Théorie des corps, théorie de Galois : une introduction

Jérémy Le Borgne

Introduction

Nous présentons dans ce cours la formulation moderne des idées de Galois, ainsi que la façon dont la théorie des corps a permis de résoudre des problèmes sur lesquels les mathématiciens butaient depuis des siècles : les « trois problèmes de l'Antiquité »ainsi que la résolubilité des équations de degré ≥ 5. Une vision possible des idées de Galois est la suivante : on se donne un certain nombre de règles (souvent liées à une forme de « construction ») et on dit qu'un objet est constructible si on peut l'obtenir à partir d'un objet de départ uniquement en suivant ces règles (par exemple, « les points de cet objet peuvent être construits à la règle et au compas à partir de ceux de l'objet de départ »). La question que l'on se pose est de savoir si un objet donné a été construit conformément à ces règles. La première étape consiste à traduire la notion de constructibilité par des équations. Plus précisément, on détermine la forme des équations dont doivent être solutions les points de l'objet que l'on veut construire. Partant d'un corps de base K, on se donne une équation algébrique à coefficients dans K vérifiant des propriétés bien précises fixées par un problème de ce type (par exemple, « cette équation est de degré 2 », ou encore « cette équation est de la forme $X^n = a$ »), et on ajoute à K toutes les combinaisons algébriques possible des solutions de cette équation, on obtient un autre corps K_1. En répétant l'opération un nombre fini n de fois, on obtient un corps $K_n = L$ contenant K. La deuxième étape à associer à L un groupe permettant de conserver toutes les informations sur les constructions intermédiaires : c'est le rôle joué par le groupe de Galois lorsque l'extension L/K est galoisienne. Cela sous-entend que le groupe de Galois est plus facile à manipuler que la connaissance de toutes les étapes de la construction, mais qu'il permet de les retrouver. La troisième étape consiste à lire directement sur ce groupe de Galois le fait que L a été construit conformément aux règles édictées au début. Plus précisément, on veut traduire les règles précises qu'on a respectées à chaque étape en propriétés précises du groupe de Galois (par exemple « le groupe de Galois de L est abélien »). Si on n'a pas perdu d'informations tout au long du processus, dire si un objet a été construit conformément aux règles du jeu reviendra à dire si le groupe de Galois d'une certaine extension de K a bien les propriétés demandées !

1 Corps, extensions de corps

Dans ce paragraphe est introduite la notion de corps, ainsi que les propriétés fondamentales des extensions de corps.

1.1 Définitions et premières propriétés

Définition 1.1. On appelle corps tout anneau commutatif unitaire (donc non nul) dans lequel tout élément non nul est inversible. On appelle morphisme de corps tout morphisme d'anneaux unitaires entre deux corps (on autorise également le morphisme nul).

Exemple 1.2. Les anneaux $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ pour p premier sont des corps. L'anneau $\mathbb{Z}$ n'est pas un corps.

Proposition 1.3. *Soit K un corps, et soit $\varphi_K : \mathbb{Z} \to K$ le morphisme canonique défini par $\varphi_K(1) = 1$. Alors le noyau de φ_K est nul ou de la forme $p\mathbb{Z}$ avec p premier.*

Démonstration. Le noyau de φ_K est un idéal de $\mathbb{Z}$, il est donc de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. Il est déjà clair que $n \neq 1$ car $1 \neq 0$ dans K. Supposons que n soit différent de 0, et soit d un diviseur strict de n. Alors $n = kd$ avec $k \in \mathbb{Z}$, et $\varphi_K(kd) = \varphi_K(k)\varphi_K(d) = 0$. Par intégrité de K, l'un de ces deux facteurs est nul. Comme d est un diviseur strict de n, $\varphi_K(d) \neq 0$ par définition de n. Par conséquent, $\varphi_K(k) = 0$ et $n \mid k$. Ainsi, $k = \pm n$ et $d = \pm 1$, donc n est premier. □

Le $n \in \mathbb{N}$ tel que $\ker \varphi_K$ soit égal à $n\mathbb{Z}$ est appelé *caractéristique* du corps K.

Remarque 1.4. La démonstration de la proposition 1.3 montre que ce résultat est en fait vraie dès que K est un anneau intègre.

Proposition 1.5. *Soient K et L des corps et $\psi : K \to L$ un morphisme de corps non nul. Alors ψ est injectif.*

Démonstration. Remarquons que les seuls idéaux du corps K sont (0) et K. En effet, si I est un idéal non nul et x un élément non nul de I, alors x a un inverse dans K, et donc $1 = x^{-1}x \in I$, d'où $I = K$.
En particulier, le noyau de ψ est K ou (0). Le morphisme ψ étant supposé non nul, $\ker \psi \neq K$, et donc $\ker \psi = \{0\}$, ce qui montre l'injectivité de ψ. □

Cette proposition montre que K est isomorphe à l'image du morphisme ψ. En particulier, L contient un sous-anneau isomorphe à K.

Définition 1.6. Soit K un corps. On appelle extension de K la donnée d'un corps L et d'un morphisme non nul $\psi : K \to L$.

En vertu de la proposition 1.5, un tel morphisme est toujours injectif, et quitte à remplacer K par l'image de ψ, on peut supposer que $K \subset L$. Cette définition permet de travailler dans un cadre un peu plus général qui est parfois plus agréable, mais on fera désormais, sauf mention contraire, l'hypothèse $K \subset L$. Cela permet notamment d'oublier le morphisme ψ et de se contenter de dire que L est une extension de K. La notation L/K signifie que L est une extension de K.

Exemple 1.7. Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in Q\}$ est une extension de $\mathbb{Q}$.

Proposition 1.8. *Soit L/K une extension de corps, alors L a une structure naturelle de K-espace vectoriel. On appelle degré de L sur K, et on note $[L : K]$, la dimension du K-espace vectoriel L. Si ce degré est fini, on dit que l'extension L/K est finie.*

Démonstration. Le corps L a déjà une structure naturelle de groupe abélien. La multiplication par un scalaire est simplement la multiplication par un élément de K dans L, qui vérifie bien les propriétés requises pour une loi externe d'espace vectoriel car L est un anneau. □

Proposition 1.9 (Formule de composition des degrés)**.** *Soient L/K et M/L des extensions de corps. Alors M est une extension de K, et $[M : K] = [M : L][L : K]$.*

Démonstration. Il est clair que $K \subset M$. Si M/L ou L/K est de degré infini, alors il est clair que M est un K-espace vectoriel de dimension infinie. Il suffit donc de démontrer la formule dans le cas où les extensions M/L et L/K sont finies. Soit $m = [M : L]$, $n = [L : K]$, $\{e_1, \ldots, e_m\}$ une base du L-espace vectoriel M, et $\{\varepsilon_1, \ldots, \varepsilon_n\}$ une base du K-espace vectoriel L. Montrons que $\{\varepsilon_i e_j, \ 1 \leq j \leq m, \ 1 \leq i \leq n\}$ est une base du K-espace vectoriel M.
Cette famille est génératrice. En effet, soit $x \in M$, $x = \sum_{1 \leq j \leq m} \lambda_j e_j$ avec $\lambda_j \in L$. De plus, pour tout $1 \leq j \leq m$, $\lambda_j = \sum_{1 \leq i \leq n} \mu_{ij} \varepsilon_j$ avec les $\mu_{ij} \in K$. Par conséquent,

$$x = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq m} \mu_{ij} \varepsilon_i e_j.$$

