République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

Faculté de Mathématiques

Département d'Algèbre et Théorie des Nombres

Mémoire de Master

Filière : Mathématique

Spécialité : Arithmétique Codage et Combinatoire

GROUPES DE GALOIS DES EXTENSIONS CUBIQUES ET QUARTIQUES

Présenté par :

Bayou Mohamed Cherif & Alliche Amrane

Encadré par :

M. Bensebaa Boualem

Devant le jury composé de :

M. enseignant 1	Président
M. enseignant 2	Examinateur

Remerciements

Table des matières

Table des figures

Liste des tableaux

Liste des Algorithmes

Introduction

Chapitre 1

EXTENSION DE CORPS

Dans tout ce qui suit K désigne un corps commutatif.

1.1 Propriété élémentaires des extensions de corps

Définition 1.1. *On appelle extension de K, la donnée d'un corps L et d'un homomorphisme $i : K \longrightarrow L$ de telle sorte qu'on ait l'isomorphisme $K \simeq i(K)$.*
L'homomorphisme i est appelé plongement de K dans L.

Ainsi définie, K est un sous-corps de L, à isomorphisme près.
Lorsque $K \subset L$, le corps L est alors considéré comme un K-espace vectoriel. Soit, dans ce cas, $\alpha \in L$ et définissons le morphisme d'anneaux suivant

$$\begin{array}{rccc} \phi_\alpha : & K[X] & \longrightarrow & K[\alpha] \\ & X & \longrightarrow & \alpha \end{array}$$

de noyau $\ker \phi_\alpha$ qui est un idéal premier et principal.

Définition 1.2. *On dit que l'élément $\alpha \in L$ est algébrique lorsque* $\ker \phi_\alpha \neq \{0\}$*, sinon il sera dit transcendant.*

Notation : L'extension L d'un corps K est notée L/K.

Exemple 1.3. *1. Tout corps de caractéristique 0 est extension du corps $\mathbb{Q}$.*

2. Tout corps de caractéristique $p \neq 0$ est extension du corps $\mathbb{Z}/p\mathbb{Z}$.

Définition 1.4. *On dit qu'un corps M est un* ***corps intermédiaire*** *pour une extension L/K, si $K \subset M \subset L$.*

Définition 1.5. *Soit $n \in \mathbb{N}^*$.*
Le corps $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, où les α_i, $1 \leq \alpha_i \leq n$ sont des élément de L , est appelée extension de K obtenue par adjonctions successives de ces éléments. On écrira alors :

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2)\,, K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3), \ldots$$
$$\ldots, K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n).$$

Définition 1.6. *Soit L/K une extension de corps. On suppose que $K \subseteq L$; alors pour tout partie non vide δ de L, le sous-corps de L engendré par $K \cup \delta$ est noté $K(\delta)$, appelé extension de K obtenue par l'adjonction de δ à K.*

Remarque 1.7. *Pour $\delta = \{\alpha\}$, où $\alpha \in L$, $K(\delta)$ s'écrit $K(\alpha)$, elle est dite* ***extension simple*** *de K obtenue par l'adjonction de α à K.*

1.1.1 degré d'une extension de corps

Pour une extension L/K donnée, le corps L est considéré comme un espace vectoriel sur K. Rappelons que tout espace vectoriel de dimension finie admet une base finie et toutes les bases ont le même cardinale, appelé dimension de cet espace vectoriel.

Définition 1.8. *Soit L/K une extension de corps.*
On appelle degré de l'extension L/K, noté $[L/K]$, la dimension du K-espace vectoriel L.
Lorsque la dimension du K-espace vectoriel L est finie, l'extension L/K est dite de degré finie et on note par $[L/K] = \dim_K L$ le degré de cette extension.

Théorème 1.9. *(Théorème de la base télescopique) Étant données les extensions de corps L/K et M/L, alors*

$$[M/K] = [M/L] \times [L/K]. \tag{1.1}$$

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [6]**). □

Du théorème (1.9), on déduit le corolaire suivant.

Corollaire 1.10. *soit L/K une extension de corps, $[L/K] < \infty$; si, $\{K_i\}$,*
$r \in \mathbb{N}^*, 1 < r \leq n$ est une famille finie, totalement ordonnée, de corps intermédiaires, alors

$$K \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r \subseteq L \text{ implique}$$
$$[L/K] = [L/K_r][K_r/K_{r-1}] \ldots [K_1/K].$$

1.2 Isomorphisme d'extension de corps

Une extension L de K est définie par la donnée d'un couple (L, i), où i est un plongement de K dans L.

Définition 1.11. *Soit K et L deux corps isomorphes, on dit que les extensions L/K et M/F, définies respectivement par les couple (L, i) et (M, j) sont isomorphes, s'il existe un couple d'isomorphisme (λ, μ), respectivement, de K sur F et de L sur M, tel que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & F \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle j} \\ L & \xrightarrow{\mu} & M \end{array}$$

C'est à dire $\mu \circ i = j \circ \lambda$.
On dit alors que le couple (λ, μ) est un isomorphismes d'extensions de corps de L/K sur M/F.

En particulier :

- *Si $K \subseteq L$ et $F \subseteq M$, on a,*

$$\mu \circ i = j \circ \lambda \iff \mu_{/K} = \lambda.$$

- *Si $K = F$, $\lambda = id_k$, le diagramme devient alors,*

$$\begin{array}{ccc} K & & \\ \downarrow{\scriptstyle i} & \searrow^{j} & \\ L & \xrightarrow{\mu} & M \end{array}$$

D'où $\mu \circ i = j$.

Si de plus, μ , α sont les injections canoniques alors,

$$\mu \circ i = j \iff \mu_{/K} = id_K.$$

et dans ce cas on dit que les corps M et L sont conjugués sur K, (on dit aussi que ils sont K-isomorphes).

1.3 Extensions algébriques - Clôtures algébriques

1.3.1 Éléments algébriques

Définition 1.12. *Soit L/K une extension de corps, soit $\alpha \in L$. α est dit algébrique sur K, s'il existe un polynôme $p(X) \in K[X]$, non nul, tel que $p(\alpha) = 0$. Dans ce cas, l'extension $K(\alpha)$ est dite* ***simple et algébrique*** *sur K.*
Lorsque α n'est pas algébrique il est dit transcendant

Proposition 1.13. *Soit L/K une extension de corps, pour tout α dans L on associe l'application*

$$\begin{aligned} f_\alpha : K[X] &\longrightarrow L \\ g(X) &\longrightarrow g(\alpha) \end{aligned}$$

où f_α désigne un morphisme d'anneaux unitaires et on a

$$f_\alpha \, est \, non \, injectif \iff \alpha \, est \, algbrique \, sur \, K$$

Démonstration. $K[\alpha]$ étant un sous-anneau du corps L, il est donc intègre et $K[\alpha] = Im f_\alpha$. De plus, on a les équivalences suivantes

$$\begin{aligned} f_\alpha \, est \, non \, injectif &\iff Ker f_\alpha \neq \{0\} \\ &\iff \exists g(X) \in K[X] \backslash \{0\} \; tel \, que \, g(\alpha) = 0 \\ &\iff \alpha \, est \, algbrique \, sur \, K \end{aligned}$$

□

Définition 1.14. *Soit L/K une extension de corps, $\alpha \in L$ un élément algébrique sur K, le polynôme non constant $p(X)$, unitaire et irréductible de $K[X]$, vérifiant $p(\alpha) = 0$, est appelé le polynôme minimal de α sur K, noté $irr_K(\alpha, X)$.*

Le résultat ci-dessous donne une caractérisation du polynôme minimal d'un élément algébrique.

Théorème 1.15. *Soit L/K une extension de corps, si $\alpha \in L$ et un élément algébrique sur K, alors*

1. Il existe un unique polynôme $p(X)$, unitaire et irréductible de $K[X]$ vérifiant

$$\forall f(X) \in K[X]\backslash\{0\} \; et \; f(\alpha) = 0 \iff p(X)|f(X) \, dans \, K[X]. \tag{1.2}$$

2. L'extension simple $K(\alpha)/K$ vérifie

$$K(\alpha) = \{f(\alpha),\, f(X) \in K[X]\}\,. \tag{1.3}$$

3.

$$[L/K] = [K(\alpha)/K] = deg\, p. \tag{1.4}$$

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [13-14]**). □

Théorème 1.16. *Soit K un corps et soit $P(X) \in K[X]$, un polynôme unitaire et irréductible, alors Il existe une extension simple de $K(\alpha)/K$, telle que α est algébrique sur K de polynôme minimal $irr_K(\alpha, X) = P(X)$.*

Démonstration. K étant un corps donc l'anneau $K[X]$ est factoriel, donc $p(X)$ unitaire et irréductible est un élément premier non nul de $K[X]$, de plus $p(X)$ est maximal dans $K[X]$, ($K[X]$ est un domaine principal), donc on a $L = \dfrac{K[X]}{(p(X))}$ corps .

Soit λ l'injection canonique de K dans $K[X]$ et soit δ la surjection canonique de $K[X]$ sur L, alors $\delta \circ \lambda$, un morphisme d'anneaux unitaire de K dans L, est un monomorphisme. On en déduit que L est une extension de K, telle que $\forall \beta \in K$ est identifiable a son image par le monomorphisme $\delta \circ \lambda$.

Dans L posons $f(X) := \alpha$.

$$L = \{f(g(X))\,;\, g(X) \in K[X]\} = \{g(\alpha)\,;\, g(X) \in K[X]\}\,.$$

D'autre part

$$f(p(X)) = 0 \Longrightarrow p(\alpha) = 0.$$

l'élément α de L est nécessairement algébrique sur K ce qui implique que $L = K(\alpha)$, on conclut que L est une extension simple et algébrique de K, de plus par hypothèse $p(X)$ est

unitaire et irréductible dans $K[X]$, donc

$$p(\alpha) = 0 \Longrightarrow p(X) = irr_K(\alpha, X).$$

□

Corollaire 1.17. *Tout extension simple et algébrique d'un corps K est isomorphe a un corps de la forme $\frac{K[X]}{(p(X))}$, où $p(X)$ est un polynôme unitaire et irréductible dans $K[X]$.*

Exemple 1.18. *Soit $p(X) = X^3 - 7$ dans $\mathbb{Q}[X]$, le polynôme $p(X)$ est unitaire, irréductible car il est d'Eisenstein pour le nombre premier $t = 7$.*
Posons $\alpha = \sqrt[3]{7}$, on a bien $p(\alpha) = 0$ donc

$$irr_K(\sqrt[3]{7}, X) = X^3 - 7\,;\, \mathbb{Q}(\sqrt[3]{7}) \simeq \frac{\mathbb{Q}[X]}{(X^3 - 7)}\,;\, [\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}] = 3.$$

la famille $\{1, \alpha, \alpha^2\}$ forme une base de $\mathbb{Q}(\sqrt[3]{7})$ comme $\mathbb{Q}$-espace vectoriel et tout élément $x \in \mathbb{Q}(\sqrt[3]{7})$ s'écrit d'une manière unique tel que on a

$$x = a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2\,;\, a, b, c \in \mathbb{Q}.$$

Définition 1.19. *Soit α et β deux élément de K et algébriques sur K, Soit $K(\alpha)/K$, $K(\beta)/K$, deux extensions simples et algébriques de K. On dit que les éléments α et β sont conjugué sur K, si*

$$irr_K(\beta, X) = irr_K(\alpha, X).$$

Dans ce cas, on dit aussi que les extensions $K(\alpha)/K$, $K(\beta)/K$ sont K-isomorphes.

Définition 1.20. *On appelle corps de rupture d'un polynôme unitaire et irréductible $p(X)$ sur K, le corps $K(\alpha)$, tel que $p(X) = irr_K(\alpha, X)$.*

1.3.2 Extension algébrique

Définition 1.21. *On dit que l'extension L/K est algébrique sur K , si tout élément de L est algébrique sur K*

Théorème 1.22. *Tout extension L/K de degré fini, est nécessairement algébrique sur K.*

Démonstration. On pose $[L/K] = n \in \mathbb{N}^*$, et soit $\alpha \in L$. Dans le cas ou $\alpha \in K$, alors α est forcément algébrique sur K. Supposons maintenant que $n > 1$ et que $\alpha \in L \setminus K$, l'ensemble

$\{\alpha^i\ ; i \in \mathbb{N}\}$ forme une base de L comme K-espace vectoriel, par suite il existe un entier $t > 1$ et des élément β_i, $0 \leq i \leq t$, non tous nul dans L, tels que

$$\sum_{0 \leq i \leq t} \beta_i \alpha^i = 0.$$

ce qui exprime que l'élément α est algébrique sur K. □

Corollaire 1.23. *Tout extension simple, algébrique d'un corps K est une extension algébrique de K.*

Théorème 1.24. *L'extension L/K est algébrique et de degré fini si et seulement si L est obtenu par l'adjonction à K d'un nombre fini d'élément algébrique sur K.*

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [18-19]**). □

Théorème 1.25. *Soient L/K et M/L deux extensions de corps ; alors*

$$L/K \text{ et } M/L \text{ algébriques } \Longrightarrow M/K \text{ algébrique.}$$

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [20]**). □

1.3.3 Clôtures algébriques

Proposition 1.26. *Soit K un corps ; les propriétés suivantes sont équivalents :*

1. *K est algébriquement clos.*
2. *Tout polynômes de $K[X]$ est scindé sur K.*
3. *Tout polynômes irréductibles de $K[X]$ est de degré 1.*

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [67]**) □

Exemple 1.27. — *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

— *Le corps $\mathbb{R}$ des réels n'est pas algébriquement clos.*

Théorème 1.28. *Pour tout corps K, il existe au moins un corps E algébriquement clos qui est extension de K.*

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [72]**)

□

Exemple 1.29. — *Pour les deux corps $\mathbb{Q}$ et $\mathbb{R}$ il existe le corps $\Omega = \mathbb{C}$ algébriquement clos, et extensions de ces deux corps.*

— *Pour les corps finis de caractéristique p (i.e., $\mathbb{F}_p$) il existe le corps $\Omega = \cup_{n\geq 0}\mathbb{F}_{p^{n!}}$ extension de $\mathbb{F}_p$ et algébriquement clos.*

Définition 1.30. *On appelle clôture algébrique L de K toute extension de K telle que :*

1. *L est algébrique sur K.*
2. *L est algébriquement clos.*

Théorème 1.31. *Tout corps K admet une clôture algébrique qu'on note $\overline{K}$. Plus précisément, si L un corps algébriquement clos, extension de K alors*

$$\overline{K} = \{\alpha \in L,\ \alpha \text{ algébrique sur } K\} \subseteq L$$

est un corps et c'est une clôture algébrique de K.

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [74]**)

□

Exemple 1.32. 1. *Nous savons déjà que $\mathbb{C}$ est un corps algébriquement clos (le théorème fondamentale de l'algèbre), et on sait que $\mathbb{C}$ est une extension algébrique sur $\mathbb{R}$ (car $\mathbb{C} = \mathbb{R}(i)$) alors $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$ et on écrit $\overline{\mathbb{R}} = \mathbb{C}$.*
2. *Tandis que $\mathbb{C}$ n'est pas extension algébrique sur $\mathbb{Q}$ (car il existe en particulier e et π deux éléments transcendants sur $\mathbb{Q}$) donc $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$. Mais comme $\mathbb{C}$ est algébriquement clos et contient $\mathbb{Q}$ alors*

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C},\ \alpha \text{ algébrique sur } \mathbb{Q}\} \subsetneq \mathbb{C}$$

est une clôture algébrique de $\mathbb{Q}$.

1.4 Extensions normales - Clôture normale

1.4.1 Corps de décomposition d'un polynôme

Rappelons quelques définitions et résultats sur les polynômes à coefficients dans un corps K.

• Tout polynôme $f(X)$ de $K[X]$, de $deg\ n > 0$, admet exacteent n racines, (distinctes ou confondus), dans K.

• dans l'anneau $K[X]$, tout polynôme $f(X) \in K[X]/K$ s'écrit d'une manière unique

$$f(X) = a(p_1(X))^{n_1}(p_2(X))^{n_2}.....(p_r(X))^{n_r},\ \text{et}\ \sum_{1\leq i\leq r} n_r = deg\ f \tag{1.5}$$

où $a \in K^*$, $r \in \mathbb{N}^*$, pour $1 \leq i \leq r$ les $p_i(X)$ sont des polynômes unitaires et irréductibles deux à deux distincts dans $K[X]$.

• Un polynôme $f(X)$ de $K[X]$ est dit scindé sur K, si dans la relation (1.5), si $\forall i\ 1 \leq i \leq r$, $p_i(X)$ est de degré 1 ;

$$f(X) = a(X-\alpha_1)^{n_1}(X-\alpha_2)^{n_2}\dots(X-\alpha_r)^{n_r}.$$

• Soit le polynôme $f(X) \in K[X]$, on suppose que α une racine de $f(X)$, $(f(\alpha) = 0)$. le polynôme f, n'a que des racines simples $\iff$ $f \wedge f' = 1$ et $f' \neq 0$, f' désigne le polynôme dérivé de f.

