كلية العلوم و التقنيات فاس
ⵜⴰⵖⵣⵓⵍⵜ ⵏ ⵜⵣⴰⵡⵉⵜⵉ ⴷ ⵜⵙⵙⵜⵙⵉ
Faculté des Sciences et Techniques de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ
Université Sidi Mohamed Ben Abdellah

Licence Sciences et Techniques (LST)

CALCUL SCIENTIFIQUE ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Titre

Groupe de Galois d'un polynôme

Présenté par :

- **Abderazzak EL-Aouni**

Encadré par :

- **Pr Seddik Gmira**

Soutenu Le 11 Juin 2019 devant le jury composé de:

- **Pr Seddik Gmira**
- **Pr Mohammed Bekkali**
- **Pr Mohamed Bellahmar**
- **Pr Mustapha Alami**

Année Universitaire 2018 / 2019

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS
B.P. 2202 – Route d'Imouzzer – FES
212 (0)5 35 61 16 86 – Fax : 212 (0)5 35 60 82 14
Site web: http://www.fst-usmba.ac.ma

Remerciements

Je dois remercier ALLAH le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir ce travail .

Je tiens à remercier Mon Encadreur de mémoire le professeur Seddik **Gmira** pour ses conseils , son accompagnement tout au long de cette expérience avec beaucoup de patience et de pédagogie.

Je tiens aussi à exprimer mes profonds remerciements aux membres de jury qui ont accepté de juger ce travail.

Je tiens aussi à remercier tous les professeurs du département de mathématiques de FST Fès .

Enfin mes remerciements vont à tous ceux qui ont contribué de prés où de loin pour l'aboutissement de ce travail.

Table des matières

Introduction

Dans ce projet de fin d'étude notre intérêt sera porté sur la résolution des équations polynômiales du type :

$$x^n + a_{n-1}x^{n-1} + \ldots\ldots + a_1x^1 + a_0 = 0$$

à coefficients dans un corps K.
En utilisant la théorie de Galois, nous pouvons associer aux racines

$$\beta_1, \beta_2, \ldots., \beta_n$$

d'une telle équation algébrique un sous-groupe de S_n de toutes les permutations sur l'ensemble des racines, appelé groupe de Galois.
En partant d'une équation polynômiale à coefficients dans un corps K , nous commençons par chercher les racines de l'équation. Ceci permet d'obtenir le corps de rupture $K(\beta_1, \beta_2, \ldots, \beta_n)$ qui est une une extension du corps K.
En suite, nous établissons une relation rationnelle entre toutes les racines :

$$R(\beta_1, \beta_2, \ldots., \beta_n) = 0$$

Un élément du groupe de Galois est en fait une permutation $\sigma \in S_n$ qui vérifie une relation rationnelle :

$$R\left(\beta_{\sigma(1)}, \beta_{\sigma(2)}, \ldots., \beta_{\sigma(n)}\right) = 0$$

Une telle permutation σ est appelée une bonne permutation, ou un élément du groupe de Galois. σ est en fait un automorphisme du corps de rupture qui laisse fixe les éléments du corps K.
La dernière partie de cette étude est consacrée à quelques exemples intéressants de calcul de groupes de Galois.

Chapitre 1

Rappels

1.1 Groupes symétriques

Définition 1.1.
Soit E un ensemble non vide. Une permutation de E est une bijection $\sigma : E \to E$. On note S_E l'ensemble de toutes les permutations de E.
Dans le cas où $E = \{1, 2, ..., n\}$, on écrit S_n au lieu de S_E.

▪ S_n est dit le **groupe symétrique** d'ordre n.
▪ Une permutation $\sigma \in S_n$ telle que $\sigma : i \mapsto \sigma(i)$ est notée :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

L'ordre des colonnes n'est pas important.
▪ La cardinal de S_n est $n!$.
▪ Une permutation est dite **cyclique** si elle est formée de la suite des transformés successifs d'un de ses éléments : on la notera alors souvent par cette suite elle-même, et on dit que c'est un **cycle**.
Exemple : Dans S_6 on a $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}$ est un 3-cycle. On le note $(2, 5, 3)$ (ou $(5, 3, 2)$ ou $(3, 2, 5)$).
▪ La **longueur** d'un cycle, ou nombre d'éléments de son **support** , est égale à son ordre ; un cycle de longueur 2 s'appelle une **transposition** , et consiste donc en l'échange de deux éléments.
▪ Deux cycles disjoints, c'est-à-dire à supports disjoints, commutent ;
▪ Toute permutation est, de manière unique, produit de cycles deux à deux disjoints, que l'on appelle ses **composantes cycliques** ;
▪ Toute permutation est produit de transpositions ; il y a plusieurs décompositions mais la parité du nombre de facteurs est constante, et permet de parler de permutations **paires** (ou de signature $+1$) et **impaires** (ou de signature -1)

. Les permutations paires de S_n forment le **groupe alterné** A_n ,seul sous-groupe d'indice 2 dans S_n.

1.2 Corps

Définition 1.2.
Un corps K est un anneau unitaire dans lequel tout élément non nul est inversible,c'est à dire que $K - \{0\}$ est un groupe pour la multiplication.
Si la multiplication d'un corps est commutatif,on dit que le corps est commutatif.

Exemples 1.1.
Les anneaux $(\mathbb{R}, +, .)$, $(\mathbb{Q}, +, .)$ et $(\mathbb{C}, +, .)$ sont des corps commutatifs.

Dans cette partie, tous les corps sont supposés commutatifs.

Propositions 1.1.
Tout corps est intègre,donc sa caractéristique est soit zéro soit un nombre premier.

Prouve : Soit K un corps.
. Soient x,$y \in K$ donc :
Si $xy = 0$ avec $x \neq 0$, alors $0 = x^{-1}xy = y$ puisque x est inversible. donc K est intègre
. Soit $n \in \mathbb{N}^*$ la caractéristique non nulle de K,
Si n n'est pas premier alors il existe un couple $(a, b) \in \mathbb{N}^{*2}$ tel que : $n = a.b$
Donc $a < n$ et $b < n$ ($a \neq n$ et $b \neq n$)
Donc $a.1_K \neq 0_K$ et $b.1_K \neq 0_K$
Mais, on a $(a.1_K).(b.1_K) = a.b.1_K = n.1_K = 0_K$, contradiction
Par suit n est premier.

Théorème 1.1. *Soit K un corps fini. Alors :*
. *Sa caractéristique est un nombre premier p.*
. *Il existe $n \in \mathbb{N}*$ tel que $Card(K) = p^n$. où $Card(K)$ est le cardinale de l'ensemble fini K.*

Définition 1.3.
*Une application f d'un corps K dans un corps L est dite un **homomorphisme** (ou morphisme) de corps si elle satisfit les relations :*
1) $f(a + b) = f(a) + f(b)$ *pour tous a, b dans K ;*
2) $f(ab) = f(a)f(b)$ *pour tous a, b dans K ;*

Définition 1.4.
- *Un **endomorphisme** est un morphisme d'un corps K dans lui même.*
- *Un **isomorphisme** est un morphisme bijectif.*
- *Un **automorphisme** est un endomorphisme bijectif.*

Propositions 1.2.
L'ensemble $Aut(K)$ des automorphismes du corps K forme un groupe pour la loi de composition.

Preuve :
Il est facile de montrer que $Aut(K)$ est un sous-groupe du groupe $S(K)$ des permutations de K.

1.3 Extensions de corps

Définition 1.5.
*Soit K un corps. On appelle **extension** de K tout corps L contenant un sous-corps isomorphe à K.*

Remarques :
- Si K est un sous-corps de L; alors L est une extension de K (on considère l'injection canonique $i : K \to L$).
- Réciproquement un homomorphisme de corps $\psi : K \to L$ est forcément injectif. Par conséquent, le sous-corps $K' = \psi(K)$ de L est isomorphe à K identifiant K et K'; on peut donc dire que K est un sous-corps de L.
- En conclusion, aux notation abusives (bien pratique) près :

L est une extension de $K \Leftrightarrow K$ est un sous-corps de L.

Exemples 1.2.
- *$\mathbb{C}$ est une extension de $\mathbb{R}$.*
- *$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : (a, b) \in \mathbb{Q}^2\}$ est une extension de $\mathbb{Q}$.*

Définition 1.6.
*Soient K un corps, L une extension de K. On appelle K-**automorphisme** du corps L tout K-isomorphisme de L dans lui-même, c'est-à-dire tout automorphisme du corps L qui laisse invariant chaque élément de K, c'est-à-dire toute application bijective $\sigma : L \longrightarrow L$ qui vérifie :*
- $\forall (x, y) \in L^2$, $\sigma(x + y) = \sigma(x) + \sigma(y)$ *et* $\sigma(xy) = \sigma(x)\sigma(y)$.
- $\sigma(1_L) = 1_L$.
- $\forall u \in K$, $\sigma(u) = u$.

