supset G_n = \{1_G\}$$

telle que $\forall i \in \{1, \ldots, n-1\}, G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est abélien.

Autrement dit un groupe résoluble est un groupe qui peut être construit à partir de groupes abéliens par une suite finie d'extensions de groupes :
pour tout $1 \leq i \leq n-1$, on a la suite exacte courte $1 \to G_i \overset{incl.}{\to} G_{i+1} \overset{\pi}{\to} G_{i+1}/G_i \to 1$

Proposition 3.3.2.
*Si K, H sont des sous-groupes de G tels que $K \subset H, K \triangleleft H$ et H/K est abélien **fini**, alors il existe une suite finie de sous-groupes de H*

$$K_0 = K \subset K_1 \subset \ldots \subset K_r = H$$

telle que $\forall i \in \{1, \ldots, r-1\}, K_{i+1} \triangleleft K_i$ et K_i/K_{i+1} est cyclique.

La démonstration est admise.

En particulier si G est un groupe résoluble **fini**, G_i/G_{i+1} est encore fini et il existe donc n' et une suite de sous-groupes

$$G'_0 = G \supset G'_1 \supset \ldots \supset G'_{n'-1} \supset G'_{n'} = \{1_G\}$$

telle que $\forall i \in \{1, \ldots, n'-1\}, G'_{i+1} \triangleleft G'_i$ et G'_i/G'_{i+1} est **cyclique**.

On note $D(G)$ le sous-groupe dérivé de G et $D^n(G) := D(D^{n-1}(G))$ le n-ième groupe dérivé itéré de G. Il sera parfois utile d'utiliser la définition équivalente suivante :

Proposition 3.3.3.
Un groupe G est résoluble si et seulement si il existe n dans $\mathbb{N}$ tel que

$$D^n(G) = \{1_G\}$$

La démonstration est admise.

Présentons quelques résultats (utiles pour la section suivante) sur la résolubilité du groupe symétrique $\mathfrak{S}_n$ suivant les valeurs de n :

Proposition 3.3.4.

a) $\forall n \geq 3, D(\mathfrak{S}_n) = \mathfrak{A}_n$

b) $\mathfrak{S}_2, \mathfrak{S}_3$ *et* $\mathfrak{S}_4$ *sont résolubles*

c) $\forall n \geq 5, \mathfrak{S}_n$ *n'est pas résoluble*

Démonstration. On note ε le morphisme signature.
$a)$ · Soient $a, b \in \mathfrak{S}_n$. $\varepsilon([a,b]) = \varepsilon(a)\varepsilon(b)\varepsilon(a^{-1})\varepsilon(b^{-1}) = 1$, donc $[a,b] \in \mathfrak{A}_n$,
et $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$.
· Réciproquement, soit (abc) un 3-cycle. $(abc) = (ac)(bc)(ac)(bc) = [(ac),(bc)] \in D(\mathfrak{S}_n)$
Or les 3-cycles engendrent $\mathfrak{A}_n$, donc $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$.

$b)$

- $\mathfrak{S}_2$ est commutatif donc $D(\mathfrak{S}_2) = \{id\}$ et $\mathfrak{S}_2$ est résoluble (caractérisation 3.3.3) ;
- $\mathfrak{A}_3$ est commutatif donc d'après $a)$, $D^2(\mathfrak{S}_3) = D(\mathfrak{A}_3) = \{id\}$, et $\mathfrak{S}_3$ est résoluble ;
- Pour $n = 4$, on note V_4 le sous-groupe de $\mathfrak{A}_4$ composé de l'identité et des produits de deux transpositions à supports disjoints. On vérifie facilement que V_4 est distingué dans $\mathfrak{A}_4$. On a ainsi la suite $\{id\} \triangleleft V_4 \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4$. Les quotients successifs sont des groupes d'ordre au plus 4 donc sont tous abéliens, et $\mathfrak{S}_4$ est donc résoluble.

$c)$ Soit $n \geq 5$. Soit (abc) un 3-cycle de $\mathfrak{A}_n$. Il existe deux éléments d, e de $\{1, \ldots, n\}$ tels que a, b, c, d, e soient deux à deux distincts. Alors $(abc) = [(adc),(bec)] \in D(\mathfrak{A}_n)$. Or les 3-cycles engendrent $\mathfrak{A}_n$, donc $\mathfrak{A}_n \subset D(\mathfrak{A}_n)$. L'autre inclusion est évidente. Ainsi $\forall k \leq 1, D^k(\mathfrak{S}_n) = \mathfrak{A}_n \neq \{id\}$, donc $\mathfrak{S}_n$ n'est pas résoluble.