Définition 1.33. *Soit $f(X)$ un polynôme non constant dans $K[X]$, on appelle corps de décomposition de f sur K noté $Dec_k(f(X))$, tout extension L de K vérifiant*

1. *$K \subseteq L$ et $f(X)$est scindé sur$L$.*
2. *$K \subseteq E \subseteq L$ et $f(X)$est scindé sur$E \Longrightarrow L = E$.*

Proposition 1.34. *Soit L un corps de décomposition d'un polynôme $f(X)$ non constant de $K[X]$, si $n = deg\, f > 0$ et si $\beta_1, \beta_2, \dots, \beta_n$ sont les racines distinctes ou confondues de f dans L, alors, $L = K(\beta_1, \beta_2, \dots, \beta_n)$, donc L est une extension algébrique de degré fini sur K.*

Démonstration. On a

$$K \subseteq L\ et\ \forall i(1 \leq i \leq n),\ \beta_i \in L \Longrightarrow K(\beta_1, \beta_2, \dots, \beta_n) \subseteq L. \tag{1.6}$$

D'autre part le polynôme f étant scindé sur L, et dans $L[X]$, $f(X)$ s'exprime par

$$f(X) = a(X-\beta_1)(X-\beta_2)\dots(X-\beta_n),\ \text{où}\ a \in K^*.$$

Donc d'après cette égalité f est scindé sur $K(\beta_1, \beta_2, \dots, \beta_n)$, de plus la relation (1.6) et

la def.1.4.1 impliquent que $L = K(\beta_1, \beta_2, \ldots, \beta_n)$, on en déduit L/K est une extension algébrique de degré fini. □

Remarque 1.35. *La construction d'un corps de décomposition d'un polynôme non constant n'est pas unique.*

Corollaire 1.36. *Deux corps de décompositions sur K d'un polynôme $f(X)$ non constant dans $K[X]$, sont K-isomorphes.*
Le polynôme $f(x)$ étant scindé sur L, qui est extension du corps K, alors L contient nécessairement un corps de décomposition de f sur K.

Remarque 1.37. *Le corps de décomposition d'un polynôme $f(X)$ non constant dans $K[X]$, est à K-isomorphisme prés, la plus petit extension de K sur laquelle $f(X)$ est scindé.*

1.4.2 Extension Normale

Définition 1.38. *L'extension L/K est dite normale si elle vérifie :*

1. *L est algébrique sur K.*
2. *Tout polynôme irréductible de $K[X]$, qui a une racine dans L est scindé sur L.*
3. *L est corps de décomposition sur K, d'un polynôme de $K[X]$.*

1.4.3 Clôture normale

Définition 1.39. *On appelle clôture normale d'une extension L/K, une extension L' de L telle que $K \subseteq L \subseteq L'$ telle que*

1. *L' est extension normale de K.*
2. *$(L \subseteq N \subseteq L'$ extensions normales de $K) \Longrightarrow N = L'$.*

Théorème 1.40. *Pour tout extension de degré fini L/K il existe une clôture normale N, de degré fini sur K à K-isomorphisme prés.*

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [41]**). □

Remarque 1.41. *Si $L = K(\alpha)$, N est une clôture normale de $K(\alpha)$ sur K si, et seulement si, N est corps de décomposition sur K du polynôme $irr_K(\alpha, X)$.*

Exemple 1.42. *On reprend l'exemple 1.18, l'extension* $\mathbb{Q}(\sqrt[3]{7})$, $\sqrt[3]{7} \in \mathbb{R}$, *n'est pas une extension normale de* $\mathbb{Q}$, *car le polynôme* $X^3 - 7$, *irréductible sur* $\mathbb{Q}$ *n'a qu'une seule racine dans* $\mathbb{Q}(\sqrt[3]{7})$. *Cependant, si* j *et* j^2 *désignent les racines cubiques non réelles de l'unité, dans* $\mathbb{C}$, *donc* $N = \mathbb{Q}(\sqrt[3]{7}, j\sqrt[3]{7}, j^2\sqrt[3]{7})$ *est corps de décomposition de* $irr_{\mathbb{Q}}(\sqrt[3]{7}, X)$, *donc* N *est une clôture normale de* $\mathbb{Q}(\sqrt[3]{7})$ *sur* $\mathbb{Q}$, *contenue dans* $\mathbb{C}$.

1.5 Extensions séparables

1.5.1 polynômes irréductibles, polynômes séparables

Définition 1.43. *On dit qu'un polynôme irréductible de* $K[X]$ *est séparable, si il n'a que des racines simples dans un corps de décomposition sur* K.

Proposition 1.44. *Soit* $f(X) \in K[X]\backslash K$, *et* $f'(X)$ *sont polynôme dérivé; alors*

1. *car* $K = 0 \Longrightarrow f'(X) \neq 0$.
2. *car* $K = p \neq 0 \Longrightarrow (f'(X) = 0 \iff f(X) = g(X^p))$, $g(X) \in K[X]$.

Démonstration. On pose $d = deg\, f > 0$, donc dans $K[X]$

$$(f(X) = \sum_{0 \leq i \leq d} \alpha_i X^i,\ \alpha_i \neq 0) \Longrightarrow f'(X) = \sum_{1 \leq i \leq d} i\alpha_i X^{i-1}.$$

1. *car* $K = 0 \Longrightarrow \alpha_i \neq 0 \Longrightarrow d\alpha_d \neq 0 \Longrightarrow f'(X) \neq 0$.
2. *car* $K = p$, où p est premier, l'expression de $f'(X)$ implique que

$$\begin{aligned} f'(X) = 0 &\iff \forall i (1 \leq i \leq d),\ i\alpha_i = 0 \\ &\iff \forall i (1 \leq i \leq d),\ (\alpha_i = 0 \,\text{ou}\, p|i). \end{aligned}$$

On en déduit que, pour $r \in \mathbb{N}^*$, $\beta_k \in K$, $\forall 0 \leq k \leq r$.

$$\begin{aligned} f'(X) = 0 &\iff f(X) = \textstyle\sum_{0 \leq k \leq r} \beta_k X^{kp} \\ &\iff f(X) = g(X^p),\ \text{où}\, g(X) = \textstyle\sum_{0 \leq k \leq r} \beta_k X^k. \end{aligned}$$

□

Définition 1.45. *1. Un polynôme* $f(X) \in K[X]\backslash K$ *est dit séparable sur* K *si ses tout diviseurs irréductibles sont séparables sur* K.

2. *Soit l'extension L/K, un élément α de L est séparable sur K si α est algébrique sur K et le polynôme $irr_k(\alpha, X)$ est séparable sur K.*
3. *L'extension L/K, est séparable si tout α de L est séparable sur K.*
4. *Un corps K est dit parfait si toute extension algébrique de K est séparable sur K.*

Remarque 1.46. *On remarque que tout extension séparable d'un corps K, est nécessairement algébrique sur K.*

Théorème 1.47.

$$K \text{ corps parfait} \iff (car\, K = 0)\, ou\, (car\, K = p\, et\, K = \{a^p;\, a \in K\}).$$

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [44-45]**). □

Corollaire 1.48. *Tout corps fini de car $p \neq 0$ est parfait.*

Corollaire 1.49. *Tout extension de $\mathbb{Q}$ est séparable.*

Proposition 1.50. *Soit L/K une extension de degré fini, normale et séparable, alors L est corps de décomposition sur K d'un polynôme séparable.*

Démonstration. On suppose que $[L/K] > 1$, L est normale et de degré fini sur K, donc L est corps de décomposition d'un polynôme non constant $f(X)$ de $K[X]$, de plus L est séparable sur K, ainsi tout facteur irréductible de $f(X)$ est scindé L, est séparable sur K, on en déduit que $f(X)$ est aussi séparable sur K. □

Théorème 1.51. *(**transitivité de la séparabilité**)*
Soient L/K et M/L deux extension de corps,alors on a l'équivalence

$$M/K \text{ séparable} \Longrightarrow M/L \text{ et } L/K \text{ sont séparables.}$$

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [45]**). □

Théorème 1.52. *(Théorème de l'élément primitif)*
Une extension finie L/K est séparable si, et seulement si, elle est simple.

Démonstration. (**Voir Calais J. Extensions de corps Théorie de Galois. Page [45-46]**) □

Définition 1.53. *Pour une extension L/K séparable et de degré fini, on dit qu'un élément $\beta \in L$ est élément primitif, si $L = K(\beta)$.*

Définition 1.54. *Étant donné une extension L/K, on dit qu'un automorphisme σ du corps L est un K-automorphisme de L, si $\sigma_{|K} = id_K$.*

1.5.2 Extension galoisienne

Définition 1.55. *On dit que l'extension L/K est galoisienne si elle est a la fois normale et séparable.*

Exemple 1.56. *Dans l'exemple 1.42, on a vu que l'extension, $\mathbb{Q}(\sqrt[3]{7}, j)/\mathbb{Q}$, est normale, de plus $[\mathbb{Q}(\sqrt[3]{7}, j)/\mathbb{Q}] = 3$, donc de degré fini, par suite la car $\mathbb{Q} = 0$, donc l'extension $\mathbb{Q}(\sqrt[3]{7}, j)/\mathbb{Q}$ est séparable, on en déduit que c'est aussi une extension galoisienne d'après la définition 1.55.*

Chapitre 2

Théorie de Galois

La théorie de Galois est l'étude des extensions de corps $L \,/\, K$ au moyens des groupes des K-automorphismes de L.

Cette méthode introduite par le mathématiciens français **Evarist Galois (1811-1832)** s'avéra d'une grande efficacité ; elle lui permit, en particulier, de résoudre un problème qui préoccupait les mathématiciens de son époque, à savoir la caractérisation des équations polynomiales dites *résolubles par radicaux*.

Par ailleurs grâce à la théorie de Galois, il a été possible d'apporter des réponses à de nombreuses questions que se posaient les mathématiciens, parfois depuis l'Antiquité, telle la construction des polygones réguliers par la règle et le compas.

2.1 Groupe de Galois et correspondance de Galois

Définition 2.1. *On appelle groupe de Galois d'une extension L/K, le groupe des K-automorphismes de L qui sera noté $Gal(L/K)$.*

Théorème 2.2. — *Soit $\overline{K}$ une clôture algébrique de corps K est soit P un polynôme irréductible de $K[X]$. Pour toute racine α de P dans $\overline{K}$, alors le nombre de K-automorphismes de $K(\alpha)$ est égale au nombre de racines distinctes de P dans $\overline{K}$(i.e., de K-conjugués de α distincts) qui appartiennent à $K(\alpha)$.*

Démonstration. Considérons le schéma suivant

$$\begin{array}{ccc} \overline{K} & & \overline{K} \\ | & & | \\ K(\alpha) & \xhookrightarrow{\sigma} & \sigma(K(\alpha)) \\ | & & | \\ K & \xhookrightarrow{id} & K \end{array} \tag{2.1}$$

On applique le théorème de prolongement dans le cas particulier du schéma ci-dessus ; on a donc $P' = P$ et le nombre d'isomorphismes de $K(\alpha)$ dans $\overline{K}$.
Il suffit de voir quels sont ceux qui donnent les automorphismes de $K(\alpha)$; or, si σ est un tel K-isomorphisme, on rappelle que $\sigma(K(\alpha)) = K(\sigma(\alpha))$, où $\sigma(\alpha)$ est une racine de P dans $\overline{K}$, et on a donc $K(\alpha) = \sigma(K(\alpha))$ si et seulement si $\sigma(\alpha) \in K(\alpha)$ (en effet, si $\sigma(\alpha) \in K(\alpha)$, on a l'inclusion $K(\sigma(\alpha)) \subseteq K(\alpha)$ qui conduit à l'égalité car $[K(\alpha)/K] = [K(\sigma(\alpha))/K] = d(P)$, d'où $[K(\alpha)/K(\sigma(\alpha))] = 1$). □

Définition 2.3. *Soit L/K une extension de groupe de Galois G. Pour tout sous-groupe H de G on définit le sous-corps des invariant de L, ou sous-corps fixé, par H, noté par L^H ou bien $Inv_L(H)$, donné par : $Inv_L(H) = \{x \in L / \sigma(x) = x, \forall \sigma \in H\}$*

Lemme 2.4. *Soit L/K une extension de corps de groupe de Galois $Gal(L/K)$*

1. *Si $K_1 \subseteq K_2$, sont des sous-corps de $L \Longrightarrow Inv_L(Gal(L/K_2)) \subseteq Inv_L(Gal(L/K_2))$.*
2. *Si $H_1 \subseteq H_2$ sont de sous-groupes de $Gal(L/K) \Longrightarrow Inv_L(H_2) \subseteq Inv_L(H_1)$.*
3. *Si $H \subseteq Gal(L/K) \Longrightarrow H \subseteq Gal(L/Inv_L(H))$.*
4. *Pour $H \leq Gal(L/K)$, si $K = Inv_L(H) \Longrightarrow K = Inv_L(Gal(L/K))$.*
5. *Si $H = Gal(L/E)$, pour un sous-corps K de $L \Longrightarrow H = Gal(L/Inv_L(H))$.*

Démonstration. **Voir [Lemme 2.9, Field and Galois Theory, Patrik Morandi, Graduate Texts in Mathematics book series (GTM, volume 167)] page[29-30]** □

Exemple 2.5. — *Soit $K = \mathbb{Q}$ et $\overline{K} = \overline{\mathbb{Q}} \subset \mathbb{C}$, et soit $P(X) = X^2 + 1$. P irréductible dans $\mathbb{Q}[X]$, car $P(X+1) = X^2 + 2X + 2$ est d'Eisenstein en $p = 2$. Soit i une racine de P dans $\mathbb{C}$; alors l'autre racine est $-i$ qui est dans $\mathbb{Q}(i)$. Le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(i)$ est d'ordre 2 (l'automorphisme non triviale étant ici est la conjugaison complexe).*

— *Toujours dans le même cadre, considérons $P(X) = X^3 - 2$ et soit $\sqrt[3]{2}$ la racine réelle de P dans $\mathbb{C}$; comme P est irréductible sur $\mathbb{Q}$ (car d'Eisenstein en $p = 2$), les $\mathbb{Q}$-conjugués de $\sqrt[3]{2}$ sont $\sqrt[3]{2}$,$j\sqrt[3]{2}$,$j^2\sqrt[3]{2}$, où $j = \frac{-i+\sqrt{-3}}{2}$ est une racine primitive cubique de l'unité ; or $j\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$, sinon on aurait $j \in \mathbb{Q}(\sqrt[3]{2})$, ce qui est absurde car $\mathbb{Q}(\sqrt[3]{2}) \subset (R)$ tandis que $j \notin (R)$. Dans ce cas, le groupe des $\mathbb{Q}$-automorphismes est réduit Ã l'identité, bien que P ait trois racines distinctes.*

Noter cependant qu'il existe trois $\mathbb{Q}$-isomorphismes distincts de $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{C}$, ce qui fournit les trois corps distincts : $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$.

Lemme 2.6. — *(i) Soit L/K une extension galoisienne de groupe de Galois G, et soit $K' = L^G$; alors $K' = K$.*

— *(ii) si F/K est une sous-extension de L/K, alors L/F est une extension galoisienne et :*

$$Gal(L/F) = \{\sigma \in G,\, \sigma(x) = x \,pour\, tout\, x \in F\} \tag{2.2}$$

Démonstration. (i) On a $K \subseteq K$ puisque les éléments de G sont des K-automorphismes. Soit alors $\sigma \in G$; on constate que la restriction de σ à K' est l'identité (utiliser la définition de K'), donc tout élément de G est un K'-automorphisme de L, d'où $Gal(L/K) \subseteq Gal(L/K')$, ce qui conduit Ã $[L/K] \leq [L/K']$; d'où $K' = K$ d'après un raisonnement classique sur le degré lorsque $K \subseteq K' \subseteq L$ □

2.2 Corps fixes, lemme d'artin

2.2.1 Lemme d'Artin

Lemme 2.7. *(d'Artin)– Soit K un corps et soit H un groupe fini d'automorphismes de K ; alors l'extension K/K^H est une extension finie galoisienne et $Gal(K/K^H) = H$.*

Démonstration. (**Voir Georges Gras — Marie - Nicole Gras. Algèbre et arithmétique fondamentale. Page [318]**)

□

Le premier énoncé fondamentale est le suivant.

