M1 2023-2024 : Corps, théorie de Galois

David Harari

Table des matières

1. Extensions de corps

1.1. Corps et espaces vectoriels

Rappelons qu'un corps K est par définition un anneau commutatif *non nul* dans lequel tout élément non nul est inversible, i.e. $K^* = K \setminus \{0\}$.

Définition 1.1 La *caractéristique* d'un corps K est l'entier $n \in \mathbf{N}$ tel que le noyau de l'application $\mathbf{Z} \to K$, $x \mapsto x.1_K$ soit $n\mathbf{Z}$.

Comme pour tout anneau intègre, la caractéristique d'un corps est zéro ou un nombre premier p. Si K est de caractéristique $p > 0$, alors l'application $x \mapsto x^p$ est un morphisme de corps de K dans K, via la formule du binôme de Newton et le fait que p divise C_p^k pour $0 < k < p$.

Exemple 1.2 a) $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ sont des corps de caractéristique zéro.

b) Pour p premier, $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z}(T)$ sont des corps de caractéristique p (noter que le second est infini).

c) $\mathbf{Q}(i) := \{a + ib, (a, b) \in \mathbf{Q} \times \mathbf{Q}\}$ est un corps de caractéristique zéro ; c'est le corps des fractions de l'anneau $\mathbf{Z}[i]$.

Définition 1.3 Soit K un corps. Une *extension* de K est un corps L tel que K soit un sous-corps de L. Une *extension intermédiaire* entre L et K est un corps F tel que $K \subset F \subset L$.

Si L est une extension de K, il est muni *ipso facto* d'une structure de K-espace vectoriel (et même de K-algèbre) via la multiplication.

Définition 1.4 Si $\varphi : K \to L$ est un morphisme de corps, il est injectif et on peut considérer L comme une extension de K en identifiant K à $\varphi(K) \simeq K$. Si L et M sont deux extensions d'un corps K, un *K-morphisme* de L dans M est un morphisme de corps qui est en même temps un morphisme de K-algèbres, i.e. qui induit l'identité sur K vu comme sous-corps de L et M.

On notera souvent L/K l'extension L de K (pour insister sur le fait qu'on regarde L pas seulement comme un corps, mais aussi comme une K-algèbre). On fera attention à ne pas confondre avec un quotient (cette notation pour les extensions est malheureusement traditionnelle).

Exemple 1.5 a) Le corps $\mathbf{C}$ est une extension de $\mathbf{Q}$ et $\mathbf{R}$ en est une extension intermédiaire. Plus généralement, tout corps de caractéristique zéro est une extension de $\mathbf{Q}$, via le morphisme $p/q \mapsto p.1/q.1$ pour $p \in \mathbf{Z}$ et q non nul dans $\mathbf{Z}$.

b) Soit K un corps de caractéristique $p > 0$. Alors le morphisme $\bar{x} \mapsto x.1$ de $\mathbf{Z}/p\mathbf{Z}$ dans K est bien défini, et fait de K une extension de $\mathbf{Z}/p\mathbf{Z}$.

Définition 1.6 Si L est de dimension finie sur K, on note $[L : K]$ la dimension du K-espace vectoriel L ; c'est un entier > 0 qu'on appelle le *degré* de L sur K. On dit dans ce cas que L est *finie* sur K. [1]

Proposition 1.7 ("Base téléscopique") *Soient M un corps, L un sous-corps de M, K un sous-corps de L. Alors si $(e_i)_{i\in I}$ est une base de L sur K et $(f_j)_{j\in J}$ est une base de M sur L, la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.*

Démonstration : Si $\sum_{(i,j)\in I\times J} \lambda_{ij} e_i f_j = 0$ avec (λ_{ij}) famille presque nulle d'éléments de K, alors $\sum_{j\in J} f_j(\sum_{i\in I} \lambda_{ij} e_i) = 0$; comme (f_j) est une famille libre du L-ev M, on obtient pour tout j de J : $\sum_{i\in I} \lambda_{ij} e_i = 0$, et comme (e_i) est une famille libre du K-ev L, on a (j étant fixé) $\lambda_{ij} = 0$ pour tout i de I. Finalement la famille (λ_{ij}) est nulle et $(e_i f_j)$ est une famille libre du K-ev M. Si maintenant $x \in M$, on peut écrire $x = \sum_{j\in J} \alpha_j f_j$ avec (α_j) famille presque nulle d'éléments de L, puis en décomposant chaque α_j sur la base (e_i) du K-ev L, on voit que x est combinaison linéaire des $e_i f_j$. Finalement $(e_i f_j)$ est aussi une famille génératrice du K-ev M.

□

Corollaire 1.8 *Si L est finie sur K et M est finie sur L, alors M est finie sur K et on a*

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

Bien que facile, ce corollaire est extrêmement utile, comme on le verra plus loin.

1.2. Éléments algébriques et transcendants

Définition 1.9 Soient L/K une extension de corps et $\alpha \in L$. On note

- $K[\alpha]$ la sous K-algèbre de L engendrée par α, qui est aussi l'ensemble des $P(\alpha)$ avec $P \in K[T]$.
- $K(\alpha)$ le sous-corps de L engendré par K et α ; c'est le corps des fractions de $K[\alpha]$, ou encore l'ensemble des $R(\alpha)$ avec $R \in K(T)$ (quand cette expression est définie, i.e. quand le dénominateur de R n'annule pas α).

1. Attention à ne pas confondre à ce que l'on appelle parfois un corps de type fini sur K, qui signifie que L est une extension finie d'un corps de fractions rationnelles $K(T_1, ..., T_n)$; par ailleurs, un théorème (difficile) affirme que si L est un corps qui est une K-algèbre de type fini, alors L est une extension finie de K. Voir les TD sur les anneaux

Définition 1.10 Soient L/K une extension de corps et $\alpha \in L$. On définit un morphisme de K-algèbres $\varphi : K[T] \to L$ par $P \mapsto P(\alpha)$.

- Si φ est injectif, alors $K[\alpha] \simeq K[T]$ et $K(\alpha) \simeq K(T)$. On dit alors que α est *transcendant* sur K.
- Si φ n'est pas injectif, on note π le générateur unitaire de $\ker \varphi$. On dit que α est *algébrique* sur K et on appelle π le *polynôme minimal* de α sur K.

Bien noter que les notions d'élément algébrique et transcendant dépendent du corps de base K (tout élément de L est évidemment algébrique sur L). Noter aussi que le polynôme minimal π est toujours irréductible sur K (car L est un anneau intègre donc si le produit de deux polynômes de $K[T]$ annule α, l'un de ces deux polynômes annule α).

Exemple 1.11 a) i est algébrique sur $\mathbf{Q}$, de polynôme minimal $X^2 + 1$.

b) L'élément T de $K(T)$ est transcendant sur K (par définition !).

c) L"ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est dénombrable car $\mathbf{Q}[X]$ est dénombrable (c'est la réunion pour $n \in \mathbf{N}$ des polynômes de $\mathbf{Q}[X]$ de degré au plus n), et chaque polynôme non nul de $\mathbf{Q}[X]$ n'a qu'un nombre fini de racines dans $\overline{\mathbf{Q}}$. L'ensemble $\mathbf{R} \cap \overline{\mathbf{Q}}$ des réels algébriques est donc également dénombrable ("presque tous les réels sont transcendants sur $\mathbf{Q}$"). Il y a donc beaucoup plus de nombres réels ou complexes transcendants sur $\mathbf{Q}$ que de nombres algébriques, bien qu'exhiber explicitement un nombre transcendant soit assez difficile !

Proposition 1.12 *Soient L/K une extension de corps et $\alpha \in L$. Il y a équivalence entre :*

1. *α est algébrique sur K.*
2. *$K[\alpha] = K(\alpha)$.*
3. *$K[\alpha]$ est un K-espace vectoriel de dimension finie.*

Si ces conditions sont satisfaites, alors l'entier $[K(\alpha) : K]$ est le degré du polynôme minimal de α ; on l'appelle le degré de α sur K.

Démonstration : 1. implique 2. car dans ce cas $K[\alpha]$ est un anneau isomorphe à $K[T]/(\pi)$ avec π irréductible, donc comme $K[T]$ est un anneau principal, $K[\alpha]$ est un corps et il est égal à son corps des fractions $K(\alpha)$.

2. implique 1. car si α est transcendant, alors l'anneau $K[\alpha]$ est isomorphe à $K[T]$ qui n'est pas un corps.

1. implique 3. car si π est le polynôme minimal de α, alors le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]/(\pi)$ qui est de dimension $\deg \pi$ (via la division euclidienne par π dans $K[T]$).

3. implique 1. car si α est transcendant, le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]$ qui est de dimension infinie.

□

Définition 1.13 Une extension L/K est dite *algébrique* si tout élément de L est algébrique sur K.

Ainsi toute extension finie est algébrique (via la caractérisation 3. de l'énoncé précédent), mais on verra que la réciproque est fausse.

Le théorème principal sur les éléments algébriques est le suivant :

Theorème 1.14 *Soit L/K une extension de corps. On note M l'ensemble des éléments de L qui sont algébriques sur K. Alors :*

1. *M est un sous-corps de L.*
2. *Tout élément de L qui est algébrique sur M est dans M ; on dit que M est la fermeture algébrique de K dans L.*
3. *En particulier, si L est algébriquement clos, M est algébriquement clos ; on dit dans ce cas que M est une clôture algébrique de K.*

Rappelons qu'un corps F est dit *algébriquement clos* si tout polynôme de $F[X]$ est scindé sur F, ou encore si les seuls polynômes irréductibles de $F[X]$ sont de degré 1. C'est aussi équivalent à dire que tout polynôme non constant de $F[X]$ admet une racine dans F. Par exemple $\mathbf{C}$ est un corps algébriquement clos.

Remarque 1.15 Plus généralement on dit qu'une extension $\overline{K}$ de K est une *clôture algébrique* de K si $\overline{K}$ est algébriquement clos, et $\overline{K}/K$ est algébrique. D'après le théorème précédent, une telle clôture existe dès qu'il existe une extension L de K qui est algébriquement close ; ceci est toujours vrai (on peut le déduire de l'existence d'un idéal maximal dans tout anneau commutatif non nul, cf. TD). D'autre part, la clôture algébrique est unique à isomorphisme près (c'est encore une conséquence du lemme de Zorn joint au théorème 1.14).

Preuve du théorème : 1. Clairement $M \supset K$, donc 0 et 1 sont algébriques sur K. Si $x \in L$ est algébrique sur K, alors il existe un polynôme unitaire $X^n + ... + a_0$ dans $K[X]$ qui annule x. Alors $(-1)^n X^n + ... + a_0$ annule $-x$ et $1 + ... + a_0 X^n$ annule x^{-1}, donc $-x$ et x^{-1} sont algébriques sur K. Il

s'agit maintenant de montrer que si x, y sont dans M, alors $x+y$ et xy sont encore dans M. Or $K[x] = K(x)$ est un corps, et y, qui est algébrique sur K l'est a fortiori sur $K[x]$, c'est-à-dire que $K[x,y] = K[x][y]$ est de dimension finie sur $K[x]$, donc aussi sur K via le théorème de la base téléscopique. Comme $K[x,y]$ contient $K[x+y]$ et $K[xy]$, il en résulte que ces deux derniers K-espaces vectoriels sont de dimension finie, ce qui signifie que $x+y$ et xy sont dans M.

2. Soit $x \in L$, algébrique sur M. Alors il existe un polynôme unitaire $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ de $M[X]$ qui annule x. Comme chaque a_i est algébrique sur K, on a par récurrence (via la base téléscopique) que $K[a_0, ..., a_{n-1}] = K(a_0, ..., a_{n-1})$ est un corps K' qui est de dimension finie sur K. Comme $P \in K'[X]$ est non nul et annule x, il en résulte que x est algébrique sur K', i.e. $K'[x]$ est de dimension finie sur K' ; comme K'/K est finie, $K'[x]$ est aussi de dimension finie sur K, et $K[x]$ (qui en est un sev) aussi, i.e. x est algébrique sur K. Finalement $x \in M$.

3. Si $P \in M[X]$ est non constant, il admet une racine x dans le corps algébriquement clos L, mais x est alors algébrique sur M, donc $x \in M$ d'après 2.