Cette famille est également libre, car si on a une combinaison linéaire nulle à coefficients dans K : $\sum_{i,j} \mu_{ij} \varepsilon_i e_j = 0$, alors $\sum_{1 \leq j \leq m} \left(\sum_{1 \leq i \leq n} \mu_{ij} \varepsilon_i \right) e_j = 0$. La famille des e_j étant libre sur L, on a pour tout $1 \leq j \leq m$: $\sum_{1 \leq i \leq n} \mu_{ij} \varepsilon_i = 0$, et comme la famille des ε_j est libre sur K, tous les μ_{ij} sont nuls.
Cette base est de cardinal mn, ce qui prouve la proposition. □

1.2 Extensions algébriques

Parmi les extensions d'un corps, nous allons nous intéresser plus particulièrement à celles qui sont algébriques, ce qui veut dire que tous les éléments de cette extension sont annulés par un polynôme à coefficients dans le corps de base.

Définition 1.10. Soit L/K une extension de corps, et soit $x \in L$. On dit que x est algébrique sur K s'il existe un polynôme P non nul à coefficients dans K, tel que $P(x) = 0$. Dans le cas contraire, on dit que x est transcendant.
L'extension L/K est dite algébrique si tous les éléments de L sont algébriques sur K.

Proposition 1.11. *Soit L/K une extension de corps, soit $x \in L$, soit Φ_x l'unique morphisme de K-algèbre $\Phi_x : K[X] \to L$ défini par $\Phi_x(X) = x$. Alors x est algébrique si et seulement si Φ_x est non injectif.*
Dans ce cas, il existe un unique polynôme unitaire engendrant le noyau de Φ_x, appelé polynôme minimal de x. Ce polynôme est en outre irréductible.

Démonstration. Si $P \in K[X]$, $\Phi_x(P)$ n'est rien d'autre que $P(x)$. Par définition, x est algébrique s'il existe $P \in K[X]$ non nul tel que $\Phi_x(P) = 0$. Par conséquent, x est algébrique si et seulement si Φ_x est non injectif. Comme $K[X]$ est principal, le noyau de Φ_x est alors engendré par un polynôme qui est unique si on le suppose unitaire. Enfin, l'image de Φ_x est un sous-anneau de L, en particulier c'est un anneau intègre. L'idéal $\ker \Phi_x$ est donc premier en vertu de l'isomorphisme $\Phi_x(K[X]) \simeq K[X]/\ker \Phi_x$. Comme $K[X]$ est principal, cet idéal est maximal, et donc le polynôme minimal de x est irréductible. □

Proposition 1.12. *Soit K un corps. Alors toute extension finie de K est algébrique.*

Démonstration. Soit L/K une extension finie, de degré n. Soit $x \in K$, et soit $X = \{x^k \ / \ k \in \mathbb{N}\}$. Si cette famille est finie, alors il existe k, k' distincts tels que $x^k = x^{k'}$, donc x est algébrique sur K. Si cette famille est infinie, alors elle est liée sur K et une relation de dépendance linéaire fournit un polynôme annulateur de x. □

Définition 1.13. Soit L/K une extension de corps et T une partie de L. On note $K(T)$ le plus petit sous-corps de L contenant K et T. Si $T = \{x_1, \ldots, x_n\}$, on note simplement $K(T) = K(x_1, \ldots, x_n)$.

Remarque 1.14. La démonstration de la proposition 1.11 montre que si $x \in L$ est algébrique, alors $K(x)$ est l'image de l'applications Φ_x définie précédemment. C'est en particulier une extension finie de K dont le degré est le degré du polynôme minimal de x.

Théorème 1.15. *Soit L/K une extension de corps. Alors L/K est finie si et seulement si il existe $x_1, \ldots, x_n \in L$, algébriques sur K, tels que $L = K(x_1, \ldots, x_n)$.*

Démonstration. Si L/K est finie, alors elle est algébrique. Soit $\{x_1, \ldots, x_n\}$ une base de L sur K, les x_i sont tous algébriques sur K et $L = K(x_1, \ldots, x_n)$.
Réciproquement, si $L = K(x_1, \ldots x_n)$ avec tous les x_i algébriques sur K, montrons que L/K est finie. Procédons par récurrence sur n. Le cas $n = 1$ découle de la remarque 1.14. Supposons la propriété vraie pour une valeur de n. Remarquons que $K(x_1, \ldots, x_n, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$. En effet, le corps $K(x_1, \ldots, x_n)(x_{n+1})$ contient K et tous les x_i. D'autre part, le corps $K(x_1, \ldots, x_n, x_{n+1})$ contient $K(x_1, \ldots, x_n)$ et x_{n+1}, ce qui montre l'égalité. Ainsi, x_{n+1}, étant algébrique sur K, est algébrique sur $K(x_1, \ldots, x_n)$, donc $K(x_1, \ldots, x_{n+1})/K(x_1, \ldots x_n)$ est finie d'après la remarque 1.14, ainsi que $K(x_1, \ldots, x_n)/K$ par hypothèse de récurrence, et la formule de multiplicativité des degrés permet de conclure. □

Corollaire 1.16. *Si M/L et L/K sont des extensions algébriques, alors M/K est une extension algébrique.*

Démonstration. Soit $x \in M$, comme x est algébrique sur L il est racine d'un polynôme non nul P à coefficients dans L. Le sous-corps de L engendré par les coefficients de P est une extension finie de K d'après le théorème 1.15, et x est algébrique sur ce corps, et il engendre donc une extension finie de ce corps. Par conséquent, x engendre une extension finie de K, et il est donc algébrique sur K. □

1.3 Constructions à la règle et au compas (I)

Dans cette partie, on considère le plan affine sur $\mathbb{R}^2$, que l'on note $\mathcal{P}$. On se demande quels points du plan peuvent être construits à la règle et au compas à partir de certains points donnés au départ. En particulier, si on se donne seulement deux points, on veut savoir quels points du plan peuvent être construits en un nombre fini d'étapes à partir de ces points. Si $\mathcal{P}_0$ est une partie de $\mathcal{P}$, on définit sur $\mathcal{P}_0$ deux opérations élémentaires :

1. Tracer une droite passant par deux points de $\mathcal{P}_0$,
2. Tracer un cercle centré en un point de $\mathcal{P}_0$ et dont le rayon soit la distance entre deux points de $\mathcal{P}_0$.

Définition 1.17. On dit qu'un point $P \in \mathcal{P}$ est constructible en une étape à partir de $\mathcal{P}_0$ s'il est dans l'intersection de deux objets géométriques distincts obtenus par l'une des deux opérations élémentaires précédentes.
On dit que P est constructible à partir de $\mathcal{P}_0$ s'il existe une suite $P_1, ⋮, P_n = P$ telle que pour tout $1 \leq i \leq n$, P_i soit constructible en une étape à partir de $\mathcal{P}_0 \cup \{P_1, \ldots, P_{i-1}\}$.

