N° d'ordre :113/2022-C/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

FACULTE DE MATHEMATIQUES

Thèse de doctorat

Présentée pour l'obtention du **grade** de **Docteur**

En : MATHEMATIQUES

Spécialité : **Algèbre et Théorie des Nombres**

Par : **MOKHTARI Soufyane**

Sujet

Groupe de Galois des $\mathbb{Q}$- trinômes de degré une puissance d'un nombre premier

Soutenue publiquement, le 20 / 11 / 2022 , devant le jury composé de :

M. Mohand Ouamar HERNANE	Professeur à l' USTHB	Président
M. Boualem BENSEBA	Professeur à l' USTHB	Directeur de thèse
M. Tarek GARICI	Maître de Conférences A à l' USTHB	Examinateur
M. Omar KIHEL	Professeur à Brok University- Canada	Examinateur
Mme Scheherazade BOUYACOUB	Maître de Conférences B à l' USTHB	Invitée

Dédicaces

A mes très chers parents

pour tous les soins et le suivi dont ils ont fait preuve depuis ma naissance et au long de mes études pour leur soutien et surtout leurs conseils et leur amour

A mes chères soeurs

A mes chers frères

A ma grande famille

A tous mes amis

A tous ceux qui m'aiment et que j'aime

Remerciements

J'exprime mes profonds remerciements à mon directeur de thèse, le professeur Boualem BENSEBA, qui n'a pas cessé de m'aider et m'encourager dans cette oeuvre.
Mes remerciement vont aussi à l'endroit du Professeur Mohand Ouamar HERNANE qui a accepté de présider le jury de ma soutenance.
Je remercie les professeurs Omar KIHEL, Tarik GARICI, et Scheherazade BOUYACOUB, pour avoir porté de l'intérêt pour mon travail en acceptant d'être des membres du jury de ma soutenance.

Table des matières

Abréviations

$\mathbb{Z}$ et $\mathbb{Q}$	: anneau des entiers rationnels et corps des nombres rationnels.
$\mathbb{Z}_p$ et $\mathbb{Q}_p$	: anneau des entiers et corps des nombres p-adiques.
E, K, F et N	: corps de nombres.
$G = Gal(f) = G(f)$	: groupes de Galois du trinôme $f(X)$.
$G = G(E/F)$	: groupes de Galois de l'extension galoisienne E/F.
$\|G\|$	: ordre du groupe G.
$\mathcal{O}_E$	: anneau des entiers du corps de nombres E.
E/F	: extension de corps de nombres.
$[E : F]$	: degré de l'extension E/F.
$\wp$ et $\mathfrak{p}_i$	: premiers respectifs d'une extension galoisienne E/F.
$e_i = e(\mathfrak{p}_i/\wp)$	: indice de ramification de $\mathfrak{p}_i$ au dessus de $\wp$.
$f_i = f(\mathfrak{p}_i/\wp)$	: degré résiduel de $\mathfrak{p}_i$ au dessus de $\wp$.
k_K et k_L	: corps résiduels respectivement des corps K et L.
$I_\mathfrak{p}$ et $D_\mathfrak{p}$	: groupes d'inertie et de décomposition de l'idéal premier $\mathfrak{p}$.
$K_\wp$	: le complété de K pour la valuation $\wp$-adique.
$\mathfrak{D}(E/F)$	: différente de l'extension de corps locaux E/F.
$D(f)$	: discriminant du trinôme $f(X)$.
d_K	: discriminant du corps K.
$\mathbb{Q}(\alpha)$	: le corps obtenu en adjoignant α au corps $\mathbb{Q}$ des nombres rationnels.
$N_{E/F}(\beta)$.	: norme dans F de l'élément β de E.
$T_{E/F}(\beta)$	: trace dans F de l'élément β de E.
A_n et S_n	: le groupe alterné et le groupe symétrique de degré n.
$GL(n, k)$	: le groupe général linéaire.

Résumé

Soit p un nombre premier impair, $n \geq 2$ un entier rationnel. Dans cette thèse, on étudie le groupe de Galois absolu G d'un trinôme $f(X) = X^{p^n} + aX + a \in \mathbb{Z}[X]$ supposé être un trinôme d'Eisenstein en p. Nous commencerons par présenter quelques résultats connus sur la ramification dans les extensions de corps de nombres.
Ensuite, nous exposerons quelques résultats sur le groupe de Galois d'un polynôme, en particulier ceux de K. Komatsu [18], [19] et A. Movahhedi [28] sur le groupe de Galois de $X^p + aX + a$.
Finalement, on montre que le groupe de Galois G de $f(X)$ est soit le groupe symétrique S_{p^n}, ou $AGL\,(1, p^n) \leq G \leq AGL\,(n, p)$. De plus, nous verrons que G est le groupe symétrique S_{p^n} dans chacun des cas suivants :

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, et il existe un diviseur premier q de $p^{n-1} + p^{n-2} + ... + p + 1$ tel que $\left(\frac{q}{p}\right) = -1$

Mots clés : Trinômes d'Eisenstein ; ramification ; Polygones de Newton ; groupes doublement transitifs ; groupe de Galois

abstract

Let p be an odd prime, $n \geq 2$ a rational integer. In this thesis, we study the absolute Galois group G of a trinomial $f(X) = X^{p^n} + aX + a \in \mathbb{Z}[X]$ assumed to be an Eisenstein trinomial with respect to p. We will start by presenting some known results on ramification in number field extensions.
Then, we will expose some results on the Galois group of a polynomial, in particular those of K. Komatsu [18], [19] and A. Movahhedi [28] on the Galois group of $X^p + aX + a$.
Finally, we show that the Galois group G of $f(X)$ is either the symmetric group S_{p^n}, or $AGL(1, p^n) \leq G \leq AGL(n, p)$. Moreover, we will see that G is the symmetric group S_{p^n} in each of the following cases :

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, and there is a prime divisor q of $p^{n-1} + p^{n-2} + ... + p + 1$ such that $\left(\frac{q}{p}\right) = -1$

Key words : Eisenstein trinomials ; Ramification ; Newton polygons ; doubly transitive groups ; Galois group

Introduction

La thèse que nous présentons traite du groupe de Galois des trinômes, à coefficients dans l'anneau des entiers relatifs, sur le corps $\mathbb{Q}$ des nombres rationnels. Les trinômes $X^m + aX^s + b$ sont, sous la condition que les exposants m et s soient premiers entre eux, généralement dits « sans affect », est que leur groupe de Galois est isomorphe a un sous-groupe du groupe symétrique S_m et dont l'avantage est d'avoir une forme simple qui permet d'obtenir assez aisément des renseignements sur le groupe de Galois.

De nombreux travaux donnent des conditions suffisantes pour qu'un trinôme donné ait un groupe de Galois isomorphe au groupe alterné. Plus récemment, à l'exception d'une liste très limitée d'entre eux, des résultats ont été obtenus dans le sens que les autres groupes de permutation„ ne peuvent se réaliser comme groupes de Galois que d'un nombre fini de trinômes.
En fait, on se propose dans cette thèse de déterminer le groupe G des $\mathbb{Q}$-automorphismes, agissant sur les différentes racines d'un trinôme $f(X) = x^{p^n} + aX + a \in \mathbb{Z}[X]$, d'Eisenstein en le nombre premier p, appelé groupe de Galois de f sur $\mathbb{Q}$. Pour cela, notons par $\alpha := \alpha_1, \ldots, \alpha_{p^n}$ les différentes racines de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\alpha_1, \ldots, \alpha_{p^n})$ sont respectivement les corps de rupture et de décomposition de $f(X)$ sur $\mathbb{Q}$. Ainsi, le groupe de Galois de ce trinôme n'est autre que le groupe de Galois de l'extension $N/\mathbb{Q}$. Ce trinôme étant irréductible, puisqu'il est d'Eisenstein en le nombre premier p, son groupe de Galois est un groupe de permutations transitif de degré $m = p^n$, ce qui nous suggère d'utiliser la classification des sous-groupes transitifs de S_m.

D'autre part, la ramification d'un nombre premier p dans K nous renseigne sur les cycles contenus dans les sous-groupes de décomposition et d'inertie de p dans $N/\mathbb{Q}$, ce qui nous permet d'affiner la classification des groupes de permutations ayant cette propriété. La ramification des idéaux premiers de K est liée aux diviseurs diviseurs premiers de son

discriminant d_K , qui est lié au discriminant D du trinôme $f(X)$

$$D = (-1)^{m(m-1)/2} a^{m-1} \left[m^m + (-1)^{m-1} (m-1)^{m-1} a \right]$$

par la relation

$$D = i(\alpha)^2 d_K$$

où $i(\alpha)$ désigne l'indice du groupe $\mathbb{Z}[\alpha]$ dans le groupe additif de l'anneau $\mathcal{O}_K$ des entiers de K.
La méthode d'Ore [31], donnant la décomposition, en produit d'idéaux premiers, d'un nombre premier dans K sera utilisée, car elle reflète la factorisation d'un polynôme dans un corps local [voir aussi [11]] et interprète la décomposition d'un nombre premier dans une extension en lien avec la notion de polynôme associé au polynôme considéré et relatif à un côté du polygone de Newton. Elle permet, en combinaison avec le Lemme d'Abhyankar [30, p.229], d'identifier la structure du groupe d'inertie dans l'extension $N/\mathbb{Q}$ d'un idéal premier $\wp$ de N au dessus d'un nombre premier p ramifié dans K . La détermination du groupe d'inertie d'un nombre premier p dans l'extension $N/\mathbb{Q}$, et la classification des groupes multi-transitifs finis simples, voir S. Abhyankar [1], sont des outils permettant de s'informer sur la possible réalisation d'un groupe de permutation comme groupe de Galois du trinôme considéré.

La thèse présentée contient des résultats nouveaux ; elle compte 4 chapitres, dont le dernier expose les contributions originales traitant des trinômes de degré une puissance d'un nombre premier p.

Dans les trois premiers chapitres, nous exposerons les notions de base fondamentales à l'étude des travaux et les résultats concernant la détermination des groupes de Galois de trinômes, Nous mettrons l'accent sur les diverses techniques et les outils utilisés à cet effet. Nous traiterons des notions de ramification et de polygones de Newton, un exposé que nous retrouvons en détail dans l'article intitulé " The factorization of polynomials over local fields" [11]. Nous exposerons dans des situations concrètes leur utilisation pour la recherche du groupe de Galois d'un trinôme irréductible sur $\mathbb{Q}$. Nous aborderons les classifications des groupes simples finis qui nous seront utiles pour décider si un groupe de permutations est susceptible de se réaliser comme groupe de Galois d'un tel trinôme.

Au chapitre 4, nous exposerons nos résultats sur le groupe de Galois du trinôme $X^{p^2}+aX+a$ et nous montrons que c'est le groupe symétrique S_{p^2} dans sous diverses hypothèses. En particulier, dans chacun des cas suivants :

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, et il existe un diviseur premier q de $p+1$ tel que $q \equiv -1 \mod 4$.

De façon générale, on montre que s'il existe un diviseur premier $q \neq p$ de a tel que $\text{pgcd}(\upsilon_q(a), p) = 1$, alors le groupe de Galois absolu G de f est le groupe symétrique complet S_{p^2}.

Aussi, nous généralisons ce résultat en montrant que le groupe de Galois du trinôme $X^{p^n}+aX+a$ est tout le symétrique S_{p^n} dès que l'une des conditions suivantes est réalisée :

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, et il existe un diviseur premier q de $p^{n-1}+p^{n-2}+...+p+1$ tel que $\left(\frac{q}{p}\right) = -1$

En fait, lorsque les conditions précédentes ne sont pas réalisées, nous montrons que le groupe de Galois absolu G de $f(X)$ est soit le groupe symétrique S_{p^n}, ou $AGL\,(1, p^n) \leq G \leq AGL\,(n, p)$.

Chapitre 1

Arithmétique dans les corps de nombres

Tous les corps considérés dans cette thèse sont commutatifs.

1.1 Notion d'extensions

Soit K un corps .

Définition 1.1. On appelle extension de K un corps L le contenant.

Notation une extension L d'un corps K sera notée L/K ou $K \subset L$.

Une extension L d'un corps K est munie d'une structure de K-espace vectoriel.

La dimension de L comme K-espace vectoriel est appelléé degré de l'extension L/K, qu'on note $[L : K]$.

On dit que l'extension L/K est finie si $[L : K] < +\infty$.

Proposition 1.2. *Soit $K \subset L \subset M$ une suite d'extensions. Alors M/K est de degré fini si et seulement si M est de degré fini sur L et L est de degré fini sur K. Dans ce cas, on a*

$$[M : K] = [M : L] \times [L : K]$$

Démonstration. Soient $(e_i)_{i\in I}$ une $K-$base de L et $(f_j)_{j\in J}$ une $L-$base de M comme espaces vectoriels. On vérifie alors que $(e_i f_j)_{(i,j)\in I\times J}$ est une $K-$base de M .

□

Remarque 1.3. La proposition précédente peut être généralisée à une tour de n extensions

$$K = K_1 \subset K_2 \subset \cdots \subset K_n = M$$

et on a :

Proposition 1.4. *l'extension K_n/K est finie si et seulement si , $\forall i; 1 \leq i \leq n-1$, l'extension K_{i+1}/K_i est finie et on a*

$$[K_n : K] = \prod_{i=1}^{n-1} [K_{i+1} : K_i]$$

1.2 Elément algébrique et polynôme minimal

Définition 1.5. Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit algébrique sur K s'il existe un polynôme non nul de $K[X]$, de degré n ayant α comme racine.

Considérons l'extension $K(\alpha)$ de K engendrée sur K par un élément $\alpha \in L$, appelée extension de K obtenue par adjonction de α à K, et soit ϕ le morphisme d'anneaux défini par :

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

Dire que α est algébrique sur K équivaut à dire que le noyau $Ker(\phi)$ de ϕ est non nul, ou encore que les éléments α^i, $1 \leq i \leq n$, sont linéairement dépendants sur K.

Théorème 1.6. *Soient L/K une extension et $\alpha \in L$ un élément algébrique sur K.*

1. Il existe un unique polynôme irréductible et unitaire $M_\alpha(X) \in K[X]$ vérifiant $M_\alpha(X) = 0$.
2. Tout polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$ est divisible par $M_\alpha(X)$.
3. Le corps $K(\alpha)$ est isomorphe à $K[X]/(M_\alpha(X))$ et $[K(\alpha) : K]$ est égal au degré du polynôme $M_\alpha(X)$. En posant ce degré égal à n, les éléments $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ forment une base du K-espace vectoriel $K(\alpha)$.

Démonstration. Par construction on a $Im(\phi) \simeq K[X]/Ker(\phi)$. Comme lanneau $K[X]$ est intègre et principal, alors l'idéal $Ker(\phi)$ est premier et principal et est engendré par un polynôme irréductible, qui est unique si on le suppose unitaire..

Soit $M_\alpha(X)$ ce polynôme, alors l'idéal $Ker(\phi)$ est maximal, ce qui entraine que $Im(\phi)$ est un corps, contenant K et α, c'est donc le corps $K(\alpha)$. Ainsi, on aura

$$dim_K(K[X]/(M_\alpha(X))) = deg(M_\alpha(X))$$

et l'isomorphisme $K[X]/(M_\alpha(X)) \to K(\alpha)$ envoie une base $\left\{1, \overline{X}, ..., \overline{X^{n-1}}\right\}$ de $K[X]/(M_\alpha(X))$ sur une base $\left\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\right\}$.

□

Définition 1.7. Avec les notations ci-dessus, le polynôme $M_\alpha(X)$ est appelé polynôme minimal de α sur K.

L'entier $deg(M_\alpha(X)) = [K(\alpha) : K]$ est appelé le degré de α sur K.

