Université de M'sila Mohamed Boudiaf
Faculté des Mathématiques et d'Informatiques
Departement des Mathématiques

Mémoire: Troisième Année L.M.D

THÈME

Rédige Par:

1)Nom Prenom

2)Nom Prenom

3)Nom Prenom

Dirigé par:

M

Année: **2012/2013**

Remerciements

En premier lieu Je remercie **ALLAH** pour m'avoir guidé et donner la force pour la finalisation de ce mémoire. Je tiens également à exprimer mes plus vifs remerciements à Monsieur **Lajelat Lahcene** MA/A à univ.de M'sila pour l'intéressant sujet qu'il m'a proposé.. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes. Je lui suis également reconnaissant pour la confiance qu'il ma accordée J'exprime ici ma profonde gratitude à Monsieur **D. Mihoubi**, Professeur à universite de M'sila. pour m'avoir fait l'honneur de présider mon jury . Je remercie vivement Messieurs **H. Lakhadar**, MA/A à univ.de M'sila Je ne saurais oublier de remercier tous mes professeurs et toutes les personnes ayant contribué de près ou de loin à l'aboutissement de ce travail.

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis, en particulier mes parents pour leur soutient tout au long de mes études.

Finalement ,nous ne manquerons pas de remercier nos collègues pour l'échange d'idées scientifiques qu'on faisait de temps en temps afin d'enrichir nos connaissances dans le domaine de notre spécialité

.

Abstract

This thesis involves the study of the structural properties of the Galois extension. In the first chapter we study the field extension, we tried to define the notions of simple extension, finite, algebraic, and present some properties This chapter brings together some elements of the theory of commutative fields, This theory is closely linked to that of an equation. If a polynomial with coefficients in field F, not necessarily accepts roots in F. we show that it is always possible to construct an extension of F in which the polynomial has all its roots and to be called the splitting field of the polynomial. In the end of this chapter we define two important concepts for this work: the normal extension and separable extension.

In the second chapter we first define the notion of the Galois extension and present some example, Then treat the theory of Galois, This theory allows to establish a correspondence between sub splitting field of a polynomial and sub normal group of group said Galois group of the polynomial and express it in an example.

In the third and last chapter we approach one of Galois theory applications in algebra, the solvable equations by radical, That means solving the equation using the four operations and the extraction of radicals only.

Keywords : algebraic extension, separable Extension, normal Extension, Galois Extension, Galois group , solvable group , Extension by radicals, solvable equation .

.

Résumé

Ce mémoire porte sur l'étude des propriétés structurales de l'extension galoisienne. Dans le premier chapitre intitulé l'extension de corps, on a essayé de définir la notion de l'extension simple, finie, algébrique, et de présenter quelques propriétés et citer quelques remarques. Ce chapitre rassemble quelques éléments de la théorie des corps commutatifs, cette théorie est étroitement liée à celle des équation. Si un polynome à cofficients dans corps F, n'admet pas nécessairement de racines dans F, nous montrerons qu'il est toujours possible de construire une extension de F dans laquelle le polynôme a toutes ses racines et qui sera appelé le corps de décomposition du polynôme. En fin de ce chapitre on a défini deux concepts importents pour ce travail : l'extension normale et l'extention séparable.

. Dans le deuxième chapitre on définit d'abord la notion de l'extension galoisienne (par fois nommé extension de Galois) et présenter quelque exemple. Puis, on traite la theorie de Galois. Cette théorie permet d'établir une correspondance entre des sous corps de décomposition d'un polynome et les sous groupes normaux d'un groupe dit groupe de Galois du polynome et nous examinons cela dans un exemple.

Dans le troisième chapitre on aborde l'une des applications de la théorie de Galois les équations résolubes par radicaux, Cela signifie que la résolution de l'équation en utilisant seulement les quatre opérations et les extaction radicales

Mots clés : Extension algébrique,Extension séparable, Extension normal ,Extension galoisienne, groupe de Galois, Groupe résoluble, Extension par radicaux, Equation résoluble .

Table des matières

Notations

- $F[\alpha]$: Le plus petite sous anneau de E qui contient à la fois F et α.
- $F(\alpha)$: Le plus petits sous corps qui contient à la fois F et α.
- $p(X)$: Le polynôme minimale.
- $[E : F]$: Le degré de l'extension.
- $G = Gal(E/F)$: Le groupe de Galois .
- S_n : Le goupe de permetation.
- A_n : Le groupe Altérne
- $C(M)$: Corps associeé à soue groupe M.

Introduction

La démarche qui débouche sur la notion d'extension de Galois (parfois nommée extension galoisienne) provient de la volonté de résoudre des conjectures, souvent vieilles et provenant de différentes branches des mathématiques : l'algèbre avec l'étude des équations algébriques et particulièrement les équations polynomiales, la géométrie avec initialement les problèmes de la construction à la règle et au compas et particulièrement les trois grands problèmes de l'antiquité comme la duplication du cube et surtout les problèmes d'arithmétique comme le dernier théorème de Fermat. Tous les problèmes initiaux cités s'expriment simplement, leurs énoncés ne demandent en effet qu'un niveau mathématique élémentaire. En revanche leurs résolutions ont demandé des siècles de patience. La raison réside dans le fait qu'une approche naïve ne permet pas d'appréhender les finesses qu'impliquent les énoncés. Pour apporter des solutions, il est nécessaire de comprendre les structures sous-jacentes à chacune de ces questions. Une analyse directe impose une démarche calculatoire trop complexe pour aboutir. Quitte à augmenter le niveau d'abstraction, il apparaît alors nécessaire de définir des structures algébriques pures, bénéficiant de théorèmes puissants qui résolvent ces vieux problèmes.

L'extension de Galois est archétypale de cette approche algébrique pure. Et cette structure dispose d'un théorème puissant, à la base de toutes les résolutions modernes des différents problèmes cités. C'est le théorème fondamental de la théorie de Galois. Ce théorème établit une relation entre un corps et un groupe. Il permet d'établir un pont entre la théorie des groupes et les problèmes d'algèbre, de géométrie ou d'arithmétique étudiés. Dans l'énoncé du théorème fondamental, le corps, le groupe et la correspondance entre les deux sont abstraits. En échange de cette abstraction, l'extension de Galois offre un cadre très général à l'étude de nombreux problèmes.

En mathématiques et plus précisément en algèbre, la théorie de Galois est l'étude des extensions de corps commutatifs, par le biais d'une correspondance avec des groupes de transformations sur ces extensions, les groupes de Galois. Cette méthode féconde, qui constitue l'exemple historique, a essaimé dans bien d'autres branches des mathématiques, avec par exemple la théorie de Galois différentielle, ou la théorie de Galois des revêtements (Cette theorie)(La théorie de Galois) est née au XIX éme siécle pour étudier l'existence de formules pour les solutions d'une ´equation polynomiale (en fonction des coefficients de l'équation). Cett théorie, à la fois puissante et élégante, fut à lérigine d'un pan entier de l'algébre moderne, et a depuis connu un développement considérable. Elle demeure un sujet de recherche extrémement actif. L'objet de ce memoir est dans un premier temps d'introduire les bases et outils d'algébre générale (extensions de corps...) qui permettront dans un deuxiéme temps de développer la théorie de Galois, ainsi quelques applications.

Dans le premier chapitre intitulé l'extension de corps, on a essayé de définir la notion de l'extension simple, finie, algébrique, et de présenter quelques propriétés et citer quelques remarques. Ce chapitre rassemble quelques éléments de la théorie des corps commutatifs, cette théorie est étroitement liée à celle des équation. Si un polynome à cofficients dans corps F, n'admet pas nécessairement de racines dans F, nous montrerons qu'il est toujours possible de construire une extension de F dans laquelle le polynôme a toutes ses racines et qui sera appelé le corps de décomposition du polynôme. En fin de ce chapitre on a défini deux concepts importents pour ce travail : l'extension normale et l'extention séparable.

Dans le deuxième chapitre on définit d'abord la notion de l'extension galoisienne par fois nommé (extension de Galois) et présenter quelque exemple. Puis, on traite la theorie de Galois. Cette théorie permet d'établir une correspondance entre des sous corps de décomposition d'un polynome et les sous groupes normaux d'un groupe dit groupe de Galois du polynome et nous exprimons cela dans un exemple.

Dans le troisième chapitre on aborde l'une des applications de théorie de Galois : les équations résolubes par radicaux

,

Chapitre 1

Extension de corps

1.1 Extension de corps

1.1.1 Quelques préliménaires sur les extensions

Définition 1.1.1 *Soient F et E deux corps commutatifs. Si $F \subseteq E$ on dit que E est une extension de F .*

Exemple 1.1.1 $\mathbb{R}$ *est une extension de* $\mathbb{Q}$

$\mathbb{C}$ *est une extension de* $\mathbb{R}$ *.*

Remarque 1.1.1 *On pourrait définir la notion d'extension de F par la donnée d'un corps commutatif E et d'un homomorphisme de corps*

$$\phi : F \to E$$

Mais tout homomorphisme non nul de corps est injectif. Ainsi l'image $\phi(F)$ de F dans E est un sous-corps de E isomorphe au corps F. Le corps Eest donc une extension de $\phi(F)$. Modulo cet isomorphisme on retrouve la définition précédente, E est une extension de F (à un isomorphisme prés).

Remarque 1.1.2 *Si E est une extension de F alors E est un espace vectoriel sur F avec l'operation interne:*

$$\begin{array}{rcl} + & : & E \times E \longrightarrow F \\ (x, y) & \longrightarrow & x + y \end{array}$$

et le produit par un scalaire(l'operation externe)

$$\begin{array}{rcl} \bullet & : & F \times E \longrightarrow E \\ (\lambda, x) & \longrightarrow & \lambda \cdot x \end{array}$$

Proposition 1.1.1 *Soient E une extension de F et $\alpha \in E$, si on définit :*

$$F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$$

et

$$F(\alpha) = \{f(\alpha)/g(\alpha) \mid f(x), g(\alpha) \in F[x] \text{ avec } g(\alpha) \neq 0\}$$

alors :

1) $F[\alpha]$ est le plus petite sous anneau de E qui contient à la fois F et α.

2) $F(\alpha)$ est le plus petits sous corps qui contient à la fois F et α.

1.1.2 Extension simple

Définition 1.1.2 *Soit E une extension d'un corps F et soit α un element de E n'appartenant pas à F. On apelle extension simple de E le plus petit sous corps de E contenant F et α. C'est à dire $F(\alpha)$*

Exemple 1.1.2 $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ *est une extension simple de $\mathbb{Q}$.*

Définition 1.1.3 *Soit E une extension de F. Un element $\alpha \in E$ est dit algébrique sur F si il existe un polynome non nul $f \in F[X]$ tel que $f(\alpha) = 0$.*

α est dit transcendent dans le cas contraire, c'est à dire s'il n'existe aucun polynome $f \in F[X]$ tel que $f(\alpha) = 0$ autre que le polynome nul.