□

Proposition 3.3.5.
L'image d'un groupe résoluble par un morphisme est un groupe résoluble.

Démonstration. Soit G un groupe résoluble et $\phi : G \to H$ un morphisme de groupes. D'après la caractérisation 3.3.3, il suffit de montrer que $D^n(\phi(G)) = \{1_H\}$ pour un certain n dans $\mathbb{N}$. Par hypothèse, il existe n dans $\mathbb{N}$ tel que $D^n(G) = \{1_G\}$. Montrons que $D^n(\phi(G)) \subset \phi(D^n(G))$:
Soit $[a,b]$ un commutateur de $\phi(G)$. Il existe x, y dans G tels que $a = \phi(x)$ et $b = \phi(y)$.

$$[a,b] = [\phi(x), \phi(y)] = \phi([x,y]) \in \phi(D(G))$$

Or les commutateurs de $\phi(G)$ engendrent $D(\phi(G))$, donc $D(\phi(G)) \subset \phi(D(G))$. Une récurrence immédiate donne $D^n(\phi(G)) \subset \phi(D^n(G))$, et $\phi(D^n(G)) = \phi(\{1_G\}) = \{1_H\}$, donc $\phi(G)$ est résoluble.

□

3.4 Théorème d'Abel-Galois

Théorème 3.4.1 (Théorème d'Abel-Galois)**.**
Soient K un corps de caractéristique nulle et $P \in K[X]$.
Alors P est résoluble par radicaux si et seulement si $Gal(P|K)$ est résoluble.

Avant de démontrer ce théorème, utilisons-le pour répondre à une question historiquement très importante :

les polynômes de degré 5 (ou plus) sont-ils tous résolubles par radicaux ?

Des réponses partielles et non constructives ont été données par Ruffini (1799) puis Abel (1824), mais il faudra attendre les travaux de Galois (vers 1830) pour obtenir un exemple concret de polynôme de degré 5 non résoluble par radicaux. Nous aurons besoin du lemme suivant :

Lemme 3.4.2.
Soient p un nombre premier et P un polynôme irréductible de $\mathbb{Q}[X]$ de degré p.
Si P a exactement 2 racines non réelles dans $\mathbb{C}$, alors $Gal(P|\mathbb{Q})$ est isomorphe à $\mathfrak{S}_p$.

Démonstration.

- Puisque P est irréductible, G agit transitivement sur l'ensemble $R = \{\alpha_1, \ldots, \alpha_p\}$ des p racines distinctes (2.1.2) de P dans $\mathbb{C}$. Par la proposition 2.1.5, G s'identifie par restriction à un sous-groupe de $\mathfrak{S}_p \simeq \mathfrak{S}_R$. Or $|\mathfrak{S}_p| = p(p-1)!$, donc par un théorème de Sylow, $\mathfrak{S}_p$ contient un groupe d'ordre p, donc un p-cycle. G "contient" donc un p-cycle (par restriction aux racines).

- La conjugaison complexe τ (d'ordre 2) fixe les coefficients de P et induit donc une permutation de R qui a par hypothèse exactement $p-2$ points fixes : c'est la transposition $(p-1 \quad p)$ si on note α_{p-1} et α_p les deux racines non réelles. De plus le corps de décomposition (dans $\mathbb{C}$) de P sur $\mathbb{Q}$ est $\mathbb{Q}(\alpha_1, \ldots, \alpha_p)$, donc $\tau(D_{\mathbb{Q}}(P)) = D_{\mathbb{Q}}(P)$, et τ induit donc par restriction un élément de G d'ordre 2, *ie* une transposition.

G "contient" ainsi un p-cycle et une transposition. Par la proposition 1.2.2, G est donc isomorphe à $\mathfrak{S}_p$.

□

Proposition 3.4.3.
Le polynôme $P := X^5 - 6X + 3$ de $\mathbb{Q}[X]$ n'est pas résoluble par radicaux.

Démonstration.

Le critère d'Eisenstein pour $p = 3$ montre que P est irréductible dans $\mathbb{Q}[X]$. Puisque $deg(P) = 5$ est premier et que $\mathfrak{S}_5$ n'est pas résoluble (3.3.4), il suffit d'après le théorème d'Abel-Galois (3.4.1) et le Lemme précédent de vérifier que P a exactement 3 racines réelles (et donc 2 non réelles).