On suppose dorénavant que $\{(0,0),(0,1)\} \subset \mathcal{P}_0$. Soit K_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathcal{P}_0$. Si $P \in \mathcal{P}$ est constructible, alors en notant $P_i(x_i, y_i)$ comme dans la définition précédente, on définit par récurrence $K_i = K_{i-1}(x_i, y_i)$.

Proposition 1.18. *Dans les notations précédentes, pour tout $1 \leq i \leq n$, x_i et y_i sont racines d'un polynôme de degré 1 ou 2 à coefficients dans K_{i-1}.*

Démonstration. Il suffit bien entendu de faire la démonstration pour $i = 1$, notons donc $x = x_1$ et $y = y_1$. Plusieurs cas se présentent. Tout d'abord, si (x, y) est sur la droite (AB), avec $A(x_A, y_A)$ et $B(x_B, y_B)$ dans K_0. Alors on a $(y_B - y_A)(x - x_A) - (x_B - x_A)(y - y_A) = 0$, donc x et y sont linéairement dépendants sur K_0. Si (x, y) est aussi sur une droite (CD) différente de (AB), alors on obtient un système linéaire à coefficients dans K_0, inversible, et x et y sont solutions d'équations de degré 1.
Si maintenant (x, y) est sur (AB) et sur un cercle de centre Ω et de rayon r, on a $(x - x_\Omega)^2 + (y - y_\Omega)^2 = r^2$, et en utilisant la dépendance linéaire entre x et y on obtient une équation de degré 2 à coefficients dans K_0 vérifiée par x, et une autre vérifiée par y.
Enfin, si (x, y) est à l'intersection de deux cercles distincts, en faisant la différence des deux équations de cercle on obtient une équation de droite, et le système formé par cette équation de droite et l'une des deux équations de cercle est équivalent au système formé des deux équations de cercle, et le cas précédent montre que x et y sont solutions d'une équation de degré 2. □

Corollaire 1.19. *Si $P(x, y)$ est constructible à partir de $\mathcal{P}_0$, alors il existe des corps $K_0 \subset K_1 \subset \cdots \subset K_n = K_0(x, y)$ tels que $[K_i : K_{i-1}] = 2$ pour tout $1 \leq i \leq n$.*

Démonstration. La démonstration découle immédiatement de la proposition précédente. □

Lemme 1.20. *Soit $x \in K_0$, alors le point $(x, 0)$ est constructible à partir de $\mathcal{P}_0$.*

Démonstration. Il suffit de montrer que si $P(x,0)$ et $Q(y,0)$ sont dans $\mathcal{P}_0$ et $y \neq 0$, alors $(x-y,0)$ et $(x/y,0)$ sont constructibles. Pour la différence, c'est clair. Pour le quotient, on trace la droite reliant $(0,1)$ et $(y,0)$. La parallèle à cette droite passant par $(x,0)$ coupe l'axe des ordonnées en $(0,x/y)$. □

Théorème 1.21 (Wantzel)**.** *Un point $P(x,y)$ de $\mathcal{P}$ est constructible à partir de $\mathcal{P}_0$ si et seulement s'il existe une suite de corps*

$$K_0 \subset K_1 \subset \cdots \subset K_n = K(x,y),$$

tels que pour tout $1 \leq i \leq n$, $[K_i : K_{i-1}] = 2$.

Démonstration. Le corollaire 1.19 montre que la condition est nécessaire. Le lemme 1.20 montre que tous les points de K_0 sont constructibles. Il suffit donc de montrer que tout élément d'une extension de degré 2 de K_0 est abscisse d'un point constructible. Soit K_1/K_0 une extension de degré 2 et soit $x \in K_1$. On peut supposer $x \notin K_0$. Alors x est racine d'un polynôme irréductible de degré 2 à coefficients dans K_0. Les coefficients de ce polynôme $Q = aX^2+bX+c$ sont abscisses de points constructibles, on peut donc supposer qu'ils sont dans $\mathcal{P}_0$. Comme x est racine de ce polynôme, il s'exprime comme $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$, et il nous suffit de montrer que si $\alpha \in K_0$, alors $\sqrt{\alpha}$ est l'abscisse d'un point constructible. Il suffit pour cela de remarquer que l'intersection du cercle dont un diamètre a pour extrémités $(-1,0)$ et $(\alpha,0)$ avec l'axe des ordonnées est formée des points d'ordonnées $\sqrt{\alpha}$ et $-\sqrt{\alpha}$. □

Les résultats précédents (essentiellement, le corollaire 1.19) permettent de résoudre le problème des *trois constructions impossibles de l'Antiquité* :

La duplication du cube : est-il possible de construire à la règle et au compas un cube de volume double d'un cube donné ?
Si c'était possible, on en prenant pour unité le côté du cube de départ, on saurait construire le côté du cube de volume double. Mais ce côté vaut $\sqrt[3]{2}$, qui ne peut être contenu dans une extension de degré une puissance de 2 de $\mathbb{Q}$ puisque son polynôme minimal est X^3-2, qui est de degré 3.
La trisection de l'angle : est-il possible de tracer deux demi-droites partageant un angle quelconque en trois angles égaux ?
Si c'était possible, on pourrait le faire notamment pour l'angle $\frac{\pi}{3}$, ce qui permettrait de construire $\cos\frac{\pi}{9}$. Ceci est impossible car ce nombre est racine du polynôme irréductible de degré trois $8X^3-6X-1$ (en utilisant la formule de trigonométrie donnant $\cos 3\theta$).
La quadrature du cercle : est-il possible de construire à la règle et au compas un carré d'aire égale à celle d'un disque donné ?
Si c'était possible, on saurait construire $\sqrt{\pi}$, et donc π d'après le théorème de Wantzel. Cela impliquerait en particulier que π est algébrique sur $\mathbb{Q}$, ce que est bien connu comme étant faux (théorème de Lindemann).

Remarque 1.22. Le théorème de Mohr-Mascheroni affirme que toute construction possible à la règle et au compas est possible au compas seul.

2 Théorie de Galois

Dans cette partie, les notions de corps de rupture et de corps de décomposition d'un polynôme sont supposées connues. On va voir comment la théorie de Galois associe à une extension de corps un groupe contenant de nombreuses informations sur la structure de cette extension. Certaines propriétés des extensions de corps se « voient »dans la structure de leur groupe de Galois.

2.1 Groupe de Galois et extensions galoisiennes

Définition 2.1. Soit L/K une extension de corps. On appelle K-automorphisme de L tout automorphisme de corps de L laissant K invariant point par point.
L'ensemble des K-automorphismes de L forme un sous-groupe du groupe d'automorphismes de L, appelé groupe de Galois de L sur K, et noté $\mathrm{Gal}(L/K)$.

Définition 2.2. Soit L/K une extension de corps et H un sous-groupe $\mathrm{Gal}(L/K)$. Alors on note L^H l'ensemble de éléments de L invariants par H.