Exemple 1.1.3 *$\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ car $\alpha = \sqrt{2}$ est une racine de $x^2 - 2 \in \mathbb{Q}$.*

$\beta \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car $\beta = \sqrt{2} + \sqrt[3]{7}$ est une racine de

$$X^6 + 30X^4 - 14X^3 + 50X^2 - 84X + 57 \in \mathbb{Q}.$$

π est trancendant sur $\mathbb{Q}$.

e est trancendant sur $\mathbb{Q}$.

Théorème 1.1.1 *Soit E une extension de F et soit $\alpha \in E$ un element algébrique sur F,alors il existe un unique polynôme normalisé $p(X) \in F[X]$ tel que :*

(1) $p(\alpha) = 0$

(2) *$p(X)$ est irréductible*

(3) *si il existe $f(x) \in F[X]$ tel que $f(\alpha) = 0$ alors $p(X)$ divise $f(X)$.*

L'unique polynome $p(X) \in F[X]$ du théorème précedent est appelé le polynôme minimal de α sur F. noté $p(x) = irr(\alpha, F, X)$.

Définition 1.1.4 *Le degré de α sur F est par definition le degré du polynome minimale $p(X)$ et on ecrit*

$$\deg_F(\alpha) = \deg\,(\mathrm{p(X)}).$$

Exemple 1.1.4 *1) $\alpha \in F$ est un élément algébrique sur F tel que $deg_F(a) = 1$, $p(x) = x - \alpha$ est le polynôm minimal de a sur F.*

2) $i \in \mathbb{C}$ est un élément algebrique sur $\mathbb{R}$ tel que $deg_{\mathbb{R}}(i) = 2$, $p(x) = x^2 + 1$ est le polynôm minimal de i sur $\mathbb{R}$.

Théorème 1.1.2 *Soient E une extension de F et $\alpha \in E$ un élément algebrique sur F avec $deg_F(\alpha) = n$ et soit $p(X)$ est le polynôme minimal de α sur F, alors :*

(1) $F(\alpha) \simeq F[X] \diagup \langle p(X) \rangle$.

(2) $\{1, \alpha, \alpha^2, \alpha^3, ...\alpha^{n-1}\}$ *est une base de l'éspace vectoriel* $F(\alpha)$ *sur* F

(3) $dim_F(F(\alpha)) = deg_F(\alpha) = deg(p(X))$.

Exemple 1.1.5 *Soit d un rationnel entier positif non carré dans $\mathbb{Q}$, donc le polynôme $X^2 - d$ est un polynôme normalisé et irréductible sur $\mathbb{Q}$. posone $\alpha = \sqrt{d} \notin \mathbb{Q}$.donc le noyau de l'épimorphisme (En algèbre générale, un épimorphisme est un homomorphisme qui est surjectif)*

$$\mathbb{Q}[X] \to \mathbb{Q}[\alpha]$$

est engendré par $X^2 - d$ qui est le polynôme minimal de α. L'élément α est donc algébrique sur $\mathbb{Q}$ et de degré 2. L'extension

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[\alpha]/(X^2 - d)$$

de $\mathbb{Q}$ est un $\mathbb{Q}-$espace vectoriel de dimension 2 et dont une base est $\{1, \alpha\}$.

1.1.3 Extension finie

Définition 1.1.5 *Une extension E de F est dite finie si la dimension de $F -$ espace vectoriel E est finie. Le degré d'extension E de F est noté*

$$[E : F] = dim_F E$$

Exemple 1.1.6 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

$[\mathbb{C} : \mathbb{R}] = 2$.

$[F(\alpha) : F] = deg_F(\alpha) = \deg(p(X))$ *ou $p(X)$est le polynôme minimale de α.*

Théorème 1.1.3 *Soit E une extension finie de F et L une extension finie E, alors L est une extension finie de F et*

$$[L : F] = [L : E] \cdot [E : F]$$

Corollaire 1.1.1 *Soit E une extension F et soient, α,$\beta \in E$ deux élémentes algébriques sur F avec $deg_F(\alpha) = n$ et $deg_F(\beta) = m$ .Alors :*

$$[\mathsf{F}(\alpha, \beta) : \mathsf{F}] \leq \mathsf{n} \cdot \mathsf{m}$$

Preuve. on a d'après le theoréme (1.1.4)

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F]$$

et d'près le theoréme (1.1.3)

$$[F(\alpha) : F] = dim_F(F(\alpha)) = deg_F(\alpha) = n$$

Il reste à prouver $\deg_{F(\alpha)}(\beta) \leq \deg_F(\beta)$, on a β est une racine de polynôme (non nul) $p(x) \in F[X]$ de $deg = m$ tel que $p(x)$ est irreductible sur $F[X]$, si $p(X)$ est irreductible sur$F(\alpha)$ alors $deg_{F(\alpha)}(\beta) = m$, si non $p(x)$ se factorise sur $F(\alpha)$ en produit des polynômes irredctubles de degré $< m$ et β est une racine de l'un de ces facteurs, par suite

$$deg_{F(\alpha)}(\beta) < m.$$

■

1.1.4 Extension algébrique

Définition 1.1.6 *Une extension E de F est dite algébrique si tout element $\alpha \in E$ est algébrique sur F.*

Exemple 1.1.7 $\mathbb{C}$ *est une extension algebrique de* $\mathbb{R}$*, car tout nombre complexe* $z \in \mathbb{C}$ *est racine d'un polynôme* $\in \mathbb{R}[X]$ *de dégré* 2*. Si* $z = a + ib \in \mathbb{C}$*, alors* z *est racine de*
$X^2 - 2aX + (a^2 + b^2) = 0$*, puisque* $(z - a)^2 = -b^2$.

Théorème 1.1.4 (Kronecker) *Soient F un corps et $f(X) \in F[X]$ un polynom non constant, alors il existe une extension E de F tell que 'il existe $\alpha \in E$ verifiant $f(\alpha) = 0$.*

Preuve. Premiérement on considére le cas particulier où $f(X)$ est irreductible sur F ,

donc $I =< f(X) >$ est un ideal maximal dans $F[X]$, et $E = F[X]/I$ est un corps. D'abord nous affirmons que .

$$\grave{F} = \{c + I \ / c \in F\}$$

est un sous corps de E isomorphe a F . Puisque I est un ideal de $F[X]$, et pour

$$(c + I), (d + I) \in \grave{F}$$

alors :

$$(c + I) - (d + I) = (c - d) + I$$

et si $d \neq 0$ dans F, alors :

$$(d + I)^{-1} = d^{-1} + I$$

$$(\mathrm{c} + \mathrm{I})(\mathrm{d} + \mathrm{I})^{-1} = \mathrm{cd} + \mathrm{I}$$

Par conséquent $\grave{F}$ est un sous corps de E.

L'aplication

$$\phi : F \to \grave{F}$$

definit par

$$\phi(c) = c + I \text{ pour tout } c \in F$$

est isomorphisme. Par identifecation entre $c \in F$ et $\phi(c) = c + I$, on remarque que E est une extension de F. Maintenant, nous montrons que E contient une racine de $f(X)$. Comme I est un ideal de

$F[X]$, nous avons

$$(X + I)^i = X^i + I$$

$$\mathrm{c}(\mathrm{X} + \mathrm{I})^i = (\mathrm{c} + \mathrm{I})(\mathrm{X}^i + \mathrm{I}) = (\mathrm{X} + \mathrm{I})^i = \mathrm{cX}^i + \mathrm{I}.$$

et plus généralement pour tout polynôme

$$f(X) = c_0 + c_1 X + ...c_m X^m \in F[X]$$

on a

$$f(X+I) = c_0 + c_1(X+I) + ...c_m(X^m + I)$$

$$= (\mathrm{c_0}+\mathrm{c_1X} + ...\mathrm{c}_m\mathrm{X}^m) + \mathrm{I} = \mathrm{f(X)} + \mathrm{I}$$

pour $\alpha = X + I, E$

$$f(\alpha) = f(X+I) = f(X) + I = 0 \text{ , dans } E$$

Ainsi α est une racine de $f(X)$. Dans cas général où $f(X)$ ne doivent pas être irréductible, appliquer le(ce) cas particulier à tout factore irréductible de $f(X)$. ■

Définition 1.1.7 *Soient F un corps et $f(X)$ un élément de $F[X]$ n'appartenant pas à F. Une extension algébrique E de Fdans laquelle $f(X)$ possède une racine s'appelle un corps de rupture sur F de $f(X)$.*

Le théorème précedant(Kronecker) prouve que $f(X)$ possède toujours un corps de rupture.

Proposition 1.1.2 *Toute extension finie est une extension algébrique.*

Définition 1.1.8 *Un corps E est algébriqument clos s'il vérifie l'une des propriétés equivalentes suivantes :*

1) tout polynome de deg ≥ 1de $E[X]$ se factorise dans $E[X]$ en un produit de polynomes de premier degré

2) tout polynome irredctuble de $E[X]$ est de degré 1

3) tout polynome de deg ≥ 1 de $E[X]$ a au moins une racine dans E.

Exemple 1.1.8 *Le corps $\mathbb{C}$ est algébriquement clos.*

Un corps fini F_q n'est jamais algébriqument clos . car si $F_q = \{a_1, a_2, ...a_q\}$, le polynôme $f(X) = (X - a_i) + 1 \in F[X]$ ne possed pas aucune racine dans F_q.

Définition 1.1.9 *Une extension E d'un corps F est dite cloture algébrique de F si elle est algébrique sur F et algebriqument clos .*

1.2 Corps de décomposition

Définition 1.2.1 *On appelle corps de décomposition (ou corps de factorisation totale) d'un polynôme f sur un corps F, une extension E de F telle que :*

1) E est un corps de factorisation de F.

2) E est un corps minimal dans l' ensemble des corps de factorisation de f, c'est-à-dire que sur tout corps intermédiare K $(F \subseteq K \subseteq E)$, f ne se décompose plus en facteurs du premier degré.

Exemple 1.2.1 $\mathbb{C}$ *est un corps de décomposition sur* $\mathbb{R}$ *pour* $f(X) = X^2 + 1 \in \mathbb{R}[X]$.

$\mathbb{Q}(\sqrt{2})$ *est un corps de décomposition sur* $\mathbb{Q}$ *pour* $f(X) = X^2 - 2$.