On a $P' = 5X^4 - 6$. En posant $x_0 := \sqrt[4]{6/5}$ (> 1), on obtient le tableau de variation de P :

x	$-\infty$		$-x_0$	-1	1	x_0		$+\infty$
$P'(x)$		$+$	0	$-$		0	$+$	
$P(x)$	$-\infty$	$\nearrow$	> 0	$\searrow$	8	$\searrow$	< 0	$\nearrow$ $+\infty$
					-2			

$P(-1) = 8$ et $P(1) = -2$, donc $P(-x_0) > 0$ et $P(x_0) < 0$. Ainsi P s'annule exactement 3 fois sur $\mathbb{R}$, d'où le résultat.

□

Ce résultat montre en particulier qu'il n'existe pas de formule générale d'expression des racines par radicaux pour les polynômes de degré 5, contrairement aux degrés 2,3 (vu au 3.2) et 4 (méthode de Ferrari).

Démonstration du théorème d'Abel-Galois :

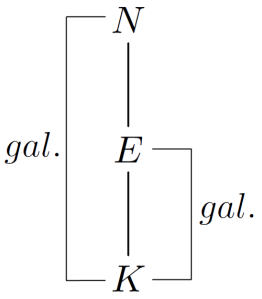
P résoluble par radicaux $\Longrightarrow$ $Gal(P|K)$ résoluble :

Si P a toutes ses racines dans K, $D_K(P) = K$ et $Gal(P|K) = \{id_K\}$ est résoluble. Dans le cas contraire, il existe par hypothèse s dans $\mathbb{N}^*$, $n_1, \ldots, n_s$ dans $\mathbb{N}^*$ et des éléments $a_1, \ldots, a_s$ tels que $D_K(P) \subset K(a_1, \ldots, a_s)$, ${a_1}^{n_1} \in K$ et $\forall i \in \{2, \ldots, s\}$, ${a_i}^{n_i} \in K(a_1, \ldots, a_{i-1})$. On note $L := K(a_1, \ldots, a_s)$ l'extension radicale obtenue et $E := D_K(P)$.

On va chercher une extension N de E telle que N/K soit galoisienne et $Gal(N|K)$ soit résoluble. En effet comme E/K est également galoisienne, le dernier point de la correspondance de Galois donnera :

$$Gal(E|K) \simeq Gal(N|K)/Gal(N|E) = \pi(Gal(N|K))$$

où π est la surjection canonique sur le quotient. $Gal(P|K)$ sera donc résoluble comme image d'un groupe résoluble par un morphisme de groupes (3.3.5).



On a $E \subset L$, mais comme L/K n'est à priori ni galoisienne ni de groupe de Galois résoluble, on va étendre L pour obtenir l'extension N désirée :

Fait . *Il existe un entier $t \geq 2$, $m_2, \ldots, m_t$ dans $\mathbb{N}^*$ et une extension $N := K(\xi, b_2, \ldots, b_t)$ contenant L telle que N/K est galoisienne radicale et vérifie :*

- *${b_i}^{m_i} \in K_{i-1}$ $\forall i \in \{2, \ldots, t\}$, où $K_1 := K(\xi)$ et $K_i := K(\xi, b_2, \ldots, b_i)$, $i \geq 2$*
- *ξ est une racine primitive m-ième de l'unité dans $\mathbb{C}$, où $m := PPCM(n_1, \ldots, n_s)$*
- *K_{i+1}/K_i est galoisienne pour tout i dans $\{1, \ldots, t-1\}$*
- *K_{i+1}/K_i est abélienne (cf. 3.1.2) pour tout i dans $\{1, \ldots, t-1\}$*

Démonstration.

Soient : ξ une racine primitive m-ième de l'unité dans $\mathbb{C}$, où $m := PPCM(n_1, \ldots, n_s)$

$L' := K(\xi, a_1, \ldots, a_s)$ l'extension de L obtenue par l'ajout de ξ

$P_i := Irr(a_i, K)$ le polynôme minimal de a_i sur K $(1 \leq i \leq s)$

$N := D_{L'}(\prod_{i=1}^{s} P_i)$ un corps de décomposition **sur** L'

R_i l'ensemble des racines de P_i dans N.