Définition 1.7. ***élément primitif***
Soit L une extension de K , pour tout élément x de L,on aura l'inclusion $K(x) \subset L$,S'il existe dans L un élément α vérifiant l'égalité $K(\alpha) = L$, on dit que α engendre L sur K , et L s'appelle alors ***extension simple*** *de K,L'élément α est un* ***élément primitif*** *de l'extension L sur K.(α n'est pas unique)*
Le ***théorème d'élément primitif*** *affirme, lorsque l'extension est de degré fini, l'existence d'un élément primitif.*

Définition 1.8.
Soient K un corps et L une extension de K, On appelle ***degré de l'extension*** *L de K (ou L/K) et on note $[L : K]$, la dimension de L comme K-espace vectoriel :*

$$[L : K] = dim_K L$$

Remarque 1.1.
▪ *Le degré d'une extension peut être infini.(exp : $[\mathbb{R}, \mathbb{Q}] = \infty$) ou fini (exp :$[\mathbb{C} : \mathbb{R}] = dim_{\mathbb{R}}\mathbb{C} = 2$).*
▪ *Pour une extension L de K on a $[L : K] = 1 \Leftrightarrow K = L$.*

Corollaire 1.1. *Soient L un corps, K un sous-corps de L Soit E un L-espace vectoriel. Les conditions suivantes sont équivalentes :*
(i) E est un L-espace vectoriel de dimension finie ;
(ii) E est un L-espace vectoriel de dimension finie et L est un K-espace vectoriel de dimension finie.
On a alors

$$dim_K E = dim_L E.dim_K L$$

1.4 Corps de rupture d'un polynôme

Définition 1.9.
Soit K un corps. Soit $P \in K[X]$ un polynôme irréductible dans $K[X]$. On dit que le corps L est un ***corps de rupture*** *de P si, et seulement si, L est une extension simple de K engendrée par K et une racine, notée α, du polynôme P.*

Exemples 1.3.
▪ *Les racines de $P(x) = x^2-2 \in \mathbb{Q}[X]$ sont $-\sqrt{2}$ et $\sqrt{2}$,donc $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : (a, b) \in \mathbb{Q}^2\}$ est le corps de rupture de P.*
▪ *Soit P un polynôme sur K, Si $deg(P) = 1$ alors K est le corps de rupture de p.*

Définition 1.10.
Soient K un corps et E une extension de K. Si $P \in K[X]$, avec $deg(P) = n \in \mathbb{N}^*$, On dit que E est un ***corps de décomposition*** *de P sur K ou un corps de dislocation de P sur K si, et seulement si :*
(i) $\exists a \in E$ *et* $(\alpha_1, ..., \alpha_n) \in E^n$ *tel que, dans* $E[X]$,

$$P(X) = a(X - \alpha_1)...(X - \alpha_n)$$

(ii) $E = K(\alpha_1, ..., \alpha_n)$

Remarque 1.2.
Terminologie *: On note* $\mathbf{D}_K(P)$ *"le corps de décomposition de P sur K".*

1.5 Élément algébrique,Corps algébriquement clos

Définition 1.11.
Soit L/K une extension de corps. Un élément α de L est ***algébrique*** *sur K s'il existe $P(X) \in K[X]\backslash 0$ tel que $P(\alpha) = 0$.*

Remarque 1.3.
. *Tout élément α de K est algébrique sur K. (α racine de $X - \alpha \in K[X]\backslash 0$).*
. *Tout radical relatif à K est algébrique sur K : si β possède sa puissance n-ième dans K, il racine de $X^n - \beta^n \in K[X]\backslash 0$.*

Définition 1.12.
Le degré d'un élément algébrique a sur K est le degré de l'extension $K(a)$ de K.

Définition 1.13.
On dit que L est ***algébrique*** *sur K si tous les élément de L sont algébrique sur K.*

Définition 1.14.
Une extension L/K est algébrique si tous les éléments de L sont algébriques sur K.

Propositions 1.3.
Si L/K est une extension finie, alors L/K est algébrique.

Preuve :
Soit a un élément de L. Comme $[L : K]$ est fini, $[K(a) : K]$ l'est aussi , Il existe donc un entier $n \geq 1$ tel que $1, a, ..., a^n$ soient linéairement dépendants sur K, c'est-à-dire qu'il existe des éléments $\alpha_i; i = 0, ..., n$ non tous nuls de K tels que $\alpha_0 + \alpha_1 a + ... + \alpha_n a^n = 0$.

Définition 1.15.

Un corps K est dit ***algébriquement clos*** *s'il vérifie l'une quelconque des propriétés équivalentes suivantes :*

1) *tout polynôme $P \in K[X]$ de degré $\geqslant 1$ admet une racine dans K ;*
2) *tout polynôme $P \in K[X]$ est produit de polynômes de degré 1 ;*
3) *les éléments irréductibles de $K[X]$ sont les $(X-a), a \in K$;*

Exemples 1.4.

▪ *$\mathbb{Q}$ n'est pas algébriquement clos. En effet, x^2-2 , x^3-2 n'ont pas de racine dans $\mathbb{Q}$.*

▪ *$\mathbb{C}$ est algébriquement clos.*

Propositions 1.4.

▪ *Tout corps algébriquement clos est infini.*

Preuve :

Si K est le corps fini $K = \{\alpha_1, ..., \alpha_q\}$; le polynôme $(X-\alpha_1)(X-\alpha_2)...(X-\alpha_q)+1$ de $K[X]$ est de degré $q \geq 2$, et n'a pas de racine dans K.

Définition 1.16.

Soit K un corps, L une extension de K.
On dit que L est une ***clôture algébrique*** *de K si, et seulement si, L est algébrique sur K et L est algébriquement close.*

Exemples 1.5.

$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Remarque 1.4.

Tout corps est contenu dans un corps algébriquement clos.

Chapitre 2

Groupe de Galois d'un polynôme

Soit P un polynôme de $K[X]$ scindé sur K , On peut trouver des relations entre les coefficients d'un polynôme scindé et ses racines.
Par exemple si l'on a un polynôme de degré 2 scindé dans $K[X]$, on peut l'écrire

$$aX^2 + bX + c = a\,(X - \lambda_1)\,(X - \lambda_2)$$

où λ_1 et λ_2 sont les racines de P non nécessairement distinctes. Alors, en effectuant les calculs on obtient les relations :

$$\begin{cases} \lambda_1 + \lambda_2 = -\frac{b}{a} & (*) \\ \lambda_1\lambda_2 = \frac{c}{a} & (**) \end{cases}$$

soit $E = \{\lambda_1, \lambda_2\}$, les permutations de E sont l'identité id et la transposition (21) qui vérifient $(*)$ et $(**)$. Or si $S = \{id, (21)\}$ On a (S, o) est un groupe.
Pour un polynôme de degré 3 : $aX^3 + bX^2 + cX + d$, en notant $\lambda_1, \lambda_2, \lambda_3$ ses trois racines distinctes ou non, on a :

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = -\frac{b}{a} & (*) \\ \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = \frac{c}{a} & (**) \\ \lambda_1\lambda_2\lambda_3 = -\frac{d}{a} & (***) \end{cases}$$

si $F = \{\lambda_1, \lambda_2, \lambda_3\}$, l'ensemble des permutations de F est

$$S_3 = \{id, (12), (23), (31), (231), (312)\}$$

qui vérifient $(*)$, $(**)$ et $(***)$, et on a (S_3, o) est un groupe.
En général, pour un polynôme de degré n , $a_0 + a_1X + \ldots + a_nX^n$ avec a_n non nul, scindé et ses racines $\lambda_1, ..., \lambda_n$ on a pour tout $1 \leq p \leq n$:

$$\sigma_p = \sum_{1 \leq i_1 < i_2 < \ldots < i_p \leq n} \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_p} = (-1)^p \frac{a_{n-p}}{a_n}$$

En particulier : $\sigma_1 = \sum_{i=1}^{i=n} \lambda_i = -\frac{a_{n-1}}{a_n}$, $\sigma_2 = \sum_{1 \leq i < j \leq n} \lambda_i\lambda_j = \frac{a_{n-2}}{a_n}$,
$\sigma_n = \prod_{i=1}^{i=n} \lambda_i = (-1)^n \frac{a_0}{a_n}$

2.1 Relation rationnelle (ou algébrique)

Définition 2.1.
Soient K un corps, et L une extension de K. Soient $x_1, x_2.., x_m \in L$.
S'il existe un polynôme $P \in K[X_1, ..., X_m]$ non nul, tel que $P(x_1, x_2..., x_m) = 0$ on dit que $x_1, x_2..., x_m$ sont algébriquement dépendant, et une telle égalité s'appelle une ***relation rationnelle****.*

Exemples 2.1.
Soit $P(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[X]$,les racines de P sont $\mp\sqrt{2}$ et $\mp\sqrt{3}$ et le corps de rupture est $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, Ainsi des relations rationnelle entre les racines seront :

$$\mathrm{R}(-\sqrt{2}, \sqrt{2}, -\sqrt{3}, \sqrt{3}) = (\sqrt{3})^2 - (\sqrt{2})^2 - 1 = 0$$
$$\mathrm{T}(-\sqrt{2}, \sqrt{2}, -\sqrt{3}, \sqrt{3}) = (\sqrt{2})^2 + (\sqrt{3})^2 - 5 = 0$$

2.2 Bonnes et mauvaises permutation des racines

Soit $\mathbf{R}$ une relation rationnelle entre l'ensemble $\{a_1, a_2.., a_m\}$ des racines d'un polynôme $P \in K[X]$.
Les **bonnes permutations** σ seront celles qui vérifieront :

$$\mathbf{R}(a_1, a_2.., a_m) = 0 \Rightarrow \mathbf{R}(a_{\sigma(1)}, a_{\sigma(2)}.., a_{\sigma(m)}) = 0$$

c'est-à-dire qui respecteront toutes les relations rationnelles entre les racines de P

Exemples 2.2.
▪ *Soit $P(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[X]$, les racines de P sont $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $a_3 = \sqrt{3}$ et $a_4 = -\sqrt{3}$,*
Avec cette numérotation on écrit : $a_3^2 - a_2^2 - 1 = 0$
soit la permutation

$$\sigma_1 = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ \sqrt{3} & -\sqrt{2} & \sqrt{2} & -\sqrt{3} \end{pmatrix}$$

On a donc $(\sigma_1(a_3))^2 - (\sigma_1(a_1))^2 - 1 = 2 - 3 - 1 = -2 \neq 0$
Donc σ_1 n'est pas une bonne permutation (mauvaise permutation).
▪ *Soit $\sigma_2 = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & \sqrt{3} & -\sqrt{3} \end{pmatrix}$ est une bonne permutation des racines.*

2.3 Groupe de Galois d'un polynôme

Reprenons notre polynôme $P \in K[X]$, de racines $a_1, ..., a_m$. Les bonnes permutations des racines définissent des transformations du corps de rupture $K(a_1, ..., a_m)$.