Proposition 2.3. *Soit L/K une extension de corps. Alors l'application qui à un sous-groupe H de $G = Gal(L/K)$ associe L^H est décroissante et à valeurs dans l'ensemble des sous-corps de L contenant K.*
D'autre part, l'application qui à un sous-corps F de L contenant K associe $Gal(L/F)$ est décroissante et à valeurs dans l'ensemble des sous-groupes de G.

Démonstration. Laissée au lecteur. □

Afin que le groupe de Galois d'une extension nous permette de bien comprendre la structure des corps intermédiaires, on aimerait que cette correspondance entre sous-corps de L contenant K et sous-groupes de $\mathrm{Gal}(L/K)$ soit bijective. Moralement, les extensions dites galoisiennes sont celles pour lesquelles cette propriété est vraie.

Définition 2.4. Soit L/K une extension de corps, et $G = \mathrm{Gal}(L/K)$. L'extension L/K est dite galoisienne si $L^G = K$.

2.2 Théorème de l'élément primitif

A partir de maintenant et sauf mention contraire, nous supposerons que le corps K est de caractéristique 0. Le cas où la caractéristique est positive pose davantage de problèmes, notamment parce que les polynômes irréductibles ne sont pas nécessairement à racines simples dans une clôture algébrique (ce que l'on appelle *séparables*). Par exemple, dans $\mathbb{F}_p(t)[X]$, le polynôme $X^p - t$ est irréductible et a une seule racine de multiplicité p. En caractéristique nulle en revanche, tous les polynômes irréductibles sont séparables.

Lemme 2.5. *On suppose K de caractéristique nulle. Soit $P \in K[X]$ et soit L une extension de K contenant une racine x de P. Alors x est racine simple de P.*

Démonstration. Si x était racine double, alors on aurait $P'(x) = 0$. Le polynôme P' serait donc un polynôme annulateur de x, à coefficients dans $K[X]$, et non nul car K est de caractéristique nulle. Il serait divisible par le polynôme minimal de x sur K, qui n'est autre que P. Cela est impossible pour des raisons de degré. □

Théorème 2.6 (de l'élément primitif)**.** *Soit L/K une extension finie, avec K de caractéristique nulle. Alors il existe $\theta \in L$ tel que $L = K(\theta)$.*

Démonstration. Comme l'extension L/K est finie, elle est engendrée par un nombre fini d'éléments algébriques (théorème 1.15). Traitons d'abord le cas où $L = K(\alpha, \beta)$ avec α et β algébriques sur K. Notons π_α et π_β leurs polynômes minimaux respectifs sur K, et $\{\alpha = \alpha_1, \ldots, \alpha_n\}$, $\{\beta = \beta_1, \ldots, \beta_m\}$ les racines respectives de π_α et π_β dans un corps de décomposition de ces deux polynômes contenant L.
Le corps K étant de caractéristique 0, il est infini, et il existe donc $t \in K$ tel que

$$t \notin \left\{ -\frac{\alpha - \alpha_i}{\beta - \beta_j} \ / \ 1 \leq i \leq n, 2 \leq j \leq m \right\}.$$

Posons $\theta = \alpha + t\beta$. Il suffit de montrer que $\beta \in K(\theta)$, car cela implique que $\alpha \in K(\theta)$. Soit $\pi = \pi_\alpha(\theta - tX)$. Alors β est racine de π, et c'est l'unique racine commune à π et à π_β. En effet, sinon, on aurait $\alpha + t\beta - t\beta_j = \alpha_i$ pour certains i, j, ce qui est exclu sauf si $\alpha_i = \alpha$ et $\beta_j = \beta$.
En particulier, comme le polynôme minimal de β sur $K(\theta)$ doit diviser π et π_β, ce polynôme a pour seule racine β. Étant irréductible, c'est d'après le lemme un polynôme de degré 1, donc $\beta \in K(\theta)$. □

2.3 Extensions normales

On suppose toujours que K est de caractéristique nulle. Nous allons voir ici une notion assez naturelle, qui est celle d'extension normale : les extension normales sont celles pour lesquelles le polynôme minimal d'un élément de l'extension a toutes ses racines dans la même extension. Nous verrons comment cela évite au groupe de Galois de l'extension d'être « trop petit ».

Définition 2.7. Soit L/K une extension de corps. On dit que L/K est normale si tout polynôme irréductible à coefficients dans K ayant une racine dans L, est scindé sur L.

Proposition 2.8. *Soit L/K une extension finie. Alors L/K est normale si et seulement si L est corps de décomposition d'un polynôme de $K[X]$.*

Démonstration. Supposons tout d'abord que L/K soit normale. Comme elle est finie elle est engendrée par un nombre fini d'éléments algébriques (théorème 1.15) : $L = K(\alpha_1, \ldots, \alpha_n)$. On note pour $1 \leq i \leq n$, π_i le polynôme minimal de α_i sur K. Comme L/K est normale, tous les π_i sont scindés sur L. Ainsi, le produit π des π_i est également scindé sur L. Le corps L contient donc un corps de décomposition E de π. Par ailleurs, E contient nécessairement tous les α_i, il contient donc L. Ainsi, $L = E$ est corps de décomposition de π.
Réciproquement, supposons que L soit corps de décomposition de $P \in K[X]$. Notant $\alpha_1, \ldots, \alpha_r$ les racines de P dans L, on a $L = K(\alpha_1, \ldots, \alpha_r)$. Soit maintenant $Q \in K[X]$ irréductible, ayant une racine $\alpha \in L$. Il existe un corps de décomposition M de PQ contenant L. On peut supposer que le degré de Q est supérieur ou égal à 2. Le polynôme Q a donc deux racines distinctes γ_1, γ_2 dans M. Nécessairement, $[K(\gamma_1) : K] = [K(\gamma_2) : K] = \deg Q$.

D'autre part, $K(\gamma_1)$ et $K(\gamma_2)$ sont isomorphes, et $L(\gamma_1)$ (respectivement, $L(\gamma_2)$ est corps de décomposition de P sur $K(\gamma_1)$ (respectivement sur $K(\gamma_2)$). Ainsi, $[L(\gamma_1) : K(\gamma_1)] = [L(\gamma_2) : K(\gamma_2)]$. En vertu de la formule de multiplicativité des degrés, on en déduit que $[L(\gamma_1) : L] = [L(\gamma_2) : L]$. Comme de plus $L(\alpha) = L$, on a $L(\gamma) = L$ pour toute racine γ de Q dans M, et donc toutes les racines de Q sont dans L. □

Proposition 2.9. *Soit L/K une extension finie. Supposons L/K normale, alors L/K est galoisienne.*

Démonstration. Comme L/K est finie, d'après le théorème de l'élément primitif, il existe $\alpha \in L$ tel que $L = K(\alpha)$. Fixons un tel α. Notons $G = \mathrm{Gal}(L/K)$. Soit $F = L^G$, nous allons montrer que $F = K$. Soit π_α le polynôme minimal de α sur K, et $\{\alpha_1, \ldots, \alpha_n\}$ les racines de π_α dans L. Comme L/K est normale, $n = [L : K] = \deg \pi_\alpha$. Pour $1 \leq i \leq n$, on définit le K-automorphisme σ_i de L par $\sigma_i(\alpha) = \alpha_i$. Les σ_i sont des éléments distincts de G. Réciproquement, un élément σ de G est nécessairement l'un des σ_i car $\pi_\alpha(\sigma(\alpha)) = 0$, donc $\sigma(\alpha)$ est racine de π_α. Ainsi, le cardinal de G est n. Le corps L est corps de décomposition de π_α sur F, et donc le cardinal de $\mathrm{Gal}(L/F)$ est égal à $[L : F]$ par le même argument que précédemment. En outre, un élément de G laisse invariants tous le élément de F, c'est donc aussi un élément de $\mathrm{Gal}(L/F)$, et donc $G = \mathrm{Gal}(L/F)$. Par conséquent, on a $[F : K] = 1$, et $F = K$. □

Remarque 2.10. La démonstration de cette proposition permet également de voir que si L/K est normale, finie, alors $|\mathrm{Gal}(L/K)| = [L : K]$.