Définition 1.8. On dit qu'une extension L/K est algébrique si tout élément de L est algébrique sur K.

Proposition 1.9. *Soit L une extension d'un corps K et $\alpha \in L$ un élément algébrique sur K, alors l'extension $K(\alpha)$ est algébrique sur K.*

Démonstration. Soit $\alpha \in L$ algébrique sur K de degré n, alors $K(\alpha)$ est un K-espace vectoriel de dimension n dont une base est $\left\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\right\}$.
Soit $x \in L$, alors la famille $\left\{1, x, x^2, ..., x^n\right\}$ est liée, ce qui montre que $\exists \lambda_i \in K$, $0 \leq i \leq n$, non tous nuls tels que $\lambda_0 + \lambda_1 x + ... + \lambda_n x^n = 0$
Ainsi, x est un zéro du polynôme $P(X) = \lambda_0 + \lambda_1 X + ... + \lambda_n X^n \neq 0$ et montre que x est algébrique sur K . Par conséquent, tout élément de L est algébrique sur K et donc que L est algébrique sur K

□

Proposition 1.10. *Toute extension L de degré fini sur K est algébrique sur K.*

Démonstration. Soient L/K une extension finie et $\alpha \in L$. Comme $dim_K(K(\alpha)) \leq dim_K(L)$, alors il existe un entier n tel que la famille $\{1, \alpha, ..., \alpha^n\}$ soit liée. Ainsi, il existe des éléments $a_0, ..., a_n$ de K tels que $a_0 + a_1\alpha^n + ... + a_n\alpha^n = 0$, ce qui prouve qu'il existe un polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$.

□

Proposition 1.11. *Soient L/K une extension et $\alpha_1, \alpha_2, ..., \alpha_n \in L$ des éléments algébriques sur K. Alors le corps $K(\alpha_1, \alpha_2, ..., \alpha_n)$, obtenu par adjonction à K des α_i, $i = 1, ..., n$, est une extension finie, donc algébrique, de K.*

Démonstration. On procède par récurrence sur l'entier n.

L'extension $K \subset K(\alpha_1)$ est bien finie, ce qui prouve l'hypothèse de récurrence.

Supposons que $K(\alpha_1, \alpha_2, ..., \alpha_{n-1})$ soit une extension finie de K . Comme $K(\alpha_1, ..., \alpha_n) = K(\alpha_1, ..., \alpha_{n-1})(\alpha_1)$, alors $K(\alpha_1, \alpha_2, ..., \alpha_n)$ est une extension finie de $K(\alpha_1, ..., \alpha_{n-1})$, donc de K.

□

Théorème 1.12. *Soient L/K et M/L des extensions, alors L'extension M/K est algébrique si et seulement si L/K et M/L le sont.*

Démonstration. Il est clair que si M/K est une extension algébrique, alors L/K et M/L le sont.

Supposons que M/L et L/K sont des extensions algébriques, alors pour tout $\alpha \in M$, il existe des éléments $a_0, ..., a_n$ de L tels que $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$.

Considérons $L_0 = K(a_0, ..., a_n)$; puisque les a_i sont dans L et sont algébriques sur K, alors l'extension L_0/K est finie (Proposition 1.11), ce qui est le cas de l'extension $L_0(\alpha)/K$, d'où α est algébrique sur K.

□

Les extensions algébriques possèdant la propriété suivante

Proposition 1.13. *Si L/K est une extension algébrique, tout K-endomorphisme de L est un K-automorphisme.*

Démonstration. Pour tout polynôme $P(X) \in K[X]$, on note R_P l'ensemble des racines de $P(X)$ dans L. L'extension L/K étant algébrique, alors $L = \bigcup_{P(X) \in K[X]} R_P$.

Pour un K-endomorphisme f de L, sa restriction à R_p est une application injective de R_P dans R_P, étant morphisme de corps, qui de plus est surjective puisque le cardinal de R_P est fini. On en déduit que $f : L \to L$ est bijective, c'est donc un automorphisme.

□

Définition 1.14. Soient k un corps et $f(X)$ un polynôme non constant à coefficients dans k. Un corps de rupture K de f est une extension K/k telle que $K = k(\alpha)$, où $\alpha \in K$ est une racine de $f(X)$.

Quitte à remplacer $f(X)$ par l'un des ses facteurs irréductibles, on supposera dans toute la suite que le polynôme $f(X)$ est irréductible dans $k[X]$.

Proposition 1.15. *Soit k un corps, alors tout polynôme $f(X)$ de $k[X]$ admet un corps de rupture.*

Démonstration. On pose $K = k[X]/(f(X))$. Puisque $f(X)$ est irréductible, l'idéal $(f(X))$ est maximal, d'où K est un corps.

En considèrant l'application $k \hookrightarrow k[X] \to K$, ce qui permet d'identifier k à un sous-corps de K et donc de considérer l'extension K/k, on note α la classe de X dans K, alors $f(\alpha) = 0$, i.e. α est une racine de f. D'après (Théorème 1.6), $K = k(\alpha)$.

□

Exemple 1.16. a) Soit $K = \mathbb{Q}$ et $f(X) = X^2 - 2$, alors $L = \mathbb{Q}(\sqrt{2})$ est un corps de rupture du polynôme f.
b) $K = \mathbb{R}, f(X) = X^2 + 1$, alors $L = \mathbb{C}$ est un corps de rupture du polynôme f.

Proposition 1.17. ***(prolongement des isomorphismes)***. *Soient k et k' deux corps, $s : k \longrightarrow k'$ un isomorphisme de corps et*

$$\bar{s} : k[X] \longrightarrow k'[X]$$

l'isomorphisme d'anneaux prolongeant s : $\bar{s}(\sum_i a_i X^i) = \sum_i s(a_i)X^i$. Alors

(i) *Pour tout polynôme irréductible $f(X) \in k[X]$, le polynôme $\bar{s}(f)(X)$ est irréductible dans $k'[X]$.*

(ii) *Soient K (resp. K') une extension de k (resp. k') et α (resp. α') une racine de $f(X)$ (resp. $\bar{s}(f)(X)$) dans K (resp. K'). Il existe un unique isomorphisme de corps $\sigma : k(\alpha) \longrightarrow k'(\alpha')$ prolongeant s et tel que $\sigma(\alpha) = \alpha'$.*

Démonstration. L'assertion (i) est évidente.

Pour l'assertion (ii), montrons d'abord l'unicité : un élément y de $k(\alpha)$ s'écrit $y = a_o + ... + a_{n-1}\alpha^{n-1}$, où n est le degré de f. Donc

$$\sigma(y) = \sigma(a_o) + ... + \sigma(a_{n-1})\sigma(\alpha)^{n-1} = s(a_o) + ... + s(a_{n-1})\alpha'^{n-1}$$

, d'où l'unicité.

Pour montrer l'existence, considérons le diagramme suivant :

$$\begin{array}{ccc} k(\alpha) & \stackrel{\sigma}{\longrightarrow} & k'(\alpha') \\ \Theta \downarrow & & \downarrow \Theta' \\ k[X]/(f(X)) & \underset{\bar{\bar{s}}}{\longrightarrow} & k'[X]/(\bar{s}(f)(X)) \end{array},$$

où Θ et Θ' sont les isomorphismes établis au (théorème 1.6), $\bar{\bar{s}}$ est obtenu à partir de $\bar{s}$ par passage au quotient et en posant $\sigma = \Theta'^{-1} \circ \bar{\bar{s}} \circ \Theta$.

□

Proposition 1.18. *Soient k un corps et $f(X)$ un polynôme irréductible de $k[X]$. Deux corps de rupture de $f(X)$ sont k-isomorphes.*

Démonstration. On applique la proposition 1.17 pour $k = k'$ et $s = id_k$.

□

Corollaire 1.19. *Soient K/k une extension et α et α' deux éléments de K algébriques sur k. Les assertions suivantes sont équivalentes :*

(i) *Les polynômes minimaux respectifs de α et α' sont égaux*

(ii) *Il existe un (unique) k-isomorphisme de $k(\alpha)$ sur $k(\alpha')$ appliquant α sur α'.*

Démonstration. L'assertion (i) implique (ii) car :

$$k(\alpha) \simeq k[X]/(M_\alpha(X)) = k[X]/(M_{\alpha'}(X)) \simeq k(\alpha').$$

D'autre part, en notant σ le k-isomorphisme dont l'assertion (ii) suppose l'existence, pour tout polynôme $P(X) \in k[X]$ on a $\sigma(P(\alpha)) = P(\sigma(\alpha)) = P(\alpha')$. D'où $P(\alpha) = 0$ si et seulement si $P(\alpha') = 0$. On en déduit que $M_\alpha(X) = M_{\alpha'}(X)$. ce qui l'assertion (ii) implique (i)

□

Définition 1.20. Lorsque les conditions équivalentes du Théorème précédent sont vérifiées, on dira que les éléments α et α' sont conjugués.

Définition 1.21. Soient k un corps, $f(X)$ un polynôme non constant de $k[X]$ et K/k une extension. Le polynôme $f(X)$ se décompose complètement, ou est scindé, dans K si $f(X) = c(X-\alpha_1)...(X-\alpha_n)$, où $c, \alpha_1, ..., \alpha_n$ sont dans K.

Autrement dit, le polynôme $f(X)$ s'écrit dans $K[X]$ comme produit de facteurs de degré 1.

Exemple 1.22. (i) Le polynôme $X^3 - 1$ de $\mathbb{Q}[X]$ est scindé dans $\mathbb{C}$.

(ii) Le polynôme $X^4 - X^2 - 2$ de $\mathbb{Q}[X]$ est scindé dans $\mathbb{Q}(i, \sqrt{2})$ car $X^4 - X^2 - 2 = (X-i)(X+i)(X-\sqrt{2})(X+\sqrt{2})$, par contre il ne l'est pas dans $\mathbb{Q}(i)$, puisque $X^4 - X^2 - 2 = (X-i)(X+i)(X^2-2)$

.

Définition 1.23. *Soient K un corps et $f(X)$ un polynôme non constant de $K[X]$. On appelle corps de décomposition de $f(X)$ sur K, une extension (algébrique) N/K telle que $f(X)$ est scindé dans N, de racines $\alpha_1, \alpha_2, ..., \alpha_n$ et $N = K(\alpha_1, \alpha_2, ..., \alpha_n)$.*

Théorème 1.24. *Soient k un corps et$f(X)$ un polynôme non constant de $k[X]$.*

(i) Il existe un corps de décomposition de $f(X)$ sur k.

(ii) Deux corps de décomposition de $f(X)$ sur k sont k-isomorphes.

Démonstration. (i). On fait un raisonnement par récurrence sur le degré de f.

– Si $d^\circ f = 1$, le résultat est évident.

– Supposons le résultat vrai pour tout corps k et tout polynôme de $k[X]$ de degré inférieur ou égal à $n-1 (n > 1)$. Soit $f(X) \in k[X]$ de degré n. Si $f(X)$ n'est pas scindé dans k, il possède un facteur irréductible $g(X)$ avec $1 < \deg g < n$. Soit $k(\alpha_1)$ un corps de rupture de $g(X)$. Dans $k(\alpha_1)[X]$, on a $f(X) = (X-\alpha_1)h(X)$ et $d^\circ h = n-1$. Donc $h(X)$ admet un corps de décomposition $k(\alpha_1)(\alpha_2, ..., \alpha_n) = K$, qui est donc un corps de décomposition de $f(X)$ sur k.

□

(ii). plus généralement, on a le résultat suivant :

Lemme 1.25. *Soient $s : k \longrightarrow k'$ un isomorphisme de corps, $f(X)$ un polynôme de $k[X]$, K (resp. K') un corps de décomposition de $f(X)$ (resp. $\bar{s}(f)(X)$). Alors, il existe un isomorphisme de corps $\sigma : K \longrightarrow K'$ qui prolonge s.*

Démonstration. – Si $d^\circ f = 1$, c'est évident.

– Supposons le résultat vrai pour tout corps et tout polynôme de degré inférieur ou égal à $n-1$ et soit f un polynôme de degré n.

On considère

$$K = k(\alpha_1, ..., \alpha_n), \qquad K' = k'(\alpha'_1, ..., \alpha'_n)$$

et

$$f(X) = c(X - \alpha_1)...(X - \alpha_n), \qquad \bar{s}(f)(X) = c'(X - \alpha'_1)...(X - \alpha'_n).$$

Soit $g(X)$ un facteur irréductible de $f(X)$ admettant α_1 comme racine dans K. En renumérotant les α'_i , on peut supposer que $\bar{s}(g)(X)$ admet α'_1 comme racine dans K. D'après la proposition 1.17, il existe $s_1 : k(\alpha_1) \to k'(\alpha'_1)$, isomorphisme de corps qui prolonge s. D'où, par hypothèse de récurrence, il existe

$$\sigma : K = k(\alpha_1)(\alpha_2, ..., \alpha_n) \longrightarrow K' = k'(\alpha'_1)(\alpha'_2, ..., \alpha'_n)$$

qui prolonge s_1, donc aussi s.

Pour démontrer l'assertion (ii) du théorème 1.24, on applique ce lemme avec $k = k'$ et $s = id_k$.

.

□

Proposition 1.26. *Soit k un corps. Les assertions suivantes sont équivalentes :*

(i) Tout polynôme non constant de $k[X]$ se décompose, dans $k[X]$, en un produit de polynômes du premier degré

(ii) Tout polynôme irréductible de $k[X]$ est du premier degré

(iii) Tout polynôme non constant de $k[X]$ a au moins une racine dans k

(iv) Toute extension algébrique de k est triviale (i.e. égale à k).

Démonstration. Il est évident que (i) implique (ii).

Montrons que (ii) implique (iii) : puisque $k[X]$ est principal, tout polynôme $f(X)$ s'écrit comme produit de polynômes irréductibles, donc du premier degré. Un polynôme du premier degré a une racine dans k. Pour montrer que (iii) implique (i), on procède par récurrence sur le degré de f :

– le résultat est vrai si $deg\, f = 1$,

– supposons le résultat vrai si $deg\, f = n - 1$ et soit f un polynôme de degré n ; il existe $\alpha \in k$ tel que $f(\alpha) = 0$, d'où $f(X) = (X - \alpha)g(X)$ et le résultat en découle par hypothèse de récurrence.

Montrons que (ii) implique (iv) : soit α un élément algébrique sur k. Le polynôme minimal de α est de degré 1, donc $dim_k k(\alpha) = 1$, i.e. α appartient à k.

Montrons que (iv) implique (ii) : soit $f(X) \in k[X]$ un polynôme irréductible. Alors $k[X]/(f)$ est un corps qui est une extension finie, donc algébrique, de k. D'où $k[X]/(f) = k$ et $dim_k k[X]/(f) = 1 = deg\, f$.

□

Définition 1.27. Un corps k qui vérifie les conditions équivalentes ci-dessus est dit algébriquement clos.

Théorème 1.28. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. (cf. [35, p. 53]).

□

Notation

Définition 1.29. Une extension L/K est une clôture algébrique de K si c'est une extension algébrique et si le corps L est algébriquement clos.

Théorème 1.30. *Tout corps admet une clôture algébrique.*

Démonstration. (cf. [36, théorème 32, §14 p.106])

□

Définition 1.31. Soient L/K et M/K deux extensions. On dit que L/K et M/K sont conjuguées dans une extension algébriquement close Ω de K s'il existe un K-automorphisme σ de Ω tel que $\sigma(L) = M$.

Deux éléments α et β de Ω sont conjugués sur K s'il existe un K-automorphisme σ de Ω tel que $\sigma(\alpha) = \beta$.