Théorème 2.8. *(Correspondance de Galois). Soit L/K une extension finie galoisienne et soit $G = Gal(L/K)$. Il existe une correspondance canonique bijective, entre l'ensemble des sous-extension F/K et L/K et les sous-groupes H de G ainsi définie :*

$$H \mapsto F := L^H$$

la correspondance inverse est donné (pour $K \subseteq F \subseteq L$) par :

$$F \mapsto H := Gal(L/F)$$

Démonstration. (**Voir Georges Gras — Marie - Nicole Gras. Algèbre et arithmétique fondamentale. Page [320]**) □

Exemple 2.9. *Prenons $K = \mathbb{Q}$ et pour L le corps des racine de $X^3 - 2$ dans $\mathbb{C}$. On a déjà construit $G = Gal(L/\mathbb{Q}) = \{id_K, \sigma, \tau\}$ avec :*

$$\sigma \begin{cases} \sqrt[3]{2} \mapsto j\sqrt[3]{2} \\ j \mapsto j \end{cases} \text{ et } \tau \begin{cases} \sqrt[3]{2} \mapsto j\sqrt[3]{2} \\ j \mapsto j \end{cases}$$

Il en résulte facilement que $G \simeq S_3 = D_6$, dont les sous-groupes sont les suivants dont les sous-groupes sont les suivant (outre les deux sous-groupes évidents) :

$$\{id, \tau\}, \{id, \sigma\tau\}, \left\{id, \sigma^2\tau\right\} \text{ d'ordre 2}, \left\{id, \sigma, \sigma^2\right\} \text{ d'ordre 3.}$$

Ceci conduit donc déjÃ Ã l'existence de quatre sous-corps distincts (autres que $\mathbb{Q}$ et L qui correspond aux sous-groupes G et $\{e\}$) :

1. *K_1, K_3, K_3 (correspondants aux trois sous-groupes d'ordre 2 et pour lesquels $[L/K_i] = 2$, donc $[K_i/\mathbb{Q}] = 3$),*
2. *K correspond au sous-groupe pour lequel on a $[L/K] = 3$ et $[K/\mathbb{Q}] = 2$*

Dans l'exemple précédent le diagramme des sous-corps de L peut s'établir alors sans difficulté ; cependant on voit que dans un cas plus compliqué il est utile de préciser les

inclusions ; or ceci résulte en fait de 2.8 qui contient le résultat plus précis suivant.

Corollaire 2.10. *Soit L/K une extension galoisienne finie de groupe de Galois G ; la correspondance de Galois*

$$F \mapsto Gal(L/F) \quad (K \subseteq F \subseteq L),$$

de l'ensemble des sous-extension L/K dans l'ensemble des sous-groupes de $Gal(L/K)$, a les propriétés de décroissance suivantes (pour l'inclusion)

1. $F_1 \subseteq F_2 \iff Gal(L/F_1) \supseteq Gal(L/F_2)$
2. $Gal(L/F_1F_2) = Gal(L/F_1) \cap Gal(L/F_2)$
3. $Gal(L/F_1 \cap F_2) = \langle Gal(L/F_1), Gal(L/F_2)\rangle$

Démonstration. On a

$$F_1 \subseteq F_2 \Longrightarrow Gal(L/F_1) \subseteq Gal(L/F_2)$$

(par définition de F_i-automorphisme, $i = 1, 2$), puis :

$$Gal(L/F_1) \subseteq Gal(L/F_2) \Longrightarrow L^{Gal(L/F_1)} \subseteq L^{Gal(L/F_2)}$$

(Par la définition 2.3), d'où $F_1 \subseteq F_2$. D'où le point 1. Le point 2. est également immédiat en vérifiant chaque inclusion. Pour le point 3., soit H un sous-groupe de G contenant $H_1 = Gal(L/F_1)$ et $H_2 = Gal(L/F_2)$, et soit F le corps fixe par H. On a donc (point précédents) $F \subseteq F_1$ et $F \subseteq F_2$; ainsi $F \subseteq F_1 \cap F_2$, d'où $Gal(L/F_1 \cap F_2) \subseteq H$. En passant Ã l'intersection sur les H (contenant H_1 et H_2), on obtient :

$$Gal(L/F_1 \cap F_2) \subseteq \bigcap_{H \supseteq H_1, H_2} H = \langle H_1, H_2\rangle \tag{2.3}$$

Réciproquement si $\sigma \in \langle H_1, H_2\rangle$, il est claire, en utilisant le théorème sur les sous-groupes engendrés par une partie, que σ laisse fixe les éléments de $F_1 \cap F_2$; on a donc $\langle H_1, H_2\rangle \subseteq Gal(L/F_1 \cap F_2)$, d'où l'égalité. □

Enfin, une fois le treillis des sous-extensions F/K de L/K établi, on peut se demander quelles extensions F/K sont galoisiennes ; on a Ã ce sujet le deuxième énoncés fondamental suivant :

Théorème 2.11. *Soit L/K une extension finie galoisienne de groupe de Galois G, soit F une sous-extension de L/K, et soit $H = Gal(L/F)$. Une condition nécessaire et suffisante*

pour que F/K soit galoisienne est que H soit normal dans G. Lorsque ceci a lieu, on a $Gal(F/K) \simeq G/H$, isomorphisme canonique qui résulte de la factorisation de l'homomorphisme de restriction

$$\begin{array}{ccc} G & \longrightarrow & Gal(F/K) \\ \sigma & \mapsto & \sigma_{|F} \end{array} \tag{2.4}$$

Dont le noyau est H.

Démonstration. (**Voir Georges Gras — Marie - Nicole Gras. Algèbre et arithmétique fondamentale. Page [323]**) □

Exemple 2.12. *Dans le treillis des sous extensions de $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, on obtient pour seule extension galoisienne (autre que $\mathbb{Q}/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$) celle qui correspond au seul sous-groupe normale (stricte et non trivial) de D_6, le groupe $\{id, \sigma, \sigma^2\}$:*

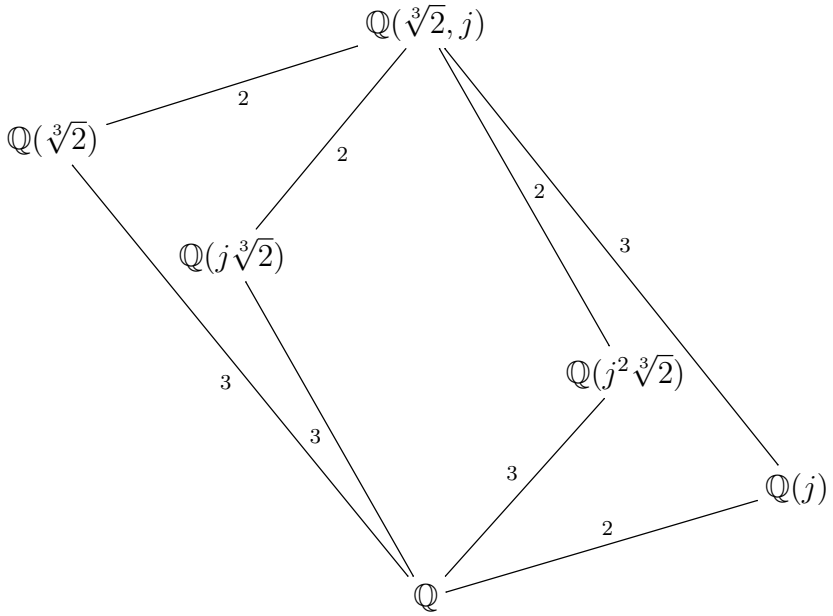


FIGURE 2.1 – Sous-extensions de $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$

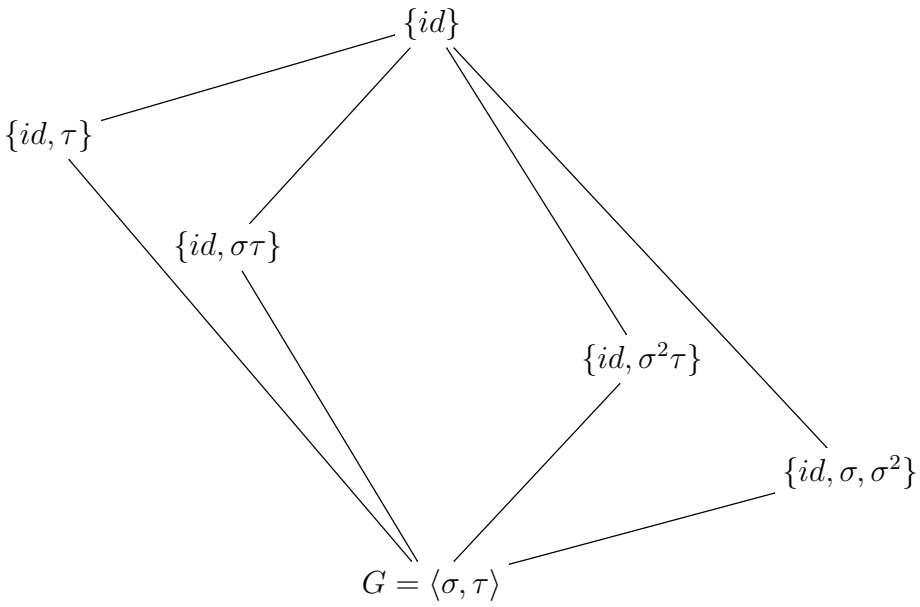


FIGURE 2.2 – Les sous-groupes de groupe de Galois de l'extensions $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$

Théorème 2.13. *Soit L/K et F/K deux sous-extensions, finies, galoisiennes, de $\overline{K}/K$. Posons successivement $G = Gal(LF/K)$, $H_F = Gal(LF/F)$ et $H_L = Gal(LF/L)$. Alors $F \cap L/K$ et galoisienne et on a*

$$Gal(L \cap F/K) \simeq G/H_L H_F \tag{2.5}$$

Démonstration. Puisque L/K et F/K sont galoisiennes, H_L et H_F sont des sous-groupes normaux de G. $\langle H_L, H_F \rangle = H_L H_F$ est normal dans G ; d'où le résultat par le 3. du corollaire 2.10. □

Théorème 2.14. *Soit K un corps, et soient L et L' deux sous-extensions d'une extension non nécessairement algébrique de K. On suppose que $L/L \cap L'$ est finie galoisienne.*
Alors l'extension LL'/L' est finie galoisienne, et l'application :

$$\begin{array}{ccc} Gal(LL'/L') & \longrightarrow & Gal(L/L \cap L') \\ \sigma & \mapsto & \sigma_{|L} \end{array} \tag{2.6}$$

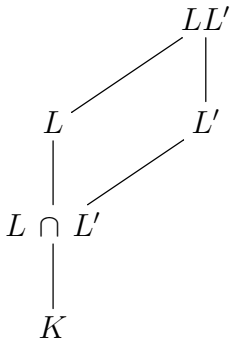
est isomorphisme canonique de groupes.

Démonstration. L'application écrite a un sens, car si σ est un L'-automorphisme de LL', par restriction à L, il laisse fixe $L \cap L'$. Si $\sigma_{|L}$ est l'identité, c'est que σ est l'identité sur L et

L', donc sur LL', d'où l'injectivité, L et L' sont linéairement disjointes sur $L \cap L'$, d'où :

$$[LL'/L'] = [LL/L \cap L']$$

ainsi le fait que l'application étudiée soit injective suffit Ã prouver qu'elle est surjective.
Ce qui précède donne lieu au schéma suivant :



(2.7)

dans lequel on a $Gal(LL'/L') \simeq Gal(L/L \cap L')$ par restriction. □

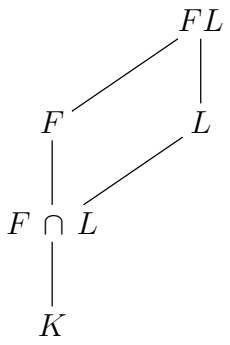
Théorème 2.15. *Soient F et L des sous-extensions de $\overline{K}/K$, galoisienne sur $F \cap L$. L'application canonique :*

$$\begin{array}{ccc} Gal(FL/F \cap L) & \longrightarrow & Gal(F/F \cap L) \times Gal(L/F \cap L) \\ \sigma & \mapsto & (\sigma_{|F}\,,\, \sigma_{|L}) \end{array} \tag{2.8}$$

est un isomorphisme canonique de groupe.

Démonstration. On sait que $FL/F \cap L$ est galoisienne ; comme les extensions $F/F \cap L$ et $L/F \cap L$ sont linéairement disjointes, on a $[FL/F \cap L] = [F/F \cap L]\,[L/F \cap L]$ et il suffit de montrer l'injectivité.
Le schéma est alors le suivant, les branches parallèles correspondant Ã des groupes de Galois isomorphes (c'est le théorème 2.14 appliqué deux fois), et où le groupe $Gal(FL/F \cap L)$ peut

aussi s'écrire $Gal(FL/F) \times Gal(FL/L)$:



Attention $F \cap L/K$ n'est pas nécessairement galoisienne car les hypothèses sont plus faibles qu'en théorème 2.13. □

2.3 Groupe de Galois des polynômes

2.3.1 Norme et trace

Soit L/K une extension de degré fini $n = [L/K]$, pour tout λ dans L on définit l'application noté M_λ définie par

$$\begin{aligned} M_\lambda : L &\to L \\ x &\mapsto \lambda x \end{aligned}$$

M_λ définie ainsi un endomorphisme d'espace vectoriel L, on l'appelle endomorphisme multiplication par λ.

Définition 2.16. *On appelle trace, respectivement norme, d'un élément λ de L, noté $Tr_{L/K}(\lambda)$, respectivement $N_{L/K}(\lambda)$, la trace et le déterminant de l'endomorphisme M_λ. On écrit alors*

$$Tr_{L/K}(\lambda) = Tr(M_\lambda) \text{ et } N_{L/K}(\lambda) = Det(M_\lambda).$$

Exemple 2.17. *Soit l'extension L/K, où $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt[3]{2})$, on veut déterminer la trace et la norme de l'élément $\lambda = \sqrt[3]{2}$. on sait que la famille $\left\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\right\} = \mathbf{F}$, forme une base de L comme K-espace vectoriel, alors l'image de chacun des éléments de cette base par endomorphisme multiplication par λ est*

$$M_\lambda(1) = \lambda 1 = \sqrt[3]{2}\,, M_\lambda(\sqrt[3]{2}) = \lambda\sqrt[3]{2} = \sqrt[3]{2^2}\,, M_\lambda(\sqrt[3]{2^2}) = \lambda\sqrt[3]{2^2} = 2$$

Ainsi la matrice associée a l'endomorphisme M_λ relativement a la base $\mathbf{F}$ *est*

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Ce qui donne

$$Tr_{L/K}(\lambda) = 0 \text{ et } N_{L/K}(\lambda) = 2$$

Lemme 2.18. *L/K est une extension finie de degré n, alors*

- *Soit x et y dans L, alors $Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y)$ et $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.*
- *si $a \in K$, alors $Tr_{L/K}(a) = na$ et $N_{L/K}(a) = a^n$ sont dans K.*

Proposition 2.19. *L/K est une extension finie de degré n, pour α dans L notons*

$$p(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 \in K[X].$$

Son polynôme minimal, alors $N_{L/K}(\alpha) = (-1)^n a_0^{nm}$ et $Tr_{L/K}(\alpha) = -\frac{n}{m}a_{m-1}$.

Démonstration. Par hypothèse $[K(\alpha)/K] = m$, $K[\alpha] \subseteq L$ donc m divise $n = [L/K]$.
On considère l'endomorphisme M_α, on note $g(X)$ le polynôme caractéristique de M_α, soit

$$g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0 \in K[X]$$

$g(X)$ et $p(X)$, on le même facteur irréductible donc $g(X)$ est une puissance du polynôme minimal de α, ce qui donne

$$g(X) = (p(X))^{nm}.$$

Comme $N_{L/K}(\alpha) = Det(M_\alpha) = (-1)^n b_0$ et $Tr_{L/K}(\alpha) = -b_{n-1}$, on retient que $g(X) = (p(X))^{n/m}$, on aura

$$b_0 = a_0^{nm} \text{ et } b_{n-1} = \frac{n}{m}a_{m-1}$$

. □

Corollaire 2.20. *L/K est une extension finie de degré n, pour α dans L notons par σ_i; $1 \leq$*

$i \leq r$, les r K-homomorphisme de $K(\alpha)$ dans une clôture algébrique de K, alors

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)^{n/r} \text{ et } Tr_{L/K}(\alpha) = \frac{n}{r}\left(\sum_{i=1}^{r} \sigma_i(\alpha)\right).$$

Démonstration. Soit Ω une clôture algébrique de K, alors le polynôme minimal de tout α dans L est

$$p(X) = \prod_{i=1}^{r}(X - \sigma_i(\alpha)) \in K[X].$$

où les $\sigma_i(\alpha)$ dans Ω, on sait que le polynôme caractéristique

$$g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0 \in K[X]$$

de l'endomorphisme M_α est lié au polynôme minimal $p(X)$ par la relation $g(X) = (p(X))^{n/r}$. D'autre parte

$$N_{L/K}(\alpha) = (-1)^n b_0 \text{ et } Tr_{L/K}(\alpha) = -b_{n-1}.$$

Avec

$$b_0 = \prod_{i=1}^{r} \sigma_i(\alpha) \text{ et } b_{n-1} = \frac{n}{r}\left(\sum_{i=1}^{r} \sigma_i(\alpha)\right).$$

□

Corollaire 2.21. *Soit L/K une extension galoisienne de groupe de Galois $G = Gal(L/K)$, alors pour tout $\alpha \in L$ on a*

$$N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \text{ et } Tr_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

2.3.2 Discriminant

Définition 2.22. *Soit L/K une extension finie de corps séparable de degré n, on appelle discriminant d'une famille finie $(\alpha_i)_{1 \leq i \leq n}$, d'élément de L.*
L'élément de L noté $D_{L/K}(\alpha_1, \ldots, \alpha_n) = (Det(\sigma_i(\alpha_j)))^2, 1 \leq j \leq n$, où les σ_i sont les n plongement de L dans une clôture algébrique de K.