Nous allons maintenant montrer la réciproque de cette proposition. Pour cela, nous allons utiliser le célèbre résultat d'Artin suivant :

Lemme 2.11 (Artin)**.** *Soit L un corps, soit G un groupe fini d'automorphismes de L, et soit $K = L^G$. Alors L est une extension de K, et $[L : K] \leq |G|$.*

Démonstration. Il est clair que K est un sous-corps de L.
Soit $n = |G|$, et $G = \{\sigma_1, \ldots, \sigma_n\}$. Soit $m > n$, et soit $a_1, \ldots, a_m$ une famille d'éléments distincts de L, tous non nuls.
Considérons le système d'équations linéaires $\sum_{j=1}^m \sigma_i(a_j)x_j$ pour $1 \leq i \leq n$. Comme $m > n$, ce système admet dans L une solution non nulle $(x_1, \ldots, x_m)$. Parmi toutes les solutions non nulles, choisissons-en une pour laquelle le nombre de x_i non nuls soit minimal. L'ensemble des solutions étant un L-espace vectoriel, on peut supposer que l'un des x_i est égal à 1, et quitte à renuméroter, on peut supposer que $x_1 = 1$. Nous allons montrer qu'alors, tous les x_i sont dans K.
Supposons le contraire, on peut supposer que $x_2 \notin K$, et donc il existe $1 \leq k \leq n$ tel que $\sigma_k(x_2) \neq x_2$. En appliquant σ_k à la i-ème équation du système, on voit que $\sum_{j=1}^m \sigma_k\sigma_i(a_j)\sigma_k(x_j) = 0$. Comme $\sigma_k G = G$, on en déduit que $(\sigma_k(x_1), \ldots, \sigma_k(x_m))$ est également solution du système, et donc $(x_1 - \sigma_k(x_1), \ldots, x_m - \sigma_k(x_m))$ aussi. Mais cette solution est non nulle et a strictement plus de coefficients nuls que la première, ce qui contredit la minimalité de cette première solution, et montre que les x_i sont dans K. Comme l'identité de L est élément de G, l'une des lignes du système se traduit par $\sum_{j=1}^m x_j a_j = 0$, donc la famille $\{a_j\}$ est liée sur K, donc $[L : K] \leq n$. □

Théorème 2.12 (Artin)**.** *Soit L un corps, G un groupe fini d'automorphismes de L, et $K = L^G$. Alors L/K est normale et finie, et $G = Gal(L/K)$.*

Démonstration. Le fait que L/K soit finie découle directement du lemme d'Artin. Soit $P \in K[X]$, irréductible sur K, ayant une racine $\alpha \in L$. Montrons que toutes les racines de P sont dans L.
Soit $\Omega = \{\sigma(\alpha) \ / \ \sigma \in G\}$ et soit $Q = \prod_{\omega\in\Omega}(X - \omega)$. Si $\sigma \in G$, alors $\sigma \cdot Q = Q$ (car $\sigma\Omega = \Omega$). Ainsi, par hypothèse, Q a tous ses coefficients dans K. Mais alors, P divise Q dans $K[X]$ car P est le polynôme minimal de α sur K et $Q(\alpha) = 0$. Comme par ailleurs les $\sigma(\alpha)$ sont des racines de P, on a aussi Q divise P dans $L[X]$ et donc dans $K[X]$. Ainsi, $P = Q$, et P est scindé sur L. Donc L/K est normale.
Enfin, G est clairement contenu dans $\mathrm{Gal}(L/K)$. De plus, $[L : K] = |\mathrm{Gal}(L/K)|$ car L/K est normale, et $|G| \geq [L : K]$, donc $G = \mathrm{Gal}(L/K)$. □

Théorème 2.13. *Soit L une extension finie d'un corps K de caractéristique 0. Alors L/K est galoisienne si et seulement si L/K est normale.*

Démonstration. L'une des implications résulte de la propostion 2.9. Supposons donc L/K galoisienne. Comme L/K est finie, le groupe $G = \mathrm{Gal}(L/K)$ est fini (un élément de G est déterminé par l'image d'un élément primitif, qui est nécessairement racine du polynôme minimal de cet élément primitif, et les éléments de G sont donc en nombre fini).
D'après le théorème d'Artin, comme $K = L^G$, L/K est normale. □

2.4 Correspondance de Galois

Le corps K est toujours supposé de caractéristique 0. Les outils précédents nous permettent de démontrer ce que nous avons affirmé précédemment, à savoir :

Proposition 2.14 (Correspondance de Galois)**.** *Soit L/K une extension finie, alors L est galoisienne si et seulement si les applications $H \mapsto L^H$ et $F \mapsto Gal(L/F)$, définies respectivement sur l'ensemble des sous-groupes de $Gal(L/F)$ et l'ensemble de sous-corps de L contenant K, sont des bijections réciproques l'une de l'autre.*

Démonstration. Notons $G = \mathrm{Gal}(L/K)$. Si ces deux applications sont des bijections réciproques, alors $L^G = K$ et L/K est galoisienne.
Réciproquement, supposons L/K galoisienne.
Soit H un sous-groupe de G. Comme H est fini, d'après le théorème d'Artin on a $H = \mathrm{Gal}(L/L^H)$, donc $H \mapsto L^H$ est injective, et $F \mapsto \mathrm{Gal}(L/F)$ est surjective.
Soit F un sous-corps de L contenant K. Comme L/K est galoisienne, elle est normale, et donc L/F est normale (L est corps de décomposition d'un polynôme à coefficients dans F). Elle est donc galoisienne, et $L^{\mathrm{Gal}(L/F)} = F$, donc $F \mapsto \mathrm{Gal}(L/F)$ est injective, et $H \mapsto L^H$ est surjective. Ainsi, ces deux applications sont des bijections réciproques l'une de l'autre. □

Théorème 2.15 (Théorème fondamental de la théorie de Galois)**.** *Soit L/K une extension galoisienne finie. Soit F un sous-corps de L contenant K. Alors L/F est galoisienne, et les deux assertions suivantes sont équivalentes :*

(i) $Gal(L/F)$ est un sous-groupe distingué de $Gal(L/K)$;

(ii) L'extension F/K est galoisienne. Dans ce cas, le groupe de Galois $Gal(F/K)$ est isomorphe au quotient $Gal(L/K)/Gal(L/F)$.