Exemple 1.2.2 *Soit α une racine du polynôme $X^3 - 2$ irréductible sur $\mathbb{Q}$. $\mathbb{Q}(\alpha)$ n'est pas un corps de décomposition car il contient pas les autres racines de ce polynôme. Par conter si ω est une racine cubique de l'unité, c'est-à-dire une racine du polynôme X^2+X+1, alors dans le corps $\mathbb{Q}(\alpha, \omega)$ on a*

$$X^3 - 2 = (X - \alpha)(X - \omega\alpha)(X - \omega^2\alpha).$$

Ainsi $\mathbb{Q}(\alpha, \omega)$ est un corps de factorisation du me $X^3 - 2$ et on a

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6.$$

car

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

selon théoréme (1.1.3).

et

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = \deg ré(X^2 + X + 1) = 2$$

, et

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg ré(X^3 - 2) = 3$$

. selons théoréme (1.1.2)

Montrons que $\mathbb{Q}(\alpha, \omega)$ est un corps de décomposition . S'il existe K, tel que

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\alpha, \omega)$$

avec K corps de décomposition du polynôme x^3-2,alors K contien α élément algébrique de degré 3et β racine du polynôme X^3-2, elément algébrique de degré 2.Donc $\mathbb{Q}(\alpha,\beta)\subset K$ serait de degré 6 et

$$\mathbb{Q}(\alpha,\beta)=\mathrm{K}=\mathbb{Q}(\alpha,\omega).$$

1.2.1 Existance de corps de décomposition

Théorème 1.2.1 *Si $f(X)$ est un polynome de dégre $n\geq 1$ sur un corps F, Alors il existe un corps de décomposition E de $f(X)$ sur F tel que*

$$[\mathsf{E}:\mathsf{F}]\leq \mathsf{n}!.$$

Preuve. Si $n=1$, $f(X)$ est factorisable sur F et $[F:F]=1$, car $ax+b\in F$ et $\alpha=-a^{-1}b\in F$. Supposons que le théorème vrai pour chaque polynôme de degré inférieur à n, et on démontrer pour $f(X)$ est

de degré n.

$f(X)$ a un polynôme irreductible et normalise $P(X)$ comme un factore, ce derniere a une racine $\alpha\notin F$ (théorème1.1.4) , donc $f(X)\in F[X]$ a une racine α dans $F(\alpha)$ tel que

$$[F(\alpha):F]=\deg P(X)\leq \deg f(X)=n.$$

on note $E=F(\alpha)$. Alors

$$\mathrm{f(X)=(X-\alpha)g(X)}$$

tel que $g(X)$ est un polynôme de degré $n-1$ sur E. Par l'hypothèse de récurrence, $g(X)$ à un corps de décomposition K avec

$$[K:F]\leq (n-1)!.$$

Ainsi

$$g(X)=a(X-\alpha_1)(X-\alpha_2).....(X-\alpha_{n-1})$$

dans $K[X]$, et

$$\mathrm{f(X)=a(X-\alpha)(X-\alpha_1)(X-\alpha_2).....(X-\alpha_{n-1}).}$$

■

Exemple 1.2.3 $\mathbb{Q}(\sqrt{2}i, -\sqrt{2}i) = \mathbb{Q}(\sqrt{2}i)$ *est un corps de décomposition sur* $\mathbb{Q}$ *pour*

$$f(X) = X^2 + 2.$$

1.2.2 Uncite de corps de décomposition

Théorème 1.2.2 *Soient*

$$\varphi : F \longrightarrow F^*.$$

Un isomorphisme de corps , f un polynôme de $F[x]$ et $f^* = \varphi(f)$ son image dans $F^*[X]$

Si E et E^* sont respectivement deux corps de décomposition de f et f^*, alors il existe un isomorphisme

$$\sigma : E \longrightarrow E^*$$

qui prolonge φ.

Preuve. Démontrons ce résultat par récurrence sur le dégré

$$\mathsf{n} = [E : F].$$

Pour $n = 1$ cela est trivial ; soit $n > 1$, les racines de f ne sont pas toutes dans F et f a donc au moins un facteur irréductible g de degré $d > 1$.

Soient α une racine de g appartenant à E et g^* l'homologue de g par φ. Le corps des racines E^* contient alors une racine α^* de g^* on peut prolonger φ en un isomorphisme

$$\psi : K(\alpha) \to K(\alpha^*)$$

tel que

$$\psi(\alpha) = \alpha^*.$$

Il est clair que E et E^* sont respectivement des corps de décomposition de f et f^* sur $K(\alpha)$ d'une part, et $K^*(\alpha)$ d'autre part. Mais

$$[E : K(\alpha)] = n/d < n$$

selons l'hypothèse de récurrence, nous pouvons prolonger ψ en un isomorphisme

$$\sigma : E \longrightarrow E^*$$

tel que l'on ait le diagramme commutatif :

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & F^* \\ \downarrow & & \downarrow \\ \mathrm{K}(\alpha) & \xrightarrow{\psi} & \mathrm{K}^*(\alpha^*) \\ \downarrow & & \downarrow \\ \mathrm{E} & \xrightarrow{\sigma} & \mathrm{E}^* \end{array}$$

σ est un isomorphisme qui prolonge φ. C'est l'isomorphisme cherché. ■

Corollaire 1.2.1 *Deux corps de décomposition E et E^* d'un polynôme f sur un corps F sont isomorphes.*

Preuve. théorème (1.2.2) pour $F = F^*$ et $\varphi = id_F$ ■

1.2.3 Extensions séparables

Définition 1.2.2 *Soit F un corps, un polynome $f(x) \in F[X]$ de degré n est dit séparable sur le corps F, s'il a n racines distinctes dans son corps de décomposition, il est dit inséparable dans le cas contraire.*

Exemple 1.2.4 $f(x) = x^3 - 2 \ \in \mathbb{Q}[X]$ *est separable sur* $\mathbb{Q}(\sqrt{2}, j)$ *ou* $j = e^{\frac{2\pi i}{3}}$.

Théorème 1.2.3 *Soit E un corps . Un polynome $f(x) \in F[X]$ est séparable sur F si et seulement si f et sa dérivée formelle f' sont des polynômes premiers entre eux dans $E[X]$ ou E est le corps de décomposition de $f(X)$.*

Preuve. Soit d le pgcd de f et f. Si f admet dans son corps de décomposition E une racine multible α d'ordre K, on peut écrire

$$\mathsf{f(X) = (X - \alpha)^K g(X),\ K > 1,\ g(X) \neq 0.}$$

Dérivons dans l'anneau $E[X]$:

$$f^{'}(X) = (X - \alpha)^K g^{'}(X) + K(X - \alpha)^{K-1} g(X)$$

$f^{'}$ est divisible par $(X - \alpha)$ si $K - 1 > 1$.

Il en résulte que d est aussi divisible par $X - \alpha$ et donc d n'est pas un polynome de degré nul.

Supposons maintenant f séparable sur K, donc

$$f(X) = a \prod_{i=1}^{n} (X_i - \alpha_i) \text{ avec } \alpha_i \neq \alpha_j$$

si $i \neq j$. On a :

$$f^{'}(X) = a \sum_{j=0}^{n} (X - \alpha_1).....(\widehat{X - \alpha_j}).....(X - \alpha_n).$$

$\widehat{\ }$ signifie que le facteur $X - \alpha_j$ est omis. Il est claire qu'aucun $X - \alpha_j$ ne divise $f^{'}$ donc d est un polynomes de degré nul. ■

Corollaire 1.2.2 *Soit $f(X) \in F[X]$ un polynome irréductible sur F et soit $f^{'}(X) \in F[X]$ sa dérivée. alors:*

$f(X)$ est séparable sur F si et seulement si sa dérivée formelle n'est pas nul.

Preuve. Soit E le corps de décomposition de f. D'apord f est séparable c'est à dire chaque racine de f dans E est de multiplicité $s = 1$, si et seulement si et seulement si aucun racine de $f(X)$ est également un racine de $f^{'}(X)$.

$(\Longrightarrow)$

Si

$$f^{'}(X) = 0 \in F[X]$$

alors chaque racine de $f(X)$ est une racine de $f^{'}(X)$, et $f(X)$ non séparable sur F.

($\Longleftarrow$)

Si

$$f(X) \neq 0 \in F[X]$$

et si $\alpha \in E$ est une racine de $f(X)$ et $f^{'}(X)$, alors $X - \alpha$ divise $f(X)$ et $f^{'}(X)$.

mais

$$deg\ f^{'}(X) < f(X)$$

donc $f(X)$ ne divise pas $f^{'}(X)$; et comme $f(X)$ est irreductible alors $f(X)$ et $f^{'}(X)$ sont premier entre eux, donc il existe

$$u(X), v(X) \in F[X]$$

tell que

$$u(X)f(X) + v(X)f^{'}(X) = 1 \in F[X].$$

et donc $X - \alpha$ divise $1 \in F[X]$ et ça est imposible. Donc n'existe aucun racine de $f(X)$ est également un racine de $f^{'}(X)$. ■

Théorème 1.2.4 *Soient les trois corps $F \subset E \subset K$. Si K est séparable sur F. Alors K est séparable sur E et E est séparable sur F.*

Théorème 1.2.5 *Soit $f(X)$ un polynome irréductible sur un corps F. Alors :*

Si la caractéristique de F egale à 0 ($cara(F) = 0$), alors $f(x)$ est séparable sur F.

Si la caractéristique de F egale à p, p premier $(cara(F) = p)$, alors $f(x)$ est séparable sur F si et seulement si $f(x) \neq g(x^p)$ pour tout $g(x) \in F[x]$.

Preuve. (1) Suppose

$$cara(F) = 0 \text{ et } f(X) \in F[X]$$

un polynome irréductible sur F de degré n.

Si $n = 1$, alors $f(X)$ a exactement une racine de multiplicity 1. Si $n > 1$, donc comme $cara(F) = 0$,

$$deg(f^{'}(X)) = n - 1 > 0.$$

d'ou

$$f(X) \neq 0$$

et $f(X)$ est séparable sur F

(2) Suppose

$$cara(F) = p \text{ et } f(X) \in F[X]$$

est irréductible sur F

$(\Longrightarrow)$

Suppose

$$f(X) = g(X^p) \text{ ou } g(X) \in F[X]$$

alors

$$f(X) = a_n X^{pn} + + a_{n-1} X^{p(n-1)} + ...a_1 X^p + a_0 \in F[X]$$

et

$$f^{'}(X) = 0$$

d'ou $f(X)$ est non séparable sur F.

$(\Longleftarrow)$

Suppose

$$f(X) \neq g(X^p) \text{ ou } g(X) \in F[X]$$

alors

$$f(X) = a_m X^m + ...a_i X^i + ...a_1 X + a_0 \in F[X]$$

pour i est le plus grand exposant de X, i n'est pas multiple de p et $a_i \neq 0$

par suite pour $f^{'}(X)$, $i-1$ est le plus grand exposant de X et $ia_i \neq 0$, Donc $f^{'}(X) \neq 0$.

et $f(X)$ est séparable sur$F$. ■

Définition 1.2.3 *Soit E une extension de F. Un elémént $\alpha \in E$ est dit séparable sur F si α est algébrique sur F et son polynome minimale $Irr(\alpha, F, X)$est séparable.*

Définition 1.2.4 *Une extension algébrique E de F est dite extension séparable sur F si tout element $\alpha \in E$ est séparable sur F.*

1.2.4 Extensions normales

Définition 1.2.5 *Soit E une extension d'un corps F. Alors E est dite extension normale de F si elle est algébrique sur F et tout polynome irréductible sur F, qui a une racine dans E, a toutes ses racines dans E.*

Exemple 1.2.5 *1) $\mathbb{Q}(i)$ est une extension normale de $\mathbb{Q}$.*

2) $E = \mathbb{Q}(\sqrt[3]{2})$ est algébrique sur $\mathbb{Q}$ mais non normale sur $\mathbb{Q}$ car $x^3 + 2$ a une racine dans E mais pas les deux autre racines $\sqrt[3]{2}\omega$ et $\sqrt[3]{2}\omega^2$ avec $\omega = e^{\frac{i2\pi}{3}}$.