Définition 1.32. Soit K un corps, on dit qu'un polynôme $f \in K[X]$ de degré n est séparable sur K s'il admet exactement n racines distinctes dans une clôture algébrique de K

Exemple 1.33. Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ admet trois racines distinctes dans son corps des racines $\mathbb{Q}(\alpha; j)$, où $\alpha = \sqrt[3]{2}$ et $j = \frac{-1+i\sqrt{3}}{2}$, il est donc séparable sur $\mathbb{Q}$.

Les polynômes séparables sont caractérisés par

Proposition 1.34. *Soit K un corps etf $\in K[X]$ un polynôme de tel que $d^\circ f \geq 2$. f est séparable sur K si, et seulement si $f(X)$ et sa dérivée formelle $f'(X)$ sont premiers entre eux.*

Démonstration. Si f a une racine multiple α dans une clôture algébrique $\bar{K}$ de K, alors $(X-\alpha)^2$ divise $f(X)$ dans $\bar{K}[X]$; donc il existe un polynôme non nul $g(X) \in \bar{K}[X]$ tel que

$$f(X) = (X-\alpha)^2 g(X),$$

d'où

$$f'(X) = 2(X-\alpha)g(X) + (X-a)^2 g'(X).$$

Par suite $(X-\alpha)$ est un diviseur commun à f et f', donc, dans l'anneau $\bar{K}[X]$, f et f' ont un pgcd de degré strictement positif, d'où $\operatorname{pgcd}(f, f') \neq 1$.

Réciproquement, supposons $\operatorname{pgcd}(f, f') \neq 1$ et posons $d = \operatorname{pgcd}(f, f')$. On a deg $d \geq 1$, donc il existe $\alpha \in \bar{K}$ tel que, dans $\bar{K}[X]$, on ait $(X-\alpha) \mid d$, d'où $(X-\alpha) \mid f$ et $(X-\alpha) \mid f'$. On en déduit l'existence de g non nul dans $\bar{K}[X]$, tel que

$$f(X) = (X-\alpha)g(X)$$

d'où

$$f' = g + (X-\alpha)g';$$

or par hypothèse, $(X-\alpha)$ divise f' ; par suite, $(X-\alpha)$ divise aussi g, d'où $(X-\alpha)^2 \mid f$. Ainsi l'hypothèse $\operatorname{pgcd}(f, f') \neq 1$ entraîne que f a au moins une racine multiple.

□

Corollaire 1.35. *Soit K un corps et $f \in K[X]$ un polynôme non constant. f n'a que des racines simples si et seulement si $pgcd(f, f') = 1$.*

Nous donnons aussi une caractérisation de la séparabilité d'un polynôme sur un corps K liée à la caractéristique de ce dernier.

Théorème 1.36. *K etant un corps et $f(X) \in K[X]$ un polynôme irréductible de degré* $\deg f \geq 1$.

- *Si K est de caractéristique* 0*, alors f est séparable sur K.*
- *si K est de caractéristique un nombre premier p, f est inséparable sur K si et seulement si $\exists g(X) \in K[X]$ tel que $f(X) = g(X^p)$.*

Démonstration. (cf. [26, Proposition 4.6]).

□

Le critère d'Eisenstein permet de décider, dans une large mesure, de l'irréductibilité d'un polynôme

Critère d'Eisenstein : Soit $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ un polynôme et soit p un nombre premier.
Si $p \mid a_i$, $0 \leq i \leq n-1$, $p \nmid a_n$ et $p^2 \nmid a_0$ alors $P(X)$ est irréductible sur $\mathbb{Q}$.
On dit alors que le polynôme $P(X)$ est d'Eisenstein en p.

Exemple 1.37. Soit le polynôme $X^9 + 6X + 6 \in \mathbb{Q}[X]$. Par le critère d'Eisenstein en $p = 3$, le polynôme ci-dessus est irréductible alors il est séparable sur $\mathbb{Q}$.

Définition 1.38. Soit L/K une extension et $\alpha \in L$ un élément algébrique sur K. On dit que α est séparable sur K si son polynôme minimal $M_\alpha(X)$ est séparable sur K.

Nous donnons dans ce qui suit quelques propriétés relatives aux extensions de corps.

Définition 1.39. On dit qu'une extension L/K est séparable sur K si tout élément de L est séparable sur K.

Théorème 1.40. ***(Théorème de élément primitif)***

Soit K un corps et L une extension de K de degré fini. Si L est séparable sur K , alors il existe $\theta \in L$ tel que $L = K(\theta)$. Dans ce cas θ est appelé élément primitif de L.

Définition 1.41. Une extension algébrique K de k est dite normale sur k si

(i) K est algébrique sur k

(ii) Tout polynôme irréductible de $k[X]$ ayant une racine dans K est scindé dans K..

Exemple 1.42. a) Un corps de décomposition d'un polynôme irréductible de $k[X]$ est une extension normale de k. Par exemple, une clôture algébrique $\overline{k}$ de k est une extension normale de k.

b) $\mathbb{Q}(\sqrt[3]{2}, j)$ est une extension normale de $\mathbb{Q}$, car le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3 - 2$ est $\mathbb{Q}(\sqrt[3]{2}, j)$.

c) $\mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension normale de $\mathbb{Q}$, car le polynôme minimal de $\sqrt[3]{2}$ n'est pas scindé dans $\mathbb{Q}(\sqrt[3]{2})$.

Remarque 1.43. a) Une extension K/k est normale si et seulement si K s'idntifie à tous ses conjuguées sur k.

b) Si K/k est normale et $\alpha \in K$, tous les conjugués de α appartiennent à K.

Définition 1.44. On dit qu'une extension L/K est galoisienne si elle est à la fois algébrique, normale et séparable sur K.

Exemple 1.45. On a les exemples suivants :

1. Les extensions quadratiques $\mathbb{Q}(\sqrt{d})$ sur $\mathbb{Q}$, d entier sans facteur carré, sont galoisiennes.
2. Les extensions cyclotomiques $\mathbb{Q}(\zeta)$, $\zeta = \exp\left(\frac{2i\pi}{n}\right)$ sont galoisiennes sur $\mathbb{Q}$.

Définition 1.46. Soit L/K une extension galoisienne. L'ensemble des K-automorphismes de L est un groupe, appelé groupe de Galois de l'extension galoisienne L/K, on le note $Gal(L/K)$.

Proposition 1.47. *Si L/K est une extension galoisienne de degré n, alors le groupe de Galois $Gal(L/K)$ est d'ordre n.*

Proposition 1.48. *Soit L/K une extnsion galoisienne, alors les K-atomorphismes de L sont exaxtement tous les K-plongements de L dans une clôture algébrique Ω de K.*

Démonstration. Tout plongement σ de L dans Ω , laissant fixe K, réalise une bijection de L dans $\sigma(L)$, donc de L dans $L = \sigma(L)$, puisque L est galoisienne sur K. Ainsi, σ est un automorphisme de L.

□

1.3 Arithmétique dans les corps de nombres

Définition 1.49. On appelle corps de nombres, toute extension de degré fini sur $\mathbb{Q}$.

Définition 1.50. Soient A un anneau commutatif et M un A-module libre de rang n. Soient u un endomorphisme de M,$\{e_1, ..., e_n\}$ une base de M et $(a_{ij})_{1\leq i\leq j\leq n}$ la matrice de u dans cette base. La trace, le déterminant et le polynôme caractéristique de l'endomorphisme u sont :

$$Tr(u) = \sum_{1\leq i\leq n} a_{ii}; \qquad det(u) = det(a_{ij}) \quad et \qquad P_u(X) = det(XI_M - u). \tag{1.3.1}$$

Ces quantités sont indépendantes du choix de la base.

Les formules (1.3.1) impliquent

$$\begin{gathered} Tr(u+u') = Tr(u) + Tr(u') \\ det(u.u') = det(u).det(u') \\ det(XI_M - u) = X^n - (Tr(u)X^{n-1} + ... + (-1)^n det(u)) \end{gathered} \tag{1.3.2}$$

.

.

Soient B un anneau et A un sous anneau de B tel que B soit un A-module libre de rang n. Pour tout $x \in B$, on définit l'endomorphisme m_x de A-module B (multiplication par x) par

$$\begin{aligned} m_x \quad B &\longrightarrow B \\ y &\longrightarrow yx \end{aligned}$$

Définition 1.51. On appelle trace (respectivement norme, polynôme caractéristique) de $x \in B$, relativement à B et A, la trace (respectivement déterminant, polynôme caractéristique) de l'endomorphisme m_x. la trace et la norme de x relativement à B et A sont notées

$$Tr_{B/A}(x) \qquad et \qquad N_{B/A}(x).$$

Remarquons que A peut être un corps et B une extension de A de degré n.

Pour $x, x' \in B$ et $a \in A$ on a $m_x + m_{x'} = m_{x+x'}$ et $m_x \circ m_{x'} = m_{x.x'}$ et $m_{ax} = am_x$. De plus , la matrice de m_a par rapport à toute base de B sur A est la matrice diagonale dont tous les éléments diagonaux sont a . A partir des formules (1.3.1) et (1.3.2) on obtient :

Remarquons que A peut être un corps et B une extension de A de degré n.

Proposition 1.52. *Pour tout $x; x' \in B$ et pour tout élément $\lambda \in A$ on a*

$$Tr_{B/A}(x+x') = Tr_{B/A}(x)+Tr_{B/A}(x') \quad , \quad Tr_{B/A}(\lambda x) = \lambda Tr_{B/A}(x) \quad et \quad Tr_{B/A}(\lambda) = n\lambda$$

et

$$N_{B/A}(x.x') = N_{B/A}(x).N_{B/A}(x') \quad , \quad N_{B/A}(\lambda x) = \lambda^n N_{B/A}(x) \quad et \quad N_{B/A}(\lambda) = \lambda^n$$

Proposition 1.53. Si on a $K \subset L \subset M$, trois corps de nombres, alors pour tout $\alpha \in M$, on a :

$$Tr_{M/K}(\alpha) = Tr_{L/K}(Tr_{M/L}(\alpha))$$
$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha))$$

Démonstration. *Il s'agit d'étendre les plongements de L dans $\mathbb{C}$ à M , et on trouve le résultat.* □

Définition 1.54. Soient B un anneau et A un sous-anneau de B tel que B soit un A-module libre de rang fini n. Pour $(x_1, \ldots, x_n) \in B^n$, on appelle discriminant du système $(x_1, \ldots, x_n)$ l'élément de A défini par

$$D(x_1, \ldots, x_n) = det\left(Tr_{B/A}(x_i x_j)\right)$$

Théorème 1.55. *Soit K un corps de nombres de degré n sur $\mathbb{Q}$. Soient $x_1, ..., x_n \in K$, et $\sigma_1, ..., \sigma_n$ les n plongements de K dans $\mathbb{C}$.*

On a

$$D(x_1, ..., x_n) = [det(\sigma_i(x_j))]^2 .$$

Démonstration. Ceci est la conséquence immédiate de l'égalité matricielle :

$$[\sigma_j(x_i)] \times [\sigma_i(x_j)] = [\sigma_1(x_i x_j) + \cdots + \sigma_n(x_i x_j)] = [Tr_{K/\mathbb{Q}}(x_i x_j)]$$

.

□

Proposition 1.56. *Si* $[x_i] = M \times [y_i]$ *avec* M *matrice* $n \times n$ *à coefficents dans* $\mathbb{Q}$ *, alors :*

$$D(x_1, ..., x_n) = det(M)^2 D(y_1, ..., y_n)$$

Démonstration. On a

$$\forall j,\ [\sigma_j(x_i)]_i = M \times [\sigma_j(y_i)]_i$$

On en déduit donc que

$$[\sigma_j(x_i)]_{i,j} = M \times [\sigma_j(x_i)]_{j,i}$$

□

Théorème 1.57. $D(x_1, ..., x_n) = 0 \Leftrightarrow x_1, ..., x_n$ *sont linéairement dépendants sur* $\mathbb{Q}$.

Démonstration. Si $x_1, ..., x_n$ sont linéairement dépendants, alors les colonnes de la matrice $[\sigma_i(x_j)]$ aussi, et donc $D(x_1, ..., x_n) = 0$.

Inversement, si $D(x_1, ..., x_n) = 0$, alors les lignes R_i de la matrice $[Tr_{K/\mathbb{Q}}(x_i x_j)]$ sont liées. Supposons que les $x_1, ..., x_n$ sont linéairement indépendants sur $\mathbb{Q}$. Soient $a_1, ..., a_n \in \mathbb{Q}$ non tous nuls tels que $a_1 R_1 + \cdots + a_n R_n = 0$. Soit $x = a_1 x_1 + \cdots + a_n x_n$. Nécessairement, $x \neq 0$. De plus, en regardant les coordonnées de chaque ligne, on obtient : $Tr_{K/\mathbb{Q}}(x x_j) = 0$, pour chaque j. Comme $x \neq 0$, et les $x_1, ..., x_n$ sont linéairement indépendant, ils forment donc une base de K sur $\mathbb{Q}$, et de même pour les $x x_1, ..., x x_n$. Mais alors, $\forall y \in Tr_{K/\mathbb{Q}}(y) = 0$, ce qui est une contradiction car $Tr_{K/\mathbb{Q}}(1) = n$.

□

Définition 1.58. Soient K un corps de nombres, x un élément d'une clôture algébrique de K de degré n sur K et de polynôme minimal $F(X)$.

Le discriminant du polynôme F noté $D(F)$ est le discriminant de la base $\left\{1, x, \ldots, x^{n-1}\right\}$.

Proposition 1.59. *Soient L/K une extension de corps de nombres, α un élément de L de degré n sur K et de polynôme minimal P, alors*

$$D\left(1,\alpha,\ldots,\alpha^{n-1}\right)=(-1)^{\frac{n(n-1)}{2}}N_{L/K}\left(P'(x)\right), \tag{1.3.3}$$

où P désigne le polynôme dérivé de P.

Démonstration. Notons $\alpha_1,\ldots,\alpha_n$ les racines de P dans $\mathbb{C}$, ce sont exactement les conjugués de α, alor

$$D\left(1,\alpha,\ldots,\alpha^{n-1}\right)=\det\left(\sigma_i\left(\alpha^j\right)\right)^2,$$

où les σ_i, $1\leq i\leq n$, sont les n plongement de $K(\alpha)$ dans $\mathbb{C}$. Plus précisément, on a

$$D\left(1,\alpha,\ldots,\alpha^{n-1}\right)=\det\left(\alpha_i^j\right)^2=\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2$$

où le terme de droite représente le déterminant de la matrice de Van der Monde. D'autre part, on a

$$\det\left(\sigma_i\left(\alpha^j\right)\right)=(-1)^{n(n-1)/2}\prod_i P'(\alpha_i)=(-1)^{n(n-1)/2}\,\mathrm{N}_{K(\alpha)/K}\left(P'(\alpha)\right)$$

□

Exemple 1.60. Examinons les exemples suivants

1. Considérons le polynôme $P=X^2+aX+b\in K[X]$, où K est un corps de nombres. On suppose que P n'admettant pas de racine multiple et soitα une des racines dans $\mathbb{C}$. On pose $L=K(\alpha)$, c'est une extension de degré 2 sur K.

   Le discriminant de P est

$$\begin{aligned}D_P&=(-1)^{2(2-1)/2}\,\mathrm{N}_{L/K}\left(P'(\alpha)\right)\\&=-\mathrm{N}_{L/K}\left(2\alpha+a\right)\\&=-\left(2\alpha+a\right)\left(2\sigma(\alpha)+a\right)\\&=-\left(4\alpha\sigma\left(\alpha\right)+2a\left(\alpha+\sigma\left(\alpha\right)\right)+a^2\right).\end{aligned}$$

   où σ est l'unique plongement non trivial de L dans $\mathbb{C}$.