Démonstration. Comme L/K est galoisienne, $L^{\mathrm{Gal}(L/F)} = F$, donc L/F est galoisienne. Montrons l'équivalence des deux assertions.
Supposons $\mathrm{Gal}(L/F) = H \triangleleft G = \mathrm{Gal}(L/K)$. Alors pour tout $\sigma \in \mathrm{Gal}(L/K)$, $F = L^{\sigma H \sigma^{-1}}$. Mais $L^{\sigma H \sigma^{-1}} = \sigma(F)$. Cela montre que F est stable par G, et on peut légitimement considérer la restriction à F d'un élément de G. Soit donc $\varphi : G \to \mathrm{Gal}(F/K)$ le morphisme de restriction. Son image est un sous-groupe fini de $\mathrm{Gal}(F/K)$, d'après le théorème d'Artin, c'est le groupe de Galois de F sur le sous-corps fixé par l'image de φ, qui est clairement K, et l'extension F/K est galoisienne. Le morphisme de restriction est surjectif, et on a donc l'isomorphisme annoncé.
Réciproquement, si F/K est galoisienne, alors elle est normale, et en particulier F est stable par les éléments de $\mathrm{Gal}(L/K)$ (car ils envoient un élément primitif de F/K sur une autre racine du polynôme minimal de cet élément primitif, qui est dans F car F/K est normale). On peut de nouveau considérer le morphisme de restriction, dont le noyau est un sous-groupe distingué qui n'est autre que $\mathrm{Gal}(L/F)$ par définition. □

3 Applications de la théorie de Galois

En préambule à cette partie, intéressons-nous à un exemple : soit K un corps de caractéristique 0, $n \geq 2$ un entier, et L un corps de décomposition sur K du polynôme $X^n - 1$. Que dire du groupe de Galois de L/K ?
Tout d'abord, si ω est une racine primitive n-ème de l'unité dans L, alors $L = K(\omega)$. Soit π_ω le polynôme minimal de ω sur K, il divise $X^n - 1$, donc les racines de π_ω sont toutes des racines n-èmes de l'unité. Notons $\{\omega = \omega_1, \ldots, \omega_r\}$ l'ensemble des racines de π_α dans L. Pour tout j, il existe k_j tel que $\omega_j = \omega^{k_j}$. Naturellement, les éléments de $G = \mathrm{Gal}(L/K)$ sont les σ_j définis par $\sigma_j(\omega) = \omega_j$. En particulier, $\sigma_i\sigma_j(\omega) = \omega^{k_i k_j} = \sigma_j\sigma_i(\omega)$.
Par conséquent, le groupe $\mathrm{Gal}(L/K)$ est abélien.

3.1 Constructions à la règle et au compas (II)

Dans cette partie, on cherche à déterminer à quelle condition un polygone régulier est constructible à la règle et au compas. Pour $n \geq 3$, on notera P_n le polygone régulier à n côtés.

Lemme 3.1. *Si P_n est constructible, alors il en est de même pour P_{2n}. De plus, si m divise n, alors P_m est constructible.*

Démonstration. C'est évident dès que l'on sait tracer une bissectrice et compter de n/m en n/m. □

Lemme 3.2. *Soient m, n des entiers premiers entre eux. Si P_m et P_n sont constructibles, alors P_{mn} aussi.*

Démonstration. Il existe $a, b \in \mathbb{Z}$ tels que $\frac{a}{m} + \frac{b}{n} = \frac{1}{mn}$. Ainsi, si l'on sait construire les points du cercle trigonométrique d'angles $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$, on sait construire l'angle $\frac{2\pi}{mn}$. □

On déduit de ces deux lemmes que si $n = 2^k p_1^{k_1} \dots p_r^{k_r}$, les p_i étant premiers, impairs, et deux à deux distincts, alors P_n est constructible si et seulement si $P_{p_i^{k_i}}$ l'est pour tout $1 \leq i \leq r$.

Proposition 3.3. *Soit p un nombre premier impair et $k \geq 1$ un entier, alors si P_{p^k} est constructible, nécessairement $k = 1$ et $p - 1$ est une puissance de 2.*

Démonstration. Si ce polygone est constructible, alors $\mathbb{Q}(\cos \frac{2\pi}{p^k}, \sin \frac{2\pi}{p^k})$ est une extension de $\mathbb{Q}$ dont le degré est une puissance de 2, et donc, en notant ω une racine primitive p^k-ème de l'unité dans $\mathbb{C}$, $[\mathbb{Q}(\omega) : \mathbb{Q}]$ est une puissance de 2. Or cette extension a pour degré $\varphi(p^k) = p^{k-1}(p-1)$, d'où la proposition. □

Théorème 3.4 (Gauss)**.** *Soit p un nombre premier impair, alors le polygone P_p est constructible si et seulement si $p - 1$ est de la forme 2^{2^k} pour un $k \in \mathbb{N}$.*

Démonstration. Il est bien connu que tout nombre premier p tel que $p - 1$ soit une puissance de 2, a la propriété que $p - 1$ soit de la forme 2^{2^k} (nombres premiers de Fermat). La condition est donc nécessaire.
Réciproquement, supposons que p soit de cette forme. Soit ω une racine primitive p-ème de l'unité. Le polynôme minimal de ω sur $\mathbb{Q}$ est le polynôme cyclotomique Φ_p. Soit $K = \mathbb{R} \cap \mathbb{Q}(\omega)$. L'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne car elle est normale (c'est un corps de décomposition du polynôme minimal de ω sur $\mathbb{Q}$), de degré 2^k. Soit $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, G est abélien. En particulier, tous les sous-groupes de G sont distingués, donc l'extension intermédiaire $K/\mathbb{Q}$ est galoisienne. Son groupe de Galois est un quotient de G, c'est donc un 2-groupe, donc il existe une suite de sous-groupes G_i de G telle que $G_0 = \{1\}$, $G_n = \mathrm{Gal}(K/\mathbb{Q})$, et $|G_i| = 2^i$. Cela fournit grâce à la correspondance de Galois une suite de sous-corps de K contenant $\mathbb{Q}$ telle que les degrés intermédiaires soient tous égaux à 2. D'après le théorème de Wantzel, $\cos \frac{2\pi}{p} \in K$ est alors constructible. □

3.2 Groupes résolubles

Définition 3.5. Soit G un groupe, on appelle suite de composition de G une suite finie de sous-groupes distingués :

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$

Définition 3.6. Un groupe G est dit résoluble s'il admet une suite de composition dont tous les quotients sont abéliens.

Exemple 3.7. Les groupes abéliens sont résolubles.

Définition 3.8. Soit G un groupe, on note $D(G)$ le sous-groupe de G engendré par les commutateurs, c'est à dire les éléments de la forme $xyx^{-1}y^{-1}$. Ce sous-groupe s'appelle groupe dérivé de G. On définit par récurrence $D^n(G) = D(D^{n-1}(G))$.

