Université de Strasbourg

Mémoire de première année
de Master de Mathématiques Fondamentales

Résolubilité par radicaux
Comparaison de deux moments historiques : Gauss et Galois

Victoria CALLET

Mémoire rédigé sous le direction de
Norbert SCHAPPACHER

Année 2018

Table des matières

1 Introduction

Résoudre une équation par radicaux, c'est à dire exprimer les solutions de cette équation en utilisant uniquement les quatre opérations élémentaires $+$, $-$, $\times$ et $\div$ et le symbole $\sqrt{}$, constitue un des thèmes majeurs de l'Algèbre. C'est un problème sur lequel les mathématiciens se sont penchés depuis longtemps et qui possède de nombreuses applications, comme par exemple pouvoir exprimer les racines d'un polynôme ou encore construire à la règle et au compas un polygone régulier.

Au cours du XVI$^{\text{ième}}$ siècle, deux mathématiciens italiens Jérôme Cardan (1501-1576) et Ludovico Ferrari (1522-1565) fournirent respectivement une méthode pour résoudre les équations du troisième degré (1545) et du quatrième degré (1540). Le mathématicien français Joseph Louis Lagrange (1736-1813) rédige en 1797 le "*Traité de la résolution des équations numériques de tous les degrés*" qui donne une méthode très générale de résolution des équations, mais elle se limite aux équations de degré strictement inférieur à cinq.

En 1801, le grand mathématicien allemand Carl Friedrich Gauss (1777-1855) publie les *Disquisitiones Arithmeticae*, dans lesquels il donne, entre autre, une méthode de résolution par radicaux d'une classe d'équations particulières : la classe des équations cyclotomiques.

En 1826, le mathématicien norvégien Niels Henrik Abel (1802-1829) démontre qu'"il n'existe pas de formule générale exprimant les solutions de l'équation du cinquième degré sous forme de radicaux", résultat connu aujourd'hui sous le nom de "Théorème d'Abel".

A la même période, le mathématicien français Evariste Galois (1811-1832) s'intéressa aussi au problème de la résolubilité par radicaux, en se posant la question suivante : quelles sont les équations qui sont résolubles par radicaux? Il rendit plusieurs mémoires à l'Académie des sciences dans lesquels il donne une condition nécessaire et suffisante pour qu'une équation soit résoluble par radicaux, mais ils furent perdus ou rejetés et aucun de ses travaux ne fut reconnu de son vivant. Il faut attendre 1846 pour que Joseph Liouville (1809-1882) publie les travaux de Galois.

Mon but dans ce mémoire est d'exposer et de comparer deux méthodes de résolubilité par radicaux : celle de Gauss et celle de Galois. Nous traiterons donc dans un premier temps la théorie de Gauss, basée sur des outils arithmétiques et certaines idées de Lagrange, puis nous exposerons la théorie de Galois, quant à elle basée sur une nouvelle vision de l'Algèbre, inspirée de Gauss et de Lagrange.

Pour réaliser ce travail, je me suis essentiellement appuyée sur l'œuvre de Jean-Pierre Tignol, "*Galois' Theory of Algebraic Equations*". Je remercie vivement Norbert Schappacher pour son soutien et ses conseils éclairés.

Portrait de Carl Friedrich Gauss (1777-1855) - Source : Wikipédia

Portrait d'Evariste Galois (1811-1832) - Source : Wikipédia

2 Théorie de Gauss et équation cyclotomique

2.1 Introduction et contexte historique

Gauss révolutionne ce qu'il appelle "la théorie de la division du cercle" lorsqu'il parvient, en 1796, à construire un polygone à dix-sept côtés en utilisant uniquement la règle et le compas. Pour cela, il résout par radicaux l'équation $\Phi_{17}(X) = 0$ (exemple qui sera traité dans la partie 2.4.3 page 13), où Φ_{17} est le polynôme cyclotomique de degré seize. Telle était donc sa motivation de trouver une solution au problème de résolubilité par radicaux d'une équation, et plus précisément les équations de la classe cyclotomique.

Au cours de ses recherches, Gauss montre que ce problème est en fait purement arithmétique : *"La théorie de la division du cercle, ou des polygones réguliers, qui compose la Section VII, n'appartient pas par elle-même à l'Arithmétique, mais ses principes ne peuvent être puisés que dans l'Arithmétique transcendante. Ce résultat pourra sembler aux géomètres, aussi inattendu que les vérités nouvelles qui en dérivent, et qu'ils verront, j'espère, avec plaisir."* (extrait de la préface des *Disquisitiones Arithmeticae* de 1801). Il explique en quoi la théorie de la division du cercle revient à trouver une méthode pour exprimer les solutions de l'équation cyclotomique $\Phi_n(X) = 0$, où n est un entier naturel. Gauss se penche d'abord sur le cas de la section en un nombre premier de parties, en assurant que l'on pourra ensuite en déduire le cas général. Il considère donc l'équation $\Phi_p(X) = 0$ avec p un nombre premier. C'est ce cas que nous allons étudier dans ce premier chapitre.

Nous allons dans un premier temps effectuer des rappels de théorie des nombres, et introduire notamment la notion de **racine primitive modulo un nombre premier** p qui sera au cœur de la théorie de Gauss. Ensuite, nous démontrerons que le polynôme cyclotomique Φ_p est irréductible. Ces deux premières parties serviront à définir l'outil arithmétique fondamental créé par Gauss, **les périodes**, et nous montrerons comment utiliser cet outil sur deux exemples. Enfin, nous parlerons de résolubilité par radicaux pour les équations qui déterminent ces périodes.

Dans tout ce qui suit, p désignera un nombre premier.

2.2 Un peu de théorie des nombres

Le but de cette partie va être de démontrer en utilisant des outils arithmétiques que l'ensemble des restes non nuls dans la divisions euclidiennes par p est engendré par un seul élément. En d'autres termes, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. Pour énoncer ce résultat, nous aurons besoin de la notion suivante :

Définition : Soient p un nombre premier et $g \in \mathbb{Z}$. On dit que g est une **racine primitive modulo** p si

$$g^{p-1} \equiv 1 \mod p \text{ et } g^i \not\equiv 1 \mod p \text{ pour } i = 1, ..., p-2.$$

Exemple : 2 est une racine primitive de 11.

Proposition 2.2.1. ***Caractérisation des racines primitives***
Soient p un nombre premier et g un entier quelconque. Les deux propositions suivantes sont équivalentes :

i) $g^{p-1} \equiv 1 \mod p$ *et* $g^i \not\equiv 1 \mod p$ *pour* $i = 1, ..., p-2$.
ii) les puissances $g^0, g^1, ..., g^{p-2}$ *sont congrues à* $1, 2, ..., p-1$ *modulo* p *(pas nécessairement dans cet ordre).*

Pour démontrer cette proposition, nous avons besoin de ce qu'on appelle le Petit théorème de Fermat, ainsi que d'un lemme (qui n'est autre qu'une reformulation de la proposition 30 du livre VII des Éléments d'Euclide disant que *si deux nombres se multipliant l'un l'autre produisent un certain nombre et si un certain nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux*). Avant de passer à la démonstration, illustrons cette caractérisation à l'aide d'un exemple concret : pour cela, reprenons l'exemple de 2 qui est une racine primitive de 11. Nous avons alors les relations suivantes :

$$2^0 \equiv 1 \mod 11;\quad 2^1 \equiv 2 \mod 11;\quad 2^2 \equiv 4 \mod 11;\quad 2^3 \equiv 8 \mod 11;\quad 2^4 \equiv 5 \mod 11;$$
$$2^5 \equiv 10 \mod 11;\quad 2^6 \equiv 9 \mod 11;\quad 2^7 \equiv 7 \mod 11;\quad 2^8 \equiv 3 \mod 11;\quad 2^9 \equiv 6 \mod 11;$$

Lemme 2.2.2. *Soient a et b deux entiers et p un nombre premier. Si $ab \equiv 0 \mod p$ alors $a \equiv 0 \mod p$ ou $b \equiv 0 \mod p$.*

Démonstration. Supposons que $ab \equiv 0 \mod p$ et que $a \not\equiv 0 \mod p$ (la preuve est symétrique en prenant $b \not\equiv 0 \mod p$). Ceci implique que a et p sont premiers entre eux, et l'identité de Bezout nous assure l'existence de deux entiers u et v tels que $au+pv = 1$. Alors, on a $bau+bpv = b$ et par hypothèse, il existe un entier e tel que $ab = pe$, d'où $peu + pbv = b$, et donc p divise b. □

Proposition 2.2.3. *(dite Petit théorème de Fermat) Soient a un entier et p un nombre premier. Si $a \not\equiv 0 \mod p$ alors $a^{p-1} \equiv 1 \mod p$.*

Démonstration. Remarquons dans un premier temps que

$$a^p \equiv a \mod p \qquad \Leftrightarrow \qquad a(a^{p-1} - 1) \equiv 0 \mod p$$

ce qui est équivalent, par hypothèse et d'après le lemme précédent à

$$a^{p-1} \equiv 1 \mod p.$$

Montrons donc par récurrence sur $a \in \mathbb{N}$ que $a^p \equiv a \mod p$. Le cas a=0 étant trivial, supposons que $a^p \equiv a \mod p$ pour un entier a fixé. On remarque que tous les coefficients binomiaux, exceptés le premier et le dernier, sont divisibles par p car ce dernier est premier, d'où

$$(a+1)^p \equiv a^p + 1 \mod p$$

et par hypothèse de récurrence,

$$a^p + 1 \equiv a + 1 \mod p$$

ce qui donne le résultat. □

Nous pouvons maintenant démontrer l'équivalence donnée par la proposition 2.2.1 :

Démonstration. $\underline{i) \Rightarrow ii)}$: Si $g^{p-1} \equiv 1 \mod p$, alors on a que $g \not\equiv 0 \mod p$. Ceci implique par le lemme 2.2.2 (page 4) que les restes dans la division euclidienne des puissances $g^0, g^1, ..., g^{p-2}$ par p sont dans l'ensemble $\{1, 2, ..., p-1\}$. Il reste donc à montrer que les puissances de g sont distinctes deux à deux modulo p.

Par l'absurde, supposons que $g^i \equiv g^j \mod p$ pour i et j dans $\{0, 1..., p-2\}$ tels que $i < j$. Alors on a

$$g^i(1 - g^{j-i}) \equiv 0 \mod p$$

ce qui implique par le lemme 2.2.2

$$g^{j-i} \equiv 1 \mod p.$$

Or i et j sont tels que $j - i \in \{0, 1, ..., p-2\}$, d'où la contradiction avec l'hypothèse donnée par i).

$\underline{ii) \Rightarrow i)}$: Par hypothèse, on a en particulier que $g \not\equiv 0 \mod p$, donc d'après le Petit théorème de Fermat,

$$g^{p-1} \equiv 1 \mod p$$

De plus, la condition donnée par ii) implique que $g^i \not\equiv g^0 \mod p$ *pour* $i = 1, 2, ..., p-2$, ce qui donne la conclusion. □

Définition : Soit a un entier relatif premier avec p. On appelle **ordre de a modulo p** le plus petit entier $e > 0$ tel que $a^e \equiv 1 \mod p$.

Lemme 2.2.4. *Supposons que a soit premier avec p, alors $a^m \equiv 1 \mod p$ si et seulement si e divise m. En particulier, e divise $p-1$.*

Démonstration. La réciproque est immédiate, tandis que le sens direct utilise simplement l'identité de Bezout sur e, m et leur pgcd. □

Lemme 2.2.5. *Soient q et p deux nombres premiers et m un entier quelconque. Si q^m divise $p-1$, alors il existe un entier d'ordre q^m modulo p.*

Démonstration. Soit l'équation modulo p

$$X^{\frac{p-1}{q}} \equiv 1 \mod p.$$

Comme p est premier, cette équation admet au maximum $\frac{p-1}{q}$ solutions modulo p. Soit x un entier qui n'est pas racine de l'équation et posons $a = x^{\frac{p-1}{q^m}}$. D'après le petit théorème de Fermat, nous avons que $x^{p-1} \equiv 1 \mod p$, d'où $x^{\frac{p-1}{q}} = a^{q^m} \equiv 1 \mod p$. Alors, d'après le lemme précédent l'ordre de a modulo p divise q^m, et comme $a^{q^{m-1}} \not\equiv 1 \mod p$, nous avons aussi que l'ordre de a ne divise pas q^{m-1}. Enfin, comme q est premier, le seul entier qui divise q^m sans diviser q^{m-1} est q^m lui-même. L'ordre de a modulo p est donc bien q^m. □

Nous avons maintenant les outils nécessaires pour énoncer et démontrer le théorème suivant, qui est le point clé de cette première partie et qui joue un rôle essentiel dans les travaux de Gauss concernant le polynôme cyclotomique.

Théorème 2.2.6. *Pour tout nombre p premier, il existe g une racine primitive modulo p.*

Démonstration. On commence par décomposer $p-1$ en produit de facteurs premiers :

$$p-1 = q_1^{m_1} q_2^{m_2} ... q_r^{m_r}$$

Alors d'après le lemme 2.2.5, pour tout $i \in 1, ..., r$, il existe un entier a_i d'ordre $q_i^{m_i}$. Montrons dans ce cas que, pour $i = 1, ..., r$, le produit des a_i est bien d'ordre $p-1$. D'abord, posons e l'ordre du produit des a_i modulo p et remarquons que, d'après le lemme 2.2.4, il divise $p-1$. Supposons maintenant par l'absurde que $e \neq p-1$, donc e divise le produit des $q_i^{m_i}$ et comme $e < p-1$, il existe un i tel que e divise $\frac{p-1}{q_i}$. Quitte à renuméroter, on peut prendre $q_i = q_1$. De plus, d'après le lemme 2.2.4,

$$(\prod_{i=1}^{r} a_i)^{\frac{p-1}{q_1}} \equiv 1 \mod p \tag{1}$$

De même, $q_i^{m_i}$ divise $\frac{p-1}{q_1}$ et donc

$$a_i^{\frac{p-1}{q_1}} \equiv 1 \mod p \quad \forall i \in 2, ..., r \tag{2}$$

Alors, en combinant les lignes (1) et (2), nous avons

$$a_1^{\frac{p-1}{q_1}} \equiv 1 \mod p.$$

Enfin, comme $q_1^{m_1}$ est l'ordre de a_1 modulo p, $q_1^{m_1}$ divise $\frac{p-1}{q_1}$ et donc $q_1^{m_1+1}$ divise $p-1$, ce qui est en contradiction avec la décomposition en produit de facteurs premiers de $p-1$. □

Ce résultat permet de conclure, par la caractérisation des racines primitives modulo p, que l'ensemble de restes non nuls dans la division euclidienne par p est en fait engendré par un seul élément g. Autrement dit, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et engendré par une racine primitive modulo p.

2.3 Le polynôme cyclotomique d'indice premier est irréductible

Définition : Soit p un nombre premier. On appelle **polynôme cyclotomique d'indice** p le polynôme noté Φ_p défini par

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X^2 + X + 1.$$

Théorème 2.3.1. *Quelque soit p un nombre premier, le polynôme cyclotomique d'indice p est irréductible.*

Ce théorème a été démontré une première fois par Gauss dans les *"Disquisitiones Arithmeticae"*, puis redémontré en utilisant le théorème suivant, appelé **Critère d'Eisenstein** que nous devons au mathématicien Ferdinand Gotthold Max Eisenstein (1823-1852) :

Critère d'Eisenstein : *Soit P un polynôme à coefficients entiers, noté*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0.$$

Supposons qu'il existe un nombre premier p tel que :

$$\begin{array}{c} \textit{pour } i = 0, ..., n, \ p \textit{ divise } a_i \\ p \textit{ ne divise pas } a_n \\ p^2 \textit{ ne divise pas } a_0 \end{array}$$

Alors, P est irréductible sur $\mathbb{Q}$.

En utilisant ce critère, démontrons que le polynôme cyclotomique d'indice premier est irréductible :

Démonstration. En substituant $X+1$ à X dans la définition de Φ_p, nous avons

$$\begin{aligned} \Phi_p(X+1) &= \frac{(X+1)^p - 1}{(X+1) - 1} \\ &= \frac{X^p + pX^{p-1} + \binom{p}{p-2} X^{p-2} + ... + \binom{p}{2} X^2 + X}{X} \\ &= X^{p-1} + pX^{p-2} + \binom{p}{p-2} X^{p-3} + ... + \binom{p}{2} X + p \end{aligned}$$

Il suffit maintenant d'appliquer le critère d'Eisenstein avec p, ce qui donne que $\Phi_p(X+1)$ est irréductible sur $\mathbb{Q}$. Comme $P(X) \in \mathbb{Q}[X]$ irréductible si et seulement si pour tout $\alpha \in \mathbb{Q}$, $P(X+\alpha)$ est irréductible, nous avons bien l'irréductibilité de $\Phi_p(X)$ sur $\mathbb{Q}$. □

Remarque : La dernière équivalence qu'utilise la démonstration est évidente : en effet, si $P \in \mathbb{Q}[X]$ est irréductible, on peut supposer par l'absurde que $P(X+\alpha) = A(X)B(X)$, pour un $\alpha \in \mathbb{Q}$ et où A et B sont des polynômes à coefficients dans $\mathbb{Q}$. Puis on évalue en $X - \alpha$, ce qui revient à

$$P(X) = A(X-\alpha)B(X-\alpha)$$

et comme P est irréductible, on en déduit que soit A soit B est constant d'où le résultat. La réciproque est triviale puisqu'il suffit de choisir $\alpha = 0$.

Grâce à ce résultat et aux rappels d'arithmétiques de la première partie, nous sommes en mesure d'introduire la notion de période qui se trouve au cœur de la théorie de Gauss.

2.4 Les périodes de Gauss

Les périodes constituent l'outil fondamental qui permet à Gauss de résoudre par radicaux les équations cyclotomiques.

2.4.1 Définitions et premières propriétés

Définitions : Soit ζ un nombre complexe et n un entier naturel non nul. On dit que ζ est une **racine $n^{\text{ième}}$ de l'unité** si $\zeta^n = 1$ et on appelle **ordre de** ζ le plus petit entier e tel que $\zeta^e = 1$.

Les lemmes 2.2.4 et 2.2.5 (page 4) s'appliquent aussi à cette définition. En particulier,

$$\zeta^m = 1 \quad \Leftrightarrow \quad e \text{ divise m.}$$

Dans tout ce qui suit, nous nous intéresserons uniquement au cas où $n = p$ avec p un nombre premier. Par ce qui précède, p est l'ordre de ζ. Les racines $p^{\text{ièmes}}$ de l'unité différentes de 1 sont alors appelées **racines primitives $p^{\text{ième}}$ de l'unité**. D'autre part, si ζ est une racine $p^{\text{ième}}$ de l'unité différente de 1, alors chaque autre racine $p^{\text{ième}}$ de l'unité est en fait une puissance de ζ. Notons μ_p

l'ensemble de ces racines auquel on a ajouté 1 (qui n'est évidemment pas une racine primitive $p^{\text{ième}}$) afin d'obtenir une structure de groupe, d'où :

$$\mu_p = \{1, \zeta, \zeta^2, ..., \zeta^{p-1}\}.$$

On peut remarquer que μ_p constitue l'ensemble des racines du polynômes cyclotomique Φ_p, et qu'il est engendré par ζ.

