N° d'ordre :
N° de série :

UNIVERSITE KASDI MERBAH - OUARGLA

Faculté de Mathématiques et sciences de la matière

Département de Mathématiques

MASTER
Spécialité : Mathématiques
Option : Algèbre et Géométrie

Par : **ACHOURI KHAMIS**

Thème :

GROUPE DE GALOIS

Soutenue le : 01 Juin 2017

Jury composé de :

GURBOUSSA yassine	**M.A. Univ KASDI Merbah Ouargla**	**Président**
BOUSSAID mohmmed	**M.A. Univ KASDI Merbah Ouargla**	**Examinateur**
YOUMBAI mohmmed laid	**M.A. Univ KASDI Merbah Ouargla**	**Examinateur**
BEN MOUSSA mohmmed	**M.A. Univ KASDI Merbah Ouargla**	**Examinateur**
BENZEGHLI Brahim	**M.C. Univ MOSTAFA Ben Boulaid Batna 2**	**Encadreur**

Année universitaire : 2016 - 2017

Table des matières

Dédicace

Je dédié ce modeste travail

A

Ma très chère mère, mon très cher père
A Mes chères sœurs, et à Mes chères frères. A toute ma famille.

A tous mes amis : sliman, naimi, yakoub, nouredine, hamdan, hamida, hamid, abbas, saddik, ali, abdelah, lotefi, hicham, khaled, ilyas, junid,...

A tous ceux qui sèment le bonheur sur mon chemin.

A tous le groupe d'algèbre et géométrie

A tous les habitants de OURAGLA , et BATNA.

A la fin je dédie tout ce qu'ils ont m'aider dans mon parcours scolaire de proche où de loin.

Remerciement

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

Je tiens à remercier Mon Encadreur de mémoire Dr. BENZEGHLI Brahim pour ses orientations et son accompagnement tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie.

Je tiens à remercier mes enseignants d'algèbre et géométrie Dr BAHYOU Mohammed Amine, Dr GEURBOUSSA Yassine , Dr BEN MOUSSA mohammed tayeb, Dr YOUMBAI Mohammed Laid, Dr AMIER belkhier, Dr BOUSAID mohmmed .

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

Je tiens aussi à remercier nos enseignants de département de mathématique université kasdi merbah ouaragla et département mathématique de hadj lakhder batna pour la formation que j'ai reçue.

Derniers remerciements et qui ne sont pas les moindres, vont à tous ceux qui ont contribué de prés où de loin pour l'aboutissement de ce travail.

Introduction

Dans ce mémoire, nous allons exposer une partie de la théorie de Galois, c'est la résolutions des équations par radicaux.

On a commencé par un premier chapitre dont le quel on a donner quelques notions de base sur les groupes et surtout on a parler de la résolubilité des groupes, qui va nous servir plus tard dans le théorème de Galois.

Le deuxième et troisième chapitres contiennent les notions des anneaux et des corps, et surtout les anneaux des polynômes ainsi que la théorie des corps finis. On aussi donner quelques critères d'irréductibilité des polynômes sur des corps finis.

Les extensions des corps et la notion du groupe de Galois sont mentionnés dans le quatrième chapitre, dont on a parler des corps de décompositions et les extensions normales, séparables et cyclotomiques pour terminer avec l'extension galoisienne .

Le cinquième chapitres est consacré à la résolution des équations par radicaux dont on a commencé par la notion de l'extension radicale et la résolubilité des polynômes par radicaux. On a aussi donner des exemples sur des polynômes non résoluble par radicaux et on a terminer par citer des exemples comment résoudre des polynômes de deuxième, troisième et quatrième degré par radicaux.

Vu l'incroyable vie d'Avariste Galois, on a ajouter la biographie de Galois dans un petit annexe.

1 Les groupes

1.1 Généralités sur les groupes

Définition 1.1 *Un groupe est la donnée d'un ensemble non vide G et d'une loi de composition interne*

$$G \times G \to G$$

$$(x, y) \to x * y$$

vérifiant les propriétés suivantes :

i) $\forall x, y, z \in G, (x * y) * z = x * (y * z)$

ii) $\exists e \in G$, *tel que* $\forall x \in G, x * e = e * x = x$

iii) $\forall x \in G, \exists x' \in G$ *tel que* $x * x' = x' * x = e$.

Définition 1.2 *Si* $(G, *)$ *est un groupe tel que la loi* $*$ *satisfasse à la propriété* $\forall x, y \in G, x * y = y * x$, *le groupe* $(G, *)$ *est dit commutatif où encore abélien.*

Exemple 1.1 *les groupes* $(\mathbb{Z}, +), (Q^*, \times)$ *sont abéliens.*

1.2 Sous-groupes

Définition 1.3 *Un sous-ensemble non vide H d'un groupe G est un sous-groupe de G si, muni de la loi induite par celle de G, c'est un groupe.*

Proposition 1.1 *Un sous-ensemble non vide H d'un groupe G est un sous-groupe de G si et seulement si*

i) $\forall (x, y) \in H \times H, xy \in H$.

ii) $\forall x \in H, x^{-1} \in H$.

Définition 1.4 *On appelle sous-groupe propre d'un groupe G tout sous-groupe distinct de G et de l'élément neutre.*

Notation. Si H est un sous-groupe de G, on notera $H < G$.

Exemple 1.2 *a)* $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

b) $(\mathbb{Q}^*, \times) < (\mathbb{R}^*, \times) < (\mathbb{C}^*, \times)$.

Proposition 1.2 *les sous-groupes de* $(\mathbb{Z}, +)$ *sont les* $nZ = nx, x \in \mathbb{Z}$, *pour n parcourant N.*

Proposition 1.3 *Soient G un groupe, I un ensemble non vide et* $\{H_i\}_{i \in I}$ *une famille de sous-groupe de G. Alors* $\bigcap_{i \in I} H_i$ *est un sous-groupe de G.*

1.3 Sous-groupes engendrés

Définition 1.5 *Soient G un groupe et S une partie de G. On appelle sous-groupe engendré par S, et on note $\langle S \rangle$, le plus petit (pour la relation d'inclusion) sous-groupe de G contenant S.*

Proposition 1.4 *C'est l'intersection de tous les sous-groupes de G qui contiennent S.*

Proposition 1.5 *Soient G un groupe et S une partie non vide de G. On a*

$$\langle S \rangle = x_1 ... x_n, n \in \mathbb{H}^*, x_i \in S où x_i^{-1} \in S, \forall i, 1 \leq i \leq n$$

Définition 1.6 *Si S est une partie non vide d'un groupe G, telle que $\langle S \rangle = G$, on dit que S est une partie génératrice de G, où que S est un ensemble de générateurs de G, où que S engendre G.*

1.4 Ordre d'un groupe, d'un élément

Définition 1.7 *Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments dans ce cas, le cardinal de G s'appelle l'ordre du groupe G et est noté $|G|$. Soient G un groupe et x un élément de G. On appelle ordre de x, qu'on note $o(x)$, le cardinal de $\langle x \rangle$. Si ce cardinal est infini, on dit que x est d'ordre infini.*

Remarque 1.1
a) Soient G un groupe fini et x un élément de G, alors $o(x) \leq |G|$.
b) Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1.
c) Dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini.

Proposition 1.6 *Soient G un groupe et x un élément d'ordre fini de G.Alors $o(x)$ est le plus petit entier positif s tel que $x^s = 1_G$.*

Définition 1.8 *Soient $(G, .)$ et $(G', *)$ deux groupes.Un morphisme (où homomorphisme) de groupes de G dans G' est une application $f : G \to G'$ vérifiant :*

$$\forall (x, y) \in G \times G, f(x, y) = f(x) * f(y)$$

.

Notation. On note $Hom(G, G')$ l'ensemble des morphismes de groupes de G dans G'. On note $End(G)$ l'ensemble des morphismes de groupes de G dans lui-même, qu'on appelle endomorphismes de G.

Proposition 1.7 *Tout élément f de $Hom(G, G')$ vérifie les propriétés suivantes :*

i) $f(1_G) = 1'_G$
ii) $f(x^{-1}) = f(x)^{-1}$ *pour tout élément x de G*
iii) $H < G \Rightarrow f(H) < G'$
iv) $H' < G' \Rightarrow f^{-1}(H') < G$ *avec* $f^{-1}(H') = \{x \in G, f(x) \in H'\}$.

Définition 1.9 *Pour tout élément f de* $Hom(G, G')$, $f(G)$ *est un sous-groupe de G' appelé image de f et noté* $Im(f)$; $f^{-1}(\{1'_G\})$ *est un sous-groupe de G appelé noyau de f et noté* $Ker(f)$.

Définition 1.10 *Un élément f de* $Hom(G, G')$ *est un isomorphisme s'il existe un morphisme réciproque g, i.e. un élément g de* $Hom(G', G)$ *tel que* $g \circ f = id_G$ *et* $f \circ g = id'_G$.

Définition 1.11 *Deux groupes G et G' sont isomorphes s'il existe un isomorphisme f de G sur G'.*

1.5 Produit direct de groupes

Proposition 1.8 *Soient G un groupe, H et K deux sous-groupes de G.Alors HK est un sous-groupe de G si et seulement si* $HK = KH$.

Remarque 1.2 *Si G est abélien, pour tous sous-groupe de H et K, HK est un sous-groupe de G.*

Définition 1.12 *le groupe défini ci-dessus est le produit direct des groupes* G_1 *et* G_2, *noté* $G_1 \times G_2$.

1.6 Groupes libres

Définition 1.13 *a) Soient G un groupe et S une partie de G. le groupe G est dit libre de base S si tout élément x de G s'écrit de manière unique*

$$x = s_{i_1}^{n_i} ... s_{i_k}^{n_k}$$

avec $k, i_1, ..., i_k \in \mathbb{N}, n_1, ..., n_k \in \mathbb{Z}, s_{i_1}, ..., s_{i_k} \in S$, *tels que* $s_{i_j} \neq s_{i_{j+1}}$. *si on dit alors que S est une famille génératrice libre de G, où encore que S est une base de G.*

b) un groupe G est dit libre s'il possède une base.

c) si le groupe G possède une base finie , il est dit libre de type fini.

1.7 Groupes opérant sur un ensmble

Définition 1.14 *Soit G un groupe (noté multiplicativement, d'élément neutre 1) et soit E un ensemble non vide. une opération à gauche de G sur E est la donnée d'une application*

$$G \times E \to E, (g, x) \longmapsto g.x$$

satisfaisant aux deux conditions suivantes :

i) $\forall (g_1 g_2) \in G \times G, \forall x \in E, (g_1 g_2).x = g_1.(g_2.x)$

ii) $\forall x \in E, 1.x = x.$

Définition 1.15 *Soit G un groupe opérant sur un ensemble E. le noyau de l'action est le noyau de l'homomorphisme de groupes* $\gamma : G \to S_E$ *définissant l'action de G sur E.*

1.8 Stabilisateurs-Orbites

Définition 1.16 *Soit G un groupe opérant sur un ensemble E et soit x un élément fixé de E. l'ensemble* $Stab_G(x) = \{g \in G : gx = x\}$ *est un sous-groupe de G, appelé le stabilisateur de x.*

Définition 1.17 *Soit G un groupe opérant sur un ensemble E et soit x un élément fixé de E. L'ensemble* $\Omega_x = \{g.x, g \in G\}$ *est appelé l'orbite de x sous l'action de G.*

1.9 Action de groupes

Soit E un ensemble et Bij(E) l'ensemble des bijections de E. Alors Bij(E) est un groupe pour la loi de composition, l'élément neutre étant l'identité de E et l'inverse d'une bijection sa bijection réciproque. Il est appelé groupe des permutations de E.

Définition 1.18 *Soit E un ensemble et G un groupe. Une action de G sur E est la donnée d'un morphisme de groupes* $\phi : G \to Bij(E)$.

1.10 Groupes résolubles

Définition 1.19 *Un groupe G résoluble s'il admet une suite de composition dont les quotients sont des groupes abéliens*

Proposition 1.9 *Le groupe G est résoluble si et seulement s'il existe un entier* $n \geq 0$ *tel que* $D_n(G) = \{e\}$.

Exemple 1.3 *Tout groupe abélien est résoluble.*

Théorème 1.1 *Soit G un groupe.*
(i) Si G est résoluble tout sous-groupe de G est résoluble.
(ii) Si H est un sous-groupe normal de G, alors G est résoluble si et seulement si H et G/H sont résoluble.