Proposition 3.9. *Un groupe G est résoluble si et seulement s'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{1\}$*

Démonstration. La condition est suffisante car $D(G)$ est un sous-groupe distingué de G et $G/D(G)$ est abélien.
Elle est nécessaire car tout sous-groupe distingué H de G tel que G/H soit abélien contient $D(G)$. □

Corollaire 3.10. *Soit G un groupe. Si G est résoluble, alors tout sous-groupe et tout quotient de G est résoluble.*

Démonstration. L'application D préserve l'injectivité et la surjectivité des morphismes. □

Proposition 3.11. *Un groupe G est résoluble si et seulement si G est abélien ou G a un sous-groupe distingué non trivial H tel que H et G/H soient résolubles.*

Démonstration. La condition est nécessaire car si G est non abélien, dans une suite de composition abélienne non triviale, G_{n-1} vérifie ces propriétés (G/G_{n-1} est résoluble car abélien). On peut aussi le voir par un argument de groupe dérivé.
Montrons que la condition est suffisante. Supposons qu'il existe un tel sous-groupe H. Alors la projection canonique $G \to G/H$ fournit un morphisme surjectif $D(G) \to D(G/H)$. Le noyau de ce morphisme est constitué des éléments de $D(G)$ qui sont triviaux modulo H, c'est donc $D(G) \cap H$.
On a donc un isomorphisme $D(G)/(D(G) \cap H) \simeq D(G/H)$. Il est alors facile de voir que pour tout $n \in \mathbb{N}$, $D^n(G)/(D^n(G) \cap H) \simeq D^n(G/H)$. En particulier, pour n suffisamment grand, G/H étant résoluble, $D^n(G)/(D^n(G) \cap H)$ est trivial, c'est à dire que $D^n(G) \subset H$. Ainsi, pour $m \geq 0$, $D^{m+n}(G) \subset D^m(H)$, et donc pour m assez grand, $D^{m+n}(G)$ est trivial. Donc G est résoluble. □

Exemple 3.12. Si G est un groupe simple non abélien, alors G n'est pas résoluble. En effet, un tel groupe n'a pas de sous-groupe distingué non trivial. En particulier, pour $n \geq 5$, le groupe alterné $\mathfrak{A}_n$ est non résoluble.

Proposition 3.13. *Soit G un groupe admettant un sous-groupe distingué H non résoluble. Alors G est non résoluble.*

Démonstration. Supposons qu'on ait une suite de composition abélienne de G : $\{1\} \subset G_1 \subset \cdots \subset G_n = G$. Pour tout $1 \leq i \leq n$, notons $H_i = G_i \cap H$. Alors la suite des H_i forme une suite de composition de H. De plus, les quotients H_i/H_{i-1} sont abéliens. En effet, si $x, y \in H_i$, alors $xyx^{-1}y^{-1}$ est clairement dans H, et il est également dans G_{i-1} car le quotient G_i/G_{i-1} est abélien. La suite des H_i formerait alors une suite de composition abélienne de H, ce que est absurde. □

Remarque 3.14. Cette proposition, avec la remarque précédente, montre que le groupe symétrique $\mathfrak{S}_n$ est non résoluble dès que $n \geq 5$.

3.3 Résolubilité des équations par radicaux

Dans cette partie, on suppose toujours que K est un corps de caractéristique 0.

Définition 3.15. Soit L/K une extension de corps. L'extension L/K est dite radicale s'il existe $\alpha_1, \dots, \alpha_n \in L$ tels que $L = K(\alpha_1, \dots, \alpha_n)$ et pour tout $1 \leq i \leq n$, il existe $n_i \in \mathbb{N}^*$ tel que $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

Définition 3.16. On dit que $P \in K[X]$ est résoluble par radicaux si, L étant un corps de décomposition de P sur K, il existe une extension M/L telle que M/K soit radicale.

Si $P \in K[X]$, notons L un corps de décomposition de P, on appelle groupe de Galois de P, noté $\mathrm{Gal}(P)$, le groupe de Galois de L/K. On admettra que ce groupe ne dépend pas à isomorphisme près du choix de L.

Lemme 3.17. *Soit $n > 1$ un entier. Si $X^n - 1$ est scindé sur $K[X]$, alors pour tout $a \in K^\star$, le groupe de Galois de $X^n - a$ est abélien.*

Démonstration. Soit L/K un corps de décomposition de $P = X^n - a$. Soit $\alpha \in L$ une racine de P, alors les autres racines de P dans L sont les $\omega_i \alpha$, où les ω_i sont les n racines de $X^n - 1$ dans K. Les racines du polynôme minimal de α sont une partie de ces racines, on peut supposer quitte à renuméroter que ce sont les r premières. On définit pour $1 \leq i \leq r$ l'élément σ_i de $G = \mathrm{Gal}(L/K)$ par $\sigma_i(\alpha) = \omega_i \alpha$. Les σ_i forment le groupe G pour des raisons de cardinal. Ainsi, pour $1 \leq i, j \leq r$, on a $\sigma_i \sigma_j(\alpha) = \sigma_i(\omega_j \alpha) = \omega_j \omega_i \alpha = \sigma_j \sigma_i(\alpha)$, et G est abélien. □

Proposition 3.18. *Soient F/K galoisienne et $F(\gamma)/F$ radicale (avec $\gamma^k \in F$ pour un $k \in \mathbb{N}^*$). Alors il existe une extension L de F contenant γ, avec L/K galoisienne, L/F radicale, et $Gal(L/F)$ résoluble. Si de plus $Gal(F/K)$ est résoluble, alors $Gal(L/K)$ aussi.*

Démonstration. Soit $n \in \mathbb{N}^*$ minimal tel que $\gamma^n \in F$, et soit $\alpha_1 = \gamma^n$. On note π_1 le polynôme minimal de α_1 sur K. Comme F/K est galoisienne, π_1 est scindé sur F, notons $\alpha_1, \dots, \alpha_d$ ses racines. Pour $1 \leq i \leq d$, on note $P_i = X^n - \alpha_i$, et L un corps de décomposition de $P = (X^n - 1) \prod_{1 \leq i \leq d} P_i$ contenant $F(\gamma)$. L'extension L/F est donc galoisienne. Comme F/K est galoisienne, il en est de même pour L/K. Soit $\omega \in L$ une racine primitive n-ième de l'unité, et pour $1 \leq i \leq d$, $\gamma_i^n = \alpha_i$ avec $\gamma_i \in L$.
On pose $F_0 = F(\gamma)$, $F_i = F_{i-1}(\gamma_i)$. On a alors $L = F_d$. Cela montre que L est radicale.
Pour tout $1 \leq i \leq d$, F_i/F_{i-1} est galoisienne, et F_0/F est galoisienne (ce sont des extensions normales). Comme $L = F_i(\gamma_{i+1}, \dots, \gamma_d)$, L/F_i est galoisienne. Par correspondance de Galois, on a une suite de composition :

$$\{1\} \subset \mathrm{Gal}(L/F_{d-1}) \subset \cdots \subset \mathrm{Gal}(L/F_0) \subset \mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K).$$