Lemme 2.4.1. *Soit ζ une racine primitive $p^{\text{ième}}$ de l'unité. Si m et n sont deux entiers tels que $m \equiv n \mod p$, alors $\zeta^m = \zeta^n$.*

Démonstration. Par hypothèse, $\exists k \in \mathbb{Z}$ tel que $m = kp + n$. Alors, $\zeta^m = \zeta^{kp+n} = \zeta^{pk}\zeta^n = \zeta^n$. □

Théorème 2.4.2. *Soient g une racine primitive modulo p et ζ une racine primitive $p^{\text{ième}}$ de l'unité. Alors, les $\zeta^{g^0}, \zeta^{g^1}, ..., \zeta^{g^{p-2}}$ sont tous distincts et égaux aux $\zeta, \zeta^2, ..., \zeta^{p-1}$ dans un certain ordre.*

Démonstration. La preuve résulte directement du théorème 2.2.6 (page 5) et du lemme précédent. □

Ce résultat permet entre autre de décrire l'ensemble des racines primitives $p^{\text{ièmes}}$ de l'unité comme suit :

$$\mu_p = \{1, \zeta_0, \zeta_1, ..., \zeta_{p-2}\} \text{ avec } \zeta_i = \zeta^{g^i} \text{ pour } i = 0, ..., p-2.$$

De plus, on appelle **permutation cyclique** l'automorphisme de μ_p défini par

$$\sigma(\zeta_i) = \zeta_{i+1} = \zeta_i^g \text{ pour } i = 0, ..., p-3$$

$$\Leftrightarrow \sigma : \zeta_0 \mapsto \zeta_1 \mapsto ... \mapsto \zeta_{p-2} \mapsto \zeta_0 \text{ et } \sigma(1) = 1.$$

Notons que cette permutation dépend du choix de g. Enfin, comme σ est un automorphisme il est en particulier multiplicatif, donc nous avons

$$\forall \rho, \omega \in \mu_p,\ \sigma(\rho\omega) = \sigma(\rho)\sigma(\omega).$$

En effet, pour tout $\rho \in \mu_p$ on a $\sigma(\rho) = \rho^g$ et comme $\rho\omega \in \mu_p$, $\sigma(\rho\omega) = (\rho\omega)^g = \rho^g\omega^g = \sigma(\rho)\sigma(\omega)$.

Définition : Soient e et f deux entiers positifs tels que $ef = p - 1$. On définit e nombres complexes par les relations suivantes :

$$\eta_0 = \zeta_0 + \zeta_e + \zeta_{2e} + ... + \zeta_{e(f-1)},$$
$$\eta_1 = \zeta_1 + \zeta_{e+1} + \zeta_{2e+1} + ... + \zeta_{e(f-1)+1},$$
$$\eta_2 = \zeta_2 + \zeta_{e+2} + \zeta_{2e+2} + ... + \zeta_{e(f-1)+2},$$
$$...$$
$$\eta_{e-1} = \zeta_{e-1} + \zeta_{2e-1} + \zeta_{3e-1} + ... + \zeta_{p-2}.$$

On appelle $\eta_0, ..., \eta_{e-1}$ les e **périodes de f termes**.

En particulier, les périodes de un terme sont les racines primitives $p^{\text{ième}}$ de l'unité $\zeta_0, \zeta_1, ..., \zeta_{p-2}$, et l'unique période de $p-1$ termes correspond à la somme de toutes les racines primitives $p^{\text{ièmes}}$ de l'unité différentes de 1, autrement dit la somme de toutes les racines de Φ_p (qui vaut en fait -1).

Illustrons cette notion à l'aide d'un exemple : reprenons $p = 11$ et $g = 2$, et choisissons $\zeta = e^{\frac{2i\pi}{11}}$. Alors, $\zeta^k = e^{\frac{2ik\pi}{11}}$ pour $k = 1, 2, ..., 10$ et $\zeta^0 = 1$. Nous avons dans un premier temps les relations suivantes :

$$\zeta_0 = \zeta^1 ; \quad \zeta_1 = \zeta^2 ; \quad \zeta_2 = \zeta^4 ; \quad \zeta_3 = \zeta^8 ; \quad \zeta_4 = \zeta^5 ;$$
$$\zeta_5 = \zeta^{10} ; \quad \zeta_6 = \zeta^9 ; \quad \zeta_7 = \zeta^7 ; \quad \zeta_8 = \zeta^3 ; \quad \zeta_9 = \zeta^6 ;$$

Si l'on veut par exemple les périodes de 2 termes, puisque $p = 11$ nous aurons $e = 5$ nombres complexes. Alors, compte tenu des choix que nous avons faits pour g et ζ, nous avons :

$$\eta_0 := \zeta_0 + \zeta_5 = 2\cos\frac{2\pi}{11} \qquad \eta_1 := \zeta_1 + \zeta_6 = 2\cos\frac{4\pi}{11}$$

$$\eta_2 := \zeta_2 + \zeta_7 = 2\cos\frac{8\pi}{11} \qquad \eta_3 := \zeta_3 + \zeta_8 = 2\cos\frac{6\pi}{11}$$

$$\eta_4 := \zeta_4 + \zeta_9 = 2\cos\frac{10\pi}{11}$$

Nous avons donc en tout cinq périodes de deux termes qui sont les $2\cos\frac{2k\pi}{11}$, pour $k = 1, ..., 5$.

De plus, la permutation cyclique σ permet d'introduire une nouvelle permutation telle que :

$$\eta_0 \mapsto \eta_1 \mapsto \eta_2 \mapsto \eta_3 \mapsto \eta_4 \mapsto \eta_0.$$

Nous pouvons maintenant généraliser au cas où $p \geq 3$: on a $\frac{p-1}{2}$ périodes de deux termes qui sont par définition les

$$\eta_j = \zeta_j + \zeta_{j+\frac{p-1}{2}}$$

avec $j = 0, ..., \frac{p-1}{2} - 1$. De plus, par définition des ζ_i, nous avons

$$\zeta_{j+\frac{p-1}{2}} = \zeta_j^{g^{\frac{p-1}{2}}}.$$

Or, $g^{\frac{p-1}{2}}$ est racine de l'équation modulo p

$$X^2 \equiv 1 \mod p$$

qui n'admet que deux solutions, ± 1. Mais comme g est une racine primitive modulo p, aucune puissance de g inférieure à $p-1$ n'est congrue à 1 modulo p, d'où

$$g^{\frac{p-1}{2}} \equiv -1 \mod p.$$

Finalement, les périodes de deux termes s'écrivent

$$\eta_j = \zeta_j + \zeta_j^{-1}.$$

Voici les deux propriétés sur les périodes dont nous nous servirons par la suite :

Première propriété : Toute période de f termes peut s'exprimer comme $\mathbb{Q}$-combinaison linéaire de n'importe quelle autre période de même nombre de termes.

Deuxième propriété : Si f et f' sont deux diviseurs de $p-1$ tels que f divise f', alors toute période de f termes est racine d'un polynôme de degré f'/f dont les coefficients sont des expressions rationnelles de périodes de f' termes.

Nous démontrerons ces propriétés après avoir introduit les notions de la partie suivante.

2.4.2 Les sous-corps $\mathbb{Q}(\mu_p)$ et K_f

On pose $\mathbb{Q}(\mu_p)$ le sous-ensemble des nombres complexes qui sont des expressions rationnelles des éléments de μ_p, défini par

$$\mathbb{Q}(\mu_p) = \Big\{ \frac{f(\zeta)}{g(\zeta)} \mid f, g \in \mathbb{Q}[X] \text{ et } g(\zeta) \neq 0 \Big\}.$$

En particulier, $\mathbb{Q}(\mu_p)$ est un sous-corps de $\mathbb{C}$, et nous avons le théorème suivant :

Théorème 2.4.3. *Tout élément de $\mathbb{Q}(\mu_p)$ peut s'écrire sous la forme d'une unique $\mathbb{Q}$-combinaison linéaire de $p^{\text{ièmes}}$ racines de l'unité différentes de 1. Autrement dit, pour tout a élément de $\mathbb{Q}(\mu_p)$, il existe des uniques $a_i \in \mathbb{Q}$ tels que :*

$$a = a_1\zeta + a_2\zeta^2 + ... + a_{p-1}\zeta^{p-1}.$$

Pour démontrer ce théorème, nous avons besoin du lemme suivant :

Lemme 2.4.4. *Soient P et Q deux polynômes à coefficients dans un corps F, et supposons que P est irréductible sur $F[X]$. Si P et Q ont une racine en commun dans un corps K qui contient F, alors P divise Q.*

Démonstration. Supposons par l'absurde que P ne divise pas Q. Alors, comme P est irréductible sur $F[X]$, P et Q sont premiers entre eux et on peut appliquer l'identité de Bezout, donc il existe U et V deux polynômes de $F[X]$ tels que :

$$P(X)U(X) + Q(X)V(X) = 1.$$

Puis, substituant a à X, avec a la racine commune à P et Q, nous avons

$$P(a)U(a) + Q(a)V(a) = 1,$$

et comme $P(a) = Q(a) = 0$, on trouve $0 = 1$, d'où la contradiction. □

Démontrons maintenant le théorème 2.4.3 :

Démonstration. Soit $\frac{f(\zeta)}{g(\zeta)}$ un élément de $\mathbb{Q}(\mu_p)$. Nous savons que ζ est racine du polynôme Φ_p qui est irréductible sur $\mathbb{Q}$ par le théorème 2.3.1 (page 5). Alors, comme $g(\zeta) \neq 0$, le polynôme g n'est pas divisible par Φ_p et g et Φ_p sont premiers entre eux. Alors, d'après l'identité de Bezout, il existe U et V dans $\mathbb{Q}[X]$ tels que

$$g(X)U(X) + \Phi_p(X)V(X) = 1.$$

Substituant ζ à X, nous avons

$$g(\zeta)U(\zeta) = 1.$$

Alors, on peut écrire

$$\frac{f(\zeta)}{g(\zeta)} = f(\zeta)U(\zeta).$$

Considérons maintenant $R \in \mathbb{Q}[X]$ le reste dans la division euclidienne de fU par Φ_p, nous avons

$$fU = \Phi_p Q + R \text{ avec } \deg R \leq p-1 \text{ et } Q \in \mathbb{Q}[X].$$

Et comme $\Phi_p(\zeta) = 0$, nous avons

$$f(\zeta)U(\zeta) = R(\zeta) \Leftrightarrow \frac{f(\zeta)}{g(\zeta)} = R(\zeta),$$

donc finalement tout élément $\frac{f(\zeta)}{g(\zeta)} \in \mathbb{Q}(\mu_p)$ peut s'écrire comme expression rationnelle du type

$$a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1}.$$

Pour prouver l'unicité, supposons qu'il existe $a_0, ..., a_{p-1}$ et $b_0, ..., b_{p-1}$ dans $\mathbb{Q}$ tels que

$$a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1} = b_0 + b_1\zeta + ... + b_{p-1}\zeta^{p-1}.$$

Alors, ζ est racine du polynôme

$$h(X) = (a_0 - b_0) + (a_1 - b_1)X + ... + (a_{p-1} - b_{p-1})X^{p-1} \in \mathbb{Q}[X],$$

et d'après le lemme précédent, nous avons que Φ_p divise h, mais comme $\deg h \leq p-1$ et que $\deg \Phi_p = p-1$, c'est impossible à moins que $h \equiv 0$. Ainsi,

$$a_0 - b_0 = a_1 - b_1 = ... = a_{p-1} - b_{p-1} = 0.$$

□

Dans la première partie, nous avions introduit la permutation cyclique σ, et nous allons maintenant voir qu'il est possible de l'étendre à $\mathbb{Q}(\mu_p)$:

Proposition 2.4.5. *La permutation cyclique σ s'étend en un automorphisme de $\mathbb{Q}(\mu_p)$ par $\mathbb{Q}$-linéarité. De plus, cet automorphisme laisse $\mathbb{Q}$ invariant.*

Lemme 2.4.6. *Le seul automorphisme de $\mathbb{Q}$ est l'identité.*

Démonstration. En effet, si φ est un automorphisme de $\mathbb{Q}$, alors par définition on aura $\varphi(1) = 1$, donc par récurrence $\varphi(n) = n$, $\forall n \in \mathbb{N}$. De plus $\varphi(-1) = -1$ (car $\varphi(-1)^2 = 1$) et donc on a directement, par multiplication par -1, que $\varphi(z) = z$, $\forall z \in \mathbb{Z}$. Enfin, on a

$$\varphi(\tfrac{a}{b}) = \varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = ab^{-1} = \tfrac{a}{b},\ \forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z}^*.$$

D'où $\varphi = id_{\mathbb{Q}}$. □

Démontrons maintenant la proposition 2.4.5 :

Démonstration. Montrons que σ est un morphisme de $\mathbb{Q}(\mu_p)$, ie : $\sigma(ab) = \sigma(a)\sigma(b)$, $\forall a, b \in \mathbb{Q}(\mu_p)$. Les éléments de μ_p privé de l'élément neutre forment une base de $\mathbb{Q}(\mu_p)$, donc on peut écrire

$$a = \textstyle\sum_{i=0}^{p-2} a_i\zeta_i \text{ et } b = \sum_{j=0}^{p-2} b_j\zeta_j.$$

De plus, par définition de la permutation cyclique sur $\mathbb{Q}(\mu_p)$, σ est $\mathbb{Q}$-linéaire, d'où :

$$\sigma(ab) = \sum_{i,j=0}^{p-2} a_i b_j \sigma(\zeta_i\zeta_j)$$

et

$$\sigma(a)\sigma(b) = \sum_{i,j=0}^{p-2} a_i b_j \sigma(\zeta_i)\sigma(\zeta_j).$$

Comme $\sigma(\rho\omega) = \sigma(\rho)\sigma(\omega)$ $\forall \rho, \omega \in \mu_p$, on a finalement $\sigma(ab) = \sigma(a)\sigma(b)$ $\forall a, b \in \mathbb{Q}(\mu_p)$. De plus, σ est un automorphisme d'espace vectoriel de dimension fini qui transforme une base en une autre base, il est donc bijectif. C'est donc bien un automorphisme de $\mathbb{Q}(\mu_p)$, et par le lemme précédent, il fixe $\mathbb{Q}$. □

Dans ce qui suit, on pose e et f deux entiers positifs tels que $ef = p - 1$ et on note K_f l'ensemble des éléments de $\mathbb{Q}(\mu_p)$ qui s'écrivent comme une unique $\mathbb{Q}$-combinaison linéaire des e périodes de f termes.

Proposition 2.4.7. *Un élément de $\mathbb{Q}(\mu_p)$ est dans K_f si et seulement si il est fixé par l'automorphisme σ^e.*

Démonstration. Sens direct : Soit $a \in \mathbb{Q}(\mu_p)$ tel que a soit combinaison linéaire des e périodes de f termes :

$$a = a_0\eta_0 + a_1\eta_1 + ... + a_{e-1}\eta_{e-1},$$

avec $a_i \in \mathbb{Q}$ et où chaque η_i est une des e période de f termes. Alors, en appliquant σ^e à cette égalité, on a

$$\sigma^e(a) = a_0\sigma^e(\eta_0) + a_1\sigma^e(\eta_1) + ... + a_{e-1}\sigma^e(\eta_{e-1}).$$

Soit $\eta_i \in \{\eta_0, ..., \eta_{e-1}\}$. Par définition, on a, pour ζ une racine primitive $p^{\text{ième}}$ de l'unité,

$$\eta_i = \zeta_i + \zeta_{e+i} + \zeta_{2e+i} + ... + \zeta_{e(f-1)+i}.$$

Alors, à nouveau en appliquant σ^e à cette égalité, on a, par définition de σ^e :

$$\begin{aligned}\sigma^e(\eta_i) &= \sigma^e(\zeta_i) + \sigma^e(\zeta_{e+i}) + ... + \sigma^e(\zeta_{e(f-1)+i}) \\ &= \zeta_{e+i} + \zeta_{2e+i} + ... + \zeta_i \\ &= \eta_i.\end{aligned}$$

D'où finalement $\sigma^e(a) = a$.

Réciproque : Soit $a \in \mathbb{Q}(\mu_p)$ et supposons que $\sigma^e(a) = a$. On réécrit la décomposition donnée par le théorème 2.4.3 (page 9)comme suit :

$$\begin{aligned} a = & a_0\zeta_0 + a_1\zeta_1 + ... + a_{e-1}\zeta_{e-1} \\ & + a_e\zeta_e + a_{e+1}\zeta_{e+1} + ... + a_{2e-1}\zeta_{2e-1} \\ & + ... \\ & + a_{e(f-1)}\zeta_{e(f-1)} + a_{e(f-1)+1}\zeta_{e(f-1)+1} + ... + a_{p-2}\zeta_{p-2}. \end{aligned}$$

Ensuite, par définition de σ, $\sigma^e(\zeta) = \zeta_e \ \forall \zeta \in \mu_p$, et comme σ est $\mathbb{Q}$-linéaire, nous avons :

$$\begin{aligned} \sigma^e(a) = & a_0\zeta_e + a_1\zeta_e + 1 + ... + a_{e-1}\zeta_{2e-1} \\ & + a_e\zeta_{2e} + a_{e+1}\zeta_{2e+1} + ... + a_{2e-1}\zeta_{3e-1} \\ & + ... \\ & + a_{e(f-1)}\zeta_{ef} + a_{e(f-1)+1}\zeta_{ef+1}. \end{aligned}$$

Puis, par hypothèse, $\sigma^e(a) = a$ et en utilisant à nouveau le théorème 2.4.3, nous avons

$$a_0 = a_e = a_{2e} = ... = a_{e(f-1)},$$

$$a_1 = a_{e+1} = a_{2e+1} = ... = a_{e(f-1)+1},$$

$$...$$

$$a_{e-1} = a_{2e-1} = a_{3e-1} = ... = a_{p-2}.$$

On obtient alors que tout élément a invariant sous σ^e peut s'écrire comme suit :

$$a = a_0(\zeta_0 + \zeta_e + ... + \zeta_{e(f-1)}) + a_1(\zeta_1 + \zeta_{e+1} + ... + \zeta_{e(f-1)+1}) + ... + a_{e-1}(\zeta_{e-1} + \zeta_{2e-1} + ... + \zeta_{p-2}).$$

Enfin, par définition des e périodes η_i de f termes,

$$a = a_0\eta_0 + a_1\eta_1 + ... + a_{e-1}\eta_{e-1}.$$

De plus, l'unicité de cette écriture est donnée par l'unicité de la décomposition du théorème 2.4.3. □

On a montré à travers cette proposition que σ^e fixe toute combinaison linéaire des e périodes de f termes. Ainsi, on peut, en langage plus moderne, noter que K_f est le corps fixé par l'automorphisme σ^e, d'où

$$K_f = \{a \in \mathbb{Q}(\mu_p) \mid \sigma^e(a) = a\},$$

et c'est cette définition qu'on privilégiera par la suite.