Remarque 2.23.

$$D_{L/K}(\alpha_1, \ldots, \alpha_n) = (Det(Tr_{L/K}\alpha_i\alpha_j) \text{ et } D_{L/K}(\alpha_1, \ldots, \alpha_n) \in K.$$

Proposition 2.24. *Soit L/K une extension finie de corps séparable de degré n, si $L = K(\alpha)$,*

alors

$$D_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) = (-1)^{n(n-1)/2}\prod_{j\neq i}(\sigma_i(\alpha)-\sigma_j(\alpha)) = (-1)^{n(n-1)/2}N_{L/K}(p'(\alpha)).$$

où les σ_i : $1 \leq i \leq n$, *sont les* n *plongements de* L *dans une clôture algébrique* Ω *et* p' *le polynôme dérivé du polynôme minimal* p *de* α.

Démonstration. On a bien

$$D_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) = (Det(\sigma_i(\alpha^j)))^2.$$

D'autre part $\sigma_i(\alpha^j) = \sigma_i(\alpha)^j$ et que la matrice $(\sigma_i(\alpha)^j)$ est une matrice de "Vandermonde" de n-uplet $\sigma_1(\alpha),\ldots,\sigma_n(\alpha)$ dont le déterminant est $\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))$ de qui donne

$$D_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) = \left(\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))\right)^2.$$

Chaque différence $\sigma_i(\alpha)-\sigma_j(\alpha)$ est associée a un couple $(\sigma_i(\alpha),\sigma_j(\alpha))$; donc on trouve $n(n-1)/2$ de ces différences dans le produit $\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))$ et donc $n(n-1)$ de ces différences dans

$$\left(\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))\right)^2$$

, on trouve le même résultat dans $\prod_{i\neq j}(\sigma_i(\alpha)-\sigma_j(\alpha))$; ainsi, on a bien

$$D_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) = \left(\prod_{i\neq j}(\sigma_i(\alpha)-\sigma_j(\alpha))\right).$$

D'autre part, on a $p = \prod_{i=1} n(X-\sigma_i(\alpha))$, alors le polynôme dérivé p' s'écrit

$$p'(X) = \sum_{j=1}^{n}\prod_{i\neq j}(X-\sigma_i(\alpha)).$$

Ce qui entraine $\forall i$, $1 \leq i \leq n$, on a

$$\sigma_i(p'(\alpha)) = p'(\sigma_j(\alpha)) = \prod_{i\neq j}(\sigma_i(\alpha)-\sigma_j(\alpha)).$$

Donc $p'(\alpha)$ s'écrit comme suite

$$N_{L/K}(p'(\alpha)) = \prod_{i=1}^{n} \sigma_i(p'(\alpha)) = \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

On en déduit alors

$$D_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(p'(\alpha)).$$

□

Définition 2.25. *Soit K un corps de caractéristique différente de 2, $p(x) \in K[X]$ un polynôme de degré n, ayant n racines distinctes $(\alpha_i)_{1 \leq i \leq n}$ dans une clôture algébrique Ω de K. On appelle discriminant de p, l'élément noté D_p de Ω défini par*

$$D_p = \left(\prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j) \right)^2$$

On note $D_p = \Delta^2$, où $\Delta = \left(\prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j) \right)$.

Remarque 2.26. *Le discriminant D_p du polynôme p est un élément de K.*

Exemple 2.27. *Soit K un corps, avec car $K \neq \{2, 3\}$, soit $\chi(X) = X^3 + pX + q \in K[X]$ un polynôme irréductible sur K, on note α une racine de $\chi(X)$ et soit $L = K(\alpha)$, donc le discriminant de χ est*

$$D_\chi = -N_{L/K}(\chi'(\alpha))$$

avec $\chi'(\alpha) = 3\alpha^2 + p$ et tel que $\alpha^3 + p\alpha + q = 0$.
On sait que $N_{L/K}(\chi'(\alpha))$ est le déterminant de la matrice de l'endomorphisme $M_{\chi'(\alpha)}$, multiplication par $\chi'(\alpha)$, de L dans la base est $\{1, \alpha, \alpha^2\}$ du K espace vectoriel L on a donc

$$M_{\chi'(\alpha)}(1) = p + 3\alpha^2,\ M_{\chi'(\alpha)}(\alpha) = -3q - 2p\alpha,\ M_{\chi'(\alpha)}(\alpha^2) = 3\alpha - 2p\alpha^2.$$

D'où la matrice suivante

$$\begin{pmatrix} p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & -2p \end{pmatrix}$$

dont le déterminant est $4p^3 + 27q^2$, on en déduit que $D_\chi = -(4p^3 + 27q^2)$

2.3.3 Cas particuliers

Polynôme de degré 3

Transformation $(X^3 + pX + q)$: Soit K un corps de caractéristique différent de 2 et 3, $a, b, c \in K$, on cherche a ramené le polynôme $t(X) = X^3 + aX^2 + bX + c \in K[X]$ a un polynôme de la forme $t_1(Y) = Y^3 + pY + q$; $p, q \in K$ et $t_1(Y) \in K[Y]$.
Pour cela, on pose $X = Y + h$, alors on a

$$t(X) = t(Y + h) = Y^3 + 3Yh(Y + h) + h^3 + a(Y^2 + 2Yh + h^2) + b(Y + h) + c.$$

Donc on aura

$$t(X) = Y^3 + (a + 3h)Y^2 + (3h^2 + 2ah + b)Y + (h^3 + ah^2 + bh + c).$$

Par suite, posons $h = -a/3$, on obtient donc $t(X) = t_1(Y) = Y^3 + pY + q$.
Or d'après l'exemple 2.27, le $D_{t_1} = -(4p^3 + 27q^2)$, de plus on a $D_t = D_{t_1} = -(4p^3 + 27q^2)$.
Formule générale : Soit $p, q, r \in K$, posons $p(X) = X^3 + pX^2 + qX + r \in K[X]$,alors

$$D_p = 18pqr - 4p^3r + p^2q^2 - 4r^3 - 27q^2.$$

Polynôme de degré 4

Transformation (méthode de Ferrari) : Soit K un corps de caractéristique différent de 2 et 3, $a_1, a_2, a_3, a_4 \in K$, $g(X) = X^4 - a_1X^3 + a_2X^2 - a_3X + a_4$.
On pose $Y = X - \frac{s_1}{4}$, (transformation de Tschirnhaus), $g(X)$ devient $f(Y) = Y^4 + pY^2 + qY + r$, $p, q, r \in K$.
La méthode consiste a mettre f sous la forme : $f(Y) = (Y^2 + uY + v)(Y^2 + u'Y + v')$, on suppose que $q \neq 0$ (car sinon on aura une équation bicarré).
Par suite l'identification nous donne le système :

$$\begin{cases} u + u' = 0 \\ uu' + v + v' = p \\ uv' + u'v = q \\ vv' = r \end{cases} \iff \begin{cases} u' = u \\ v + v' = p + u^2 \\ v + v' = \dfrac{q}{u} \\ vv' = r \end{cases}$$

Donc, on en déduit que

$$\begin{cases} v &= (\frac{1}{2u})\,(u(p+u^2)-q) \\ v' &= (\frac{1}{2u})\,(u(p+u^2)+q)\,. \end{cases}$$

Par suite $vv' = r$ donne

$$u^2(u^2+p)^2 - q^2 = 4ru^2.$$

On pose $z = u^2 + p$, on en déduit que z est racine de l'équation du troisième degré

$$Z^3 - pZ^2 - 4rZ + 4rp - q^2. \tag{2.9}$$

L'équation (2.9) est dite cubique résolvante de l'équation

$$Y^4 + pY^2 + qY + r = 0. \tag{2.10}$$

la résolution de (2.9) donne z et donc u et par suite v et v'.
L'équation (2.10) est donc ramenée Ã la résolution du système suivant

$$\begin{cases} (E_1)\; Y^2 + uY + v &= 0 \\ (E_2)\; Y^2 + u'Y + v' &= 0 \end{cases} \longmapsto \begin{cases} D_{(E_1)} &= u^2 - 4v \\ D_{(E_2)} &= u'^2 - 4v'. \end{cases}$$

Formules connues : Soit $p, q, r, t \in K$, on pose $p(X) = X^4 + pX + q$ et $f(X) = X^4 + rX^2 + t$, alors

$$\begin{aligned} D_p &= -27p^4 + 256q^3 \\ D_f &= 16t(r^2 - 4t)^2 \end{aligned}$$

Polynôme de degré n $(\mathbf{X^n + pX + q})$:

Soit $p(X) = X^n + aX + b$, $a, b \in K$, soit $\alpha := \alpha_1, \alpha_2, \ldots, \alpha_n$ ses n racines distinctes dans une clôture algébrique de K, on note que

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i)$$

Posons $p(\alpha_i) = \alpha_i^n + a\alpha_i + b$, on a $p(\alpha_i) = 0,\ \forall 1 \leq i \leq n$, donc

$$\alpha_i^n + a\alpha_i + b = 0 \iff \alpha_i^n = -a\alpha_i - b$$

Donc si p' désigne le polynôme dérivé de p alors on a,

$$p'(\alpha_i) = n\alpha_i^{n-1} + a = n(\frac{\alpha_i^n}{\alpha_i}) + a = \frac{n(-a\alpha_i - b) + a\alpha_i}{\alpha_i} = \frac{(1-n)a\alpha_i - nb}{\alpha_i}.$$

Soit

$$N(p'(\alpha_i)) = \prod_{i=1}^{n} p'(\alpha_i) = \prod_{i=1}^{n} \frac{(1-n)a\alpha_i - nb}{\alpha_i} = \frac{\prod_{i=1}^{n}(1-n)a\alpha_i - nb}{\prod_{i=1}^{n}\alpha_i}. \tag{2.11}$$

Pour venir about de ce calcul on considère l'égalité suivante

$$(1-n)a\alpha_i - nb = a(1-n)\alpha_i - nb = -a(1-n)(\frac{nb}{a(1-n)} - \alpha_i)$$

on pose alors $q = \dfrac{nb}{a(1-n)}$ et on remplace dans l'équation 2.11, on a donc

$$\frac{\prod_{i=1}^{n}(1-n)a\alpha_i - nb}{\prod_{i=1}^{n}\alpha_i} = \frac{(-1)^n a^n (1-n)^n \prod_{i=1}^{n}(q-\alpha_i)}{\prod_{i=1}^{n}\alpha_i} = \frac{(-1)^n a^n (1-n)^n p(q)}{(-1)^n b} = \frac{a^n(1-n)^n p(q)}{b}.$$

On pose $t = \dfrac{a^n(1-n)^n}{b}$ donc on a bien

$$N(p'(\alpha_i)) = tf(q)$$

.

Sachant que $D_p = (-1)^{\frac{n(n+1)}{2}} N(p'(\alpha_i))$ donc le discriminant de p est donné par

$$(-1)^{\frac{n(n+1)}{2}} (tf(q)), \ avec\, t = \frac{a^n(1-n)^n}{b}, \ et\ q = \frac{nb}{a(1-n)}$$

Exemple 2.28. *Soit $p(X) = X^5 + 5X + 1 \in \mathbb{Q}[X]$, le discriminant de p d'après le résultat précédent est donné par*

$$D_p = (-1)^{\frac{5(5+1)}{2}}(\frac{5^5(1-5)^5}{1})p(\frac{5}{5(1-5)}) = 5^5 + 5^6(-4)^4 - 5^5(4)^5 = 800005.$$

2.3.4 Groupe de Galois d'un polynôme

Définition 2.29. *Pour Tout polynôme $P(X) \in K[X]$, séparable sur K, et de corps de décomposition L sur K, le groupe de Galois du polynôme P, noté $Gal(P/K)$ est le groupe de Galois $G = Gal(L/K)$ de l'extension galoisienne L/K.*

Notons que si $P(X) \in K[X]$ un polynôme irréductible sur K de degré n de groupe de Galois G, alors pour tout $\sigma \in G$, et pour tout racine α de $P(X)$, l'élément $\sigma(\alpha)$ est aussi racine de $P(X)$, En d'autre terme, si on a α,β deux racines de $P(X)$, $\exists\sigma \in G$ tel $\sigma(\alpha) = \beta$. On dira que σ agit sur les racines du polynôme $P(X)$ par permutation de celles-ci et cette action est dite transitive.

Définition 2.30. *On dit qu'un sous-groupe de G de permutation du groupe S_n est transitif si,*

$$\forall i \neq j;\ 1 \leq i, j \leq n, \exists\sigma \in G;\ \sigma(i) = j.$$

Théorème 2.31. *Soit $p(X) \in K[X]$ un polynôme de degré n et de groupe de Galois G alors*

1. *G peut être identifié à sous-groupes du groupe symétrique S_n.*
2. *Si $p(X)$ irréductible, alors $n \mid |G|$ et G est isomorphe à un sous-groupe transitif de S_n.*

Démonstration. Notons par $\alpha := \alpha_1, \ldots, \alpha_n$ les différentes racines de $p(X)$ dans un corps de décomposition L de celui-ci, $deg\, p \geq n \geq 1$.

1. Tout $\sigma \in G$ induit une permutation de l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$ des racines de $p(X)$, ce qui définit un homomorphisme $\Phi : G \to S_n$ qui est injectif, ainsi donc $G \simeq Im\Phi$ sous-groupes de S_n.
2. Si $p(X)$ est irréductible, alors pour toute raine α de $p(X)$, dans une clôture algébrique de K, $[K(\alpha)/K] = n = deg\, p.$ d'autre part $K(\alpha) \subseteq L$; où L est corps de décomposition de $p(X)$, on en déduit que $n \mid |G| = [L/K]$.
   De plus $\forall i, j\ , 1 \leq i, j \leq n\ (i \neq j)$, il existe un K-isomorphisme $\sigma : K(\alpha_i) \to K(\alpha_j)$, donné par $\sigma(\alpha_i) = \alpha_j$, qui se prolonge en un K-automorphisme de L, ce qui montre que G est transitif, $G \simeq S_n$.

□

Exemple 2.32. *Soit K un corps de caractéristique différente de 2 et soit $f(X) \in K[X]$ un polynôme irréductible de degré 2, on pose $K(\alpha) = L$ avec α une racine de $f(X)$ dans une clôture de K, soit alors le groupe de Galois $G = Gal(L/K)$, $f(X)$ est séparable car la car $K \neq 2$, si les racines de $f(X)$ sont dans K alors il est évident que $L = K$, ce qui montre que $G = id_K$, sinon si les racines de $f(X)$ ne sont pas dans K, alors $|G| = 2 = |S_2|$ et donc $G \simeq S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.*

Chapitre 3

GROUPES DE GALOIS DES EXTENSIONS CUBIQUES ET QUARTIQUES

Dans ce chapitre nous allons décrire une procédure afin de déterminer les groupes de Galois des polynômes irréductibles, séparables de degré 3 et 4 sur des corps de caractéristique différente de 2, cela dit nous allons pas expliciter les formules classique des racines de ces polynômes

Dans tout ce qui suit K désigne un corps commutatif de caractéristique différente de 2.