Proposition 1.10 *Les groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Corollaire 1.1 *Les groupes S_n, pour $n \geq 5$, ne sont pas résoluble.*

Corollaire 1.2 *Si p est un nombre premier, tout p-groupe fini est résoluble.*

2 Les anneaux et les corps

2.1 Anneaux

Définition 2.1 *Un anneau est un ensemble A muni de deux applications $+ : A \times A \to A$ et $\times : A \times A \to A$ commutatives telles que $(A, +)$ est un groupe, $\times$ est associative, munie d'un élément neutre, distributive sur $+ : x \times (y + z) = x \times y + x \times z$ pour tous $x, y, z \in A$.*

Définition 2.2 *Un corps est un anneau non nul dans lequel tout élément non nul admet un inverse pour $\times$.*

Exemple 2.1 *L'ensemble des entiers relatifs $\mathbb{Z}$,*
des entiers modulo n (noté $\mathbb{Z}/n\mathbb{Z}$), les fonctions d'un ensemble à valeurs réelles,
les séries entières convergentes (munis des lois usuelles) sont des exemples d'anneaux, mais pas des corps en général.
L'ensemble $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p premier est un corps, comme les ensembles $\mathbb{Q}$ des nombres rationnels,
$\mathbb{R}$, $\mathbb{C}$ des nombres réels, complexes (munis des lois usuelles).

Définition 2.3 *Un morphisme d'anneaux $f : A \to B$ est une application telle que $f(1) = 1$ et que vérifie $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$ pour tous $a, b \in A$. Son noyau $Ker(f) \subset A$ est l'ensemble des éléments annulés par f. L'ensemble de ces morphismes est noté $Hom(A, B)$*

Définition 2.4 *Un idéal I d'un anneau A est un sous-groupe de A pour $+$ tel que $xy \in I$ pour tous $x \in A, y \in I$.*

2.1.1 Anneau des polynômes

Soit A un anneau. Alors considérons l'ensemble $A[X]$ des polynômes à une variable à coefficients dans A. Muni de l'addition et la multiplication des polynômes, $A[X]$ a une structure naturelle d'anneau. Lorsque $A = k$ est un corps, on dispose de la division euclidienne dans $k[X]$: pour tous $A, B \in k[X]$ avec $B \neq 0$, il existe un unique couple (Q, R) de polynômes tels que $A = QB + R$ et $deg(R) < deg(B)$.

2.1.2 Morphisme de corps

Proposition 2.1 *Le seul idéal non nul d'un corps est le corps lui-même.*

Proposition 2.2 *Un morphisme de corps est toujours injectif.*

Définition 2.5 *Une extension d'un corps K est un corps K' contenant K.*

2.1.3 Anneaux quotients

Proposition 2.3 *A/I muni des lois + et × est un anneau. Le neutre de + est $\overline{0}$ et le neutre de × est $\overline{1}$.*

Définissons la surjection canonique

$$\pi : A \twoheadrightarrow A/I$$

par $a \mapsto \overline{a}$(le symbole$\twoheadrightarrow$ signifie que l'application est surjective). On voit $\overline{a} = \pi(a)$ comme la classe A modulo I, exactement comme en arithmétique usuelle.

Proposition 2.4 *π est un morphisme surjectif d'anneaux de noyau $Ker(\pi) = I$.*

Preuve : On a pour $a, a' \in A$

$$\pi(1) = \overline{1}, \overline{a}.\overline{a'} = \overline{a.a'}, \overline{a + a'} = \overline{a} + \overline{a'}$$

donc π est un morphisme d'anneaux. Il est clairement surjectif. Pour $a \in Ker(\pi)$, on a $\overline{a} = \overline{0}$, c'est-à-dire $a \in I$. Réciproquement, chaque $a \in I$ vérifie $\overline{a} = I$.

Remarque 2.1 *Si $f : A \to B$ est un morphisme d'anneaux, on a donc une factorisation canonique $\overline{f} : A/Ker(f) \to B$ de f à travers $A \to A/Ker(f)$ puisque $f(Ker(f)) = 0$. Comme on a précisément le noyau de f, celui de $\overline{f}$ est nul de sorte que $\overline{f}$ est injective. Si f est supposée surjective, on a donc un isomorphisme canonique $\overline{f} : A/Ker(f) \xrightarrow{\sim} B$.*

2.1.4 Caractéristique

Lemme 2.1 *Soit A un anneau. Il existe un unique morphisme d'anneaux $\gamma : \mathbb{Z} \to A$.*

Preuve : Un tel morphisme γ vérifie pour $n \geq 0, \gamma(n) = 1 + ... + 1$ n fois, et pour $n \leq 0, \gamma(n) = -1 - 1 - ... - 1(-n)$ fois. Il est donc unique. De plus ces formules définissent un morphisme d'anneaux. Le noyau de γ est un idéal de $\mathbb{Z}$. Il existe donc un unique entier $n \geq 0$ tel que $Ker(\gamma) = n\mathbb{Z}$.

Définition 2.6 *L'unique entier $n \geq 0$ tel que $Ker(\gamma) = n\mathbb{Z}$ est appelé caractéristique de A.*

Exemple 2.2 *la caractéristique de $\mathbb{Z}$ est nulle, la caractéristique de $\mathbb{Z}/n\mathbb{Z}$ est n.*

Proposition 2.5 *La caractérstique d'un corps k est nulle où est un nombre premier.*

Proposition 2.6 *Soit k un corps. Si la caractéristique de k est nulle, alors k est infini et contient un sous-corps isomorphe à $\mathbb{Q}$. Si la caractéristique de k est un nombre premier p, alors k contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ appelé sous-corps premier de k.*

2.1.5 Anneaux intègres,propriétes des idéaux

Définition 2.7 *On dit qu'un anneau A est intègre si il est non nul et si le produit de deux éléments non nuls de A est non nul.*

Définition 2.8 *Soit I un idéal d'un anneau A. On suppose $I \neq A$.*
- *On dit que I est premier si A/I est intègre.*
- *On dit que I est maximal si A/I est un corps.*

Lemme 2.2 *L'image inverse d'un idéal premier par un morphisme d'anneaux est un idéal premier.*

Définition 2.9 *Un élément a d'un anneau intègre est dit irréductible s'il n'est ni nul ni inversible et si ses diviseurs sont où bien inversibles où bien multiples de a.*

Proposition 2.7 *Un idéal propre d'un anneau A est maximal si et seulement si le seul idéal qui le contient strictement est A.*

Exemple 2.3 *Soit k un corps et $P \in k[X]$. Alors l'anneau $k[X]/(P)$ est un corps si seulement si P est un polynôme non nul irréductible. Par exemple, pour $k = \mathbb{R}$ et $P(X) = X^2 + 1$ irréductible dans $\mathbb{R}[X]$, on obtient le corps*

$$(\mathbb{R}[X]/(X^2 + 1)) \simeq \mathbb{C}$$

des nombres complexes

Définition 2.10 *Un anneau intègre A tel que tout idéal de A est engendré par un élément est dit principal.*

Lemme 2.3 *Soit A un anneau principal et a un élément non nul de A. Les 3 propriétés suivantes sont équivalentes :*

1. *a est irréductible ;*
2. *$(a) = aA$ est premier ;*
3. *$(a) = aA$ est maximal.*

Proposition 2.8 *Soit $n > 0$ un entier. Alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. Ceci équivaut aussi à $\mathbb{Z}/n\mathbb{Z}$ intègre.*

2.1.6 Le lemme Chinois

On sait que les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes si n et m sont premiers entre eux. Cette dernière condition peut s'écrire aussi $(n) + (m) = \mathbb{Z}$ d'après l'identité de Bézout. Plus généralement, supposons qu'on ait des idéaux $I_1, ..., I_n$ d'un anneau A, deux à deux étrangers, i.e tels que $I_i + I_j = A$ pour $i \neq j$.

Lemme 2.4 (Lemme Chinois) *Sous ces conditions, l'application canonique $A \to \prod_{1 \leq j \leq n} A/I_j$ se factorise à travers $\cap_{1 \leq j \leq n} I_j$ pour donner un isomorphisme*

$$A/(I_1 \cap ... \cap I_n) \xrightarrow{\sim} \prod_{1 \leq j \leq n} A/I_j$$

De plus, on a

$$I_1 \cap ... \cap I_n = I_1 ... I_n$$

2.1.7 Le morphisme de Frobenius

Théorème 2.1 *(Morphisme de Frobenius) Soit p un nombre premier et A un anneau de caractéristique p. Alors l'application $F : a \mapsto a^p$ définit un endomorphisme de l'anneau A.*

2.2 Les corps

2.2.1 Corps

Définition 2.11 *On appelle k corps tout anneau non nul dans lequel tout élément non nul est inversible.*

Proposition 2.9 *Soit k un corps. alors k est un anneau intègre*

Proposition 2.10 *Soit k un anneau. k est un corps si et seulement si les seuls idéaux de k sont* (0) *et k.*

Proposition 2.11 *Soit* $n \in \mathbb{N}, n \geq 2$. *Les conditions suivantes sont équivalentes :*

i) n est un nombre premier ;
ii) $\mathbb{Z}/n\mathbb{Z}$ *est un anneau intègre ;*
iii) $\mathbb{Z}/n\mathbb{Z}$ *est un corps.*

2.2.2 Sous-corps

Définition 2.12 *Soit k un corps. Soit P une partie de k. Les conditions suivantes sont équivalentes :*

i) P est non vide, est une partie stable (pour + et $\times$*) de k, et P muni des lois induites par celles de k est lui-même un corps ;*
ii) P est un sous-anneau de $k, 1 \in P$, *et*$(x \in P \Rightarrow x^{-1} \in P)$ *;*
iii) P est un sous-groupe de $(k, +)$ *et* $P^* = P \setminus 0$ *est un sous-groupe du groupe multiplicatif* $(k^*, \times)$.

On dit alors que P est un sous-corps de k

Exemple 2.4 $\mathbb{Q}$ *est un sous-corps de* $\mathbb{R}$, $\mathbb{R}$ *est un sous-corps de* $\mathbb{C}$.

Proposition 2.12 *Soit k un corps.Toute intersection de sous-corps de k est un sous-corps de k.*

2.2.3 Sous-corps premier d'un corps

Définition 2.13 (Corps premier) *Un corps K est dit premier si et seulement si K n'a pas d'autre sous-corps que lui-même.*

Proposition 2.13 *Soit K un corps, P son sous-corps premier, et c sa caractéristique. On a :*

- *Ou bien* $c = 0$ *et alors P est isomorphe à* $\mathbb{Q}$.
- *Ou bien c est un nombre premier p et alors P est isomorphe à* F_p.

Proposition 2.14 *Soit p un nombre premier. Tout corps fini de cardinal p est isomorphe à F_p.*

Définition 2.14 *On dit qu'un corps K est premier s'il ne contient aucun sous-corps distinct de lui-même.*

3 Les corps finis

3.1 Cardinal d'un corps fini

Rappels :

a) Tout corps fini (c'est-à-dire de cardinal fini) est nécessairement de caractéristique non nulle.

b) Pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p et de caractéristique p.

c) Si V est un espace vectoriel sur un corps K, alors (voir un cours d'algèbre Linéaire)

$$dim_K V = n < \infty \Longleftrightarrow V \simeq K^n$$

.

Théorème 3.1 *Si K est un corps fini de caractéristique p, il existe alors un entier $n \geq 1$ tel que $|K| = p^n$.*

Proposition 3.1 *Tout anneau intègre ayant un nombre fini $n \geq 2$ d'éléments est un corps.*

Théorème 3.2 *Soit F un corps fini.Alors :*

- *Sa caractéristique est un nombre premier p.*
- *Son sous-corps premier est isomorphe à F_p.*
- *Il existe $n \in \mathbb{N}^*$ tel que $Card(F) = p^n$.*

Théorème 3.3 *Tout corps fini est commutatif.*

Théorème 3.4 *Soit K un corps commutatif. Tout sous-groupe fini du groupe multiplicatif K^* est cyclique.*

Corollaire 3.1 *Le groupe multiplicatif d'un corps fini est cyclique.*

Théorème 3.5 *(de l'élément primitif pour les corps finis) Soit K un corps fini. Soit L une extension de degré fini de K. Alors L est monogène. (Autrement dit, il existe $\xi \in L$ tel que $L = K(\xi)$:un tel élément ξ est appelé un élément primitif de l'extension L de K).*

Proposition 3.2 (Cas particulier du théorème de DIRICHLET) *a) $\Phi_{n(X)}$ désigne le n-i ème polynôme cyclotomique. Si un nombre premier p divise $\Phi_n(a)$, où a est entier, mais aucun $\Phi_d(a)$ où d décrit l'ensemble des diviseurs stricts de n, alors $p \equiv 1[mod n]$.*

b) Il existe une infinité de nombres premiers de la forme $\lambda n + 1, \lambda \in \mathbb{N}^*$.