Corollaire 2.4.8. *Soit η une période de f termes. Tout élément de K_f peut s'écrire comme combinaison linéaire des puissances de η et de coefficients rationnels, ie :*

$$\forall a \in K_f, \ \exists a_0, ..., a_{e-1} \in \mathbb{Q} \text{ tels que } a = a_0 + a_1\eta + a_2\eta^2 + ... + a_{e-1}\eta^{e-1}.$$

Démonstration. K_f est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$: on peut donc le voir comme un $\mathbb{Q}$-espace vectoriel. De plus, d'après la proposition précédente, on a $\dim_{\mathbb{Q}} K_f = e$. La preuve consiste donc à montrer que l'ensemble $\{1, \eta, ..., \eta^{e-1}\}$ forme une famille libre de K_f sur $\mathbb{Q}$. Pour cela, supposons qu'il existe $a_0, ..., a_{e-1} \in \mathbb{Q}$ tels que

$$a_0 + a_1\eta + ... + a_{e-1}\eta^{e-1} = 0.$$

Alors, η est racine du polynôme

$$P(X) = a_0 + a_1X + ... + a_{e-1}X^{e-1}.$$

On remarque que $\sigma(\eta)$,$\sigma^2(\eta)$,...$\sigma^{e-1}(\eta)$ sont aussi racines du polynômes P, puisque la permutation cyclique σ fixe $\mathbb{Q}$. On sait de plus que les $\eta, \sigma(\eta), ..., \sigma^{e-1}(\eta)$ sont les e périodes de f termes, qui sont toutes distinctes d'après la proposition 2.4.7. Mais le polynôme P étant de degré $e-1$, il ne peut pas avoir e racines, ce qui implique que $P \equiv 0$, et donc que

$$a_0 = ... = a_{e-1} = 0,$$

ce qui prouve l'indépendance linéaire des $1, \eta, ..., \eta^{e-1}$. L'ensemble $\{1, \eta, ..., \eta^{e-1}\}$ forme donc bien une base de K_f. □

Corollaire 2.4.9. *Si η et η' sont des périodes de f termes, alors il existe $a_0, ..., a_{e-1} \in \mathbb{Q}$ tels que*

$$\eta' = a_0 + a_1\eta + ... + a_{e-1}\eta^{e-1}.$$

Démonstration. C'est immédiat : il suffit de remarquer que si η' est une période de f termes, alors $\eta' \in K_f$ et donc on peut appliquer la proposition précédente. □

Remarquons que ce corollaire prouve la première propriété que nous avons énoncée sur les périodes. Pour prouver la seconde, nous avons besoin d'introduire f' et h, deux entiers positifs tels que $hf' = p-1$. Supposons que f divise f' : alors, comme $ef = p-1$, h divise e et nous avons le lemme suivant :

Lemme 2.4.10. *Soient f, f', e et h des entiers positifs tels que $ef = hf' = p-1$. Alors, f divise f' si et seulement si $K_{f'} \subset K_f$.*

Démonstration. Sens direct : On rappelle qu'avec les notations $hf' = p-1$, on a $K_{f'} = \{a \in \mathbb{Q} \mid \sigma^h(a) = a\}$. De plus, si $a \in K_{f'}$, alors

$$\sigma^e(a) = (\sigma^h)^{e/h}(a), \text{ et donc par hypothèse } \sigma^e(a) = a.$$

Ainsi tout élément invariant par σ^h est aussi invariant par σ^e, d'où $K_{f'} \subset K_f$.

Réciproque : On suppose que $K_{f'}$ est inclus dans K_f. Alors, nous avons

$$\sigma^h(a) = a \Rightarrow \sigma^e(a) = a,$$

donc h divise e, et comme $fe = f'h$, f divise f'. □

Proposition 2.4.11. *Soient f et f' deux diviseurs de $p-1$. Si f divise f', alors tout élément de K_f est racine d'un polynôme de degré f'/f à coefficients dans $K_{f'}$.*

Démonstration. Soit $a \in K_f$. On pose $k = f'/f = e/h$, et on considère le polynôme suivant :

$$P(X) = (X-a)(X-\sigma^h(a))(X-\sigma^{2h}(a))...(X-\sigma^{h(k-1)}(a)).$$

P est bien de degré $k = f'/f$, il reste à montrer que ses coefficients sont dans $K_{f'}$: ce sont les produits des $a, \sigma^h(a), ..., \sigma^{h(k-1)}$. De plus, nous avons

$$\sigma^h(a) = \sigma^h(a),\ \sigma^h(\sigma^h(a)) = \sigma^{2h}(a),\ ...,\sigma^h(\sigma^{h(k-1)}(a)) = \sigma^e(a) = a,$$

donc σ^h permute les racines $a, \sigma^h(a), ..., \sigma^{h(k-1)}(a)$ entre elles, et donc laisse les coefficients de P invariants. Ces derniers sont bien dans $K_{f'}$, donc P satisfait les conditions demandées. □

Le corollaire suivant va maintenant permettre de démontrer la deuxième propriété énoncée sur les périodes :

Corollaire 2.4.12. *Soient f et f' deux diviseurs de $p-1$ et η et ξ deux périodes respectivement de f et f' termes. Si f divise f', alors η est racine d'un polynôme de degré f'/f dont les coefficients sont des expressions rationnelles de ξ.*

Démonstration. D'une part, $\eta \in K_f$ est une période de f termes, donc en appliquant la proposition 2.4.11, η est bien racine d'un polynôme de degré f'/f à coefficient dans $K_{f'}$. D'autre part ξ est une période de f' termes, donc en appliquant la proposition 2.4.7 (page 10), on a que tout élément de $K_{f'}$ s'écrit comme $\mathbb{Q}$-combinaison linéaire de puissances de ξ, donc les coefficients du polynôme sont bien des expressions rationnelles de ξ. □

2.4.3 Applications des périodes au polynôme cyclotomique

Appliquons maintenant cette notion de périodes à des exemples concrets. Tout d'abord, observons l'algorithme suivant : pour $i = 0, ..., r$, on considère η_i une période de f_i termes, où les f_i sont tels que, pour $i = 1, ..., r$,

$$p - 1 = f_0, f_1, ..., f_{r-1}, f_r = 1 \text{ et } f_i \text{ divise } f_{i-1}.$$

Le but va être d'établir, grâce à la méthode fournie par Gauss dans *"Disquisitiones Arithmeticae"*, r équations dont les η_i seront solutions.

Pour $i = 0$, on a η_0 qui correspond à l'unique période de $p - 1$ termes (autrement dit à la somme de toutes les racines primitives $p^{\text{ième}}$ de l'unité), donc $\eta_0 = -1 \in \mathbb{Q}$. Ensuite, d'après la deuxième propriété sur les périodes, nous savons que, pour $i = 1, ..., r$, chaque η_i se détermine en résolvant une équation de degré f_{i-1}/f_i dont les coefficients sont des expressions rationnelles des η_{i-1}. Enfin, pour $i = r$, nous aboutissons à une période d'un seul terme, d'où $\eta_r \in \{\zeta_0, \zeta_1 ..., \zeta_{p-2}\}$, avec ζ_i une racine primitive $p^{\text{ième}}$ de l'unité. En outre, cette méthode permet de trouver une racine primitive $p^{\text{ième}}$ de l'unité, et toutes les autres pourront être déterminées en prenant les puissances de η_r.

Remarque : Le choix de la période η_i n'influe pas sur la solution trouvée puisque, d'après la première propriété, chaque période de f_i termes est l'expression rationnelle d'une autre période de f_i termes.

Exemple 1 : Considérons le polynôme cyclotomique $\Phi_{17}(X) = X^{16} + ... + X + 1$. On a ici $p = 17$, donc $p - 1 = 16$. Pour $i = 1$, on sait qu'il existe $e = 16/8 = 2$ périodes de huit termes qui sont racines d'une équation de degré $16/8 = 2$. De même, pour respectivement $i = 2, 3$ et 4, il existe quatre périodes des quatre termes, huit périodes de deux termes et enfin seize périodes de un terme (qui correspondent aux racines primitives $17^{\text{ième}}$ de l'unité différentes de 1), et toutes ces périodes sont racines d'équations quadratiques.

On va maintenant déterminer les équations qui permettent d'exprimer les racines de Φ_{17}.

Pour ce faire, commençons par choisir une racine primitive modulo 17 : 3 engendre l'ensemble des restes dans la division euclidienne par 17 et, en notant $\zeta^k = \exp \frac{2ik\pi}{17}$ une racine primitive $17^{\text{ième}}$ de l'unité, nous avons les relations suivante :

$$\zeta_0 = \zeta^1 ; \quad \zeta_1 = \zeta^3 ; \quad \zeta_2 = \zeta^9 ; \quad \zeta_3 = \zeta^{10} ; \quad \zeta_4 = \zeta^{13} ; \zeta_5 = \zeta^5 ; \quad \zeta_6 = \zeta^{15} ; \quad \zeta_7 = \zeta^{11} ; \quad \zeta_8 = \zeta^{16} ;$$
$$\zeta_9 = \zeta^{14} ; \quad \zeta_{10} = \zeta^8 ; \quad \zeta_{11} = \zeta^7 ; \quad \zeta_{12} = \zeta^4 ; \quad \zeta_{13} = \zeta^{12} ; \quad \zeta_{14} = \zeta^2 ; \quad \zeta_{15} = \zeta^6.$$

Pour $i = 1$: nous savons que la première équation à trouver est une équation quadratique dont les deux périodes de huit termes suivantes

$$\begin{cases} \eta_1 = \zeta_0 + \zeta_2 + \zeta_4 + \zeta_6 + \zeta_8 + \zeta_{10} + \zeta_{12} + \zeta_{14} \\ \eta_1' = \zeta_1 + \zeta_3 + \zeta_5 + \zeta_7 + \zeta_9 + \zeta_{11} + \zeta_{13} + \zeta_{15} \end{cases}$$

sont les racines. Pour la déterminer, il suffit d'utiliser le lien entre les coefficients d'un polynôme du second degré et ses racines, ce qui donne après une suite de calculs l'équation $x^2 + x - 4 = 0$.

Pour $i = 2$: nous avons quatre périodes de quatre termes, donc il nous faut trouver deux équations quadratiques. Pour cela, Gauss remarque que les périodes de quatre termes sont en fait contenues dans les périodes de huit termes. C'est en effet évident puisqu'on a :

$$\begin{cases} \eta_2^{(1)} &= \zeta_0 + \zeta_4 + \zeta_8 + \zeta_{12} \\ \eta_2^{(2)} &= \zeta_1 + \zeta_5 + \zeta_9 + \zeta_{15} \\ \eta_2^{(3)} &= \zeta_2 + \zeta_6 + \zeta_{10} + \zeta_{14} \\ \eta_2^{(4)} &= \zeta_3 + \zeta_7 + \zeta_{11} + \zeta_{13} \end{cases}$$

Ceci facilite la recherche des coefficients, puisqu'on peut alors les exprimer en fonction des η_1 et η_1'. On trouve finalement deux équations quadratiques, dont les racines sont respectivement les sommes $\eta_2^{(1)}$, $\eta_2^{(3)}$ et $\eta_2^{(2)}$, $\eta_2^{(4)}$ et dont les coefficients sont des expressions rationnelles de η_1 et η_1' :

$$\begin{cases} x^2 - \eta_1 x - 1 = 0 \\ x^2 - \eta_1' x - 1 = 0 \end{cases}$$

Pour $i = 3$: nous cherchons à déterminer quatre équations quadratiques dont les racines sont les périodes de deux termes que nous notons, pour $j = 0, ..., 7$:

$$\xi_j = \zeta_j + \zeta_{j+8}.$$

En appliquant à nouveau les relations entre les coefficients et les racines d'un polynôme du second degré, on trouve les équations suivantes :

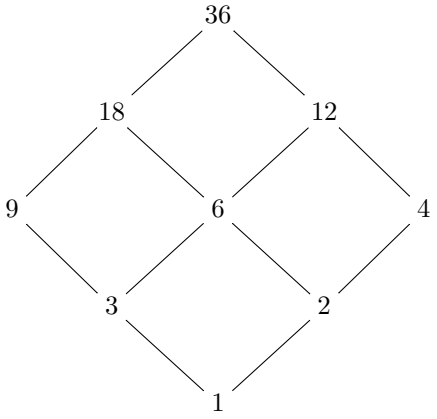
$$\begin{cases} x^2 - \eta_2^{(1)} x + \eta_2^{(2)} = 0 \\ x^2 - \eta_2^{(3)} x + \eta_2^{(4)} = 0 \\ x^2 - \eta_2^{(1)} x + \eta_2^{(3)} = 0 \\ x^2 - \eta_2^{(2)} x + \eta_2^{(4)} = 0 \end{cases}$$

Pour $i = 4$: il reste simplement à déterminer les huit équations qui donnent exactement les racines de Φ_{17} différentes de 1. En utilisant toujours la même méthode que précédemment, on trouve finalement les équations suivantes, pour $j = 0, ..., 7$:

$$x^2 - \xi_j x + 1 = 0.$$

Exemple 2 : Considérons maintenant le polynôme cyclotomique $\Phi_{37}(X) = \frac{X^{37}-1}{X-1}$. Il est évident que ce cas va imposer un nombre plus important d'équations à résoudre afin de trouver les trente-six racines primitives $37^{\text{ième}}$ de l'unité différentes de 1, c'est pourquoi nous n'allons pas le traiter de la même façon que le premier. En effet, nous allons simplement rassembler à travers un schéma les différentes façon d'arriver aux équations dont les racines sont celles de Φ_{37}.

On a pris ici $p = 37$, donc $p - 1 = 36$. Il s'agit dans un premier temps de trouver l'ensemble des diviseurs de 36 : $\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Ensuite, on construit le diagramme suivant, en sachant qu'un trait représente une **relation de divisibilité**.



Le diagramme fonctionne comme suit : chaque chemin qui part de 1 pour arriver à 36 représente un **motif de solutions** de l'équation $\Phi_{37}(X) = 0$. Celles-ci se trouvent, d'après l'algorithme proposé au début de cette partie, en résolvant successivement un certain nombre d'équations dont les degrés sont fixés.

Par exemple, si on choisit le chemin

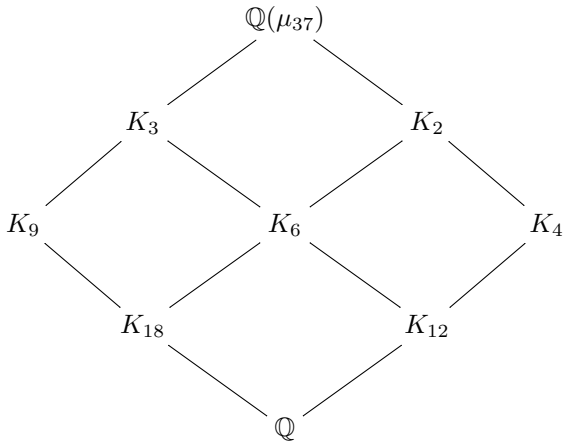
$$1 \to 3 \to 6 \to 18 \to 36,$$

alors il s'agit d'abord de déterminer une période de dix-huit termes en résolvant une équation de degré $36/18 = 2$. Ensuite, on détermine une période de six termes en résolvant une équation de degré $18/6 = 3$, puis une période de trois termes en résolvant une équation de degré $6/3 = 2$. Enfin,

on trouve une période de un terme, autrement dit une racine $37^{\text{ième}}$ de l'unité différentes de 1, en résolvant une équation de degré 3.

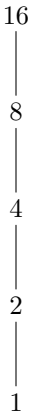
Notons qu'il est également possible de construire un diagramme similaire en se basant sur l'équivalence donnée par le lemme 2.4.10. En effet, puisque $K_{f'} \subset K_f$ si et seulement si f divise f', il est naturel de constater que K_1 est le corps le plus gros qu'on puisse avoir. Comme on a choisi $p = 37$, on peut écrire que $K_1 = \mathbb{Q}(\mu_{37})$ et de même, $K_{36} = \mathbb{Q}$. Par analogie avec les chemins qu'il était possible de prendre dans le diagramme précédent, nous avons aussi différents types de chemins ici, comme par exemple :

$$K_1 \subset K_2 \subset K_4 \subset K_{12} \subset K_{36}.$$



Il s'agit cependant d'un diagramme plus moderne puisqu'il fait intervenir des corps, notions qui n'était pas encore définie à l'époque où Gauss établit sa théorie. Ici, un trait représente une **relation d'inclusion.**

Remarques : **1)** Le diagramme correspondant au premier exemple que nous avons traité est le suivant :



On constate qu'il n'y a ici qu'un motif de solutions de l'équation $\Phi_{17} = 0$ puisqu'il n'y a qu'un chemin qui permet de passer de 1 à 16.

2) Nous avons ici traité deux cas assez simples, dans le sens où les équations auxquelles nous aboutissions étaient toutes de degré 2 ou 3, donc en particulier de degré inférieur à 5, ce qui implique qu'elles sont toutes résolubles (à l'aide de formules bien connues) par radicaux. Mais il se peut que cela ne soit pas toujours le cas ; ceci fera l'objet de la partie suivante.

2.5 Résolubilité par radicaux

La principale utilité des périodes de Gauss est le résultat suivant, qu'il montre dans *"Disquisitiones Arithmeticae"* (Art. 359-360) : **les équations qui déterminent les périodes sont résolubles par**

radicaux.

Comme précédemment, on pose f, e et f', h deux paires d'entiers tels que

$$ef = hf' = p-1, \text{ et on pose } k = \frac{f'}{f} = \frac{e}{h},$$

et on suppose de plus que f divise f'. Posons également η_i et ξ_j des périodes de respectivement f et f' termes, définies pour $i, j = 0, ..., e-1$ telles que

$$\eta_i = \zeta_i + \zeta_{e+i} + \zeta_{2e+i} + ... + \zeta_{e(f-1)+i},$$

$$\xi_j = \zeta_j + \zeta_{h+j} + \zeta_{2h+j} + ... + \zeta_{e(f'-1)+i}.$$

D'après le corollaire 2.4.12 (page 12), nous savons que si les périodes $\xi_0, ..., \xi_{h-1}$ sont connues, alors toute période η_i peut être déterminée en résolvant une équation de degré f'/f. Cependant, il existe des cas où les équations à résoudre sont de degré supérieur ou égal à 5 et dans ce cas, l'équation peut ne pas être résoluble par radicaux. Le but de cette partie va être de montrer que, dans ce cas précis, l'équation de degré f'/f est toujours résoluble par radicaux.

Considérons le cas où l'on cherche l'équation qui conduit à trouver une expression pour η_0 (l'argument sera exactement le même pour les autres périodes). Notons cette équation de degré f'/f par $P(X) = 0$, dont nous savons que les coefficients sont dans $K_{f'}$. De ce fait, ils sont invariants sous σ^h. Appliquant ce dernier à $P(\eta_0) = 0$, nous obtenons :

$$P(\sigma^h(\eta_0)) = 0,\ P(\sigma^{2h}(\eta_0)) = 0, ...,\ P(\sigma^{(k-1)h}(\eta_0)) = 0.$$

Ceci permet de voir que les racines de P sont en fait les η_0 et ses images par les puissance de σ^h, que l'on note respectivement $\eta_h, \eta_{2h}, ..., \eta_{(k-1)h}$.