Propositions 2.1.
Soit $\overline{\sigma}$ la transformation associée à la permutation σ. Alors :
1) *$\overline{\sigma}$ est un endomorphisme du corps de rupture de P ;*
2) *$\overline{\sigma}$ laisse fixe les éléments de K ;*
3) *$\overline{\sigma}$ est un automorphisme du corps de rupture de P ;*

Preuve :
1) Rappelons que $K(a_1, ..., a_m)$ est quotient de l'anneau de polynômes $K[X_1, ..., X_m]$ par l'idéal des polynômes nuls en $(a_1, ..., a_m)$, c'est-à-dire

$$K(a_1, ..., a_m) = K[a_1, ..., a_m]/ < P >$$

où $< P >$ est l'idéale engendré par P. Donc l'application $\overline{\sigma}$ n'est autre que la composée de deux homomorphismes

$$\mathrm{K}(a_1, ..., a_m) \to \mathrm{K}[X_1, ..., X_m]/ < P > \to \mathrm{K}(a_1, ..., a_m)$$

donc $\overline{\sigma}$ est un endomorphisme de $\mathrm{K}(a_1, ..., a_m)$.
2) $\overline{\sigma}$ ne change que les racines qui sont hors du corps K.
3) On a σ^{-1} est aussi une bonne permutation et l'endomorphisme $\overline{\sigma^{-1}}$ qui lui correspond est l'inverse de $\overline{\sigma}$. Donc $\overline{\sigma}$ est un endomorphisme bijectif donc est un automorphisme .

Tout cela est facile à vérifier :

À toute bonne permutation σ correspond un automorphisme du corps de rupture , laissant K fixe , que l'on notera aussi σ.

Un automorphisme d'une extension de K laissant K fixe s'appelle un **K-automorphisme** de l'extension.
Réciproquement, si l'on part d'un K-automorphisme φ du corps de rupture de P sur K et si x est une racine de P, l'égalité $P(x) = 0$ donne $\varphi(P(x)) = 0$ (car φ est un automorphisme) puis $P(\varphi(x)) = 0)$ (car les coefficients de P sont fixes par φ) et par suite, φ définit bien une permutation des racines qui respecte bien sûr les relations rationnelles.

Définition 2.2.
À tout polynôme $P \in K[X]$ on associe un groupe , noté $\mathbf{G(P|K)}$ *ou* $\mathbf{G(H|K)}$,

avec H le corps de rupture de P sur K , que l'on appelle ***groupe de Galois*** *de P sur K. on peut le voir de deux manières :*
• *C'est un groupe des bonnes permutations des racines du polynôme, celle qui respectent les relations rationnelle entre les racines ; c'est alors un sous-groupe de S_m où m est le nombre de racines de P, et son ordre divise $m!$ (d'après Lagrange).*
• *C'est le groupe des automorphismes du corps de rupture laissant fixe le corps de base, c'est alors un sous-groupe du groupe de tous les automorphisme du corps de rupture.*

Propositions 2.2.
1) *Sur un corps algébriquement clos, tout groupe de Galois est réduit à l'identité.*
2) *Pour un polynôme de degré 2, le groupe de Galois est d'ordre 1 ou 2 suivant que le polynôme est réductible ou non.*
3) *Pour un polynôme réel sans racines réelles, le groupe de Galois sur $\mathbb{R}$ est formé de l'identité de $\mathbb{C}$ et la conjugaison complexe.*
4) *Le groupe de Galois de P est le même que celui de P^n.*

Prouve :
1) Dans un corps K algébriquement clos, le corps de rupture d'un polynôme $P \in K[X]$ est K lui même, Et donc $\mathbf{G}(P|K) = \{id\}$
2) **.** Si P est réductible, alors les racines sont dans K, donc $\mathbf{G}(P|K) = \{id\}$ et $|\mathbf{G}(P|K)| = 1$
. Si P est irréductible alors les racines sont de la forme $a \pm b\sqrt{\Delta}$ (avec Δ est le discriminant de P, et $\sqrt{\Delta} \notin K$)
Donc

$$\mathbf{G}(P|K) = \{id, \sigma\}$$

avec

$$\sigma : a + b\sqrt{\Delta} \longmapsto a - b\sqrt{\Delta} \quad \forall (a, b) \in K^2$$

Donc

$$|\mathbf{G}(P|K)| = 2$$

3) Les seules $\mathbb{R}$-automorphismes de $\mathbb{C}$ sont l'identité et la conjugaison complexe (qui échange i et $-i$)
4) Le corps de rupture de P et P^n est le même (car $P^n(x) = 0 \Leftrightarrow P(x) = 0$),

Remarque 2.1.
On ne sait pas si, pour tout groupe fini, il existe un polynôme sur $\mathbb{Q}$ dont il est le groupe de Galois.

2.4 Exemple

Reprenons le polynôme

$$P(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[X]$$

dont le corps de rupture est

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{\alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6} \quad : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}\}$$

Les quatre automorphisme de corps de rupture sont :

$$id : \alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6} \mapsto \alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6}.$$
$$\sigma_1 : \alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6} \mapsto \alpha_0 + \alpha_1\sqrt{2} - \alpha_2\sqrt{3} - \alpha_3\sqrt{6}.$$
$$\sigma_2 : \alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6} \mapsto \alpha_0 - \alpha_1\sqrt{2} + \alpha_2\sqrt{3} - \alpha_3\sqrt{6}.$$
$$\sigma_3 : \alpha_0 + \alpha_1\sqrt{2} + \alpha_2\sqrt{3} + \alpha_3\sqrt{6} \mapsto \alpha_0 - \alpha_1\sqrt{2} - \alpha_2\sqrt{3} + \alpha_3\sqrt{6}.$$

les $\alpha_i \in \mathbb{Q}, i = 0, 1, 2, 3$

Donc le groupe de Galois de P est :

$$\mathbf{G}(P|\mathbb{Q}) = \{id, \sigma_1, \sigma_2, \sigma_3\}$$

et $|\mathbf{G}(P|\mathbb{Q})| = 4$.

Chapitre 3

La détermination de groupe de Galois

3.1 L'ordre du groupe de Galois d'un polynôme

Soient K un corps, et P un polynôme de $K[X]$ de degré n, et $(a_1, a_2, ..., a_m)$ l'ensemble de ses racines. Le corps de rupture est $K(a_1, a_2, ..., a_m)$. Soit q son degré.
Soit x un élément primitif ($K(x) = K(a_1, a_2, ..., a_m)$). son polynôme minimal M_x est alors de degré q et il fixe par tout K-automorp-hisme de :

$$K(a_1, a_2, ..., a_m) = K(x)$$

Par conséquent, l'image de x par un tel K-automorphisme est une racine de M_x, et cette image détermine l'automorphisme, car le corps est engendré par x sur K.
Question : peut-on prendre pour image de x une racine arbitraire y de M_x ? S'il existe un K-automorphisme ψ de $K(x)$ transformant x en y, ce ne peut être qu'une éventuelle $\ll$ substitution de x par y $\gg$: tout élément de K(x) s'écrit R(x) pour un R $\in$ K[X], son image devra être R(y) . Mais attention : un élément de K(x) s'écrit R(x) pour plusieurs polynômes R $\in$ K[X], différant entre eux par des multiples de M_x . La valeur $R(y) \in K(y)$ est-elle la même pour tous les polynômes R correspondant à une même valeur de R(x) ? Oui, car $\mathbf{M}_x(y)$ est nul : on voit pourquoi il est nécessaire que x et y aient le même polynôme minimal. Dans ces condition l'application suivante est bien définie

$$\varphi : K(x) \to K(y)$$

$$\mathbf{R}(x) \to \mathbf{R}(y)$$

et c'est bien sur un isomorphisme de corps, laissant fixe le corps de base K.
Ce sera un K-automorphisme de $K(x)$ si, seulement, si $K(y)$ est un sous-corps de $K(x)$. Il suffit pour cela que $K(y)$ contienne $K(x)$; mais $K(x)$ est engendré par les racines de P, et ces racines sont permutées par l'isomorphisme φ puisque

P est fixe. Dès alors $K(y)$, image de φ , contient les racines de P et contient donc $K(x)$: il lui égal.
On vient d'établir une bijection naturelle entre :
• Le groupe de Galois $\mathbf{G}(P)$, formé des bonnes permutations des racines de P(les K-automorphismes $K(x)$ laissant fixe le corps de base K)
• Les racines du polynôme minimum d'un élément primitif du corps de rupture.
Or, le nombre des racine du polynôme minimal est égale au degré (car un polynôme minimal est irréductible ,et les racines sont simple)
D'où le résultat fondamental :

L'ordre du groupe de Galois d'un polynôme est le degré de son corps de rupture.