Sachant que

$$P = X^2 + aX + b = (X - \alpha)(X - \sigma(\alpha))$$

alors on aura

$$\alpha + \sigma(\alpha) = -a \text{ et } \alpha\sigma(\alpha) = b$$

ce qui entraine la valeur suivante du discriminant du polynôme P

$$D_P = -\left(4b - a^2\right) = a^2 - 4b,$$

une formule bien connue !

2. Soit K un corps de nombres, $P = X^3 + pX + q \in K[X]$ un polynôme irréductible sur K, et soit $L = K(\alpha)$, où α est une racine de P dans $\mathbb{C}$, alors le discriminant de P est

$$D_P = -\mathrm{N}_{L/K}(P'(\alpha))$$

avec $P'(\alpha) = 3\alpha^2 + p$ et tel que $\alpha^3 + p\alpha + q = 0$.

On sait que $\mathrm{N}_{L/K}(P'(\alpha))$ est le déterminant de la matrice de l'endomorphisme $m_{P'(\alpha)}$, multiplication par $P'(\alpha)$, de L dans la base $\left\{1, \alpha, \alpha^2\right\}$ du K-espace vectoriel L.

On a alors

$$m_{P'(\alpha)}(1) = p + 3\alpha^2, \quad m_{P'(\alpha)}(\alpha) = -3q - 2p\alpha \text{ et } m_{P'(\alpha)}\left(\alpha^2\right) = 3\alpha - 2p\alpha^2$$

ce qui permet d'avoir la matrice M de l'endomorphisme $m_{P'(\alpha)}$

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

dont le déterminant est $4p^3 + 27q^2$, ce qui entraine que

$$D_P = -\left(4p^3 + 27q^2\right).$$

Définition 1.61. Un nombre algébrique est dit entier algébrique s'il est racine d'un polynôme unitaire à coefficients entiers. On note $\mathcal{O}$, l'ensemble des entiers algébriques.

L'anneau des entiers d'un corps de nombre K est $\mathcal{O} \cap K$. On le note $\mathcal{O}_K$.

Dans le cas des extensions de corps on a :

Théorème 1.62. *Soit K un corps de nombres de degré n sur $\mathbb{Q}$ et $\mathcal{O}_K$ l'anneau des entiers de K. Alors le $\mathbb{Z}$-module $\mathcal{O}_K$ est libre de rang n.*

Démonstration. (cf. [30, théorème 2.10])

□

Proposition 1.63. *L'anneau des entiers de $\mathbb{Q}$ est $\mathbb{Z}$*

Démonstration. Montrons que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Il est évident que $\mathcal{O}_{\mathbb{Q}}$ contient $\mathbb{Z}$. Soit a dans $\mathcal{O}_{\mathbb{Q}}$, et écrivons $a = {}^{n}/_{m}$, avec n et $m > 0$ des entiers premiers entre eux. Prenons f dans $\mathbb{Z}[X]$ unitaire tel que $f(a) = 0$. Posons alors :

$$f = x^r + a_{r-1}x^{r-1} + \cdots + a_0.$$

cela donne :

$$n^r + a_{r-1}n^{r-1}m + \cdots + a_0 m^r = 0.$$

Supposons qu'un nombre premier p divise m, alors p divise $a_{r-1}n^{r-1}m + \cdots + a_0 m^r$, ce qui sera le cas pour n^ret donc de n. ce qui est absurde, puisque n et m sont premiers entre eux. Il en résulte que $m = \pm 1$, ce qui entraine que a est dans $\mathbb{Z}$.

□

Nous allons montrer dans la suite que $\mathcal{O}_k$ est en fait un sous-anneau de k, contenant $\mathbb{Z}$.

Proposition 1.64. *Soit K un corps de nombres, alors pour tout élément α de $\mathcal{O}_K$ on a $N_{K/\mathbb{Q}}(\alpha)$ et $Tr_{K/\mathbb{Q}}(\alpha)$ sont dans $\mathbb{Z}$.*

Démonstration. Soit P_α le polynôme minimal de α, alors pour tout morphisme de conjugaison σ, $P_\alpha(\sigma(\alpha)) = \sigma(P_\alpha(\alpha)) = P_\alpha(\alpha) = 0$. Ainsi, $\sigma(\alpha)$ est un entier de K.

Étant produit et somme d'entiers de K, $N_{K/\mathbb{Q}}(\alpha)$ et $Tr_{K/\mathbb{Q}}(\alpha)$ sont des entiers et qu'ils sont dans $\mathbb{Q}$, ce qui montrent qu'ils sont dans $\mathbb{Z}$

□

Définition 1.65. Soient K un corps de nombres de degré n sur $\mathbb{Q}$ et $\alpha_1, \ldots, \alpha_n$ des entiers de K.

On dit que $(\alpha_1, \ldots, \alpha_n)$ est une base intégrale si $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_n$. Autrement dit, $(\alpha_1, \ldots, \alpha_n)$ est une base de $\mathcal{O}_K$ comme $\mathbb{Z}$-module.

Théorème 1.66. *Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ un corps quadratique, avec d un entier rationnel sans facteur carré. Alors :*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right] & si\ d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & si\ d \equiv 1 \pmod 4 \end{cases}.$$

Démonstration. Un élément $\alpha = a + b\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right)$ est entier algébrique si, et seulement si il est racine d'une équation à coefficients dans $\mathbb{Z}$.

Ainsi, α est racine de $X^2 - 2aX + \left(a^2 - b^2 d\right) \in \mathbb{Z}[X]$, ce qui entraine que la trce et la norme de α sont dans $\mathbb{Z}$. On en tire que

$$\begin{cases} 2a \in \mathbb{Z} & (1) \\ \text{et} & \\ a^2 - b^2 d \in \mathbb{Z} & (2) \end{cases}$$

La propriété (2) entraine :

$$4\left(a^2 - db^2\right) = (2a)^2 - d(2b)^2 \in 4\mathbb{Z} \subset \mathbb{Z},$$

ce qu montre que $d\left(2b^2\right) \in \mathbb{Z}$, et comme d est sans facteur carré, alors $2b \in \mathbb{Z}$.

Posons alors $a' = 2a$ et $b' = 2b$, alors $a'^2 - db'^2 \in 4\mathbb{Z}$.

Si $d \equiv 1 \pmod 4$, alors $a'^2 \equiv b'^2 \pmod 4$ ce qui veut dire que a' et b' sont de même parité.

Si $d \equiv 2,3 \pmod 4$, sachant que $db'^2 \equiv 0, 2 \text{ ou } 3 \pmod 4$ et que $a'^2 \equiv 0 \text{ ou } 1 \pmod 4$, alors $a'^2 \equiv 0 \pmod 4$ et $db'^2 \equiv 0 \pmod 4$ ce qui entraine que $a'^2 \equiv b'^2 \equiv 0 \pmod 4$ et donc $a', b' \in 2\mathbb{Z}$.

En résumé,

— Si $d \equiv 1 \pmod 4$, alors $\alpha = \frac{1}{2}(a' + b'\sqrt{d})$ avec a' et b' de même parité,

— Si $d \equiv 2,3 \pmod 4$, alors $\alpha = a + b\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$

□

Proposition 1.67. *Si $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ sont deux bases intégrales de $\mathcal{O}_K$ alors*

$$D(x_1, \ldots, x_n) = D(y_1, \ldots, y_n)$$

Démonstration. On note par (a_{ij}) et ${}^t(a_{ij})$ les matrices de passage de la base $(x_1, \ldots, x_n)$ à la base $(y_1, \ldots, y_n)$ et de la base $(y_1, \ldots, y_n)$ à la base $(x_1, \ldots, x_n)$, alors (d'aprés proposition 1.56)

$$D(y_1, \ldots, y_n) = det(a_{ij})^2 D(x_1, \ldots, x_n),$$

avecc $det(a_{ij}) \in \mathbb{Z}$, ce qui donne

$$det\left((a_{ij})\,{}^t(a_{ij})\right)^2 = det\left({}^t a_{ij}\right)^2 det\,(a_{ij})^2 = 1$$

puisque $det\,({}^t a_{ij})^2 \in \mathbb{Z}^*$ est inversible, en d'autres termes $det\,({}^t a_{ij})^2 = det\,(a_{ij})^2 = 1$ ou -1, ce qui montre $det\,({}^t a_{ij})^2 = det\,(a_{ij})^2 = 1$, d'où

$$D(x_1, \ldots, x_n) = D(y_1, \ldots, y_n)$$

□

Définition 1.68. Soient K un corps de nombres d'anneau d'entiers $\mathcal{O}_K$, le discriminant d'une base intégrale de $\mathcal{O}_K$ est appelé discriminant du corps K, qu'on notera d_K.

Exemple 1.69. Déterminons le discriminant du corps de nombres K dans chacun de cas suivant

1. Soit $m \in \mathbb{Z}$ un entier sans facteur carré, on pose $K = \mathbb{Q}(\sqrt{m})$.

   D'après le (Théorème 1.66) , alors $\mathcal{O}_K = \mathbb{Z}[\theta]$ où θ est donné par

   $$\theta = \begin{cases} \sqrt{m} & \text{si } m \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{m}}{2} & \text{si } m \equiv 1 \pmod 4 \end{cases}$$

   Ainsi, le discriminant D_K du corps K est

   $$D_K = \begin{cases} \operatorname{disc}(1, \sqrt{m}) & \text{si } m \equiv 2,3 \pmod 4 \\ \operatorname{disc}\left(1, \frac{1+\sqrt{m}}{2}\right) & \text{si } m \equiv 1 \pmod 4 \end{cases}$$

   ce qui donne

   $$D_K = \begin{cases} 4m & \text{si } m \equiv 2,3 \pmod 4 \\ m & \text{si } m \equiv 1 \pmod 4 \end{cases}$$

2. Soit $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, une base intégrale de l'anneau $\mathcal{O}_K$ des entiers de K est $\left\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\right\}$.

   Sachant que le discriminant de la base $\left\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\right\}$ est celui du polynôme minimal, $X^3 - 2$, du générateur $\alpha = \sqrt[3]{2}$ de K sur $\mathbb{Q}$, alors

   $$\operatorname{disc}\left(1, \sqrt[3]{2}, \sqrt[3]{2^2}\right) = -3^3 \times 2^2 = -108$$

   Ainsi, le discriminant D_K du corps K est

   $$D_K = disc\left(1, \sqrt[3]{2}, \sqrt[3]{2^2}\right) = -108$$

Proposition 1.70. *Si $[K : \mathbb{Q}] = n$ et les nombres $a_1, ..., a_n$ de $\mathcal{O}_K$ sont linéairement indépendant sur $\mathbb{Q}$, alors*

$$D(a_1, ...a_n) = m^2 d_k$$

où m est l'indice dans $\mathcal{O}_K$ du $\mathbb{Z}$-module M engendré par les a_i.

Démonstration. (cf . [30, proposition 2.13]).

□

1.4 Ramification Dans un corps de nombres

Dans cette partie, K et L seront des corps de nombres, avec $K \subset L$. De plus $\mathcal{O}_K$ et $\mathcal{O}_L$ désigneront les anneaux des entiers de K et L. Le terme idéal premier désignera un idéal premier non nul.

Théorème 1.71. *[25, Théorème 19] Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$, alors on a les équivalences suivantes :*
$\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L \Leftrightarrow \mathfrak{P} \supset \mathfrak{p}\mathcal{O}_L \Leftrightarrow \mathfrak{P} \supset \mathfrak{p} \Leftrightarrow \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \Leftrightarrow \mathfrak{P} \cap K = \mathfrak{p}$

Définition 1.72. Quand les conditions équivalentes du théorème sont remplies, on dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$

Remarque 1.73. Les idéaux premiers au-dessus de $\mathfrak{p}$ sont les diviseurs de $\mathfrak{p}\mathcal{O}_L$.

Théorème 1.74. *Tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ est au-dessus d'un unique idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. Tout idéal premier $\mathfrak{p}$ est en-dessous d'au moins un idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$*

Démonstration. Montrons que $\mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier non nul. Il est non nul car il contient la norme de chacun des éléments de $\mathfrak{P}$. De plus, il est premier, car si a et b sont dans $\mathcal{O}_K$ et $ab \in \mathfrak{P} \cap \mathcal{O}_K$, alors $a \in \mathfrak{P} \cap \mathcal{O}_K$, ou $b \in \mathfrak{P} \cap \mathcal{O}_K$. Enfin il ne contient pas 1, et est donc différent de $\mathcal{O}_K$.

Pour la seconde partie, les idéaux premiers au-dessus de $\mathfrak{p}$ sont les diviseurs de $\mathfrak{P}\mathcal{O}_L$. Montrons que $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, et a donc au moins un diviseur. De manière équivalente, nous devons montrer que $1 \notin \mathfrak{p}\mathcal{O}_L$. D'après[25, lemme 2 du théorème 15] , $\exists \gamma \in K - \mathcal{O}_K$ tel que $\gamma\mathfrak{p} \subset \mathcal{O}_K$. Ainsi $\gamma\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$. Si $1 \in \mathfrak{p}\mathcal{O}_L$, alors $\gamma \in \mathcal{O}_L$, et est donc un entier algébrique, ce qui contredit le choix de γ.

□

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. comme L'ensemble des idéaux premiers $\mathfrak{P}$ de $\mathcal{O}_L$ qui contiennent $\mathfrak{p}\mathcal{O}_L$ est fini il existe donc une décomposition, unique à l'ordre près des facteurs,

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_1^{e_1} ... \mathfrak{P}_g^{e_g}$$

où $g \geq 1$ est un entier ,$\mathfrak{P}_1, ..., \mathfrak{P}_g$ sont des idéaux premiers de $\mathcal{O}_L$, distincts deux à deux.

Définition 1.75. On appelle indice de ramification de $\mathfrak{P}$ sur $\mathfrak{p}$, la puissance exacte $\mathfrak{P}^e$ de $\mathfrak{P}$ qui divise $\mathfrak{p}\mathcal{O}_L$, noté $e(\mathfrak{P} \mid \mathfrak{p})$.

Proposition 1.76. *Soit $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$, alors $\mathcal{O}_L/\mathfrak{P}$ et $\mathcal{O}_K/\mathfrak{p}$ sont des corps finis, et $\mathcal{O}_K/\mathfrak{p}$ s'injecte canoniquement dans $\mathcal{O}_L/\mathfrak{P}$. On appelle degré résiduel de $\mathfrak{P}$ et on note $f(\mathfrak{P} \mid \mathfrak{p})$ l'entier $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p},]$.*

Démonstration. $\mathfrak{p}$ et $\mathfrak{P}$ sont maximaux, donc $\mathcal{O}_K/\mathfrak{p}$ et $\mathcal{O}_L/\mathfrak{P}$ sont des corps. Ils sont finis, [25, preuve de théorème 14]. On a donc le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{i} & \mathcal{O}_L \\ & & \downarrow \pi \\ & & \mathcal{O}_L/\mathfrak{P} \end{array}$$

Le noyau de $\pi \circ i$ est $\mathcal{O}_K \cap \mathfrak{P} = \mathfrak{p}$, d'après le théorème 1.74 . Il se factorise donc en :

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{i} & \mathcal{O}_L \\ \downarrow & & \downarrow \pi \\ \mathcal{O}_K/\mathfrak{p} & \xrightarrow[i']{} & \mathcal{O}_L/\mathfrak{P} \end{array}$$

Or i' est un morphisme d'anneaux entre corps et est donc injective.