Définition : Soit ω une racine $k^{\text{ième}}$ de l'unité. On appelle **résolvante de Lagrange** en les $x_1, ..., x_k$ le polynôme

$$t(\omega) = x_1 + \omega x_2 + \omega^2 x_3 + ... + \omega^{k-1} x_k.$$

Formule de Lagrange : Si $t(\omega)$ désigne la résolvante de Lagrange avec les notations de la définition précédente, alors nous avons, pour $i = 1, ..., n$,

$$x_i = \frac{1}{n}\Big(\sum_{\omega} \omega^{-(i-1)} t(\omega)\Big).$$

Dans la proposition suivante, on prendra pour $i = 0, h, 2h..., (k-1)h$, $x_i = \eta_i$.

Proposition 2.5.1. *On considère cette fois la résolvante de Lagrange en ayant substituer les $\eta_0, ..., \eta_{(k-1)h}$ aux $x_1, ..., x_k$, c'est à dire*

$$t(\omega) = \eta_0 + \omega\eta_h + ... + \omega^{k-1}\eta_{(k-1)h}.$$

Pour toute ω racine $k^{\text{ième}}$ de l'unité, le nombre complexe $t(\omega)^k$ est une $\mathbb{Q}$-combinaison linéaire des puissances de ω et de périodes de f' termes.

Démonstration. D'après la proposition 2.4.7 (page 10), le produit de deux périodes quelconques est une combinaison linéaire de périodes de f termes. On a alors des relations entre les périodes, qui peuvent être utilisées pour réduire à 1 le degré de n'importe quelle expression polynômiale de périodes. En particulier,

$$\begin{aligned} t(\omega)^k &= (\eta_0 + \omega\eta_h + ... + \omega^{k-1}\eta_{(k-1)h})^k \\ &= a_0\eta_0 + ... + a_{h-1}\eta_{h-1} \\ &+ a_h\eta_h + ... + a_{2h-1}\eta_{2h-1} \\ &+ ... \\ &+ a_{(k-1)h}\eta_{(k-1)h} + ... + a_{e-1}\eta_{e-1} \end{aligned} \tag{1}$$

où les $a_0, ..., a_{e-1}$ sont des $\mathbb{Q}$-combinaison linéaire de puissances de ω. De plus, puisque les périodes $\eta_0, .., \eta_{e-1}$ dont préservés par σ^h, on peut, par définition de σ, les remplacer dans le calcul de $t(\omega)^k$ par respectivement $\sigma^h(\eta_0) = \eta_h, ..., \sigma^h(\eta_{e-1}) = \eta_{h-1}$. On trouve alors

$$\begin{aligned} t(\omega)^k &= (\eta_h + \omega\eta_{2h} + ... + \omega^{k-1}\eta_0)^k \\ &= a_0\eta_h + ... + a_{h-1}\eta_{2h-1} \\ &+ a_h\eta_{2h} + ... + a_{2h-1}\eta_{3h-1} \\ &+ ... \\ &+ a_{(k-1)h}\eta_{(0} + ... + a_{e-1}\eta_{h-1}. \end{aligned} \tag{2}$$

De plus, si on applique σ^h à $t(\omega)$, nous avons naturellement

$$\sigma^h(t(\omega)) = \omega^{-1}t(\omega)$$

et donc

$$(\sigma^h(t(\omega)))^k = t(\omega)^k.$$

Ceci implique directement que (1) et (2) sont deux expressions de $t(\omega)^k$. Si on remplace, pour $i = 0, ..., e-1$, les η_i par $\sigma^{2h}(\eta_i), ..., \sigma^{(k-1)h}$ dans le calcul initial de $t(\omega)^k$, alors on trouvera $k-2$ autres expressions de $t(\omega)^k$. Les coefficients d'une période η_i dans une de ces expressions sont donc les $a_i, a_{i+h}, ..., a_{(k-1)h+i}$ et enfin, si on somme ces k expressions, on obtient

$$\begin{aligned} kt(\omega)^k &= (a_0 + ... + a_{(k-1)h})(\eta_0 + ... + \eta(k-1)h \\ &+ (a_1 + ... + a_{(k-1)h+1})(\eta_1 + ... + \eta_{(k-1)h+1}) \\ &+ ... \\ &+ (a_{h-1} + ... + a_{e-1})(\eta_{h-1} + ... + \eta_{e-1}). \end{aligned}$$

Or puisque, pour $i = 0, ..., h-1$, $\eta_i + \eta_{h+i} + ... + \eta_{h(k-1)+i} = \xi_i$, il s'en suit que

$$t(\omega)^k = \frac{1}{k}((a_0 + ... + a_{h(k-1)})\xi_0 + ... + (a_{h-1} + ... + a_{e-1})\xi_{h-1}),$$

donc $t(\omega)^k$ est bien une $\mathbb{Q}$-combinaison linéaire de puissance de ω et de ξ. □

Cette proposition va notamment servir à démontrer le théorème suivant, qui est la clé de cette partie :

Théorème 2.5.2. *Pour tout entier $n \in \mathbb{N}$, les racines $n^{\text{ièmes}}$ de l'unité ont une expression par radicaux.*

Pour montrer ce théorème, nous avons besoin de distinguer le cas où n est un entier positif qui n'est pas premier et où $n = p$ avec p un nombre premier. Le lemme suivant va permettre de montrer le théorème dans le cas où n n'est pas premier :

Lemme 2.5.3. *Soient n un entier positif. Si pour chaque facteur premier p de n les racines $p^{\text{ièmes}}$ de l'unité ont une expression par radicaux, alors les racines $n^{\text{ièmes}}$ ont aussi une expression par radicaux.*

Démonstration. Le cas où n est premier est évidemment trivial. Dans le cas contraire, on raisonne par récurrence sur le nombre de facteurs premiers de n : supposons qu'il existe r et s deux entiers positifs tels que $r, s \neq 1$ et $n = rs$. Alors, le nombre de facteurs premiers dans la décomposition de r, respectivement dans celle de s, est strictement inférieur au nombre de facteurs premiers dans la décomposition de n donc par récurrence, les racines $r^{\text{ièmes}}$ de l'unité $\xi_1, ..., \xi_r$ et les racines $s^{\text{ièmes}}$ de l'unité $\eta_1, ..., \eta_s$ ont une expression par radicaux.

D'autre part, les racines $n^{\text{ièmes}}$ de l'unité sont de la forme $\xi_i \sqrt[r]{\eta_j}$: en effet, cela découle de la factorisation du polynôme $X^n - 1$ dont les racines sont les racines $n^{\text{ièmes}}$ de l'unité : pour $n \in \mathbb{N}$, nous avons :

$$X^n - 1 = \prod_{k=1}^{n}(X - \zeta_k),$$

avec ζ_k les racines $n^{\text{ièmes}}$ de l'unité. Alors, en substituant X^r à X et en prenant $n = s$, nous avons

$$X^{rs} - 1 = \prod_{j=1}^{s} (X^r - \eta_j).$$

Ainsi, les racines de ce polynôme qui sont les racines $n^{\text{ièmes}}$ de l'unité sont bien les racines $r^{\text{ièmes}}$ des η_j, pour $j = 1, ..., s$, que multiplient les ξ_i, pour $i = 1, ..., r$. Ainsi les racines $n^{\text{ièmes}}$ de l'unité ont bien une expression par radicaux. □

Passons maintenant à la preuve du théorème 2.5.2 :

Démonstration. On raisonne par récurrence forte sur n : le théorème est évidemment vrai pour $n = 1$ et $n = 2$, supposons donc qu'il est vrai pour tout entier $k < n$. Dans le cas où n n'est pas premier, on utilise simplement le lemme précédent ainsi que l'hypothèse de récurrence qui prouvent que les racines $n^{\text{ièmes}}$ de l'unité ont une expression par radicaux. Si $n = p$ avec p un nombre premier, alors, si ζ est une racine primitive $p^{\text{ième}}$ de l'unité, on peut réordonner toutes les racines primitives $p^{\text{ièmes}}$ différentes de 1 à l'aide d'une racine primitive modulo p, et ainsi considérer la résolvante de Lagrange en prenant $x_i = \zeta_i$, pour $i = 0, ..., p - 2$. On a donc

$$t(\omega) = \zeta_0 + \omega\zeta_1 + ... + \omega^{p-2}\zeta_{p-2},$$

où ω est évidemment une racine primitive $(p-1)^{\text{ième}}$ de l'unité. Par hypothèse de récurrence, ω peut donc s'exprimer à l'aide de radicaux. Puis, appliquant la proposition 2.5.1 avec $k = f' = p - 1$, on trouve que $t(\omega)^{p-1}$ est une expression rationnelle de ω, qui s'exprime par radicaux. Enfin, la formule de Lagrange nous donne que

$$\zeta_i = \frac{1}{p-1}\Big(\sum_{\omega} \omega^{-i\ \sqrt[p-1]{t(\omega)^{p-1}}}\Big).,$$

ce qui conclut la démonstration. □

Remarque : Nous venons de montrer ce théorème pour tout entier n positif, mais le cas qui nous intéressait ici était plus particulier celui où n est un nombre premier.

Gauss s'est ici occupé d'une certaine classe d'équation. Leurs racines sont tellement explicites qu'on peut construire la résolution par radicaux à l'aide d'outil arithmétique. Nous allons voir dans la partie suivante que Galois utilisera cet exemple en cherchant à généraliser pour caractériser toutes les équations, sachant qu'elles ne sont pas toutes résolubles par radicaux.

3 Théorie de Galois et résolubilité par radicaux

3.1 Introduction et contexte historique

Evariste Galois est un mathématicien connu pour avoir révolutionné l'Algèbre au cours du XIX$^{\text{ième}}$ siècle et avoir construit toute une théorie qui porte aujourd'hui son nom. Cependant, ce jeune prodige était très incompris par les mathématiciens de l'époque : sa façon de voir et de penser les mathématiques et notamment l'Algèbre n'était pas la même que celle de ses prédécesseurs. En effet lorsque Galois dépose en 1831 son "*Mémoire sur les conditions de résolubilité d'une équation par radicaux*" à l'académie des sciences, ce dernier est jugé, par les mathématiciens Siméon-Denis Poisson (1781-1840) et Sylvestre François Lacroix (1765-1843), ni assez clair ni assez développé.

Dans ce mémoire, Galois cherche à répondre à la question "quelles sont les équations dont les solutions peuvent être exprimées par radicaux ?" et il donne un critère qui permet de répondre à cette question. Pour établir ce critère, il utilise trois notions : les **permutations de racines**, le **groupe d'une équation** et l'**adjonction de quantités**. La première notion est en fait déjà introduite par Lagrange, et Galois s'en est très certainement inspiré : c'est ce qui consiste à échanger les racines d'une équation entre elles. Le groupe d'une équation correspond à l'ensemble des permutations des solutions de cette équation qui vérifie des propriétés particulières. Enfin l'adjonction de quantités est le fait d'ajouter à un ensemble sur lequel un polynôme est irréductible, des quantités qui permettent à ce polynôme de se factoriser. Galois ne possédait évidemment pas le vocabulaire que nous utilisons aujourd'hui, mais on peut faire l'analogie avec ce que nous appelons "corps" et "extensions de corps".

Le but de cette partie va être d'introduire toutes ces notions et d'arriver au critère de résolubilité d'une équation. Dans un premier temps, nous expliquerons ce qu'est le groupe de Galois d'une équation ainsi que ses propriétés, tout en faisant un parallèle avec la définition de groupe en tant que structure algébrique que nous connaissons aujourd'hui. Ensuite, nous parlerons d'adjonction de racines en utilisant les notions d'extensions de corps et d'**extensions radicielles**. Enfin, la dernière partie sera consacrée à la condition nécessaire et suffisante pour qu'une équation soit résoluble par radicaux.

3.2 Le groupe de Galois d'une équation

Dans tout ce chapitre, on considèrera uniquement des corps de caractéristique nulle. On rappelle que $F(x_1, ..., x_n)$ désigne le corps des fractions rationnelles en $x_1, ..., x_n$ à coefficients dans F et $F[x_1, ..., x_n]$ l'ensemble des polynômes en $x_1, ..., x_n$ à coefficients dans F.

3.2.1 Définitions et premières propriétés

Dans tout ce qui suit, on considèrera un polynôme P de degré $n \in \mathbb{N}$ sur un corps F et dont les n racines $\{r_1, ..., r_n\}$ sont distinctes dans un corps K contenant F. On note alors

$$F(r_1, ..., r_n) = \{f(r_1, ..., r_n) \mid f \in F(x_1, ..., x_n)\},$$

en ne considérant uniquement les fractions rationnelles de $F(x_1, ..., x_n)$ qui sont définies, c'est à dire dont le dénominateur ne s'annule pas.

Définitions : 1) On appelle **résolvante de Galois** de l'équation $P(X) = 0$ sur le corps F un élément $V \in F(r_1, ..., r_n)$ qui vérifie

$$r_i \in F(V) \text{ pour } i = 1, ..., n.$$

2) On appelle **polynôme minimal** de $V \in F(x_1, ..., x_n)$ sur F le polynôme irréductible et unitaire noté $\pi \in F[X]$ qui vérifie

$$\pi(V) = 0.$$

Remarques : **1)** Pour résoudre une équation $P(X) = 0$ il suffit de déterminer V, puisque les racines $r_1, ..., r_n$ de P sont des fractions rationnelles en V.
2) Il sera démontré plus loin qu'il existe toujours un tel $V \in F(r_1, ..., r_n)$.

Le lemme suivant va permettre de démontrer une propriété importante de la résolvante de Galois d'une équation $P(X) = 0$ qui lie cette dernière aux racines du polynôme P.

Lemme 3.2.1. *Soient $f \in F(X)$ une fraction rationnelle en X sur un corps F et V une racine d'un polynôme irréductible $\pi \in F[X]$. Si $f(V) = 0$, alors $f(W) = 0$ pour toute racine W de π.*

Démonstration. Soit $f \in F(X)$, alors il existe $\varphi, \psi \in F[X]$ tels que $f = \varphi/\psi$. Supposons de plus que $\varphi(V) = 0$ et $\psi(V) \neq 0$. Alors, d'après le lemme 2.4.4 (page 9), π divise φ, ce qui donne directement que $\varphi(W) = 0$ pour toute racine W de π. Si d'autre part on suppose que $\psi(W) = 0$ pour une certaine racine W de π, alors on aurait par le même argument $\psi(V) = 0$ ce qui est en contradiction avec l'hypothèse de départ. Ainsi $\varphi(W) = 0$ et $\psi(W) \neq 0$, donc $f(W) = 0$ pour toute racine W de π. □

Notations : Si V est une résolvante de Galois de l'équation $P(X) = 0$, alors par définition il existe, pour $i = 1, ..., n, f_i(X) \in F(X)$ tels que $r_i = f_i(V)$. On note alors $V = V_1, V_2, ..., V_m$ les différentes racines du polynôme minimal de V sur F. De plus, ces racines appartiennent à $F(r_1, ..., r_n)$.

Proposition 3.2.2. *Soient r_i, f_i et V_j comme ci-dessus. Alors, pour $i = 1, ..., n$ et $j = 1, ..., m$, $f_i(V_j)$ est une racine de P. De plus, quelque soit $j \in \{1, ..., m\}$, les racines $f_1(V_j), ..., f_n(V_j)$ sont distinctes deux à deux, de telle sorte que*

$$\{f_1(V_j), ..., f_n(V_j)\} = \{r_1, ..., r_n\}.$$

Démonstration. Pour $i = 1, ..., n$, nous avons $f_i(V) = f_i(V_1) = r_i$ ce qui implique que $P\big(f_i(V_1)\big) = 0$. Alors en appliquant le lemme 3.2.1 à la fraction $P\big(f_i(X)\big) \in F(X)$, nous avons immédiatement, pour $j = 1, ..., m$,

$$P\big(f_i(V_j)\big) = 0.$$

De plus, si on suppose que pour deux certains $i, k = 1, ..., n$ et un certain $j = 1, ..., m$,

$$f_i(V_j) = f_k(V_j),$$

alors V_j est racine de la fraction rationnelle $f_i - f_k$ donc à nouveau d'après le lemme 3.2.1,

$$f_i(V_1) = f_k(V_1),$$

ce qui prouve bien que $r_i = r_k$, donc que $i = k$ puisque les racines $r_1, ..., r_n$ sont supposées distinctes deux à deux. □

Après avoir énoncé et démontré cette proposition, il est naturel de vouloir construire des automorphismes qui, à chaque $f_i(V_j)$ associent une racine $r_1, ..., r_n$ du polynôme P. Puisqu'il a été montré que chacun de ces $f_i(V_j)$ est aussi une racine du polynôme P, on peut dire que ces automorphismes agiront par permutation sur les racines de P. Autrement dit, on construit pour $j = 1, ..., m$, les automorphismes suivants :

$$\sigma_j : r_i \mapsto f_i(V_j) \text{ pour } i = 1, ..., n.$$

Définition : On appelle **groupe de Galois** de l'équation $P(X) = 0$ sur F et on note $Gal(P/F)$ l'ensemble des automorphismes $\{\sigma_1, ..., \sigma_m\}$ définis ci-dessus. .

Attention ! Il n'est pas clair a priori que le groupe de Galois est un groupe au sens de la structure algébrique, d'autant que la définition qui vient d'être donnée est celle présentée par Galois dans son *"Mémoire sur les conditions de résolubilité des équations par radicaux"* et qu'à cette époque, la notion de groupe en tant que structure algébrique n'était pas encore établie. Cependant, nous démontrerons dans la partie suivante qu'il s'agit bien d'un groupe au sens où nous l'entendons aujourd'hui.

3.2.2 Première proposition de Galois

Pour cette partie, on construit un automorphisme σ qui agit par permutation sur les racines de P de la façon suivante :

$$\sigma\big(f(r_1,...,r_n)\big) = f\big(\sigma(r_1),...,\sigma(r_n)\big), \tag{1}$$

avec $f \in F(x_1,...,x_n)$ une fraction rationnelle dont le dénominateur ne s'annule pas pour $x_i = \sigma(r_i)$.

Le théorème qui suit correspond à la Proposition 1 établie par Galois dans son *"Mémoire sur les conditions de résolubilité des équations par radicaux"*. Il permettra entre autre de justifier de manière rigoureuse la construction de la permutation σ, et en particulier l'égalité (1).