3.1 Groupes de Galois des extensions cubiques

On a vu dans l'exemple 2.32 que le groupe de Galois sur un corps K d'un polynôme de degré 2 et soit il est égale a l'identité, soit il est isomorphe au groupe de permutation $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Dans cette section nous allons nous intéresser particulièrement aux groupes de Galois des polynômes de degré 3, pour cela, rappelons que dans le corps K que on a supposer de caractéristique différente de 2, un polynôme unitaire de degré 3 s'écrit nécessairement sous la forme $X^3 + aX^2 + bX + c$, où les coefficients a, b, c sont dans K, cependant on a vu dans le chapitre II que on peut toujours ramener la forme précédente a un polynôme de la forme $X^3 + pX + q$, avec p, q, dans K, maintenant si on pose $p(X) = X^3 + pX + q$, avec $p(X)$ un polynôme dans $K[X]$, alors son discriminant comme on la vu au chapitre II est donné par la formule explicite suivante : $D_p = -(4p^3 + 27q^2)$, dans la suite on s'intéresseras d'une manière particulière aux résultats obtenus après le calcul de ce discriminant et finalement on va déterminé d'une manière précise le groupe de Galois associé, pour débuter considérons le théorème suivant :

Théorème 3.1. *Soit Soit $f(X) \in K[X]$ un polynôme irréductible et séparable de degré n. Le groupe de Galois de $G(f/K)$ est un sous groupe de $A_n \iff D_f$ est un carré dans K.*

Démonstration. Soit $\Delta = \prod_{i<j}(\alpha_j - \alpha_i) \neq 0,\ 1 \leq i, j \leq n$, donc $\Delta \in K(\alpha_1, \ldots, \alpha_n)$ et $\Delta^2 = D_f \in K$. par suite le discriminant de f est dans K si et seulement si $\Delta \in K$.
Pour $\sigma \in Gal(K(\alpha_1, \ldots, \alpha_n) : K)$, soit $\epsilon_\sigma = \pm 1$ la signature de σ, de plus σ est identifié soit a une permutation paire soit a une permutation impaire, on pose alors

$$\sigma(\Delta) = \prod_{i<j}(\sigma(\alpha_j) - \sigma(\alpha_i)) = \epsilon_\sigma \prod_{i<j}(\alpha_j - \alpha_i) = \epsilon_\sigma \Delta,$$

alors $\sigma(\Delta) = \pm\Delta$, puisque $\Delta \neq 0$, alors $\Delta \neq -\Delta$, on a donc$\sigma \in A_n \iff \epsilon_\sigma = 1$, alors $\sigma \in A_n \iff \sigma(\Delta) = \Delta$, on en déduit que $G(f/K) \simeq A_n \iff \Delta \in K$ □

Corollaire 3.2. *Soit $f(X) \in K[X]$ un polynôme irréductible et séparable de degré 3.*
Si $D_f = \delta^2$, $\delta \in K$, (i.e. D_f est un carré dans K), alors le groupe de Galois de $f(X)$ sur K, $G(f/K) \simeq A_3$, sinon si D_f n'est pas un carré dans K, (i.e. $\nexists \delta \in K$, tel que $D_f = \delta^2$), alors $G(f/K) \simeq S_3$.

Démonstration. D'après le théorème 2.31, comme $f(X)$ est irréductible alors $G(f/K)$ est isomorphes a un sous-groupe transitif de S_3, on sait que les deux seules groupes transitifs de S_3, Sont le groupe alterné A_3 et le groupe symétrique S_3, et d'après le théorème 3.1, $G(f/K) \simeq A_3 \iff D_f$ est un carré, sinon on aura $G(f/K) \simeq S_3$ □

Exemple 3.3. *Dans le tableau suivant, nous allons lister les discriminants et les groupes de Galois $G(f/\mathbb{Q})$ sur $\mathbb{Q}$ des polynômes de degrés 3 irréductibles de la forme $f_a(x) = X^3 - aX - 1, a \in \mathbb{Z}$, pour $1 \leq a \leq 6$. Nous sautons le cas pour $a = 2$ car $f_2(X)$ n'est pas irréductible sur $\mathbb{Q}$ (en effet ± 1 est racine $X^3 - 2X - 1$). Pour le cas $a = 3$ (i.e. la seconde ligne du tableau) on voit bien que $D_{f_3} = 81 = 9^2$, un carré dans $\mathbb{Q}$ alors son groupe de Galois est isomorphe à A_3 (i,e, $G(f_3/\mathbb{Q}) \simeq A_3$). Pour les autre exemple, on a $D_{f_a} \neq \delta^2$ dans $\mathbb{Q}$ donc leur groupes de Galois sont isomorphes à S_3 (i,e, $G(f_a/\mathbb{Q}) \simeq S_3$)*

l'irréductibilité de f_a. On sait bien que un polynôme est irréductible sur un corps K (qui dans notre cas $K = \mathbb{Q}$) s'il n'admet pas de racine dans K. Or si $\alpha \in \mathbb{Q}$ est racine de f_a alors $\alpha^3 - a\alpha - 1 = 0$ ce qui implique que $\alpha(\alpha^2 - a) = 1$, et donc $\alpha \mid 1$, ce qui veut dire que $\alpha = \pm 1$ et par conséquent $\alpha^2 - a = \pm 1$ et donc on a bien $a = 0$ ou bien $a = 2$. ainsi $\forall a \in \mathbb{Z}$, avec $a \neq 0, a \neq 2 \implies f_a$ irréductible sur $\mathbb{Q}$ □

$f_a(X)$	D_{f_a}	$G(f_a/\mathbb{Q})$
$X^3 - X - 1$	-23	S_3
$X^3 - 3X - 1$	81	A_3
$X^3 - 4X - 1$	229	S_3
$X^3 - 5X - 1$	473	S_3
$X^3 - 6X - 1$	837	S_3
$X^3 - 7X - 1$	1345	S_3
$X^3 - 8X - 1$	1940	S_3
$X^3 - 9X - 1$	2889	S_3

TABLE 3.1 – Quelques groupes de Galois sur $\mathbb{Q}$

Il s'avère que pour un $a \in \mathbb{Z} - \{0, 2\}$, le groupe de Galois $G(f_a/\mathbb{Q}) \simeq A_3 \iff a = 3$, chose qui est étroitement lié au dernier théorème de Fermat pour l'exposent 3. Une telle connexion n'est pas du tout évidente !, d'après le corollaire 3.2 le groupe de Galois $G(f_a/\mathbb{Q}) \simeq A_3 \iff D_{f_a}$ est un carré avec $D_{f_a} = -(4(-a)^3 + 27)$, puisque D_{f_a} est un entier et c'est un carré dans $\mathbb{Q} \iff$ c'est un carré dans $\mathbb{Z}$, nous voulons dans trouver toutes solutions intégrales de l'équation $y^2 = 4x^3 - 27$, cette équation admet pour solution $\{(3, 9), (3, -9)\}$, on travaillant avec des nombres rationnelles, pas seulement des entiers et sous le changement non évident

des variables $r = \dfrac{9-y}{6x}$ *et* $s = \dfrac{9+y}{6x}$, *leurs inverses respectifs sont donnés par* $x = \dfrac{3}{r+s}$ *et* $y = \dfrac{-9(r-s)}{r+s}$, *la condition* $y^2 = 4x^3 - 27 \iff r^3 + s^3 = 1$, *alors l'équation* $y^2 = 4x^3 - 27$ *admet une solution rationnelle (avec* $y \neq \pm 9$*) si et seulement si l'équation* $r^3 + s^3 = 1$ *admet une solution rationnelle avec* $r \neq 0$ *et* $s \neq 0$. *Alors que* $r^3 + s^3 = 1$ *n'admet pas de solution* (r, s) *non trivial. Et c'est le résultat du dernier théorème de Fermat.*

Remarque 3.4. *Si* $G(f/\mathbb{Q}) \simeq A_3$, *alors toutes ses racines génèrent la même extension de* $\mathbb{Q}$, *et toutes ses racines sont réelles puisque au moins une racine est réelle. Cependant cela ne veut dire que si un polynôme cubique (unitaire et irréductible sur* $\mathbb{Q}$*) admet que des racines réelles que son groupe de Galois est* A_3, *si on prend par exemple le polynôme* $X^3 - 4X - 1$. *On sait que il admet que des racines réelles mais on a bien vu que son groupe de Galois est isomorphe à* S_3*(i.e.* $G(X^3 - 4X - 1/\mathbb{Q}) \simeq S_3$*). Les racines de* $X^3 - 4X - 1$ *génèrent des corps différents l'un de l'autre qui sont contenus dans* $\mathbb{R}$.

Remarque 3.5. *Si la caractéristique du corps* K *vaut* 3, *alors il faut s'assuré que le polynôme est bien séparable, le cas ou la caractéristique est différente de* 3, *alors tout polynôme de degré* 3 *est nécessairement séparable.*

Corollaire 3.6. *Soit* $a = k^2 + k + 7$, $k \in \mathbb{Z}$ *et soit* $p(X) = X^3 - aX + a$, *alors*

1. $p(X)$ *est irréductible sur* $\mathbb{Q}$.
2. $G(p/\mathbb{Q}) \simeq A_3$.

1. On sait que $\forall k \in \mathbb{Z}$, $a \in \mathbb{Z}$ est toujours impaire, donc

$$p(X) \equiv X^3 + X + 1 \mod 2,$$

un polynôme qui est irréductible sur $\mathbb{F}_2$, donc forcément irréductible sur $\mathbb{Q}$.

(a) On a par les résultats 2.27, $D_p = -4(-a)^3 - 27a^2 = a^2(4a - 27)$. et comme $a = k^2 + k + 7$ on aura donc

$$D_p = (k^2 + k + 7)^2(4(k^2 + k + 7) - 27) = (k^2 + k + 7)^2(4k^2 + 4k + 1)$$

$$= (k^2 + k + 7)^2(2k + 1)^2 = ((k^2 + k + 7)(2k + 1))^2$$

ce qui veut dire que D_p est un carré dans $\mathbb{Q}$, et par 3.2 nous aurons $G(p/\mathbb{Q}) \simeq A_3$.

Théorème 3.7. *Soit $f(X) \in K[X]$ un polynôme séparable de degré 3 et soit $\Delta = D_f$, si α est une racine de de $f(X)$, alors le corps de décomposition de $f(X)$ sur K est $Dec_K(f(X)) = K(\alpha, \sqrt{\Delta})$, en particulier, si $f(X)$ est réductible alors $Dec_K(f(X)) = K(\sqrt{\Delta})$*

Démonstration. Posons $f(X) \in K[X]$ un polynôme unitaire et séparable de degré 3, soit $\alpha_1, \alpha_2, \alpha_3$ les racines de $f(X)$ dans une extension de K, on pose alors $f(X) = (X - \alpha_1)g(X)$, donc α_2 et α_3 sont des racines de $g(X)$, en particulier $g(\alpha_1) \neq 0$, nécessairement $g(X)$ est un polynôme de degré 2 sur $K(\alpha_1)[X]$. On peut alors écrire l'égalité suivante

$$K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1)(\alpha_2, \alpha_3) = K(\alpha_1)(\sqrt{D_g}).$$

Puisque $f(X)$ est unitaire et divisible par $g(X)$ sur $K(\alpha_1, \alpha_2, \alpha_3)$;
Alors

$$D_f = g(\alpha_1)^2 D_g$$

et donc $K(\alpha_1, \sqrt{D_g}) = K(\alpha_1, \sqrt{D_f}) = K(\alpha_1, \sqrt{\Delta})$.
Si $f(X)$ est réductible, en choisissant $\alpha_1 \in K$ racine de $f(X)$. Alors $K(\alpha_1, \sqrt{D_g}) = K(\Delta)$
Il important que le corps de base K ne serait pas de caractéristique 2. La preuve qu'on a utilisé l'impose, car nous avons utilisé la forme quadratique qui ne fonctionne pas en caractéristique 2.
Alors une question se pose, 3.7 peut il être prouver avec différents arguments en $carK = 2$? ;
La réponse est non ; en en effet, le théorème telle qu'il est écrit, il est faux dans le cas où $carK = 2$. Si nous prenons le contre exemple suivant : $K = F(u)$ avec $carF = 2$ et u un nombre transcendant sur F, et le polynôme $f(X) = X^3 + uX + u$ qui est irréductible dans $K[X]$ avec $D_f = u^2$, alors $K(\alpha_1, \sqrt{\Delta})) = K(\alpha_1, \sqrt{D_f}) = K(\alpha_1, u) = K(\alpha_1)$. On peut montrer que le degré du corps de décomposition de $f(X)$ sur K est égale à 6 et non 3, et par conséquent $K(\alpha_1, \sqrt{\Delta})$ n'est pas le corps de décomposition de $f(X)$ sur K.
Preuve que le corps de décomposition de $f(X)$ est de degré 6 sur K. En effet comme α_1 est racine du $f(X)$ alors $f(X)$ s'écrit de la manière suivante

$$f(X) = (X - \alpha_1)g(X) \,\text{dans}\, K(\alpha_1, \sqrt{D_g}),$$

et donc on a D_g divise D_f et donc u^2 dans $K = F(u)$, alors $\exists \delta \in K$ tel que $\delta D_g = u^2$, et $\delta > 1$, et comme $D_g \in K$ alors il s'écrit de la manière unique $D_g = a + bu + cu^2$ et comme $D_g < D_f = u^2$ alors $D_g = a + bu$ et posons $\delta = a' + b'u$ ainsi calculons $\delta D_g = aa' + (ab' + a'b)u + bb'u^2$

nous trouverons que $\delta = u$ et $D_g = u$, par suite, on aura

$$f(X) \in K(\alpha_1, \sqrt{D_g}) = K(\alpha_1, \sqrt{u}) = Dec_K(f)$$

mais on sait que $\sqrt{u} \notin K$ et $u \in K$ alors $[K(\sqrt{u})/K] = 2)$, et d'un autre côté on a $[K(\alpha_1)/K] = 3$ et nous savons aussi que $\sqrt{u} \notin K(\alpha_1)$ et en utilisant le théorème de la base télescopique nous aurons $[K(\sqrt{u})/K]\,[K(\alpha_1)\,/\,K] = [K(\alpha_1, \sqrt{u})/K] = 3 \times 2 = 6$ □

Remarque 3.8. *Soient F un corps et u un nombre transcendant sur F. Sur $F(u)[X]$ le polynôme $f(X) = X^3 + uX + u$ est irréductible par d'Eisenstein en $p = u$. Son discriminant $D_f = -u^2(4u + 27)$.*

1. *Si $carF \notin \{2, 3\}$, alors D_f n'est pas un carré sur $F(u)$ car $4u + 27$ ne l'est pas. Si $carF = 3$ alors $D_f = -4u^3 = -u^3$ n'est pas un carré sur $F(u)$. Et par conséquent lorsque $carF \neq 2$ alors $G(f/F(u)) \simeq S_3$.*
2. *Nous ne pouvons rien dire à propos de $G(f/F(u))$ lorsque $carF = 2$. Même si $D_f = u^2$ est bien un carré parfait sur $F(u)$, mais ça n'implique pas forcément que $G(f/F(u)) \simeq A_3$. Le théorème 3.1 et la remarque 3.5 dont cette remarque dépend nécessitent que $carF \neq 2$, autrement dit, dans un corps F de caractéristique 2 nous ne pouvons pas dire que $Gal(f/F)$ est isomorphe ou pas à A_n en vérifiant seulement D_f et en utilisant les théorèmes qu'on a cités.*

Exemple 3.9. *Si nous prenons au hasard un polynôme p de degré 3, irréductible sur un corps $\mathbb{Q}[X]$, il est fortement probable que son groupe de Galois soit isomorphe à S_3, car son discriminant ne soit, probablement, pas un carré dans $\mathbb{Q}$. Il est donc agréable d'avoir quelques uns dont $Gal(p/\mathbb{Q}) \simeq A_3$.*

$p(X)$	D_p	les racines de p
$X^3 - 3X - 1$	9^2	$r\,, r^2 - r - 2\,, -r^2 + 2$
$X^3 - X^2 - 2X + 1$	7^2	r, $r^2 - r - 1$, $-r^2 + 2$
$X^3 + X^2 - 4X + 1$	13^2	r, $r^2 - r + 3$, $-r^2 - 2r + 2$
$X^3 + 2X^2 - 5X + 1$	19^2	r, $r^2 + 2r - 4$, $-r^2 - 3r + 2$

TABLE 3.2 – quelques polynômes cubiques dont le groupes de Galois est isomorphe à A_3

Le tableau 3.3 propose quelques polynômes de degré 3, irréductible sur $\mathbb{Q}$ -car ils sont irréductibles sur $\mathbb{F}_2$. puisque ils n'ont pas de racine sur $\mathbb{F}_2$ et dont le discriminant est un carré parfait sur $\mathbb{Q}$. Nous énumérons les trois racines de chaque polynôme en fonction d'une

de ses racines que nous notons r. Cette liste des racine nous dit essentiellement quels sont les éléments de $Gal(p/\mathbb{Q})$ car chaque automorphisme est déterminé par son effet sur r. c'est une famille des A_3

Exemple 3.10. *Dans cet exemple nous donnerons quelques groupes de Galois des polynômes sur des corps fini, on préciseras a chaque fois la caractéristique du corps, les résultats du tableau suivant sont obtenus a l'aide d'un programme informatique.*

$p(X)$	$\mathbb{F}_p$	D_p	$G(p/\mathbb{F}_p)$
$X^3+99X+103$	$\mathbb{F}_{107}$	11 et $15^2 \equiv 11 \mod [107]$	A_3
$X^3+99X+103$	$\mathbb{F}_{2011}$	1164 et $177^2 \equiv 1164 \mod [2011]$	A_3
$X^3+798X^2+145X+225$	$\mathbb{F}_{2011}$	880 n'est pas un carré $\mod [2011]$	S_3
$X^3+8X^2+94X+13$	$\mathbb{F}_{107}$	33 et $51^2 \equiv 33 \mod [107]$	A_3
X^3+1X^2+2X+7	$\mathbb{F}_{13}$	4 et $2^2 \equiv 4 \mod [13]$	A_3
$X^3+1X^2+789X+456$	$\mathbb{F}_{2003}$	642 n'est pas un carré $\mod [2003]$	S_3
$X^3+78X^2+2002X+2001$	$\mathbb{F}_{2003}$	1012 et $538^2 \equiv 1012 \mod [2003]$	A_3

TABLE 3.3 – Quelques groupes de Galois des polynômes cubiques sur des corps fini

3.2 Groupes de Galois des extensions quartiques

3.2.1 Les sous-groupes transitifs de S_4

Afin de déterminer les groupes de Galois des extensions quartiques, il est préférable, dans un premier temps, de lister tout les sous-groupes transitifs de S_4.
Alors ce qu'il faut savoir c'est que les éléments de ces sous-groupes de S_4 sont des permutations agissantes sur un ensemble a 4 éléments qu'on notera $\{1,2,3,4\}$, donc on aura

1. Les sous-groupes d'ordre 4
   - Le groupe cyclique isomorphe à $\mathbb{Z}/4\mathbb{Z}$, engendré par un cycle. Par exemple (1234).
   - Le groupe de Klein engendré par des doubles transposition, notons le V avec :

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

.