On a $a_j \in \bigcup_{i=1}^{s} R_i$ pour tout j dans $\{1, \ldots, s\}$, et :

$$N = L'(\bigcup_{i=1}^{s} R_i) = L(\xi, \bigcup_{i=1}^{s} R_i) = K(\xi, \bigcup_{i=1}^{s} R_i) = D_K\Big(\overbrace{(X^m - 1)(\prod_{i=1}^{s} P_i)}^{:=Q}\Big) = D_K(Q)$$

Donc N est galoisienne **sur** K (*ie* N/K est galoisienne). On note $\bigcup_{i=1}^{s} R_i := \{b_2, \ldots, b_t\}$, où on numérote successivement les éléments de R_1, R_2 , ..., R_s. Montrons que N/K est radicale, et plus précisément que pour $j \in \{2, \ldots, t\}$,

si $b_j \in R_i$, alors ${b_j}^{n_i} \in K(\xi, \bigcup_{l=1}^{i-1} R_l)$ $(\subset \overbrace{K(\xi, b_2, \ldots, b_{j-1})}^{=K_{j-1}})$. On pose alors $m_j := n_i$, $j \geq 2$

Pour tout $i \in \{1, \ldots, s\}$, P_i est un facteur irréductible (sur K) du polynôme Q, donc d'après 2.1.5 b), R_i est une orbite sous $Gal(N|K)$ de l'ensemble des racines de Q : si $b_j \in R_i$ $(2 \leq j \leq t)$, alors il existe $g \in Gal(N|K)$ tel que $g(a_i) = b_j$. On a alors :

$${b_j}^{n_i} = g({a_i}^{n_i}), \text{ et par hypothèse } {a_i}^{n_i} \in K(\xi, \bigcup_{l=1}^{i-1} R_l) = D_K\left((X^m - 1)(\prod_{i=1}^{i-1} P_l)\right) := N_{i-1}$$

Comme $g(N_{i-1}) = N_{i-1}$ (car g fixe K, $g(\xi) = \xi^k$ est encore une racine de $X^m - 1$, et $g(R_l) = R_l$ pour chaque l), on a ${b_j}^{n_i} \in N_{i-1}$ $(2 \leq j \leq t)$. En notant $b_1 := \xi$, on a également ${b_1}^m \in K$, donc N/K est radicale.

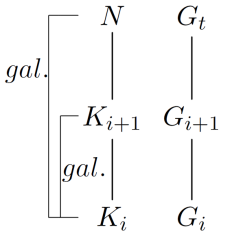
K_{i+1}/K_i est abélienne : en effet, m_i divise m pour tout i, et $\xi \in K_i$, donc (proposition 3.1.4) K_i contient une racine primitive m_i-ième de l'unité (ξ^{m/m_i}). Or on vient de voir que $u := (b_{i+1})^{m_{i+1}} \in K_i$, donc d'après la proposition 3.1.3,

$$K_{i+1}/K_i = K_i(b_{i+1}) = D_{K_i}(X^{m_{i+1}} - u) \text{ extension cyclique de } K_i$$

□

On en déduit l'implication cherchée :
Soit N comme dans le Fait. Montrons que $Gal(N|K)$ est résoluble (*cf.* définition 3.3.1) : Posons $G_0 := Gal(N|K)$ et $G_i := Gal(N|K_i)$, $i \in \{1, \ldots, t\}$.

$$\text{On a : } G_t = \{id_N\} \subset G_{t-1} \subset \ldots \subset G_1 \subset G_0$$



N/K est galoisienne, donc (1.1.7) N/K_i est encore galoisienne pour tout $i \in \{1, \ldots, t-1\}$, et :
· On a $G_{i+1} \triangleleft G_i$ d'après la correspondance de Galois, car K_{i+1}/K_i est galoisienne.
· Le quotient G_i/G_{i+1} est abélien d'après la correspondance de Galois : $G_i/G_{i+1} \simeq Gal(K_{i+1}|K_i)$, groupe cyclique.

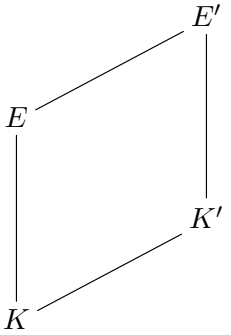
Donc $Gal(N|K)$ est résoluble.

Pour la preuve de l'autre implication, nous aurons besoin du lemme suivant :

Lemme 3.4.4 (Lemme "du trapèze").
Soit E/K une extension galoisienne. Soit K' un corps contenant K, et soit $E' := K'(E)$. Alors E'/K' est galoisienne, et $Gal(E'|K')$ est isomorphe à un sous-groupe de $Gal(E|K)$.

Démonstration.