Théorème 3.2.3. *Soient $f(x_1,...,x_n) \in F(x_1,...,x_n)$ et $\sigma \in Gal(P/F)$. Alors,*

$$f\big(\sigma(r_1),...,\sigma(r_n)\big) \in F(r_1,...,r_n)$$

est défini dès que $f(r_1,...,r_n)$ existe. De plus, $f(r_1,...,r_n) \in F$ si et seulement si pour tout $\sigma \in Gal(P/F)$,

$$f\big(\sigma(r_1),...,\sigma(r_n)\big) = f(r_1,...,r_n).$$

Démonstration. Soient $f = \varphi/\psi$, avec $\varphi, \psi \in F[x_1,...,x_n]$ et $\sigma \in Gal(P/F)$. Supposons que $\psi(r_1,...,r_n) \neq 0$. Alors, en remplaçant $r_1,...,r_n$ par les fractions rationnelles $f_1(V),...,f_n(V)$, nous avons

$$\psi(r_1,...,r_n) = \psi\big(f_1(V),...,f_n(V)\big) = g(V),$$

avec $g \in F(X)$. De même, si V' est une autre racine de π qui vérifie

$$\sigma : r_i \mapsto f_i(V'),$$

alors

$$\psi\big(\sigma(r_1),...,\sigma(r_n)\big) = \psi\big(f_1(V'),...,f_n(V')\big) = g(V').$$

Si on suppose que $\psi\big(\sigma(r_1),...,\sigma(r_n)\big) = 0$, alors V' est une racine de g ce qui implique par le lemme 3.2.1 que $g(V) = 0$, et que donc $\psi(r_1,...,r_n) = 0$, ce qui est absurde. Ceci prouve donc que $\psi\big(\sigma(r_1),...,\sigma(r_n)\big) \neq 0$ et que donc $f\big(\sigma(r_1),...,\sigma(r_n)\big)$ est bien défini quand $f(r_1,...,r_n)$ l'est aussi.

Pour prouver l'équivalence, on va à nouveau remplacer les $r_1,...,r_n$ par leurs expressions rationnelles en V mais cette fois dans $f(r_1,...,r_n)$, ce qui donne

$$f(r_1,...,r_n) = f\big(f_1(V),...,f_n(V)\big) = h(V),$$

avec comme avant $h \in F(X)$.

Si on suppose, pour le sens direct, que $f(r_1,...,r_n) \in F$, alors

$$h(X) - f(r_1,...,r_n) \in F(X).$$

De plus, la fraction rationnelle s'annule en $X = V$, elle s'annule aussi sur toutes les racines de π par le lemme 3.2.1, donc pour $X = V_1,...,V_m$. Ainsi, nous avons pour $j = 1,...,m$,

$$h(V_j) = f\big(f_1(V_j),...,f_n(V_j)\big) = f(r_1,...,r_n)$$

et, par définition de σ_j,

$$f\big(\sigma_j(r_1),...,\sigma_j(r_n)\big) = f(r_1,...,r_n) \text{ pour } j = 1,...,m.$$

Pour la réciproque, supposant que cette dernière égalité est vérifiée, nous avons

$$f(r_1,...,r_n) = h(V_j) \text{ pour } j = 1,...,m,$$

et donc

$$f(r_1,...,r_n) = \frac{1}{m}\big(h(V_1) + ... + h(V_m)\big). \tag{1}$$

On remarque que la fraction rationnelle $h(x_1)+...+h(x_m)$ est symétrique en les m variables $x_1,...,x_m$, on peut donc d'après le rappel l'exprimer sous forme d'une fraction rationnelle des polynômes symétriques élémentaires $s_1,...,s_m$. Alors, substituant les $V_1,...,V_m$ aux $x_1,...,x_m$, on voit que la partie droite de l'équation (1) peut être calculée à partir des coefficients du polynôme π dont les racines sont les $V_1,...,V_m$ et dont les coefficients sont dans F. Ainsi, on en conclut d'après l'équation (1) que $f(r_1,...,r_n) \in F$. □

Remarque : Pour un σ fixé dans $Gal(P/F)$, l'élément $f\big(\sigma(r_1),...,\sigma(r_n)\big) \in F(r_1,...,r_n)$ ne dépend pas de la fraction rationnelle $f \in F(x_1,...,x_n)$ mais seulement de $f(r_1,...,r_n)$.

En effet, si on suppose qu'il existe $g \in F(x_1,...,x_n)$ telle que

$$f(r_1,...,r_n) = g(r_1,...r_n),$$

alors la fraction rationnelle $f-g$ s'annule en $x_i = r_i$, pour $i = 1,...,n$. Or d'après le théorème précédent, nous avons pour tout $\sigma \in Gal(P/F)$,

$$(f-g)\big(\sigma(r_1),...,\sigma(r_n)\big) = (f-g)(r_1,...,r_n) = 0,$$

ce qui implique directement que

$$f\big(\sigma(r_1),...,\sigma(r_n)\big) = g\big(\sigma(r_1),...,\sigma(r_n)\big).$$

Le corollaire suivant justifie la construction de l'automorphisme σ :

Corollaire 3.2.4. *Toute permutation $\sigma \in Gal(P/F)$ peut être étendue à un automorphisme de $F(r_1,...,r_n)$ qui fixe F, en posant*

$$\sigma\big(f(r_1,...,r_n)\big) = f\big(\sigma(r_1),...,\sigma(r_n)\big)$$

pour toute fraction rationnelle $f(x_1,...,x_n)$ pour laquelle $f(r_1,..,r_n)$ est définie.

Démonstration. σ est clairement bijective sur $F(r_1,...,r_n)$. Nous avons

$$\begin{aligned}\sigma\big(f(r_1,...,r_n)\big) + \sigma\big(g(r_1,...,r_n)\big) &= f\big(\sigma(r_1),...,\sigma(r_n)\big) + g\big(\sigma(r_1),...,\sigma(r_n)\big)\\ &= (f+g)\big(\sigma(r_1),...,\sigma(r_n)\big) = \sigma\big(f+g(r_1,...,r_n)\big)\end{aligned}$$

et de même

$$\begin{aligned}\sigma\big(f(r_1,...,r_n)\big)\cdot\sigma\big(f(r_1,...,r_n)\big) &= f\big(\sigma(r_1),...,\sigma(r_n)\big)\cdot g\big(\sigma(r_1),...,\sigma(r_n)\big)\\ &= (fg)\big(\sigma(r_1),...,\sigma(r_n)\big) = \sigma\big(f\cdot g(r_1,...,r_n)\big).\end{aligned}$$

□

Corollaire 3.2.5. *L'ensemble $Gal(P/F)$ ne dépend pas du choix de la résolvante de Galois.*

Démonstration. Posons $V' \in F(r_1,...,r_n)$ une autre résolvante de Galois de l'équation $P(X)=0$ et π' son polynôme minimal sur F. Alors, il existe, pour $i = 1,...,n$, des $f_i' \in F(X)$ telle que

$$r_i = f_i'(V'). \tag{1}$$

Le but est alors de montrer que tout élément de $Gal(P/F)$ défini avec V peut être défini de la même façon avec V'. Prenons $\sigma \in Gal(P/F)$ et montrons qu'il existe une racine W' de π' qui vérifie

$$\sigma : r_i \mapsto f_i'(W').$$

Nous avons, par construction de σ et en appliquant ce dernier à (1), nous avons

$$\sigma(r_i) = \sigma\big(f_i'(V')\big) = f_i'\big(\sigma(V')\big).$$

De même puisque V' est une racine de π', il s'en suit que

$$\sigma\big(\pi'(V')\big) = \pi'\big(\sigma(V')\big) = 0,$$

donc que $\sigma(V')$ est aussi une racine de π'. Il suffit donc, pour conclure la démonstration, de prendre $W' = \sigma(V')$.

□

Corollaire 3.2.6. *L'ensemble $Gal(P/F)$ est un sous-groupe du groupe de toutes les permutations de $r_1,...,r_n$.*

Démonstration. On sait que, pour $i = 1, ..., n$, $\sigma_1 : r_i \mapsto f_i(V_1) \in Gal(P/F)$. Or cet automorphisme correspond à l'identité puisque, par construction $f_i(V_1) = \sigma_1(r_i)$, pour tout $i \in \{1, ..., n\}$. Il reste à voir que $Gal(P/F)$ est stable par composition d'automorphismes et par passage à l'inverse.

Soient σ, τ deux automorphismes de $Gal(P/F)$. Il suffit de prendre la définition de ces automorphismes, pour $j, k = 1, ..., m$:

$$\begin{cases} \sigma : r_i \mapsto f_i(V_j) & \text{pour } i = 1, ..., n \\ \tau : r_i \mapsto f_j(V_k) & \text{pour } i = 1, ..., n \end{cases}$$

Il s'en suit directement que

$$\tau \circ \sigma : r_i \mapsto f_i(V_k),$$

d'où $\tau \circ \sigma \in Gal(P/F)$.

Soit $\sigma \in Gal(P/F)$. A nouveau par construction des automorphismes de $Gal(P/F)$, nous avons, pour un certain $j = 1, ..., m$,

$$\sigma(r_i) = f_i(V_j).$$

De pus, d'après la proposition 3.2.2, $f_i(V_j)$ est aussi une racine de P, donc V_j est une autre résolvante de Galois de l'équation $P(X) = 0$. Et comme $V = V_1$ et V_j sont deux racines du même polynôme minimal π, il s'en suit que l'automorphisme

$$f_i(V_j) \mapsto f_i(V_1)$$

est un élément de $Gal(P/F)$. Cet automorphisme que nous avons construit est tout simplement l'inverse de σ, ce qui implique que l'ensemble $Gal(P/F)$ est bien stable par passage à l'inverse. □

3.2.3 Existence de la résolvante de Galois et de son polynôme minimal

Dans la première partie, nous avons défini ce qu'était la résolvante de Galois d'une équation $P(X) = 0$. Dans ce qui suit, nous allons montrer que, quelque soit une équation donnée, il existe toujours une résolvante de Galois associée à cette équation ainsi qu'un polynôme irréductible de degré minimal annulateur de cette résolvante.

Par la suite, nous aurons besoin des deux lemmes suivant :

Lemme 3.2.7. *Soit g un polynôme en $x_1, ..., x_n$ sur un corps K. Si g est invariant sous toute permutation de $x_2, ..., x_n$, alors on peut l'écrire comme un polynôme en x_1 et en les polynômes symétriques élémentaires $s_1, ..., s_{n-1}$ à n variables $x_1, ..., x_n$.*

Démonstration. On considère g un polynôme en n variables $x_1, ..., x_n$ à coefficients dans K, que l'on regarde comme un polynôme en $n-1$ variables $x_2, ..., x_n$ et à coefficients dans $K[x_1]$. Supposons de plus que g est invariant par toute permutation de $x_2, ...x_n$. Alors, d'après le rappel 1 (page 40), g peut être écrit comme un polynôme en les $s'_1, ..., s'_{n-1}$ en $x_2, ..., x_n$ à coefficients dans $K[x_1]$, donc il existe $h \in K[x_1]$ tel que

$$g(x_1, ..., x_n) = h(x_1, s'_1, ..., s'_{n-1}). \tag{1}$$

Par définition des polynômes symétriques élémentaires en $n-1$ variables, on a

$$s'_1 = x_2 + ... + x_n,\ s'_2 = x_2x_3 + ... + x_{n-1}x_n, ..., s'_{n-1} = x_2x_3...x_n.$$

Il faut maintenant constater qu'on peut écrire les $s'_1, ..., s'_{n-1}$ en terme d'un polynôme en x_1 et en $s_1, ..., s_{n-1}$. En effet, d'après le rappel 2 (page 40), on a

$$(X - x_1)...(X - x_n) = X^n - s_1X^{n-1} + ... + (-1)^n s_n$$

et si on divise cette égalité par le polynôme $X - x_1$, alors on a

$$(X - x_2)...(X - x_n) = X^{n-1} - s'_1X^{n-2} + ... + (-1)^{n-1}s'_{n-1}.$$

On obtient donc les relations suivantes :

$$\begin{aligned} s'_1 &= s_1 - x_1, \\ s'_2 &= s_2 - s_1 x_1 + x_1^2, \\ s'_3 &= s_3 - s_2 x_1 + s_1 x_1^2 - x_1^3, \\ &... \\ s'_{n-1} &= s_{n-1} - s_{n-2} x_1 + ... + (-1)^{n-1} x_1^{n-1}, \end{aligned}$$

d'où, en remplaçant dans l'équation (1),

$$g(x_1, ..., x_n) = h(x_1, s_1 - x_1, ..., s_{n-1} - s_{n-2} x_1 + ... + (-1)^{n-1} x_1^{n-1}),$$

donc g est bien un polynôme en x_1 et en les $s_1, ..., s_{n-1}$. □

Lemme 3.2.8. *Il existe un polynôme $f \in F[x_1, ..., x_n]$ tel que les $n!$ éléments de $F(r_1, ..., r_n)$ obtenus en substituant $r_1, ..., r_n$ aux $x_1, ..., x_n$ dans toutes les permutations possibles sont deux à deux distincts.*

Démonstration. Soit $L(x_1, ..., x_n) = A_1 x_1 + ... + A_n x_n$ où les $A_1, ..., A_n$ sont des coefficients dans F que l'on va déterminer par la suite. Si on choisit deux permutations parmi les $n!$ de $\mathfrak{S}_n$ et que les deux valeurs de L obtenues en substituant $r_1, ..., r_n$ aux $x_1, ..., x_n$ avec ces deux permutations sont égales, alors on obtient une équation linéaire en les $A_1, ..., A_n$. Si on prend l'ensemble des paires de permutations possibles, on obtient de la même façon $\binom{n!}{2}$ équations en $A_1, ..., A_n$. Il suffit donc de trouver un $n-$uplet $(\alpha_1, ..., \alpha_n)$ qui ne vérifie aucune de ces équations, et le polynôme L vérifiera ainsi la propriété du lemme.

Comme on a un nombre fini d'équations, leurs solutions forment un sous-espace vectoriel de dimension finie de F^n. Or par hypothèse F est de caractéristique nulle, donc en particulier il est de dimension infinie et par conséquent F^n aussi, donc il existe bien un $n-$uplet $(\alpha_1, ..., \alpha_n) \in F^n$ qui ne vérifie aucune des équations. En conclusion, le polynôme

$$L(x_1, ..., x_n) = \alpha_1 x_1 + ... + \alpha_n x_n \text{ où } \alpha_i \in F$$

vérifie bien la propriété du lemme. □

Comme précédemment, on pose P un polynôme de degré n à coefficients dans F dont les racines sont les $r_1, ..., r_n \in K$ tel que $K \supset F$. Alors, par le rappel 2 (page 40), on a

$$P(X - r_1)...(X - r_n) = X^n - a_1 X^{n-1} + ... + (-1)^n a_n X^n,$$

où chaque $a_i \in F$ correspond au polynôme symétrique élémentaire s_i à n variables évalué en $r_1, ..., r_n$.

Passons maintenant à la proposition qui donne l'existence de la résolvante de Galois, qui correspond au Lemme 3 du "*Mémoire sur les conditions de résolubilité des équations par radicaux*" d'Evariste Galois :

Proposition 3.2.9. *Soient P un polynôme à coefficients dans F et $r_1, ..., r_n$ les racines de ce polynôme. Alors, il existe un élément $V \in F(r_1, ..., r_n)$ tel que*

$$r_i \in F(V) \text{ pour } i = 1, ..., n.$$

Démonstration. Nous montrerons l'argument pour le cas $i = 1$, auquel on se réduit par permutation des $r_1, ..., r_n$.

Soit $f \in F[x_1, ..., x_n]$ un polynôme vérifiant la propriété du lemme précédent et posons

$$V = f(r_1, ..., r_n) \in F(r_1, ..., r_n).$$

On considère le polynôme

$$g(x_1, ..., x_n) = \prod_\sigma \Big(V - f\big(x_1, \sigma(x_2), ..., \sigma(x_n)\big) \Big) \in F(V)[x_1, ..., x_n]$$

où σ décrit toutes les permutations de $x_2, ..., x_n$. Alors, g est un polynôme symétrique en les $n-1$ variables $x_2, ..., x_n$ donc, d'après le lemme 3.2.7, il peut être écrit en terme d'un polynôme en x_1 et des polynômes symétriques élémentaires $s_1, ..., s_{n-1}$ en les variables $x_1, ..., x_n$:

$$g(x_1, x_2, ..., x_n) = h(x_1, s_1, ..., s_{n-1}),$$

où h est à coefficients dans $F(V)$. Alors, en substituant les $r_1, ..., r_n$ aux $x_1, ..., x_n$, on obtient

$$g(r_1, r_2, ..., r_n) = h(r_1, a_1, ..., a_{n-1}) \tag{1}$$

De même, pour $i \neq 1$ on a

$$g(r_i, r_1, r_2, ..., r_{i-1}, r_{i+1}, ..., r_n) = h(r_i, a_1, ..., a_{n-1}). \tag{2}$$

Maintenant, utilisant le fait que f vérifie la propriété du lemme 3.2.8 et que $V = f(r_1, ..., r_n)$, nous avons

$$V \neq f\big(r_i, \sigma(r_1), \sigma(r_2), ..., \sigma(r_{i-1}), \sigma(r_{i+1}), ..., \sigma(r_n)\big)$$

pour $i \neq 1$ et pour toute permutation $\sigma \in \{r_1, ..., r_{i-1}, r_{i+1}, ..., r_n\}$. Ainsi, pour $i \neq 1$ nous avons

$$g(r_i, r_1, r_2, ..., r_{i-1}, r_{i+1}, ..., r_n) \neq 0.$$

D'autre part, les définitions de g et V nous donnent directement que

$$g(r_1, ..., r_n) = 0.$$

Cette dernière équation montre, en reprenant les équations (1) et (2) que le polynôme

$$h(X, a_1, ..., a_{n-1}) \in F(V)[X]$$

s'annule en $X = r_1$ mais pas en $X = r_i$ pour $i \neq 1$, ce qui montre qu'il est divisible par $X - r_1$ mais pas par $X - r_i$ pour $i \neq 1$.

Soit maintenant $D(X) \in F(V)[X]$ le plus grand diviseur unitaire commun de $P(X)$ et $h(X, a_1, ..., a_{n-1})$. De plus,

$$P(X) = (X - r_1)...(X - r_n) \in F(r_1, ..., r_n)[X],$$

donc D se scinde en un produit de facteurs de la forme $X - r_i$ sur $F(r_1, ..., r_n)$. D'une part, $X - r_1$ divise à la fois $P(X)$ et $h(X, a_1, ..., a_{n-1})$, donc il divise aussi D et d'autre part, comme $X - r_i$ ne divise pas $h(X, a_1, ..., a_{n-1})$ pour $i \neq 1$, on conclut que $D(X) = X - r_1$. Or comme $D \in F(V)[X]$, on trouve finalement que $r_1 \in F(V)$ ce qui achève la démonstration. □

Nous allons maintenant montrer qu'à toute résolvante de Galois d'une équation il est possible d'associer un polynôme minimal. Plus généralement, on peut le faire pour n'importe quel $u \in F(r_1, ..., r_n)$. Pour montrer ce résultat, on va utiliser la proposition suivante, qui est en fait une généralisation du théorème 2.4.3 (page 9) :

Proposition 3.2.10. *Si $u \in K$ est racine d'un polynôme irréductible de degré d à coefficients dans un corps $F \subset K$, alors tout élément de $F(u)$ peut s'écrire comme une unique $\mathbb{Q}$-combinaison linéaire des puissances de u, c'est à dire :*

$$u = a_0 + a_1 u + a_2 u^2 + ... + a_{d-1} u^{d-1} \text{ avec } a_i \in F.$$

Démonstration. Il suffit de copier la preuve du théorème 2.4.3 en remplaçant ζ par u. □

Proposition 3.2.11. *a) Pour tout $u \in F(r_1, ..., r_n)$, il existe un polynôme $\varphi \in F[x_1, ..., x_n]$ tel que*

$$u = \varphi(r_1, ..., r_n).$$

b) Pour chaque $u \in F(r_1, ..., r_n)$, il existe un unique polynôme irréductible $\pi \in F[X]$ tel que $\pi(u) = 0$. De plus, ce polynôme est scindé sur $F(r_1, ..., r_n)$.