3.2 Existence et unicité d'un corps de cardinal primaire

Proposition 3.3 *Soit K un corps de caractéristique $p \in P$. L'application $F : K \to K, x \to x^p$ est un F_p-endomorphisme du corps K, appelé endomorphisme de FROBENIUS de K.*

- *Si K est fini, F est un automorphisme.*
- *Si $K = F_p, F$ est l'identité.*

Corollaire 3.2 *Dans un corps fini de caractéristique p, chaque élément admet exactement une racine p-i ème.*

Théorème 3.6 *Soient p un nombre premier et $n \in N^*$. On note $q = p^n$.*

1. *Il existe un corps fini à q éléments.Il est corps de décomposition sur F_p du polynôme $X^p - X$.*
2. *Si F et F' sont deux corps à q éléments, ils sont F_p-isomorphes.*

3.3 Groupe des automorphisme d'un corps fini

Théorème 3.7 *Soit F un corps fini, de caractéristique p, de cardinal $q = p^n$. Le groupe des automorphismes de F est d'ordre $n = [F : F_p] = log_{caract(F)} card(F)$. Il est cyclique.Il est engendré par l'automorphisme de FROBENIUS : $G : F \to F, x \to G(x) = x^p$.*

3.4 Polynômes irréductibles sur F_p

Théorème 3.8 *Soient p premier, $n \in N^*$. Notons $q = p^n$.$F_p = F_p[X]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur F_p.*

Corollaire 3.3 *· Il existe des polynômes irréductibles de tout degré dans $F_p[X]$. · Si π est un polynôme irréductible de degré n sur F_p, alors $\pi(X)$ divise $X^{p^n} - X$ dans $F_p[X]$, donc est scindé sur F_p^n, donc son corps de rupture $F_{p^n} = F_p[X]/(\pi)$ est aussi son corps de décomposition.*

Exemple 3.1 *Examinons les cas :*

1. *$p = 2, n = 2$:le polynôme irréductible de degré 2 sur F_2 est $X^2 + X + 1$.*

$$F_4 = F_2[X]/(X^2 + X + 1)$$

2. *$p = 2, n = 3$:les polynômes irréductibles de degré 3 sur F_2 sont $X^3 + X + 1$ et $X^3 + X^2 + 1$(il suffit de vérifier que les 6 autres polynômes de degré 3 ne sont pas irréductibles).*

$$F_8 = F_2[X]/(X^3 + X + 1)$$

3. $p = 3, n = 2$ *:les polynômes unitaires irréductibles de degré* 2 *sur* F_3 *sont* $X^2 + 1, X^2 + X - 1$ *et* $X^2 - X - 1$ *(il suffit de vérifier que les* 6 *autres polynômes unitaires de degré* 2 *ne sont pas irréductibles).*

$$F_9 = F_3[X] \diagup (X^2 + X - 1)$$

3.5 Critère d'Eisenstein

Définition 3.1 *Soit* $P(X) = a_0 + a_1 + ... + a_n X^n \in \mathbb{Z}[X]$ *et p un nombre premier. On suppose que :*

i. p *ne divise pas* a_n.

ii. p *divise* $a_0, a_1, ..., a_{n-1}$.

iii. p^2 *ne divise pas* a_0. *Alors le polynôme de* $P(X)$ *est irréductible dans* $\mathbb{Z}[X]$, *donc dans* $\mathbb{Q}[X]$.

Exemple 3.2 *Le polynome est* $X^3 + 7X^2 + 14X + 21$ *est irréductible sur* $\mathbb{Q}[X]$, *il suffit d'appliquer le critère d'Eisenstein avec le nombre premier* $p = 7$

3.6 Sous-corps d'un corps fini

Théorème 3.9 *Soient p premier,* $n \in N^*$, *et* $q = p^n$.

1. K *sous-corps de* $F_q \Rightarrow$ *il existe d diviseur de n tel que* $Card(K) = p^d$.
2. *Pour chaque diviseur d de n,* F_q *a un et un seul sous-corps de cardinal* p^d. *Ce sous-corps est isomorphe à* F_p^d.

4 Groupe de galois

4.1 Extensions de corps

4.1.1 Degré d'une extension

Définition 4.1 (Extension d'un corps) *Soit k un corps. On appelle extension de k tout corps K tel qu'il existe un homomorphisme de corps j de k dans K. La notation abréviative "K/k", dont nous userons et abuserons dans la suite, signifie : le corps K est une extension du corps k.*

Remarque 4.1
- *Si k est un sous-corps de K, alors K est une extension de k (considérer l'injection canonique $i : k \to K$).*
- *Réciproquement un homomorphisme de corps $j : k \to K$ est forcément injectif. Par conséquent, le sous-corps $k' = j(k)$ de K est isomorphe à k. Identifiant k et k', on peut donc dire que k est un sous-corps de K.*
- *En conclusion, aux notations abusives(...bien pratiques)près : $\{$ K est une extension de $k\} \iff \{k$ est un sous-corps de $K\}$.*

Exemple 4.1 $\mathbb{C}$ *est une extension de* $\mathbb{R}, \mathbb{R}$ *est une extension de* $\mathbb{Q}$.
- *Tout corps K est une extension de son sous-corps premier P. Par suite tout corps de caractéristique nulle est une extension de $\mathbb{Q}$, et tout corps de caractéristique p est une extension de F_p.*
- *Le corps $k(T)$ des fractions rationnelles à coefficients dans k est une extension de k.*

Proposition 4.1 *Soient k un corps,K une extension de k : il existe un homomorphisme de corps j de k dans K.Muni du "produit par un scalaire" défini par :$(\lambda \in k, \forall x \in K, \lambda x = j(\lambda).x), K$ est une k-algèbre.*

Définition 4.2 (Degré d'une extension) *Soient k un corps, K une extension de k. On appelle degré de l'extension K de k(ou K/k)et on note $[K : k]$, la dimension de K comme k-espace vectoriel : $[K : k] = dim_k K$.*

Remarque 4.2
- *Pour K extension de k, on a :$[K : k] = 1 \iff k = K$. En effet si $[K : k] = 1$, comme (1) est k-libre, c'est une base de K comme k-e.v ; donc $(\forall x \in K, \exists \lambda \in k; tq : x = \lambda 1)$, soit $K \subseteq k$.*
- *Le degré d'une extension peut être fini(par exemple $[\mathbb{C} : \mathbb{R}] = 2$) ou infini(par exemple $[\mathbb{R} : \mathbb{Q}] = +\infty$).*

Définition 4.3 *On appelle tour d'extension toute suite finie de corps croissante pour l'inclusion. Si $K_1 \subseteq K_2 \subseteq ... \subseteq K_r$ est une tour d'extension, alors : $(\forall (i, j) \in [1, r]^2) i \leq j \Rightarrow K_j$ est une extension de K_i.*

4.1.2 Sous-extensions d'une extension de corps

Définition 4.4 *Soient L un corps, k un sous-corps de L. On appelle sous-extension de L/k, ou corps intermédiaire de l'extension L/k, tout sous-corps H de L qui contient k, c'est-à-dire tout corps H tel que $k \subseteq H \subseteq L$.*

Proposition 4.2 *Soient L un corps, k un sous-corps de L, P une partie de L. L'ensemble des sous-corps de L qui contiennent k et P admet, au sens de l'inclusion,un plus petit élément. Ce plus petit élément est noté $k(P)$ et appelé la sous-extension de L/k engendrée par P.*

Définition 4.5 *Soit k un corps, L une extension de k. On dit que L est une extension de type fini de k si, et seulement si, il existe une partie finie $\{\alpha_1, ..., \alpha_n\}$ de L telle que $L = k(\alpha_1, ..., \alpha_n)$.*

Proposition 4.3 *Une extension L de degré fini de K est de type fini sur K.*

Définition 4.6 *Soit k un corps, L une extension de k. On dit que L est une extension monogène (où une extension simple) de k si, et seulement si, il existe un élément α de L tel que $L = k(\alpha)$. Remarquons qu'il n'y a pas alors unicité de α. Tout élément u de L tel que $L = k(u)$ est appelé un élément primitif de L/k*

Exemple 4.2 *K est une extension monogène de lui-même et pour tout $\alpha \in K, K(\alpha) = K$: tout élément est primitif.*

Proposition 4.4 (Extension de degré premier) *Soient k un corps, L une extension de k avec $[L : k]$ premier. Alors L est une extension monogène de k.*

4.1.3 Groupe de Galois d'une extension

Définition 4.7 *Soient L et M deux extensions d'un même corps K. On appelle K-homomorphisme (de corps) de L dans M tout homomorphisme (de corps) de L dans M qui laisse invariant chaque élément de K, c'est-à-dire toute application $f : L \to M$ qui vérifie :*

- $\forall (x, y) \in L^2, f(x + y) = f(x) + f(y)$ *et* $f(xy) = f(x)f(y)$
- $f(1_L) = 1_M$
- $\forall u \in K, f(u) = u$.

· Lorsque $L = M$, on dit que f est un K-endomorphisme de L.
· Lorsque f est bijective (c'est-à-dire surjective),on dit que f est un K-isomorphisme de L dans M.

Remarque 4.3 *f K-homomorphisme de L dans $M \Leftrightarrow f$ homomorphisme de K-algèbres de L dans M.*

Définition 4.8 (Automorphisme de corps) *Soit K un corps. On appelle automorphisme du corps K tout homomorphisme de corps de K dans K qui est bijectif, c'est-à-dire toute application bijective $\sigma : K \to K$ qui vérifie :*

- $\forall (x,y) \in K^2, \sigma(x+y) = \sigma(x) + \sigma(y)$ *et* $\sigma(xy) = \sigma(x)\sigma(y)$
- $\sigma(1_K) = 1_K$.

Proposition 4.5 *L'ensemble $Aut(K)$ des automorphismes du corps K forme un groupe pour la loi $\circ$ de composition des application.*

Définition 4.9 *Soient k un corps, L une extension de k. On appelle k-automorphisme de k-algèbre de L, c'est-à-dire tout automorphisme du corps L qui laisse invariant chaque élément de k, c'est-à-dire toute application bijective $\sigma : L \to L$ qui vérifie :*

- $\forall (x,y) \in L^2, \sigma(x+y) = \sigma(x) + \sigma(y)$ *et* $\sigma(xy) = \sigma(x)\sigma(y)$
- $\sigma(1_L) = 1_L$
- $\forall u \in k, \sigma(u) = u$

Définition 4.10 *On note $Gal(L/k)$ l'ensemble des k-automorphismes du corps L. $Gal(L/k)$ est un groupe pour la loi $\circ$ de composition des applications. On l'appelle le groupe de Galois de L sur k.*

Lemme 4.1 *Soit f un endomorphisme de corps de K. L'ensemble $\{x \in K / f(x) = x\}$ est un sous-corps de K. On le note $Fix(f)$ où $Inv(f)$.*

Preuve $f(1) = 1$, soit :$1 \in Fix(f)$. Soit $(a,b) \in (Fix(f))^2 . f(a) = a$ et $f(b) = b$, donc $f(a+b) = f(a) + f(b) = a + b$ et $f(ab) = f(a)f(b) = ab$. Par conséquent $a+b$ et ab appartiennent à $Fix(f)$. Soit $x \in Fix(f)$ avec $x \neq 0$. Alors $f(x) = x$. Or $f(x^{-1}) = (f(x))^{-1}$. Donc $f(x^{-1}) = x^{-1}$,c'est-à-dire $x^{-1} \in Fix(f)$.