□

Proposition 1.77. *Si on a trois corps de nombres $K \subset L \subset M$, d'anneaux d'entiers respectifs $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$, et des idéaux premiers $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{r}$, alors :*

$$e(\mathfrak{r} \mid \mathfrak{p}) = e(\mathfrak{r} \mid \mathfrak{q})e(\mathfrak{q} \mid \mathfrak{p}) \quad et \quad f(\mathfrak{r} \mid \mathfrak{p}) = f(\mathfrak{r} \mid \mathfrak{q})f(\mathfrak{q} \mid \mathfrak{p})$$

Démonstration. On a

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}\mathfrak{q}_2 ... \mathfrak{q}_k.$$

De même :

$$\mathfrak{q}\mathcal{O}_M = \mathfrak{r}^{e(\mathfrak{r}|\mathfrak{q})}\mathfrak{r}_2...\mathfrak{r}_n,$$

donc

$$\mathfrak{p}\mathcal{O}_M = (\mathfrak{q}\mathcal{O}_M)^{e(\mathfrak{q}|\mathfrak{p})}(\mathfrak{q}_2\mathcal{O}_M)...(\mathfrak{q}_k\mathcal{O}_M) = \mathfrak{r}^{e(\mathfrak{q}|\mathfrak{p})e(\mathfrak{r}|\mathfrak{q})}\mathfrak{r}'_{2,1}...\mathfrak{r}'_{k,n_k},$$

avec $\mathfrak{r}_{i,j}$ au-dessus de $\mathfrak{q}_i$, et donc différents de $\mathfrak{r}$. D'où la première égalité par unicité de la décomposition. La deuxième vient du diagramme suivant et de la formule de multiplicativité des degrés

$$\begin{array}{ccccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_L & \longrightarrow & \mathcal{O}_M \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{O}_K/\mathfrak{p} & \longrightarrow & \mathcal{O}_L/\mathfrak{q} & \longrightarrow & \mathcal{O}_M/\mathfrak{r} \end{array}$$

□

Théorème 1.78. *Soit $n = [L : K]$ et soient $\mathfrak{P}_1, ..., \mathfrak{P}_g$, les idéaux premiers de $\mathcal{O}_L$ au-dessus d'un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. Soient $e_1, ..., e_g$ et $f_1, ..., f_g$ leurs degrés de ramification et résiduel respectifs. Alors :*

$$\sum_{i=1}^{g} e_i f_i = n$$

Nous allons démontrer ce théorème en même temps que le suivant. Pour un idéal $\mathfrak{i}$ de $\mathcal{O}_K$, on rappelle que $|\mathcal{O}_K/i|$ est fini et se note $\|\mathfrak{i}\|$.

Théorème 1.79. *Soit $n = [L : K]$. Alors :*

1. *Pour les idéaux $\mathfrak{i}$ et $\mathfrak{j}$ de $\mathcal{O}_K$, on a :*

$$\|\mathfrak{i}\| \, \|\mathfrak{j}\| = \|\mathfrak{ij}\|$$

2. *Soit $\mathfrak{i}$ un idéal de $\mathcal{O}_K$, alors : $\mathfrak{i}\mathcal{O}_L = \|\mathfrak{i}\|^n$*

Démonstration. Nous allons montrer 1 dans le cas où $\mathfrak{i}$ et $\mathfrak{j}$ sont premiers entre eux, puis que $\|\mathfrak{p}^m\| = \|\mathfrak{p}\|^m$ pour tout idéal premier $\mathfrak{p}$. Ce qui impliquera que

$$\|\mathfrak{p}_1^{m_1}...\mathfrak{p}_r^{m_r}\| = \|\mathfrak{p}_1\|^{m_1} ... \|\mathfrak{p}_r\|^{m_r} .$$

En factorisant $\mathfrak{i}$ et $\mathfrak{j}$ en idéaux premiers et en appliquant la formule ci-dessus.

Supposons que $\mathfrak{i}$ et $\mathfrak{j}$ sont premiers entre eux. Alors d'aprés [25, théorème 17]

$$\mathfrak{i}+\mathfrak{j}=\mathcal{O}_K \text{ et } \mathfrak{i}\cap\mathfrak{j}=\mathfrak{ij}$$

. D'après le théorème des restes chinois, on a donc un isomorphisme :

$$\mathcal{O}_K/\mathfrak{ij}\longrightarrow \mathcal{O}_K/\mathfrak{i}\times\mathcal{O}_K/\mathfrak{j}.$$

On a donc

$$\|\mathfrak{ij}\|=\|\mathfrak{i}\|\,\|\mathfrak{j}\|\,.$$

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On a une chaîne d'idéaux :

$$\mathcal{O}_K\supset\mathfrak{p}\supset\cdots\supset\mathfrak{p}^m.$$

Il suffit donc de montrer que $\|\mathfrak{p}\|=\left|\mathfrak{p}^k/\mathfrak{p}^{k+1}\right|$, pour tout k, où les $\mathfrak{p}^k$ sont considérés comme des groupes additifs. Soit $\alpha\in\mathfrak{p}^k\setminus\mathfrak{p}^{k+1}$.

On a un isomorphisme clair :

$$\mathcal{O}_K/\mathfrak{p}\longrightarrow \alpha\mathcal{O}_K/\alpha\mathfrak{p}$$

Or on a l'inclusion $\alpha O_K\subset\mathfrak{p}^k$, ce qui induit :

$$\alpha O_K\longrightarrow \mathfrak{p}^k/\mathfrak{p}^{k+1}$$

Le noyau de ce morphisme est $(\alpha O_K)\cap\mathfrak{p}^{k+1}$, et l'image $((\alpha O_K)+\mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}$.

$\mathfrak{p}^k$ est l'exacte puissance de $\mathfrak{p}$ qui divise αO_K, d'où $(\alpha O_K)+\mathfrak{p}^{k+1}=\mathfrak{p}^k$, car c'est le plus grand commun diviseur. $(\alpha O_K)+\mathfrak{p}^{k+1}=\alpha\mathfrak{p}$ car c'est le plus petit commun multiple de $\alpha O_K=\mathfrak{p}^k\mathfrak{q}_1\cdots\mathfrak{q}_r$ et $\mathfrak{p}^{k+1}$.

□

Nous allons ensuite démontrer un cas particulier du théorème 1.78 ; dans le cas où $K=\mathbb{Q}$ et $\mathfrak{p}=p\mathbb{Z}$, pour un nombre premier p.

Démonstration. On a :

$$\mathfrak{p}\mathcal{O}_L=\prod_{i=1}^{r}\mathfrak{P}_i^{e_i}$$

Donc :

$$\|\mathfrak{p}\mathcal{O}_L\|=\prod_{i=1}^{r}\|\mathfrak{P}_i\|^{e_i}=\prod_{i=1}^{r}(p^{f_i})^{e_i}$$

On sait de plus que : $\mathfrak{p}\mathcal{O}_L = p^n$, ce qui établit le résultat.

□

Pour démontrer le 2 du théorème 1.79, nous avons besoin du lemme suivant :

Lemme 1.80. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls d'un anneau de Dedekind $\mathcal{R}$, tels que $\mathfrak{b} \subset \mathfrak{a}$ et $\mathfrak{a} \neq \mathcal{R}$. Alors il existe un $\gamma \in K$, l'anneau des fractions de $\mathcal{R}$, tel que $\gamma\mathfrak{b} \subset \mathcal{R}$ et $\gamma\mathfrak{b} \not\subseteq \mathfrak{a}$.*

Démonstration. Par [25, théorème 15], il existe un idéal non nul $\mathfrak{c}$ tel que $\mathfrak{b}\mathfrak{c} = (\alpha)$. Alors $\mathfrak{b}\mathfrak{c} \not\subseteq \alpha\mathfrak{a}$, soit $\beta \in \mathfrak{c}$ tel que $\beta\mathfrak{b} \not\subseteq \alpha\mathfrak{a}$.

Alors $\gamma = \beta/\alpha$ convient.

□

Nous pouvons démontrer le 2 du théorème 1.79

Démonstration. Il suffit de le démontrer pour $\mathfrak{p}$ idéal premier, et d'appliquer le 1, et le théorème de décomposition en idéaux premiers. Remarquons que $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ est un espace vectoriel sur le corps $\mathcal{O}_K/\mathfrak{p}$, car c'est un anneau qui contient $\mathcal{O}_K/\mathfrak{p}$. Il faut démontrer que sa dimension est n. Elle est au plus n : en effet, si $\alpha_1, ..., \alpha_{n+1} \in \mathcal{O}_L$, ils sont linéairement dépendants sur K, et donc sur $\mathcal{O}_K$.

Donc il existe $\beta_1, ..., \beta_{n+1} \in \mathcal{O}_K$ non tous nuls tels que $\sum_{i=1}^{n+1} \beta_i\alpha_i = 0$. Il faut réduire l'équation modulo $\mathfrak{p}$. Mais si tous les β_i sont dans $\mathfrak{p}$, alors il faut appliquer le lemme à $\mathfrak{a} = \mathfrak{p}$, et $\mathfrak{b} = (\beta_1, ..., \beta_{n+1})$, et on obtient alors le résultat.

Il faut montrer qu'on a bien l'égalité. Soit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, et considérons les idéaux premiers $\mathfrak{p}_i$ de $\mathcal{O}_K$ au-dessus de p.

Soit $n_i = Dim_{\mathcal{O}_K/\mathfrak{p}_i}(\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L) \leq n$.

Nous allons montrer l'égalité pour tout i. Soit $e_i = e(\mathfrak{p}_i|p)$ et $f_i = f(\mathfrak{p}_i|p)$. Alors $\sum_i e_i f_i = [K : \mathbb{Q}] = m$, d'après le cas particulier du théorème 1.78. On a $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$, donc $p\mathcal{O}_L = \prod_i (\mathfrak{p}_i\mathcal{O}_L)^{e_i}$, d'après le 1, on a

$$\|p\mathcal{O}_L\| = \prod_i \|\mathfrak{p}_i\mathcal{O}_L\|^{e_i} = \prod_i \|\mathfrak{p}_i\|^{n_i e_i} = \prod_i (p^{f_i})^{n_i e_i} = p^{mn}.$$

Donc $mn = e_i f_i n_i$. Comme pour tout i, $n_i \leq n$, et $\sum_i e_i f_i = m$, on a l'égalité pour tout i.

□

Démonstration. **(cas général du théorème 1.78)**

On a

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i},$$

d'où :

$$\|\mathfrak{p}\mathcal{O}_L\| = \prod \|\mathfrak{P}_i\|^{e_i} = \prod \|\mathfrak{p}\mathcal{O}_L\|^{f_i e_i} = \|\mathfrak{p}\|^n$$

D'après le théorème 1.79 1 et 2 ; et la définition des f_i. D'où le résultat..

□

Définition 1.81. Suivant les notations ci-dessus :

- On dit que $\mathfrak{P}_i$ est ramifié au dessus de $\mathfrak{p}$ si l'indice de ramification $e(\mathfrak{P}_i \mid \mathfrak{p})$ est ≥ 2.
- On dit que $\mathfrak{p}$ est ramifié dans L si l'un des $\mathfrak{P}_i$ est ramifié.
- On dit que $\mathfrak{p}$ est totalement ramifie si $e(\mathfrak{P} \mid \mathfrak{p}) = n$. (et donc $g = 1$ et $f(\mathfrak{P} \mid \mathfrak{p}) = 1$).
- On dit que $\mathfrak{p}$ est totalement décomposé dans K si $g = n$ et donc on a $e_i = f_i = 1$, $1 \leq i \leq n$.
- On dit que $\mathfrak{p}$ est inerte si $g = e_1 = 1$ (c-à-d. $\mathfrak{p}\mathcal{O}_L$ est premier).

1.5 Ramification dans un extension normale

Dans cette partie , L/K est une extension normale des corps des nombres . G sera le groupe de Galois $Gal(L/K)$; son ordre est $n = [L : K]$. On fixe $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. alors on a :

Théorème 1.82. *Soit L une extension normale de K, $\mathfrak{P}_1$ et $\mathfrak{P}_2$, deux idéaux premiers au-dessus de $\mathfrak{p}$, idéal premier de $\mathcal{O}_K$. Alors il existe $\sigma \in Gal(L/K)$ tel que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.*

Démonstration. Supposons que $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2$ pour tout $\sigma \in Gal(L/K)$. Alors, d'après le théorème des restes chinois, on a une solution du système de congruences :

$$\begin{aligned} x &\equiv 0 \mod \mathfrak{P}_2 \\ x &\equiv 1 \mod \sigma(\mathfrak{P}_1) \text{ pour tout } \sigma \in Gal(L/K) \end{aligned}$$

Soit $\alpha \in \mathcal{O}_L$ une telle solution, nous avons $N_{L/K}(\alpha) \in \mathcal{O}_K \bigcap \mathfrak{P}_2 = \mathfrak{p}$. D'un autre côté, on a $\alpha \notin \sigma(\mathfrak{P}_1)$, ainsi $\sigma^{-1}(\alpha) \notin \mathfrak{P}_1$. Comme$N_{L/K}(\alpha)$ est le produit des $\sigma^{-1}(\alpha)$, et aucun n'est dans l'idéal premier $\mathfrak{P}_1$, alors $N_{L/K}(\alpha) \notin \mathfrak{P}_1$, ce qui est une contradiction.

□

Corollaire 1.83. *Si L est normale sur K, et $\mathfrak{P}_1$, $\mathfrak{P}_2$ sont deux idéaux premiers au-dessus de $\mathfrak{p}$, idéal premier de $\mathcal{O}_K$; alors $e(\mathfrak{P}_1 \mid \mathfrak{p}) = e(\mathfrak{P}_2 \mid \mathfrak{p}) = e$ et $f(\mathfrak{P}_1|p) = f(\mathfrak{P}_2|\mathfrak{p}) = f$. De plus, si g est le nombre d'idéaux premier distincts de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, alors*

$$gef = [L : K].$$

Théorème 1.84. Soit p un nombre premier de $\mathbb{Z}$, on suppose que p est ramifié dans un anneau d'entiers $\mathcal{O}_K$, alors $p|d_K$.

Démonstration. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ tel que $e(\mathfrak{p}|p) > 1$. $p\mathcal{O}_K = \mathfrak{p}\mathfrak{i}$, où $\mathfrak{i}$ est un idéal divisible par tous les idéaux premiers au-dessus de p. Soient $\sigma_1, ..., \sigma_n$, les plongements de K dans $\mathbb{C}$, étendus en automorphismes de L, une clôture normale de de K . Soit $\{\alpha_1, ..., \alpha_n\}$ une base intégrale de $\mathcal{O}_K$. Soit $\alpha \in \mathfrak{i} \setminus p\mathcal{O}_K \neq \emptyset$ que l'on écrit $\alpha = \sum m_i\alpha_i$, avec $m_i \in \mathbb{Z}$. Comme $\alpha \notin p\mathcal{O}_K$, alors il y a au moins un des m_i qui n'est pas divisible par p. On peut supposer que $p \nmid m_1$. Soit $d_K = D(\alpha_1, ..., \alpha_n)$; alors il est facile de voir que $D(\alpha, \alpha_2, ..., \alpha_n) = m_1^2 d_K$. Il suffit donc de montrer que $p \mid D(\alpha, \alpha_2, ..., \alpha_n)$. Comme α est dans tous les idéaux premiers de $\mathcal{O}_K$ au-dessus de p, il est dans tous les idéaux premiers de $\mathcal{O}_L$ au-dessus de p. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de p. Alors $\sigma^{-1}(\mathfrak{P})$est aussi un idéal premier au-dessus de p, et donc $\sigma(\alpha) \in \mathfrak{P}$, pour tout σ. Donc $\mathfrak{P}$ contient $D(\alpha, \alpha_2, ..., \alpha_n)$. Comme le déterminant est dans $\mathbb{Z}$, il est donc dans $\mathbb{Z} \cap \mathfrak{P} = p\mathbb{Z}$..