3) $\mathbb{Q}(\sqrt[3]{2}\omega)$ est une extension normale de $\mathbb{Q}$.

Théorème 1.2.6 *Soit E une extension finie d'un corps F. Alors les deux conditions suivantes sont équivalentes :*

(1) E est une extension normale sur F.

(2) E est le corps de décomposition d'un polynome de $F[X]$.

Preuve. (1) $\Longrightarrow$ (2)

Supposons que E est une extension normal et fini sur F. alors $E = F(\alpha_1, \alpha_2, ...\alpha_n)$ pour $\alpha_1, \alpha_2, ...\alpha_n$ algébrique sur F. Si $m_K(X)$ est le polynome minimale de α_k sur F pour $1 \leq k \leq n$. alors toute $m_K(X)$ a une racine $\alpha_k \in E$ et par conséquent tout $m_k(X)$ est factorisable sur F car E est normale sur F, donc E est le corps de décomposition de

$$p(X) = m_1(X) \cdot m_2(X)..... \cdot m_n(X)$$

sur F.

(2) $\Longrightarrow$ (1)

Supposons que E est le corps de décomposition de $f(X)$ sur F. Alors

$$E = F(c_1, c_2, ...c_n)$$

ou

$$c_1, c_2, ...c_n$$

sont des racines de $f(X)$, donc $[E : F]$ est finie.

Pour montrer que Eest normale sur F, on suppose que $p(X)$est irréductible sur F et $p(X)$ a une racine $c \in E$, mais n'est pas factorisable sur F. Nous allons montrent que cela conduit à une contradiction.

On considérer que $p(X) \in E[X]$, puis ajouter une racine ($d \notin E$) pas dans F, pour obtenir le corps $E(d)$ alors il existe un isomorphisme

$$\phi : F[c] \longrightarrow F[d]$$

telque

$$\phi(c)) = d$$

et laissant tous les élément de F fixe , comme c et d sont deux racines de $p(X)$ sur F. Par notre hypothèse initiale, E est le corps de décomposition de de $f(X)$ sur F et par conséquent sur $F[c]$. Cependant $E(d)$ est le corps de décomposition de $f(X)$ sur $F[d]$. D'apres (théorème 1.1.2) il existe un isomorphisme

$$\phi^* : E \longrightarrow E[d]$$

telque ϕ^* prolonger ϕ. Cela implique

$$[E : F] = [E(d) : F]$$

ce qui est impossible, car $d \notin E$. et cette contradiction complète la preuve. ■

Corollaire 1.2.3 *Toute extension finie, normale et séparable d'un corps est le corps de décomposion d'un polynome séparable.*

Corollaire 1.2.4 *Si E est une extension fini et normal d'un corps F, alors E est normal sur tout corps K compris F et E.*

Preuve. Soit $\sigma : E \longrightarrow \bar{F}$ un monomorphisme prolongeant id_K. Il est clair que σ est un monomorpisme prolongeant id_F, donc un $F - automorphisme$ de E. Ainsi tout monomorphisme σ prolongeant id_K est un $F - automorphisme$ de E. Donc E est une extension normale de K. ■

Chapitre 2

Theorie de Galois

2.1 Extension galoisienne

Définition 2.1.1 *Soit E une extension algébrique de F. On dit qu'elle est galoisienne si elle est à la fois normale et séparable.*

Exemple 2.1.1 *Toute extension finie et normale L du corps $\mathbb{Q}$ est séparable donc galoisienne. L est aussi le corps de décomposition d'un polynome irréductible sur $\mathbb{Q}$.*

$\mathbb{Q}(\sqrt[3]{2}, w)$ est une extension galoisienne de $\mathbb{Q}$.

$\mathbb{C} = \mathbb{R}(i)$ est une extension galoisienne de $\mathbb{R}$.

$\mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension galoisienne de $\mathbb{Q}$, car $X^3 - 2 \in \mathbb{Q}$ a une racine $\sqrt[3]{2}$mais pas les deux autre racines

Tout corps fini est extension galoisienne de n'importe lequel de ses sous-corps.

Définition 2.1.2 *Soit E une extension de F. Un $F-$automorphisme*

$$\phi : E \longrightarrow E$$

est un automorphisme de corps tel que $\phi(a) = a$ pour tout $a \in F$.

2.2 Groupe de Galois

Théorème 2.2.1 *Si E est une extension d'un corps F, alors :*

L'ensemble $Aut(E)$ des automorphismes de E est muni d'une structure de groupe pour la loi de composition des automorphismes.

L'ensemble des $F-$ autmorphismes de E est un sous groupe de $Aut(E)$.

Définition 2.2.1 *Soit E une extension d'un corps F. Le groupe des $F-$automorphisemes de E est appelé le groupe de Galois de E sur F et noté $Gal(E/F)$.*

$$Gal\ (\mathsf{E/F}) = \{\sigma \in \mathit{Aut}\ (\mathsf{E}) \setminus \sigma(\mathsf{a}) = \mathsf{a}, \forall \mathsf{a} \in \mathsf{F}\}$$

Exemple 2.2.1 *1.$Gal(\mathbb{C}/\mathbb{R}) = Gal(\mathbb{R}(i)/\mathbb{R}) = \{\tau_0 = id_{\mathbb{C}}, \tau_1\}$. Ou τ_1 designe la conjugaison complexe*

2.$Gal(\ \mathbb{Q}(\sqrt{2})/\ \mathbb{Q})\ =\ \{id, \sigma\}$, pour $a, b \in \mathbb{Q}$.$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$

3. $Gal(\ \mathbb{Q}(\sqrt[3]{2})/\ \mathbb{Q})\ = \{id\}$.

4. $Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{\tau_0 = id, \tau_1\}$ ou τ_1 designe la conjugaison complexe.´

Proposition 2.2.1 *Soient E une extension de F, et $G = Gal(E/F)$. Si K est un corps intermédiare, c'est-a-dire compris entre E et F. Alors $Gal\ (E/K)$ est un sous groupe de G.*

Preuve. car tout $K-$*automorphisme* de E est à fortiori, un $F-$*automorphisme*. ■

Exemple 2.2.2 *$\mathbb{Q}(i, \sqrt{2})$ est une extension de $\mathbb{Q}$, et*

$$[\ \mathbb{Q}(\mathrm{i},\sqrt{2}) : \mathbb{Q}] = [\ \mathbb{Q}(\mathrm{i},\sqrt{2}) : \mathbb{Q}(\mathrm{i})].[\ \mathbb{Q}(\mathrm{i}) : \mathbb{Q}]$$

– $[\ \mathbb{Q}(i) : \mathbb{Q}] = 2,\ \mathbb{Q}(i)$ est le corps de décomposition de $x^2 + 1 \in \mathbb{Q}[X]$.

– Pour $\phi \in Gal(\ \mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$, $\phi(i)$ est une racine de $x^2 + 1$, Donc $\phi(i) = +i$ ou $\phi(i) = -i$.

Alors il existe deux $\mathbb{Q}-$*autmorphismes* de $\mathbb{Q}(i)$:

$$\begin{array}{rcl} \sigma_1 & : & \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i) \\ a+bi & \longrightarrow & a+bi \end{array}$$

$$\begin{array}{rcl} \sigma_2 & : & \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i) \\ a+bi & \longrightarrow & a-bi \end{array}$$

ou $a, b \in \mathbb{Q}$.

– $[\ \mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(i)] = 2$, $\mathbb{Q}(i,\sqrt{2})$ est le corps de décomposition de $x^2 - 2 \in \mathbb{Q}(i)$.

– Pour $\phi \in$Gal($\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$) , $\phi(\sqrt{2})$ est une racine de $x^2 - 2$, Donc $\phi(i) = +\sqrt{2}$ ou $\phi(i) = -\sqrt{2}$.

	τ_1	τ_2	τ_3	τ_4
τ(i)	i	i	-i	-i
$\tau(\sqrt{2})$	$\sqrt{2}$	-$\sqrt{2}$	$\sqrt{2}$	-$\sqrt{2}$

- σ_1 est prolongé par deux $\mathbb{Q}(i) - autmorphismes$ de $\mathbb{Q}(i,\sqrt{2})$:

$$\begin{array}{rcl} \tau_1 & : & \mathbb{Q}(i,\sqrt{2}) \longrightarrow \mathbb{Q}(i,\sqrt{2}) \\ \alpha+\beta\sqrt{2} & \longrightarrow & \alpha+\beta\sqrt{2} \end{array}$$

$$\begin{array}{rcl} \tau_2 & : & \mathbb{Q}(i,\sqrt{2}) \longrightarrow \mathbb{Q}(i,\sqrt{2}) \\ \alpha+\beta\sqrt{2} & \longrightarrow & \alpha-\beta\sqrt{2} \end{array}$$

ou α, $\beta \in \mathbb{Q}(i)$

- σ_2 est prolongé par deux $\mathbb{Q}(i) - automorphismes$ de $\mathbb{Q}(i,\sqrt{2})$:

$$\begin{array}{rcl} \tau_3 & : & \mathbb{Q}(i,\sqrt{2}) \longrightarrow \mathbb{Q}(i,\sqrt{2}) \\ \alpha+\beta\sqrt{2} & \longrightarrow & \bar{\alpha}+\bar{\beta}\sqrt{2} \end{array}$$

$$\begin{array}{rcl} \tau_4 & : & \mathbb{Q}(i,\sqrt{2}) \longrightarrow \mathbb{Q}(i,\sqrt{2}) \\ \alpha+\beta\sqrt{2} & \longrightarrow & \bar{\alpha}-\bar{\beta}\sqrt{2} \end{array}$$

Donc: $\tau_1\,,\tau_2\,,\tau_3\,,\tau_4$ son des $\mathbb{Q} - automorphisme$ de $\mathbb{Q}(i,\sqrt{2})$. Ce sone les élément de $Gal(\ \mathbb{Q}(i,\sqrt{2})/\ \mathbb{Q})$, groupe d'order 4

et muni de la loi donnée par la table

$\circ$	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_1
τ_4	τ_4	τ_3	τ_2	τ_1

D'autre part, les $\mathbb{Q}(i)$-automorphismes de $\mathbb{Q}(i,\sqrt{2})$ sont τ_1 et τ_2 d'ou

$$Gal(\ \mathbb{Q}(i,\sqrt{2})/\ \mathbb{Q}(i)) = \{\tau_1,\tau_2\}.$$

et on a

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

alors : $Gal\ (\ \mathbb{Q}(\sqrt{2},\sqrt{3})/\ \mathbb{Q}(\sqrt{2}))$ est un sous groupe de $Gal(\ \mathbb{Q}(\sqrt{2},\sqrt{3})/\ \mathbb{Q})$.