Proposition 4.6 *Soit K un corps, P son sous-corps premier. $Aut(K) = Gal(K/P)$.*

Exemple 4.3 *$Aut(R) = Gal(\mathbb{R}/\mathbb{Q}) = \{id_{\mathbb{R}}\}$.*

Exemple 4.4 *Soit R le corps des racine du polynôme $X^4 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$. Nous avons $R = \mathbb{Q}(i, \sqrt[4]{2})$. Degré de R sur $\mathbb{Q}$: Nous avons $[R : \mathbb{Q}] = [R : \mathbb{Q}(\sqrt[4]{2})][Q(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$, car $X^4 - 2$ est irréductible dans $\mathbb{Q}[X]$. $[R : \mathbb{Q}(\sqrt[4]{2})] = 2$, car $Irr(i, \mathbb{Q}(\sqrt[4]{2})) = X^2 + 1$. D'où $[R : \mathbb{Q}] = 8$. Groupe $G(R/\mathbb{Q})$: Si $\sigma \in G(R/\mathbb{Q})$, alors*

- *$\sigma(i)$ est une racine de $X^2 + 1$. Donc $\sigma(i) = \pm i$.*
- *$\sigma(\sqrt[4]{2})$ est une racine de $X^4 - 2$. Donc*

$$\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$$

où

$$\sigma(\sqrt[4]{2}) = \pm i\sqrt[4]{2}$$

Or σ est complètement déterminé par son action sur i et $\sqrt[4]{2}$ car ces éléments engendrent R sur $\mathbb{Q}$. Il en résulte que le groupe de Galois de l'extension R de $\mathbb{Q}$ est Groupe de Galois de l'extension de R/Q

$$\sigma_1 : \sigma(i) = i, \sigma(\sqrt[4]{2}) = \sqrt[4]{2}$$

$$\sigma_2 : \sigma(i) = i, \sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$$

$$\sigma_3 : \sigma(i) = i, \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$$

$$\sigma_4 : \sigma(i) = i, \sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$$

$$\sigma_5 : \sigma(i) = -i, \sigma(\sqrt[4]{2}) = \sqrt[4]{2}$$

$$\sigma_6 : \sigma(i) = -i, \sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$$

$$\sigma_7 : \sigma(i) = -i, \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$$

$$\sigma_8 : \sigma(i) = -i, \sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$$

Sous-groupe de $G(R/\mathbb{Q})$:

- *Sous-groupe d'ordre* $1 : \{\sigma_1\}$
- *Sous-groupe d'ordre* $2 : A = \{\sigma_1, \sigma_2\}, B = \{\sigma_1, \sigma_5\}, C = \{\sigma_1, \sigma_6\}, D = \{\sigma_1, \sigma_7\}$ *et* $E = \{\sigma_1, \sigma_8\}$.
- *Sous-groupe d'ordre* $4 : F = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}, G = \{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}$ *et* $H = \{\sigma_1, \sigma_2, \sigma_7, \sigma_8\}$.
- *Sous-groupe d'ordre :* $G(R/\mathbb{Q})$.

4.1.4 Ordre du groupe de Galois

Théorème 4.1 (Ordre du groupe de Galois) *Soient k un corps, L une extension de degré fini de k. Alors $|Gal(L/k)| \leq [L : k]$*

Définition 4.11 *Soit k un corps. On appelle extension galoisienne finie de k toute extension L de k de degré fini vérifiant $|Gal(L/k)| = [L : k]$.*

Exemple 4.5

1. *Tout corps est une extension galoisienne finie de lui-même (puisque $Gal(k/k) = \{id_k\}$ et $[k : k] = 1$).*
2. *$\mathbb{R}$ n'est pas une extension galoisienne de $\mathbb{Q}$.*

Définition 4.12 *Soient k un corps, L une extension de k. L'ensemble $F = \{x \in L/k \forall g \in Gal(L/k), g(x) = x\}$ est un sous-corps de L et F contient k. F est appelé le corps fixe de $Gal(L/k)$.*

Théorème 4.2 *Soient k un corps, L une extension de degré fini de k, F le corps fixe de $Gal(L/k)$.*

- $|Gal(L/k)| = |Gal(L/F)| = [L : F]$
- *L est une extension galoisienne finie de $k \Leftrightarrow k = F$.*

4.2 Extensions algébriques-extensions transcendantes

4.2.1 Extension algébrique

Définition 4.13 *Soit E/K une extension. Un élément α de E est algébrique sur K s'il existe $P(X) \in K[X]$ tel que $P(\alpha) = 0$*

Définition 4.14 *Une extension E/K est algébrique si tout élément de E est algébrique sur K.*

4.2.2 Extensions transcendantes

Définition 4.15 *Soit E/K une extension. Un élément de E qui n'est pas algébrique sur K est dit transcendant sur K. Si l'extension E n'est pas algébrique, elle est dite transcendante(sur K).*

4.3 Extensions normales-Extensions séparables

4.3.1 Corps de décomposition d'un polynôme

Définition 4.16 *Étant donné un polynôme $f(X)$, non constant dans $K[X]$, on appellera corps de rupture de f sur K, tout corps de rupture d'un facteur irréductible quelconque de $f(X)$ dans $K[X]$.*

4.3.2 Notion de corps de décomposition d'un polynôme

Théorème 4.3 *Soit $f(X)$ un polynôme non constant de $K[X]$; alors il existe une extension E de K telle que*

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

Définition 4.17 *Etant donné un polynôme $f(X)$ non constant dans $K[X]$, on appellera corps de décomposition de f sur K, toute extension E de K vérifiant les propriétés 1 et 2 du Thé.*

Proposition 4.7 *Soit E un corps de décomposition d'un polynôme $f(X)$ non constant de $K[X]$; si $n = degf > 0$ et $\alpha_1, ..., \alpha_n$ sont les racines distinctes ou confondues de f dans E, alors*

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

donc E est une extension algébrique, de degré fini sur K.

Preuve : On a

$$(K \subseteq Eet \forall i(1 \leq i \leq n), \alpha_i \in E) \Longrightarrow K(\alpha_1, ..., \alpha_n) \subseteq E. \tag{4.1}$$

Le polynôme f étant scindé sur E (Thé), dans $E[X]$, $f(X)$ s'écrit :

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

où $a \in K^*$.

Cette égalité exprime que f est scindé sur $K(\alpha_1, ..., \alpha_n)$; alors, la relation (4.1) et la proposition 4.7 du Théorème 4.3 impliquent

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

donc l'extension $E : K$ est algébrique, de degré fini.

Remarque 4.4 *Si, dans la preuve précédente $\alpha_1, ..., \alpha_m$, $m \leq n$, sont les racines distincts de $f(X)$ dans E, alors $E = K(\alpha_1, ..., \alpha_m)$.*

Corollaire 4.1 *$f(X)$ étant un polynôme non constant de $K[X]$, si $f(X)$ est scindé sur un corps L, extension de K, alors L contient un corps de décomposition de f sur K.*

Exemple 4.6
1. *Le corps $\mathbb{Q}(\sqrt[3]{2}, j) \subset \mathbb{C}$ est corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3 - 2$.*
2. *$\mathbb{C}$ est corps de décomposition sur $\mathbb{R}$, du même polynôme $X^3 - 2$.*

4.3.3 Extensions normales-Clôture normale

4.3.4 Extensions normales

Définition 4.18 *Une extension L de K est dite normale sur K, si*

i) L est algébrique sur K.

ii) Tout polynôme irréductible de $K[X]$, qui a une racine dans L, est scindé sur L.

Exemple 4.7 *1. On remarque que tout corps K est extension normale de lui-même ; en effet, K est algébrique sur K et de plus, tout polynôme irréductible de $K[X]$, qui a une racine dans K, est nécessairement de degré 1, donc est (trivialement) scindé sur K.*

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

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

Théorème 4.4 *L étant une extension de K, alors L est normale et de degré fini sur K si et seulement si L est corps de décomposition sur K d'un polynôme de $K[X]$.*

4.3.5 Clôture normale

Définition 4.19 *On appelle clôture normale d'une extension de corps $K : L$, une extension N de L telle que $K \subseteq L \subseteq N$ et*

i) N est une extension normale de K ;

ii) $(L \subseteq M \subseteq N$ et M extension normale de $K) \Longrightarrow M = N$.

4.3.6 Extensions séparables

4.3.7 Polynômes irréductibles séparables

Définition 4.20 *1. On dit qu'un polynôme irréductible de $K[X]$ est séparable sur K s'il n'a que des racines simples dans un corps de décomposition sur K.*

2. Un polynôme irréductible de $K[X]$, qui n'est pas séparable sur K, sera dit inséparable sur K.

Exemple 4.8 *Soit $X^5 - 1$ dans $\mathbb{Q}[X]$; on a*

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Le polynôme $p(X) := X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Q}$ et ses racines sont les $exp\frac{2k\pi i}{5}, 1 \leq k \leq 4$, deux à deux distinctes dans $\mathbb{C}$. Le polynôme irréductible $p(X)$ est donc séparable sur $\mathbb{Q}$.

Proposition 4.8 *Soit $f(X) \in K[X] \setminus K$ et $f'(X)$ son polynôme dérivé ; alors,*

1. $carK = 0 \Longrightarrow f'(X) \neq 0$.

2. $carK = p \neq 0 \Longrightarrow f'(X) = 0 \Leftrightarrow f(X) = g(X^p))$,

où $g(X)$ est un polynôme de $K[X]$.

Preuve : Posons $n = degf > 0$; alors dans $K[X]$,

$$(f(X) = \sum_{0 \leqslant i \leqslant n} a_i X^i, a_n \neq 0) \Longrightarrow f'(X) = \sum_{1 \leqslant i \leqslant n} i a_i X^{i-1}.$$

1. $carK = 0$; alors, $a_n \neq 0 \Longrightarrow na_n \neq 0 \Longrightarrow f'(X) \neq 0$.
2. $carK$ est un nombre premier p ; l'expression de $f'(X)$ implique

$f'(X) = 0 \Leftrightarrow \forall i(1 \leqslant i \leqslant n), ia_i = 0 \Leftrightarrow \forall i(1 \leqslant i \leqslant n), (a_i = 0$ où $p \mid i)$. On en déduit que

$f'(X) = 0 \Leftrightarrow f(X) = \sum_{0 \leqslant k \leqslant r} b_k X^{k_p}$, où $r \in \mathbb{N}^*, b_k \in K, \forall k(0 \leqslant k \leqslant r)$
$\Leftrightarrow f(X) = g(X^p)$, où $g(X) = \sum_{0 \leqslant k \leqslant r} b_k X^k$.

Théorème 4.5 *K étant un corps,*

- *Si $carK = 0$, alors tout polynôme irréductible de $K[X]$ est séparable sur K.*
- *Si $carK = p \neq 0$, alors un polynôme irréductible $f(X)$ de $K[X]$ est inséparable sur K si et*

seulement si $f(X) = g(X^p)$, où $g(X) \in K[X]$.