Démonstration. La preuve de cette proposition se fera comme suit : on montrera d'abord le résultat **b)** pour des éléments $u \in F(r_1, ..., r_n)$ qui ont une expression polynômiale en terme de $r_1, ..., r_n$, puis on en déduira **a)**, ce qui permettra finalement d'achever la démonstration de **b)**.

Prenons donc pour commencer u comme décrit dans **a)** : $u = \varphi(r_1, ..., r_n)$ avec $\varphi \in F[x_1, ..., x_n]$. Il faut donc montrer que u est racine d'un polynôme à coefficients dans F qui se scinde en un produit de facteurs linéaires sur $F(r_1, ..., r_n)$. Posons alors

$$\Theta(X, x_1, ..., x_n) = \prod_{\sigma} \Big(X - \varphi\big(\sigma(x_1), ..., \sigma(x_n)\big) \Big)$$

où σ décrit l'ensemble des permutations des $x_1, ..., x_n$. A nouveau, en utilisant le rappel 3.2.7, Θ peut être écrit en terme d'un polynôme en X et des polynômes symétriques élémentaires $s_1, ..., s_n$ en $x_1, ..., x_n$. Donc il existe Ψ à coefficients dans F tel que

$$\Theta(X, x_1, ..., x_n) = \Psi(X, s_1, ..., s_n).$$

Alors, substituant $r_1, ..., r_n$ aux $x_1, ...x_n$, on obtient

$$\Theta(X, r_1, ..., r_n) = \Psi(X, a_1, ..., a_n) \in F[X].$$

Par définition de Θ,

$$\Theta(u, r_1, ..., r_n) = 0,$$

donc $\Psi(X, a_1, ..., a_n)$ est un polynôme de $F[X]$ pour lequel u est racine. De plus, puisque $\Theta(X, r_1, ..., r_n)$ est un produit de facteurs linéaires, $\Psi(X, a_1, ..., a_n)$ se scinde aussi en un produit de facteurs linéaires sur $F(r_1, ..., r_n)$.

Soit $V \in F(r_1, ..., r_n)$ une résolvante de Galois pris comme au début de la preuve de la proposition 3.2.9, c'est à dire qu'on prend f un polynôme en $x_1, ..., x_n$ qui vérifie la propriété du lemme 3.2.8 et $V = f(r_1, ..., r_n)$. Alors, puisque les $r_1, ..., r_n$ sont des fractions rationnelles en V, u est aussi une fraction rationnelle en V, donc $u \in F(V)$ et comme V a une expression polynomiale en $r_1, ..., r_n$, on peut appliquer le début de la preuve et la proposition précédente pour montrer que u peut s'écrire comme un polynôme en V :

$$u = Q(V) \text{ pour un } Q \in F[X].$$

Puis, substituant $f(r_1, ..., r_n)$ à V, on obtient

$$u = Q\big(f(r_1, ..., r_n)\big).$$

On a donc trouvé une expression pour u en terme d'un polynôme en $r_1, ..., r_n$. □

Corollaire 3.2.12. *Soient V une résolvante de Galois de l'équation $P(X) = 0$ sur un corps F et $V_1, ..., V_m$ les racines de son polynôme minimal π sur F. Alors,*

$$F(r_1, ..., r_n) = F(V) = F(V_1, ..., V_m).$$

Démonstration. Puisque $r_1, ..., r_n$ sont des fractions rationnelles en V, nous avons

$$F(r_1, ..., r_n) \subset F(V).$$

De plus, la proposition précédente nous indique les racines du polynôme minimal π sont dans $F(r_1, ..., r_n)$, donc

$$F(V_1, ..., V_m) \subset F(r_1, ..., r_n).$$

Enfin nous avons évidemment

$$F(V) \subset F(V_1, ..., V_m),$$

d'où finalement

$$F(r_1, ..., r_n) = F(V) = F(V_1, ..., V_m).$$

□

3.2.4 Exemples de construction du groupe de Galois d'une équation

D'après les définitions et propriétés qui ont été énoncées dans les partie précédentes, nous pouvons résumer les étapes intermédiaires de la détermination du groupe de Galois d'une équation donnée sur un corps comme suit :

a) trouver les racines r_i de l'équation
b) déterminer une résolvante de Galois V
c) déterminer son polynôme minimal π
d) déterminer les racines de π.

Afin d'appliquer cette méthode, nous allons construire le groupe de Galois de l'équation $P(X) = 0$ sur $\mathbb{Q}$, où P est le polynôme défini par :

$$P(X) = X^5 - X^4 - 5X^3 + 5X^2 + 6X - 6.$$

a) On peut remarquer que 1 est racine évidente de ce polynôme, ce qui donne la factorisation suivante :

$$P(X) = (X-1)(X^4 - 5X^2 + 6).$$

Ensuite, substituant X^2 à X au deuxième facteur, on trouve que

$$\begin{aligned} P(X) &= (X-1)(X^2-2)(X^2-3) \\ &= (X-1)(X-\sqrt{2})(X+\sqrt{2})(X-\sqrt{3})(X+\sqrt{3}) \end{aligned}$$

Les racines de P sont donc les

$$r_1 = 1, \quad r_2 = \sqrt{2}, \quad r_3 = -\sqrt{2} \quad r_4 = \sqrt{3} \quad r_5 = -\sqrt{3}.$$

b) Posons

$$V = r_2 + r_3 = \sqrt{2} + \sqrt{3}$$

et montrons que V vérifie bien la définition d'une résolvante de Galois pour l'équation $P(X) = 0$. C'est bien une fraction rationnelle en r_i, il reste donc à montrer que, pour $i = 1, ..., n$, r_i est une fraction rationnelle de V.

On a déjà trivialement que $r_1 = 1$ est une fraction rationnelle de V. Si on écrit $V - r_2 = r_4$ on a, en élevant cette équation au carré,

$$V^2 - 2r_2V + 2 = 3,$$

ce qui donne que

$$r_2 = \frac{V^2 - 1}{2V} \qquad r_3 = -r_2 = \frac{1 - V^2}{2V}.$$

De même, en écrivant $V - r_4 = r_2$ et en élevant au carré, on a

$$V^2 - 2r_4V + 3 = 2,$$

ce qui donne que

$$r_4 = \frac{V^2 + 1}{2V} \qquad r_5 = -r_4 = \frac{-1 - V^2}{2V}.$$

Ceci prouve bien que toutes les racines de P sont des fractions rationnelles de V, donc cette dernière est bien une résolvante de Galois de l'équation $P(X) = 0$ sur le corps $\mathbb{Q}$.

c) Si on reprend par exemple l'expression de r_2 en fonction de V, on a, en élevant au carré :

$$2 = \frac{V^4 - 2V^2 + 1}{4V^2} \quad \Leftrightarrow \quad V^4 - 10V^2 + 1 = 0.$$

On déduit de cette équivalence que $X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$ est bien annulateur de V. De plus, on trouve facilement, en substituant X^2 à X, que

$$X^4 + 10X^2 + 1 = \big(X - (\sqrt{2} + \sqrt{3})\big)\big(X - (\sqrt{2} - \sqrt{3})\big)\big(X - (-\sqrt{2} + \sqrt{3})\big)\big(X - (-\sqrt{2} - \sqrt{3})\big),$$

ce qui montre qu'il n'existe pas de polynôme (non trivial) à coefficients rationnels qui divise $X^4 + 10X^2 + 1$. Ce dernier est donc irréductible à coefficients dans $\mathbb{Q}$ et annulateur de V, on en conclut que $\pi(X) = X^4 + 10X^2 + 1$ est bien le polynôme minimal de V sur $\mathbb{Q}$.

d) Par la partie **c)** on a directement les racines du polynôme π :

$$V_1 = V = \sqrt{2} + \sqrt{3}, \quad V_2 = \sqrt{2} - \sqrt{3},$$
$$V_3 = -\sqrt{2} + \sqrt{3}, \quad V_4 = -\sqrt{2} - \sqrt{3}.$$

Nous avons à présent tout ce qu'il faut pour déterminer le groupe de Galois $Gal(P/F)$: en effet, le but est de trouver les $f_i \in F(V)$ pour chaque $i \in \{1, ..., 5\}$ qui vérifie $r_i = f_i(V)$. Ces f_i sont en fait donnés par les fractions rationnelles de chaque r_i en fonction de V que nous avons explicitées à la partie **b)**, d'où :

$$f_1(X) = 1 \quad f_2(X) = \frac{X^2 - 1}{2X} \quad f_3(X) = -f_2(X) = \frac{1 - X^2}{2X}$$
$$f_4(X) = \frac{X^2 + 1}{2X} \quad f_5(X) = -f_4(X) = \frac{-1 - X^2}{2X}.$$

Enfin, par construction du groupe de Galois $Gal(P/F)$, nous avons, pour $j = 1, ..., 4$:

$$\sigma_j : r_i \mapsto f_i(V_j),$$

ce qui permet de déterminer explicitement chaque σ_j. On trouve finalement les relations suivantes :

$$\sigma_1 : \begin{cases} r_1 \mapsto r_1 \\ r_2 \mapsto r_2 \\ r_3 \mapsto r_3 \\ r_4 \mapsto r_4 \\ r_5 \mapsto r_5 \end{cases} ; \quad \sigma_2 : \begin{cases} r_1 \mapsto r_1 \\ r_2 \mapsto r_2 \\ r_3 \mapsto r_3 \\ r_4 \mapsto r_5 \\ r_5 \mapsto r_4 \end{cases} ; \quad \sigma_3 : \begin{cases} r_1 \mapsto r_1 \\ r_2 \mapsto r_3 \\ r_3 \mapsto r_2 \\ r_4 \mapsto r_4 \\ r_5 \mapsto r_5 \end{cases} ; \quad \sigma_4 : \begin{cases} r_1 \mapsto r_1 \\ r_2 \mapsto r_3 \\ r_3 \mapsto r_2 \\ r_4 \mapsto r_5 \\ r_5 \mapsto r_4 \end{cases}$$

En outre, le groupe de Galois de l'équation $P(X) = 0$ est le groupe des automorphismes qui fixent r_1 et qui permutent les racines r_2, r_3 et r_4, r_5.

Remarque : Si on reprend la factorisation de P suivante : $P(X) = (X - 1)(X^2 - 1)(X^3 - 3)$, on peut constater qu'une racine d'un même facteur est envoyée sur l'autre racine du même facteur, mais jamais sur une racine d'un autre facteur. C'est logique compte tenu du fait que, par exemple, la racine $r_2 = \sqrt{2}$ vérifie $r_2^2 - 2 = 0$, ce qui n'est le cas ni pour r_4 ni pour r_5. Les permutations σ_1, σ_2, σ_3 et σ_4 décrites ci-dessus sont en fait les seuls automorphismes à préserver ces relations au sein racines.

Traitons à présent un exemple un peu moins concret mais que nous avons longuement évoqué au cours du premier chapitre, celui de l'équation cyclotomique de degré $p - 1$ avec p un nombre premier :

$$\Phi_p(X) = X^{p-1} + X^{p-2} + ... + X + 1 = 0.$$

Commençons par prendre ζ une racine primitive $p^{\text{ième}}$ de l'unité quelconque, qui est évidemment racine de Φ_p. Comme toutes les autres racines de Φ_p sont les puissances de ζ, on peut prendre ζ comme résolvante de Galois de l'équation $\Phi_p(X) = 0$. De plus, nous avons montré au théorème 2.3.1 (page 5) que $\Phi_p(X)$ est irréductible sur $\mathbb{Q}$, c'est donc le polynôme minimal de ζ sur $\mathbb{Q}$. De plus, si on choisit g une racine primitive modulo p, on peut poser, pour $i = 0, ..., p - 2$,

$$\zeta_i = \zeta^{g^i}.$$

Ainsi, les racines de Φ_p sont les $\zeta_0, ..., \zeta_{p-2}$, ce qui permet de définir les fractions rationnelles f_i par la relation suivante :

$$f_i(X) = X^{g^i}.$$

D'après la définition de $Gal(\Phi_p/\mathbb{Q})$, les automorphismes qui permutent les racines de Φ_p sont les

$$\sigma_j : \zeta_i \mapsto f_i(\zeta_j) \text{ pour } j = 0, ..., p - 2.$$

De plus, nous avons

$$f_i(\zeta_j) = (\zeta^{g^i})^{g^j} = \zeta^{g^{i+j}} = \zeta_{i+j},$$

d'où finalement

$$\sigma_j : \zeta_i \mapsto \zeta_{i+j}.$$

3.3 Comportement du groupe de Galois sous extension de corps

Dans cette partie, on considère K un corps contenant F comme sous-corps (autrement dit K est une **extension du corps** F que l'on note K/F), et on construit K par **adjonction de racines** à F. Cela signifie que, partant du corps F et d'une équation $P(X) = 0$ où P est un polynôme à coefficients dans F, on construit K en lui ajoutant une ou plusieurs racines de P, ce qui donne un corps plus gros dans lequel P se factorise. On dit en fait que K/F est une **extension algébrique** et on note $K = F(r_1, ..., r_k)$, où les r_i sont les racines de P qu'on a ajoutées au corps F, avec $k \leq \deg P = n$. On peut aussi construire K en lui ajoutant les racines de plusieurs polynômes à coefficients dans F.

Le but de cette partie va être d'identifier les liens qu'il peut y avoir entre $Gal(P/K)$ et $Gal(P/F)$. Pour commencer, on a le résultat suivant :

Proposition 3.3.1. *Si K est un corps contenant F, alors $Gal(P/K)$ est un sous-groupe de $Gal(P/F)$.*

Démonstration. Il est clair que $Gal(P/K)$ possède la structure d'un sous-groupe du groupe de toutes les permutations des racines de P. Montrons donc que $Gal(P/K) \subset Gal(P/F)$.

Soit V une résolvante de Galois de l'équation $P(X) = 0$ sur F. Par définition

$$r_i \in F(V) \text{ pour } i = 1, ..., n,$$

et comme $F(V) \subset K(V)$, on a en particulier $r_i \in K(V)$ et donc la même fraction f_i peut être utilisée pour déterminer $Gal(P/K)$ et $Gal(P/F)$. Cependant, il se peut que le polynôme minimal π de V sur F ne soit pas irréductible sur K.

Soit θ le polynôme minimal de V sur K. Alors θ et π sont tous deux à coefficients dans K et ont une racine en commun dans $K(V) \supset K$ donc, d'après le lemme 2.4.4 (page 9), θ divise π et par conséquent, l'ensemble des racines de θ est inclus dans l'ensemble des racines de π. De plus si V' est une des racines de θ, les permutations de $Gal(P/K)$ sont de la forme

$$\sigma : r_i \mapsto f_i(V') \text{ pour } i = 1, ..., n$$

et nous avons la même construction si V' est une racine de π, d'où l'inclusion recherchée. □

On va maintenant construire K par adjonction à F de racines d'un polynôme **irréductible** sur F. On pose T ce polynôme et on note t son degré. Alors comme F est de caractéristique nulle, le polynôme dérivé T' de T est non nul. Comme T est irréductible, T et T' sont premiers entre eux, ce qui implique que T est scindé à racines simples dans un corps convenable, par exemple un corps K qui contient les $u_1, ..., u_t$:

$$T(X) = (X - u_1)...(X - u_t)$$

avec les $u_1, ..., u_t$ deux à deux distinctes.

Définition : On appelle **indice** de $Gal(P/K)$ dans $Gal(P/F)$ le nombre $\frac{|Gal(P/K)|}{|Gal(P/F)|}$.

Supposons dans un premier temps qu'on construit K en lui ajoutant une racine du polynôme T, disons u_1. On a alors le résultat suivant :

Théorème 3.3.2. *L'indice de $Gal\big(P/F(u_1)\big)$ dans $Gal(P/F)$ divise t.*

Démonstration. Soit V une résolvante de Galois de l'équation $P(X) = 0$ sur F. D'après la proposition 3.3.1, V est aussi une résolvante de Galois de la même équation sur le corps $F(u_1)$. Posons θ et π les polynômes minimaux de V sur respectivement $F(u_1)$ et F. Ainsi, pour montrer le résultat de la proposition, on peut de manière équivalente montrer que

$$\tfrac{\deg \pi}{\deg \theta} \text{ divise } t.$$

A nouveau d'après lemme 2.4.4 (page 9), θ divise π, autrement dit il existe un polynôme $\lambda \in F(u_1)[X]$ tel que

$$\pi = \theta\lambda. \tag{1}$$

De plus, on a

$$\theta(X) = X^r + b_{r-1}X^{r-1} + ... + b_1X + b_0 \text{ avec } b_i \in F(u_1).$$

Alors, appliquant la proposition 3.2.10, les $b_0, ..., b_{r-1}$ ont une expression polynômiale en u_1 :

$$b_i = \theta_i(u_1) \text{ pour } i = 0, ..., r-1 \text{ et un certain } \theta_i \in F[Y].$$

De plus, posons

$$\Theta(X, Y) = X^r + \theta_{r-1}(Y)X^{r-1} + ... + \theta_1(Y)X + \theta_0(Y) \in F[X, Y] \text{ si bien que } \Theta(X, u_1) = \theta(X).$$

On fait la même chose avec λ, en posant

$$\Lambda(X, Y) = X^r + \lambda_{r-1}(Y)X^{r-1} + ... + \lambda_1(Y)X + \lambda_0(Y) \in F[X, Y] \text{ si bien que } \Lambda(X, u_1) = \lambda(X).$$

Ainsi, l'équation (1) se réécrit

$$\pi(X) = \Theta(X, u_1)\Lambda(X, u_1),$$

ce qui implique directement que

$$\pi(X) = \Theta(X, u_i)\Lambda(X, u_i) \text{ pour } i = 1, ..., t,$$

d'où, en multipliant ces deux équations,

$$\pi(X)^t = \Theta(X, u_1)...\Theta(X, u_t)\Lambda(X, u_1)...\Lambda(X, u_t) \in F(u_1, ..., u_t)[X].$$

Par ailleurs, le polynôme $\Theta(X, Y_1)...\Theta(X, Y_t)$ est symétrique en les variables $Y_1, ..., Y_t$: il peut donc être exprimé en terme d'un polynôme en X et des polynômes symétriques élémentaires en $Y_1, ..., Y_t$. Alors, substituant $u_1, ..., u_t$ aux $Y_1, ..., Y_t$, on trouve un polynôme en X dont les racines sont exactement ces $u_1, ..., u_t$. Comme T est un polynôme à coefficients dans F, nous avons

$$\Theta(X, u_1)...\Theta(X, u_t) \in F[X].$$

D'autre part, l'équation (2) montre que ce produit divise $\pi(X)^t$. Mais π étant le polynôme minimal de V sur F, il est irréductible sur ce corps et donc en fait

$$\Theta(X, u_1)...\Theta(X, u_t) = \pi(X)^k$$

pour un certain entier k tel que $1 \leq k \leq t$. Enfin, comparant les degrés des deux côtés de cette équation, on a

$$tr = k \deg \pi$$

et puisque $r = \deg \theta$, on a finalement que le quotient $\frac{\deg \pi}{\deg \theta}$ divise t, ce qui est bien équivalent au fait que le quotient $\frac{\left|Gal\big(P/F(u_1)\big)\right|}{|Gal(P/F)|}$ divise t. □

On construit maintenant K en lui ajoutant toutes les racines de T, ce qui donne le résultat fondamental suivant :

Théorème 3.3.3. *Le groupe de Galois $Gal\big(P/F(u_1, ..., u_t)\big)$ vérifie la propriété suivante : si $\sigma \in Gal(P/F)$ et $\tau \in Gal\big(P/F(u_1, ..., u_t)\big)$ alors*

$$\sigma \circ \tau \circ \sigma^{-1} \in Gal\big(P/F(u_1, ..., u_t)\big).$$

Remarque : On dit que le groupe $Gal\big(F(u_1, ..., u_t)\big)$ est **distingué** dans $Gal(P/F)$ et on note $Gal\big(F(u_1, ..., u_t)\big) \triangleleft Gal(P/F)$.