En effet, F_i/F_{i-1}, F_0/F et F/K étant galoisiennes, tous les sous-groupes considérés sont distingués. De plus, les groupes de Galois de ces extensions sont abéliens en vertu de résultats précédents. Par conséquent, les quotients de la suite sont abéliens (sauf peut-être $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$), et le groupe $\mathrm{Gal}(L/F)$ est résoluble. Si en outre $\mathrm{Gal}(F/K)$ est résoluble, alors $\mathrm{Gal}(L/K)$ est résoluble par la proposition 3.11. □

Corollaire 3.19. *Soit M/K radicale, alors il existe L/M telle que L/K soit galoisienne, et $Gal(L/K)$ soit résoluble.*

Démonstration. Notons comme dans la définition $M = K(\alpha_1, \dots, \alpha_r)$. Pour tout i, on fixe n_i minimal tel que $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$. Soit ω une racine n_1-ème de l'unité, et $F = K(\omega)$. Alors F/K est galoisienne, et $F_1 = F(\alpha_1)$ est une extension radicale de F. D'après le lemme précédent, il existe une extension L_1 de F contenant α_1, radicale, avec L_1/K galoisienne et $\mathrm{Gal}(L_1/F)$ résoluble. En outre, comme $\mathrm{Gal}(L/K)$ est résoluble, $\mathrm{Gal}(L_1/K)$ est résoluble. On poursuit par récurrence en posant $F_i = L_{i-1}(\alpha_i)$, et L_i une extension radicale de F_i, galoisienne sur K, avec $\mathrm{Gal}(L_i/K)$ résoluble, jusqu'à trouver $L = L_s$ galoisienne sur K contenant M, de groupe de Galois résoluble. □

Corollaire 3.20. *Soit $P \in K[X]$ résoluble par radicaux, alors le groupe de Galois de P est résoluble.*

Démonstration. Soit E un corps de décomposition de P sur K, il existe une extension M de E telle que M/K soit radicale. D'après le corollaire 3.19, il existe une extension L de M avec L/K galoisienne et $\mathrm{Gal}(L/K)$ résoluble. Comme l'extension E/K est galoisienne, on a un isomorphisme $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$. Étant un quotient d'un groupe résoluble, $\mathrm{Gal}(E/K)$ est résoluble. □

Lemme 3.21. *Soit p un nombre premier. On suppose que K contient toutes les racines p-èmes des l'unité. Soit L/K galoisienne finie de degré p. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ et dont le polynôme minimal sur est de la forme $X^p - a$.*

Démonstration. Le groupe de Galois G de L/K est d'ordre p, donc cyclique. Notons σ un générateur de G. Soit ω une racine primitive p-ème de l'unité dans K. Pour $x \in L$, on note $\alpha_x = \sum_{i=0}^{p-1} \sigma^i(x) \prod_{j=0}^{i} \sigma^j(\omega)$. On a alors $\sigma(\alpha_x) = \sum_{i=0}^{p-1} \sigma^{i+1}(x) \prod_{j=1}^{i+1} \sigma^j(\omega) = \frac{1}{\omega} \sum_{i=1}^{p} \sigma^i(x) \prod_{j=0}^{i} \sigma^j(\omega) = \frac{\alpha_x}{\omega}$ car le produit des conjugués de ω est 1.
On admet qu'il existe $x \in L$ pour lequel $\alpha_x \neq 0$ (cela résulte directement d'un résultat assez connu, le théorème d'indépendance linéaire des caractères). On fixe un tel x, et on note $\alpha = \alpha_x$. On a alors $\sigma(\alpha) \neq \alpha$, donc $\alpha \notin K$, et $\sigma(\alpha^p) = \sigma(\alpha)^p = (\omega^{-1}\alpha)^p = \alpha^p$, donc $a = \alpha^p \in K$. Le corps $K(\alpha)$ est corps de décomposition de $X^p - a$ sur K, et $K \subset K(\alpha) \subset L$, et comme L/K n'a pas d'extensions intermédiaires, $L = K(\alpha)$ et $X^p - a$ est le polynôme minimal de α sur K. □

Proposition 3.22. *Soit L/K une extension galoisienne finie dont le groupe de Galois est résoluble. Alors il existe une extension R de L radicale sur K.*

Démonstration. On procède par récurrence sur $n = [L : K]$. Le cas $n = 1$ est trivial, supposons $n > 1$.
Notons $G = \mathrm{Gal}(L/K)$, G est d'ordre n. Soit $H \triangleleft G$ un sous-groupe distingué maximal. Le quotient G/H est alors simple (sinon, on aurait un sous-groupe distingué contenant strictement H) et résoluble car G l'est. C'est donc un groupe abélien (une suite de composition est forcément triviale) et donc cyclique (le sous-groupe engendré par un élément non trivial est distingué et non trivial). Il est donc d'ordre un nombre premier. Soit $p = |G/H|$, soit F/L un corps de décomposition de $X^p - 1$. Notant ω une racine p-ème de l'unité différente de 1, on a $F = L(\omega)$. Considérons le

sous-corps $M = K(\omega) \subset F$. Les extensions F/L et M/K sont radicales. L'extension F/M est galoisienne car c'est un corps de décompostion du même polynôme dont L est corps de décomposition sur K.
D'autre part, on sait que $\mathrm{Gal}(F/L)$ est abélien donc résoluble, et le théorème fondamental montre que $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/L) \simeq \mathrm{Gal}(L/K)$. Comme $\mathrm{Gal}(F/L)$ et $\mathrm{Gal}(L/K)$ sont résolubles, $\mathrm{Gal}(F/K)$ est résoluble.
La restriction à L d'un élément de $\mathrm{Gal}(F/M)$ est un automorphisme de L fixant le corps K car F/L est normale. De plus, si un élément de $\mathrm{Gal}(F/M)$ fixe L, alors il fixe F car F est engendrée par L et M, et c'est donc l'identité. Le morphisme de restriction est donc injectif, et $\mathrm{Gal}(F/M)$ s'identifie à un sous-groupe de $\mathrm{Gal}(L/K)$. En particulier, il est résoluble.
Si $|\mathrm{Gal}(F/M)| < |\mathrm{Gal}(L/K)|$, par hypothèse de récurrence, il existe une extension radicale R/F telle que R/M soit radicale. Comme M/K est radicale, R/K aussi.
Sinon, $\mathrm{Gal}(F/M)$ est $\mathrm{Gal}(L/K)$ sont isomorphes. Soit H' distingué dans $\mathrm{Gal}(F/M)$, maximal, d'indice p. Notons $E = F^H$. L'extension F/E est galoisienne, et comme H' est distingué, E/M aussi, de groupe de Galois H'. D'après le lemme 3.21, il existe $\alpha \in E$, dont le polynôme minimal est $X^p - a$, tel que $E = M(\alpha)$. Le degré de F sur E est strictement inférieur à n, et le groupe $\mathrm{Gal}(F/E)$ est résoluble. Donc il existe R/F avec R/M radicale (car α est racine de $X^p - a$ avec $a \in M$), et R est une extension de L. Comme M/K est radicale, R/K est radicale, et R remplit les conditions du théorème. □