□

Exemple 1.16 L'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est un corps algébriquement clos dénombrable, et c'est une clôture algébrique de $\mathbf{Q}$. L'extension algébrique $\overline{\mathbf{Q}}/\mathbf{Q}$ n'est pas finie, car il existe des polynômes irréductibles de degré arbitraire sur $\mathbf{Q}$ (par exemple $X^d - p$ pour $d \in \mathbf{N}^*$ et p premier via le critère d'Eisenstein), qui fournissent donc des nombres algébriques de degré arbitrairement grand sur $\mathbf{Q}$.

1.3. Corps de rupture, corps de décomposition

Étant donnés K un corps et P un polynôme de $K[X]$, on cherche une extension L de K dans laquelle P a une racine. Cela amène la définition suivante :

Définition 1.17 Soit P un polynôme *irréductible* de $K[X]$. On dit qu'une extension L de K est un *corps de rupture* pour P sur K s'il existe une racine α de P dans L telle que $L = K[\alpha]$ $(= K(\alpha)$ puisque α est algébrique sur $K)$.

Ainsi un corps de rupture est une extension dans laquelle P a une racine, et qui est minimale pour cette propriété.

Theorème 1.18 *Pour tout polynôme irréductible $P \in K[X]$, il existe un corps de rupture L. De plus L est unique à K-isomorphisme près.*

Remarque 1.19 Noter qu'on n'aurait pas unicité si P n'était pas irréductible, prendre $P = (X^2-2)(X^2-3)$ sur $\mathbf{Q}$, et les corps $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ (ils ne sont pas isomorphes car 2 est un carré dans le premier et pas dans le second).

Démonstration : Comme P est irréductible et l'anneau $K[X]$ est principal, la K-algèbre $L = K[X]/(P)$ est un corps vu que (P) est un idéal maximal de $K[X]$. Si on prend pour α la classe de X dans $K[X]/(P)$, on a $P(\alpha) = 0$ et $L = K[\alpha]$, donc L est un corps de rupture pour P sur K. D'où l'existence.

Si maintenant L' est un corps de rupture pour P sur K, soit α' avec $L' = K[\alpha']$ et $P(\alpha') = 0$. Alors le morphisme de K-algèbres défini par $K[X] \to L'$, $Q \mapsto Q(\alpha')$ est surjectif, de noyau (P) car le noyau (qui ne contient pas 1) contient (P) avec P irréductible (donc (P) maximal puisque $K[X]$ est principal). Finalement on obtient un K-isomorphisme de $L = K[X]/(P)$ sur L'.

□

Remarque 1.20 On a plus précisément que si $L = K[\alpha]$ est un corps de rupture pour P, L' une extension de corps de K, et β une racine de P dans L', il existe un unique K-morphisme de L dans L' qui envoie α sur β : on l'obtient en envoyant tout $Q(\alpha) \in L$ (avec $Q \in K[X]$) sur $Q(\beta)$, ce qui a bien un sens car si Q et R sont deux polynômes de $K[X]$ tels que $Q(\alpha) = R(\alpha)$, alors $(Q - R)$ est divisible par le polynôme minimal P de α donc $Q(\beta) = R(\beta)$.

Exemple 1.21 a) $\mathbf{C}$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{R}$.

b) $\mathbf{Q}(i)$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{Q}$.

c) $\mathbf{Q}(\sqrt[3]{2})$ est le corps de rupture[2] de $X^3 - 2$ sur $\mathbf{Q}$. Noter qu'ici le polynôme $X^3 - 2$ *n'est pas scindé* sur $\mathbf{Q}(\sqrt[3]{2})$ (il a deux racines complexes non réelles). Ce phénomène ne se produit pas pour les polynômes de degré 2 parce que si $X^2 + aX + b$ possède une racine x dans L, alors l'autre racine $-x - a$ est encore dans L.

Le dernier exemple ci-dessus conduit à la définition suivante :

Définition 1.22 Soient K un corps et P un polynôme (qu'on ne suppose pas irréductible) de $K[X]$. On dit qu'une extension L/K est un *corps de décomposition* pour P sur K si L vérifie les deux propriétés suivantes :

i) P est scindé sur L.

ii) On a $L = K(\alpha_1, ..., \alpha_n)$, où $\alpha_1, ..., \alpha_n$ sont les racines de P dans L.

2. Ici on devrait vraiment dire "un" corps de rupture parce qu'il n'y a pas unicité en tant que sous-corps de $\mathbf{C}$: $\mathbf{Q}(j^3\sqrt{2})$ et $\mathbf{Q}(j^2.^3\sqrt{2})$ conviennent aussi, où j est une racine primitive cubique de 1.

Ainsi un corps de décomposition est une extension minimale de K sur laquelle P est scindé. Noter qu'on a aussi $L = K[\alpha_1, ..., \alpha_n]$ vu que les α_i sont algébriques sur K.

Theorème 1.23 *Pour tout P de $K[X]$, il existe un corps de décomposition L, qui est unique à K-isomorphisme près.*

Démonstration : On commence par un lemme un peu plus précis que l'unicité voulue, qui est utile en lui-même (on en aura besoin sous cette forme pour la théorie de Galois) :

Lemme 1.24 *Soient $\varphi : K \to K'$ un isomorphisme de corps, P un polynôme de $K[X]$, et L, L' des corps de décomposition respectifs de P sur K, $\varphi(P)$ sur K'. Alors il existe un isomorphisme de corps $\psi : L \to L'$ qui prolonge φ (en abrégé, les extensions L/K et L'/K' sont isomorphes), c'est à dire qu'on a un diagramme commutatif :*

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i'} \\ K & \xrightarrow{\varphi} & K' \end{array}$$

En particulier $[L : K] = [L' : K']$. De plus, le nombre d'isomorphismes ψ comme ci-dessus est au plus $[L : K]$, et il est égal à $[L : K]$ si on suppose en outre que P est à racines simples dans L.

Noter que le polynôme P n'est pas supposé irréductible dans cet énoncé.

Preuve du lemme 1.24 : On procède par récurrence sur $\deg P$. Si P est scindé (en particulier si $\deg P \leq 1$), on a $L = K$, $L' = K'$ et l'assertion est évidente. Sinon soit α racine de P dans $L \setminus K$, de polynôme minimal $Q \in K[X]$. Alors $\varphi(Q)$ admet une racine α' dans L' et $K[\alpha]$, $K[\alpha']$ sont des corps de rupture respectifs de Q, $\varphi(Q)$ sur K, K'. On prolonge φ en un isomorphisme $\varphi_1 : K[\alpha] \to K'[\alpha']$ en envoyant α sur α' : plus précisément pour tout polynôme R de $K[X]$, on définit $\varphi_1(R(\alpha)) = \varphi(R)(\alpha')$, ce qui a bien un sens (cf. remarque 1.20 dans le cas $K' = K$) puisque les polynômes minimaux de α, α' sur K, K' sont respectivement Q, $\varphi(Q)$. On écrit $P = (X - \alpha)P_1$ et $\varphi_1(P) = (X - \alpha')\varphi_1(P_1)$ avec $P_1 \in K[\alpha][X]$, puis on applique l'hypothèse de récurrence au polynôme P_1. L, L' sont des corps de décomposition respectifs de P_1, $\varphi_1(P_1)$ sur $K[\alpha]$, $K'[\alpha']$, d'où un isomorphisme $\psi : L \to L'$ qui prolonge φ_1, donc aussi φ.

Comptons maintenant le nombre de prolongements ψ qui conviennent.

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ K[\alpha] & \xrightarrow{\varphi_1} & K'[\alpha'] \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Pour définir φ_1 (prolongement de φ sur $K[\alpha]$), on a autant de choix pour α' que de racines de $\varphi(Q)$, notons ce nombre r. On a $r \leq \deg Q = [K[\alpha] : K]$, avec égalité si et seulement si Q est à racines simples (dans son corps de décomposition, donc aussi dans L). Puis par hypothèse de récurrence, on a s choix pour prolonger φ_1 en ψ (de $K[\alpha]$ à L), avec : $s \leq [L : K[\alpha]]$ et $s = [L : K[\alpha]]$ si P_1 est à racines simples dans L. Par multiplicativité des degrés, on a $rs \leq [L : K]$ choix pour ψ, avec égalité si Q et P_1 sont à racines simples dans L, ce qui est le cas si P est à racines simples dans L puisque Q et P_1 divisent P dans $L[X]$.

□

Reprenons la preuve du théorème 1.23. L'unicité découle du lemme 1.24, en prenant $K = K'$, $\varphi = \mathrm{Id}$. Pour l'existence, on procède à nouveau par récurrence sur $\deg P$. Le cas $\deg P \leq 1$ est trivial. Soit Q un facteur irréductible de P. Alors Q admet un corps de rupture $K' = K[x] = K(x)$ sur K. Dans $K'[X]$, on a alors $P = (X - x)P_1$ avec $\deg P_1 < \deg P$. On applique alors l'hypothèse de récurrence à P_1 sur K' : il existe un corps de décomposition L pour P_1 sur K'. Alors $P = (X - x)P_1$ est scindé sur L, et d'autre part $L = K'(x_2, ..., x_n)$, où $x_2, ..., x_n$ sont les racines de P_1 donc $L = K(x, x_2, ..., x_n)$ est engendré sur K par les racines de P, i.e. c'est un corps de décomposition de P sur K.

□

Remarque 1.25 L'unicité est "meilleure" que celle du corps de rupture car si deux corps de décomposition L, L' d'un polynôme $P \in K[X]$ sont des sous-corps d'une même extension M de K, alors $L = L'$ vu que ces deux corps sont égaux à $K(x_1, ...x_n)$, où $x_1, ...x_n$ sont les racines de P dans L.

Exemple 1.26 Sur $\mathbf{R}$, le corps de décomposition d'un polynôme est $\mathbf{R}$ ou $\mathbf{C}$, suivant que le polynôme a ou non toutes ses racines réelles. Sur $\mathbf{Q}$, le corps de décomposition de $X^3 - 2$ est $\mathbf{Q}(\sqrt[3]{2}, j)$ (noter qu'il est de degré 6 sur $\mathbf{Q}$).

2. Corps finis

2.1. Existence et unicité des corps finis

Les résultats ci-dessus vont nous permettre de construire les corps finis. Rappelons qu'un corps fini K est de caractéristique $p > 0$. Il peut être vu comme extension de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ via le morphisme $\mathbf{F}_p \to K$, $\bar{x} \mapsto x.1_K$. En particulier c'est un $\mathbf{F}_p$-espace vectoriel de dimension finie (disons d) donc le cardinal de K est une puissance de p puisque K est isomorphe à $(\mathbf{Z}/p\mathbf{Z})^d$ en tant que $\mathbf{F}_p$-espace vectoriel. En sens inverse, on a :

Theorème 2.1 *Soit $q = p^n$ avec $n \in \mathbf{N}^*$. Alors il existe un corps de cardinal q, unique à isomorphisme près. C'est le corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. On note ce corps $\mathbf{F}_q$.*

Démonstration : Soit K le corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. On note que l'ensemble K' des racines dans K de $X^q - X$ est déjà un corps, via le fait que $x \mapsto x^q$ est un morphisme de corps (et même un isomorphisme vu que K est fini) de K dans K : en effet c'est la n-ième itérée de $x \mapsto x^p$. Par définition du corps de décomposition, on a $K = K'$. D'autre part la dérivée de $X^q - X$ est $qX^{q-1} - 1 = -1$, donc toutes les racines sont simples et il y en a donc q. Finalement K est bien un corps de cardinal q.

Si maintenant L est un corps de cardinal q, alors tout élément x de L vérifie $x^q = x$ (c'est clair pour $x = 0$, et si $x \neq 0$ on a $x^{q-1} = 1$; d'après le théorème de Lagrange, parce que L^* est un groupe de cardinal $q - 1$). Ainsi $X^q - X$ est scindé sur L, et L contient donc un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$, i.e. un corps K_1 isomorphe à K. Par cardinalité $L = K_1$, et L est isomorphe à K.

□

Par exemple on a

$$\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2 + X + 1); \mathbf{F}_8 = \mathbf{F}_2[X]/(X^3 + X + 1); \mathbf{F}_9 = \mathbf{F}_3[X]/(X^2 + 1).$$

En effet, dans chacun de ces exemples, on quotiente $\mathbf{F}_p[X]$ (avec $p = 2$ ou $p = 3$) par l'idéal engendré par un polynôme irréductible P (car P est sans racine dans $\mathbf{F}_p$ et de degré 2 ou 3), d'où un corps de dimension $\deg P$ (donc de cardinal $p^{\deg P}$) sur $\mathbf{F}_p$.