□

Corollaire 1.85. *Il n'y a qu'un nombre fini de nombres premiers ramifiés dans $\mathcal{O}_K$.*

Corollaire 1.86. *Il n'y a qu'un nombre fini d'idéaux premiers de $\mathcal{O}_K$ qui se ramifient dans $\mathcal{O}_L$.*

Démonstration. Si $\mathfrak{p}$ est un idéal premier qui se ramifie dans $\mathcal{O}_L$, alors $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ donc p est un nombre premier qui se ramifie dans $\mathcal{O}_L$, or ils sont en nombre fini, et il n'y a qu'un nombre fini d'idéaux premiers dans $\mathcal{O}_K$ au-dessus de chacun d'eux.

□

Définition 1.87. On définit deux sous-groupes de G importants pour la suite :

Le groupe de décomposition $D = D(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in G, \sigma\mathfrak{P} = \mathfrak{P}\}$

Le groupe d'inertie $I = I(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in G, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}, \forall \alpha \in \mathcal{O}_L\}$.

Il est clair que D et I sont des sous-groupes de G, et que $I \subset D$. (La condition $\sigma\mathfrak{P} = \mathfrak{P}$ peut être exprimée comme $\sigma(\alpha) \equiv 0 (\mathrm{mod} \mathfrak{P}) \Leftrightarrow \alpha \equiv 0 (\mathrm{mod} \mathfrak{P})$; évidemment la condition pour I implique ceci.)

Proposition 1.88. *Soit $\sigma \in D$, nous avons alors le diagramme commutatif suivant :*

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \pi \downarrow & & \downarrow \pi \\ \mathcal{O}_L/\mathfrak{P} & \xrightarrow[\bar{\sigma}]{} & \mathcal{O}_L/\mathfrak{P} \end{array}$$

avec $\bar{\sigma} \in Gal(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p}) = \bar{G}$.

Démonstration. $\pi \circ \sigma$ est un morphisme d'anneau de noyau $\sigma^{-1}(\mathfrak{P}) = \mathfrak{P}$, donc il se factorise en un morphisme $\bar{\sigma}$ de $\mathcal{O}_L/\mathfrak{P}$ dans lui-même. Ce sont des corps car $\mathfrak{P}$ est premier donc maximal, donc le morphisme est injectif, et comme ils sont finis [25, preuve de théorème 14], c'est un automorphisme.

□

De plus σ fixe point par point $\mathcal{O}_K$, et $\mathfrak{P} \bigcap \mathcal{O}_K = \mathfrak{p}$, donc $\bar{\sigma}$ fixe $\mathcal{O}_K/\mathfrak{p}$ point par point donc par définition de I , on a

Corollaire 1.89. *On a un morphisme de groupe :*

$$\Psi : \begin{cases} D \longrightarrow \bar{G} \\ \sigma \longrightarrow \bar{\sigma} \end{cases}$$

Son noyau est I et donc :

- $I \lhd D$
- $Im(\Psi) \simeq D/I$.

Si H est un sous-groupe de G, nous noterons L^H le sous-corps de L des invariant par H. Si X est une partie de L , alors X^Hsera $X \cap L^H$, donc $\mathcal{O}_L^H$sera l'anneau des entiers de L^H , et $\mathfrak{P}^H$, l'unique idéal premier de $\mathcal{O}_L^H$, en dessous de $\mathfrak{P}$. De plus $\mathfrak{P}^H$ est au-dessus de $\mathfrak{p}$, et donc $\mathcal{O}_L^H/\mathfrak{P}^H$ est un corps intermédiaire entre $\mathcal{O}_L/\mathfrak{P}$ et $\mathcal{O}_K/\mathfrak{p}$.

Théorème 1.90. *nous avons alors le diagramme commutatif suivant :*

degré	L	$\mathfrak{P}$	*Indices de ramification*	*Degréd'inertie*
e	|	|	e	1
	L^I	$\mathfrak{P}^I$		
f	|	|	1	f
	L^D	$\mathfrak{P}^D$		
g	|	|	1	1
	K	$\mathfrak{p}$		

L^D s'appelle le corps de décomposition, et L^I, le corps d'inertie.

Démonstration. Commençons par montrer que $[L^D : K] = g$. D'après la théorie de Galois, on sait que $[L^D : K] = [G : D]$. Or chaque classe à droite σD envoie $\mathfrak{P}$ sur $\sigma\mathfrak{P}$, et il est clair que $\sigma D = \tau D \Leftrightarrow \sigma P = \tau\mathfrak{P}$. Nous avons donc une bijection entre les classes à droite de D et les $\sigma\mathfrak{P}$. D'après le théorème 1.82, cela inclut tout ceux de la décomposition de $\mathfrak{p}\mathcal{O}_L$, et il ne peux y avoir que ceux-là. Comme il y en a g, on a bien le résultat. Montrons que $e(\mathfrak{P}^D \mid \mathfrak{p}) = f(\mathfrak{P}^D \mid \mathfrak{p}) = 1$. Comme L est une extension normale de L^D, et que son groupe de Galois est D, $\mathfrak{P}$ est le seul idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{P}^D$, car ils sont necessairement permutés de manière transitive par D. D'après le théorème 1.78 : $[L : L^D] = e(\mathfrak{P}|\mathfrak{P}^D)f(\mathfrak{P} \mid \mathfrak{P}^D)$. Le nombre de gauche est ef, car on a déja vu que $[L^D : K] = g$ et $gef = n$. D'après la multiplicativité de e et f (cf proposition 1.77), donc on a bien le résultat souhaité.

Montrons que $f(\mathfrak{P} \mid \mathfrak{P}^I) = 1$, ce qui équivaut à montrer que $\mathcal{O}_L/\mathfrak{P} = \mathcal{O}_L^I/\mathfrak{P}^I$. Il suffit donc de montrer que $Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_L^I/\mathfrak{P}^I))$ est trivial. Soit $\theta \in \mathcal{O}_L/\mathfrak{P}$, il faut montrer que $\theta \in \mathcal{O}_L^I/\mathfrak{P}^I$

Nous allons montrer pour cela que le polynôme $(X-\theta)^m$ est à coefficients dans $\mathcal{O}_L^I/\mathfrak{P}^I$, pour un certain $m > 0$. Dans ce cas le groupe de Galois envoie θ sur un de ses conjugués qui ne pourra être que θ, et on aura le résultat souhaité. Soit $\alpha \in \mathcal{O}_L$ correspondant à $\theta \in \mathcal{O}_L/\mathfrak{P}$, par la projection canonique. Alors

$$P(X) = \prod_{\sigma \in I}(X - \sigma(\alpha))$$

est à coefficients dans $\mathcal{O}_L^I$; en réduisant modulo $\mathfrak{P}$, on trouve $\bar{P} \in (\mathcal{O}_L/\mathfrak{P})[X]$, qui a ses coefficients dans $\mathcal{O}_L^I/\mathfrak{P}^I$. Mais tous les $\sigma(\alpha)$ se réduisent en θ, par définition de I. Donc $\bar{P}(X) = (X - \theta)^{|I|}$.

Ainsi, $\forall \theta \in \mathcal{O}_L/\mathfrak{P}$, $\forall \sigma \in Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_L^I/\mathfrak{P}^I))$, $\sigma(\theta) = \theta$ c-à-d. $\sigma = id$, ce qui prouve $f(\mathfrak{P} \mid \mathfrak{P}^I) = 1$.

Avec $f(\mathfrak{P}^D \mid \mathfrak{p}) = 1$, on a $f(\mathfrak{P}^I \mid \mathfrak{P}^D) = f(\mathfrak{P} \mid \mathfrak{p}) = f$. Donc, d'après le théorème 1.78, $[L^I : L^D] \geq f$. Mais nous avons vu que $I \lhd D$, et que D/I se plonge dans $\bar{G}$, de cardinal f. Donc $L^D \subset L^I$ est normale, de groupe de Galois D/I, et donc $[L^I : L^D] = |D/I| \leq f$, donc on a l'égalité. Donc on en déduit que $e(\mathfrak{P}^I \mid \mathfrak{P}^D) = 1$. Finalement, on en déduit facilement que $[L : L^I] = e$, et que $e(\mathfrak{P} \mid \mathfrak{P}^I) = e$.

□

Corollaire 1.91. *D/I est cyclique d'ordre f.*

Démonstration. On a déja vu que D/I se plonge dans $\bar{G}$ qui est cyclique d'ordre f. De plus, les deux groupes ont même cardinal f car $|D/I| = [L^I : L^D]$, d'où le résultat..

□

Soit K', un corps intermédiaire entre K et L . Il existe H un sous-groupe de G tel que $K' = L^H$. L'anneau des entiers de K' est $\mathcal{O}_L^H$. Soit $\mathfrak{p}' = \mathfrak{P} \cap \mathcal{O}_{K'}$, l'unique idéal premier de $\mathcal{O}_{K'}$ en dessous de $\mathfrak{P}$, alors $\mathfrak{p}'$ est au-dessus de $\mathfrak{p}$. L est une extension normale de K', et on a :

$$D(\mathfrak{P} \mid \mathfrak{p}') = D \cap H \text{ et } I(\mathfrak{P} \mid \mathfrak{p}') = I \cap H$$

On en déduit, de par la théorie de Galois, que $L^D K'$ et $L^I K'$ sont les corps de décomposition et d'inertie pour $\mathfrak{P}$ sur $\mathfrak{p}'$. De plus, on a les caractérisations :

Théorème 1.92. *Avec les notations ci-dessus*

L^D est le plus grand corps intermédiaire K' tel que $e(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{p}' \mid \mathfrak{p}) = 1$

L^D est le plus petit corps intermédiaire K' tel que $\mathfrak{P}$ est le seul idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}'$.

L^I est le plus grand corps intermédiaire K' tel que $e(\mathfrak{p}' \mid \mathfrak{p}) = 1$ et $f(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{P} \mid \mathfrak{p}) = f$

L^I est le plus petit corps intermédiaire K' tel que $\mathfrak{p}'$ est totalement ramifié dans L (c-à-d. $e(\mathfrak{P} \mid \mathfrak{p}') = [L : K']$).

Démonstration. (cf. [25, théorème 29]).

□

Chapitre 2

Corps de nombres $p-$adiques

2.1 Définitions et notations

Définition 2.1. Soit K un corps. Une valeur absolue sur K est une application $x \longmapsto |x|$ de K dans $\mathbb{R}_+$ vérifiant les trois propriétés suivantes :

(i) $|x| = 0 \Leftrightarrow x = 0 \; \forall x \in K$;

(ii) $|xy| = |x|\,|y| \; \forall x, y \in K$;

(iii) $|x + y| \leq |x| + |y| \; \forall x, y \in K$.

Une valeur absolue sur K est dite non archimédienne, si elle vérifie la condition

(iii') $|x + y| \leq \max(|x|\,, |y|) \forall x, y \in K$

sinon, on dira que la valeur absolue est archimédienne.

Si K est un corps muni d'une valeur absolue $||$, et x, y sont deux éléments de K, on pose $d(x, y) = |x - y|$. Les propriétés (i) et (iii) de la valeur absolue assurent que d est une distance sur K et donc définit une topologie sur K.

Lemme 2.2. *Si $||$ est non archimédienne et $|x| \neq |y|$, alors $|x + y| = max(|x|\,, |y|)$ $\forall x, y \in K$.*

Démonstration. — Quitte à permuter x et y, on peut supposer $|x| > |y|$. On a alors

$$|x + y| \leq |x| = |(x + y) - y| \leq \max(|x + y|\,, |y|)$$

et comme $|y| < |x|$, on en déduit l'égalité $\max(|x + y|\,, |y|) = |x + y|$, ce qui permet de conclure.

□

Définition 2.3. Si K est un corps, une valuation υ sur K est une application $x \longmapsto \upsilon(x)$ de K dans $\mathbb{R} \cup +\infty$ vérifiant les trois conditions suivantes :

(i) $\upsilon(x) = +\infty \Leftrightarrow x = 0$.

(ii) $\upsilon(xy) = \upsilon(x) + \upsilon(y)\ \forall x, y \in K$

(iii) $\upsilon(x+y) \geq \min(\upsilon(x), \upsilon(y)) \forall x, y \in K$.

Remarque 2.4. (i) Si K est un corps muni d'une valeur absolue non archimédienne $||$ et si $\lambda < 0$, alors $\upsilon : K \longrightarrow \mathbb{R}^+ \cup +\infty$ défini par $\upsilon(x) = \lambda \log |x|$ est une valuation sur K.

(ii) Réciproquement, si υ est une valuation sur K et $0 < a < 1$, alors $|x| = a^{\upsilon(x)}$ est une valeur absolue non archimédienne sur K.

(iii) Il résulte du lemme 2.2 que l'on a $\upsilon(x+y) = \min(\upsilon(x), \upsilon(y))$, si $\upsilon(x) \neq \upsilon(y)$.

On dit que la valuation est discrète si $\upsilon(K^*)$ est un sous-groupe discret de $\mathbb{R}$ (il est alors de la forme $a\mathbb{Z}$) . Pour ce type de valuation, il existe donc $\pi \in K$ tel que $\upsilon(\pi)$ soit un générateur de $\upsilon(K^*)$. Un tel élément π est appelé une uniformisante de υ

Tout nombre $\alpha \in \mathbb{Q}$ s'écrit

$$\alpha = p^k \frac{a}{b}$$

où a et b sont premiers entre eux, p un nombre premier et $k \in \mathbb{Z}$.

Définition 2.5. On appelle valuation p-adique de $\alpha \in \mathbb{Q}$, l'entier k noté $v_p(\alpha)$.

Le nombre p^{-k} est appelé valeur absolue p-adique de α et est noté $|\alpha|_p$.

On écrit alors

$$v_p(\alpha) = k \text{ et } |\alpha|_p = p^{-k}.$$

De cette définition on obtient que

$$v_p(0) = +\infty \text{ et } |0|_p = 0.$$

Ce qui induit les applications suivantes

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\} \text{ et } |.|_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$$

vérifiant

$$v_p(ab) = v_p(a) + v_p(b) \text{ et } |ab|_p = |a|_p . |b|_p$$

$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\} \text{ et } |a+b|_p \leq \max\left\{|a|_p, |b|_p\right\}$$

$$v_p(a) = +\infty \Leftrightarrow a = 0 \text{ et } |a|_p = 0 \Leftrightarrow a = 0$$

La valeur absolue p-adique $|.|_p$ induit une métrique p-adique noté d_p définie par

$$d_p(a,b) = |a-b|_p .$$

Théorème 2.6. ***(Ostrowski)***. — *Une valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à la valeur absolue usuelle $||_\infty$ ou à la valeur absolue p-adique pour un nombre premier p.*

Démonstration. (cf.[15, théorème 3.1.4.]).

□

Lemme 2.7. *(formule du produit)*

Soit $\alpha \in \mathbb{Q}$, alors

$$\prod_v |\alpha|_v = 1$$

où $v \in \{+\infty, 2, 3, 5, \dots\}$ et où $|\alpha|_\infty$ représente la valeur absolu $|\alpha|$ réelle.

Démonstration. Il suffit de montrer la propriété pour α entier positif.

Soit donc α de la forme

$$\alpha = p_1^{t_1} \dots . p_g^{t_g}$$

alors

$$|\alpha|_v = \begin{cases} 1 & \text{si } v \neq p_i \\ p^{-t_i} & \text{si } v = p_i \\ p_1^{t_1} \dots . p_g^{t_g} & \text{si } v = +\infty \end{cases}$$

On en déduit que

$$\begin{aligned} \prod_v |\alpha|_v &= \prod_{i=1}^{g} |\alpha|_{p_i} . \prod_{v=+\infty} |\alpha|_v . \prod_{\substack{v \neq +\infty, \\ v \neq p_i, \forall i}} |\alpha|_v \\ &= \left(p_1^{-t_1} \dots . p_g^{-t_g}\right) . \left(p_1^{t_1} \dots . p_g^{t_g}\right) .1 = 1. \end{aligned}$$

□

Les nombres premiers, y compris celui à l'infini, sont appelés places de $\mathbb{Q}$.