2. Les sous-groupes d'ordre 8 isomorphes au groupe Diédrale noté D_4 avec :

$$D_4 = \{id, (1234)(13), (1243)(14), (1324)(12)\}$$

.

3. Le groupe alterné A_4 qui est d'ordre 12.

4. Le groupe symétrique S_4 qui est d'ordre 24.

Le tableau suivant regroupe alors les sous-groupes transitifs de S_4

Cycle	S_4	A_4	D_4	$\mathbb{Z}/4\mathbb{Z}$	V
$(1,1,1,1)$	1	1	1	1	1
$(1,1,2)$	6		2		
$(2,2)$	3	3	3	1	3
(1.3)	8	8			
(4)	6		2	2	
$\sum$	24	12	8	4	4

TABLE 3.4 – Les sous-groupes transitifs de S_4

Remarque 3.11. *1. Les seuls sous-groupes transitifs de S_4 qui sont contenu da A_4 sont A_4 et V.*

2. Les seuls sous-groupes transitifs de S_4 dont l'ordre est divisible par 3 sont S_4 et A_4.

3. Les seuls sous-groupes transitifs de S_4 contenant un cycle de type $(1,1,2)$ sont S_4 et D_4.

3.2.2 Groupes de Galois des extensions quartiques

Supposons que le polynôme $p(X) = X^4 + aX^3 + bX^2 + cX + d,\ a,b,c,d \in K$, unitaire et irréductible dans $K[X]$, donc $D_p \neq 0$, notons par $(1 \leq \alpha_i \leq 4)$, les racines de $p(X)$ dans un corps de décomposition de ce dernier, soit alors l'égalité suivante :

$$X^4 + aX^3 + bX^2 + cX + d = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4). \tag{3.1}$$

On a vu que un groupe de Galois d'un polynôme $f(X)$ cubique irréductible et séparable dans un corps $K[X]$, est entièrement déterminé par son discriminant $D_f = \Delta$, si oui ou non ce dernier est un carré dans K ; chose qui peut être pensé en terme de polynôme quadratique a savoir un polynôme de la forme $X^2 - \Delta$ ayant une racine dans K, on peut alors pensé qu'un polynôme quartique dépend du comportement d'un polynôme cubique associé, pour cela on essayeras de déterminer un polynôme cubique ayant des racines dans le corps de décompositions de $p(X) = X^4 + aX^3 + bX^2 + cX + d,\ a,b,c,d \in K$ sur $K[X]$ notons le L, sachant que ces groupes de Galois étant dans S_4, on chercheras donc un polynôme a 4 variables qui sous les 24 permutation possible admettrais 3 valeurs.

Cependant on sait que le sous-groupe V est normal dans S_4, ce dernier laisse fixe les éléments suivant dans L :

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4,\ \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4,\ \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Les $1 \leq \beta_i \leq 3 \in L$ engendrent un sous-corps de L noté $K(\beta_1, \beta_2, \beta_3)$, et ce sont des racines d'un polynôme $\phi(X)$ défini par

$$\phi(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3). \tag{3.2}$$

Définition 3.12. *le polynôme $\phi(X)$ est appelé résolvant cubique du polynôme $p(X)$.*
On développent la formule (3.2) *on aura*

$$\phi(X) = X^3 - (\beta_1 + \beta_2 + \beta_3)X^2 + (\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)X - (\beta_1\beta_2\beta_3). \tag{3.3}$$

Par calcule on obtient les résultats suivantes :

1. $$(\beta_1 + \beta_2 + \beta_3) = -(\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_4 + \alpha_2\alpha_3) = -b.$$

2. $$(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) = \alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2 + \alpha_2\alpha_3\alpha_4^2 + \alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3^2\alpha_4 + \alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4 = ac - 4d$$

3. $$(\beta_1\beta_2\beta_3) = -(\alpha_1\alpha_2 + \alpha_3\alpha_4)(\alpha_1\alpha_3 + \alpha_2\alpha_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) = -(a^2d + c^2 - 4bd).$$

Chose qui ramène l'équation (3.3) *a la formule suivante :*

$$\phi(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd).$$

Remarque 3.13.
— *Dans le cas ou $p(X)$ est unitaire, pour vérifié si $p(X)$ est irréductible il suffit de voir si $\phi(X)$ est irréductible.*
— *Si $a = b = 0$, alors $p(X) = X^4 + cX + d \Longrightarrow X^3 - (4d)X - c^2$.*

Proposition 3.14. *Sous les hypothèses précédente si $p(X)$ un polynôme unitaire et irréduc-*

tible de degré 4 de $K[X]$ et $\phi(X)$ sa résolvante cubique associé alors

$$D_p = \prod_{i<j}(\alpha_i - \alpha_j)^2 = D_\phi = \prod_{i<j}(\beta_i - \beta_j)^2. \tag{3.4}$$

Démonstration. On applique la méthode de Ferrari **??** sur le polynôme $p(X)$, le résultat 3.4 est immédiat, de plus d'après **??** on a

$$D_\phi = D_p = 18pqr - 4p^3r + p^2q^2 - 4r^3 - 27q^2.$$

□

Théorème 3.15. *Avec les notation précédente, $G(p/K)$ est décrit comme l'indique le tableau suivant :*

$D_p \in K$	$\phi(X) \in K[X]$	$G(p/K)$
n'est pas un carré	irréductible	S_4
un carré	irréductible	A_4
n'est pas un carré	réductible	D_4 ou $\mathbb{Z}/4\mathbb{Z}$
carré	réductible	V

TABLE 3.5 – Tableau représentent les groupes de Galois des extensions quartiques

Démonstration. Nous vérifierons chaque ligne dans le tableau.

D_p n'est pas un carré et $\phi(X)$ est irréductible sur K : comme D_p n'est pas un carré alors $G(p/K) \not\subset A_4$, et comme la résolvante $\phi(X)$ est irréductible sur K et que ses racines sont dans le corps de décomposition de $p(X)$ sur K (i.e., $\alpha_i \in Dec_K(p(X))$, $\forall i$, α_i est racine de $p(X)$), adjoignant une racine de $\phi(X)$ à K nous donne une extension de degré 3 incluse dans $Dec_K(p(X))$, donc $|G(p/K)|$ est divisible par 3, il est aussi divisible par 4, donc $G(p/K) \simeq S_4$ ou A_4, mais nous savons que $G(p/K) \not\simeq A_4$, et ceci implique que $G(p/K) \simeq S_4$.

D_p est un carré et $\phi(X)$ est irréductible sur K : On a $G(p/K) \subset A_4$ et $G(p/K)$ est divisible par 3 et 4, ce qui implique que $G(p/K) \simeq A_4$.

D_p n'est pas un carré et $\phi(X)$ est réductible sur K : puisque D_p n'est pas un carré, alors $G(p/k) \not\subset A_4$, donc $G(p/K)$ est isomorphe soit a S_4, D_4 ou $\mathbb{Z}/4\mathbb{Z}$; nous allons montrer $G(p/K) \not\simeq S_4$. Ce qui distingue S_4 des deux autres choix c'est que il contient 3-cycles. Si $G(p/K) \simeq S_4 \Longrightarrow (123) \in G(p/K)$, par suite on applique cet automorphisme dans le groupe de Galois aux racines de $\phi(X)$, on aura donc un seul orbite qui est le suivant :

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 \mapsto \alpha_2\alpha_3 + \alpha_1\alpha_4 \mapsto \alpha_3\alpha_1 + \alpha_2\alpha_4 \mapsto \alpha_1\alpha_2 + \alpha_3\alpha_4.$$

Ces nombres sont distincts puisque $\phi(X)$ est séparable, donc au moins une racine de $\phi(X)$ se trouve dans K, alors $G(p/K)$-orbite de cette racine est elle même, contradiction, on a pas trouver un 3-cycle.

D_p est un carré et $\phi(X)$ est réductible sur K : Comme $G(p/K) \subset A_4$, alors $g(p/K) \simeq V$ ou $g(p/K) \simeq A_4$, nous allons éliminer le choix où $g(p/K) \simeq A_4$, on peut distinguer V de A_4 en effet A_4 contient un 3-cycle contrairement a V, si on a un 3-cycle sur les racines de $p(X)$ dans $G(p/K)$, et si nous appliquons cela a une racines de $\phi(X)$ on obtiendra que toutes les racines sont dans une seule $G(p/K)-$orbite, contradiction, $\phi(X)$ est séparable et irréductible sur K, on en déduit que $G(p/K)$ ne contient pas un 3-cycles. □

Exemple 3.16. *Le tableau suivant donne quelques exemples des groupe de Galois des polynômes de degré* 4 *sur* $\mathbb{Q}$.

$p(X)$	D_p	$\phi(X)$	$G(p/\mathbb{Q})$
$X^4 - X - 1$	-283	$X^3 + 4X - 1$	S_4
$X^4 + 2X + 2$	101×4^2	$X^3 - 8X - 4$	S_4
$X^4 + 8X + 12$	576^2	$X^3 - 48X - 64$	A_4
$X^4 + 3X + 3$	21×15^2	$(X + 3)(X^2 - 3X - 3)$	D_4 ou $\mathbb{Z}/4\mathbb{Z}$
$X^4 + 5X + 5$	5×55^2	$(X - 5)(X^2 + 5X + 5)$	D_4 ou $\mathbb{Z}/4\mathbb{Z}$
$X^4 + 36X + 63$	4320^2	$(X - 18)(X + 6)(X + 12)$	V

TABLE 3.6 – Quelques exemples des groupe de Galois des polynômes de degré 4 sur $\mathbb{Q}$

Exemple 3.17. *Le tableau suivant donne quelques exemples des groupe de Galois des polynômes de degré* 4 *sur* $\mathbb{F}_p$.

$f(X)$	$\mathbb{F}_p$	D_f	$\phi(X)$	$G(p/\mathbb{F}_p)$
$X^4 + X^3 + 12X^2 + 7X + 9$	$\mathbb{F}_{13}$	9, $3^2 \equiv 9 \mod [13]$	réductible	V
$X^4 + 14X^3 + 6X + 58$	$\mathbb{F}_{103}$	39 n'est pas un carré mod [103]	réductible	D_4 ou $\mathbb{Z}/4\mathbb{Z}$
$X^4 + 2010X^3 + 2009X^2 + 2007X + 2006$	$\mathbb{F}_{2011}$	1816, $665^2 \equiv 1816 \mod [2011]$	irréductible	A_4
$X^4 + 7X^2 + 8X + 14$	$\mathbb{F}_{4127}$	1522 n'est pas un carré mod [4127]	irréductible	S_4
$X^4 + 201X^3 + 2003X + 207$	$\mathbb{F}_{3217}$	3009 n'est pas un carré mod [3217]	irréductible	S_4
$X^4 + 14X^3 + 13X + 7$	$\mathbb{F}_{23}$	15 n'est pas un carré mod [23]	réductible	D_4 ou $\mathbb{Z}/4\mathbb{Z}$

TABLE 3.7 – Quelques exemples des groupe de Galois des polynômes de degré 4 sur $\mathbb{F}_p$

Proposition 3.18. *Soit F un corps est u un élément transcendant sur F, Dans $F(u)[X]$, le polynôme $p(X) = X^4 + uX + u$, irréductible et unitaire alors*

$$G(p/F(u)) = S_4.$$

Démonstration. On a bien $p(X)$ irréductible (il est d'Eisenstein en $t = u$) et on sait que $D_p = -27u^4 + 256u^3 = u^3(256 - 27u)$, Si *car* $F \neq 2$ où 3, on vois clairement que D_p n'est pas

un carré.

Maintenant si $car\, F = 3 \Longrightarrow D_p = u^3$, qui n'est pas un carré.

La résolvante cubique de $p(X)$, $\phi(X) = X^3 - 4uX - u^2$, qui est irréductible dans $F(u)[X]$ puisque in n'admet pas de racine dans $F(u)$, par suite et d'après le théorème précédent on en déduit que $G(p/F(u)) \simeq S_4$. □

Corollaire 3.19. *1. $G(p/K) \simeq V \iff \phi(X)$ est scindé sur K.*

2. $G(p/K) \simeq D_4$ ou $\mathbb{Z}/4\mathbb{Z} \iff \phi(X)$ admet une seule racine dans K.

Démonstration. 1. La condition pour que $G(p/K) \simeq V$ est que D_p soit un carré dans K et $\phi(X)$ soit réductible sur K.

Puisque $D_p = D_\phi$ et $G(p/K) \simeq V \iff D_\phi$ soit un carré dans K et que $\phi(X)$ soit réductible sur K.

Et par le théorème 3.7, $Dec_K(\phi(X)) = K(r, \sqrt{D_\phi})$ où r est une racine de $\phi(X)$, ainsi $G(p/K) \simeq V \iff \phi$ est scindé sur K.

2. La condition pour que $G(p/K) \simeq D_4$ ou $\mathbb{Z}/4\mathbb{Z}$ est que D_p soit un carré dans K et que $\phi(X)$ soit réductible sur K. Ces conditions, et par le théorème 3.7 pour $\phi(X)$ sont équivalentes avec le fait que $\phi(X)$ a une racine dans K mais qu'il ne soit scindé sur K ce qui implique que $\phi(X)$ a une unique racine dans K.

□

Théorème 3.20. *Soit $p(X)$ un polynôme irréductible de degré 4 dans $\mathbb{Q}[X]$, si $G(p/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ alors $D_p > 0$, par conséquent si $G(p/\mathbb{Q}) \simeq D_4$, ou $\mathbb{Z}/4\mathbb{Z}$ et $D_p < 0$ alors $G(p/\mathbb{Q}) \simeq D_4$.*

Démonstration. Si $G(p/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, alors $[Dec_{\mathbb{Q}}(p(X))] = 4$, tout racine de $p(X)$ génère une extension de $\mathbb{Q}$ de degré 4, donc le corps généré sur K par une seule racine de $p(X)$ contient nécessairement les autres racines, cela dit si $p(X)$ admet une seule racine réelle alors il admet 4 autre racine réelles, donc le nombre de racine réelles de $p(X)$ et soit 0 soit 4.

Maintenant si $p(X)$ n'admet pas de racine réelle alors forcément il admettrait des racines complexes deux a deux conjugués, alors D_p est un carré de :

$$(z - \bar{z})(z - w)(z - \bar{w})(\bar{z} - w)(\bar{z} - \bar{w})(w - \bar{w}) = |z - w|^2 |z - \bar{w}|^2 (z - \bar{z})(w - \bar{w}). \qquad (3.5)$$

Les différences $z - \bar{z}$ et $w - \bar{w}$ sont purement imaginaires et non nulles, puisque z et w ne sont pas des nombres réels, donc nécessairement leurs produit est réel et non nul, ainsi donc si on met au carré l'égalité (3.5), on trouve que $D_p > 0$.

On dernier si $p(X)$ admet 4 racines réelles alors le produits des différences de ses racines est nécessairement un nombre réel no nul, donc $D_p > 0$. □

Exemple 3.21. *Soit le polynôme* $p(X) = X^4 + 4X^2 - 2 \in \mathbb{Q}$, *il est irréductible car il est d'Eisenstein en* $t = 2$, *sont discriminant est* $D_p = -18432$, *sa résolvante cubique associé est* $\phi(X) = X^3 - 4X^2 + 8X - 32 = (X - 4)(X^2 + 8)$, *donc d'après le théorème 3.15* $G(p/\mathbb{Q}) \simeq D_4$, *ou* $\mathbb{Z}/4\mathbb{Z}$. *Or d'après le théorème 3.20 et comme on* $D_p < 0$ *alors* $G(p/\mathbb{Q}) \simeq D_4$.

3.2.3 Distinction entre $\mathbb{Z}/4\mathbb{Z}$ et D_4 (Théorème Kappe, Warren)

On ne peut décider on utilisant le théorème 3.20 si un groupe de Galois d'un polynôme est isomorphe a D_4 ou $\mathbb{Z}/4\mathbb{Z}$ dans le cas ou son discriminant est strictement positif, dans la suite nous donnerons une méthode a fin de calculer précisément par le théorème Kappe, Warren le groupe de Galois associé par le théorème.
On a vu dans la section précédente que $G(p/K) \simeq D_4$ *ou* $\mathbb{Z}/4\mathbb{Z}$, si et seulement si, D_p est un carré dans K et sa résolvante cubique associé noté $\phi(X)$, est réductible sur $K[X]$ et quand cela se produit $\phi(X)$ admettrais une seule racine dans K.