Il n'est pour l'instant pas clair qu'on puisse ainsi faire apparaître tous les corps finis de caractéristique p comme corps de rupture sur $\mathbf{F}_p$. Pour cela, on a besoin de savoir qu'il y a des polynômes irréductibles de tout degré sur $\mathbf{F}_p$, ce qu'on va voir au prochain paragraphe.

Remarque 2.2 a) Toute anneau à division fini est un corps (théorème de Wedderburn), autrement dit il n'y a pas de "corps non commutatifs" finis (cf. TD).

b) Le corps $\mathbf{F}_{p^n}$ est une extension de $\mathbf{F}_{p^m}$ si et seulement si m divise n (et non pas p^m divise p^n). Par exemple $\mathbf{F}_8$ n'est pas une extension de $\mathbf{F}_4$. Cela résulte immédiatement de la caractérisation de $\mathbf{F}_q$ comme ensemble des racines du polynôme $X^q - X$.

2.2. Polynômes irréductibles et corps finis

Le théorème suivant donne un résultat d'existence de polynômes irréductibles sur un corps fini. Trouver explicitement des polynômes irréductibles est en revanche une question difficile.

Theorème 2.3 *Soit $K = \mathbf{F}_q$ un corps fini. Soit $d \in \mathbf{N}^*$. Notons L une extension finie de K de degré d (qui existe et est unique d'après le théorème 2.1). Alors il existe un polynôme irréductible $P \in K[X]$, de degré d, dont L est le corps de rupture.*

Démonstration : On sait (voir cours sur les groupes) que le groupe multiplicatif L^* est cyclique ; on en choisit un générateur α. Comme tout élément x de L^* s'écrit alors $x = \alpha^n$ avec $n \in \mathbf{Z}$, on a a fortiori $L = K[\alpha]$ et il suffit alors de prendre pour P le polynôme minimal de α sur K.

□

Remarque 2.4 Il est possible (voir exercice en TD) de compter précisément le nombre de polynômes irréductibles de degré d dans un corps fini.

Proposition 2.5 *Soit K un corps fini. Soit P un polynôme irréductible de $K[X]$. Alors, le corps de rupture de P coïncide avec son corps de décomposition.*

Démonstration : Notons q le cardinal de K et d le degré de P. Le corps de rupture L de P s'écrit $L = K[\alpha]$, et c'est le corps fini $\mathbf{F}_{q^d}$. Comme on l'a déjà vu, l'application $F : x \mapsto x^q$ est un automorphisme de corps de L, et F induit l'identité sur $K = \mathbf{F}_q$; ainsi F envoie toute racine de P sur une racine de P. Notons F^m la m-ième itérée de F ; on observe que d est le plus petit entier $m > 0$ tel que $F^m(\alpha) = \alpha$: en effet si on avait un tel $m < d$, alors α serait dans le corps $\mathbf{F}_{q^m}$ (qui est le corps de décomposition sur $\mathbf{F}_p$ de $X^{q^m} - X$ d'après le théorème 2.1), donc on aurait $[K[\alpha] : K] \leq m$, ce qui est exclu vu que $[K[\alpha] : K] = \deg P = d$. On voit alors que P admet d racines

distinctes $\alpha, F(\alpha), ..., F^{d-1}(\alpha)$ dans L puisque si on avait $F^i(\alpha) = F^j(\alpha)$ pour $0 \leq i < j < d$, on aurait $F^i(\alpha) = F^i(F^{j-i}(\alpha))$ d'où $F^{j-i}(\alpha) = \alpha$, vu que F^i est un automorphisme. Finalement, L est bien un corps de décomposition de P sur K.

□

3. Compléments sur l'irréductibilité

Avant d'aborder la théorie de Galois en général, il est utile de voir quelques exemples de polynômes irréductibles, qui peuvent ensuite servir à construire des corps de rupture.

3.1. Irréductibilité sur Q et sur $\mathbf{Z}/p\mathbf{Z}$

Pour étudier l'irréductibilité d'un polynôme de $\mathbf{Q}[X]$, on peut toujours se ramener (en multipliant par un entier) à un polynôme primitif de $\mathbf{Z}[X]$. Le critère le plus efficace sera alors en général celui d'Eisenstein. Voici une autre façon d'utiliser la réduction modulo p :

Proposition 3.1 *Soit $P = a_nX^n + ... + a_0$ un polynôme de $\mathbf{Z}[X]$. Soit p un nombre premier. On suppose que p ne divise pas a_n. Alors, si la réduction $\overline{P}$ de P dans $\mathbf{Z}/p\mathbf{Z}[X]$ est irréductible, P est irréductible sur $\mathbf{Q}$.*

Remarque : On fera attention aux hypothèses ($2X^2 + X$ est irréductible modulo 2, mais il n'est pas irréductible dans $\mathbf{Q}[X]$) et à la conclusion (P n'est pas forcément irréductible sur $\mathbf{Z}$, par exemple $3X$ est irréductible modulo 2). Ce critère paraît séduisant, mais d'abord il ne donne qu'une condition suffisante (par exemple le polynôme $X^2 - 3$ est irréductible sur $\mathbf{Q}$ mais il devient réductible modulo 3 ; cf aussi remarque 3.6), ensuite il n'est en général pas facile de déterminer si un polynôme de $\mathbf{Z}/p\mathbf{Z}[X]$ est irréductible si le degré est grand ! Bien entendu la proposition se généralise immédiatement à un anneau factoriel et à un idéal premier.

Démonstration : On a déjà $\deg P \geq 1$ sinon $\overline{P}$ ne serait pas irréductible sur $\mathbf{Z}/p\mathbf{Z}$. Si P était réductible sur $\mathbf{Q}$, le polynôme primitif $P/c(P)$ le serait donc aussi sur $\mathbf{Z}$ (d'après ce qu'on a vu dans le chapitre sur les anneaux factoriels) et on pourrait écrire $P = QR$ dans $\mathbf{Z}[X]$ avec Q et R de degré au moins 1. Mais comme p ne divise pas a_n, $\overline{P}$ a même degré que P, donc $\overline{Q}$ et $\overline{R}$ sont non constants, ce qui contredit l'irréductibilité de $\overline{P}$.

□

Rappelons que pour tout corps K, un polynôme de $K[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine dans K. Voici un autre critère, souvent utile pour les corps finis :

Proposition 3.2 *Soit $P \in K[X]$ de degré n. On suppose que pour toute extension L de K de degré au plus $n/2$, le polynôme P n'a pas de racines dans L. Alors P est irréductible dans $K[X]$.*

Noter que réciproquement, un polyn ôme irréductible de $K[X]$ de degré d ne peut avoir de racine dans une extension de K de degré $< d$, vu que son corps de rupture est de degré d sur K.

Démonstration : Si P est réductible, on peut écrire $P = \prod_{i=1}^{r} P_i$ avec les P_i irréductibles et $r \geq 2$. L'un des P_i (notons le π) est donc de degré d au plus $n/2$. Comme π a une racine dans une extension de degré d de K (un corps de rupture), la proposition en résulte.

□

Par exemple $X^4 + X + 1$ est irréductible sur $\mathbf{F}_2$. En effet il n'a clairement pas de racines dans $\mathbf{F}_2$, ni dans son extension $\mathbf{F}_4$ de degré 2, puisque tout élément x de $\mathbf{F}_4$ vérifie $x^4 = x$, d'où $x^4 + x + 1 = 2x + 1 = 1$.

3.2. Polynômes cyclotomiques

Soit $\mu_n \subset \mathbf{C}^*$ le groupe multiplicatif des racines de l'unité. On note μ_n^* l'ensemble des racines *primitives* n-ièmes de l'unité, c'est l'ensemble des générateurs de $(\mu_n, \times)$. Le cardinal de μ_n^* est $\varphi(n)$, cet ensemble consiste en les $e^{2ik\pi/n}$ avec k entier premier à n.

Pour tout entier $n > 0$, on définit le *n-ième polynôme cyclotomique* Φ_n de $\mathbf{C}[X]$ par

$$\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

Par exemple si p est premier, on a

$$\Phi_p = \frac{X^p - 1}{X - 1} = 1 + X + ... + X^{p-1}.$$

Rappelons que si F, G sont deux polynômes de $\mathbf{Z}[X]$ avec G *unitaire*, on a une division euclidienne de F par G dans $\mathbf{Z}[X]$, c'est-à-dire qu'il existe un unique couple H, R de polynômes de $\mathbf{Z}[X]$ vérifiant $F = GH + R$ avec

$\deg R < \deg G$ (cela se montre aisément par récurrence sur $\deg F$, et s'étend à tout anneau commutatif A dès lors que le coefficient dominant de G est inversible dans A). Par unicité, cette division euclidienne est aussi celle de F par G dans $\mathbf{Q}[X]$, ou encore dans $\mathbf{C}[X]$.

Proposition 3.3 *On a $X^n - 1 = \prod_{d|n} \Phi_d$. Pour tout $n \in \mathbf{N}^*$, le polynôme Φ_n est dans $\mathbf{Z}[X]$.*

Démonstration : La première assertion vient de ce que $X^n - 1$ et $\prod_{d|n} \Phi_d$ sont deux polynômes unitaires, scindés et à racines simples dans $\mathbf{C}[X]$, qui ont les mêmes racines (en effet μ_n est la réunion des μ_d^* pour d divisant n, comme on le voit en triant les éléments de μ_n suivant leur ordre). La deuxième assertion se montre par récurrence sur n : pour $n = 1$, on a $\Phi_1 = X - 1$, et si tous les Φ_d sont dans $\mathbf{Z}[X]$ pour $d < n$, la formule précédente donne $X^n - 1 = R.\Phi_n$ (dans $\mathbf{C}[X]$), avec R dans $\mathbf{Z}[X]$ et unitaire ; ainsi Φ_n est aussi dans $\mathbf{Z}[X]$ en considérant la division euclidienne de $X^n - 1$ par le polynôme unitaire R de $\mathbf{Z}[X]$.

□

Le théorème principal sur les polynômes cyclotomiques est le suivant :

Theorème 3.4 *Le polynôme Φ_n est irréductible sur $\mathbf{Q}$.*

Ainsi si ζ est dans μ_n^*, le polynôme minimal de ζ dans $\mathbf{Q}[X]$ est Φ_n et le degré $[\mathbf{Q}(\zeta) : \mathbf{Q}]$ est $\varphi(n)$. Noter que $\mathbf{Q}(\zeta)$ est aussi le corps de décomposition de Φ_n. Le cas où n est premier est plus facile, il a été vu dans le cours sur les anneaux comme application du critère d'Eisenstein.

Pour démontrer le théorème, le lemme-clef est le suivant :

Lemme 3.5 *Soit $\zeta \in \mu_n^*$. On fixe un nombre premier p ne divisant pas n, puis on appelle f, g les polynômes minimaux respectifs de ζ, ζ^p sur $\mathbf{Q}$. Alors*

1. *f et g sont dans $\mathbf{Z}[X]$.*
2. *$f = g$.*

Démonstration : 1. Il suffit de montrer le résultat pour f car comme p est premier à n, g est encore le polynôme minimal d'une racine primitive n-ième de l'unité. Comme $X^n - 1$ annule ζ, f divise $X^n - 1$. Comme $\mathbf{Z}[X]$ est factoriel, on peut décomposer $X^n - 1$ en un produit de facteurs irréductibles $P_1 ... P_r$ dans $\mathbf{Z}[X]$, et on peut choisir les P_i unitaires quitte à en multiplier certains par -1, vu que $X^n - 1$ est unitaire. alors $P_1 ... P_r$ est aussi la décomposition

en produit de facteurs irréductibles dans $\mathbf{Q}[X]$, donc f (qui est irréductible et divise $X^n - 1$) est l'un des P_i et $f \in \mathbf{Z}[X]$. [3]

2. Supposons le contraire. Alors f et g sont premiers entre eux et divisent Φ_n, donc fg divise Φ_n (dans $\mathbf{Q}[X]$, donc aussi dans $\mathbf{Z}[X]$ puisque tous ces polynômes sont unitaires). On observe que le polynôme $h = g(X^p)$ annule ζ. Par conséquent il est divisible par f (dans $\mathbf{Q}[X]$, ou dans $\mathbf{Z}[X]$, toujours parce que f est unitaire). Ainsi la réduction $\bar{h}$ de h modulo p est divisible par $\bar{f}$ dans $\mathbf{Z}/p\mathbf{Z}[X]$. Mais comme tout élément $\bar{a}$ de $\mathbf{Z}/p\mathbf{Z}$ vérifie $\bar{a}^p = \bar{a}$, on obtient $\bar{h} = \bar{g}^p$. Ainsi $\bar{f}$ divise $\bar{g}^p$ puisque f divise h. Le polynôme unitaire $\bar{f}$ n'est pas forcément irréductible dans $\mathbf{Z}/p\mathbf{Z}[X]$, mais il admet un facteur irréductible $\varphi \in \mathbf{Z}/p\mathbf{Z}[X]$. On a alors $\varphi \mid \bar{g}$. Comme d'autre part $\bar{f}\bar{g}$ divise $\bar{\Phi}_n$, on obtient a fortiori que φ^2 divise le polynôme $Q = X^n - \bar{1}$ dans $\mathbf{Z}/p\mathbf{Z}[X]$. Mais ceci n'est pas possible car Q est premier avec son polynôme dérivé Q', via l'identité de Bezout dans $\mathbf{Z}/p\mathbf{Z}[X]$:

$$(X/\bar{n})Q' - Q = \bar{1}$$

qui a un sens parce que p ne divise pas n, donc $\bar{n}$ est inversible dans $\mathbf{Z}/p\mathbf{Z}$.