L'ensemble des places de $\mathbb{Q}$ noté $\mathcal{M}_\mathbb{Q}$ est

$$\mathcal{M}_\mathbb{Q} = \{+\infty, 2, 3, 5, \dots\}.$$

Définition 2.8. Soit K un corps et soit $||$une valeur absolue sur K.

(i) Une suite d'éléments $u_n \in K$ est appelée une suite de Cauchy si pour tout $\epsilon > 0$ on peut trouver une borne M telle que l'on ait $|u_n - u_{n+p}| < \epsilon \ \forall, n \geq M$ et $p \in \mathbb{N}$.

(ii) Le corps K est dit complet par rapport à $||$ si toute suite de Cauchy d'éléments de K a une limite dans K.

(iii) Un sous-ensemble $S \subset K$ est dit dense en K si chaque boule ouverte autour de chaque élément de K contient un élément de S ; en symboles, si pour tout $x \in K$ et tout $\epsilon > 0$ on a

$$B(x, \epsilon) \cap S \neq \emptyset.$$

Soit K un corps et soit $||$une valeur absolue sur K, on note Ω l'ensemble des suites de Cauchy à valeurs dans K.

Soit $\mathfrak{I} \subset \Omega$ l'ensemble des suites tendant vers 0, i.e

$$\mathfrak{I} = \left\{ (u_n) \in \Omega;\ \text{tels que } \lim_{n \to +\infty} u_n = 0 \right\}$$

.

Lemme 2.9. *(i) Si $(a_n)_{n\in\mathbb{N}} \in \Omega$, alors la suite de terme général $|a_n|$ converge dans $\mathbb{R}_+$.*

(ii) Si on suppose de plus que $||$ est non archimédienne et que $(a_n)_{n\in\mathbb{N}} \notin \mathfrak{I}$, alors la suite de terme général $|a_n|$ est constante à partir d'un certain rang.

(iii) Si $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux éléments de Ω différant par un élément de $\mathfrak{I}$, alors

$$\lim_{n \to +\infty} |a_n| = \lim_{n \to +\infty} |b_n| .$$

Démonstration. L'inégalité triangulaire implique que l'on a $||a_{n+p}| - |a_n|| \leq |a_{n+p} - a_n|$ quels que soient n et p et donc que la suite de terme général $|a_n|$ est de Cauchy. On en déduit le (i).

D'autre part, si $(a_n)_{n\in\mathbb{N}} \in \Omega - \mathfrak{I}$ il existe $\delta > 0$ tel que l'on ait $|a_n| > \delta$ pour une infinité de n et la limite de la suite $|a_n|$ est donc supérieure ou égale à δ. Il existe donc $N \in \mathbb{N}$ tel que si $n > N$, alors $|a_n| > \frac{2}{3}\delta$ et $|a_{n+p} - a_n| < \frac{\delta}{2}$ quel que soit $p \in \mathbb{N}$. Ceci implique $|a_{n+p} - a_n| < |a_n|$ et donc, comme $||$ est supposée non archimédienne, $|a_{n+p}| = |a_n|$ quel que soit $p \in \mathbb{N}$; d'où le (ii).

On a $||a_n| - |b_n|| \leq |a_n - b_n|$ et l'hypothèse implique que cette dernière suite tend vers 0 d'où le (iii).

□

Lemme 2.10. *Ω est un anneau et $\mathfrak{I}$ est un idéal maximal de Ω.*

Démonstration. Le fait que Ω est un anneau et $\mathfrak{I}$ un idéal est immédiat. L'élément unité de Ω est la suite constante 1 dont tous les termes sont égaux à 1.

Si $a = (a_n)_{n\in\mathbb{N}} \in \Omega - \mathfrak{I}$, d'après ce qui précède, il existe $\delta > 0$ et $N \in \mathbb{N}$ tels que l'on ait $|a_n| > \delta$ si $n > N$. La suite $b = (b_n)_{n\in\mathbb{N}}$ définie par $b_n = 0$ si $n < N$ et $b_n = a_n^{-1}$ si $n \geq N$ est de Cauchy et $ab - 1$ est élément de $\mathfrak{I}$, ce qui montre que a est inversible dans $\Omega/\mathfrak{I}$ et permet de conclure au fait que $\mathfrak{I}$ est maximal.

□

Il résulte du lemme précédent que $\hat{K} = \Omega/\mathfrak{I}$ est un corps et du lemme 2.9, que $||$ s'étend à $\hat{K}$.

.

Proposition 2.11. *$||$ est une valeur absolue sur $\hat{K}$ et $\hat{K}$ est complet pour cette valeur absolue et contient K comme sous-corps dense.*

Démonstration. La multiplicativité de la valeur absolue et l'inégalité triangulaire (resp. ultramétrique) passent à la limite.

D'autre part, $|a| = 0 \Leftrightarrow \lim\limits_{n\longrightarrow+\infty} |a_n| = 0 \Leftrightarrow a \in \mathfrak{I}$ et donc $||$ est une valeur absolue sur $\hat{K}$ qui est non archimédienne si $||$ est non archimédienne sur K.

Maintenant, si $a = (a_n)_{n\in\mathbb{N}} \in \Omega$, alors $|a - a_n| \geq \sup_{p\geq 1} |a_{n+p} - a_n|$ tend vers 0 quand n tend vers $+\infty$ puisque la suite $(a_n)_{n\in\mathbb{N}}$ est de Cauchy. On a donc $a = \lim\limits_{n\longrightarrow+\infty} a_n$ dans $\hat{K}$ et donc que K est dense dans $\hat{K}$.

Finalement, si $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\hat{K}$, comme K est dense dans $\hat{K}$, on peut trouver pour chaque n un élément b_n de K tel que l'on ait $|a_n - b_n| \leq 2^{-n}$ et la suite b_n est de Cauchy dans K donc converge dans $\hat{K}$ vers une limite qui est aussi celle de la suite $(a_n)_{n\in\mathbb{N}}$; ce qui prouve que $\hat{K}$ est complet.

□

Définition 2.12. Le corps $\hat{K}$ (muni de la valeur absolue $||$) s'appelle le complété de K pour la valeur absolue $||$.

Exemple 2.13. (i) $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la valeur absolue $||_\infty$.

(ii) $\mathbb{C}$ est le complété de $\mathbb{Q}(i)$ pour la valeur absolue $|a + ib| = \sqrt{a^2 + b^2}$.

(iii) De manière générale, si K est un corps complet pour une valeur absolue $||$, et L est un sous-corps dense de K, alors K est le complété de L pour la valeur absolue induite..

Définition 2.14. On note $\mathbb{Q}_p$, corps des nombres $p-$adiques, le complété de $\mathbb{Q}$ pour la valeur absolue $||_p$.

Proposition 2.15. *Si K est un corps muni d'une valuation υ, alors $\mathcal{O}_K = \{x \in K \mid \upsilon(x) \geq 0\}$ est un anneau local d'idéal maximal $\mathfrak{m}_K = \{x \in K \mid \upsilon(x) > 0\}$.*

Démonstration. Le fait que $\mathcal{O}_K$ soit un anneau et $\mathfrak{m}_K$ un idéal est une conséquence immédiate des propriétés d'une valuation. D'autre part, si x est un élément de $\mathcal{O}_K$ n'appartenant pas à $\mathfrak{m}_K$, alors $\upsilon(x) = 0$ et donc x^{-1} est un élément de K de valuation 0 donc appartient à $\mathcal{O}_K$, ce qui prouve que $\mathcal{O}_K - \mathfrak{m}_K$ n'est autre que le groupe des unités $\mathcal{O}_K^*$ de $\mathcal{O}_K$, et permet de conclure.

□

Définition 2.16. L'anneau $\mathcal{O}_K$ s'appelle l'anneau des entiers de K associé à υ et le corps $k_K = \mathcal{O}_K/\mathfrak{m}_K$ est le corps résiduel de K.

Définition 2.17. Soit K un corps et $||$ une valeur absolue non archimédienne sur K.

Le sous-anneau

$$\mathcal{O} = \{x \in K : |x| \leq 1\} \subset K$$

est appelé l'anneau de valuation de $||$.

L'idéal

$$\mathfrak{P} = \{x \in K : |x| < 1\} \subset O$$

est appelé l'idéal de valuation de $||$.

Le quotient

$$\kappa = \mathcal{O}/\mathfrak{P}$$

est appelé le corps résiduel de $||$.

Exemple 2.18. Soit $K = \mathbb{Q}$ et soit $|| = ||_p$ la valeur absolue $p-$adique. Alors :

i) l'anneau de valuation associé est $\mathcal{O} = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$;

ii) l'idéal de valuation est $\mathfrak{P} = p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b \text{ et } p|a\}$;

iii) le corps résiduel est $\kappa = \mathbb{F}_p$.

Définition 2.19. L'anneau des entiers $p-$adiques est l'anneau de valuation

$$\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p : |x|_p \leq 1\right\} = \{x \in \mathbb{Q}_p \mid \upsilon(x) \geq 0\}$$

Les unités $p-$adiques sont les éléments inversibles de $\mathbb{Z}_p$. Nous noterons l'ensemble de tous ces éléments par ${\mathbb{Z}^\times}_p$.

Puisque $x \in \mathbb{Z}_p$ implique que $|x|_p \leq 1$ et $x^{-1} \in \mathbb{Z}_p$ ce qui implique que $\left|x^{-1}\right|_p = |x|_p^{-1} \leq 1$, on voit que ${\mathbb{Z}^\times}_p = \left\{x \in \mathbb{Q}_p : |x|_p = 1\right\}$.

Proposition 2.20. (Critère d'irréductibilité d'Eisenstein)
Soit $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}_p[X]$ un polynôme vérifiant les conditions
i) $|a_n| = 1$,
ii) $|a_i| < 1$ pour $0 \leq i < n$, et
iii) $|a_0| = 1/p$. Alors $f(X)$ est irréductible sur $\mathbb{Q}_p$.

Théorème 2.21. *Soit $K/\mathbb{Q}_p$ une extension finie de degré n. La fonction*

$|| : K \longrightarrow \mathbb{R}_+$ *défini par*

$$|x| = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|_p}$$

est une valeur absolue non archimédienne sur K qui étend la valeur absolue $p-$adique sur $\mathbb{Q}_p$.

Démonstration. (cf. [15, théorème 6.3.5])

□

2.2 Extensions finies de $\mathbb{Q}_p$

Définition 2.22. Soit K une extension finie de $\mathbb{Q}_p$, et soit $||$ la valeur absolue $p-$adique sur K. Pour tout $x \in K, x \neq 0$, on définit la valuation $p-$adique $\upsilon_p(x)$ est le nombre rationnel unique satisfaisant $|x| = p^{-\upsilon_p(x)}$.

Nous étendons formellement la définition en posant $\upsilon_p(0) = +\infty$. Il est facile de voir que υ_p est une valuation, au sens que nous avons défini :

i) $\upsilon_p(x+y) \geq \min \upsilon_p\{(x), \upsilon_p(y)\}$, et
ii) $\upsilon_p(xy) = \upsilon_p(x) + v(y)$.

Il est utile de remarquer que puisque nous savons exactement comment calculer la valeur absolue $p-$adique d'un élément de K, nous savons aussi comment calculer υ_p. Voici la formule : pour tout $x \in K^*$,

$$\upsilon_p(x) = \frac{1}{n}\upsilon_p(N_{K/\mathbb{Q}_p}(x)).$$

Proposition 2.23. La valuation $p-$adique υ_p est un homomorphisme du groupe multiplicatif $K^\times$ vers le groupe additif $\mathbb{Q}$. Son image est de la forme $\frac{1}{e}\mathbb{Z}$, où e est un diviseur de $n = [K : \mathbb{Q}_p]$.

Démonstration. υ_p est un homomorphisme est juste la propriété (ii) ci-dessus ; son image est donc un sous-groupe additif de $\mathbb{Q}$. On sait déjà que l'image est contenue dans $\frac{1}{n}\mathbb{Z}$. On sait aussi que l'image contient tout $\mathbb{Z}$, puisque l'image de υ_p sur $\mathbb{Q}_p^*$ le fait .

Choisissons $x \in K$ avec $\upsilon_p(x) = \frac{d}{e}$ avec d et e premiers entre eux, de sorte que le dénominateur e soit le plus grand possible. Maintenant, puisque d et e sont premiers entre eux, il doit y avoir un multiple de d congru à 1 modulo e, c'est-à-dire que nous pouvons trouver des entiers r et s tels que $rd = 1 + se$. Mais alors

$$r\frac{d}{e} = \frac{1+se}{e} = \frac{1}{e} + s$$

est dans l'image; puisque $s \in \mathbb{Z}$ est dans l'image, il s'ensuit que $\frac{1}{e}$ est dans l'image. Puisque e a été choisi pour être le plus grand dénominateur possible dans l'image, il s'ensuit que l'image doit être exactement $\frac{1}{e}\mathbb{Z}$.

□

Définition 2.24. *Soit $K/\mathbb{Q}_p$ une extension finie, et soit $e = e(K/\mathbb{Q}_p)$ l'unique entier positif (divisant $n = [K : \mathbb{Q}_p]$) défini par $\upsilon_p(K^\times) = \frac{1}{e}mathbbZ$. On appelle e l'indice de ramification de K sur $\mathbb{Q}_p$. On dit que l'extension $K/\mathbb{Q}_p$ est non ramifiée si $e = 1$. On dit que l'extension est ramifiée si $e > 1$, et totalement ramifiée si $e = n$. Enfin, nous écrivons $f = f(K/\mathbb{Q}_p) = n/e$ et appelons cela le degré résiduel de K sur $\mathbb{Q}_p$.*

.

Définition 2.25. Soit $K/\mathbb{Q}_p$ une extension finie, et soit $e = e(K/\mathbb{Q}_p)$. On dit qu'un élément $\pi \in K$ est une uniformisante si $\upsilon_p(\pi) = \frac{1}{e}$.

Ceci posé, nous pouvons décrire la structure algébrique de K.

Tout d'abord, rappelons que nous avons défini l'anneau de valuation :

$$\mathcal{O} = \{x \in K : |x| \leq 1\} = \{x \in K : \upsilon_p(x) \geq 0\}$$

et son idéal maximal

$$\mathfrak{m} = \{x \in K : |x| < 1\} = \{x \in K : \upsilon_p(x) > 0\}.$$

et le corps résiduel est le quotient $k = \mathcal{O}/\mathfrak{m}$.

.

Proposition 2.26. ***[30, théorème 5.11]*** *Soient K un corps de nombres , $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, et $K_\mathfrak{p}$ la complété de K, correspondant à $\mathfrak{p}$. De plus, soit L/K une extension de degré n, $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, et $L_\mathfrak{P}$ la complété correspondante. Enfin, soit R et S les anneaux d'entiers dans $K_\mathfrak{p}$ et $L_\mathfrak{P}$, respectivement. Alors nous avons :*

(i) $[L_\mathfrak{P} : K_\mathfrak{p}] = e_{L/K}(\mathfrak{P}) f_{L/K}(\mathfrak{P})$,

(ii) le corps $L_\mathfrak{P}$ est le composé de L et $K_\mathfrak{p}$,

(iii) L'anneau S est la fermeture intégrale de R dans $L_\mathfrak{P}$,

(iv) Si $\bar{\mathfrak{p}}$ et $\bar{\mathfrak{P}}$ sont les idéaux premiers de R et S, respectivement, alors $\bar{\mathfrak{P}}$ est au-dessus de $\bar{\mathfrak{p}}$ et $e_{L_\mathfrak{P}/K_\mathfrak{p}}(\bar{\mathfrak{P}}) = e_{L/K}(\mathfrak{P})$, $f_{L_\mathfrak{P}/K_\mathfrak{p}}(\bar{\mathfrak{P}}) = f_{L/K}(\mathfrak{P})$.