Proposition 2.2.2 *Soit E une extension de F et soit $\phi \in Gal(E/F)$. Alors pour tout $\alpha \in E$ et $f(x) \in F[x]$*

$$\phi(f(\alpha)) = f(\phi(\alpha)).$$

Preuve. Soit

$$f(x) = a_n x^n + ... + a_1 x + a_0 \in F[x].$$

Alors

$$\phi[\mathrm{f}(\alpha)] = \phi(\mathrm{a}_n\alpha^n + ... + \mathrm{a}_1\alpha + \alpha_0) = \phi(\mathrm{a}_n\alpha^n) + ... + \phi(\mathrm{a}_1\alpha) + \phi(\mathrm{a}_0)$$

$$= \phi(\mathrm{a}_n)\phi(\alpha^n) + ... + \phi(\mathrm{a}_1)\phi(\alpha) + \phi(\mathrm{a}_0) = \mathrm{a}_n\phi(\alpha^n) + ... + \mathrm{a}_1\phi(\alpha) + \mathrm{a}_0 = \mathrm{f}(\phi(\alpha)).$$

■

Corollaire 2.2.1 *Soient E une extension de F, $\phi \in Gal(E/F)$, $f(x) \in F[x]$ et $\alpha \in E$. Alors α est une racine de $f(x)$ si et seulement si $\phi(\alpha)$ est une racine de $f(x)$.*

Preuve. On utilise la proposition précedent ■

.

Lemme 2.2.1 *Soient E une extension fini de F et $\{v_1, v_2, ...v_n\}$ une base de l'espace vectoriel E. Alors pour tout $\phi \in Gal(E/F)$, ϕ est complétement détermine par $\phi(v_i)$, pour $1 \leq i \leq n$.*

Preuve. on a $\{v_1, v_2, ...v_n\}$ est une base de l'espace vectoriel E sur F , alors tout element $u \in E$ s'écrit de manière unique comme combinaison linéaire

$$\mathrm{u} = \mathrm{c}_1\mathrm{v}_1 + \ldots\ldots + \mathrm{c}_n\mathrm{v}_n \text{ ou } \mathrm{c}_i \in \mathrm{F} \text{ pour } 1 \leq \mathrm{i} \leq \mathrm{n}.$$

et comme $\phi \in Gal(E/F)$

$$\phi(u) = c_1\phi(v_1) + \ldots\ldots + c_n\phi(v_1).$$

Par conséquent ϕ est une transformation linéaire et uniquement déterminé par $\phi(v_i)$ pour $1 \leq i \leq n$. ■

Exemple 2.2.3 *On calcule le group de Galois de corps de décomposition de* $p(X) = X^3 - 2$ *sur* $\mathbb{Q}$. $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ *ou*

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

est une racine primitive de polynome minimal $X^2 + X + 1$. *Donc*

(1) Les trois racine de $X^3 - 2$ *sont*

$$\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2.$$

(2) Les deux racine $X^2 + X + 1$ *sont :*

$$\omega, \omega^2$$

.

(3) La base de $F-$*espace vectoriel* E *est*

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$$

(4) D'apres le lemme précedent . pour tout $\phi \in Gal(E/F)$, ϕ *est complétement détermine par* $\phi(\sqrt[3]{2})$ *et* $\phi(\omega)$

(5) D'apres le corollaire précedent $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$ *ou* $\sqrt[3]{2}\omega$ *ou* $\sqrt[3]{2}\omega^2$ *et* $\phi(\omega) = \omega$ *ou* ω^2.

Lemme 2.2.2 [1]*Soient* F *un corps,* $f(X) \in F[X]$ *et* E *le corps de décomposition de* $f(X)$ *sur* F, $p(X) \in F[X]$ *un polynome irréductible divisant* $f(X)$ *et* α_1 *et* α_2 *deux racines de* $p(X)$ *dans* E. *Alors il existe un* $F -$ *automorphisme* $\psi \in Gal(E/F)$ *telle que*

$$\psi(\alpha_1) = \alpha_2.$$

2.2.1 Order de groupe de Glois

Théorème 2.2.2 *Soient F un corps, $f(x) \in F[x]$ un polynome séparable sur F,et E le corps de décomposition de $f(x)$ sur F. Alors*

$$|Gal(E\ /F)| = [E : F].$$

Preuve. (L'ordre d'un groupe est le cardinal de son ensemble sous-jacent. Le groupe est dit fini ou infini suivant que son ordre est fini ou infni) Nous utilisons le principe de récurrence sur le degré de l'extension.$[E : F]$ Si $[E : F] = 1$ alors $E = F$ et $Gal(E/F)$ est le groupe trivial. Donc supposons que le théorème est vrai lorsque le degré del'extension est inférieur à n et on considérer le cas où

$$[E : F] = n$$

Comme $[E : F] > 1$, $f(X)$ n'est pas factorisable déjà sur F et donc a un diviseur $p(X)$ qui est irréductible sur F et de degré $k > 1$.

Comme $f(X)$ est séparable sur F et E est le corps de décomposition de $f(X)$ sur F, $f(X)$ est factorisable sur E et tous ses racines sont de multiplicité 1. puisque $p(X)$ divise $f(X)$, $p(X)$ également factorisable dans E et tous ses racines sont de multiplicité 1. Ainsi, il existe k racines distincts : $\alpha_1, ..., \alpha_k$ de $p(X)$ dans E. Maintenant, nous appliquons le lemme précédent. pour chaque i $1 \leq i \leq k$ il existe au moins un $F - automorphisme$ $\psi \in Gal(E/F)$ avec $\psi(\alpha_1) = \alpha_i$. Choisissez l'un de ces $F - automorphisme$ et l'appeler ψ_i.

on a

$$[F(\alpha_1) : F] = k$$

et

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F].$$

par suite $[E : F(\alpha_1)] = m$, ou $m = n/k$. Comme E est le corps de décomposition de $f(X)$ sur $F(\alpha_1)$, et $[E : F(\alpha_1)] < n$ nous pouvons appliquer notre hypothèse se récurrence et cela nous dit que

$$|Gal(E\ /F(\alpha_1))| = [E : F(\alpha_1)] = m.$$

Soient $\theta_1, ...\theta_m$ les élément de $Gal(E\ /F(\alpha_1))$.

Revendication 1[1]: Les $km = n$ compositions $\psi_i \circ \theta_r$ for $1 \leq i \leq k$ et $1 \leq r \leq m$ sont tous distincts, et par conséquent

$$|Gal(E\ /F(\alpha_1))| \geq km = n.$$

Revendication 2 [1]: Toute $F - automorphisme\ \phi : E \longrightarrow E$ est égal à $\psi_i \circ \theta_r$ pour certains $1 \leq r \leq k$ et $1 \leq r \leq m$, et par conséquent

$$|Gal(E\ /F(\alpha_1))| \leq km = n.$$

■

Exemple 2.2.4 *1.*$Gal(\ \mathbb{Q}(\sqrt{2})/\ \mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$*, car* $(\ \mathbb{Q}(\sqrt{2})$ *est une extension galoisienne de* $\mathbb{Q}$ *de degré* 2*, d'apres le theoreme précédant*

$$\left|Gal(\ \mathbb{Q}(\sqrt{2})/\ \mathbb{Q})\right| = 2.$$

2.$Gal(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$ *idem que l'exemple au-dessus.*

$$|Gal(\mathbb{C}/\mathbb{R})| = 2.$$

3. $Gal(\ \mathbb{Q}(\sqrt[3]{2})/\ \mathbb{Q}) = \{id\}$*est un groupe de Galois trivial, car il n'a que l'automorphisme identité.*

$$\left|Gal(\ \mathbb{Q}(\sqrt[3]{2})/\ \mathbb{Q})\right| = 1.$$

Définition 2.2.2 *Soient* F *un corps,* f *un polynome de* $F[X]$ *de degré* n *et* E *le corps de décomposition de* f *sur* F*. Alors le groupe de Galois* $G = Gal(E/F)$ *de* E *sur* F *est aussi appelé le groupe de Galois du polynôme* f *sur* F*.*

Définition 2.2.3 *Soient* E *une extension de* F*,* H *un sous-groupe de* $G = Gal(E/F)$*. Le corps fixe de* H*, noté* E^H *est l'ensemble des éléments* x *de* E *tel que pout tout* σ *de* H

$$\sigma(x) = x.$$

$$\mathsf{E}^H = \{\mathsf{x} \in \mathsf{E}\ \text{tel que}\ \forall \sigma \in \mathsf{H}\ \sigma(\mathsf{x}) = \mathsf{x}\}$$

Remarque 2.2.1 *IL est clair que E^H est un sos corps de E.*

Théorème 2.2.3 (Emil Artin) *[5] Soient E une extension de F et H un sous-groupe fini d'ordre r de $Gal(E|F)$. Alors E est une extension normale de E^H de degré r et*

$$Gal(L/E^H) = H.$$

2.3 La corresponence de Galois

Théorème 2.3.1 *Soit E une extension galoisienne de F et G son groupe de Galois,*

alors $F = E^G$. Si K est un corps intermédiare, alors E est une extension galoisienne de K.

L'application

$$K \longrightarrow G(E/F)$$

de l'ensemble des corps intermédiaires dans l'ensemble des sous-groupes de G est bijective et décroissante vis à vis la relation d'inclusion.

Preuve. Soit $\alpha \in E^G$ et σ un monomorphisme

$$F(\alpha) \longrightarrow \bar{E}$$

prolongeons id_F. Prolongeons σ en un monomorphisme $\overset{*}{\sigma}$ de E dans $\overset{*}{E}$. $\overset{*}{\sigma}$ estt un $F-$ *automorphisme* , donc un element de G , d'ou $\overset{*}{\sigma}(\alpha) = \alpha$, et a fortiori, $\sigma(\alpha) = \alpha$.

Il n'y a donc qu'un monomorphisme

$$\sigma : F(\alpha) \longrightarrow \bar{E}$$

prolongeant id_F; de plus α est séparable sur F donc

$$deg(Irr(\alpha, F, X)) = 1$$

c'est à dire que

$$[F(\alpha) : F] = 1$$

et donc

$$F(\alpha) = F.$$

Ainsi $\alpha \in F$ ce qui entraine $E^G \subseteq F$ d'ou l'galité.