4.3.8 Notion d'extension séparable-Corps parfaits

Définition 4.21

1. *Un polynôme $f(X) \in K[X] \setminus K$ sera dit séparable sur K si tous ses diviseurs irréductibles sont séparables sur K.*
2. *Étant donné une extension L de K, on dit qu'un élément $\alpha \in L$ est séparable sur K si α est algébrique sur K et le polynôme $Irr_k(\alpha, X)$ est séparable sur K.*
3. *On dit qu'une extension L de K est séparable sur K(où que l'extension $L : K$ est séparable) si tout $\alpha \in L$ est séparable sur K.*
4. *Un corps K est dit parfait si toute extension algébrique de K est séparable sur K.*

Théorème 4.6 *Un corps K est parfais si et seulement si $carK = 0$ où $carK = p \neq 0$ et $K = \{a^p; a \in K\}$.*

Remarque 4.5 *Si K est un corps tel que $carK = p \neq 0$ et $K = K^p$, alors $K = K^{p^n} := \{a^{p^n}; a \in K\}$, quel que soit l'entier $n > 0$.*

Théorème 4.7 *Etant donné des extensions de corps $L : K$ et $M : L$, on a $M : K$ séparable $\Longrightarrow M : L$ et $L : K$ séparables.*

Proposition 4.9 *Soit $L : K$ une extension de degré fini, normale et séparable, alors L est corps de décomposition sur K d'un polynôme séparable.*

Théorème 4.8 (Théorème de l'élément primitif) *Soit L une extension d'un corps K telle que $[L : K] < \infty$ et $L : K$ séparable, alors L est une extension simple de K.*

Définition 4.22 *Pour une extension $L : K$ séparable et de degré fini, on dit que $\lambda \in L$ est un élément primitif, si $L = K(\lambda)$.*

4.3.9 Extensions purement inséparables

Définition 4.23 *Soit $L : K$ une extension de corps ;*

1. *Un élément $\alpha \in L$ est dit purement inséparable sur K si*
   i) α est algébrique sur K,
   ii) il existe $m \in \mathbb{N}^*$ tel que $Irr_K(\alpha, X) = (X - \alpha)^m$, dans $L(X)$.
2. *L'extension L de K est purement inséparable sur K si tout $\alpha \in L$ est purement inséparable sur K.*

Remarque 4.6 *Toute extension $L : K$ purement inséparable est une extension algébrique.*

Proposition 4.10 *Etant donné une extension de corps $L : K$, un élément $\alpha \in L$ est à la fois, purement inséparable et séparable sur K, si et seulement si $\alpha \in K$.*

Proposition 4.11 *Soit L une extension d'un corps K, et un élément $\alpha \in L$ algébrique sur K ; il existe alors $k \in \mathbb{N}$ tel que α^{p^k} est séparable sur K.*

Théorème 4.9 *Etant donné une extension L d'un corps K, un élément $\alpha \in L$ est purement inséparable sur K si et seulement s'il existe $r \in \mathbb{N}$ et $a \in K$ tels que*

$$f_\alpha(X) := Irr_K(\alpha, X) = X^{p^r} - a.$$

Théorème 4.10 *K étant un corps, si $L : K$ est une extension purement inséparable, de degré fini, alors $[L : K]$ est une puissance de p.*

Théorème 4.11 *K étant un corps, soit $a \in K \backslash K^p$; alors, pour tout entier $n \geq 0$, le polynôme $f(X) := X^{p^n} - a$ est irréductible sur K.*

Théorème 4.12 *Soit L une extension d'un corps K, alors $\alpha \in L$ est purement inséparable sur K si et seulement s'il existe $r \in \mathbb{N}$ tel que $\alpha^{p^r} \in K$.*

4.4 Polynômes et extension cyclotomique

4.4.1 Notion de racine $n^{\text{ème}}$ primitive de l'unité

Définition 4.24 *Etant donné un corps K et un entier $n \geq 1$, on appelle racine $n^{ème}$ de l'unité de K,tout $\alpha \in \overline{K}$ racine du polynôme $X^n - 1$ de $K[X]$.*

Proposition 4.12 *Les notations étant celles de la défi, si car $K = p > 0$ et $n = p^m, m \in \mathbb{N}^*$, alors, dans $\overline{K}$,1 est l'unique racine du polynôme $X^n - 1$ de $K[X]$.*

Preuve : Les hypothèses car $K = p$ et $n = p^m$ impliquent, dans $K[X]$, $X^n - 1 = X^{p^m} - 1 = (X-1)^{p^m}$, donc 1 est l'unique racine du polynôme $X^{p^m} - 1$, à l'ordre de multiplicité p^m.

Proposition 4.13 *Si un corps K et un entier $n \geq 1$ vérifient la condition de défi, alors le polynôme $X^n - 1$ a n racines distinctes dans $\overline{K}$. L'ensemble U_n, des n racines $n^{ème}$ de l'unité de K, est un sous-groupe cyclique du groupe multiplicatif $\overline{K^*} = \overline{K} \backslash 0$.*

Définition 4.25 *Etant donné un corps K et un entier $n \geq 1$ vérifiant la condition de défi, on appelle racine $n^{ème}$ primitive de l'unité de K, tout générateur du groupe cyclique U_n.*

4.4.2 Extension cyclotomiques-Polynômes cyclotomiques

Proposition 4.14 *Compte tenu des notations définies précédemment, pour tout $\omega \in \Omega_n$, le polynôme $Irr_K(\omega, X)$ est séparable et $K(\omega)$ est une extension de degré fini et normale sur K.*

4.5 Extensions galoisiennes

Définition 4.26 *L'extension K/k est dite galoisienne si elle est algébrique et si les conjugués d'un élément arbitraire de K sont dans K.*

Lemme 4.2 *Soit K/k une extension algébrique de la forme $K = k[x_1, ..., x_n]$ avec les $x_i \in K$.Alors K/k est galoisienne si et seulement si les conjugués de tous les x_i sur k sont dans K.*

Proposition 4.15 *Soit E/k une sous-extension de K/k galoisienne et supposons E parfait. Alors, K/E est galoisienne.*

Preuve : En effet, le polynôme minimal de $x \in K$ sur k est a fortiori à coefficients dans E donc x est aussi algébrique sur E. Son polynôme minimal sur k divisible par le polynôme minimal de x sur E. Donc, tous les E-conjugués de x sont aussi des k-conjugués, donc sont dans K par hypothèse.

Corollaire 4.2 *L'inclusion $Aut_k(K) \hookrightarrow Hom_k(K,\Omega)$ est bijective si et seulement si K/k est galoisienne.*

Définition 4.27 *On appelle groupe de Galois d'une extension galoisienne K/k le groupe $Gal(K/k) = Aut_k(K) = Hom_k(K,\Omega)$.*

Remarque 4.7 *Comme les conjugués de $x \in K$ sont les $\sigma(x), \sigma \in Hom_k(K,\Omega)$, si K/k est galoisienne de groupe de Galois G, les conjugués de x sont les $g(x), g \in G$.*

Lemme 4.3 *L'extension $\mathbb{C}/\mathbb{R}$ est galoisienne de groupe de Galois $Gal(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$ engendré par la conjugaison complexe.*

Preuve : On a $\mathbb{C} = \mathbb{R}[i]$ et les conjugués de i étant i et $-i$, l'extension est galoisienne. Un élément de $G = Gal(\mathbb{C}/\mathbb{R})$ est uniquement déterminé par sa valeur en i, qui ne peut-être que i où $-i$. Donc son ordre $|G|$ est 1 où 2. Or la conjugaison complexe est bien dans G et satisfait $\bar{i} = -i$, ce qui implique le résultat.

Proposition 4.16 *Soit E/k une sous-extension de l'extension galoisienne K/k avec E parfait.Alors,*

1. *$Gal(K/E)$ est un sous-groupe de $Gal(K/k)$;*

2. *Si E/k est galoisienne, la restriction des morphismes de K à E induit un morphisme*
$$Gal(K/k) \to Gal(E/k)$$
qui est surjectif. Son noyau est $Gal(K/E)$. Autrement dit, on a la suite exacte
$$1 \to Gal(K/E) \to Gal(K/k) \to Gal(E/k) \to 1$$

4.5.1 Caractérisations des extensions galoisiennes

Théorème 4.13 *Soit K/k une extension finie. Alors K/k est galoisienne si et seulement si l'action de $Aut_k(K)$ sur les conjugués de tout élément de K est transitive.*

Théorème 4.14 *Les extensions galoisiennes finies de k sont exactement les corps des racines de polynôme.*

4.5.2 Groupe de Galois des corps finis

Proposition 4.17 *L'extension F_{q^n}/F_q est galoisienne, de groupe de Galois cyclique d'ordre n engendré par*

$$F_q : x \mapsto x^q$$

les sous-corps de F_q^n contenant F_q sont les F_q^m avec $m|n$.

4.5.3 Points fixes

Proposition 4.18 *Soit K/k galoisienne de groupe Galois G. Alors, G est de cardinal $[K : k]$ et l'espace des points fixes K^G de K sous l'action de G est réduit à k.*

Théorème 4.15 (Lemme d'artin) *Soit K un corps parfais et G un sous-groupe fini du groupe des automorphismes de corps de K.Alors,K^G est parfait et l'extension K/K^G est finie de groupe de Galois G.*

Théorème 4.16 *(Correspondance de Galois)*

1. *L'application*
$$f : \{F \to GL \mapsto Gal(K/L)\}$$
est bijective, strictement décroissante, d'inverse
$$g : \{G \to FH \mapsto K^H\}$$
Soit maintenant $H \in G$
2. *L'extension K/K^H est galoisienne de groupe de Galois H.*
3. *L'application de restriction*
$$r_H : G = Hom_k(K, \Omega) \to Hom_k(K^H, \Omega)$$
identifie l'ensemble quotient G/H à $Hom_k(K^H, \Omega)$.
4. *L'extension K^H/k est galoisienne si et seulement si H est un sous-groupe distingué de K. Dans ce cas, l'identification précédente induit un isomorphisme*
$$G/H \xrightarrow{\sim} Gal(K^H/k)$$
5. *En particulier, si L/k est galoisienne, on a une suite exacte canonique*
$$1 \to Gal(K/L) \to Gal(K/k) \to Gal(L/k) \to 1$$

Preuve : On doit d'abord vérifier qu'on a bien

$$g(f(L)) = g(Gal(K/L)) = K^{Gal(K/L)} = L$$

Mais comme K est galoisienne sur L de groupe de Galois $H = Gal(L/K)$, on a bien $K^H = L$ d'après propos de points fixes. Ensuite, on a

$$f_g(H) = Gal(K/K^H) = H \tag{4.2}$$

les deux applications f et g sont bien inverses l'une de l'autre, et en particulier sont bijectives. La décroissance est claire, son caractère strict découlant de la bijectivité : on a prouvé 1). Le point 2) est le lemme d'Artin. Prouvons le point 3). Soit H un sous-groupe de G et prouvons la surjectivité de r_H. Tout k-morphisme $\sigma_H \in Hom_k(K^H, \Omega)$ se prolonge en $\sigma \in Hom_k(K, \Omega)$ d'après le théorème de prolongement des homomorphismes. Comme K/k est galoisienne, on a $\sigma(K) = K$ i.e $\sigma \in G$ de sorte que $r_H(\sigma) = \sigma_H$: l'application de restriction r_H est surjective. Bien entendu, g et gh ont même image si $h \in H$ de sorte qu'on a une surjection

$$\rho_H : G/H \twoheadrightarrow Hom_k(K^H, \Omega)$$

On a alors $cardHom_k(K^H, \Omega) = [K^H : k] = [K : k]/[K : K^H] = cardG/cardH = card(G/H)$ de sorte que ρ_H est bijective. Prouvons le point 4). Soit H un sous-groupe de G. Bien entendu $g \in G$ envoie K^H dans $K^{gHg^{-1}}$ et donc g^{-1} envoie $K^{gHg^{-1}}$ dans K^H prouvant

$$g(K^H) = K^{gHg^{-1}}$$

. Supposons K^H/k galoisienne. On a alors

$$K^H = g(K^H) = K^{gHg^{-1}}$$

. Supposons K^H/k galoisienne. On a alors

$$K^H = g(K^H) = K^{gHg^{-1}}$$

et donc $H = gHg^{-1}$ par injectivité de la correspondance de Galois et donc $H \lhd G$. Inversement, si $H \lhd G$, on a

$$g(K^H) = K^{gHg^{-1}} = K^H$$

et K/K^H est galoisienne. L'isomorphisme de groupes est celui de propos 1. Maintenant 5) découle clairement des autres points.