Exemples 3.1.

Reprenons le polynôme $P(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[X]$,*dont le corps de rpture est* $\mathbb{Q}(\sqrt{2},\sqrt{3})$,*et* $x = \sqrt{2}+\sqrt{3}$ *est un élément primitif.*
En effet : Montrons que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$
On a d'une part,

$$\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3}) \Longrightarrow \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

D' autre part, vérifions que $\sqrt{2}$ *et* $\sqrt{3}$ *appartiennent à* $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

$$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6} \Longrightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$
$$\sqrt{6}(\sqrt{2}+\sqrt{3}) = 2\sqrt{3}+3\sqrt{2} = 2(\sqrt{2}+\sqrt{3})+\sqrt{3}$$

d'où $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$; *on en déduit que* $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ *et par suite :*

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

Le polynôme minimum M_x *de* x *sur* $\mathbb{Q}$ *est :*

$$\begin{aligned} M_x(X) &= (X-(\sqrt{2}+\sqrt{3}))(X-(-\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X-(-\sqrt{2}-\sqrt{3})) \\ &= (X^2-(\sqrt{2}+\sqrt{3})^2)(X^2-(\sqrt{2}-\sqrt{3})^2) \\ &= (X^2-5-2\sqrt{6})(X^2-2+2\sqrt{6}) \\ &= (X^2-5)^2-(2\sqrt{6})^2 \\ &= X^4-10X^2+1 \end{aligned}$$

En effet : (Montrons que M_x *est le polynôme minimal de* $x = \sqrt{2}+\sqrt{3}$*).*
Il suffit de montrer, soit qu'il est irréductible sur $\mathbb{Q}$*, soit* $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ *est de degré* 4 *sur* $\mathbb{Q}$*.*
On a $\sqrt{2}+\sqrt{3}$ *est contenu dans* $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ *qui de degré* 4,*car*(X^2-3) *est polynôme minimum de* $\sqrt{3}$ *sur* $\mathbb{Q}$,*est irréductible sur* $\mathbb{Q}[\sqrt{2}]$,*Dès lors le degré* q *de* $\sqrt{2}+\sqrt{3}$ *divis* $4 \Longrightarrow q \in \{1,2,4\}$.

▪ $q \neq 1$ *car* $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$
▪ $q \neq 2$ *car* $(\sqrt{2}+\sqrt{3})^2$ *n'est pas combinaison* $\mathbb{Q}$*-linéaire de* 1 *et* $\sqrt{2}+\sqrt{3}$.
Ce degré est donc $q = 4$.
Donc le nombre des racine du polynôme minimal M_x *de* $x = \sqrt{2}+\sqrt{3}$ *est* $q = 4 = |\mathbf{G}(P)|$.

3.2 Groupe de Galois d'un polynôme réductible

Soient K un corps, et P un polynôme réductible de $K[X]$. Donc il existe S, T deux polynômes de $K[X]$ pas nécessairement irréductibles ($deg(S) \geq 1$ et $deg(T) \geq 1$) tel que $P = ST$, pour tout K-automorphisme, l'image d'une racine de S reste racine de S, et de même pour T. ce qui signifie que si $\sigma \in \mathbf{G}(P)$, la restriction de σ sur les racines de S , T donne une bonne permutation . Appelons σ_S et σ_T ces restrictions .
Les deux applications $\sigma \to \sigma_S$ et $\sigma \to \sigma_T$ sont des homomorphismes de groupes, D'où l'homomorphisme de groupe suivant :

$$\mathbf{G}(P) \to \mathbf{G}(S) \times \mathbf{G}(T)$$
$$\sigma \to (\sigma_S, \sigma_T)$$

Toute racine de P étant racine de S ou T, Cet homomorphisme est injectif. mais en général n'est pas surjectif, exemples :
• Le cas le plus flagrant est celui où S et T sont égaux,le groupe de Galois est donc :

$$\mathbf{G}(P) = \mathbf{G}(S^2) = \mathbf{G}(S) \neq \mathbf{G}(S) \times \mathbf{G}(S)$$

• Prenons

$$P(x) = (x^2-2)(x^2-8)$$

Les racines de P sont : $\mp\sqrt{2}$ et $\mp 2\sqrt{2}$, et on ne peut échanger les deux premières sans échanger les deux dernières.
Autrement dit, la seule bonne permutation autre que l'identité est la transposition simultanée des deux premières et des deux dernières.D'où :

$$\mathbf{G}((x^2-2)(x^2-8)) \neq \mathbf{G}(x^2-2) \times \mathbf{G}(x^2-8))$$

Le corps de rupture est d'ailleurs $\mathbb{Q}(\sqrt{2})$, de degré 2.
Tout ce que l'on peut dire, c'est que :

Le groupe de Galois d'un produit est un sous-groupe du produit cartésien des groupes de Galois.

On dire plus dans le cas où il y a une racine de S qui n'est pas racine de T.
Car alors aucun élément de $\mathbf{G}(P)$ ne la transformera en une racine donnée de T
Introduisons alors la notion suivante :"Un sous-groupe $\mathbf{G}$ de S_n est dit **transitif** si, quel que soit le couple d'indice (i, j), il existe un élément de $\mathbf{G}$ transformant i en j".
On vient de voir que si P est égal à ST où il y a une racine de S qui n'est pas racine de T, alors le groupe de Galois de P n'est pas transitif.
La conclusion est donc vraie pour tout polynôme non primaire,c'est-à-dire non puissance d'un polynôme premier.
Et que se passe-t-il si S et T ont même racines, le cas extrême étant celui où ils sont égaux ? Dans se dernier cas, $\mathbf{G}(P)$ peut être transitif : il suffit de prendre $\mathbf{G}(X^2)$, la seule racine est 0 , et il est clair que $\mathbf{G}(X^2) = \{id\}$ est transitif sur (0).
Mais si, au lieu de considéré $\mathbf{G}$ comme l'ensemble de permutations de l'ensemble des racines, on le considère comme un groupe de permutation de la famille des racines (dont un sous-groupe de S_n, avec n le degré de P), alors dans tous les cas on écrit la famille des racines de $P = ST$ comme :

$$(a_1, ..., a_s, b_1, ..., b_t)$$

où les a_i sont la famille des racines de S et les b_j sont celle des racines de T. Dans ces conditions, aucun élément de $\mathbf{G}(P)$ ne transformera un a_i en un b_j.

La famille des racines de X^2 est $(0, 0)$, et $\mathbf{G}(X^2) = \{id\}$ n'est pas transitif sur $(0, 0)$.

Le groupe de Galois d'un polynôme réductible n'est pas transitif sur la famille de ces racines.

3.3 Groupe de Galois d'un polynôme dans le cas des corps finis

Quelques rappels :

• Soit G un groupe, et t un élément de G ; le sous-groupe engendré par t est constitué par l'ensemble des $t^n, n \in \mathbb{Z}$. Un groupe engendré par un élément, est appelé groupe **monogène** . On a :

$$G =< t >= \{t^n : n \in \mathbb{Z}\}$$

Un groupe monogène fini d'ordre n est un groupe **cyclique $\mathbf{C}_n$.**
• Soit K un corps fini :

▪ La caractéristique de K est un nombre premier p.

▪ Tout extension de degré fini de K, est un corps fini. Plus précisément, si L est une extension de degré fini,alors on a l'égalité :

$$card(L) = (card(K))^{[L:K]}$$

• On appelle **sous-corps premier** de K le sous-corps de K engendré par l'élément 1_K . Il est contenu dans tout sous-corps de K .

• Soit K un corps , alors :

▪ Si K est fini , le sous-corps premier de K est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p est la caractéristique de K).

▪ Si K est infini, le sous-corps premier de K est isomorphe à $\mathbb{Q}$.

Propositions 3.1.

Soit K un corps de caractéristique p (premier) . L'application

$$\begin{aligned} \mathcal{F} : K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

*est un $\mathbb{F}_p$-endomorphisme du corps K(appelé endomorphisme de **Frobenius** de K). Alors si K est fini, $\mathcal{F}$ est un automorphisme.*

Preuve :

▪ Montrons que le Frobenius $\mathcal{F}$ est bien un endomorphisme de corps de K :

On a : - $\mathcal{F}(1_K) = 1_K$ (trivial)

- $\mathcal{F}(ab) = \mathcal{F}(a)\mathcal{F}(b)\ \forall (a,b) \in K$, (car K est commutatif).

- $\mathcal{F}(a+b) = \mathcal{F}(a) + \mathcal{F}(b)\ \forall (a,b) \in K$ (par la formule du binôme de Newton).

▪ Comme $\mathbb{F}_p^*$ est un groupe d'ordre $p-1$, on a d'après le théorème de Lagrange : $(\forall x \in \mathbb{F}_p^*, x^{p-1} = 1)$; d'où de suite$(\forall x \in \mathbb{F}_p, x^p = x)$.