Soit K un corps intermédiaire, alors E est normal sur K (corollaire1.2.4) et est séparable sur K (théorème 1.2.4), donc E est une extension galoisienne sur K. Si $H = Gal(E/K)$, le resultat ci dessus permet d'écrire $K = E^H$. Soient donc K et $K^{'}$ deux corps intermédiaires, $H = Gal(E/K)$ et $H^{'} = Gal(E/K^{'})$, alores $K = E^H$ et $K^{'} = E^{H^{'}}$; l'application de E vers G

$$K \longrightarrow Gal(E/K)$$

est donc injective ; elle est surjective car si H est un sous groupe de G alors K une extension galoisienne de $K = E^H$ dont le groupe de Galois est H

Si $K \subset K^{'}$ et $\sigma^{'} \in H^{'}$ avec $x \in K$, alors $\sigma(x) = x$, car , à fortiori $x \in K^{'}$, donc $\sigma^{'} \in H$ et $H^{'} \subset H$. Réciproquement, si $H^{'} \subset H$, alors

$$K = E^H = \{x/\sigma(x) = x, \text{ pour tout } \sigma \in H\}$$

donc $x \in K$ entraine à fortiori $\sigma^{'}(x) = x$, pour tout $\sigma^{'} \in H^{'}$ et donc $F \subset F^{'}$. ■

Corollaire 2.3.1 *Soit E une extension galoisienne de F . Les groupes de Galois $Gal(E/K)$ et $Gal(E/K^{'})$ de deux corps intermédiaires Ket $K^{'}$ isomorphes, sont des sous-groupes conjugués de $Gal(E/F)$.*

Preuve. (On dit que deux sous groupes H et K de G sont conjugués si il existe un élément g de G tel que $g.H.g^{-1} = K$)

Notons λ le $F - isomorphisme$ de E qui est prolonge l'isomorphisme $K \longrightarrow K^{'}$. Si

$$\sigma \in Gal(E/K) = H, \sigma \in Gal(E/K^{'}) = H^{'}$$

x$\in K$ et$y = \lambda(x) \in K^{'}$, alors

$$\lambda \circ \sigma \circ \lambda^{-1}(y) = \lambda(x) = y$$

et

$$\lambda^{-1} \circ \sigma^{'} \circ \lambda(x) = x$$

donc

$$\lambda \circ \sigma \circ \lambda^{-1} \in H^{'}, \text{et } \lambda^{-1} \circ \sigma^{'} \circ \lambda \in H.$$

L'application

$$H \longrightarrow H^{'}$$

telle que $\sigma \longrightarrow \lambda \circ \sigma \circ \lambda^{-1}$ est un isomorphisme ayant pour inverse $\tau \longrightarrow \lambda^{-1} \circ \tau \circ \lambda$.Il en résulte que

$$H^{'} = \lambda H \lambda^{-1}$$

c'est-à-dire que $H^{'}$ est un soue groupe conjigué de H dans le groupe $Gal(E/F)$. ■

Théorème 2.3.2 *Soient E une extension galoisienne d'un corps F, G son groupe de Galois, K un corps intermédiare et $H = Gal(E/K)$. Le corps K est normale sur F(ie: K est une extension normale F) si et seulement si H est un sous groupe normale de G.*

Si K est normale sur F, alors $Gal(K/F) \cong G/H$.

Preuve. On dit qu'un sous-groupe H d'un groupe G est normale (ou distingué) dans G s'il est stable par conjugaison, c'est-à-dire si :

$$(\forall h \in H, \forall x \in G \quad x.h.x^{-1} \in H.)$$

Supposons que K est normale sur F et soit $G^{'} = Gal(K/F)$ son groupe de Galois . L'application

$$h : G \longrightarrow G^{'}$$

telle que $\sigma^{'} = h(\sigma)$ est la restrication de σ à K, est un morphisme de noyau

$$\ker\ h = \{\sigma \in G \backslash h(\sigma) = id_K\}.$$

Les élément du noyau son donc les $K - automorphisme$ c'est dire $\ker h = G(E/K) = H$; H est donc un sous groupe normal de G . De plus tout élément de $G^{'}$ se prolonge en un monomorphisme $E \longrightarrow \bar{E}$ qui est nécessairement un automorphisme de E, donc un élément de G ; h est donc une surjection d'ou

$$Gal(K/F) = G/H$$

Supposons que K n'est pas normal sur F, alors il existe un monomorphisme

$$\lambda : K \longrightarrow E$$

prolongeant id_F § qui n'est pas un automorphisme (théorème1.2.7) $\lambda K \neq K$.

Les deux corps intermédiares λK et K sont isomorphe mais distincts. Les groupes de Galois $Gal(E/K)$ et $Gal(E/\lambda K)$ sont conjugués mais distincts , donc H n'est pas normale dans G. ■

Exemple 2.3.1 *Le polynome* x^4-3 *de* $\mathbb{Q}(x)$ *est irréductible d'aprés le théoréme d'Eisenstien. Soit* $\sqrt[4]{3}$ *une racine, alors* $-\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}$ *sont les autres racines.*

$\mathbb{Q}(i, \sqrt[4]{3})$ *est le corps de décomposition de* $x^4 - 3$, *donc elle est une extension galoisienne de* $\mathbb{Q}$.

Nous avons

$$[\ \mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}] = [\ \mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}(i)].[\ \mathbb{Q}(i) : \mathbb{Q}]$$

$$[\ \mathbb{Q}(\mathrm{i}, \sqrt[4]{3}) : \mathbb{Q}(\mathrm{i})] = 4, \textit{ car } \mathrm{irr}\ (\sqrt[4]{3}, \mathbb{Q}(\mathrm{i}), \mathrm{X}) = \mathrm{x}^4-3.$$

$$[\ \mathbb{Q}(\mathrm{i}) : \mathbb{Q}] = 2 \textit{ car } \mathrm{irr}\ (\mathrm{i}, \mathbb{Q}, \mathrm{X}) = \mathrm{x}^2+1$$

d'ou .

$$[\ \mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}] = \left|Gal(\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q})\right| = 8$$

Gal($\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q}$*) :*

Si $\phi \in$*Gal(* $\mathbb{Q}(i, \sqrt[4]{3})/\mathbb{Q}$*) , alors :*

- $\phi(i)$ *est une racine de* $x^2 + 1$, *Donc* $\phi(i) = +i$ *ou* $\phi(i) = -i$.

Donc il existe deux $\mathbb{Q} -$ *autmorphismes de* $\mathbb{Q}(i)$ $\tau_1 = id(\mathbb{Q}(i))$ *et* τ_2 *ou :*

$$\begin{array}{rcl} \tau_1 & : & \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i) \\ a + bi & \longrightarrow & a + bi \end{array}$$

$$\begin{array}{rcl} \tau_2 & : & \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i) \\ a + bi & \longrightarrow & a - bi \end{array}$$

$\phi(\sqrt[4]{3})$ est une racine de x^4-3, Donc $\phi(\sqrt[4]{3})=+\sqrt[4]{3}$ ou $\phi(\sqrt[4]{3})=-\sqrt[4]{3}$ ou $\phi(\sqrt[4]{3})=+i\sqrt[4]{3}$ou $\phi(\sqrt[4]{3})=-i\sqrt[4]{3}$.

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\sigma(\mathrm{i})$	i	i	i	i	-i	-i	-i	-i
$\sigma(\sqrt[4]{3})$	$\sqrt[4]{3}$	-$\sqrt[4]{3}$	$i\ \sqrt[4]{3}$	-$i\ \sqrt[4]{3}$	$\sqrt[4]{3}$	-$\sqrt[4]{3}$	$i\ \sqrt[4]{3}$	-$i\ \sqrt[4]{3}$

- τ_1 est prolongé par qautre $\mathbb{Q}(i)-$autmorphismes de $\mathbb{Q}(i,\sqrt[4]{3})$: $\{\sigma_1,\sigma_2,\sigma_3,\sigma_{4\}}$

Soit $a=\alpha+\beta\sqrt[4]{3}+\gamma(\sqrt[4]{3})^2+\delta(\sqrt[4]{3})^3$

$$\begin{aligned}\sigma_1 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \alpha+\beta\sqrt[4]{3}+\gamma(\sqrt[4]{3})^2+\delta(\sqrt[4]{3})^3\end{aligned}$$

$$\begin{aligned}\sigma_2 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \alpha-\beta\sqrt[4]{3}+\gamma(\sqrt[4]{3})^2-\delta(\sqrt[4]{3})^3\end{aligned}$$

$$\begin{aligned}\sigma_3 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \alpha+\beta i\ \sqrt[4]{3}-\gamma(\sqrt[4]{3})^2-\delta i\ (\sqrt[4]{3})^3\end{aligned}$$

$$\begin{aligned}\sigma_4 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \alpha-\beta i\ \sqrt[4]{3}-\gamma(\sqrt[4]{3})^2+\delta i\ (\sqrt[4]{3})^3\end{aligned}$$

ou $\alpha,\ \beta,\gamma,\delta\in\mathbb{Q}(i)$.

- τ_2 est prolongépar qautre $\mathbb{Q}(i)-$autmorphismes de $\mathbb{Q}(i,\sqrt{2})$: $\{\sigma_5,\sigma_6,\sigma_7,\sigma_8\}$

$$\begin{aligned}\sigma_5 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \bar{\alpha}+\bar{\beta}\sqrt[4]{3}+\bar{\gamma}(\sqrt[4]{3})^2+\bar{\delta}(\sqrt[4]{3})^3\end{aligned}$$

$$\begin{aligned}\sigma_6 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3})\longrightarrow\mathbb{Q}(i,\sqrt[4]{3})\\ a \quad &\longrightarrow \quad \bar{\alpha}-\bar{\beta}\sqrt[4]{3}+\bar{\gamma}(\sqrt[4]{3})^2-\bar{\delta}(\sqrt[4]{3})^3\end{aligned}$$

$$\begin{aligned} \sigma_7 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3}) \longrightarrow \mathbb{Q}(i,\sqrt[4]{3}) \\ a \quad &\longrightarrow \quad \bar{\alpha} + \bar{\beta}\ i\ \sqrt[4]{3} - \bar{\gamma}(\sqrt[4]{3})^2 - \bar{\delta} i\ (\sqrt[4]{3})^3 \end{aligned}$$

$$\begin{aligned} \sigma_8 \quad &: \quad \mathbb{Q}(i,\sqrt[4]{3}) \longrightarrow \mathbb{Q}(i,\sqrt[4]{3}) \\ a \quad &\longrightarrow \quad \bar{\alpha} - \bar{\beta}\ i\ \sqrt[4]{3} - \bar{\gamma}(\sqrt[4]{3})^2 + \bar{\delta}\ i\ (\sqrt[4]{3})^3 \end{aligned}$$

Donc: $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\}$ *son des* $\mathbb{Q} - automorphisme\ de\ \mathbb{Q}(i,\sqrt[4]{3})$. *Ce sont les éléments de* $Gal(\ \mathbb{Q}(i,\sqrt[4]{3})/\ \mathbb{Q})$, *groupe d'order* 8

et muni de la loi donnée par la table :

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5	σ_8	σ_7
σ_3	σ_3	σ_4	σ_2	σ_1	σ_7	σ_8	σ_6	σ_5
σ_4	σ_4	σ_3	σ_1	σ_2	σ_8	σ_7	σ_5	σ_6
σ_5	σ_5	σ_6	σ_8	σ_7	σ_1	σ_2	σ_4	σ_3
σ_6	σ_6	σ_5	σ_7	σ_8	σ_2	σ_1	σ_3	σ_4
σ_7	σ_7	σ_8	σ_5	σ_6	σ_3	σ_4	σ_1	σ_2
σ_8	σ_8	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

Sous groupe de $Gal(\ \mathbb{Q}(i,\sqrt[4]{3})/\ \mathbb{Q})$.*:*

Sous-groupe d'ordre 1 $\{\sigma_1\}$

Sous-groupe d'ordre 2 *:*$A = \{\sigma_1, \sigma_2\}, B = \{\sigma_1, \sigma_5\}, C = \{\sigma_1, \sigma_6\}, D = \{\sigma_1, \sigma_7\}, E = \{\sigma_1, \sigma_8\}$

Sous-groupe d'ordre 4 *:*$F = \{\sigma_1, \sigma_2, , \sigma_3, \sigma_4\}, J = \{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}, H = \{\sigma_1, \sigma_2, \sigma_7, \sigma_8\}$.