4.6 Théorie de Galois des extension finies

4.6.1 Extensions galoisiennes finies

Théorème 4.17 *Soit K un corps. Soit L une extension algébrique de K. L/K est normale et séparable$\Longleftrightarrow K = Inv(Gal(L/K))$.*

Proposition 4.19 *Soit K un corps. Soit G un groupe fini d'automorphismes de K. Soit $F = Fix(G)$ le corps fixe de G. Alors :*

1. *K/F est algébrique, normale et séparable*
2. *K/F est de degré fini*
3. *$[K : F] = [G]$ et $G = Gal(K/F)$.*

Définition 4.28 *Soit K un corps. On dit que L est une extension galoisienne de K si, et seulement si, L est une extension algébrique, normale et séparable de K. On dit que L est une extension galoisienne finie de K si, et seulement si, L est une extension galoisienne et finie de K.*

Exemple 4.9 *Toute extension de degré fini et normale L du corps $\mathbb{Q}$ est galoisienne finie car $L/\mathbb{Q}$ est séparable car $\mathbb{Q}$ est de caractéristique 0.*

Théorème 4.18 (Extensions galoisiennes finies) *Soit K un corps. Soit L une extension de degré fini de K. Les conditions suivantes sont équivalentes :*

1. *L/K est normale et séparable*
2. *$K = Inv(Gal(L/K))$*
3. *$|Gal(L/K)| = [L : K]$.*

Théorème 4.19 (Extension galoisiennes finies et corps de décomposition) *Soit K un corps. Soit L une extension de degré fini de K. Les conditions suivantes sont équivalentes :*

1. *L/K est normale et séparable*
2. *il existe $P(X) \in K[X], P$ séparable sur K, tel que $L = D_K(P)$*
3. *$\exists M(X) \in K[X]$, M irréductible et séparable sur K, tel que $L = D_K(M)$.*

Proposition 4.20 *Soit K un corps parfais(par exemple K corps de caractéristique 0, où K corps fini). Soit $P(x) \in K[X]$. Alors $D_K(P)/K$ est galoisienne finie.*

5 Résolution des équation par radicaux

5.1 Extensions radicales

Définition 5.1 *Une extension de corps $L : K$ est dite radicale, si*

$$L = K(\alpha_1, \alpha_2, ..., \alpha_m), m \in \mathbb{N}^*$$

et

$$\forall i(1 \leq i \leq m), \exists n_i \in \mathbb{N}^*; \alpha_1^{n_1} \in K, \alpha_i^{n_i} \in K(\alpha_1, \alpha_2, ..., \alpha_{i-1}).$$

On dit que les éléments $\alpha_i, 1 \leq i \leq m$, forment une suite radicale pour l'extension $L : K$. Une extension $K(\alpha) : K$ sera dite simple radicale, s'il existe un entier $n \geq 1$ tel que $\alpha^n \in K$.

Définition 5.2 *Etant donné un corps K de caractéristique 0 et un polynôme $f(X)$, non constant dans $K(X)$, on désigne par E, un corps de décomposition de $f(X)$ sur K. On dira que le polynôme $f(X)$ est résoluble par radicaux, s'il existe une extension R de E radicale sur K.*

Définition 5.3 *Etant donné $f(X)$, non constant dans $K(X)$ et E un corps de décomposition de $f(X)$ sur K, le groupe de Galois $G(E : K)$ est appelé groupe de Galois du polynôme $f(X)$ sur K.*

5.2 Polynômes résolubles par radicaux

5.3 Caractérisation des polynômes résolubles par radicaux

Théorème 5.1 (Théorème de Galois) *Soit K un corps, de caractéristique 0, et $f(X) \in K[X] \setminus K$, alors $f(X)$ est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Lemme 5.1 *Si, pour un entier $n > 1$, le polynôme $X^n - 1$ de $K[X]$ est scindé sur K, alors, pour tout $a \neq 0$ dans K, le groupe de Galois du polynôme $X^n - a$ est abélien.*

Lemme 5.2 *Soit $F : K$ une extension galoisienne, de degré fini et $F(\gamma)$ une simple, radicale de F ; alors il existe une extension L de F telle que*

a) $L : F$ est radicale.
b) $L : F$ et $L : K$ sont galoisiennes.
c) Le groupe $G(L : F)$ est résoluble. Si, de plus, on suppose $G(F : K)$ résoluble, alors $G(L : K)$ est résoluble.

Lemme 5.3 *Si $M : K$ est une extension radicale, il existe, alors, une extension L de K, contenant M, telle que $L : K$ est galoisienne, de degré fini, et $G(L : K)$ est résoluble.*

Théorème 5.2 *Si $f(X) \in K(X) \setminus K$ est un polynôme résoluble par radicaux, alors son groupe de Galois est résoluble.*

Preuve : On suppose que $f(X) \in K[X] \setminus K$, est résoluble par radicaux, donc Il existe une extension radicale $M : K$ telle que $K \subseteq E \subseteq M$, où E désigne un corps de décomposition de $f(X)$ sur K. implique alors l'existence d'une extension L de M telle que $L : K$ est galoisienne, de degré fini et $G(L : K)$ est résoluble. L'application du Théorème fondamental de Galois aux extension $K \subseteq E \subseteq L$ donne

$$G(E : K) \simeq G(L : K) \diagup G(L : E).$$

Le groupe $G(E : K)$ est alors résoluble, en tant que quotient d'un groupe résoluble.

Théorème 5.3 *Étant donné un corps K de caractéristique 0, soit L une extension de degré fini, normale sur K telle que $G(L : K)$ est résoluble ; alors, il existe une extension $R : L$ telle $R : K$ est radicale.*

Remarque 5.1
a) Un polynôme $f(X) \in K[X] \setminus K$ (car $K = 0$), dont le groupe de Galois est abélien est résoluble par radicaux ; en particulier, quel que soit $n > 1, X^n - 1 \in \mathbb{Q}[X]$, est résoluble par radicaux.
b) Pour tout $n \geqslant 5$, le groupe symétrique S_n étant non résoluble, tout polynôme de $K[X]$, dont le groupe de Galois est isomorphe à un groupe symétrique S_n $n \geqslant 5$, est non résoluble par radicaux.

5.4 Exemples de polynômes non résolubles par radicaux

5.5 Polynômes de degré premier impair

Proposition 5.1 *Soit p un nombre premier impair et, dans $\mathbb{Q}[X]$, un polynôme $f(X)$, irréductible, de degré p, ayant exactement deux racines complexes, non réelles, alors le groupe de Galois de $f(X)$ sur $\mathbb{Q}$ est le groupe symétrique S_p.*

Remarque 5.2 *Un polynôme de degré premier $p \geq 5$, satisfaisant aux hypothèses de la , est non résoluble par radicaux.*

5.6 Applications de résolution d'une équation algébrique par radicaux

5.6.1 Équation de degré 2 quelconque

Soit l'équation $x^2 + 2bx + c = 0$. On a

$$\begin{aligned} x^2 + 2bx + c = 0 &\Leftrightarrow x^2 + 2bx + b^2 - b^2 + c \\ &\Leftrightarrow (x+b)^2 + c - b^2 \end{aligned}$$

On pose $u = x + b$

$$\begin{aligned} &\Leftrightarrow u^2 + c - b^2 = 0 \\ &\Leftrightarrow u = \mp\sqrt{b^2 - c} \\ &\Leftrightarrow x = -b \mp \sqrt{b^2 - c} \\ &\Leftrightarrow x = \frac{-2b \mp \sqrt{(2b)^2 - 4c}}{2} \end{aligned}$$

Alors si on pose que $eq = x^2 + 2bx + c = 0$ on aura

$$\begin{aligned} eq &\Leftrightarrow (x - \frac{-2b - \sqrt{(2b)^2 - 4c}}{2})(x - \frac{-2b + \sqrt{(2b)^2 - 4c}}{2}) = 0 \\ &\Leftrightarrow T_1 T_2 = 0 \\ &\Leftrightarrow T_1 = 0 \quad \text{ou} \quad T_2 = 0 \end{aligned}$$

.

Avec T_1, T_2 des résolvantes partielles de l'équation $x^2 + 2bx + c = 0$.

5.6.2 Équation du troisième degré quelconque

Méthode de Cardan : on cherche à résoudre $x^3 + px + q = 0$; l'idée de la méthode de Cardan consiste à chercher x sous la forme $x = u + v$ afin d'obtenir une équation plus simple à résoudre. En remplaçant dans l'équation, on obtient $(u+v)^3 + p(u+v) + q = 0 \Leftrightarrow u^3 + v^3 + (u+v)(3uv + p) + q = 0$; On va imposer la condition $3uv + p = 0$, donc $3uv + p = 0 \Leftrightarrow uv = -\frac{p}{3}$. Alors on obtient le système suivant :

$$\begin{cases} u^3 + v^3 = -q \\ (uv)^3 = -(\frac{p}{3})^3 \end{cases} \Leftrightarrow \begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = (-\frac{p}{3})^3 \end{cases}$$

Or si on connait la somme et le produit de deux nombres ici (u^3, v^3) on peut trouver ces nombres comme solutions d'équation du second degré.

On effet, $(X-u^3)(X-v^3)=0 \Leftrightarrow X^2-X(u^3+v^3)-(\frac{p}{3})^3=0$

$$X^2+Xq-(\frac{p}{3})^3=0$$

D'où $x=u+v=\sqrt[3]{\frac{-q+\sqrt{q^2+4(\frac{p}{3})^3}}{2}}+\sqrt[3]{\frac{-q-\sqrt{q^2+4(\frac{p}{3})^3}}{2}}$ alors toute équation de degré 3 et résoluble par radicaux.

Remarque 5.3 *Expliquons pourquoi nous sommes contentées de résoudre des équation du troisième degré du type $x^3+px+q=0$. Soit l'équation $(E): x^3+ax^2+bx+c=0$, on pose le changement du variable $x=(y-\frac{a}{3})$ et on remplace dans (E), on trouve l'équation $y^3+p'y+q'=0$.*

5.6.3 Équation du quatrième degré quelconque

Méthode de ferrari : on cherche de résoudre $x^4+cx^2+dx+e=0$; Deux cas sont alors possibles : si $d=0$, l'équation $x^4+cx^2+e=0$ est bicarrée, en posant $x'=x^2$, on retrouve une équation de degré 2. Si $d\neq 0$, posons $x'=x^2+t$, où t paramètre à choisir judicieusement. Élevons au carré, et injections l'équation $x^4+cx^2+dx+e=0$:

$$\begin{aligned} x'^2=(x^2+t)^2 &= x^4+2tx^2+t^2 \\ &= -cx^2-dx-e+2tx^2+t^2 \\ &= (2t-c)x^2-dx+(t^2-e) \end{aligned}$$

Donc on a $(x^2+t)^2=(2t-c)x^2-dx+(t^2-e)$, il reste à poser une condition sur t. L'idée de Ferrari est d'écrire le membre de droit de cette dernière équation sous la forme d'un carré, et ainsi d'obtenir $x'^2=y^2\Leftrightarrow(x'+y)(x'-y)=0$, où $(x'+y)$ et $(x'-y)$ sont des équations de degré 2. Pour cela, choisissons t de manière à ce que le discriminant de $(2t-c)x^2-dx+(t^2-e)$ soit nul, c'est-à-dire

$$d^2-4(2t-c)(t^2-e)=0$$

Nous savons résoudre une telle équation d'ordre 3 (Méthode de Cardan). Une fois t déterminé, la résolution est simple, car : x solution de $x^4+cx^2+dx+e=0$, $d\neq 0\Leftrightarrow x$ et solution de $(x'+y)(x'-y)=0, d^2-4(2t-c)(t^2-e)=0$. Nous savons résoudre ce dernier système, composé d'une équation de degré 4 factorisable en deux équations de degré 2, et d'une équation de degré 3.

Remarque 5.4 *Expliquons pourquoi nous sommes contentées de résoudre des équations du quatrième degré du type $x^4+cx^2+dx+e=0$. Soit l'équation $(E): x^4+bx^3+cx^2+dx+e=0$, on pose le changement du variable $x=(y-\frac{b}{4})$ et on remplace dans (E), on trouve l'équation $y^4+c'y^2+d'y+e'=0$.*

Annexe - Biographie d'Évariste Galois [1]

La vie d'Évariste Galois est la plus célèbre et la plus commentée des vies de mathématiciens. Elle est même devenue mythique.

La connaissance que nous en avons est assez lacunaire pour laisser une certaine latitude à notre rêverie ou aux historiens des sciences ou aux romanciers.

Enfance, 1811 – 1823

Évariste Galois est né à Bourg-la-Reine (Bourg-légalité pendant la Révolution, à 10 km au sud de Paris) le 25 octobre 1811. Son père, Nicolas Gabriel, a 36 ans. Il est libéral, maire de la commune pendant les cent jours et confirmé sous la Restauration à cause de sa forte personnalité. Il est directeur d'un collège fondé par son propre père. La mère d'Évariste, Adélaïde Marie, née Demante, a 23 ans (1788–1872). Elle est d'une famille de juristes et magistrats. Elle aurait pris une part importante dans l'éducation de son jeune fils, pour la culture classique au moins. Louis-le-Grand, 1823 – 1829

À douze ans, Évariste entre en classe de quatrième comme interne à Louis-le-Grand, à l'époque collège royal. C'est sans doute un bouleversement de cadre très éprouvant pour lui. Il est bon élève jusqu'en troisième et obtient un accessit de grec au Concours général. Sa seconde est moins bonne : maladie ou premiers refus. En octobre 1826, il entre en classe de rhétorique mais doit retourner en seconde au début du deuxième trimestre en raison de ses résultats médiocres. Les études sont à base classique et les sciences peuvent être abordées comme cours supplémentaires (c'est une régression par rapport au rôle fondamental des mathématiques dans l'enseignement à l'époque napoléonienne et surtout à l'époque révolutionnaire). Galois entre en classe de mathématiques préparatoires première année.