Pour démontrer ce théorème, nous aurons besoin de ce lemme :

Lemme 3.3.4. *Soient π un polynôme irréductible sur un corps F et K un corps contenant F tel que π se scinde en un produit de facteurs linéaires sur K. Posons aussi f, g et $h \in F[X, Y]$. Alors, si pour une certaine racine $V \in K$ de π on a*

$$f(X, V) = g(X, V)h(X, V) \in K[X]$$

alors

$$f(X, W) = g(X, W)h(X, W) \in K[X]$$

pour toute racine W de π.

Démonstration. On peut voir f, g et h comme des polynômes en X sur $F[Y]$, autrement dit il existe $c_r(Y), ..., c_0(Y) \in F[Y]$ tels que

$$f(X,Y) - g(X,Y)h(X,Y) = c_r(X)X^r + ... + c_0(Y).$$

Si on suppose que

$$f(X,V) = g(X,V)h(X,V),$$

alors

$$c_i(V) = 0 \text{ pour } i = 0, ..., r.$$

D'après le lemme 3.2.1, on a aussi pour tout racine W de π :

$$c_i(W) = 0 \text{ pour } i = 0, ..., r,$$

ce qui implique donc que

$$f(X,W) = g(X,W)h(X,W).$$

□

Passons maintenant à la démonstration du théorème 3.3.3 :

Démonstration. Soit V une résolvante de Galois de l'équation $P(X) = 0$ sur F, donc a fortiori sur $F(u_1, ..., u_t)$. Comme pour la démonstration du théorème 3.3.2, posons φ et π les polynômes minimaux de V sur respectivement $F(u_1, .., u_t)$ et F. Posons aussi $f_1, ..., f_n \in F(X)$ les fractions rationnelles telles que $r_i = f_i(V)$, pour $i = 1, ..., n$. Toute permutation $\tau \in Gal\big(P/F(u_1, ..., u_n)\big)$ est de la forme

$$\tau : r_i = f_i(V) \mapsto f_i(V') \tag{1}$$

pour $i = 1, ..., n$, où V' est racine du polynôme φ. Par définition de π et de V, on a

$$\pi(V) = 0.$$

Alors d'après le corollaire 3.2.4, si $\sigma \in Gal(P/F)$, σ peut être étendu à un automorphisme de $F(r_1, ..., r_n)$ qui fixe F donc, appliquant σ à l'équation précédente,

$$\pi\big(\sigma(V)\big) = 0,$$

d'où $\sigma(V)$ est aussi une racine de π. Ainsi, par la proposition 3.2.2, toute racine $r_1, ..., r_n$ du polynôme P est une fraction rationnelle de $\sigma(V)$. Autrement dit, $\sigma(V)$ est une résolvante de Galois de $P(X) = 0$ sur F, et donc a fortiori sur $F(u_1, ..., u_t)$.

D'autre part le corollaire 3.2.5 montre que le groupe $Gal\big(P/F(u_1, ..., u_t)\big)$ne dépend pas du choix de la résolvante de Galois, donc par l'équation (1) on a

$$\sigma \circ \tau \circ \sigma^{-1} : f_i\big(\sigma(V)\big) \mapsto f_i\big(\sigma(V')\big).$$

En outre, pour prouver que $\sigma \circ \tau \circ \sigma^{-1} \in Gal\big(P/F(u_1, ..., u_t)\big)$, il suffit de montrer que $\sigma(V')$ est racine du polynôme minimal de $\sigma(V)$ sur $F(u_1, ..., u_t)$.

Cherchons donc dans un premier temps le polynôme minimal de $\sigma(V)$ sur $F(u_1, ..., u_t)$. Soient W une résolvante de Galois de l'équation $T(X) = 0$ et $W_1, ..., W_s$ les racines du polynôme minimal de W sur F, où W est l'un des W_i. Alors d'après le corollaire 3.2.12 (page 26), nous avons

$$F(u_1, ..., u_t) = F(W) = F(W_1, ..., W_s).$$

De plus, comme $W \in \{W_1, ..., W_s\}$, on a aussi

$$F(u_1, ..., u_t) = F(W_i) \text{ pour un certain } i = 1, ..., s.$$

Imitant la preuve du théorème 3.3.2, on construit $\Phi(X,Y) \in F[X,Y]$ tel que

$$\varphi(X) = \Phi(X, W_1) \in F(u_1, ..., u_t)[X],$$

et on obtient

$$\pi(X)^l = \Phi(X, W_1)...\Phi(X, W_s)$$

pour un certain entier l tel que $1 \leq l \leq s$. Cette équation montre entre autre que $\sigma(V)$ est racine de $\Phi(X, W_k)$, donc pour prouver que c'est son polynôme minimal sur F, il suffit de montrer qu'il est irréductible sur F.

Supposons qu'il se factorise sur $F(u_1, ..., u_t)$. Alors, puisque $F(u_1, ..., u_t) = F(W_k)$, il existe Γ et Δ deux polynômes à coefficients dans F tels que

$$\Phi(X, W_1) = \Gamma(X, W_k)\Delta(X, W_k).$$

D'après le lemme 3.3.4,

$$\Phi(X, W_1) = \Gamma(X, W_1)\Delta(X, W_1),$$

et comme $\varphi(X) = \Phi(X, W_1)$ et que φ est irréductible, cette factorisation est triviale. On en conclut que $\Phi(X, W_k)$ est irréductible et est le polynôme minimal de $\sigma(V)$ sur $F(u_1, ..., u_t)$.

Montrons maintenant que ce polynôme est annulateur de $\sigma(V')$. Supposons que V' est racine de $\Phi(X, W_1)$. D'après le corollaire 3.2.12, $F(r_1, ..., r_n) = F(V)$ et donc il existe une fraction $g \in F(X)$ telle que

$$V' = g(V).$$

De plus, puisque $\Phi(V', W_1) = 0$, on a

$$\Phi(g(V), W_1) = 0,$$

donc V est racine du polynôme $\Phi\big(g(X), W_1\big) \in F(u_1, ..., u_t)[X]$ et par le lemme 2.4.4 (page 9), $\Phi(X, W_1)$ divise $\Phi\big(g(X), W_1\big)$.Autrement dit

$$\Phi\big(g(X), W_1\big) = \Phi(X, W_1)\Psi(X, W_k)$$

pour un certain $\Psi \in F[X,Y]$. Alors, d'après le lemme 3.3.4, on a

$$\Phi\big(g(X), W_k\big) = \Phi(X, W_k)\Psi(X, W_k),$$

et puisque $\sigma(V)$ est racine de $\Phi(X, W_k)$, on a

$$\Phi\Big(g\big(\sigma(V)\big), W_k\Big) = 0.$$

Alors, appliquant σ à l'équation $V' = g(V)$, on obtient

$$\sigma(V') = g\big(\sigma(V)\big)$$

et par l'équation précédente $\sigma(V')$ est racine de $\Phi(X, W_k)$, ce qui achève la démonstration. □

Remarque : Ce théorème ne fournit pas de résultat concret sur l'indice de $Gal\big(P/F(u_1, ..., u_t)\big)$ dans $Gal(P/F)$, mais on peut utiliser le théorème 3.3.2 pour avoir des informations supplémentaires sur cet indice : en effet, puisque u_2 est racine du polynôme

$$\frac{T(X)}{X - u_1} \in F(u_1)[X],$$

qui est de degré $t-1$, il s'en suit que le degré du polynôme minimal de u_2 sur $F(u_1)$ est au moins $t-1$, donc par le théorème 3.3.2, on a

$$\frac{\mid Gal\big(P/F(u_1)\big) \mid}{\mid Gal\big(P/F(u_1, u_2)\big) \mid} \leq t - 1.$$

Alors, on a naturellement que

$$\frac{|\ Gal(P/F)\ |}{|\ Gal\big(P/F(u_1,u_2)\big)\ |} = \frac{|\ Gal(P/F)\ |}{|\ Gal\big(P/F(u_1)\ |} \cdot \frac{|\ Gal\big(P/F(u_1)\big)\ |}{|\ Gal\big(P/F(u_1,u_2)\big)\ |} \leq t(t-1),$$

et donc par récurrence

$$\frac{|\ Gal(P/F)\ |}{|\ Gal\big(P/F(u_1,...,u_t)\big)\ |} = \frac{|\ Gal(P/F)\ |}{|\ Gal\big(P/F(u_1)\big)\ |} \cdot \frac{|\ Gal\big(P/F(u_1)\big)\ |}{|\ Gal\big(P/F(u_1,u_2)\big)\ |} ... \frac{|\ Gal\big(P/F(u_1,...,u_{t-1})\big)\ |}{|\ Gal\big(P/F(u_1,...,u_t)\big)\ |} \leq t!.$$

Nous pouvons maintenant introduire la notion d'extension radicielle de corps, qui servira à donner un dernier résultat sur l'indice du groupe $Gal(P/K)$ dans $Gal(P/F)$, mais qui est surtout indispensable à la partie suivante de ce chapitre.

Définitions : 1) Soit K/F une extension de corps. On dit que K/F est une **extension radicielle de taille** 1 s'il existe un nombre premier p, un élément $a \in F$ qui n'est pas une puissance $p^{\text{ième}}$ dans F et un élément $u \in K$ tels que

$$K = F(u) \text{ et } u^p = a.$$

2) Soit $t \in \mathbb{N}$. On dit que K/F est une **extension radicielle de taille** t s'il existe un corps K_1, avec $F \subset K_1 \subset K$, tel que K/K_1 est une extension radicielle de taille 1 et K_1/F est une extension radicielle de taille $t-1$. Dans ce cas, il existe une suite de sous-corps $K_1, K_2, ..., K_{t-1}$ telles que

$$F = K_t \subset K_{t-1} \subset ... \subset K_2 \subset K_1 \subset K_0 = K$$

et

$$K_i = K_{i+1}(u_i)$$

avec p_i un nombre premier et $u_i^p = a_i \in K_{i+1}$ tel que a_i n'est pas une puissance $p_i^{\text{ième}}$ dans K_{i+1}.

Remarques : 1) On dit aussi simplement que K/F est une extension radicielle.
2) Par la suite on se permettra de noter $u = a^{1/p}$.
3) Tout corps F est une extension radicielle de lui-même de taille 0.

Corollaire 3.3.5. *Soit K/F une extension radicielle de taille* 1. *Si F contient une racine primitive $p^{\text{ième}}$ de l'unité, alors $Gal(P/K)$ est un sous-groupe d'indice* 1 *ou p dans $Gal(P/F)$.*

Démonstration. On considère le polynôme

$$T(X) = X^p - a$$

irréductible sur F. Par hypothèse, F contient une racine primitive $p^{\text{ième}}$ de l'unité que l'on note ζ, donc si on adjoint $u = a^{1/p}$ une racine de T au corps F, alors on les adjoint toutes. En effet, les racines de T sont de la forme $u, \zeta u, \zeta^2 u, ..., \zeta^{p-1} u$. Autrement dit, on construit K de la façon suivante :

$$K = F(u) = F(u, \zeta u, \zeta^2 u, ..., \zeta^{p-1} u)$$

et donc $Gal(P/K)$ est bien un sous-groupe distingué de $Gal(P/F)$ par la proposition 3.3.1 et le théorème 3.3.3 et le nombre $\frac{|Gal(P/K)|}{|Gal(P/F)|}$ est un diviseur de p, donc il vaut bien soit 1 soit p. □

3.4 Résolubilité par radicaux

Le but de cette partie est de démontrer la Proposition 5 du *"Mémoire sur les conditions de résolubilité des équations par radicaux"* d'Evariste Galois, qui donne une condition nécessaire et suffisante sur ce que Galois appelle la "complète résolubilité" d'une équation.

Pour démontrer ce résultat, nous utiliserons comme annoncé la notion essentielle d'**extension radicielle** introduite précédemment ainsi que des résultats relatifs à cette notion que nous démontrerons par la suite, mais aussi des résultats de théories des groupes qui sont énoncés dans la partie "Rappels" page 40.

Définitions : **1)** Soit P un polynôme à coefficients dans un corps F. L'équation $P(X) = 0$ est dite **résoluble par radicaux sur** F s'il existe une extension radicielle de F qui contient une racine de cette équation (autrement dit une racine de P).
2) L'équation $P(X) = 0$ est dite **complètement résoluble par radicaux sur** F s'il existe une extension radicielle de F qui contient toutes les racines de cette équation.

Définition : Un groupe fini G est dit **résoluble** s'il existe une suite de sous-groupes $G_0, G_1, ..., G_t$ tels que

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_t = \{id\}$$

et tels que, pour $i = 1, ..., t$ le sous-groupe G_i est distingué dans G_{i-1} et l'indice de G_i dans G_{i-1} est un nombre premier.

Proposition 3.4.1. *Soient K un corps contenant F et $u \in K$ tel que $u^n \in F$ avec $n \in \mathbb{N}$. Si $K = F(u)$ et que F contient une racine primitive $n^{\text{ième}}$ de l'unité, alors K/F est une extension radicielle.*

Démonstration. On raisonne par récurrence forte sur n, en distinguant le cas où n est un nombre premier et le cas où n ne l'est pas. Si $n = 1$, alors $u \in F$ donc il suffit de prendre $K = F$ et F est une extension radicielle (de taille 0). Supposons donc que la proposition est vraie pour tout entier $k < n$. Si n n'est pas premier, alors il existe $r, s \in \mathbb{N}$ tels que $n = rs$ et $r, s < n$. Alors, par hypothèse de récurrence, $F(u)$ est une extension radicielle de $F(u^r)$ et $F(u^r)$ est une extension radicielle de F (puisque $(u^r)^s \in F$). Alors, comme $F \subset F(u^r) \subset F(u)$, $F(u)$ est une extension radicielle de F.

Si n est un nombre premier, alors il faut distinguer le cas où u^n est une puissance $n^{\text{ième}}$ d'un élément de F et où il ne l'est pas. S'il ne l'est pas, alors K est par définition une extension radicielle. S'il l'est, alors il existe $b \in F$ tel que

$$u^n = b^n,$$

donc soit $b = 0 \Rightarrow u = 0$ et donc $K = F$ est une extension radicielle de taille 0, soit $b \neq 0$ et on a

$$\left(\frac{u}{b}\right)^n = 1,$$

donc u/b est une racine $n^{\text{ième}}$ de l'unité. Ainsi, comme F possède toutes les racines $n^{\text{ièmes}}$ de l'unité (puisqu'il en possède une par hypothèse) $u/b \in F$, et donc $u \in F$ ce qui donne à nouveau $K = F$. □

Proposition 3.4.2. *Pour tout entier n strictement positif et tout corps F, les racines $n^{\text{ièmes}}$ de l'unité sont contenues dans une extension radicielle de F.*

Démonstration. Soit ζ une racine primitive $n^{\text{ième}}$ de l'unité. Comme les racines $n^{\text{ièmes}}$ sont des puissances de ζ, il suffit de montrer le résultat pour ζ. A nouveau, on raisonne par récurrence sur n et en distinguant si n est premier ou non. Pour $n = 1$, on a $\zeta = 1$ donc $\zeta \in F$ qui est bien une extension radicielle de taille 0. Supposons donc le proposition vrai pour tout entier $k < n$. Si n n'est pas premier, on peut écrire $n = rs$ avec $r, s \in \mathbb{N}$. Alors, ζ^r est une racine $s^{\text{ième}}$ de l'unité et par hypothèse de récurrence, on peut trouver une extension K_1/F qui contienne ζ^r. De même, on peut trouver une extension radicielle K_2/K_1 qui contient une racine primitive $r^{\text{ième}}$ de l'unité. Alors d'après la proposition précédente, comme $\zeta^r \in K_2$, $K_2(\zeta)$ est une extension radicielle de K_2, donc de F, ce qui achève la démonstration quand n n'est pas premier.

Dans le cas contraire, on peut, par hypothèse de récurrence, trouver une extension radicielle K_1/F qui contient les racines $(n-1)^{\text{ièmes}}$ de l'unité. On considère alors la résolvante de Lagrange $t(\omega)$ que nous avons introduite page 16 avec $x_i = \zeta_i$. Par la proposition 2.5.1, nous avons

$$t(\omega)^{n-1} \in K_1$$

avec ω une racine $(n-1)^{\text{ièmes}}$ de l'unité. Alors, par la proposition précédente, $K_1\big(t(\omega)\big)$ est une extension radicielle de K_1. En répétant cela avec toutes les résolvantes de Lagrange, on trouvera une extension K_2 de K_1 et donc de F qui contient $t(\omega)$ pour tout $\omega \in \mu_{n-1}$. Enfin, d'après la formule de Lagrange (page 16), ζ peut être calculée rationnellement à partir des résolvantes de Lagrange, donc $\zeta \in K_2$, ce qui complète la démonstration. □

Lemme 3.4.3. *Soit L un corps contenant F. Pour toute extension radicielle K/F, il existe une extension radicielle S/L telle que K est un sous-corps de S.*

Démonstration. Soit $t \in \mathbb{N}$ la taille de l'extension K/F. Le raisonnement se fait par récurrence sur t : si $t = 0$, alors on prend $K = F$ et $S = L$ et la proposition est vérifiée. Pour l'hérédité, nous aurons besoin de considérer le cas où $t = 1$: dans ce cas, on peut poser $K = F(u)$ où u est tel que $u^p = a$ pour un certain $a \in F$ qui n'est pas une puissance $p^{\text{ième}}$ dans F. Soit M un corps tel que $L, K \subset M$ et dans lequel le polynôme $X^p - a$ se factorise en un produit de facteurs linéaires. Puisque u est une racine de ce polynôme, il peut être identifié à un élément de M, et toute fraction rationnelle en u à coefficients dans F, c'est à dire en fait tout élément de K peut être identifié à un élément de M. D'une part, si a n'est pas une puissance $p^{\text{ième}}$ dans L, alors $L(u)$ est une extension radicielle de taille 1 de L, et cette extension contient K donc elle satisfait bien les conditions du théorème. D'autre part, si a est une puissance $p^{\text{ième}}$ dans L, alors il existe un $b \in L$ tel que

$$b^p = a,$$

ce qui implique directement que

$$\left(\frac{u}{b}\right)^p = 1.$$

Alors, u/p est une puissance $p^{\text{ième}}$ de l'unité et donc par la proposition 3.4.1, il existe une extension radicielle S/L qui continet u/b. Puisque $b \in L$, on a $u \in S$ et donc $K \subset S$ donc le preuve est complète pour le cas $t = 1$.