Sous-groupe d'ordre 8 *:*

$$\mathrm{G} = \mathrm{Gal}(\ \mathbb{Q}(\mathrm{i},\sqrt[4]{3})/\ \mathbb{Q}).$$

Le treillis des sous groupes de $Gal(\ \mathbb{Q}(i,\sqrt[4]{3})/\ \mathbb{Q})$ *est donné par le diagramme d'inclusion: dans figur 1.*

d'aprés le théorème (2.3.1) *il ya* 8 *corps intermédiaires entre* $\mathbb{Q}$ *et* $\mathbb{Q}(i,\sqrt[4]{3})$. *Le treillis des corps intermédiaires est donné par diagramme d'i nclusion dans figur 2*

Ou $C(M)$ est le corps intermédiaire associé au sous-groupe M de $Gal(\ \mathbb{Q}(i,\sqrt[4]{3})/\ \mathbb{Q})$. Pour déterminer ces corps intermédiaires, on considère une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}(i,\sqrt[4]{3})$

exprimée en termes de i et $\sqrt[4]{3}$. Nous avons la base

$$\{1, i, \sqrt[4]{3}, i\sqrt[4]{3}, (\sqrt[4]{3})^2, i(\sqrt[4]{3})^2, (\sqrt[4]{3})^3, i\ (\sqrt[4]{3})^3\}$$

Obtenue en multipliant terme à terme la base $\{1, i\}$ de l'extension $\mathbb{Q}(i)$ de $\mathbb{Q}$ et la base $\{1, \sqrt[4]{3}, (\sqrt[4]{3})^2, (\sqrt[4]{3})^3\}$ de l'extension $\mathbb{Q}(i,\sqrt[4]{3})$ de $\mathbb{Q}(i)$.

Un elément $x \in \mathbb{Q}(i,\sqrt[4]{3})$ s'écrit, d'une manière unique, sous la forme :

$$\mathrm{x} = \mathrm{b_0}+\mathrm{b_1 i} + \mathrm{b_2}\sqrt[4]{3}+\mathrm{b_3 i}\sqrt[4]{3}+\mathrm{b_4}(\sqrt[4]{3})^2+\mathrm{b_5 i}(\sqrt[4]{3})^2+\mathrm{b_6}(\sqrt[4]{3})^3+\mathrm{b_7 i}(\sqrt[4]{3})^3.$$

ou $b_j \in \mathbb{Q}$, $0 \leq j \leq 7$

Pour déterminer $C(A)$, on utilise l'équivalence

$$[\mathrm{x} \in \mathrm{C(A)}] \Longleftrightarrow [\sigma_2(\mathrm{x}) = \mathrm{x}]$$

$$\sigma_2(\mathrm{x}) = \mathrm{b_0}+\mathrm{b_1 i} - \mathrm{b_2}\sqrt[4]{3}-\mathrm{b_3 i}\sqrt[4]{3}+\mathrm{b_4}(\sqrt[4]{3})^2+\mathrm{b_5 i}(\sqrt[4]{3})^2-\mathrm{b_6}(\sqrt[4]{3})^3-\mathrm{b_7 i}(\sqrt[4]{3})^3.$$

$$[\mathsf{x} \in \mathsf{C(A)}] \Longleftrightarrow [\sigma_2(\mathsf{x}) = \mathsf{x}] \Longleftrightarrow [\mathsf{b_2} = \mathsf{b_3} = \mathsf{b_6} = \mathsf{b_7} = 0]$$

$$\begin{aligned} &\Longleftrightarrow \quad \mathsf{x} = b_0+\mathsf{b_1 i} + \mathsf{b_4}(\sqrt[4]{3})^2+\mathsf{b_5 i}(\sqrt[4]{3})^2 \\ &\Longleftrightarrow \quad \mathsf{x} \in [\mathbb{Q}(i,(\sqrt[4]{3})^2)]. \end{aligned}$$

et

$$\mathrm{C(A)} = \mathbb{Q}(\mathrm{i},(\sqrt[4]{3})^2) = \mathbb{Q}(\mathrm{i},\sqrt{3}).$$

D'une manière analogue, on détermine les autres corps intermédiaires. Les résultats sont résumés dans le tableau suivant :

Sous groupe	Corps intermédiaire associé
A	C(A)=$\mathbb{Q}(i,\sqrt{3})$
B	C(B)=$\mathbb{Q}(\sqrt[4]{3})$
C	C(C)=$\mathbb{Q}(i\sqrt[4]{3})$
D	C(D)=$\mathbb{Q}((1+i)\sqrt[4]{3})$
E	C(E)=$\mathbb{Q}((1-i)\sqrt[4]{3})$
F	C(F)=$\mathbb{Q}(i)$
J	C(J)=$\mathbb{Q}(i\sqrt{3})$
H	C(H)=$\mathbb{Q}(\sqrt{3})$
$\{\sigma_1\}$	C($\{\sigma_1\}$)=$\mathbb{Q}(i,\sqrt[4]{3})$
G	C(G)=$\mathbb{Q}$

Sous-groupes normal de G : Les sous-groupes d'ordre 4 sont distingués. A est le seul sous-groupe distingué d'ordre 2.

Extensions normale de $\mathbb{Q}$: Les corps intermédiaires qui sont des extensions normales de $\mathbb{Q}$ sont ceux associés aux sous-groupes distingués de G . Ces corps sont:

$$\mathbb{Q}(\mathrm{i},\sqrt{3}),\mathbb{Q}(\mathrm{i}),\mathbb{Q}(\mathrm{i}\sqrt{3}),\mathbb{Q}(\mathrm{i},\sqrt{3}).$$

Selon théorème (2.3.2):

$$\mathrm{Gal}(\mathrm{C(A)}/\mathbb{Q})\cong \mathrm{G/A},\ \mathrm{Gal}(\mathrm{C(F)}/\mathbb{Q})\cong \mathrm{G/F},\ \mathrm{Gal}(\mathrm{C(J)}/\mathbb{Q})\cong \mathrm{G/J},\ \mathrm{Gal}(\mathrm{C(H)}/\mathbb{Q})\cong \mathrm{G/H},$$

D'apres théorème (2.3.1), $\mathbb{Q}(i,\sqrt[4]{3})$ est une extension galoisienne de chaque un corps intermédiaire .

Chapitre 3

Application

3.0.1 Groupe résoluble

Définition 3.0.1 *Soit G un groupe, on appelle suite de composition de G une suite finie de sous-groupes distingués :*

$$G_n = \{e\} \lhd .....G_3 \lhd G_2 \lhd G_1 \lhd G_0 = G$$

Définition 3.0.2 *Un groupe G est dit résoluble s'il admet une suite de composition dont tous les quotients(ou les facteures) sont abéliens, c'est à dire G_i/G_{i+1} est commutatif pour $i \in \{0, 1, 2, ..., n-1\}$*

Proposition 3.0.1 *Tout groupe commutatif est résoluble .*

Preuve. On prend $G_0 = G$ et $G_1 = \{e\}$: G_1 est bien un sous-groupe distingué de G et G_0/G_1 est isomorphe à G et est donc commutatif. ■

Proposition 3.0.2 *[3] Soit G un groupe. Si G est résoluble, alors tout sous-groupe et tout groupe quotient de G est résoluble.*

Théorème 3.0.3 *[8]Soit H un sous -groupe normal et résoluble d'un groupe G. Si G/H est un groupe résoluble, alors G est résoluble.*

Proposition 3.0.3 *Les groupes A_n et S_n sont résolubles pour $n = 2, 3, 4$ et non résolubles pour $n \geq 5$.*

Exemple 3.0.2 *Il y a juste à montrer la résolubilité des S_n pour n=2 ,3 et 4puisque tout sous-groupe d'un groupe résoluble est résoluble (P) , Pour S_2 ;*

$$S_2 = \{id; (1,2)\}$$

est commutatif donc résoluble . Pour S_3, Soient

$$G_0 = S_3, G_1 = A_3, G_2 = \{id\}$$

avec id permutation identique (élément neutre) de S_n et montrons que l'on a bien les conditions :

(1) G_1 est bien un sous-groupe distingué de G_0 (car A_n est toujours un sous-groupe d'indice $(G : H) = 2$ de S_n, donc toujours un sous-groupe distingué) ainsi que G_2 sous-groupe distingué de G_1

(2) $G_0/G_1 = S_3/A_3$ est un groupe d'ordre 2 donc commutatif, $G_1/G_2 = A_3/\{id\}$ est isomorphe à A_3qui est commutatif.

Pour S_4,Cette fois on pose

$$G_0 = S_4, G_1 = A_4, G_2 = V = \{id; (12), (34), (13), (24), (14), (23)\}, G_3 = \{id\} .$$

Preuve que A_n et S_n sont non résolubles pour $n \geq 5$. Il suffit de montrer que A_n est non résoluble car alors S_n est forcément non résoluble (si non il serait résoluble, et donc A_n le serait, en tant que sous-groupe d'un groupe résoluble).preuve résulte du fait que pour $n \geq 5$ A_n est simple, c'est-à-dire ses seuls sous-groupes distingués sont $\{id\}$ et lui même, et que A_n n'est pas commutatif , on termine en montrant qu'il est alors impossible d'avoir une suite $G_i$vérifiant la définition.

F désignera dans touts ce paragraphe un corps de caractéristique nulle.

Théorème 3.0.4 *Si α est un élément non nul du corps F, alors le groupe de Galois du polynome $X^n - \alpha$ est résoluble.*

Preuve. suposons tout d'abord que F contient une racine primitive de l'unité d'order n sur $\mathbb{Q}$ et soit $\alpha \notin F$ un zeros de $X^n - a$, Puisque F contient une racine primitiv $n^{ième}$ de l'unité ε, le corps $K = F(\alpha)$ contient les n racines $\varepsilon^r\alpha$(r entier de 0 à $n-1$) et donc

est le corps de décomposition sur F du polynome $X^n - a$. Un elément σ de $G(K/F)$ est caractérisé par $\sigma(\alpha)$ qui est un certain $\varepsilon^r\alpha$. De méme, si

$$\tau \in G(K/F), \tau(\alpha) = \varepsilon^k\alpha$$

,et on a

$$\sigma(\tau(\alpha)) = \sigma(\varepsilon^k\alpha) = \varepsilon^k\sigma(\alpha).$$

car σ est un $F - automorphisme$ de K laissant invariant $\varepsilon^k \in F$. Ainsi

$$\sigma\tau(\alpha) = \varepsilon^{k+r}\alpha$$

et aussi

$$\tau\sigma(\alpha) = \varepsilon^{r+k}\alpha$$

ce qui implique

$$\sigma\tau = \tau\sigma.$$

Le groupe $G(K/F)$ est donc commutatif.