□

Preuve du théorème : Fixons une racine primitive n-ième ζ de l'unité, et appelons f son polynôme minimal sur $\mathbf{Q}$. Si ζ' est un autre élément de μ_n^*, on peut écrire $\zeta' = \zeta^m$ avec m premier à n ; ainsi $m = \prod_{i=1}^r p_i$ où les nombres premiers p_i (qui ne sont pas forcément deux à deux distincts) ne divisent pas n. D'après la proposition précédente, on voit par récurrence sur r que le polynôme minimal de ζ' sur $\mathbf{Q}$ est encore f. Finalement f est divisible dans $\mathbf{C}[X]$ par tous les $(X - \zeta')$ avec $\zeta' \in \mu_n^*$, donc f est divisible par Φ_n (dans $\mathbf{C}[X]$, donc aussi dans $\mathbf{Q}[X]$ par unicité de la division euclidienne). Comme $\Phi_n(\zeta) = 0$, Φ_n est multiple de f et finalement $\Phi_n = f$ donc Φ_n est irréductible sur $\mathbf{Q}$ en tant que polynôme minimal de ζ.

□

Remarque 3.6 Le polynôme $\Phi_8 = X^4 + 1$ a une réduction modulo p qui n'est pas irréductible, et ce pour tout nombre premier p. C'est évident si $p = 2$ car dans $\mathbf{Z}/2\mathbf{Z}$ on a $X^4 + 1 = (X + 1)^4$. Si maintenant p est premier impair, alors le groupe multiplicatif du corps fini $\mathbf{F}_{p^2}$ est cyclique d'ordre $p^2 - 1$, donc comme $p^2 - 1$ est divisible par 8, il possède un élément α d'ordre 8. Alors α est une racine de $X^4 + 1$ dans $\mathbf{F}_{p^2}$ puisque $\alpha^8 = 1$ et $\alpha^4 \neq 1$. Ceci

3. Le même argument donne que pour tout anneau factoriel A, le polynôme minimal sur $K := \mathrm{Frac}\, A$ d'un élément x qui annule un polynôme *unitaire* à coefficients dans A est encore dans $A[X]$.

exclut que X^4+1 soit irréductible sur $\mathbf{F}_p$, sinon son corps de rupture $\mathbf{F}_p(\alpha)$ serait de degré 4 sur $\mathbf{F}_p$ alors que $\mathbf{F}_p(\alpha) \subset \mathbf{F}_{p^2}$.

4. Théorie de Galois

L'idée fondamentale introduite par Galois consiste à relier les extensions finies de corps L/K aux groupes $\mathtt{Aut}(L/K)$ des K-automorphismes de L qui leur sont associés. On doit d'abord introduire quelques notions supplémentaires, qui font l'objet des deux paragraphes suivants.

4.1. Extensions normales

Définition 4.1 Une extension de corps L/K est dite *normale* si tout polynôme irréductible de $K[X]$ qui possède une racine dans L est scindé sur L.

Exemple 4.2 a) Une extension L/K est automatiquement normale si elle est de degré 2 car si $x \in L$ est racine d'un polynôme irréductible unitaire $P \in K[X]$, le degré de P est 1 ou 2 (car c'est la dimension du K-ev $K[x] \subset L$) ; or, si $P = X^2 + aX + b$, l'autre racine de P est $-x - a$, qui est encore dans L.

b) L'extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ n'est pas normale vu que le polynôme $X^3 - 2$ n'est pas scindé sur $\mathbf{Q}(\sqrt[3]{2})$.

c) Pour la même raison, l'extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$, corps de rupture du polynôme irréductible $X^4 - 2$ sur $\mathbf{Q}$, n'est pas normale.

d) La proposition 2.5 montre que toute extension de corps finis est normale.

Les extensions normales finies sont décrites par le théorème suivant :

Theorème 4.3 *Soit K un corps. Soit L une extension finie de K. Alors L est normale*[4] *si et seulement s'il existe un polynôme P dont elle est le corps de décomposition.*

Démonstration : Supposons d'abord que L soit normale et finie sur K. Soit $(a_1, ..., a_n)$ une base de L en tant que K-espace vectoriel, en particulier chaque a_i est algébrique sur K et on peut considérer son polynôme minimal M_i, qui est irréductible. Posons $P = M_1 ... M_n$, alors chaque M_i possède le

4. On dit parfois *quasi-galoisienne* au lieu de normale.

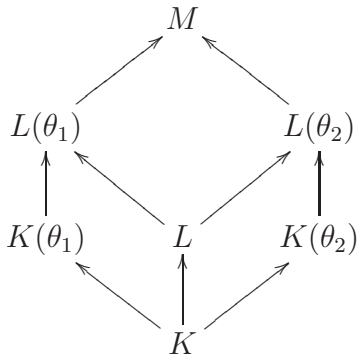
zéro a_i sur L, donc est scindé sur L puisque par hypothèse L est normale. Ainsi, P est scindé sur L, et son corps de décomposition est clairement alors L puisque le corps L est engendré par K et les zéros de P (tout élément de L est même combinaison linéaire à coefficients dans K des a_i).

En sens inverse, soit L le corps de décomposition sur K d'un polynôme G (ainsi L est une extension finie de K). Soit $F \in K[X]$ irréductible possédant un zéro dans L, il s'agit de montrer que F est scindé sur L. Soit $M \supset L$ le corps de décomposition de FG sur K, considérons deux racines θ_1 et θ_2 de F dans M. Il suffit de montrer le

Lemme 4.4 *On a* $[L(\theta_1) : L] = [L(\theta_2) : L]$.

En effet, en appliquant ceci à un zéro θ_1 de F dans L et à un zéro quelconque θ_2 de F dans M, on obtient $[L(\theta_2) : L] = 1$, i.e. $\theta_2 \in L$ comme on voulait.

Il reste à prouver le lemme. On a le diagramme de corps suivant :



On note que $K(\theta_1)$ et $K(\theta_2)$ sont des corps de rupture de F sur K, ils sont donc K-isomorphes par le théorème 1.18. Par ailleurs, pour $j = 1, 2$, le corps $L(\theta_j)$ est (par définition de L) un corps de décomposition de G sur $K(\theta_j)$, ce qui implique par le lemme 1.24 (en prolongeant un K-isomorphisme $\varphi : K(\theta_1) \to K(\theta_2)$ en un isomorphisme de $L(\theta_1)$ sur $L(\theta_2)$, vu qu'ici $\varphi(G) = G$) que

$$[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)].$$

Le lemme 4.4 en découle via la formule

$$[L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)].[K(\theta_j) : K] = [L(\theta_j) : L].[L : K],$$

qui est valable pour $j = 1, 2$.

□

On a aussi la propriété de "stabilité" suivante des extensions normales :

Proposition 4.5 *Soient $K \subset F \subset L$ des extensions de corps.*

a) On suppose que F/K est finie et normale. Alors tout K-morphisme de corps $f : F \to L$ vérifie $f(F) = F$, autrement dit f induit un K-automorphisme du corps F.

b) On suppose que L/K est finie et normale. Alors tout K-morphisme u de F dans L se prolonge en un K-automorphisme de L. De plus L/F est normale.

Démonstration : a) Soit $x \in F$, alors le polynôme minimal P de x sur K est irréductible dans $K[X]$. Comme f est un K-morphisme de corps de F dans L, il envoie x sur une racine de P : en effet si $P = X^n + a_{n-1}X^{n-1} + ... + a_0$, alors

$$0 = f(x^n + a_{n-1}x^{n-1} + ... + a_0) = f(x)^n + a_{n-1}f(x)^{n-1} + ... + a_0$$

puisque f est un K-morphisme. Ainsi $f(x) \in F$ puisque F/K est normale. On a donc $f(F) \subset F$, et on conclut en observant que f est alors un endomorphisme injectif du K-ev de dimension finie F.

b) D'après le théorème 4.3, il existe un polynôme $G \in K[X]$ dont L est le corps de décomposition sur K. Alors, L est aussi le corps de décomposition de G sur F (ou sur $u(F)$) et il suffit d'appliquer le lemme 1.24 en prenant pour φ l'isomorphisme $u : F \to u(F)$, et $L' = L$. Le fait que L/F soit normale résulte immédiatement du théorème 4.3.

□

Définition 4.6 Soient L/K une extension algébrique et $x \in L$ de polynôme minimal P sur K. On suppose P scindé sur L. Les *conjugués* de x dans L (sur K) sont les racines de P dans L.

Il s'agit donc de la généralisation de la notion de deux nombres complexes conjugués (qui correspond à être conjugué sur $\mathbf{R}$).

Proposition 4.7 *Soit L/K une extension finie et normale. Soient $\alpha, \beta \in L$, qu'on suppose conjugués sur K, alors il existe $\sigma \in \mathtt{Aut}(L/K)$ qui envoie α sur β. Si F est une extension intermédiaire entre L et K, elle est normale sur K si et seulement si elle vérifie $\sigma(F) \subset F$ pour tout K-automorphisme σ de L.*

Rappelons que la notation $\mathtt{Aut}(L/K)$ désigne le groupe (pour la loi $\circ$) des K-automorphismes de L.

Démonstration : On observe que comme α et β ont même polynôme minimal sur K, les corps $K[\alpha]$ et $K[\beta]$ sont des corps de rupture de ce polynôme. Par le théorème 1.18 et la remarque 1.20, il existe un K-isomorphisme de $K[\alpha]$ sur $K[\beta]$ envoyant α sur β. Il se prolonge en un élément de $\mathtt{Aut}(L/K)$ d'après la proposition 4.5 b).

Considérons maintenant une extension intermédiaire F. On a déjà vu (proposition 4.5, a) que si F est normale, alors $\sigma(F) \subset F$ pour tout K-automorphisme σ de L. Supposons réciproquement cette dernière propriété satisfaite. Soit $P \in K[X]$ irréductible et possédant une racine $\alpha \in F$; si $\beta \in L$ est une autre racine de P, c'est un conjugué de α sur K, et on vient de voir qu'il existe alors $\sigma \in G$ tel que $\sigma(\alpha) = \beta$. Comme $\sigma(F) \subset F$, on obtient $\beta \in F$, ce qui montre que F/K est normale.

□

Remarque 4.8 a) On notera bien que cette notion est relative au corps K. Par exemple, si on prend $K = \mathbf{R}$ comme corps de base, le seul conjugué dans $\mathbf{C}$ de $z := (\sqrt[3]{2})$ est lui-même, mais si on prend $K = \mathbf{Q}$, alors z admet les deux autres conjugués $j(\sqrt[3]{2})$ et $j^2(\sqrt[3]{2})$, où $j = \frac{-1+i\sqrt{3}}{2}$.

b) Avec les notations ci-dessus, si u est un K-morphisme de L dans L, alors $u(x)$ est un conjugué de x (appliquer u à l'équation $P(x) = 0$). Noter aussi que si $Q \in K[X]$ vérifie $Q(x) = 0$, il est multiple du polynôme minimal de x et vérifie donc $Q(y) = 0$ pour tout K-conjugué y de x.

Exemple 4.9 Attention, si L/K est une extension normale finie et F/K est une extension intermédiaire, on a vu que que L/F reste normale mais *ce n'est pas forcément le cas de* F/K : par exemple $\mathbf{Q}(j, \sqrt[3]{2})/\mathbf{Q}$ est normale (en tant que corps de décomposition de $X^3 - 2$ sur $\mathbf{Q}$), mais pas $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$. Noter aussi que F/K et L/F peuvent être normales sans que L/K le soit, ex. $K = \mathbf{Q}$, $F = \mathbf{Q}(\sqrt{2})$, $L = \mathbf{Q}(\sqrt[4]{2})$.