▪ Comme $\mathcal{F}$ est un endomorphisme de corps de K, $\mathcal{F}$ est injectif. Si K est fini, $\mathcal{F}$ est bijectif. Donc $\mathcal{F}$ est un automorphisme.

Théorème 3.1.

Soient p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$:
Il existe un corps fini à q éléments. C'est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.

Remarque 3.1.

***Terminologie** : Pour tout nombre premier p et tout $n \in \mathbb{N}^*$, il y a donc existence et unicité, à isomorphisme près, d'un corps à p^n éléments. Ce corps est noté $\mathbb{F}_p$ ou $\mathbf{CG}[p^n]$ ("corps de Galois").*

Preuve :

▪ Soit K un corps à q éléments. Comme $caract(K)$ est un nombre premier

qui divise q, $caract(K) = p$ et le sous-corps premier de K est $\mathbb{F}_p$. $(K^*, \times)$ est un groupe à $q-1$ éléments, donc $(\forall x \in K^*, x^{q-1} = 1)$, d'où de suite $(\forall x \in K, x^q = x)$. Or le polynôme $X^q - X \in \mathbb{F}_p[X]$, qui est de degré q, admet au plus q racines distinctes dans K. Comme tout élément de K est une racine de ce polynôme, on a bien $K = \mathbf{D}_{\mathbb{F}_p}(X^q - X)$ ($\mathbf{D}_{\mathbb{F}_p}(X^q - X)$ est le corps de décomposition $X^q - X$ sur $\mathbb{F}_p$) et $X^q - X$ a q racines distinctes.

▪ Réciproquement, soit $K = \mathbf{D}_{\mathbb{F}_p}(X^q - X)$, et soit k l'ensemble des racines dans K de $(X^q - X)$. L'application $g : K \to K : t \to t^q$ n'est autre que l'automorphisme de Frobenius itéré n fois, $\mathcal{F}^n$, donc g est un automorphisme de K. Par suite, $k = \{x \in K, g(x) = x\}$ est un sous-corps de K. Donc k contient $\mathbb{F}_p$, sous-corps premier de K. Le dérivé du polynôme $X^q - X$ est $qX^{q-1} - 1 = -1$ (car p divise q), qui est évidemment premier avec $X^q - X$.
Donc toutes les racines de $X^q - X$ sont simples. Ainsi $Card(k) = q$, k est un corps à q éléments (et, reprenant le premier point de cette démonstration), $k = K = \mathbf{D}_{\mathbb{F}_p}(X^q - X)$.

►Groupe des automorphismes d'un corps fini

Théorème 3.2.

Soit K un corps fini, de caractéristique p, de cardinal $q = p^n$. Le groupe des automorphismes de K est d'ordre $n = [K : \mathbb{F}_p]$. Il est cyclique, engendré par l'automorphisme de Frobenius :

$$\begin{aligned} \mathcal{F} : K &\longrightarrow K \\ x &\longmapsto \mathcal{F}(x) = x^p \end{aligned}$$

Preuve :

▪ Tout élément σ de $Aut(K)$ vérifie $\sigma(1_K) = 1_K$ et donc laisse fixe le sous-corps premier $\mathbb{F}_p$ de K : c'est donc un $\mathbb{F}_p$-automorphisme de K.
Ainsi :

$$Aut(K) = \mathbf{G}(K|\mathbb{F}_p)$$

Or K est un espace vectoriel sur $\mathbb{F}_p$ et $[K : \mathbb{F}_p] = n$.
Ainsi :

$$|Aut(K)| \leq n \quad (car \ \ |\mathbf{G}(K|\mathbb{F}_p)| \leq [K : \mathbb{F}_p] = n)$$

▪ Le Frobenius $\mathcal{F}$ est un automorphisme de corps de K (d'après Proposition 3-1)

▪ On montre aisément par récurrence que :

$$\forall k \in \mathbb{N}, \forall x \in K, \mathcal{F}^k(x) = x^{p^k}$$

L'ordre de $\mathcal{F}$ est :

$$\omega = min\{k \in \mathbb{N}^* | \forall x \in K, \mathcal{F}^k(x) = x\}$$

K^* est un groupe d'ordre $p^n - 1$, donc (théorème de Lagrange) :

$$\forall x \in K^*, x^{p^n-1} = 1_K$$

Donc

$$\forall x \in K, x^{p^n} = x$$

soit $\mathcal{F}^n = id_K$. Ainsi ω divise n.
Or

$$\mathcal{F}^n = id_K \Longleftrightarrow \forall x \in K, x^{p^n} = x$$

Le polynôme $X^{p^\omega} - X$ à coefficients dans le corps commutatif K et de degré p^ω a donc $card(K) = p^n$ racines, donc $p^\omega \geq p^n$. Ainsi $\omega = n$.

Sur un corps fini, le groupe de Galois de tout polynôme est cyclique engendré par l'automorphisme de Frobenius $\mathcal{F} : x \longmapsto x^p$.

Chapitre 4

Quelques exemples de groupes de Galois

La détermination de groupe de Galois d'un polynôme donné n'est pas toujours facile. Mais quelques remarques sont souvent utiles :
▪ Si un polynôme de degré n possède de manière évidente au moins m racines dans le corps de base, son groupe de Galois est un sous-groupe de S_{n-m}.
▪ Le degré du corps de rupture est souvent relativement facile à déterminer, et il donne l'ordre de groupe de Galois ; si p est cet ordre, le problème revient à trouver p bonnes permutations des racines, ou encore p automorphismes conservant le corps de base. On utilisera à cet effet la propriété suivante : l'image de tout élément (racine) par un tel automorphisme est encore racine de son polynôme minimum. cette remarque permet de limiter le nombre de ces automorphismes quand on connait des éléments engendrant le corps de rupture.
▪ Si le corps de rupture est donné a priori comme engendré par plusieurs éléments, on peut commencer par considérer les automorphismes conservant certains de ces éléments. Par exemple, si le corps de rupture est $\mathbb{Q}(\alpha, \beta)$, les automorphismes laissant fixe α, c'est-à-dire les $\mathbb{Q}(\alpha)$-automorphismes sont en nombre égal au degré de β sur $\mathbb{Q}(\alpha)$; on passera ensuite aux automorphismes qui ne laissent pas fixe α, ils transforment alors α en une autre racine de son polynôme minimum .

Exemples :

▪ Pour tout polynôme réel de degré 2 irréductible sur $\mathbb{R}$, le corps de rupture est $\mathbb{R}(i) = \mathbb{C}$, et le groupe de Galois est :

$$\mathbf{G}(P|\mathbb{R}) = \{id, \sigma\}$$

avec σ est la conjugaison complexe :

$$a + ib \longmapsto a - ib \quad \forall (a, b) \in \mathbb{R}^2$$

▪ Prenons maintenant un polynôme rationnel sans racine dans $\mathbb{Q}$.
Le corps de rupture est $\mathbb{Q}(\sqrt{\Delta})$ de degré 2 (Δ est le discriminant), formé de l'identité et d'un autre $\mathbb{Q}$-automorphisme.
Deux cas se présentent, suivant que Δ est négatif ou positif :
cas $\Delta < 0$: Les deux sont complexes conjuguées, le corps de rupture est

$$\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(i\sqrt{-\Delta})$$

est non réel, et l'automorphisme correspondant à l'échange des deux racines est la trace sur $\mathbb{Q}(\sqrt{\Delta})$ de la conjugaison complexe,soit

$$a + ib\sqrt{-\Delta} \longmapsto a - ib\sqrt{-\Delta}$$

$(a, b \in \mathbb{Q}, et\sqrt{-\Delta} \in \mathbb{R})$.
cas $\Delta > 0$: ici les deux racines sont réelles, le corps de rupture $\mathbb{Q}(\sqrt{\Delta})$ est réel et l'automorphisme autre que l'identité est :

$$a + b\sqrt{\Delta} \longmapsto a - b\sqrt{\Delta} \quad \forall (a, b) \in \mathbb{Q}$$

▪ Le groupe de $P(x) = x^3 - 1 = (x - 1)(x^2 + x + 1)$ sur $\mathbb{Q}$.
Les racines de P sont $1 \in \mathbb{Q}$ et $j = \frac{-1}{2} + i\frac{\sqrt{3}}{2}, j^2 \notin \mathbb{Q}$
Donc $\mathbf{G}(P|\mathbb{Q})$ est un sous-groupe de S_2
Or le corps de rupture est $\mathbb{Q}(j) = \mathbb{Q}(i\sqrt{3})$ de degré 2
Alors $\mathbf{G}(P|\mathbb{Q})$ est d'ordre 2 et :

$$\mathbf{G}(P|\mathbb{Q}) = \{id, \sigma_1\}$$

avec

$$id : a + ib\sqrt{3} \longmapsto a + ib\sqrt{3}$$

et

$$\sigma_1 : a + ib\sqrt{3} \longmapsto a - ib\sqrt{3}$$

▪ Les racines de polynôme $1 + X^2 + X^4$ sont les racines carrées de j et j^2, elles forment donc la suite $(-j^2, -j, j, j^2)$.
Le corps de rupture sur $\mathbb{Q}$ est :

$$\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$$

Donc le groupe de Galois est d'ordre 2, c'est le même pour $1 + X + X^2$ ou pour $X^3 - 1$.
La seule bonne permutation autre que l'identité correspond à $j \to j^2$, c'est-à-dire à la conjugaison complexe, c'est donc :

$$(-j^2, -j, j, j^2) \to (-j, -j^2, j^2, j)$$

que l'on écrit

$$(1\ 2)(3\ 4) \text{ en notation cyclique.}$$

4.1 Le groupe de Galois d'un polynôme de degré 3

Soit P un polynôme de degré 3 sur un corps K . Alors :
• P est irréductible si, et seulement si, il n'a pas de racine dans K ;
• Si P est réductible, il possède 1 ou 3 racines dans K (en tenant compte des ordres de multiplicité) ;
• Le groupe de Galois $\mathbf{G}(P)$ est un sous-groupe de S_3.
• Les seuls sous-groupes de S_3 autre que $\{id\}$ sont le groupe alterné A_3, d'ordre $3(= \frac{3!}{2})$, et les trois groupes d'ordre 2 formé par l'identité et une transposition (chacun est bien sûr isomorphe à C_2 cyclique d'ordre 2) ; seuls S_3 et A_3 sont transitifs.
D'où les premiers équivalences :

$$\mathrm{G(P)} = \{id\} \Leftrightarrow \mathrm{P \text{ est totalement factorisable sur K.}}$$
$$\mathrm{G(P)} = \mathrm{C_2} \Leftrightarrow \mathrm{P \text{ possède une, et une seule, racine dans K.}}$$