Supposons maintenant que la proposition est vérifiée pour tout entier $k < t$. Alors par définition de K/F, on peut trouver un sous-corps K_1 de K qui soit une extension radicielle de taille $t - 1$ de F et telle que K soit une extension radicielle de taille 1 de K_1. Par hypothèse de récurrence, K_1 contient une extension radicielle S_1 de L et par le cas $t = 1$, K peut être identifié à un sous-corps d'une extension radicielle S/S_1. Le corps S est donc une extension radicielle de L qui satisfait bien les conditions du lemme. □

Proposition 3.4.4. *Soit P un polynôme à coefficients dans un corps F. Si l'équation $P(X) = 0$ est résoluble par radicaux sur le corps F, alors elle est résoluble par radicaux sur tout corps L contenant F.*

Démonstration. Soit K/F une extension radicielle telle que $r \in K$ où r est une racine de P. Il suffit alors d'appliquer le lemme précédent, puisqu'on peut supposer qu'il existe une extension radicielle S/L qui contiennent K. Alors, $r \in S$ et donc l'équation $P(X) = 0$ est résoluble par radicaux sur L. □

Lemme 3.4.5. *Soit N un sous-groupe distingué d'indice premier dans $Gal(P/F)$. Si F possède une racine primitive $p^{\text{ième}}$ de l'unité, alors il existe une extension radicielle K/F dans $F(r_1, ..., r_n)$ qui soit de la forme*

$$K = F(a^{1/p})$$

pour un certain $a \in F$, et telle que $Gal(P/K) = N$.

Démonstration. La preuve de ce lemme va se faire en cinq étapes, où chacune de ces étapes permettra de donner un résultat intermédiaire au résultat annoncé, jusqu'à finalement arriver à ce dernier. On commence par poser $\sigma \in Gal(P/F)$ tel que $\sigma \notin N$.

Étape 1 : Posons $x \in F(x_1, ..., x_n)$ tel que $\nu(x) = x$ pour tout $\nu \in N$ et X le sous-groupe des permutations de $Gal(P/F)$ qui fixent x, autrement dit

$$X = \{\tau \in Gal(P/F) \mid \tau(x) = x\}.$$

Comme x est fixé par toutes permutations de N, on a

$$N \subset X \subset Gal(P/F).$$

Or l'indice de N dans $Gal(P/F)$ est un nombre premier, donc par le rappel 4 on a

$$\text{soit } X = N \text{ soit } X = Gal(P/F).$$

Si $\sigma(x) = x$, alors $\sigma \in X$ et donc $X \neq N$ puisqu'on a pris $\sigma \notin N$. Ainsi $X = Gal(P/F)$ et donc par le théorème 3), on a $x \in F$.
Si $\sigma(x) \neq x$, alors $\sigma \notin X$, donc $X \neq Gal(P/F)$. Ainsi $X = N$, donc toutes les permutations de $Gal(P/F)$ qui fixent x est dans N.

Cette étape a donc permis de montrer que si $\sigma(x) = x$, alors $\sigma \in X$ et sinon, si on suppose de plus que $\tau(x) = x$ pour un certain $\tau \in Gal(P/F)$, alors $\tau \in N$.

Étape 2 : Posons $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ qui possède la propriété du lemme 3.2.8 (page 24), c'est à dire que les $n!$ éléments de $F(r_1, ..., r_n)$ qui sont obtenus en substituant $r_1, ..., r_n$ aux $x_1, ..., x_n$ de toutes les façons possibles sont deux à deux distincts. Posons aussi $V = f(r_1, ..., r_n)$. et considérons le polynôme

$$\prod_{\nu \in N} \big(X - \nu(V)\big).$$

Les coefficients de ce polynôme son clairement invariants sous N. S'ils étaient tous dans F, alors V serait racine du polynôme de degré $\mid N \mid$ sur F, ce qui est impossible car le degré du polynôme minimal de V sur F est de degré $\mid Gal(P/F) \mid$, qui est clairement supérieur à $\mid N \mid$. Cette étape a donc permis de montré qu'il existe au moins un des coefficients de ce polynôme qui n'est pas dans F, tout en étant fixé par toutes permutations de N. On appelle cet élément v, et pour toutes racines $p^{\text{ième}}$ de l'unité $\omega \in F$, on définit la résolvante de Lagrange suivante :

$$t(\omega) = v + \omega\sigma(v)) + ... + \omega^{p-1}\sigma^{p-1}(v).$$

Étape 3 : On veut montrer ici que $\sigma\big(t(\omega)\big) = \omega^{-1}t(\omega)$ et $\nu\big(t(\omega)\big) = t(\omega)$ pour tout $\nu \in N$.

Toutes les puissances de ω sont dans F, elles sont donc invariantes par toutes permutations de $Gal(P/F)$ d'après le théorème 3.2.3 (page 21).

$$\sigma\big(t(\omega)\big) = \sigma(\nu) + \omega\sigma^2(\nu) + ... + \omega^{p-1}\sigma^p(\nu),$$

ce qui est équivalent à

$$\sigma\big(t(\omega)\big) = \omega^{-1}\big(\sigma^p(\nu) + \omega\sigma(\nu) + ... + \omega^{p-1}\sigma^{p-1}(\nu)\big),$$

et de même, pour tout $\nu \in N$,

$$\nu\big(t(\omega)\big) = \nu(v) + \omega\nu\sigma(v) + ... + \omega^{p-1}\nu\sigma^{p-1}(v).$$

D'après le rappel 3, on a $\sigma^p \in N$ et donc $\sigma^p(v) = v$, d'où

$$\sigma\big(t(\omega)\big) = \omega^{-1}t(\omega).$$

D'autre part, N est un sous-groupe distingué de $Gal(P/F)$, donc par définition

$$\sigma^{-i} \circ \nu \circ \sigma^i \in N \text{ pour tout } \nu \in N \text{ et } i = 0, ..., p-1$$

ce qui implique que

$$\sigma^{-i} \circ \nu \circ \sigma^i(v) = v \text{ pour tout } \nu \in N \text{ et } i = 0, ..., p-1.$$

Alors, appliquant σ^i à cette dernière égalité, on a

$$\nu \circ \sigma^i(v) = v \text{ pour tout } \nu \in N \text{ et } i = 0, ..., p-1,$$

ce qui donne finalement

$$\nu\big(t(\omega)\big) = t(\omega) \text{ pour tout } \nu \in N.$$

Étape 4 : Montrons que, pour toutes racines $p^{\text{ième}}$ de l'unité ω, $t(\omega)^p \in F$ et qu'il existe une racine $p^{\text{ième}}$ de l'unité $\omega \neq 1$ telle que $t(\omega) \neq 0$.

D'après l'étape 3, $t(\omega)^p$ est fixé par σ et par toutes permutations de N. L'étape 1 montre alors que $t(\omega)^p \in F$. Si on suppose que, pour une racine $p^{\text{ième}}$ de l'unité $\omega \neq 1$, $t(\omega) = 0$, alors la formule de Lagrange de la page 16 qui nous donne que

$$v = \frac{1}{p}\Big(\sum_{\omega} t(\omega)\Big)$$

conduit directement à

$$v = \frac{1}{p}t(1).$$

Alors, d'après cette dernière égalité et l'étape 3, v est fixé par σ. Or v est aussi fixé par toutes permutations de N, donc d'après l'étape 1, v est dans F ce qui est en contradiction avec l'étape 2 dans laquelle nous avons pris v dans N mais pas dans F, donc $t(\omega) \neq 0$.

Étape 5 : Posons maintenant ω une racine $p^{\text{ième}}$ de l'unité telle que $\omega \neq 1$ et $t(\omega) \neq 0$ et posons

$$K = F\big(t(\omega)\big).$$

D'après la proposition 3.4.1 et l'étape 4, on sait que K est une extension radicielle de F de la forme $F(a^{1/p})$. Il ne reste donc plus qu'à montrer que $Gal(P/K) = N$, et la preuve du lemme sera complète.

On a déjà que $t(\omega) \neq 0$ et $\omega \neq 1$ donc d'après l'étape 3, $t(\omega)$ n'est pas fixé par σ. Ainsi, K est bien différent de F, donc K/F est une extension radicielle de taille 1. D'après le corollaire 3.3.5 (page 33), $Gal(P/K)$ est un sous-groupe d'indice p dans $Gal(P/F)$, d'où

$$|\, Gal(P/K)\,| = |\, N\,|\,.$$

De plus, comme $\sigma\big(t(\omega)\big) \neq t(\omega)$, l'étape 1 nous montre que toutes les permutations de $Gal(P/F)$ qui fixent $t(\omega)$ sont dans N. Comme $t(\omega) \in K$, le théorème 3.2.3 (page 21) assure que les permutations de $Gal(P/K)$ fixent $t(\omega)$, donc

$$Gal(P/K) \subseteq N.$$

Enfin, puisque ces deux groupes ont même ordre, $Gal(P/K)$ ne peut pas être strictement inclus dans N, d'où finalement

$$Gal(P/K) = N.$$

□

Voici à présent la Proposition 5 du mémoire d'Evariste Galois, qui conclut cette partie :

Théorème 3.4.6. *Soit P un polynôme sur un corps F, et supposons que P n'a que des racines simples dans K contenant F. L'équation $P(X) = 0$ est complètement résoluble par radicaux si et seulement si le groupe de Galois $Gal(P/F)$ est résoluble.*

Démonstration. Sens direct : Montrons que si l'équation $P(X) = 0$ est complètement résoluble par radicaux sur F, alors le groupe de Galois $Gal(P/F)$ est résoluble. On raisonne par récurrence forte sur $|\, Gal(P/F)\,|$. Si $|\, Gal(P/F)\,| = 1$, alors $Gal(P/F) = \{id\}$, et ce groupe est évidemment résoluble. Supposons donc que les équations résolubles par radicaux dont le groupe de Galois est d'ordre strictement inférieur à celui de $Gal(P/F)$ ont leur groupe de Galois résoluble.

Soit R/F une extension radicielle qui contient toutes les racines de P. Alors, d'après le théorème 3.2.3 (page 21), tout élément de K est invariant sous $Gal(P/R)$, donc toute racine de P est fixée par toutes les permutations de $Gal(P/R)$, ce qui prouve que $Gal(P/R) = \{id\}$. Ceci montre qu'il existe une extension radicielle K/F telle que

$$|\, Gal(P/K)\,| < |\, Gal(P/F)\,|\,.$$

On considère alors le plus petit nombre premier p tel que, si on enlève une racine $p^{\text{ième}}$ d'un élément, alors l'ordre du groupe de Galois de P diminue. Concrètement, on pose p comme étant le plus petit nombre premier pour lequel il existe une extension radicielle L/F telle que

$$Gal(P/L) = Gal(P/F)$$

et

$$\mid Gal\big(P/L(a^{1/p})\big) \mid < \mid Gal(P/F) \mid$$

avec $a \in S$ qui n'est pas une racine primitive $p^{\text{ième}}$ dans L.

D'après la proposition 3.4.2 (page 34), il existe une extension radicielle de L qui contient une racine primitive $p^{\text{ième}}$ de l'unité. De plus, la preuve de cette proposition nous indique qu'il existe une telle extension R' qui s'obtient à partir de L en extrayant des racines $q^{\text{ième}}$ de l'unité, où q est un nombre premier tel que $q < p$. Alors, par définition de p, on a

$$Gal(P/R') = Gal(P/L) = Gal(P/F).$$

De plus, d'après la proposition 3.3.1 (page 29), on a

$$Gal\big(P/R'(a^{1/p})\big) \subset Gal\big(P/L(a^{1/p})\big),$$

et donc

$$\mid Gal\big(P/R'(a^{1/p})\big) \mid < \mid Gal(P/F) \mid .$$

Comme R' contient une racine primitive $p^{\text{ième}}$ de l'unité, $Gal\big(P/R'(a^{1/p})\big)$ est un sous-groupe distingué d'indice p dans $Gal(P/R') = Gal(P/F)$, d'après le corollaire 3.3.5 (page 33). Or par hypothèse, $P(X) = 0$ est complètement résoluble par radicaux sur F donc aussi sur $R'(a^{1/p})$ d'après la proposition 3.4.4 (page 35). Ainsi, par hypothèse de récurrence, on peut trouver une suite de sous-groupes $G_1, ..., G_t$ telle que

$$Gal\big(P/R'(a^{1/p})\big) = G_1 \supset G_2 \supset ... \supset G_t = \{id\}$$

telle que chaque sous-groupe est distingué et d'indice premier dans le précédent. En posant $G_0 = Gal(P/F)$, on obtient

$$Gal(P/F) \supset Gal\big(P/R'(a^{1/p})\big) = G_1 \supset G_2 \supset ... \supset G_t = \{id\},$$

ce qui prouve que $Gal(P/F)$ est résoluble.

Réciproque : Montrons que si le groupe de Galois $Gal(P/F)$ est résoluble, alors l'équation $P(X) = 0$ est complètement résoluble par radicaux sur F. On raisonne à nouveau par récurrence forte sur $\mid Gal(P/F) \mid$. Si $\mid Gal(P/F) \mid = 1$, alors la seule permutation de $Gal(P/F)$ est l'identité, qui fixe bien toute racine de P. D'après le théorème 3.2.3 (page 21), toutes les racines de P sont dans F qui est bien une extension radicielle de taille 0 de lui-même. Supposons donc que les équations dont le groupe de Galois résoluble est d'ordre strictement inférieur à celui de $Gal(P/F)$ sont résolubles par radicaux.

Comme $Gal(P/F)$ est résoluble, il contient un sous-groupe N d'indice premier que l'on note p. D'après la proposition 3.4.2 (page 34), il existe une extension radicielle R/F qui contient toutes les racines $p^{\text{ièmes}}$ de l'unité. Si

$$\mid Gal(P/R) \mid < \mid Gal(P/F) \mid,$$

alors par hypothèse de récurrence et d'après le rappel 6), $Gal(P/R)$ est un groupe résoluble. L'équation $P(X) = 0$ est alors complètement résoluble par radicaux sur R, donc par définition il existe une extension radicielle R'/R qui contient toutes les racines de P. Comme R'/F est aussi une extension radicielle, la preuve est achevée dans ce cas. Si au contraire

$$Gal(P/R) = Gal(P/F),$$

alors, d'après le lemme précédent, il existe une extension radicielle R''/R telle que $Gal(P/R'') = N$. On a donc

$$\mid Gal(P/R'') \mid < \mid Gal(P/F) \mid,$$

ce qui nous amène au cas précédent et le même raisonnement s'applique. □

On s'est placé ici à un niveau beaucoup plus abstrait que chez Gauss : en effet Galois n'utilise pas les racines primitives modulo p ni l'outil arithmétique que Gauss a introduit dans sa théorie, mais il garde en tête l'exemple de l'équation cyclotomique afin de généraliser le travail de Gauss. En regardant le groupe de l'équation qui contient exactement toutes les permutations qu'on peut faire avec les racines, il parvient à décortiquer ce qui se passe avec l'équation étape par étape, ce qui lui permet d'arriver à la condition qui fait l'objet du dernier théorème que nous avons énoncé. En cela il est arrivé à une théorie générale qui caractérise toutes les équations.

4 Annexes

Cette partie est composée de rappels sur les polynômes symétriques et sur la théorie des groupes qui servent notamment dans les parties "4.2 : Le groupe de Galois d'une équation" et "4.4 : Résolubilité par radicaux".

4.1 Rappels sur les polynômes symétriques

Définitions : **1)** P est un **polynôme symétrique** en n variables si, pour toute permutation $\tau \in \mathfrak{S}_n$,

$$P(X_1, ..., X_n) = P(X_{\tau(1)}, ..., X_{\tau(2)}).$$

2) Pour $1 \leq k \leq n$ le $k^{\text{ième}}$ **polynôme symétrique élémentaire** en n variables est

$$s_k(X_1, ..., X_n) = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k}.$$

Rappel 1. *Un polynôme en n variables $x_1, ..., x_n$ sur un corps F peut être écrit en terme d'un polynôme en $s_1, ...s_n$ si et seulement si il est symétrique.*

Rappel 2. *Si $s_1, ..., s_n$ sont les n polynômes symétriques élémentaires en n variables $x_1, ..., x_n$, alors on a*

$$(X - x_1)...(X - x_n) = X^n - s_1 X^{n-1} + ... + (-1)^n s_n.$$

4.2 Rappels de théorie des groupes

Définition : Soient G un groupe fini et H un sous-groupe de G. Pour $\sigma \in G$, on appelle l'**ensemble des classes à gauche modulo** H l'ensemble σH défini par

$$\sigma H = \{\sigma\xi \mid \xi \in H\}.$$

Le cardinal de cet ensemble est l'**indice de** H **dans** G, noté $[G : H]$. On a aussi le résultat suivant, fourni par le théorème de Lagrange : $[G : H] = \frac{|G|}{|H|}$.

Rappel 3. *Soit $G_1 \supset G_2 \supset G_3$ une chaîne de sous-groupes. Si G_1 est fini, alors*

$$[G_1 : G_3] = [G_1 : G_2][G_2 : G_3].$$

En particulier, si G_3 est un sous-groupe d'indice premier dans G_1, alors soit $G_2 = G_1$ soit $G_2 = G_3$.

Rappel 4. *Soient H et N deux sous-groupes de G. On pose HN un sous-ensemble de G défini par*

$$HN = \{\xi\nu \mid \xi \in H, \nu \in N\}.$$

Si $N \triangleleft G$, alors HN est un sous-groupe de G et $H \cap N \triangleleft H$. Si de plus N est d'indice premier dans G et que G est fini, alors soit $HN = N$ et $H \subset N$ donc $H \cap N = N$, soit $HN = G$ et l'indice de $H \cap N$ dans H est égal à l'indice de N dans G.

Rappel 5. *Soit N un sous-groupe distingué d'indice premier p dans un groupe fini G. Si $\sigma \in G$ et $\sigma \notin N$, alors $\sigma^p \in N$.*

Rappel 6. *Tout sous-groupe H d'un groupe résoluble fini G est résoluble.*

5 Bibliographie

· Tignol, Jean-Pierre *Galois' theory of algebraic equations*. Second edition. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2016.

· Gauss, Carl Friedrich *Disquisitiones arithmeticae*. Traduites par A.-C.-M. POULLET-DELISLE, éditions Jacques Gabay (1989).

· Galois, Évariste *Écrits et mémoires mathématiques*. Édition critique intégrale des manuscrits et publications. Préface de Jean Dieudonné. Notes et commentaires de Robert Bourgne et Jean-Pierre Azra (1962).

· Ehrhardt, Caroline *Itinéraire d'un texte mathématique*. Éditions Hermann (2012).