4.2. Extensions séparables

La question se pose maintenant de savoir si un polynôme irréductible de $K[X]$ peut acquérir des racines multiples dans un corps de décomposition. Cela motive la définition suivante :

Définition 4.10 Un polynôme irréductible de $K[X]$ est dit *séparable* sur K si toutes ses racines dans un corps de décomposition sont simples. Un élément algébrique sur K d'une extension L/K est *séparable* si son polynôme minimal est séparable. Une *extension algébrique séparable* est une extension dont tous les éléments sont séparables.

Autrement dit, un élément x algébrique sur K est séparable si l'ensemble de ses conjugués (dans un corps de décomposition de son polynôme minimal) est de cardinal $[K[x] : K]$.

On peut étendre la définition d'un polynôme séparable à tout polynôme de $K[X]$ en demandant encore que toutes ses racines (dans un corps de décomposition) soient simples [5], ce qui équivaut à P premier avec sa dérivée P'.

Exemple 4.11 Soit K un corps de caractéristique $p > 0$ contenant un élément $a \in K^*$ qui n'est pas une puissance p-ième dans K (exemple : $K = \mathbf{Z}/p\mathbf{Z}(T)$ avec $a = T$). Alors, le polynôme $X^p - a$ est irréductible dans $K[X]$: en effet sinon on pourrait écrire soit $X^p - a = Q^\alpha$ avec Q irréductible unitaire et $\alpha \geq 2$, soit $X^p - a = RS$, avec R et S premiers entre eux de degré au moins 1. Dans le premier cas, comme $X^p - a$ est de dérivée nulle, on aurait $\alpha Q^{\alpha-1}Q' = 0$; ceci impose soit $Q' = 0$ (auquel cas Q n'a que des termes dont le degré est un multiple de p et est non constant, d'où $\deg Q \geq p$ et $\deg(Q^\alpha) \geq 2p$, ce qui est impossible), soit α est multiple de p, ce qui impose $\alpha = p$ et $\deg Q = 1$ (toujours pour des raisons de degré), mais alors a est puissance p-ième du terme constant de Q qui est dans K, ce que l'on a exclu. Si enfin on est dans le deuxième cas où $X^p - a = RS$, avec R et S premiers entre eux de degré au moins 1, alors $RS' + R'S = 0$, donc S divise S' (puisqu'il est premier avec R), ce qui impose $S' = 0$, puis S de degré au moins p, ce qui est impossible vu qu'alors RS est de degré $> p$.

D'autre part $X^p - a$ n'est pas séparable car sa dérivée est nulle. Son corps de rupture est donc une extension inséparable de K.

Remarque 4.12 Si L/K est une extension algébrique séparable, et F/K est une extension intermédiaire, alors les extensions F/K et L/F sont encore séparables. C'est évident pour F/K (le polynôme minimal sur K d'un élément x de F est par définition le même que si on regarde x comme un élément de L). Pour L/F, on observe que si $\alpha \in L$, alors son polynôme minimal sur F divise son polynôme minimal sur K, donc est séparable dès que ce dernier est séparable.

Les problèmes d'inséparabilité ne se produisent pas en caractéristique zéro, ni sur un corps fini, comme le montre le théorème suivant.

Theorème 4.13 *Soit P un polynôme irréductible de $K[X]$. Alors P est séparable dans les deux cas suivants :*

5. Attention, certains auteurs demandent juste que tous les facteurs irréductibles soient séparables, ce qui n'exclut pas une puissance d'un polynôme irréductible séparable.

a) Le corps K est de caractéristique zéro.

b) Le corps K est de caractéristique p et parfait, i.e. le morphisme de corps $x \mapsto x^p$ est bijectif de K dans K (ex. K est fini).

En particulier, toute extension algébrique d'un corps de caractéristique zéro, ou d'un corps parfait de caractéristique $p > 0$, est séparable.

Démonstration : Comme P est irréductible, le pgcd de P et P' dans $K[X]$ est 1 dès que P ne divise pas P', donc (pour raison de degré) dès que P' est non nul. Dans le cas a), c'est toujours le cas et comme le pgcd ne dépend pas du corps de base (via par exemple l'algorithme d'Euclide), les polynômes P et P' n'ont pas de racine commune dans un corps de décomposition de P, ce qui prouve que P est séparable.

Si K est de caractéristique p, un polynôme irréductible P inséparable de $K[X]$ doit vérifier $P' = 0$, donc être de la forme

$$P = a_0 + a_1 X^p + ... + a_n X^{pn},$$

avec $n \geq 1$ et $a_n \neq 0$. Si K est parfait, on peut pour chaque $i = 0, ..., n$ écrire $a_i = b_i^p$ avec $b_i \in K$, d'où

$$P = (b_0 + b_1 X + ... + b_n X^n)^p,$$

ce qui contredit l'hypothèse que P est irréductible.

□

Remarque 4.14 Le théorème précédent et l'exemple 4.11 montrent qu'un corps K de caractéristique $p > 0$ est parfait si et seulement si toute extension finie (ou encore toute extension algébrique) de K est séparable. On en déduit que toute extension finie (et même en corollaire toute extension algébrique) d'un corps parfait reste parfait via la remarque 4.12. On peut retrouver ce résultat de façon plus élémentaire (voir TD).

Terminons ce paragraphe par le classique *théorème de l'élément primitif* :

Theorème 4.15 *Soit L/K une extension finie séparable. Alors il existe $z \in L$ tel que $L = K[z]$.*

Autrement dit, toute extension finie séparable est un corps de rupture.

Démonstration : D'après la proposition 2.3, on peut supposer que le corps K est infini. Comme L s'écrit $L = K[a_1, ..., a_r]$ (puisque L est de dimension finie sur K, donc a fortiori de type fini comme K-algèbre), on peut (en raisonnant par récurrence sur r via la remarque 4.12) supposer que $L = K[x, y]$ avec $x, y \in L$. Notons alors P et Q les polynômes minimaux de x, y sur K, et M un corps de décomposition de PQ sur K. L'idée va maintenant être de fabriquer un élément $z \in L$ qui *possède beaucoup de conjugués* dans M, afin que son polynôme minimal sur K soit de degré le plus grand possible (en l'occurrence $[L : K]$).

On pose

$$P = (X - x)\prod_{i=2}^{n}(X - x_i)$$

$$Q = (X - y)\prod_{j=2}^{m}(X - y_j)$$

avec les x_i et les y_j dans M. Comme P et Q sont par hypothèse des polynômes séparables, on a pour tous indices $i, j : x \neq x_i$ et $y \neq y_j$. On peut alors trouver $t \in K^*$ tel que pour tous indices i, j, on ait

$$x + ty \neq x_i + ty_j.$$

En effet, il s'agit juste de choisir un t non nul qui n'est pas parmi tous les $\frac{x-x_i}{y_j-y}$, ce qui est possible puisque K est infini.

Posons alors $z = x + ty$ et $K' = K[z]$, puis $F(X) = P(z - tX)$. Le polynôme F est dans $K'[X]$. Calculons le pgcd de F et Q dans M (corps sur lequel Q est scindé à racines simples) : par construction $F(y) = Q(y) = 0$, mais les autres racines y_j de Q n'annulent pas F puisque $z - ty_j$ n'est jamais l'un des x_i, ni x (si $z-ty_j = x$, alors y serait l'un des y_j car $t \neq 0$). Finalement, le pgcd cherché est $(X - y)$, et comme il doit être dans $K'[X]$, on en déduit que $y \in K'$, puis $x = z - ty \in K'$. Ceci implique que $L = K[z]$ comme on voulait.

□

On verra en TD que ce résultat peut tomber en défaut pour une extension inséparable.

4.3. La correspondance de Galois

Définition 4.16 Pour tout corps L, on note $\mathtt{Aut}(L)$ le groupe (pour la loi $\circ$) des automorphismes du corps L. Si L/K est une extension de corps, on

note $\mathtt{Aut}(L/K) \subset \mathtt{Aut}(L)$ le sous-groupe des K-automorphismes de L. Pour tout sous-groupe H de $\mathtt{Aut}(L)$, on pose

$$L^H := \{x \in L, \forall \sigma \in H, \sigma.x = x\}.$$

Il est clair que L^H est un sous-corps de L, qu'on appelle le *corps fixe* de H. Si L/K est une extension et H est un sous-groupe de $\mathtt{Aut}(L/K)$, alors L^H est une extension intermédiaire entre L et K. Réciproquement, si $K \subset F \subset L$ sont des extensions de corps, alors $\mathtt{Aut}(L/F)$ est un sous-groupe de $\mathtt{Aut}(L/K)$. Attention, ce n'est pas le cas en général de $\mathtt{Aut}(F/K)$, qui sous certaines conditions s'identifiera à un *quotient* de de $\mathtt{Aut}(L/K)$. Le groupe $\mathtt{Aut}(L/K)$ opère naturellement sur L, et aussi sur $L[X]$ par automorphismes de K-algèbres.

On passe au premier théorème important de ce paragraphe, qui est l'étape cruciale vers la correspondance de Galois.

Theorème 4.17 *Soit L/K une extension finie de corps. Notons G le groupe $\mathtt{Aut}(L/K)$. Alors $\#G \leq [L : K]$. De plus, on a équivalence entre :*

a) $\#G = [L : K]$.

b) Il existe un polynôme irréductible séparable de degré $[L : K]$ de $K[X]$ dont L est le corps de décomposition sur K.

c) $K = L^G$.

Ces propriétés sont aussi équivalentes à b') : même énoncé que b), en supposant seulement que P est séparable (pas forcément irréductible ni de degré $[L : K]$).

Démonstration : Montrons d'abord qu'on a $\#G \leq [L : K]$. L'idée est similaire à celle de la preuve du théorème de l'élément primitif : construire un $a \in L$ qui possède un maximum de conjugués dans L, et utiliser alors que ce nombre de conjugués est majoré par $[L : K]$, car majoré par le degré $[K[a] : K]$ de a sur K. Plus précisément, on commence par démontrer :

Lemme 4.18 *Soit T une partie finie de G. Il existe $a \in L$ tel que les $\sigma(a), \sigma \in T$ soient deux à deux distincts.*

Preuve du lemme : Posons $T = \{\sigma_1, ..., \sigma_m\}$. Considérons, pour tous i, j distincts de $\{1, ..., m\}$:

$$F_{ij} = \{x \in L, \sigma_i(x) = \sigma_j(x)\}.$$

chaque F_{ij} est un sous-corps de L distinct de L. Ceci implique que la réunion des F_{ij} n'est pas L tout entier : en effet si K est fini, alors L l'est aussi donc

L^* est cyclique et il suffit de prendre un générateur de L^*, qui ne peut pas être dans un des F_{ij} (sinon $F_{ij} = L$) ; si K est infini, c'est un fait bien connu qu'un K-ev de dimension finie n'est pas réunion d'un nombre fini de sous-espaces stricts. Choisissons alors $a \in L$ qui n'est dans aucun des F_{ij}, alors les $\sigma_i(a)$ pour $i = 1, ..., m$ sont deux à deux distincts.

□

Nous reprenons la preuve du théorème 4.17, en montrant d'abord que $\#G \leq [L : K]$. Si G contient une partie finie T de cardinal m, le lemme permet de fabriquer m éléments deux à deux distincts (les $\sigma(a), \sigma \in T$) qui sont racines du polynôme minimal P de a, qui est alors de degré au moins m. Ainsi, $[K[a] : K] \geq m$ et a fortiori $[L : K] \geq m$, ce qui signifie finalement que T (et donc aussi G) est de cardinal au plus $[L : K]$.

Supposons maintenant a) ; on peut prendre $m = n := [L : K]$ dans la construction ci-dessus. Le polynôme P est alors de degré exactement n et possède n racines distinctes dans L, avec de plus $L = K[a]$ puisque $K[a]$ est de dimension $n = [L : K]$ sur K ; on a donc b).

Supposons maintenant b') (qu' implique évidemment b), c'est-à-dire que L est le corps de décomposition d'un polynôme séparable P. Alors on a bien a) d'après la fin du lemme 1.24 appliqué à $K = K'$, $L = L'$ et $\varphi = \mathrm{Id}_K$.

a) implique c) : posons $K' = L^G$, alors K' est une extension de K telle que $G = \mathtt{Aut}(L/K')$. On a vu qu'alors $\#G \leq [L : K']$ mais a) dit que $\#G = [L : K]$ d'où finalement $[L : K'] = [L : K]$, donc $[K' : K] = 1$ par multiplicativité des degrés et $K = K'$ comme on voulait.