· E/K est galoisienne, donc de la forme $D_K(P) = K(\alpha_1, \ldots \alpha_n)$, où $R := \{\alpha_1, \ldots \alpha_n\}$ est l'ensemble des racines de $P \in K[X]$.
$E' = K'(E) = K'(\alpha_1, \ldots \alpha_n) = D_{K'}(P)$ car $P \in K'[X]$,
donc E'/K' est galoisienne.
· Si $g \in Gal(E'|K')$, g fixe K et $g(R) = R$, donc la restriction : $\rho : Gal(E'|K') \longrightarrow Gal(E|K)$ est bien définie et est un morphisme de groupes.



Enfin, $E' = K'(\alpha_1, \dots \alpha_n)$, donc pour $g \in Gal(E'|K')$,

$$\rho(g) = id_E \Longrightarrow g \text{ fixe } K' \text{ et chaque } \alpha_i \Longrightarrow g = id_{E'}$$

Donc ρ est injectif, et $Gal(E'|K')$ est isomorphe à un sous-groupe de $Gal(E|K)$.

□

$Gal(P|K)$ résoluble $\Longrightarrow$ P résoluble par radicaux :

Soit E un corps de décomposition de P sur K.

a) **Premier cas :** K contient une racine primitive n-ième de l'unité ξ, où $n = |G|$:
Puisque $G := Gal(P|K)$ est résoluble **finie**, il admet (proposition 3.3.2) une suite

$$G = G_0 \subset G_1 \subset \ldots \subset G_m = \{id_E\} \text{ de sous-groupes}$$

telle que pour tout $i \in \{0, \dots, m-1\}$, $G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est **cyclique**.
On va montrer grâce à la correspondance de Galois que E/K est radicale :
Pour $i \in \{0, \dots, m\}$, posons $K_i := \Phi(G_i) = E^{G_i}$. Ainsi on a une suite

$$K = K_0 \subset K_1 \subset \ldots \subset K_m = E$$

Comme E/K est galoisienne, E/K_i est galoisienne pour tout i d'après la correspondance de Galois, et $Gal(E|K_i) = \Gamma \circ \Phi(G_i) = G_i$. Puisque $G_{i+1} \triangleleft G_i$, K_{i+1}/K_i est galoisienne (deuxième point de la correspondance de Galois). De plus on a $Gal(K_{i+1}|K_i) \simeq Gal(K|K_i)/Gal(K|K_{i+1}) = G_i/G_{i+1}$, cyclique, donc K_{i+1}/K_i est cyclique, de degré $\dfrac{|G_i|}{|G_{i+1}|} := n_{i+1}$ (et n_{i+1} divise n).
Comme K contient une racine primitive (n_{i+1})-ième de 1 (proposition 3.1.4), les hypothèse de la proposition 3.1.5 sont donc vérifiées, et il existe donc $b_{i+1} \in K_{i+1}$ tel que $K_{i+1} = K_i(b_{i+1})$, et $(b_{i+1})^{n_{i+1}} \in K_i$.
On trouve ainsi par récurrence $E = K(b_1, \dots, b_m)$, extension radicale de K.

b) **Cas général :** On va se ramener au premier cas :
Soit ξ une racine primitive n-ième de 1 dans $D_E(X^n - 1) = E(\xi)$. Par le lemme "du trapèze" (3.4.4), $Gal(E(\xi)|K(\xi))$ est isomorphe à un sous-groupe de $Gal(E|K)$ qui est résoluble par hypothèse, donc $Gal(E(\xi)|K(\xi))$ est résoluble (3.3.3).
On est ainsi ramené au premier cas, et $E(\xi)/K(\xi)$ est donc radicale, de la forme $K(\xi)(a_1, \dots, a_s) = K(\xi, a_1, \dots, a_s)$ avec ${a_i}^{n_i} \in K(\xi, a_1, \dots, a_i - 1)$ $\forall i \geq 1$, et $\xi^n \in K$, donc $E(\xi)/K$ est encore radicale, et E/K est résoluble par radicaux.

□

Remarque :
D'après le Fait de la première partie de la preuve, il suffit pour qu'un polynôme $P \in K[X]$ **irréductible** soit résoluble par radicaux qu'un corps de rupture de P soit résoluble par radicaux.
En effet, si $K(\alpha)$ est un corps de rupture de P résoluble par radicaux, il existe une extension radicale L/K contenant $K(\alpha)$. On peut alors prendre N comme dans le Fait : N est radicale et **galoisienne**, donc P est scindé dans N (point c de la proposition 2.1.10), donc $D_K(P) \subset N$.

FIN