Galois découvre alors les mathématiques. Il lit les grands découvreurs : Legendre (Éléments de géométrie), Lagrange (textes sur la résolution des équations), Euler, Gauss, Jacobi. La capacité d'assimilation de Galois semble avoir été exceptionnelle ; ce qu'il lit est immédiatement assimilé. Il a le premier prix au Concours général de mathématiques (il n'obtiendra qu'un accessit l'année suivante, adoptant peut-être un point de vue trop général pour traiter le sujet proposé). Mais il n'a plus aucun intérêt pour les études scolaires. C'est la fureur des mathématiques qui le domine indique, début 1828, un de ses professeurs qui suggère qu'il quitte le lycée pour pouvoir

1. Ce texte est une version modifiée, rectifiée et étendue du chapitre 13 du livre Théorie de Galois, Dunod, 2000, de Jean-Pierre Escofier.

s'y consacrer entièrement.

En 1828, il échoue au concours d'entrée à l'École polytechnique et entre en octobre dans la classe de mathématiques spéciales de Louis-le-grand. Le professeur, Richard, est remarquable ; il a 33 ans et admire le génie de son élève. Il conserve les copies de Galois qu'il confiera plus tard à un autre de ses élèves, Charles Hermite.

Richard encourage Galois à publier ses premiers travaux ; un article paraît le 1er avril 1829, dans les Annales de mathématiques, la revue fondée par Joseph Gergonne, démontrant un théorème sur les fractions continues périodiques. Selon Joseph Bertrand, qui le tenait d'Antoine Masson, Galois aurait démontré en quelques minutes le fameux résultat que Sturm présente à l'Académie le 13 mai sur les racines des polynômes. L'été 1829

Les épreuves et les drames commencent et vont s'accumuler. Un article présenté fin mai à l'Académie des sciences, confié à Cauchy, est perdu (celui-ci avait déjà perdu un mémoire d'Abel).

Le 2 juillet 1829, le père de Galois, ne pouvant supporter les attaques du curé de Bourg-la-Reine (des lettres anonymes), se suicide dans son appartement parisien (par asphyxie écrit Paul Dupuy).

Quelques jours après ce deuil, le concours d'entrée à l'École polytechnique est catastrophique. Galois y échoue à la stupéfaction de son professeur. L'examinateur, Dinet ou Lefébure de Fourcy, probablement Dinet, aurait posé une question sur les logarithmes, jugée trop simple, voire stupide, par Galois. Le geste de Galois de jeter le chiffon pour effacer le tableau à la tête de son examinateur serait une légende selon Joseph Bertrand. Galois parlera plus tard du rire fou de MM. les examinateurs des candidats à l'École polytechnique (que je m'étonne en passant de ne pas voir occuper chacun un fauteuil à l'Académie des sciences, car leur place n'est certainement pas dans la postérité) Publications et perte

Sur les conseils de son professeur, Galois entre en octobre 1829 à l'École normale (appelée École préparatoire de 1826 à août 1830 et d'un niveau bien inférieur à l'École polytechnique) située dans les locaux de Louis-le-grand. Il passe ses baccalauréats ès lettres (un succès le 17 décembre après un échec devant Guizot et Villemain le 9 décembre) et ès sciences (le 29 décembre). Il rédige le résultat de ses recherches et le présente en février 1830 à l'Académie des sciences pour concourir au grand prix de mathématiques. Fourier, Secrétaire perpétuel pour les mathématiques, emporte le manuscrit chez lui et meurt le 16 mai. Le manuscrit est perdu : la perte de ce mémoire est une chose très simple. Il était chez M. Fourier qui devait le lire et, à la mort de ce dernier, le mémoire a été perdu. Ce sont les travaux d'Abel (mort l'année précédente) et de Jacobi qui sont couronnés par le grand prix en juin.

Le journal fondé par le baron de Férussac en 1823, le Bulletin général et universel des annonces et nouvelles scientifiques, avait pour projet, immense, de répandre partout les connaissances et découvertes scientifiques ; il comportait huit sections, la première consacrée aux mathématiques, à l'astronomie, à la physique et à la chimie ; en huit ans, 170 volumes furent publiés. Galois y donne en avril 1830 un texte de deux pages avec des propositions sur la résolubilité des équations par radicaux déduites de la théorie des permutations. En juin 1830, il y présente une Note sur la résolution des équations numériques mises sous la forme $\varphi(x) = x$ et un texte Sur la théorie des nombres où il développe ses résultats sur les corps finis ; Galois précise en sous-titre : Ce Mémoire fait partie des recherches de *M*. Galois sur la théorie des permutations et des équations algébriques. Il envisage d'autres publications. Mais les temps changent. Révolution et révolte

Les manifestations contre le régime de Charles *X* se multiplient, la répression se durcit. L'engagement politique de Galois semble avoir évolué très rapidement. Il va désormais vivre avec la même intensité les événements historiques et mathématiques. Lors des journées des 27, 28, 29 juillet 1830, il ne peut participer à l'action, consigné dans son école, contrairement aux polytechniciens qui font le mur et resteront dans l'histoire. Galois passe ses examens de licence. En octobre 1830, à la rentrée des classes, il est républicain, actif, intrépide et prêt à défendre le droit des masses selon l'expression d'un membre de sa famille ; soixante-dix ans après, une de ses cousines se souvenait encore avec quelle sombre véhémence Évariste exprimait ses idées. Il adhère à la Société des Amis du Peuple le 10 novembre, société dont la première réunion a eu lieu le 30 juillet. Il critique l'opportunisme du directeur de l'École normale et du philosophe Victor Cousin. A ses critiques politiques, il mêle des critiques sur l'enseignement. Il est consigné jusqu'à nouvel ordre.

Le dernier article mathématique publié de son vivant, très court, paraît le 1er décembre dans les Annales de Gergonne. Le 5 décembre, Galois serait l'auteur d'une longue lettre dans la Gazette des écoles, signée Un élève de l'École normale, où le directeur est tourné en dérision : Tout en lui annonce les idées les plus étroites et la routine la plus complète. La lettre sème le trouble dans l'école entre les élèves littéraires et les élèves scientifiques. Le 3 janvier 1831, par une décision exceptionnelle, le Conseil royal exclut Galois de l'École normale (le brouillon de l'arrêté est de Victor Cousin). Galois vient de s'enrôler dans l'artillerie de la garde nationale.

Le 2 janvier 1831, toujours dans la Gazette des écoles paraît une lettre Sur l'enseignement des sciences, sous-titrée Des professeurs. Des ouvrages. Des examinateurs, où Galois dénonce la médiocrité de l'enseignement aux

étudiants : Quand leur laissera-t-on du temps pour méditer cet amas de connaissances… pourquoi les examinateurs ne posent-ils les questions aux candidats que d'une manière entortillée ? Il semblerait qu'ils craignissent d'être compris de ceux qu'ils interrogent… Croit-on donc la science trop facile ? Le cours d'algèbre de janvier 1831

Sans ressources, Galois ouvre le 13 janvier un cours public d'algèbre supérieure chez le libraire Caillot au 5, rue de la Sorbonne. L'annonce parue dans la Gazette des écoles précise : Ce cours aura lieu tous les jeudis, à une heure et quart ; il est destiné aux jeunes gens qui, sentant combien est incomplète l'étude de l'algèbre dans les collèges, désirent approfondir cette science. Le cours se composera de théories dont quelques-unes sont neuves et dont aucune n'a jamais été exposée dans les cours publics. Nous nous contenterons de citer une théorie nouvelle des imaginaires, la théorie des équations qui sont solubles par radicaux, la théorie des nombres et les fonctions elliptiques traitées par l'algèbre pure. La première leçon réunit 30 auditeurs. Le cours semble n'avoir eu que peu de séances.

L'académicien Denis Poisson conseille à Galois d'écrire une nouvelle version du mémoire présenté un an auparavant à Fourier et perdu. Le 17 janvier, l'Académie le charge d'examiner ce manuscrit avec Sylvestre Lacroix. Le 31 mars, Galois presse l'Académie, écrivant pour que son mémoire soit étudié. Le banquet aux Aux Vendanges de Bourgogne

Cependant les tensions politiques sont très fortes, Louis-Philippe ayant habilement manœuvré pour écarter les républicains du pouvoir et de la garde nationale, qui n'est plus réservée, en mars, qu'aux gens aisés. Le 9 mai 1831, après un acquittement de jeunes républicains, un banquet est organisé dans les salons du restaurant Aux Vendanges de Bourgogne à Belleville. Alexandre Dumas et François-Vincent Raspail y participent. Des toasts se succèdent. Lisons Alexandre Dumas, même si son récit est un peu arrangé et comporte des inexactitudes.

Galois est arrêté le lendemain chez sa mère et écroué à Sainte-Pélagie (près du Jardin des Plantes). Les fumées du vin m'avaient ôté la raison, écrit Galois à son ami Auguste Chevalier. Il est jugé le 15 juin. Ce jour là, le journal Le Globe prend la défense de Galois, évoquant son génie mathématique, les difficultés dont il est victime, les mémoires successifs déposés à l'Académie. Reprenons le récit d'Alexandre Dumas.

L'incompréhension de Poisson et Lacroix

Le 4 juillet, Poisson et Lacroix publient enfin leur rapport sur le mémoire de Galois : …nous avons fait tous nos efforts pour comprendre la démonstration de Galois. Ses raisonnements ne sont ni assez clairs ni assez développés pour que nous ayons pu juger de leur exactitude… On peut attendre que l'auteur ait publié en entier son travail pour se former une

opinion définitive… ; pour le moment nous ne pouvons pas vous proposer d'y donner votre approbation.

Énorme déception de Galois. Mais on peut penser que Poisson et Lacroix avaient tout de même un peu raison : le texte n'était pas facile à comprendre et l'auteur pouvait bien s'expliquer un peu plus. Liouville écrit en 1846 : Les commissaires reprochèrent au jeune analyste une rédaction obscure et il reproche à Galois de ne pas avoir profiter de leurs avis. La prison

Le 14 juillet, Galois, à la tête de plusieurs centaines de manifestants, est arrêté sur le Pont-Neuf , avec une carabine chargée, des pistolets, un poignard ; il est écroué de nouveau à Sainte-Pélagie. Après trois mois de détention, il est condamné le 23 octobre, à sa profonde surprise, à six mois de prison supplémentaires ; le motif trouvé est le port illégal de l'uniforme de la garde nationale. Son ami Ernest Duchatelet, arrêté en même temps que lui, n'est condamné qu'à trois mois pour le même motif. Galois fait appel, mais la condamnation est confirmée le 3 décembre : il doit rester incarcéré jusqu'au 29 avril 1832. Son signalement indique sa taille : 1 mètre 67 ; ses cheveux sont châtains, ses yeux bruns, son visage ovale.

En prison, Galois rencontre Nerval et Raspail. Auguste Chevalier, sa tante, sa sœur lui rendent visite.

Raspail apprécie Galois. Il raconte en 1839 que les autres détenus passaient leur temps à boire et qu'une fois, Galois, provoqué par un codétenu, s'empara d'une bouteille d'eau de vie, la vida d'un trait avant de la jeter sur son provocateur, puis de confier son désarroi de la perte de son père à Raspail avant de s'effondrer ivre mort son corps plein de soubresauts.

Nerval a été brièvement incarcéré à Sainte Pélagie en février 1832. Il raconte son séjour dans Mes prisons, en 1841, ce qui permet d'imaginer que la vie de Galois à Sainte Pélagie n'était pas si difficile qu'on pourrait l'imaginer. Les détenus chantaient La Marseillaise, pouvaient se faire apporter leurs repas, etc. Nerval raconte son départ : Il était cinq heures. L'un des convives me reconduisit jusqu'à la porte, et m'embrassa, me promettant de venir me voir en sortant de prison. Il avait, lui, deux ou trois mois à faire encore. C'était le malheureux Gallois, que je ne revis plus, car il fut tué en duel le lendemain de sa mise en liberté. De ce séjour vient aussi le poème Politique des Petits châteaux de Bohème publié d'abord en décembre 1831.