Dans ce dernier cas, l'échange des racines hors de K est la seule bonne permutation autre que l'identité.

Les deux cas restant correspondent donc aux polynômes de degré 3 irréductibles sur K le groupe de Galois est alors A_3 ou S_3, et il nous faut caractériser les deux circonstances.

Soit l'équation : $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$ avec $\alpha \neq 0$ on pose $x \to x - \frac{\beta}{3\alpha}$, on obtient l'équation : $x^3 + px + q = 0$
Partons donc de P irréductible sur K , et prenons-le directement sous la forme

$$\mathrm{P}(X) = \mathrm{X}^3 + p\mathrm{X} + q$$

Notons a, b, c ses racines, toutes hors de K et deux à deux distinctes (à cause de l'irréductibilité).
On a donc :

$$a + b + c = 0$$
$$ab + bc + ac = p$$
$$abc = -q$$

Il est clair que tout corps contenant a et b contient c : le corps de rupture est engendré par K et deux racines.
Mais si l'on connaît une racine a , on connaît la somme des deux autres, donc il suffit de connaitre leur différence.
Donc :

$$(b-c)^2 = (b+c)^2 - 4bc = a^2 + \frac{4q}{a} = \frac{a^3 + 4q}{a}$$
$$= \frac{-pa + 3q}{a} = -p + 3\left(-a^2 - p\right)$$

d'où finalement les égalités :

$$(b-c)^2 = -3a^2 - 4p$$
$$a = \frac{3q}{(b-c)^2 + p}$$

Tout corps contenant a contient $(b-c)^2$, et réciproquement. En particulier, le corps de rupture est engendré par K et $(b-c)$.

Le corps de rupture d'une équation de degré 3 est engendré par le corps de base et la différence de deux racines.

En conclusion, le corps de rupture de X^3+pX+q est l'extension simple $K(b-c)$, égale encore à :

$$\mathrm{K}\left(\sqrt{-3a^2-4p}\right)$$

L'ordre du groupe de Galois est égal au degré de $x = \sqrt{-3a^2-4p}$ sur K :ce degré devra être 3 ou 6, le groupe de Galois correspondant étant respectivement A_3 et S_3.
On trouve facilement une équation dont x^2 est racine, en effectuant, dans l'équation aux carrés de $P(X) = 0$, la substitution de X par $-\frac{X+4p}{3}$. Plus précisément, l'équation aux carrés est :

$$X(X+p)^2 - q^2 = 0$$

Soit

$$\mathrm{X}^3 + 2p\mathrm{X}^2 + p^2\mathrm{X} - q^2 = 0$$

et la substitution de X par $-\frac{X+4p}{3}$ donne :

$$-\frac{\mathrm{X}+4p}{3}\left(\frac{-\mathrm{X}-p}{3}\right)^2 - q^2 = 0$$
$$(\mathrm{X}+4p)(\mathrm{X}+p)^2 + 27q^2 = 0$$
$$\mathrm{X}(\mathrm{X}+3p)^2 + 4p^3 + 27q^2 = 0$$

Autrement dit, l'élément primitif

$$x = b - c = \sqrt{-3a^2-4p}$$

est racine de polynôme de degré 6 :

$$\mathrm{Q} = \mathrm{X}^2\left(\mathrm{X}^2+3p\right)^2 + 4p^3 + 27q^2$$

Tout va dépendre de l'irréductibilité de ce polynôme : s'il est irréductible, le corps de rupture est degré 6 et le groupe de Galois est S_3; sinon, c'est A_3.

Notons que les racines de Q sont les six différences deux à deux des racines.

Le discriminant au degré 3 :

Au point où on en est, on voit réapparaitre la fameuse expression :

$$\Delta = -4p^3 - 27q^2$$

appelée **discriminant** du polynôme

$$\mathrm{P} = \mathrm{X}^3 + p\mathrm{X} + q$$

C'est l'opposé du produit des différences deux à deux des racines, car c'est l'opposé du terme constant Q(0) de Q. En d'autres termes, on peut écrire :

$$\Delta = (a-b)^2(a-c)^2(b-c)^2$$

et la nullité de Δ équivaut, dans le cas général, à l'existence d'une racine multiple (bien entendu la question ne se pose pas ici car notre polynôme est supposé irréductible).

Revenons au problème de l'irréductibilité, sur K, de

$$\mathrm{Q} = \mathrm{X}^2\left(\mathrm{X}^2+3p\right)^2 - \Delta$$

• Si Δ possède une racine carrée dans K, la décomposition

$$\mathrm{Q} = \left(\mathrm{X}\left(\mathrm{X}^2+3p\right) + \sqrt{\Delta}\right)\left(\mathrm{X}\left(\mathrm{X}^2+3p\right) - \sqrt{\Delta}\right)$$

dans K[X] montre que Q est réductible, donc le groupe de Galois est A_3
• Montrons réciproquement que, si Q est réductible sur K, alors Δ possède une racine carrée dans K. Notons d'abord que, si Q est réductible, il a forcément un facteur irréductible de degré 3 . Posons donc Q = RS, avec R irréductible de degré 3 sur K. L'égalité $\mathrm{Q}(X) = \mathrm{Q}(-X)$ donne :

$$\mathrm{R(X)S(X)} = \mathrm{R}(-\mathrm{X})\mathrm{S}(-\mathrm{X})$$

d'où l'on déduit que $\mathrm{R}(X)$ divise $\mathrm{R}(-X)$ ou $\mathrm{S}(-X)$.
En prenant les coefficients dominants de R et S égaux à 1, ce que l'on peut toujours faire, il reste soit l'égalité :

$$\mathrm{R(X)} = -\mathrm{S}(-\mathrm{X})$$

soit l'égalité

$$\mathrm{R(X)} = -\mathrm{R}(-\mathrm{X})$$

Le dernier cas donne R(0) = 0, d'où $Q(0) = 0$ et $\Delta = 0$, ce qui est à exclure comme on l'a signalé (irréductibilité de P).
Reste donc la condition $R(X) = -S(-X)$. d'où :

$$\mathrm{Q(X)} = -\mathrm{R(X)R}(-\mathrm{X})$$

qui donne

$$Q(0) = -(R(0))^2$$

et Δ est le carre de $\mathrm{R}(0) \in \mathrm{K}$.
Autrement dit. dans le cas irréductible, ou bien Δ n'a pas de racine carrée dans K, et alors le corps de rupture est de degré 6 et le groupe de Galois est S_3 , ou bien Δ a une racine carrée dans K et le corps de rupture est de degré 3, le groupe de Galois étant A_3.
Dans ce dernier cas, chaque racine est élément primitif du corps de rupture.
Dans le premier cas ($\sqrt{\Delta} \notin \mathrm{K}$) toutes les permutations des racines sont bonnes,alors que. dans le second cas, les transpositions sont des mauvaises permutations : on le voit directement en considérant la relation rationnelle suivante sur K

$$(a-b)(b-c)(a-c) = \sqrt{\Delta}$$

qui n'est pas respectée par une transposition de deux racines.

Si l'on veut compléter le rôle du discriminant pour tous les cas, il convient d'examiner aussi les cas où

$$\mathrm{P} = \mathrm{X}^3 + p\mathrm{X} + q$$

est réductible, ce qui correspond aux groupes de Galois $\{id\}$ ou C_2

•$\mathrm{G(P)} = \{id\}$: alors a, b, c sont dans K, et

$$(a-b)(b-c)(c-a)$$

est une racine carrée de Δ dans K.

•$\mathrm{G(P)} = \mathrm{C}_2$: il y a une racine dans K, soit a, et deux hors de K, racines du polynôme de degré 2 irréductible sur K

$$\frac{\mathrm{P(X)}}{\mathrm{X}-a} = \mathrm{X}^2 + u\mathrm{X} + v$$

En ce cas $(b-c)^2$ est égal à $u^2 - 4v$, donc sans racine carrée dans K, alors que $a-b$ et $a-c$ ont pour produit

$$a^2 - (b+c)a + bc$$

qui est dans K : donc Δ est égal à

$$\left(a^2 + ua + v\right)^2 \left(u^2 - 4v\right)$$

et n 'a pas de racine carrée dans K.