Supposons maintenant que F ne contienne aucune racine primitive de l'unité d'order n sur $\mathbb{Q}$ et soit $\alpha \notin F$ une racine de $X^n - a$. posons $F' = F(\varepsilon)$, avec ε racine primitive de l'unité d'order n. F' est le corps de décomposition du polynome $X^n - 1$ sur F, c'est donc une extension normale de F et G(F$'$/F) est un groupe commutatif . puisque les $\varepsilon^r\alpha$(r entier de 0 à $n-1$) sont les n racine du polynome $X^n - a$, le corps de décomposition K de ce polynome contient F'. d'apres le théoréme (2.1.6)

$$G(K/F') \lhd G(K/F)$$

$$\mathrm{G(F'/F)} \approxeq \frac{G(K/F)}{G(K/F')}$$

$G(K/F')$ est un soue groupe normal et résoluble du groupe $G(K/F)$. Selons théoréme (2.3.2)Donc le groupe $G(K/F)$ est aussi résoluble. ■

3.0.2 Extension par radicaux(ou Extension radicale)

Définition 3.0.3 *α est un radical sur F signifie que α est dans une extension de F et qu'il existe un entier naturel p non nul tel que α^p soit dans F.*

Exemple 3.0.3 *i est un radical sur $\mathbb{R}$ ($i^2 = -1$).*

ω est un radical sur $\mathbb{R}$ ($\omega^3 = 1$), $\omega = e^{\frac{i2\pi}{3}}$.

Définition 3.0.4 *On dit un corps E est une extension de F par radicaux (ou extension radicale) de F s'il existe une suite d'extensions simples telle que :*

$$F = F_0 \subset F_1 ..... \subset F_n = E$$

et si $n \geq 1$, pour $i = 1, 2, ..., n$, il existe α_i dans F_i qui soit un radical sur F_{i-1} [c'est-à-dire il existe un entier naturel $n(i) = n_i$ non nul tel que $\alpha_i^{n(i)}$ soit dans F_{i-1}] et tel que

$$\mathrm{F}_{i-1}(\alpha_i) = \mathrm{F}_i$$

La suite F_i est aussi appelée tour radicale.

Exemple 3.0.4

1) $\mathbb{C}$ est une extension par radicaux de $\mathbb{R}$ ($n = 1, \mathbb{C} = \mathbb{R}(i)$).

2) $\mathbb{Q}(\sqrt{2})$ est une extension par radicaux de $\mathbb{Q}$.

3) Le nombre $\sqrt[7]{\sqrt[3]{2} + \sqrt{-3}}$ est contenu dans une extension radicale de $\mathbb{Q}$, car on peut par exemple construire une tour radicale $(\mathbb{Q}_i)0_{\leq i \leq 3}$ de $\mathbb{Q}$ de la maniére suivante :

$$\mathbb{Q}_0 = \mathbb{Q}, \mathbb{Q}_1 = \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}_2 = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}), \mathbb{Q}_3 = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}, \sqrt[7]{\sqrt[3]{2}, \sqrt{-3}}).$$

4) $E = \mathbb{Q}(\zeta)$, ou ζ est une racine n-ième de l'unité, est une extension radicale de $\mathbb{Q}$, $\zeta^n = 1 \in \mathbb{Q}$.

Remarque 3.0.1 *1) Si E est une extension par radicaux de F, alors les α_i sont algébriques sur F, et E est une extension finie de F.*

2) Si E est une extension par radicaux de F, une extension intermédiaire entre F et E n'est pas forcément une extension par radicaux de F.

Preuve. Preuve de la remarque (1) de c-a-d : prouvons que si E est une extension par radicaux de F, alors les α_i sont algébriques sur F, et E est une extension finie de F. Tout d'abord, pour tout i dans $\{1, 2, ..., n\}$, α_i est algébrique sur F_{i-1}, car il est racine du polynôme $X^{n(i)} - \alpha_i$ lequel est à coefficients dans F_{i-1}. Donc α_1 est algébrique sur F et l'extension

$$F \subset F_1 = F(\alpha_1)$$

est finie . De même α_2 est algébrique sur F_1 et l'extension

$$F_1 \subset F_2 = F_1(\alpha_2)$$

est finie. Donc l'extension F_2 de F est finie, donc algébrique (voir Proposition 1.1.2) et ainsi α_2 (qui est dans F_2) est algébrique sur F. etc : pour tout i dans $\{1, 2, ..., n\}$

$$F_i = F(\alpha_1, ..., \alpha_i)$$

est une extension finie de F et α_i est algébrique sur F. En particulier E extension radicale de F est une extension finie de F.

Voici un contre-exemple du fait que si E est une extension par radicaux de F, une extension intermédiaire entre F et E n'est pas forcément une extension par radicaux de F.

On prend $F = \mathbb{Q}$, $E = \mathbb{Q}(\omega)$ avec $\omega = exp(2i\ \pi/7)$, qui est bien un radical de $\mathbb{Q}$, car $\omega^7 = 1$. Soit $\alpha = cos(2\pi/7)$: il est dans E car $\alpha = (\omega + \omega^6)/2$ et donc

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\omega)$$

(puisque $\mathbb{Q}(\alpha)$ est le plus petit corps contenant α et $\mathbb{Q}$), et pourtant $\mathbb{Q}(\alpha)$ n'est pas une extension par radicaux de F. ■

Proposition 3.0.4 [2]*Soit E une extension de F par radicaux, alors il existe une extension galoisiénne par radicaux de F contenant E.*

3.0.3 Equation résoluble par radicaux

Définition 3.0.5 *Un polynôme $P(X)$ de $F[X]$ est dit résoluble par radicaux sur F s'il existe une extension radicale L de F contenant le corps de décomposition E de P.*

Théorème 3.0.5 *[4]Si E une extension galoisiénne par radicaux de F. Alors son groupe de Galois est résoluble.*

Corollaire 3.0.2 *Soit $f \in F[X]$ un polynome non constant. Si f est résoluble par radicaux , alors $Gal(E/F)$ est résoluble avec E est le corps de décomposition de f.*

Preuve. Si f est résoluble par radicaux, alors il existe une extension radical L de F telle que :

$$\mathsf{F} \subset \mathsf{E} \subset \mathsf{L}$$

d'apres la propsition précdente L est une extension galoisienne de F, soit

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

et comme E est une extension normale de F, alors E est une extension gaoisienne de F

soit

$$G = Gal(E/F)$$

donc par theoréme (2.1.6)

$$Gal(E/F) = H\ /G$$

mais H est résoluble d'aprés le theoréme (3.0.3) donc H/G est résoluble. Finalement $Gal(E/F)$ est résoluble. ■

Corollaire 3.0.3 *Soient F un corps et $f(X) \in F[X]$ un polynome de degré m avec*

$$1 \leq m \leq 4$$

. alors l'equation $f(X) = 0$ est résoluble par radicaux.

Théorème 3.0.6 [8]*Il existe un corps L contenant F et un polynôme irréductible f sur L de degré ≥ 5 telle que l'quation $f(X) = 0$ est non résoluble par radicaux.*

Exemple 3.0.5 *Le polynome*

$$P(X) = X^5 - 4X^3 - 2 \in \mathbb{Q}[X]$$

n'est pas résoluble.par radicaux.

Démonstration. D'apres le corollaire précedent, il suffi de déterminer son groupe de Galois et de monter que ce n'est pas un groupe résoluble

Soit E le corps de décomposition de P sur $\mathbb{Q}$ et $G = Gal(E/\mathbb{Q})$ son groupe de Galois. le polynome P est irréductible sur $\mathbb{Q}$ d'apres le critère d'Eisenstein . Il a trois racines réelles $\mathrm{x}_{1,}x_2, x_3$et deux racines complexes conjuguées qu'on notera a et b :ce la résulte de l'étude des variations de P à laide de la dérivée de P,

$$\mathrm{P}^{'} = (X^2)(5X^2 - 12)$$

La conjugaison de $\mathbb{C}$ (i.e. l'automorphisme qui à un nombre complexeassocie son conjugué complexe) restreinte à E est un élément de G qui ´echange a et b et qui laisse invariant x_1, x_2, x_3. Cela correspond en fait à une transposition de S_5. On a

$$|G| = [E : \mathbb{Q}] = [E : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}].$$

ou

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5$$

car a est algébrique de *degré* 5 sur $\mathbb{Q}$ (puisque P est le polynome minimal). Cela implique que l'ordre de G est un multiple de 5. Par Cauchy il existe donc un élément σ d'ordre 5 dans G, correspondant à un $5-cycle$ de S_5. G est alors identifiable à un sous-groupe de S_5 qui contient un $5-cycle$ et une transposition. Comme S_5 peut etre engendré par justement un $5-cycle$ et unetransposition, alors G est isomorphe à S_5, qui n'est pas résoluble. Donc G est non résoluble et P non résoluble par radicaux. ■

3.1 Conclusion générale

L'objet de ce memoir est dans un premier temps d'introduire les bases et outils d'algébre générale (extensions de corps...) qui permettront dans un deuxiéme temps de développer la théorie de Galois, ainsi l'une des applications de cette théorie : les équations résolubes par radicaux .

Bibliographie

[1] **Aigli Papantonnopulo**, Algebra pure & applied, Prentice -Hall. Upper Saddle Riner, 2002.

[2] **Carstensen, Celine, Benjamin Fine, and Gerhard Rosenberger**. Abstract Algebra: Applications to Galois Theory, Algebraic Geometry, and Cryptography. Vol. 11. Walter de Gruyter, 2011.

[3] **Derek J. S. Robinson**, An Introduction To Abstract Algebra, Walter de Gruyter, Berlin, New York, 2003

[4] **Goldstein, Larry Joel**. Abstract algebra: a first course. 1973, Prentice-Hall Inc Englewood Cliffs New jersey, 1973.

[5] **Jean Pierre Escofier**, Theorie de Galois Cours et exercice corrigés, 2^eédition, Dunod,paris, 1997.

[6] **John R. Durbin**, Modern Algebra An Introduction, sixth Eddition, Ellipses Edition Marketing S, A, 2006.

[7] **Josette Calais**, Extensions De Corps Théorie de Galois, Ellipses Edition Marketing S. A, 2006.

[8] **Querré, Julien,** Cours d'algèbre, Masson paris New York Barcelone Milan, 1976.

[9] http://alain.pichereau.pagesperso-orange.fr/equation7.html.

.