Théorème 3.22. *(Kappe, Warren) Sous les hypothèses de la section précédente, Soit* $\Delta = D_p$, *on suppose que* $\Delta \notin K^2$ *et* $\phi(X)$ *est réductible dans* $K[X]$ *avec une seule racine* $\beta \in K$, *alors* $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$ *si les polynômes* $X^2 + aX + (b - \beta)$ *et* $X^2 - \beta X + d$ *sont scindé sur* $K(\sqrt{\Delta})$, *sinon* $G(p/K) \simeq D_4$.

Démonstration. Soit $1 \leq \alpha_i \leq 4$, les racines de $p(X)$, on pose $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$, D_4 et $\mathbb{Z}/4\mathbb{Z}$ étant tout les deux des sous-groupes de S_4, contenant un 4-cycle (les éléments d'ordre 4 dans S_4 sont des 4-cycle), dans le tableau suivant nous décrivons l'effet de chaque un des 4-cycle sur β, cela dit nous virons si ce 4-cycle appartient a un groupe de Galois, les racines distincts de $\phi(X)$ sont dans la deuxième ligne.

σ	(1234)	(1432)	(1243)	(1342)	(1324)	(1423)
$\sigma(\beta)$	$\alpha_2\alpha_3 + \alpha_4\alpha_1$	$\alpha_4\alpha_1 + \alpha_2\alpha_3$	$\alpha_2\alpha_4 + \alpha_1\alpha_3$	$\alpha_3\alpha_1 + \alpha_4\alpha_2$	$\alpha_3\alpha_4 + \alpha_2\alpha_1$	$\alpha_4\alpha_3 + \alpha_1\alpha_2$

TABLE 3.8 – Représentation des 4-cycle

Puisque β est fixé par $G(p/K)$, les seules 4-cycle possible sont (1324) et (1423), les deux sont dans $G(p/K)$, puisque au moins un des deux l'est et il sont des inverses. Soit alors $\sigma = (1324)$.

Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$ alors $G(p/K) \simeq \langle\sigma\rangle$, si $G(p/K) \simeq D_4$, alors $G(p/K) = \langle(13240), (12)\rangle = \{(1), (1324), (12)(34), (1423), (12), (34), (13)(24), (14)(23)\}$, et les éléments de $G(p/K)$ fixant α_1 sont (1) et (34), on pose $\tau = (34)$, le tableau suivant représente le produit σ et τ en tant que cycle disjoint

1	σ	σ^2	σ^3	τ	$\tau\sigma$	$\sigma^2\tau$	$\sigma^3\tau$
(1)	(1324)	(12)(34)	(1423)	(34)	(13)(24)	(12)	(14)(23)

TABLE 3.9 – le produit σ et τ en tant que cycle disjoint

Les sous-groupes engendrés par $\langle\sigma\rangle$ et $\langle\sigma, \tau\rangle$, sont très différent, voir le treillis suivant

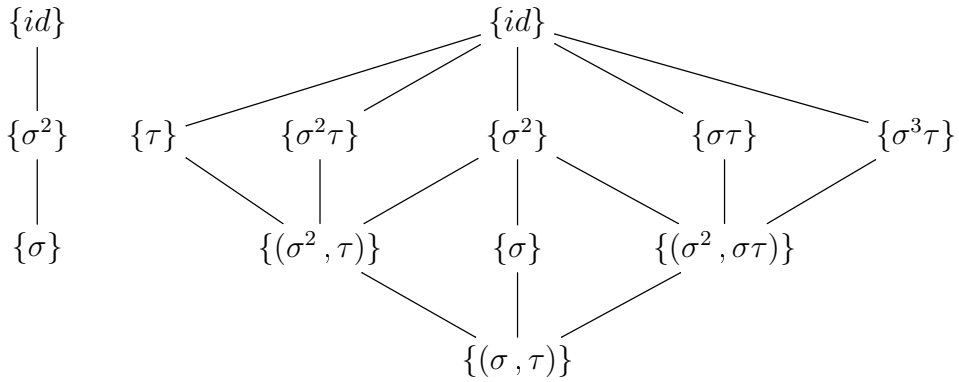


FIGURE 3.1 – Sous-groupes engendrés par $\langle\sigma\rangle$ et $\langle\sigma, \tau\rangle$

En se basant sur le treillis ci-dessus, le treillis suivant représente les sous-corps du corps de décomposition de $p(X)$, L ici désigne dans les deux cas l'unique extension quadratique de K contenue dans $K(\alpha_1)$: Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$, alors L correspond au sous-groupe engendré par $\langle\sigma^2\rangle$, tandis que si $G(p/K) \simeq D_4$, alors L correspond au sous-groupe engendré par $\langle\sigma^2, \tau\rangle$, puisque $\Delta \notin K^2$ alors $[K(\sqrt{\Delta})/K] = 2$.

Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$, alors $L = K(\sqrt{\Delta})$ puisque il existe une seule extension quadratique de K dans le corps de décomposition de $p(X)$.
Si $G(p/K) \simeq D_4$, on sait que $K(\alpha_1)$ correspond a $\langle\tau\rangle$, $K(\alpha_3)$ correspond a $\langle\sigma^2\tau\rangle$, et $K(\sqrt{\Delta})$ correspond $\langle\sigma^2, \sigma\tau\rangle$. $[K(\alpha_1)/K] = 4$, donc son sous-groupe correspond dans D_4 a $\langle\sigma, \tau\rangle$ d'ordre 8, $\frac{8}{4} = 2$ et $\tau = (34)$ fixe α_1 et son ordre est 2. D'une manière similaire, on a $[K(\alpha_3)/K] = 4$ et $\sigma^2\tau = (12)$ fixe α_3. Le sous-groupe correspond à $K(\sqrt{\Delta})$ sont les permutations paires dans le groupe de Galois, et c'est $\{(1), (12)(34), (13)(24), (14)(23)\} \simeq \langle\sigma^2, \sigma\tau\rangle$.

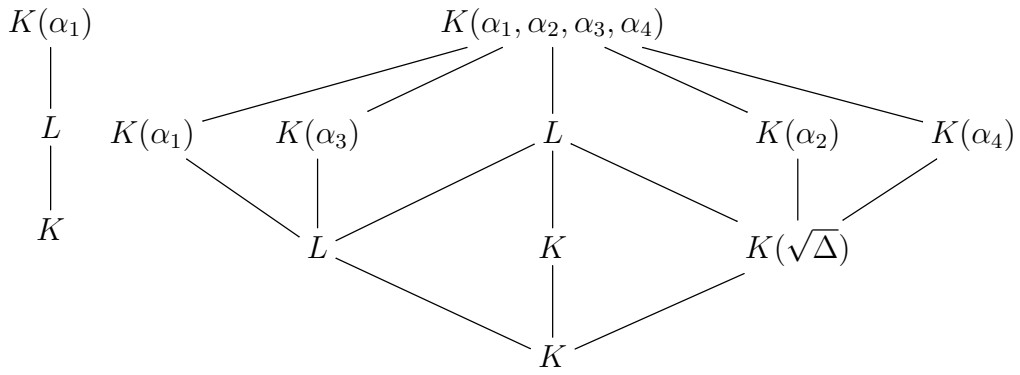


FIGURE 3.2 – Les sous-corps du corps de décomposition de $p(X)$

Bien que les deux cas $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$ et $G(p/K) \simeq D_4$ soient différents, nous allons développé quelques idées pour les deux concernant les extensions quadratiques $K(\alpha_1)/, L$ et L/K avant de distinguer ces deux derniers l'un de l'autre.
Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}, Gal(K(\alpha_1)/L) = \{1, \sigma^2\}$. Si $G(p/K) \simeq D_4, Gal(K(\alpha_1)/L) = \langle 1, \sigma^2 \rangle / \langle \tau \rangle = \{1, \sigma^2\}$. Alors dans les deux cas, le conjugué de α_1 dans L est $\sigma^2(\alpha_1) = \alpha_2$, le polynôme minimal de α_1 sur L est alors

$$(X - \alpha_1)(X - \alpha_2) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2.$$

Par conséquent $\alpha_1 + \alpha_2$ et $\alpha_1\alpha_2$ sont dans L, puisque $[K(\alpha_1)/K] = 4$, ce polynôme n'est pas dans $K[X]$:

$$\alpha_1 + \alpha_2 \notin K \text{ ou } \alpha_1\alpha_2 \notin K. \tag{3.6}$$

Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$, alors $Gal(L/K) = \langle \sigma \rangle / \langle \sigma^2 \rangle = \{1, \bar{\sigma}\}$, la classe de σ dans $Gal(L/K)$ cette classe est aussi non trivial, donc $L^\sigma = K$, c'est un élément de L fixé par σ dans K, puisque $\sigma(\alpha_1 + \alpha_2) = \alpha_3 + \alpha_4$ et $\sigma(\alpha_1\alpha_2) = \alpha_3\alpha_4$, les polynômes suivantes :

$$(X - (\alpha_1 + \alpha_2))(X - (\alpha_3 + \alpha_4)) = X^2 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)X + (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \tag{3.7}$$

et

$$(X - \alpha_1\alpha_2)(X - \alpha_3\alpha_4) = X^2 - (\alpha_1\alpha_2 + \alpha_3\alpha_4)X + \alpha_1\alpha_2\alpha_3\alpha_4. \tag{3.8}$$

Ont tous les deux des coefficients dans $L^\sigma = K$.
Les coefficients linières présent dans l'équation (3.7) sont a et le terme constant est

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 = b - (\alpha_1\alpha_2 + \alpha_3\alpha_4) = b - \beta,$$

donc l'équation (3.7) est égale a $X^2 + aX + (b - \beta)$, le polynôme quadratique (3.8) est $X^2 - \beta X + d$, si $\alpha_1 + \alpha_2 \notin K$, (3.7) est irréductible dans $K[X]$, alors son discriminant n'est pas un carré dans K, sinon si $\alpha_1 + \alpha_2 \in K$ alors (3.7) admet une racine double et son discriminant vaut alors 0.

De la même manière le discriminant de (3.8) n'est pas un carré ou bien il vaut 0, par conséquent le corps de décomposition de (3.8) ou (3.7) sur K est soit L soit K et d'après (3.6) au moins un discriminant de l'une des deux équations (3.8) ou (3.7) n'est pas un carré dans K, donc son corps de décomposition est L.

Puisque $\alpha_1 + \alpha_2$ et $\alpha_1\alpha_2$ sont dans L et $[L/K] = 2$, chacun deux engendre l'extension L sur K dans le cas ou il ne sont pas de K, et cela se produit pour au moins un des deux nombres.

Premièrement on suppose que $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$ alors $L = K(\sqrt{\Delta})$, donc $X^2 + aX + (b - \beta)$ et $X^2 - \beta X + d$, se décomposent complément sur $K(\sqrt{\Delta})$, puisque leurs racines sont dans L.

Maintenant on suppose que $G(p/K) \simeq D_4$, alors $L \neq K(\sqrt{\Delta})$, on sait que au moins l'un des polynômes (3.8),(3.7) est irréductible sur K, donc leurs racines engendrent l'extension L sur K donc elle ne sont pas dans $K(\sqrt{\Delta})$, ainsi le polynômes (3.8) ou (3.7) est irréductible sur $K(\sqrt{\Delta})$, si il est irréductible sur K.

Cela dit puisque les conclusion sur les deux polynôme quadratiques sur $K(\sqrt{\Delta})$ sont différentes et elle dépende du choix de $G(p/K)$, donc la détermination de groupe de Galois associé dépend aussi de ces deux polynômes. Ce qui achève la démonstration. □

Corollaire 3.23. *Sous les hypothèses précédentes, le tableau suivant décrit les groupes de Galois d'un polynôme de degré* 4 *:*

$\Delta \in K$	$\phi(X) \in K[X]$	$(a^2 - 4(b - \beta))\Delta$ et $(\beta^2 - 4d)\Delta$	$G(p/K)$
n'est pas un carré	irréductible		S_4
carré	irréductible		A_4
n'est pas un carré	$\beta \in K$	au moins une racine $\notin K^2$	D_4
n'est pas un carré	$\beta \in K$	les deux racines $\in K^2$	$\mathbb{Z}/4\mathbb{Z}$
carré	réductible		V

TABLE 3.10 – Les groupes de Galois d'un polynôme de degré 4

Démonstration. Les polynômes $X^2 + aX + (b - \beta)$ et $X^2 + \beta X + d$, sont scindé sur $K(\sqrt{\Delta})$, si et seulement si, leurs discriminant respectifs, $a^2 - 4(b - \beta)$ et $\beta^2 - 4d$ sont des carré dans $K(\sqrt{\Delta})$, comme on a vu dans le théorème précédent leurs discriminants valent soit 0 soit un nombre qui n'est pas un carré dans K, cela dit un nombre qui n'est pas un carré dans

K ; est un carré dans $K(\sqrt{\Delta})$, si est seulement si, sont produit avec le discriminant Δ et un carré, ce résultat est aussi vérifié pour 0. □

Exemple 3.24. *Dans le tableau suivant on vas donner quelques exemples des groupes de Galois d'un polynôme unitaire (X^4+cX+d) sur $\mathbb{Q}$, on vas tout de même mettre en évidence les cas ou on doit décider entre D_4 et $\mathbb{Z}/4\mathbb{Z}$.*

X^4+cX+d	Δ	$X^3-4dX-c^2$	$4\beta\Delta$ et $(\beta^2-4d)\Delta$	$G(p/K)$
X^4+3X+3	21×15^2	$(X+3)(X^2-3X-3)$	$-56700,-14175$	D_4
X^4+5X+5	5×55^2	$(X-5)(X^2+5X+5)$	550^2,275^2	$\mathbb{Z}/4\mathbb{Z}$
$X^4+8X+14$	2×544^2	$(X-8)(X^2+8X+8)$	4352^2,2176^2	$\mathbb{Z}/4\mathbb{Z}$
$X^4+13X+39$	13×1053^2	$(X-13)(X^3+13X+13)$	27378^2, 13689^2	$\mathbb{Z}/4\mathbb{Z}$
$X^4+36X+63$	4320^2	$(X-18)(X+6)(X+12)$	//	V

TABLE 3.11 – Groupes de Galois d'un polynôme unitaire (X^4+cX+d) sur $\mathbb{Q}$

Exemple 3.25. *Le tableau suivant donne quelques exemples des groupe de Galois des polynômes de degré 4 sur $\mathbb{F}_p$. on précisent cette fois si c'est D_4 ou $\mathbb{Z}/4\mathbb{Z}$,*
$\Delta_1=(a^2-4(b-\beta))\Delta$ *et* $\Delta_2=(\beta^2-4d)\Delta$.
$\phi(X)$ *réductible dont la racine est* β.

$f(X)$	$\mathbb{F}_p$	Δ	β	Δ_1 et Δ_2	$G(p/K)$
$X^4+10X^3+X^2+7X+2$	$\mathbb{F}_{11}$	$2\notin(\mathbb{F}_{11})^2$	$\beta=4$	$\Delta_1=4\in(\mathbb{F}_{11})^2$,$\Delta_2=5\in(\mathbb{F}_{11})^2$	$\mathbb{Z}/4\mathbb{Z}$
X^4+7X^3+3X+1	$\mathbb{F}_{13}$	$7\notin(\mathbb{F}_{13})^2$	$\beta=6$	$\Delta_1=4\in(\mathbb{F}_{13})^2$,$\Delta_2=3\in(\mathbb{F}_{13})^2$	$\mathbb{Z}/4\mathbb{Z}$
$X^4+201X^3+2001X^2+2002X+4$	$\mathbb{F}_{2003}$	$1244\notin(\mathbb{F}_{2003})^2$	$\beta=3$	$\Delta_1=412\notin(\mathbb{F}_{2003})^2$,$\Delta_2=1307\notin(\mathbb{F}_{2003})^2$	D_4
$X^4+2X^3+17X^2+26$	$\mathbb{F}_{71}$	$21\notin(\mathbb{F}_{71})^2$	$\beta=56$	$\Delta_1=23\notin(\mathbb{F}_{71})^2$,$\Delta_2=56\notin(\mathbb{F}_{71})^2$	D_4
$X^4+14X^3+6X+58$	$\mathbb{F}_{103}$	$39\notin(\mathbb{F}_{103})^2$	$\beta=77$	$\Delta_1=86\notin(\mathbb{F}_{103})^2$,$\Delta_2=12\notin(\mathbb{F}_{103})^2$	D_4
$X^4+2016X^3+2015X^2+2014X+2013$	$\mathbb{F}_{2017}$	$980\notin(\mathbb{F}_{2017})^2$	$\beta=516$	$\Delta_1=116\in(\mathbb{F}_{2017})^2$,$\Delta_2=1219\notin(\mathbb{F}_{2017})^2$	D_4

TABLE 3.12 – Quelques exemples des groupe de Galois des polynômes de degré 4 sur $\mathbb{F}_p$

Corollaire 3.26. *Soit $f(X)=X^4+bX^2+d\in K[X]$, un polynôme unitaire irréductible de degré 4, alors*

1. $d\in K^2\Longrightarrow G(f/K)\simeq V$.
2. $d\notin K^2$, $(b^2-4d)d\in K^2\Longrightarrow G(f/K)\simeq\mathbb{Z}/4\mathbb{Z}$.
3. $d\notin K^2$, $(b^2-4d)d\notin K^2\Longrightarrow G(f/K)\simeq D_4$.