Si l'on récapitule, on écrira dans tous les cas :

$$\sqrt{\Delta} \notin \mathrm{K} \Leftrightarrow \mathrm{G(P)} = S_3 \text{ ou } \mathrm{G(P)} = \mathrm{C}_2$$
$$\sqrt{\Delta} \in \mathrm{K} \Leftrightarrow \mathrm{G(P)} = \mathrm{A}_3 \text{ ou } \mathrm{G(P)} = \{id\}$$

Dans le cas irréductible, seule la première partie des seconds membres est à retenir.

Une remarque : si le coefficient de X^2 n'est pas nul, la transformation usuelle permet le calcul du discriminant de

$$X^3 + a_1X^2 + a_2X + a_3$$

On trouve

$$\Delta = 18a_1a_2a_3 - 4a_1^3a_3 + a_1^2a_2^2 - 4a_2^3 - 27a_3^2$$

Quelques exemples au degré 3 :

• Sur $\mathbb{R}$, une équation de degré 3 a toujours une racine réelle, le groupe de Galois est donc C_2 ou id, ceci suivant que $\Delta = -4p^3 - 27q^2$ est strictement négatif ou non.
Dans le cas $\Delta < 0$ il y a une unique racine réelle, alors que pour $\Delta \geqslant 0$ il y en a trois, toutes simples, si Δ est non nul, et une double ou une triple si Δ est nul.
• Le discriminant de $1 + X + X^3$ est $\Delta = -4 - 27 = -31$ sans racine carrée dans Q. Comme le polynôme n'a pas de racine dans $\mathbb{Q}$, il y est irréductible, et son groupe de Galois sur $\mathbb{Q}$ est S_3 : il y a six automorphismes du corps de rupture (sous-corps de $\mathbb{C}$) correspondant aux six permutations des trois racines complexes.
Le fait que $1 + \mathrm{X} + \mathrm{X}^3$ n'ait pas de racine rationnelle s'obtient en écrivant que $\frac{p}{q}$(p et q premiers entre eux) est racine, d'où légalité

$$q^3 + pq^2 + p^3 = 0$$

qui montre que p divise q et q divise p.
• Les deux polynômes :

$$1 - 3X + X^3 \quad \text{et} \quad 1 + 3X + X^3$$

sont irréductibles sur $\mathbb{Q}$, car sans racines, leurs discriminants valent 81 et -135, donc les groupes de Galois sont respectivement A_3 et S_3.

4.2 Groupe de Galois du corps cyclotomique

Définition 4.1.

On appelle fonction ***indicatrice d'Euler*** *la fonction* $\varphi : \mathbb{N} \to \mathbb{N}$ *qui à* n *associe le nombre* $\varphi(n)$ *d'entiers* $\{1, ..., n\}$ *premiers avec* n.
$\varphi(n)$ *est le cardinale du groupe des éléments inversibles dans l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, *en particulier* $\varphi(n) = n - 1$ *si* n *premier.*

Définition 4.2.

Soit $m \in \mathbb{N}^*$. *Considérons l'ensemble* $\mathbb{U}_m = \{z \in \mathbb{C} : z^m = 1\}$ *des racines* m*-ièmes de l'unité dans* $\mathbb{C}$.
$\mathbb{U}_m$ *est un groupe cyclique d'ordre* m *pour la multiplication (l'application* $\mathbb{Z}/m\mathbb{Z} \to \mathbb{U}_m$ *est un isomorphisme de groupes).*
On appelle ***racine primitive*** m*-ième de l'unité tout générateur de* $\mathbb{U}_m$ *, c'est-à-dire tout élément* ξ *de* $\mathbb{U}_m$ *tel que* $\xi^d \neq 1$ *pour* $1 \leq d < m$.
On notera $\mathbf{P}_m(\mathbb{C})$ *l'ensemble des racines primitives* m*-ièmes de l'unité.*

Proprété 4.1.

$\mathbf{P}_m(\mathbb{C}) = \{exp(2i\pi k/m), 1 \leq k < m,$ *k premier avec* $m\}$ *a pour cardinal* $\varphi(m)$.

Propositions 4.1.

Soit $m \in \mathbb{N}^*$. *Soit* ξ *une racine primitive* m*-ième de l'unité dans* $\mathbb{C}$. *Alors les racines primitives* m*-ièmes de l'unité sont les* ξ^k, *où* $1 \leq k \leq m$ *et* k *est premier avec* m.

Lemme 4.1.

Soit n *un entier naturel,* $n \geq 2$, $a \in \mathbb{N}$, *et* $\bar{a}$ *la classe de* a *modulo* n.
Les conditions suivantes sont équivalentes :

1) a *et* n *sont premiers entre eux,*
2) $\bar{a}$ *est un générateur du groupe additif* $\mathbb{Z}/n\mathbb{Z}$.

Preuve :

On considère les éléments suivants de $\mathbb{Z}/n\mathbb{Z}$, où a est un entier, $\overline{a}$ son image dans $\mathbb{Z}/n\mathbb{Z}$:

$$0, \overline{a}, 2\overline{a}, \ldots, m\overline{a}, \ldots, (n-1)\overline{a}$$

1) Si a est premier à n, alors $\overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.
Si $m\overline{a} = 0$, alors $ma \equiv 0(\text{ mod. } n)$, alors $ma = rn$. Si a est premier à n, comme $n|ma$, alors $n|m$ ce qui est impossible car $m < n$. Donc pour tout $m < n, m\overline{a} \neq 0$, donc les éléments $0, \overline{a}, 2\overline{a}, \ldots, m\overline{a}, \ldots, (n-1)\overline{a}$ sont distincts. Donc $\overline{a}$ est bien générateur de $\mathbb{Z}/n\mathbb{Z}$.
2) Si a n'est pas premier à n, alors $\overline{a}$ n'est pas un générateur de $\mathbb{Z}/n\mathbb{Z}$.
Soit p tel que $p|a$ et $p|n$.

On a $\frac{n}{p}a = \frac{a}{p}n$, donc $\frac{n}{p}a \equiv 0(\text{ mod. } n)$

Donc les éléments $0, \overline{a}, 2\overline{a}, \ldots, m\overline{a}, \ldots, (n-1)\overline{a}$ ne sont pas distincts.
Alors $\overline{a}$ n'est pas un générateur de $\mathbb{Z}/n\mathbb{Z}$.

Preuve (Proposition 4-1) :
Comme ξ est d'ordre m, l'application $\mathbb{Z}/m\mathbb{Z} \to \mathbb{U}_m$,$\bar{k} \mapsto \xi^k$ est un isomorphisme de groupes. D'où de suite, d'après (Lemme 4.1), le résultat annoncé.

Définition 4.3.

Le sous-corps $\mathbb{Q}(\xi)$ de $\mathbb{C}$ ne dépend pas de la racine m-ième primitive ξ de l'unité dans $\mathbb{C}$ considérée. Le sous-corps $\mathbb{Q}(\mathbb{U}_m)$ de $\mathbb{C}$ engendré par les racines m-ièmes de l'unité, qui est $\mathbb{Q}(\xi)$ où ξ est une racine primitive m-ième quelconque, est appelé ***corps cyclotomique d'indice*** *m .*

Définition 4.4.

Soit $m \in \mathbb{N}^*$. On appelle m-ième ***polynôme cyclotomique*** *le polynôme :*

$$\Phi_{m,\mathbb{Q}}(X) = \prod_{\xi \in \mathbf{P}_m} (X - \xi)$$

$\Phi_{m,\mathbb{Q}}$ est un polynôme unitaire de degré $\varphi(m)$ à coefficients dans $\mathbb{C}$.

Propositions 4.2.

On a :

$$X^m - 1 = \prod_{d/m} \Phi_{d,\mathbb{Q}}(X)$$

Lemme 4.2.

Soit $m \in \mathbb{N}^*$. Les $\mathbf{P}_d$, d décrivant l'ensemble des diviseurs de m dans $\mathbb{N}^*$, forment une partition de $\mathbb{U}_m$.

Preuve :

Si d divise m, $\mathbf{P}_d(\mathbb{C}) \subseteq \mathbb{U}_d \subseteq \mathbb{U}_m$.
Chaque racine m-ième de l'unité dans $\mathbb{C}$ a un unique ordre (multiplicatif) qui est un diviseur de m d'après le théorème de Lagrange ; autrement dit chaque élément de $\mathbb{U}_m$ appartient à un et un seul des $\mathbf{P}_d(\mathbb{C})$, d diviseur de m.

Preuve (Proposition) : Soit $\omega^k = exp(\frac{2\pi ik}{m})$ pour $0 \leq k \leq m-1$ et soit d l'ordre de w^k dans $\mathbb{U}_m$. On a nécessairement $d|m$. Par ailleurs, $\left(w^k\right)^d = 1$, on a donc $w^k \in \mathbb{U}_d$ et w^k étant d'ordre d, on a $\left|< w^k >\right| = d = |\mathbb{U}_d|$.
On a donc $w^k \in \mathbf{P}_d$
Ainsi, $\left(X - w^k\right)$ divise Φ_d et, par conséquent, divise $\prod_{d|m} \Phi_d$

Les valeurs $w^k (0 \leq k \leq m-1)$ étant distinctes, les polynômes $\left(X - w^k\right)$ sont donc premiers entre eux.
On en déduit que $X^m - 1 = \Pi_{k=0}^{m-1} \left(X - w^k\right)$ divise $\Pi_{d|m} \Phi_d$.
Ces polynômes étant, de plus, unitaires et de même degré car :

$$\sum_{d|m} \deg\left(\Phi_d\right) = \sum_{d|m} \varphi(d) = m$$

Alors ils sont égaux.