Supposons enfin c) et montrons b'), ce qui d'après ce qui précède terminera la démonstration. Soit S une partie finie de L qui l'engendre en tant que K-ev. Quitte à remplacer S par $\{\sigma(s), s \in S, \sigma \in G\}$ (qui reste fini car G est fini vu que son cardinal est majoré par $n = [L : K]$), on peut supposer que S est stable sous l'action de G. Posons alors

$$P = \prod_{s \in S} (X - s),$$

c'est un polynôme scindé à racines simples à coefficient dans L. Pour tout $\sigma \in G$, la restriction de σ à S est injective, donc bijective de S dans S, ce qui implique que

$$\sigma(P) = \prod_{s \in S} (X - \sigma(s)) = P.$$

Tous les coefficients de P sont donc dans L^G, ce qui avec l'hypothèse c) signifie que $P \in K[X]$. On obtient alors b') en remarquant que L est le corps

de décomposition de P sur K, avec P séparable, puisque L est engendré par S comme K-espace vectoriel, donc a fortiori comme K-algèbre.

□

Remarque 4.19 Si K est de caractéristique zéro, on peut montrer directement que c) implique b), en écrivant $L = K[s]$ via le théorème de l'élément primitif, puis en considérant le polynôme $P = \prod_{\sigma \in G}(X - \sigma(s))$, qui est dans $K[X]$ (même argument que dans la preuve plus haut). En effet, comme les $\sigma(s)$ sont les conjugués de s (deux à deux distincts vu que l'extension est séparable), le polynôme P est le polynôme minimal de s et il est donc irréductible sur K. En caractéristique $p > 0$, la difficulté est qu'on ne sait pas encore que l'hypothèse c) implique que L/K est séparable, ce que nous allons montrer un peu plus bas.

Définition 4.20 Une extension finie L/K est dite *galoisienne* si elle vérifie les conditions équivalentes du théorème 4.17. On note alors $\mathrm{Gal}\,(L/K)$ pour $\mathtt{Aut}(L/K)$, qu'on appelle le *groupe de Galois*[6] de l'extension L/K. Il est donc de cardinal $[L : K]$.

Le lemme suivant sera utile pour étudier les propriétés des extensions galoisiennes :

Lemme 4.21 *Soit L/K une extension finie galoisienne. Soit $F \subset L$ une extension intermédiaire. Soit A l'ensemble des K-morphismes de F dans L. Alors, l'application $u : \mathrm{Gal}\,(L/K) \to A$ qui envoie tout K-automorphisme de L sur sa restriction à F est surjective, et pour tout $\tau \in A$, l'image réciproque A_τ de τ par u est de cardinal $\#\mathtt{Aut}(L/F)$.*

Démonstration : La surjectivité de u vient de ce que L/K est normale (via la définition d'une extension galoisienne et le théorème 4.3) et de la proposition 4.5, b). On observe alors que deux éléments σ, ρ de $\mathrm{Gal}\,(L/K)$ ont même image par u si et seulement si $\sigma(x) = \rho(x)$ pour tout $x \in F$, ce qui est équivalent à $(\sigma^{-1} \circ \rho)(x) = x$; ainsi, A_τ est une classe à gauche de $\mathrm{Gal}\,(L/K)$ selon $\mathtt{Aut}(L/F)$, d'où le résultat.

□

Rappelons qu'en général F/K n'est pas normale (par contre l'énoncé suivant donnera que L/F reste galoisienne). Ceci est lié au fait que A n'est pas un groupe, mais s'identifie seulement à l'ensemble quotient des classes à gauche de $\mathrm{Gal}\,(L/K)$ selon $\mathrm{Gal}\,(L/F)$. On précisera cela un peu plus loin.

6. On évitera d'employer cette notation et cette expression si L/K n'est pas galoisienne.

Theorème 4.22 *Une extension finie L/K est galoisienne si et seulement si elle est normale et séparable. Dans ce cas, pour toute extension intermédiaire $E \subset L$, l'extension $[L : E]$ est galoisienne.*

Démonstration : Supposons que L est normale et séparable. Alors il existe $a \in L$ tel que $L = K[a]$ via le théorème de l'élément primitif. Le polynôme minimal P de a est irréductible et séparable par définition d'une extension séparable, et L est le corps de rupture de P sur K, donc aussi son corps de décomposition puisque L est normale. Ainsi l'assertion b) du théorème 4.17 est satisfaite et L est galoisienne sur K (On peut éviter d'utiliser le théorème de l'élément primitif en écrivant L comme corps de décomposition d'un polynôme P sur K, puis en décomposant P en produits d'irréductibles).

Supposons réciproquement L/K galoisienne, elle est en particulier normale via la caractérisation b) du théorème 4.17 et le théorème 4.3. Soit $a \in L$, de polynôme minimal P, on pose $F = K[a]$ et $r = \deg P = [F : K]$, puis $n = [L : K]$. Il s'agit de montrer que P possède r racines distinctes dans L. Soit A l'ensemble des K-morphismes de F dans L, il y en a autant que de racines de P dans L (car se donner un tel K-morphisme est équivalent à se donner l'image de a parmi les racines de P, cf. remarque 1.20). Le lemme 4.21 et le fait que L/K soit galoisienne donnent $n = (\#A)(\#\mathtt{Aut}(L/F))$. Le théorème 4.17 dit que $\#\mathtt{Aut}(L/F) \leq [L : F]$, donc comme $n = r[L : F]$, on obtient que $\#A \geq r$, donc finalement $\#A = r$ (P ne peut pas avoir plus de r racines), ce qui conclut la preuve de la séparabilité de L/K.

Maintenant, pour toute extension intermédiaire E, on sait que L/E reste normale (théorème 4.5, b) et séparable (remarque 4.12), donc est galoisienne. □

Un cas particulier d'extension galoisienne apparaît dans la proposition suivante, qui sera utile pour établir la correspondance de Galois.

Proposition 4.23 *Soit L un corps. Soit H un sous-groupe fini du groupe des automorphismes du corps L, on pose $K = L^H$. Supposons L/K finie.*[7]

Alors L/K est galoisienne et $H = \mathtt{Aut}(L/K)$.

Démonstration : Posons $G = \mathtt{Aut}(L/K)$. Comme $H \subset G$, a fortiori $L^G = K$ et par le théorème 4.17 (caractérisation c), l'extension L/K est galoisienne. Le lemme 4.18 fournit alors $a \in L$ tel que les $\sigma(a), \sigma \in G$ soient

7. C'est en fait automatique, mais un peu plus difficile à démontrer ; voir par exemple le livre de Stewart [3], où cette proposition sert de base à toute la théorie au lieu de passer par les notions de corps de rupture ou de décomposition.

deux à deux distincts. Ceci implique que le polynôme minimal de a sur K (qui s'annule en tous les conjugués de a) est

$$P := \prod_{\sigma \in G} (X - \sigma(a)).$$

Comme $L^H = K$, on observe que le polynôme

$$Q := \prod_{\sigma \in H} (X - \sigma(a))$$

est aussi dans $K[X]$, car il est invariant sous l'action de H. Comme $Q(a) = 0$, on en déduit que $Q = P$, et donc finalement $H = G$.

□

On en vient au théorème fondamental de la théorie de Galois qui établit, pour toute extension galoisienne, une correspondance entre extensions intermédiaires et sous-groupes du groupe d'automorphismes.

Theorème 4.24 *Soit L/K une extension finie galoisienne. Soit $\mathcal{E}$ l'ensemble des extensions intermédiaires $F \subset L$ et $\mathcal{G}$ l'ensemble des sous-groupes de $G := \mathrm{Gal}\,(L/K)$. On ordonne ces deux ensembles par inclusion. Alors :*

a) Les applications $u : F \mapsto \mathrm{Gal}\,(L/F)$ de $\mathcal{E}$ dans $\mathcal{G}$ et $v : H \mapsto L^H$ de $\mathcal{G}$ dans $\mathcal{E}$ sont inverses l'une de l'autre, et établissent des bijections décroissantes entre $\mathcal{E}$ et $\mathcal{G}$.

b) Pour toute extension intermédiaire F, l'indice de $u(F)$ dans G est $[F : K]$.

c) Soit $\tau \in G$. On a alors, dans le groupe G :

$$u(\tau(F)) = \tau u(F) \tau^{-1}.$$

d) Une extension intermédiaire F est galoisienne sur K si et seulement si le sous-groupe $u(F)$ est distingué dans G. Dans ce cas $\mathrm{Gal}\,(F/K)$ est isomorphe au groupe quotient $G/u(F)$.

Démonstration : a) Il est clair que les applications u et v sont décroissantes. Soit F une extension intermédiaire, alors L/F est galoisienne par le théorème 4.22, donc $L^{u(F)} = F$ par la caractérisation c) du théorème 4.17. Si enfin H est un sous-groupe de G, et $F := L^H$, alors $\mathrm{Gal}\,(L/F) = H$ par la proposition 4.23.

b) Comme L/F est galoisienne, le cardinal de $u(F)$ est $[L : F]$, et son indice dans G est donc $[L : K]/[L : F]$, soit $[F : K]$.

c) Soit $\sigma \in u(F)$, alors pour tout $y \in \tau(F)$ on peut écrire $y = \tau(x)$ avec $x \in F$; d'où

$$(\tau\sigma\tau^{-1})(y) = \tau(\sigma(x)) = \tau(x) = y,$$

ce qui montre que $\tau\sigma\tau^{-1} \in u(\tau(F))$, soit finalement $\tau u(F)\tau^{-1} \subset u(\tau(F))$. On a de même $\tau^{-1}u(\tau(F))\tau \subset u(F)$ (en changeant τ en τ^{-1} et F en $\tau(F)$; on peut aussi observer que les deux membres de l'inclusion sont des sous-groupes de G de même indice, donc de même cardinal), qui donne bien $u(\tau(F)) = \tau u(F)\tau^{-1}$.

d) Si maintenant F/K est galoisienne, alors tout $\tau \in G$ induit par restriction un K-automorphisme de F par la proposition 4.5, a). On a donc $\tau u(F)\tau^{-1} = u(F)$ d'après c), i.e. $u(F) \lhd G$. Si réciproquement $u(F) \lhd G$, c) donne encore que pour tout $\tau \in G$, on a $\tau(F) = F$ puisque u est bijective. La proposition 4.7 donne alors que F/K est normale, donc galoisienne puisque séparable.

Supposons encore F/K galoisienne. On définit alors un morphisme de groupes $G \to \mathrm{Gal}\,(F/K)$ en restreignant tout $\tau \in G$ à F. Le noyau de ce morphisme est par définition $\mathrm{Gal}\,(L/F)$. Le théorème de factorisation et l'égalité

$$\#G = [L : K] = [L : F][F : K] = (\#\mathrm{Gal}\,(L/F))(\#\mathrm{Gal}\,(F/K))$$

donnent alors que c'est un isomorphisme.

□

Noter que c) donne en particulier que pour $\alpha, \beta \in L$, dire que α et β sont conjugués correspond au fait que les sous-groupes $\mathrm{Gal}\,(L/K(\alpha))$ et $\mathrm{Gal}\,(L/K(\beta))$ sont conjugués.

4.4. Quelques exemples

Nous passons en revue quelques exemples de groupes de Galois.

Exemple 4.25 L'extension $\mathbf{C}/\mathbf{R}$ est galoisienne, de groupe de Galois isomorphe à $\mathbf{Z}/2$ (il consiste en l'identité et la conjugaison complexe). Plus généralement, si K est un corps de caractéristique différente de 2 et $a \in K^*$ n'est pas un carré dans K^*, alors $K(\sqrt{a})/K$ est galoisienne de groupe $\mathbf{Z}/2$.

Exemple 4.26 Soit K un corps de caractéristique différente de 2. Soient $a, b \in K^*$ tels que : ni a, ni b, ni ab ne soient des carrés dans K^*. Alors l'extension $L := K(\sqrt{a}, \sqrt{b})/K$ est galoisienne, car c'est le corps de décomposition du polynôme séparable $(X^2 - a)(X^2 - b)$. On a trois extensions

intermédiaires distinctes (grâce à l'hypothèse que a, b et ab ne sont pas des carrés) de degré 2 sur K, à savoir $K(\sqrt{a})$, $K(\sqrt{b})$ et $K(\sqrt{ab})$. Ceci impose que le groupe de Galois $G = \mathrm{Gal}\,(L/K)$ est d'ordre 4 et a trois sous-groupes d'ordre 2, il est donc isomorphe à $(\mathbf{Z}/2)^2$. Noter que ces trois sous-groupes sont abstraitement isomorphes, mais les extensions intermédiaires correspondantes ne le sont pas (le point est que les trois sous-groupes ne sont pas conjugués dans G).