Dans la seconde condition, nous pourrions simplifier les hypothèses pour que $(b^2-4d)\times d$ soit un carré dans K puisque ceci implique que d ne soit pas un carré : si

$$((b^2-4d)\times d) \text{ est un carré et } d \text{ est un carré}$$

alors

$$b^2-4d \text{ est un carré,}$$

ce qui contredit que

$$X^4 + bX + d$$

soit irréductible.

Démonstration. Soit $p(X) = X^4 + bX + d$, et soit $D_p = 16 \times d \times (b^2 - 4d)^2$.
Par hypothèse,$D_p \neq 0$, alors si on lève au carré les facteurs ce sera le même que d.
La résolvante cubique $\phi(X)$ est

$$\phi(X) = X^3 - bX^2 - 4dX + 4bd = (X - b)(X^2 - 4d)$$

qui est irréductible sur K avec comme racine est b. Dans les notations du corollaire 3.23, si Δ n'est pas un carré, alors $\beta = b$, ce qui donne $\beta^2 - 4d = b^2 - 4d$ et $a^2 - 4(d - \beta) = 0$,et nous achevons la démonstration en utilisant le corollaire 3.23.
Nous présentons dans le tableau suivant quelques exemples qui illustre ce qu'on vient de dire, le polynômes $p(X)$ sont sur $\mathbb{Q}[X]$ □

$p(X)$	d	$(b^2 - 4d) \times d$	$G(p/K)$
$X^4 + 4X^2 + 1$	1	12	V
$X^4 - 4X^2 + 2$	2	16	$\mathbb{Z}/4\mathbb{Z}$
$X^4 + 4X^2 - 2$	-2	-16	D_4
$X^4 + 5X^2 + 2$	2	34	D_4
$X^4 + 5X^2 + 5$	5	25	$\mathbb{Z}/4\mathbb{Z}$
$X^4 + 5X^2 + 3$	3	13	D_4

TABLE 3.13 – Quelques exemples pour illustrer le corollaire 3.23

3.2.4 Distinction entre $\mathbb{Z}/4\mathbb{Z}$ et D_4 (Méthode Classique)

Dans la suite nous donnerons la méthode classique pour déterminer les groupes de Galois d'uu polynôme de degré 4 ; pour cela considérons le théorème suivant :

Théorème 3.27. *Sous les hypothèses précédente, soit $p(X)$ un polynôme irréductible, on suppose que $D_p = \Delta \notin K^2$ et $\phi(X)$ réductible dans $K[X]$ alors $G(p/K)$ est décrit comme suit :*

1. *si $p(X)$ est irréductible sur $K(\sqrt{\Delta}) \Longrightarrow G(p/K) \simeq D_4$.*
2. *si $p(X)$ est réductible sur $K(\sqrt{\Delta}) \Longrightarrow G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$.*

Démonstration. Si $G(p/K) \simeq D_4$, on sait d'après le treillis précédent que $Dec_K(p(X))$ est $K(\alpha_1, \sqrt{\Delta})$, puisque $[K(\alpha_1, \sqrt{\Delta})/K] = 8\,; [K(\alpha_1, \sqrt{\Delta})/K(\sqrt{\Delta})] = 4$, alors $p(X)$ doit être

nécessairement irréductible sur $K(\sqrt{\Delta})$.
Si $G(p/K) \simeq \mathbb{Z}/4\mathbb{Z}$, $[Dec_K(p(X))/K(\sqrt{\Delta})] = 2$, alors $p(X)$ est réductible sur $K(\sqrt{\Delta})$. □

Exemple 3.28. *Posons $K = \mathbb{Q}$, les polynômes $p_1(X) = X^4+3X+2$ et $p_2(X) = X^2+5X+5$ dont les discriminants sont D_{p_1} et D_{p_2} présentés dans le tableaux suivants, vérifient tout les deux les hypothèses du théorème 3.27. Nous allons utiliser ce théorème afin de leur trouver leurs groupes de Galois sur $\mathbb{Q}$*

$p_i(X)$	D_{p_i}	$\phi_i(X)$	$G(p_i/K)$
$p_1(X)$	21×15^2	$(X+3)(X^2-3X-3)$	D_4
$p_2(X)$	5×55^2	$(X-5)(X^2+5X+5)$	$\mathbb{Z}/4\mathbb{Z}$

TABLE 3.14 – Les groupes de Galois de p_1 et de p_2

Afin de trouver le groupe de Galois en utilisant le théorème 3.27, nous devons savoir si p_1 est irréductible sur $\mathbb{Q}(\sqrt{21})$ et si p_2 est irréductible sur $\mathbb{Q}(\sqrt{5})$. En fait, ce théorème dit que si un polynôme P est irréductible sur un sous corps quadratique de son corps de décomposition, alors $G(P/K) \simeq D_4$; Si P est réductible sur un sous-corps de son corps de décomposition, alors $G(P/K) \simeq \mathbb{Z}/2^2\mathbb{Z}$.
Ces polynômes sont tous les deux irréductibles sur $\mathbb{Q}$, alors leurs racines sont de degré 4 sur $\mathbb{Q}$ et par conséquent ils n'appartiennent pas au sous-corps quadratique du corps de décomposition de ces deux polynômes. Ceci veut dire que s'ils sont réductibles sur les sous-corps quadratiques de leurs corps de décompositions, ceci doit être un produit de deux polynômes de degré 2.
Afin de connaître si $p_1(X)$ est irréductible sur $\mathbb{Q}(\sqrt{21})$, nous supposons que p_1 se factorise de la manière suivante

$$p_1(X) = X^4 + 3X + 3 = (X^2 + AX + B)(X^2 + CX + D)$$

et nous calculons les coefficients des polynômes de degré 2. Nous trouverons le système suivant

$$\begin{cases} A + C = 0 \\ B + D + AC = 0 \\ AD + BC = 3 \\ BD = 3 \end{cases} \tag{3.9}$$

ce qui implique que $C = -A$ et $D = -AC - B = A^2 - B$, alors la troisième condition devient

$A(A^2-2B)=3$. *Ceci nécessite que* $A\neq 0$ *et par suite nous pourrons trouver* B *:*

$$B=\frac{A^3-3}{2A}$$

Et par suite nous aurons la quatrième condition $BD=3$ *devient*

$$3=\frac{A^3-3}{2A}\left(A^2-\frac{A^3-3}{2A}\right)=\frac{A^6-9}{4A^2}$$

et par suite

$$0=A^6-12A^2-9=(A^2)(A^4-3A^2-3)$$

Cette dernière équations doit avoir une solution A *dans* $\mathbb{Q}(\sqrt{21})$. *L'équation* $A^2+3=0$ *n'a aucune solution dans* $\mathbb{R}$ *donc de même dans* $\mathbb{Q}(\sqrt{21})$. *Comme* X^4-3X^2-3 *est irréductible sur* $\mathbb{Q}$, *alors ses racines sont de degrés* 4 *sur* $\mathbb{Q}$ *et celles-ci ne peuvent être dans* $\mathbb{Q}(\sqrt{21})$, *ce qui est absurde. Et ceci prouve bien que* $p_1(X)$ *est irréductible sur* $\mathbb{Q}(\sqrt{21})$. *Et ceci implique que*

$$G(p_1/\mathbb{Q})\simeq D_4$$

et ceci est exactement le résultat que nous avons vu dans le tableau de l'exemple 3.24.
Nous utilisons exactement la même méthode de factorisation qu'on a vu pour le polynôme $p_1(X)$ *pour factoriser* $p_2(X)$ *sur* $\mathbb{Q}(\sqrt{5})$, *nous aurons à la fin ces égalités suivantes :*

$$0=A^6-20A^2-25=(A^2-5)(A^4+5A+5)$$

cette équation a pour $A=\sqrt{5}$ *une solution dans* $\mathbb{Q}(\sqrt{5})$, *et ceci permet la factorisation sur ce corps*

$$p_2(X)=X^4+5X+5=\left(X^2+\sqrt{5}X+\frac{5-\sqrt{5}}{2}\right)\left(X^2-\sqrt{5}X+\frac{5+\sqrt{5}}{2}\right)$$

ce qui implique que

$$G(p_2/\mathbb{Q})\simeq\mathbb{Z}/4\mathbb{Z}$$

3.3 Algorithme de détermination des groupes de Galois des extension cubiques et quartiques

Dans cette section nous proposons deux algorithmes qui illustrent les résultats obtenus dans le chapitre 3, on vas définir dans un premier temps les fonctions communes entre les deux algorithmes, la liste suivante donne les noms des fonctions ainsi que leurs utilités :

1. **Fonction Pow() :** Calcule la puissance d'un nombre.
2. **Fonction TestRedu() :** Test si un polynôme est réductible.
3. **Fonction Disc() :** Calcule le discriminant d'un polynôme.
4. **Fonction TestCarre() :** Test si le discriminant est un carré.
5. **Fonction RechercheRacine() :** Recherche d'une racine d'un polynôme.

Ensuite nous donnerons les deux algorithmes a savoir le premier pour les extensions cubiques (**Algorithme GroupeGaloisCubique**), le deuxième pour les quartiques basé sur la méthode de Kappe, Warren, (**Algorithme GroupeGaloisQuartique**). Le liens suivant et le QR code représente une application écrite avec le langage C++, des deux algorithmes précédent :

`https://github.com/root-bayou/M2ACCPFE.git`

Vous pouvez l'exécuter directement en ligne :

`https://onlinegdb.com/SZ-36t7yp`

Algorithme 1 : Pow(a, i)

Entrées : a, i : entier
$j \leftarrow 2$;
tant que $j \leq i$ **faire**
  $a \leftarrow a \times a$;
  $j \leftarrow j + 1$;
fin
retourner *[a]*

Algorithme 2 : TestRedu$(f(X) = X^3 + pX^2 + qX + r, car)$

Entrées : p, q, r, car : entier
$TRed \leftarrow faux$;
$i \leftarrow 1$;
si $(r = 0)$ **alors**
  $TRed \leftarrow vrai$;
fin
si $(car = 0 \ et \ r \neq 0)$ **alors**
  si $(r < 0)$ **alors**
    $r \leftarrow r \times (-1)$
  fin
  tant que $(i \leq r \ et \ TRed = faux)$ **faire**
    si $(i \mod r = 0)$ **alors**
      si $(f(i) = 0 \ ou \ f(-i) = 0)$ **alors**
        $TRed \leftarrow vrai$;
      fin
    fin
    $i \leftarrow i + 1$;
  fin
fin
sinon si $(car \neq 0 \ et \ r \neq 0)$ **alors**
  $i \leftarrow 0$;
  tant que $(i < car \ et \ TRed = faux)$ **faire**
    si $(f(i) \mod car = 0)$ **alors**
      $TRed \leftarrow vrai$;
    fin
    $i \leftarrow i + 1$;
  fin
fin
retourner *[TRed]*

Algorithme 3 : Disc$(f(X) = X^3 + pX^2 + qX + r, car)$

Entrées : p, q, r, car : entier
$Det \leftarrow 18pqr - 4Pow(p, 3)r + Pow(p, 2)Pow(q, 2) - 4Pow(q, 3) - 27Pow(r, 2)$;
si $(car \neq 0)$ **alors**
  $det \leftarrow det \mod car$;
fin
retourner *[det]*

Algorithme 4 : TestCarre(D_f, car)

Entrées : $disc, car$: entier
$carre \leftarrow faux$;
$i \leftarrow 0$;
$j \leftarrow 0$;
si *(*$car = 0$*)* **alors**
  si *(*$\sqrt{disc} \in \mathbb{Z}$*)* **alors**
    $carre \leftarrow vrai$;
  sinon
    $carre \leftarrow faux$;
  fin
sinon
  tant que *(*$i < car$ *et* $carre = faux$*)* **faire**
    $j \leftarrow Pow(i, 2)$;
    si *(*$j \mod car = 0$*)* **alors**
      $carre \leftarrow vrai$;
    sinon
      $carre \leftarrow faux$;
    fin
    $i \leftarrow i + 1$;
  fin
fin
retourner *[carre]*

Algorithme 5 : RechercheRacine($f(X), car$)

Entrées : p, q, r, car : entier
$trouve \leftarrow faux$;
$i \leftarrow 0$;
$racine \leftarrow 0$;
si *(*$car = 0$*)* **alors**
  tant que *(*$trouve = faux$*)* **faire**
    si *(*$f(i) = 0$*)* **alors**
      $trouve \leftarrow vrai$;
      $racine \leftarrow i$;
    fin
    sinon si *(*$f(-i) = 0$*)* **alors**
      $trouve \leftarrow vrai$;
      $racine \leftarrow -i$;
    fin
    sinon
      $trouve \leftarrow faux$;
      $i \leftarrow i + 1$;
    fin
  fin
sinon
  tant que *(*$trouve = faux$ *et* $i < car$*)* **faire**
    si *(*$f(i) \mod car = 0$*)* **alors**
      $trouve \leftarrow vrai$;
      $racine \leftarrow i$;
    sinon
      $trouve \leftarrow faux$;
      $i \leftarrow i + 1$;
    fin
  fin
fin
retourner *[racine]*

Algorithme 6 : GroupeGaloisCubique

Entrées : p, q, r, car : entier
si *(*$TestRedu(p, q, r, car) = faux$ *et* $TestCarre(Disc(p, q, r, car), car) = faux$ *)*
alors
  Résultat : Le groupe de Galois $\simeq S_3$
fin
si *(*$TestRedu(p, q, r, car) = faux$ *et* $TestCarre(Disc(p, q, r, car), car) = vrai$ *)* **alors**
  Résultat : Le groupe de Galois $\simeq A_3$
fin

Algorithme 7 : GroupeGaloisQuartique

Entrées : p, q, r, s, car : entier
$a \leftarrow -q$;
$b \leftarrow pr - 4s$;
$c \leftarrow Pow(p, 2)s + Pow(r, 2) - qs$;
si $car \neq 0$ **alors**
  $a \leftarrow a \mod car$;
  $b \leftarrow b \mod car$;
  $c \leftarrow c \mod car$;
fin
$\phi(X) = X^3 + aX^2 + bX + c$;
$\Delta \leftarrow Disc(a, b, c, car)$;
si $(TestCarre(Disc(a, b, c, car), car) = vrai)$ **alors**
  si $(TestRedu(a, b, c, car) = faux)$ **alors**
    Résultat : Le groupe de Galois $\simeq A_4$
  sinon
    Résultat : Le groupe de Galois $\simeq V$
  fin
sinon
  si $(TestRedu(a, b, c, car) = faux)$ **alors**
    Résultat : Le groupe de Galois $\simeq S_4$
  sinon
    $\beta \leftarrow RechercheRacine(a, b, c, car)$;
    $f_1(X) = X^2 + pX + (q - \beta)$;
    $f_2(X) = X^2 - \beta X + s$;
    $\Delta_1 \leftarrow (Pow(p, 2) - 4(q - \beta)) \times \Delta$;
    $\Delta_2 \leftarrow (Pow(\beta, 2) - 4s) \times \Delta$;
    si $(Testcarre(\Delta_1, car) = vrai \ et \ Testcarre(\Delta_2, car) = vrai)$ **alors**
      Résultat : Le groupe de Galois $\simeq \mathbb{Z}/4\mathbb{Z}$
    sinon
      Résultat : Le groupe de Galois $\simeq D_4$
    fin
  fin
fin

Conclusion

Bibliographie

[1] J. Calais, *Extension de corps - Théorie de Galois.*, Ellipses,(2006).

[2] G. Gras et M-N. Gras, *Algèbre et Arithmétique fondamentales.*, Ellipses,(2018).

[3] J. Calais, *Éléments de théorie des groupes.*, Ellipses,(2006).

[4] J. Calais, *Éléments de théorie des anneaux - anneaux commutatifs.*, Ellipses,(2006).

[5] I. Gozard, *Théorie de Galois.*, Ellipses,(1997).

[6] C. Mutafian, *Équations algébriques et théorie de Galois.*, THÈMES VUIBERT UNIVERSITÉ MATHÉMATIQUES,(1997).

[7] I. Kaplansky, *Fields and Rings.*, 2nd ed., Univ. of Chicago Press,(1972).

[8] L-C. Kappe et B. Warren , *An Elementary Test for the Galois Group of a Quartic Polynomial.*, Amer.Math. Monthly 96,(1989).pp.133–137.

[9] P. Morandi, *Field and Galois Theory.* Graduate Texts in Mathematics book series. GTM, Volume 167, Springer(1996).pp.29–30.