Théorème 4.1. ***Groupe des automorphismes d'un corps cyclotomique***
Soient $n \geqslant 2$ un entier et ξ une racine primitive n-ième de l'unité dans $\mathbb{C}$,
a) $\mathbb{Q}(\xi)$ *est une extension de* $\mathbb{Q}$ *;*
b) $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$ *;*
c) $\mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q}) \simeq \mathbf{U}(\mathbb{Z}/n\mathbb{Z})$ *; en particulier le groupe est abélien.*
$\mathbf{U}(\mathbb{Z}/n\mathbb{Z})$ *ensemble des éléments inversibles de l'anneau* $\mathbb{Z}/n\mathbb{Z}$

Preuve :
a) $\mathbb{Q}(\xi)$ est en effet le corps de décomposition de $X^n - 1$, ou de Φ_n, sur $\mathbb{Q}$
b) Le polynôme minimal de ξ sur $\mathbb{Q}$ est Φ_n dont le degré est $\varphi(n)$
c) Posons $G = \mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})$ et soit $\sigma \in G$; σ est déterminée par $\sigma(\zeta)$ qui, étant conjugué de ζ, est une racine primitive n-ième de l'unité donc de la forme ξ^k avec k premier avec n; ceci permet de construire une application $\psi : G \to \mathbf{U}(\mathbb{Z}/n\mathbb{Z})$ définie par $\psi(\sigma) = k$.
Si $\sigma'(\xi) = \xi^{k'}$, on a $(\sigma \circ \sigma')(\xi) = \sigma\left(\xi^{k'}\right) = \xi^{kk'}$ d'où $\psi(\sigma \circ \sigma') = \psi(\sigma) \cdot \psi(\sigma')$, ce qui prouve que ψ est un homomorphisme de groupes.
ψ est injectif car si $\psi(\sigma) = 1$ on a $\sigma = id$; comme

$$|G| = [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n) = |\mathbf{U}(\mathbb{Z}/n\mathbb{Z})|$$

ψ est un isomorphisme.

Remarque 4.1.
Par conséquent $\mathbf{G}(\mathbb{Q}(\mathbb{U}_n)|\mathbb{Q})$ *est d'ordre* $\varphi(n)$*, est toujours abélien, et il est cyclique si, et seulement si,* $\mathbf{U}(\mathbb{Z}/n\mathbb{Z})$ *est cyclique. (on sait que* $\mathbf{U}(\mathbb{Z}/n\mathbb{Z})$ *est cyclique).*

Si n est premier, le groupe de Galois de $X^n - 1$ sur $\mathbb{Q}$ est cyclique d'ordre $n-1$

4.3 Groupe de Galois d'une équation binôme $X^n - a$

Soient K un corps, et $P(X) = X^n - a \in K[X]$, avec $a \in K$.
Appelons α une racine n-ième de a dans le corps de rupture, et ω_n une racine

primitive n-ième de l'unité (par exemple $\omega_n = e^{\frac{2i\pi}{n}}$ dans le cas d'un sous-corps de $\mathbb{C}$). La famille des racines de $X^n - a$ est :

$$\alpha, \omega_n\alpha, \omega_n^2\alpha, \ldots, \omega_n^{n-1}\alpha$$

et le corps de rupture est $\mathrm{K}(\alpha, \omega_n)$.
Tout K-automorphisme est donné par l'image de α et l'mage de ω_n alors qu'un $\mathrm{K}(\omega_n)$-automorphisme est donné par l'image de α seulement.
Bornons-nous aux $\mathrm{K}(\omega_n)$-automorphismes. Tout $\sigma \in \mathrm{G}(\mathrm{K}(\alpha, \omega_n) | \mathrm{K}(\omega_n))$ est déterminé par $\sigma(\alpha)$ qui est de la forme $\omega_n^q\alpha$. Pour σ et τ dans le groupe de Galois ,l'égalité :

$$\tau\sigma(\alpha) = \omega_n^q\tau(\alpha)$$

montre qu'au produit de deux $\mathrm{K}(\omega_n)$-automorphismes correspond la somme modulo n des exposants de ω_n.
Bref, l'application $\sigma \to q$ est un homomorphisme injectif de groupes du groupe de Galois dans le groupe additif des entiers modulo n, c'est-à-dire le groupe cyclique d'ordre n.

Sur un corps contenant les racines n-ièmes de l'unité, le groupe de Galois d'une équation binôme de degré n est un sous-groupe du groupe cyclique d'ordre n.

En particulier, ce groupe est lui-même cyclique, d'ordre diviseur de n. Or cet ordre est le degré, sur $\mathrm{K}(\omega_n)$, du corps de rupture.

Sur un corps contenant les racines adéquates de d'unité, le degré du corps de rupture d'une équation binôme divise le degré de l'équation.

Bien entendu, le groupe de Galois peut être un sous-groupe propre de C_n; le cas extrême est celui où a possède une racine n-ième dans le corps de base, car alors le groupe de Galois est l'identité.
D'autre part, le groupe de Galois de $X^n - a$ sera C_n tout entier si, et seulement si, le corps de rupture est de degré n. Comme il est engendré par une racine n-ième arbitraire de a, cette racine doit avoir un polynôme minimum de degré n, ce qui équivaut à dire que $X^n - a$ est irréductible.

Sur un corps contenant les racines n-ièmes de l'unité, le groupe de Galois d'une équation binôme de degré n est le groupe cyclique d'ordre n si, et seulement si, elle est irréductible.

Un cas particulier important est celui où le degré est premier. Si p est premier, les seuls sous-groupes de C_p sont C_p et $\{id\}$, donc le corps de rupture de $X^p - a$ est soit de degré p sur K(et alors le polynôme est irréductible), soit égal à K (et alors K contient une racine p-ième de a, donc toutes).

Si p est premier et si a n'a pas de racine p-ième dans un corps K contenant les racines p-ièmes de l'unité, le groupe de Galois de $\mathbf{X}^p - a$ est cyclique d'ordre p.

Conclusion

Nous avons vu au cours de ce travail que si K un corps, et $P \in K[X]$ un polynôme de degré n et des racines $\{a_1, a_2, ..., a_m\}$, et L son corps de rupture . le groupe de Galois de P sur K noté $G(P|K)$ est le groupe formé des bonnes permutation des racines, donc c'est un sous-groupe de groupe symétrique S_m, ou bien c'est le groupe des K-automorphismes de L. de plus l'ordre de ce groupe est égale à le degré de l'extension L/K, et on a $dim_K L = [L : K] = |G(P|K)|$.
Si P est réductible dans $K[X]$, $P = ST$, le groupe $G(P|K)$ est un sous-groupe de produit $G(S|K) \times G(T|K)$,
Si K est fini, la groupe de Galois de tout polynôme de $K[X]$ est cyclique, engendré par l'automorphisme de Frobenius $\mathcal{F} : x \longmapsto x^p$.
Pour un polynôme P de degré 3 , le corps de rupture L est engendré par le corps de base K et la différence de deux racines , si Δ le discriminent de P,on a :

$$\sqrt{\Delta} \notin \mathrm{K} \Leftrightarrow \mathrm{G(P)} = S_3 \text{ ou } \mathrm{G(P)} = \mathrm{C}_2$$
$$\sqrt{\Delta} \in \mathrm{K} \Leftrightarrow \mathrm{G(P)} = \mathrm{A}_3 \text{ ou } \mathrm{G(P)} = \{id\}$$

dans le cas P est irréductible, seule la première partie des seconds membres est à retenir.
Le groupe de Galois de polynôme $X^n - 1$ sur $\mathbb{Q}$ est cyclique , de plus si n premier le groupe est d'ordre $n - 1$
Soit $a \in K$, le corps de rupture de l'équation binôme $X^n - a$ est engendré par K et α une racine n-ième de a , et une racine primitive n-ième de l'unité ω_n, si K contenant les racines n-ièmes de l'unité, le groupe de Galois de l'équation binôme est un sous-groupe du groupe cyclique d'ordre n., mais si n est premier et si a n'a pas de racine n-ième dans K contenant les racines n-ièmes de l'unité, le groupe de Galois de $X^n - a$ est cyclique d'ordre n.

Bibliographie

[1] Claude Mutafian, **Équations algébriques et théorie de Galois**,(1980).

[2] Y.Gozard, **Théorie de Galois**,Ellipses Marketing (1997).

[3] A.Jeanneret, D.Lines ,**Invitation à l'algèbre** : Théorie des groupes, des anneaux, des corps et des modules, Editions Cépaduès (2008).

[4] D.Perrin, **Cours d'algèbre**,Ellipses Marketing (1998).

[5] J.Escofier,**Théorie de Galois** :Cours et exercices corriges,Dunod (2000)

[6] P.Tauvel,**Corps communicatifs et théorie de Galois** :Cours et exercices (2008)

[7] J.Calais,(Mathématiques à l'Université)**Extensions de corps et Théorie de Galois** , Niveau M1-M2-Ellipses Marketing (2006)