Exemple 4.27 Soit F/K une extension séparable de corps. D'après le théorème de l'élément primitif, on peut écrire F comme corps de rupture d'un polynôme irréductible séparable $P \in K[X]$. Soit L le corps de décomposition de P, le théorème 4.17 donne que c'est une extension galoisienne de K, qui est clairement la plus petite extension galoisienne de K contenant F (au sens : L admet un morphisme de corps vers toute extension galoisienne de K contenant F). On l'appelle la *clôture galoisienne* de l'extension F/K. Si F/K n'est pas normale, le sous-groupe $\mathrm{Gal}\,(L/F)$ n'est pas distingué dans $\mathrm{Gal}\,(L/K)$, et en particulier ce dernier n'est pas abélien.

Exemple 4.28 Soient $F = \mathbf{Q}(\sqrt[3]{2})$. La clôture galoisienne de l'extension $F/\mathbf{Q}$ est l'extension $L = F(j)$, où $j = \frac{-1+i\sqrt{3}}{2}$, car L est le corps de décomposition du polynôme irréductible $X^3 - 2$ sur $\mathbf{Q}$. Le groupe de Galois $G = \mathrm{Gal}\,(L/\mathbf{Q})$ est de degré 6, et comme l'extension $F/\mathbf{Q}$ n'est pas normale, cela signifie que G n'est pas abélien. Il est donc isomorphe à $\mathcal{S}_3$. Comme $\mathcal{S}_3$ possède un unique sous-groupe distingué non trivial ($\mathcal{A}_3$, qui est d'indice 2), il y a une unique extension intermédiaire entre $\mathbf{Q}$ et L qui est galoisienne et de degré 2 sur $\mathbf{Q}$: c'est $\mathbf{Q}(j)$.

Exemple 4.29 Soit $E = \mathbf{Q}(\sqrt{2})$. Posons $\alpha = \sqrt{1+\sqrt{2}}$ et $F = \mathbf{Q}(\alpha) = E(\alpha)$, alors $\mathbf{Q} \subset E \subset F$, et $[F : E] = 2$ (on n'a pas $F = E$ car on voit facilement que $\alpha \notin E$), d'où $[F : \mathbf{Q}] = 4$. Le polynôme minimal de α sur $\mathbf{Q}$ est donc $(X^2-1)^2-2$, et ses conjugués sont $\pm\alpha$ et $\pm\beta$ avec $\beta = \sqrt{1-\sqrt{2}} := i\sqrt{\sqrt{2}-1}$. La clôture galoisienne $L := \mathbf{Q}(\alpha, \beta) = F(\beta)$ de F sur $\mathbf{Q}$ est de degré 2 sur F (le carré de β est dans F, mais $L \neq F$ car $F \subset \mathbf{R}$ mais $\beta \notin \mathbf{R}$). Ainsi $[L : \mathbf{Q}] = 8$ et $\mathrm{Gal}\,(L/\mathbf{Q})$ est un groupe d'ordre 8 contenant au moins un sous-groupe d'ordre 2 non distingué, il est donc isomorphe au groupe diédral D_4.

Si maintenant on prend $\gamma = \sqrt{2+\sqrt{2}}$, l'extension $F' = \mathbf{Q}(\gamma)/\mathbf{Q}$ est normale comme corps de décomposition du polynôme $(X^2-2)^2-2$: ici en effet $\sqrt{2-\sqrt{2}} = (\sqrt{2}/\gamma) \in F'$, et $\mathrm{Gal}\,(F'/\mathbf{Q})$ est cyclique d'ordre 4, engendré par l'automorphisme σ de F' qui envoie γ sur $\sqrt{2-\sqrt{2}} = \sqrt{2}/\gamma$: il suffit

pour le voir de vérifier que $\sigma^2 \neq \mathrm{Id}$. Or σ envoie $\gamma^2 = 2+\sqrt{2}$ sur $2-\sqrt{2}$, donc $\sqrt{2}$ sur $-\sqrt{2}$; ainsi σ^2 envoie γ sur $-\sqrt{2}/(\sqrt{2}/\gamma) = -\gamma$.

Exemple 4.30 Soient K un corps fini de cardinal q et L une extension finie de K de degré d. Le théorème 2.3 et la proposition 2.5 disent que L est à la fois le corps de rupture et le corps de décomposition d'un polynôme irréductible de degré d de $K[X]$. Comme K est parfait, l'extension L/K est également séparable, donc galoisienne. Soit F l'élément de $\mathrm{Gal}\,(L/K)$ défini par $x \mapsto x^q$. Comme on l'a vu, les itérés F^i pour $0 \leq i < d$ sont deux à deux distincts, ce qui montre que $\mathrm{Gal}\,(L/K)$ (qui est de degré d) est cyclique engendré par F (qu'on appelle automorphisme *de Frobenius*).

Exemple 4.31 Soit n un entier ≥ 2. Soit L le corps de décomposition sur $\mathbf{Q}$ du polynôme $X^n - 1$, i.e. $L = \mathbf{Q}(\zeta)$ avec $\zeta = e^{2i\pi/n}$. C'est une extension galoisienne de $\mathbf{Q}$. Soit U_n le groupe multiplicatif des racines n-ièmes de l'unité. Alors le groupe de Galois $G = \mathrm{Gal}\,(L/\mathbf{Q})$ opère sur U_n, ce qui produit un morphisme $\theta : G \to \mathtt{Aut}(U_n)$, où $\mathtt{Aut}(U_n)$ désigne le groupe des automorphismes du groupe U_n. Ce morphisme est injectif car un élément de G qui fixe ζ fixe L tout entier. Par ailleurs, le polynôme minimal de ζ sur $\mathbf{Q}$ est le polynôme cyclotomique Φ_n d'après le théorème 3.4. Il en résulte que

$$\varphi(n) = [L : \mathbf{Q}] = \#G,$$

et comme U_n est cyclique d'ordre n, le groupe $\mathtt{Aut}(U_n)$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$, qui est aussi d'ordre $\varphi(n)$. Finalement $G \simeq (\mathbf{Z}/n\mathbf{Z})^*$. Si on remplace $\mathbf{Q}$ par un corps de base quelconque K de caractéristique ne divisant pas n, on a encore un morphisme injectif de $\mathrm{Gal}\,(L/K)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$, mais ce morphisme n'est pas surjectif en général (prendre par exemple $K = \mathbf{R}$). On dit que L est une *extension cyclotomique* de K.

Exemple 4.32 Soit K un corps de caractéristique zéro sur lequel le polynôme $X^n - 1$ est scindé. Soit $a \in K^*$. Soit L le corps de décomposition du polynôme $P := X^n - a$ sur K. Soit α une racine de P et $\zeta \in K$ une racine primitive n-ième de l'unité, alors les racines de P sont les $\zeta^k\alpha$, $k = 0, ..., n-1$, d'où $L = K(\alpha)$. Soit m le plus petit entier strictement positif tel que α soit conjugué de $\zeta^m\alpha$, et soit $\sigma \in \mathrm{Gal}\,(L/K)$ le K-automorphisme de L qui envoie α sur $\zeta^m\alpha$. Alors m divise n (et $m = 1$ si a n'a pas de racine k-ièmes dans K pour $k \geq 2$ divisant n, ce qui équivaut à P irréductible sur K), et le groupe de Galois $\mathrm{Gal}\,(L/K)$ est engendré par σ, donc cyclique d'ordre n/m divisant n. Une telle extension s'appelle une *extension de Kummer*.

Remarque 4.33 Si K est un corps de caractéristique zéro dont on fixe une clôture[8] algébrique K, on peut encore démontrer une correspondance de Galois entre les sous-groupes de $\mathtt{Aut}(\overline{K}/K)$ et les extensions intermédiaires, mais elle ne concerne que les sous-groupes *fermés* (pour une certaine topologie, dite de Krull) de $\mathtt{Aut}(\overline{K}/K)$, les extensions finies correspondent alors aux sous-groupes ouverts de $\mathtt{Aut}(\overline{K}/K)$ (condition plus forte qu'être un sous-groupe fermé). On démontre aussi que le groupe de Galois $\mathtt{Aut}(\overline{K}/K)$ est alors la *limite projective* des $\mathrm{Gal}\,(L/K)$ pour les extensions intermédiaires L finies et galoisiennes sur K.

5. Applications de la théorie de Galois

5.1. Permutation des racines, équation générique de degré n

Définition 5.1 Soient K un corps et P un polynôme irréductible de $K[X]$, supposé séparable si K est imparfait de caractéristique p. On appelle *groupe de Galois de P* le groupe de Galois $\mathrm{Gal}\,(L/K)$, où L est le corps de décomposition de P.

Proposition 5.2 *Soient K, P et L comme ci-dessus. Alors le groupe de Galois G de P opère fidèlement et transitivement sur l'ensemble $A \subset L$ des racines de P. Réciproquement, si M est le corps de décomposition sur K d'un polynôme séparable Q et $\mathrm{Gal}\,(M/K)$ opère transitivement sur l'ensemble des racines de M, alors Q est irréductible sur K.*

Démonstration : Si $\sigma \in G$ vérifie $\sigma(\alpha) = \alpha$ pour tout $\alpha \in A$, alors σ est l'identité sur L puisque le corps L est engendré par K et les éléments de A, d'où la fidélité de l'action. La transitivité est la proposition 4.7.

Pour la réciproque, on note que si $Q = Q_1...Q_r$ est la décomposition de Q en produit de polynômes irréductibles deux à deux premiers entre eux (noter qu'il n'y a pas de multiplicité > 1 dans la décomposition car Q est supposé séparable), alors pour chaque indice i, toute racine de Q_i est envoyée par tout élément de $\mathrm{Gal}\,(M/K)$ sur une racine de Q_i, donc l'action de $\mathrm{Gal}\,(M/K)$ sur les racines de Q ne peut pas être transitive si $r \geq 2$.

□

Ainsi, le groupe de Galois d'un polynôme irréductible séparable de degré n sur K peut se voir comme un sous-groupe *transitif* de $\mathcal{S}_n$ (i.e. qui opère

8. Si K est imparfait, on doit remplacer clôture algébrique par clôture séparable.

transitivement sur $\{1, ..., n\}$).

Exemple 5.3 a) Si P est de degré 3, son groupe de Galois est $\mathcal{S}_3$ ou $\mathcal{A}_3$.

b) Si P est de degré 4, le groupe de Galois peut a priori être isomorphe à $\mathbf{Z}/2 \times \mathbf{Z}/2$, $\mathbf{Z}/4$, D_4, $\mathcal{A}_4$, ou $\mathcal{S}_4$. il se trouve qu'en fait, tous les cas se produisent si $K = \mathbf{Q}$.

c) Si $K = \mathbf{Q}$, supposons que P a r racines réelles et $2s$ racines complexes non réelles (conjuguées deux à deux) avec $s > 0$. Alors le groupe de Galois G de P contient un élément d'ordre 2, la conjugaison complexe, dont l'action sur l'ensemble des racines est la composée de s transpositions à supports disjoints. Si $\deg P = 3$ et P n'a qu'une racine réelle, ceci implique que G contient une transposition, donc est isomorphe à $\mathcal{S}_3$ tout entier puisqu'il ne peut alors pas être isomorphe à $\mathcal{A}_3$.

On peut se demander s'il existe des polynômes irréductibles de degré n sur certains corps dont le groupe de Galois est $\mathcal{S}_n$ tout entier. Nous allons maintenant voir un exemple de cette situation.

Définition 5.4 Soit K_0 un corps. Soit K le corps de fractions rationnelles $K_0(T_1, ..., T_n)$. Le *polynôme générique* sur $K_0(T_1, ..., T_n)$ est le polynôme P de $K[X]$ défini par

$$P = X^n - T_1X^{n-1} + T_2X^{n-2} - ... + (-1)^nT_n.$$

Theorème 5.5 *Le polynôme P est irréductible sur K, de groupe de Galois $\mathcal{S}_n$.*

Démonstration : L'idée va être de réaliser $\mathcal{S}_n$ comme groupe de Galois sur le corps $E = K_0(T_1, ..., T_n)_s$ des fractions rationnelles symétriques (c'est le corps des fractions de la K_0-algèbre $K_0[T_1, ..., T_n]_s$ des polynômes symétriques, voir le cours sur les anneaux), puis d'utiliser l'isomorphisme de $K_0[T_1, ..., T_n]_s$ avec $K_0[T_1, ..., T_n]$ vu dans le cours sur les anneaux.