Projets de décembre 1831

En décembre, Galois envisage une nouvelle tentative de publication de ses travaux.

Sa préface est tellement polémique que le texte complet n'en sera publié qu'en 1948 par René Taton. Amer de la perte de ses manuscrits, de

l'incompréhension de Poisson, il attaque violemment les hommes politiques et scientifiques, les plaçant sur le même plan : Si j'avais à adresser quelque chose aux grands du monde ou aux grands de la science… je jure que ce ne seraient point des remerciements.

Il analyse la marche des idées en mathématiques : les simplifications produites par l'élégance des calculs… ont leurs limites, puis ajoute : Sauter à pieds joints sur les calculs ; grouper les opérations, les classer suivant leurs difficultés et non suivant leur forme ; telle est, suivant moi, la mission des géomètres futurs ; telle est la voie où je suis entré dans cet ouvrage. Rimbaud dirait : C'est prophète.

Pour conclure en soulignant ce qu'il n'a pu éclaircir, il rêve d'un temps où l'égoïsme ne régnera plus dans les sciences, où on s'associera pour étudier, au lieu d'envoyer aux académies des plis cachetés, on s'empressera de publier ses moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : "Je ne sais pas le reste".

À côté de sa propre rédaction de son premier mémoire, après une note qu'a cru devoir y apposer M. Poisson, il écrit simplement : On jugera.

On jugera

Dans une note sur Abel jointe à ce texte, rappelant qu'Abel avait cru avoir trouvé la résolution des équations générales du cinquième degré, Galois rédige sous la forme d'une note de l'éditeur : Même erreur est arrivée en 1828 à l'auteur (il avait seize ans).

La pension Faultrier

L'épidémie de choléra qui sévit à Paris au début de 1832 (le président du conseil, Casimir Périer, en meurt le 16 mai) conduit, le 16 mars, au transfert de Galois dans une pension ou maison de santé d'un sieur Faultrier, rue de Lourcine, près de la place d'Italie (le long de la Bièvre, non loin du moulin de Croulebarbe). En théorie, Galois devait être remis en liberté le premier juin, mais on est sûr qu'il est sorti de prison avant.

En mai 1832, une brève aventure amoureuse lie Galois à une jeune femme, Stéphanie D., dont on discute toujours l'identité. Il écrit son nom, mêle leurs initiales. Il rompt le 14 mai. Un duel semble en résulter ; il a lieu le mercredi 30 mai. La nuit du mardi 29 mai 1832

La nuit précédente, Évariste rassemble ses dernières découvertes dans une splendide lettre à son ami Auguste Chevalier. La scène est dramatique. Pressentant sa mort, pressé par le temps, l'urgence absolue est pour lui de transmettre ce si court résumé de son œuvre scientifique :

Paris, le 29 mai 1832

Mon cher ami,

J'ai fait en analyse plusieurs choses nouvelles.

Les unes concernent la théorie des Équations, les autres les fonctions Intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par radicaux…

Il rappelle l'ensemble des résultats qu'il a obtenus, concluant sept pages plus loin par une esquisse obscure de notions créées plus tard par Riemann

Les derniers jours : des détails qu'on ne connaîtra sans doute jamais

Les circonstances exactes de toute cette aventure ne sont pas connues, pas plus que le nom de son adversaire (même si Alexandre Dumas en donne un) ni le nom de la jeune fille (Stéphanie semble certain, mais Dumotel non) ; en vertu de quels critères absurdes Galois a-t-il accepté ce duel ? Pourquoi aucun des protagonistes n'a jamais parlé ? Robert Bourgne a écrit sur ce sujet un article qui fait le tour des questions en 1983.

République française

Robert Bourgne donne en particulier le témoignage, rédigé en janvier 1909, de Gabriel Demante, un neveu de la mère de Galois qui a été professeur à la Faculté de droit de Paris, se souvenant, il avait onze ans, lors d'une promenade en famille avec son père, avoir rencontré Galois, très élégant, à l'angle de la rue Soufflot et de la rue Saint-Jacques le samedi 26 mai 1832 : Galois aurait alors affirmé reconnaître l'impuissance de ses efforts dans la vie politique et sa résolution de se consacrer désormais exclusivement à la science. Apparemment, le duel ne s'annonçait pas encore. L'élégance de Galois est-elle un signe d'une récente aventure amoureuse ?

Dans la matinée du mercredi 30 mai, Galois, abandonné (Dupuy suggère que ses témoins étaient partis chercher des secours), est relevé, grièvement blessé, par un paysan et conduit à l'hôpital Cochin où il meurt de péritonite le jeudi 31 à 10 heures dans les bras de son jeune frère Alfred : Ne pleure pas, j'ai besoin de tout mon courage pour mourir à vingt ans.

Il est enterré dans la fosse commune du cimetière Montparnasse le 2 juin 1832, sans que sa famille soit présente ; aucun document pour nous aider à comprendre. Les jours suivants

Des récits de la mort de Galois sont publiés dans quelques journaux. Les détails donnés sont contradictoires. Ses amis préparent un soulèvement, reporté à l'annonce du décès du général Lamarque ; ce dernier a lieu le 5 juin et aboutit au massacre du cloître Saint-Merry. Victor Hugo en fera une des parties mémorables des Misérables : l'épopée rue Saint-Denis.

Le rapport de l'autopsie pratiquée le 7 juin décrit en détail les proportions des os du crâne de Galois, les circonvolutions de son cerveau, les différentes parties de l'abdomen lésées par la balle, tirée à 25 pas ; c'est assez horrible. Le cerveau et le cervelet de Galois réunis pesaient trois livres,

deux onces moins un gros (1560 grammes environ).

La fidélité d'Auguste Chevalier et de son frère permettent de réunir les papiers d'Évariste Galois. Sa lettre-testament est publiée en septembre 1832, dans la Revue Encyclopédique, sans écho. En la présentant, Auguste Chevalier donne un grand nombre de renseignements sur la vie de son ami. Par exemple : Une seconde condamnation le rejeta pour six mois encore sous les verrous. La mort l'attendait à la sortie. Le mythe romantique naîtra de ces beaux matériaux. Les années suivantes

En 1835, Lacroix signale en note terminale de la 6ème édition des Compléments des élémens d'algèbre le mémoire de Galois qu'il avait lu avec Poisson :

En 1828, Abel écrivait à Legendre : "J'ai été assez heureux de trouver une règle sûre, à l'aide de laquelle on pourra reconnaître si une équation quelconque proposée est résoluble à l'aide de radicaux, ou non. Un corollaire de ma théorie fait voir que généralement il est impossible de résoudre les équations supérieures au quatrième degré." (Journal de Crelle, année 1830, 1er cahier, p. 73) Cette découverte fut annoncée par Legendre à l'Académie des Sciences, le 23 février 1829 ; mais Abel n'a rien publié à ce sujet, et l'on n'a rien trouvé qui s'y rapporte dans ses papiers. . .

En 1831, un jeune Français, Évariste Gallois (sic), mort l'année suivante, avait annoncé, dans un mémoire présenté à l'Académie des Sciences, que "pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement" : mais ce mémoire parut à peu près inintelligible aux commissaires chargés de l'examiner. La première mise en lumière

C'est le 4 septembre 1843 (Poisson et Lacroix sont morts) que Liouville annonce à l'Académie des Sciences qu'il vient de trouver dans les papiers de Galois, transmis par Auguste Chevalier, une solution aussi exacte que profonde au problème de la résolubilité des équations par radicaux (Comptes rendus hebdomadaires des séances de l'Académie des sciences, vol. 17, pages 448 – 449). Voulant sans doute mieux la comprendre, ce n'est qu'en octobre et novembre 1846 qu'il publie des textes de Galois dans le tome 11 de son Journal de mathématiques pures et appliquées, pages 385 – 444, en n'y joignant finalement aucun commentaire mathématique. L'œuvre de Galois est enfin mise à la disposition de tous et avec la caution scientifique d'un des grands mathématiciens de l'époque. En route vers la gloire

Dans les années 1850, les textes des mémoires de Galois sont enfin accessibles aux mathématiciens. Ils suscitent de nombreux travaux de Serret, Betti, Kronecker, Dedekind (cours à Göttingen pendant l'hiver 1857 –

1858), Cayley, Hermite, Jordan (un commentaire paru dans les Mathematische Annalen, le Traité des substitutions de 1870)… En 1895, Sophus Lie publie dans Le centenaire de l'École normale 1795 – 1895 une étude de neuf pages : Influence de Galois sur le développement des mathématiques. L'importance de Galois dans les grandes idées des mathématiques du vingtième siècle est immense ; parmi d'autres échos récents : La longue marche à travers la théorie de Galois rédigée par Alexandre Grothendieck en 1980 – 81, etc.

Liouville joint à sa publication de 1846 une courte note, pages 381 – 384, reprenant la notice d'Auguste Chevalier. Nous avons dit qu'il reproche à Galois son manque de clarté ; il reproche aussi à Poisson et Lacroix la sécheresse de leurs conclusions. Il dit avoir travaillé sous les yeux de son frère, Alfred Galois. Une vie de Galois paraît dans le tome *XVI* du Magasin pittoresque, juillet 1848, pages 227 – 228, à laquelle est jointe un portrait de mémoire par son frère Alfred ; elle serait d'un condisciple de Galois à Louis-le-grand nommé P.-P. Flaugergues. Cinquante ans plus tard, Paul Dupuy, surveillant général de l'École normale supérieure, publie dans les Annales de l'École normale supérieure : La vie d'Évariste Galois. On peut considérer ce texte comme une biographie quasiment définitive : Dupuy a presque complètement fait le tour des archives, il a recueilli des témoignages directs des proches de Galois encore en vie, il est plein de sympathie pour son sujet et son livre est très vivant. Depuis 100 ans, comme le retrace René Taton en 1983, des biographies plus ou moins exactes, plus ou moins inventives se sont succédées. Il est toujours tentant d'ajouter sa version aux précédentes : Évariste Galois est tellement proche de nous par ses révoltes, son génie est si extraordinaire, il a un destin absolument unique et il est tellement fascinant avec ses zones d'ombre !

Résumé :

L’idée globale de ce mémoire est - dans un premier temps - de donner tout les outils nécessaires pour accéder à la théorie de Galois, ensuite de comprendre l’utilité des groupes résolubles et leurs liens avec la résolubilité des polynômes par radicaux et de l’appliquer sur les groupes de Galois.

ملخص

الفكرة العامة لهذه المذكرة هي تقديم جميع المفاهيم اللازمة كمرحلة أولى من أجل الولوج إلى نظرية جالوا و من ثم محاولة فهم علاقة الزمر القابلة للحل بالمعادلات القابلة للحل بالجذور و تطبيقها على زمر جالوا

Conclusion

Ce travail consiste à donner une idée sur la résolubilité des groupes et la résolubilité par radicaux des polynômes et le liens entre les deux ! Autrement dit, on a explicité d'une manière plus au moins généreuse la façon dans laquelle on peut appliquer le théorème de Galois en passant par la constructions du groupe de Galois associé aux racines d'un polynôme et sa résolubilité.

Références

[1] Serge Lang : Algebra, tome 211 Graduate Texts in Mathematics. Springer-Verlag, New York, Third Edition 2002.

[2] Josette Calais,Extension de corps , Théories de Galois niveau $M1 - M2$

[3] David Hernandez et Yves Laszlo Introduction à la théorie de Galois 12 février 2012

[4] Ivan Gozard,Théorie de Galois MATHÉMATIQUE 2^e cycle collection dirigée par Charles-Michel Marle et Philippe P bossian Ellipse

[5] Jean-Pierre Escofier, THÉORIE DE GALOIS cours et exercices corrigés, Master. CAPES. Agrégation 2^e édition DUNOD

[6] Daniel Guin et Thomas Hausberger Algèbre I GROUPES,CORPS ET THÉORIE DE GALOIS

[7] Carrega J-C,Théorie des corps-La règle et au compas, Herman, 1981