Notons σ_1, ..., σ_n les polynômes symétriques élémentaires. Soit

$$Q = \prod_{i=1}^{n}(X - T_i) = X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} - ... + (-1)^n\sigma_n,$$

c'est un polynôme séparable de $E[X]$, dont le corps de décomposition sur E est par définition K. On peut voir les éléments de $\mathcal{S}_n$ comme des éléments de $\mathtt{Aut}(K/E)$, et comme $K^{\mathcal{S}_n} = E$, la proposition 4.23 dit que K/E est galoisienne de groupe $\mathcal{S}_n$. Comme l'action de $\mathcal{S}_n$ sur l'ensemble des racines

$\{T_1, ..., T_n\}$ de Q est transitive, le polynôme Q est irréductible sur E, de groupe de Galois $\mathrm{Gal}\,(K/E) \simeq \mathcal{S}_n$

Le théorème de structure des polynômes symétriques (et son corollaire sur les fractions rationnelles symétriques) dit maintenant qu'il existe un K_0-isomorphisme Φ du corps E, sur le corps K, qui envoie chaque σ_i sur T_i. Il en résulte en appliquant Φ que le polynôme $P = \Phi(Q)$ est irréductible sur K, de groupe de Galois isomorphe à $\mathcal{S}_n$.

□

Remarque 5.6 Bien entendu, cela ne signifie pas que sur un corps quelconque, on peut toujours réaliser $\mathcal{S}_n$ comme groupe de Galois, par exemple sur $\mathbf{R}$ les seuls groupes de Galois possibles sont $\{1\}$ et $\mathbf{Z}/2$ et sur un corps fini tous les groupes de Galois sont cycliques. En revanche, on peut démontrer qu'il y a une infinité de polynômes irréductibles de degré n sur $\mathbf{Q}$ dont le groupe de Galois est $\mathcal{S}_n$. On écrit (via le théorème de l'élément primitif) le corps de décomposition L de $P = X^n - T_1X^{n-1} + T_2X^{n-2} - ... + (-1)^nT_n$ sur $K = \mathbf{Q}(T_1, ..., T_n)$ comme $L = K[T]/(\pi)$, où $\pi = \pi(T_1, ..., T_n, T) \in K[T]$ est irréductible unitaire de degré $n!$ sur K. La difficulté consiste maintenant à trouver une infinité de valeurs $(t_1, ..., t_n) \in \mathbf{Q}^n$ telles que $R := \pi(t_1, ..., t_n, T)$ reste irréductible [9] dans $\mathbf{Q}[T]$, auquel cas $\mathbf{Q}[T]/(R)$ est bien un corps de degré $n!$ sur $\mathbf{Q}$, qui apparaît comme le corps de décomposition de $P(t_1, ..., t_n, T)$ (lequel est de degré n) sur $\mathbf{Q}$. Ceci est possible via le *théorème d'irréductibilité de Hilbert* , voir par exemple le chapitre 9 de [2]. On verra en TD (cf. aussi exemple 5.8 ci-dessous) des exemples explicites sur $\mathbf{Q}$ où le groupe de Galois est effectivement $\mathcal{S}_n$.

Remarque 5.7 Le *problème inverse de Galois* consistant à déterminer si tout groupe fini G est groupe de Galois sur $\mathbf{Q}$ est très loin d'être résolu à l'heure actuelle. La correspondance de Galois et le théorème de Cayley permettent, après avoir réalisé $\mathcal{S}_n$ comme groupe de Galois $\mathrm{Gal}\,(L/\mathbf{Q})$, de réaliser G comme groupe de Galois de l'extension finie L^G de $\mathbf{Q}$, mais pas a priori de $\mathbf{Q}$ lui-même.

Exemple 5.8 Soit $p \geq 3$ un nombre premier. Soit $f \in \mathbf{Q}[X]$ un polynôme irréductible de degré p admettant exactement deux racines complexes non réelles. Alors le groupe de Galois de f est $\mathcal{S}_p$. Soient en effet L le corps de décomposition de f et $G = \mathrm{Gal}\,(L/K)$. Le corps de rupture $F \subset L$ de f est de degré p sur K, ce qui implique que le cardinal de G est divisible par p et divise $p!$ (puisque G est un sous-groupe de $\mathcal{S}_p$). Le théorème de Sylow donne alors que G possède un sous-groupe de cardinal p, qui correspond donc au groupe

9. Noter qu'il ne suffit pas que $P(t_1, ..., t_n, T)$ reste irréductible.

engendré par un p-cycle c dans $\mathcal{S}_p$. Par ailleurs, G contient la conjugaison complexe τ, qui laisse fixe les $p-2$ racines réelles et échange les deux racines complexes conjuguées ; ainsi τ correspond à une transposition dans $\mathcal{S}_p$. Or, le sous-groupe de $\mathcal{S}_p$ engendré par τ et c est $\mathcal{S}_p$ tout entier : en effet si par exemple $c = (1, ..., p)$ et $\tau = (1, 2)$, alors G contient les transpositions $(2, 3) = c\tau c^{-1}$, $(3, 4) = c^2\tau c^{-2}$, ... , $(p, 1) = c^{p-1}\tau c^{1-p}$; puis toutes les transpositions $(1, r)$ par récurrence sur r (en utilisant $(1, r+1) = (1, r)(r, r+1)(1, r)$), puis enfin toutes les transpositions (r, s) via $(r, s) = (1, r)(1, s)(1, r)$. On conclut en utilisant que $\mathcal{S}_p$ est engendré par les transpositions.

5.2. Résolubilité par radicaux

C'est une question historiquement importante de savoir si on peut exprimer les solutions d'une équation polynomiale $P(x) = 0$ à l'aide de *radicaux*, c'est-à-dire d'éléments obtenus par extraction successive de racines n-ièmes (pour divers n, ex. $\sqrt[3]{1+\sqrt{2}}$). Cela conduit à la définition suivante :

Définition 5.9 Soit K un corps de caractéristique zéro [10]. Une *extension radicale* de K est une extension du type $L = K(\alpha_1, ...\alpha_m)$ (pour $m = 0$, on convient que $K(\alpha_1, ...\alpha_m) = K$) telle que pour tout $i \in \{1, ..., m\}$, il existe un entier n_i tel que $\alpha_i^{n_i} \in K(\alpha_1, ..., \alpha_{i-1})$. On dit qu'un polynôme $f \in K[X]$ est *résoluble par radicaux* s'il existe une extension radicale L_1 de K qui contient le corps de décomposition L de f.

Une suite du type $(\alpha_1, ..., \alpha_m)$ comme ci-dessus s'appelle une *suite radicale*. Noter que f résoluble par radicaux n'implique pas que l'extension de décomposition L/K soit elle-même radicale, on demande juste que les éléments de L (en particulier les racines de P) puissent être exprimés avec des radicaux.

Lemme 5.10 *Soit L/K une extension radicale. Alors la clôture galoisienne (cf. exemple 4.27) M de L sur K est une extension radicale de K.*

Démonstration : Écrivons $L = K(\alpha_1, ...\alpha_m)$ avec $\alpha_i^{n_i} \in K(\alpha_1, ..., \alpha_{i-1})$ pour tout i. On montre le résultat par récurrence sur m. Le cas $m = 0$ est trivial. Supposons le résultat vrai jusqu'à $m - 1$. Alors la clôture galoisienne

10. En caractéristique $p > 0$, la définition serait un peu plus compliquée, il faudrait en particulier considérer aussi les corps de décomposition des polynômes du type $X^p - X - a$. On fera attention à ne pas confondre extension radicale et extension *radicielle*, ce dernier terme désignant une extension d'un corps de caractéristique p obtenue comme corps de rupture d'un polynôme de la forme $X^p - a$ comme dans l'exemple 4.11.

M_{m-1} de $L_{m-1} := K(\alpha_1, ..., \alpha_{m-1})$ est une extension radicale de K, soit $M_{m-1} = K(\gamma_1, ..., \gamma_s)$, où $\gamma_1, ..., \gamma_s$ est une suite radicale. On a alors $L = L_{m-1}(\alpha_m)$ et $M = M_{m-1}(\beta_1, ..., \beta_r)$, où les β_i sont les conjugués de α_m sur K. Ainsi $M = K(\gamma_1, ..., \gamma_s, \beta_1, ..., \beta_r)$ et $(\gamma_1, ..., \gamma_s, \beta_1, ..., \beta_r)$ est une suite radicale car chaque β_i vérifie $\beta_i^{n_m} \in M_{m-1}$ puisque $\alpha_m^{n_m} \in L_{m-1}$ et M_{m-1} est la clôture galoisienne de L_{m-1}.

□

Theorème 5.11 *Soit K un corps de caractéristique 0. Soit $f \in K[X]$ un polynôme de corps de décomposition L. Si f est résoluble par radicaux, alors le groupe de Galois* $\mathrm{Gal}\,(L/K)$ *est résoluble.*

Démonstration : D'après le lemme 5.10, on peut supposer que L possède une extension L_1 qui est normale et radicale sur K. Il suffit de montrer que $\mathrm{Gal}\,(L_1/K)$ est résoluble, puisqu'alors $\mathrm{Gal}\,(L/K)$ sera résoluble comme quotient de $\mathrm{Gal}\,(L_1/K)$. On peut donc supposer que L est normale et radicale.

On peut aussi supposer que $L = K(\alpha_1, ..., \alpha_m)$, où pour chaque α_i on a un nombre premier p_i tel que ${\alpha_i}^{p_i} \in K(\alpha_1, ...\alpha_{i-1})$, quitte à insérer d'autres α_i. On procède alors par récurrence sur m. Le cas $m = 0$ est clair. Supposons le résultat vrai jusqu'à $m - 1$. On peut supposer $\alpha_1 \notin K$ (sinon on applique l'hypothèse de récurrence). Il existe p premier tel que $\alpha_1^p = a \in K$; si on choisit un conjugué β de α_1 autre que α_1 (qui existe car L est séparable sur K vu que K est de caractéristique zéro), on a $\beta \in L$ (car L est normale sur K), donc finalement $\alpha_1/\beta \in L$, ce qui montre que L contient une racine p-ième ζ de l'unité autre que 1. Comme p est premier, cela signifie que le polynôme $X^p - 1$ est scindé sur L. Posons alors $M = K(\zeta)$. On a donc les extensions de corps

$$K \subset M \subset M(\alpha_1) \subset L.$$

Par hypothèse de récurrence, le groupe $\mathrm{Gal}\,(L/M(\alpha_1))$ est résoluble. On sait aussi que $\mathrm{Gal}\,(M(\alpha_1)/M)$ est abélien, donc résoluble (exemple 4.32), ainsi que $\mathrm{Gal}\,(M/K)$ (exemple 4.31). On conclut via le fait qu'une extension d'un groupe résoluble par un groupe résoluble est résoluble : ici $\mathrm{Gal}\,(L/M)$ est extension de $\mathrm{Gal}\,(M(\alpha_1)/M)$ par $\mathrm{Gal}\,(L/M(\alpha_1))$ puis $\mathrm{Gal}\,(L/K)$ est extension de $\mathrm{Gal}\,(M/K)$ par $\mathrm{Gal}\,(L/M)$.

□

Exemple 5.12 Le polynôme $X^5 - 6X + 3$ n'est pas résoluble par radicaux sur $\mathbf{Q}$. En effet, il est irréductible par le critère d'Eisenstein, et on vérifie facilement qu'il a 3 racines réelles et deux racines complexes conjuguées. Le critère de l'exemple 5.8 donne que son groupe de Galois est $\mathcal{S}_5$, qui n'est pas résoluble.

La réciproque du théorème 5.11 est vraie, mais demande un ingrédient supplémentaire, le *théorème de Hilbert 90*, afin d'écrire toute extension galoisienne de groupe de Galois $\mathbf{Z}/p$ de K sous la forme $K(\sqrt[p]{a})$ quand K contient les racines p-ièmes de l'unité. Voir par exemple [3].

Références

[1] D. Perrin : *Cours d'algèbre*, Ellipses 1996.

[2] J-P. Serre : *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics. Friedr. Vieweg and Sohn, Braunschweig, 1997.

[3] I. Stewart : *Galois theory*, Second edition, Chapman and Hall, Ltd., London, 1989.