Proposition 2.27. *Soit les notations comme ci-dessus, et fixons une uniformisante π dans K. Alors :*

i) L'idéal $\mathfrak{m}$ est principal, et π est un générateur de $\mathfrak{m}$.

ii) Tout élément $x \in K$ peut s'écrire sous la forme $x = u\pi^{e\upsilon_p(x)}$, où $u \in \mathcal{O}^\times$ est une unité, et vérifie donc $\upsilon_p(u) = 0$. En particulier, $K = \mathcal{O}[\frac{1}{\pi}]$.

iii) Le corps résiduel k est une extension finie de $\mathbb{F}_p$ dont le degré est inférieur ou égal au degré $[K : \mathbb{Q}_p]$.

iv) Tout élément de $\mathcal{O}$ est une racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}_p$.

v) Inversement, si $x \in K$ est une racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}_p$, alors $x \in \mathcal{O}$.

Démonstration. (cf.[15, Proposition 6.4.5]).

□

Théorème 2.28. (**Lemme de HENSEL**)

Soit le polynôme $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}_p[X]$. *On suppose qu'il existe deux polynômes* $g(X)$ *et* $h(X)$ *dans* $\mathbb{F}_p[X]$ *tels que*

$g(X)$ *et unitaire ,*

$g(X)$ *et* $h(X)$ *premiers entre eux dans* $\mathbb{F}_p[X]$.

$\overline{f}(X) = g(X).h(X)$

Alors il existe deux polynômes $G(X)$ *et* $H(X)$ *dans* $\mathbb{Z}_p[X]$ *tels que* $\overline{G}(X) = g(X)$ *et* $\overline{H}(X) = h(X)$ *vérifiant* $f(X) = G(X).H(X)$.

2.3 Ramification dans une extension de $\mathbb{Q}_p$

Soit p un nombre premier et E un corps de nombres $p-$adiques , clairement E est une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_E$ l'anneau des entiers de E, c'est un anneau local, de valuation discrète d'idéal maximal $\mathfrak{M}$, et on a

$$p\mathcal{O}_E = \mathfrak{M}^e$$

où e est l'indice de ramifiaction de l'extension $E/\mathbb{Q}_p$. Le degré résiduel f est donné par

$$f = \left[\frac{\mathcal{O}_E}{\mathfrak{M}} : \mathbb{F}_p\right]$$

et on a $[E : \mathbb{Q}_p] = ef$.

De façon plus générale, si $K \subset L$ deux corps de nombres $p-$adiques d'idéaux maximaux $\mathfrak{p}$ et $\mathfrak{P}$ respectivement des anneaux d'entiers $\mathcal{O}_K$ et $\mathcal{O}_L$ avec $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$ alors $[L : K] = ef$ où e et f sont respectivement l'indice de ramification et le degré résiduel de l'extension L/K :

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e \text{ et } \left[\frac{\mathcal{O}_L}{\mathfrak{P}} : \frac{\mathcal{O}_K}{\mathfrak{p}}\right] = f$$

Définition 2.29. Soit L/K une extension de corps $p-$adiques.

On dit que l'extension L/K est non ramifiée si $e = 1$,

On dit que l'extension L/K est totalement ramifiée si $e = n$,

On dit que l'extension L/K est sauvagement ramifiée si p divise e, sinon on dit que l'extension est modérément ramifiée.

Les résultats suivats permettront de caractériser les différentes d'extensions ci-dessus.

Théorème 2.30. *On suppose que $L = K(\alpha)$, où α est une uniformisante de L. Alors, l'extension L/K est totalement ramifiée si, et seulement si α est racine d'un polynôme d'Eisenstein.*

Démonstration. (cf. [8, Théorème 1, Chap. 1, p. 23]).

□

Corollaire 2.31. *Il existe une unique extension totalement ramifiée de degré donné.*

Démonstration. le corps engendré sur K par une racine du polynôme $x + \pi^n$ est totalement ramifié sur K.

□

Les extension non ramifiées sont caractérisées par

Théorème 2.32. *Soit L/K une extension de corps locaux d'anneaux d'entiers $\mathcal{O}_L \supset \mathcal{O}_K$ respectivement. Soit $\mathfrak{p}$ l'unique idéal maximal de l'anneau des entiers de K*

Si L/K est non ramifiée, alors il existe un élément a de $\mathcal{O}_L$ avec $k_L = k(\overline{a})$. De plus, si $g(X)$ est le polynôme minimal de a sur K, alors $L = K(a)$ et $\overline{g}(X)$, la réduction de $g(X) \mod \mathfrak{p}$ de ses coefficients, est irréductible et séparable sur k.

Soit $g(X)$ un polynôme unitaire dans $\mathcal{O}_K[X]$, tel que $\overline{g}(X)$ est irréductible et séparable sur k. Si a est une racine de $g(X)$, alors l'extension $L = K(a)/K$ est non ramifiée et $k_L = k(\overline{a})$.

Démonstration. 1) Comme k_L est séparable sur k alors, il existe $a \in \mathcal{O}_L$ tel que $k_L = k(\bar{a})$ et où le polynôme minimal $G(X)$ de $\bar{a}$ sur k est séparable. De plus on a

$$[L : K] \geq d^\circ g(X) \geq d^\circ G(X) = [k_L : k] = [L : K]$$

Par suite, $G(X) = \bar{g}(X)$, i.e.$\bar{g}(X)$ est irréductible, et $L = K(a)$.

(2) On a

$$[L : K] = d^\circ g(X) = [k(\bar{a}) : k] \leq [k_L : k] \leq [L : K]$$

D'une part on a $[L : K] = f(L/K)$, i.e. $e(L/K) = 1$, et d'autre part on a $k_L = k(\bar{a})$, i.e. k_L est séparable sur k..

□

Corollaire 2.33. *Si L/F est non ramifiée et $K/\mathbb{Q}_p$ est finie alors, LK/FK est non ramifiée.*

Démonstration. Par le théorème 2.32, il existe a tel que $L = F(a)$, donc $LK = KF(a)$ où l'image de a dans le corps résiduel de LK est une racine simple d'un polynôme $\varphi(X)$, minimal pour l'image de a dans l'extension du corps résiduel de L sur celui de F. Par le théorème 2.32 précédent, LK/FK est donc non ramifiée.

□

Corollaire 2.34. *Si L/K et F/K sont non ramifiées, il en est de même de LF/K.*

Démonstration. Il suffit d'appliquer la propriété multiplicative des indices de ramification et utiliser le corollaire précédent..

□

Corollaire 2.35. *Il existe une unique extension non ramifiée de degré donné.*

Démonstration. Il y a exactement une extension d'un degré donné du corps fini k_K.

□

Corollaire 2.36. *Si L/K est non ramifié, alors son groupe de Galois est cyclique.*

Démonstration. Toute extension finie d'un corps fini est cyclique.

□

Les extensions modérément ramifiées sont caractérisées par :

Proposition 2.37. *Une extension L/K de degré $n \in \mathbb{N}^*$ est totalement et modérément ramifiée si, et seulement si, L est engendré sur K par une racine d'un binôme $X^n - b$, où b est de valeur absolue $\mathfrak{p}-$adique égale à 1.*

Démonstration. (cf. [30, Theorem 5.11, p. 234]).

□

Lemme 2.38. (Lemme d'Abhyankar)

Soient L et M deux extensions d'un corps $p-$adique K telles que M/K soit modérément ramifiée. Si $e(M/K)$ divise $e(L/K)$, alors LM/L est non ramifiée.

Démonstration. (cf. [30, Corollary 4, p. 229]).

□

Proposition 2.39. *Soient T/k et N/k deux extensions finies d'un corps local k telles que T/k soit totalement ramifiée et N/k soit non ramifiée. Alors T et N sont linéairement disjointes sur k..*

2.4 Groupe de Galois et interprétation de la localisation

Soit L/K une extension normale de corps $p-$adiques, de groupe de Galois G. Soit $\mathfrak{P}$ l'idéal premier non nul de l'anneau $\mathcal{O}_L$ des entiers de L sur K.

Définition 2.40. On appelle groupe d'inertie de $\mathfrak{P}$ dans L, le sous groupe G_0 du groupe de Galois G donné par :

$$G_0 = \{\sigma \in G, \sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L\}$$

Pour tout $i \geq 1$, le sous groupe G_i du groupe d'inertie donné par

$$G_i = \left\{\sigma \in G_i, \sigma(x) \equiv x \mod \mathfrak{P}^{i+1}, \forall x \in \mathcal{O}_L\right\}$$

est appelé $i-$ème groupe de ramification.

Par la théorie de Galois, à chaque sous groupe G_i, $i \geq 0$, correpond un sous-corps L_i laissé fixé par G_i qui est le groupe de Galois de l'extension galoisienne L/L_i.

Théorème 2.41. *Sous les hypothèses ci dessous on a :*

1. L'extension maximale non ramifiée L_0/K contenue dans L correspond à G_0. G_0 est normal dans G et est d'ordre $e(L/K)$ et le groupe quotient G/G_o est cyclique d'ordre $f(L/K) = [k_L : k_K]$.

2. L'extension maximale modérément ramifiée L_1/K contenue dans L correspond au premier groupe de ramification G_1. Le groupe G_1 est normal dans G_0 ; c'est un $p-$groupe et le groupe quotient G_0/G_1 est cyclique d'ordre non divisible par p.

Démonstration. (cf. [30, Corollary 5.34, p. 233]).

□

Théorème 2.42. *(Critère de van der Waerden-Dedekind)*

Soit K un corps de nombres algébrique et L la clôture normale de K sur $\mathbb{Q}$ de groupe de Galois G. Soit $\mathfrak{P}$ un idéal premier de L au dessus d'un nombre premier p. On considère D et I les deux sous groupes de G que sont respectivement le groupe de décomposition et le groupe d'inertie de $\mathfrak{P}$ dans L.

On suppose que la décomposition de $p\mathcal{O}_K$ est de la forme

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}...\mathfrak{p}_g^{e_g};\ \text{avec } N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i};\ f_i = \left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}}\right]$$

On considère l'action de G sur $\underline{K} = Hom_{\mathbb{Q}}(K; L)$ par composition à gauche, alors $\underline{K}$ se décompose en g $D-$orbites de longueurs respectives $e_i f_i$ et chacune d'elles se décompose en f_i $I-$ orbites de longueur e_i.

Proposition 2.43. *Soient K, K' deux corps et $\sigma \in Hom_{\mathbb{Q}}(K, K')$. On considère $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers de K et K' respectivement, $||_{\mathfrak{p}}$ et $||_{\mathfrak{p}'}$ les valeurs absolues définies sur K et K' respectivement. Alors σ préserve les valeurs absolues si, et seulement si, $\sigma^{-1}(\mathfrak{p}') = \mathfrak{p}$.*

En particulier, si on considère L un corps de nombres galoisien, et si on applique la proposition précédente à $K = K' = L$, on obtient ce que l'on voulait, c'est-à-dire :

Corollaire 2.44. *Soit L un corps de nombres galoisien. Pour tout premier $\mathfrak{P}$ de L, le sous-groupe de $Gal(L/\mathbb{Q})$ qui préserve la valeur absolue $||_{\mathfrak{P}}$ associée à $\mathfrak{P}$ n'est rien d'autre que le groupe de décomposition de $\mathfrak{P}$, noté $D_{\mathfrak{P}}$.*

Corollaire 2.45. *.Soit $L/\mathbb{Q}$ une extension galoisienne, $\mathfrak{P}$ un idéal premier de L au dessus de p alors, l'extension $L_{\mathfrak{P}}/\mathbb{Q}_p$ est galoisienne de groupe de Galois $Gal(L_{\mathfrak{P}}/\mathbb{Q}_p) = D_{\mathfrak{P}}$, le groupe de décomposition de $\mathfrak{P}$ dans $L/\mathbb{Q}$.*

Nous donnerons dans ce qui suit une déclinaison d'un dictionnaire qui interprète des situations locales au niveau global. On considère un corps de nombre L, galoisien sur $\mathbb{Q}$ et de groupe de Galois G, et $K/\mathbb{Q}$ une extension de degré n contenue dans L. Soit $p \in \mathbb{Z}$, p un nombre premier, et $\mathfrak{P}$ un idéal premier de L au dessus de p. On considère la factorisation de p dans K

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}...\mathfrak{p}_g^{e_g};\ \text{avec}\ N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$$

On pose $K_i = K_{\mathfrak{p}_i}$, $1 \leq i \leq g$, et on note $\underline{K_i}$ l'ensemble formé par les n_i $\mathbb{Q}_p-$morphismes $K_i \longrightarrow L_{\mathfrak{P}}$ où $n_i = e_i f_i$.

Chaque$\underline{K_i}$ est isomorphe canoniquement à l'orbite de $\underline{K}$ sous l'action de D associé à $\mathfrak{p}_i$.

On note par K_i^{gal} le composé des $\sigma(K_i)$, $\sigma \in \underline{K_i}$, c'est une extension galoisienne de $\mathbb{Q}_p$. Connaissant les groupes d'inertie des extensions locales $K_i^{gal}/\mathbb{Q}_p$, $1 \leq i \leq g$, on en déduit des précisions sur I. Nous sommes en mesure de déduire quelques résultats de l'aritmétique des corps au niveau local et global. Commençons par l'isomorphisme suivant.

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{i=1}^{g} K_i$$

Du point de vue des dimension, on aura

$$\begin{aligned} n = \dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}_p}(K \otimes_{\mathbb{Q}} \mathbb{Q}_p) \\ = \dim_{\mathbb{Q}_p} \prod_{i=1}^{g} K_i = \sum_{i=1}^{g} \dim_{\mathbb{Q}_p} K_i \\ = \sum_{i=1}^{g} n_i = \sum_{i=1}^{g} e_i f_i \end{aligned}$$

Du point de vue des anneaux des entiers on a

$$\mathcal{O}_K \otimes_{\mathbb{Q}} \mathbb{Z}_p \simeq \prod_{i=1}^{g} \mathcal{O}_{K_i},$$

ainsi les discriminants de K et des K_i sont liés par la relation

$$d_K \simeq \prod_{i=1}^{g} d_{K_i}$$

par suite

$$\upsilon_p(d_K) \simeq \sum_{i=1}^{g} \upsilon_p(d_{K_i})$$

ce qui assure le passage du local au global.

Un invariant, la différente, est défini au niveau local par :

Définition 2.46. Soit L/F une extension de corps de locaux, $\mathcal{O}_F$ et $\mathcal{O}_L$ sont respectivement les anneaux d'entiers de F et L. On appelle différente de l'extension L/F, qu'on note $\mathfrak{D}(L/F)$, l'idéal fractionnaire de L défini par

$$\mathfrak{D}(L/F) = \left(\left\{x \in L \ / \ T_{L/F}(x\mathfrak{p}) \subset \mathcal{O}_F\right\}\right)^{-1}$$

où $\mathfrak{p}$ est un l'idéal maximal de L.

La différente vérifie entre autre la propriété de la transitivité appliquée à une tour d'extension $E \subset F \subset L$,

$$\mathfrak{D}(L/E) = \mathfrak{D}(L/F)\mathfrak{D}(F/E)$$

Théorème 2.47. *La différente $\mathfrak{D}(L/F)$ est donnée par*

$$\mathfrak{D}(L/F) = \mathfrak{p}^{\sum_{i=0}^{t}(\#G_i - 1)}$$

où G_i est le $i-$ème groupe de ramification, et G_t le dernier groupe de ramification.

Démonstration. (cf. [30, théorème 5.36, p. 236]).

□

Remarque 2.48. notons quelques conséquences du théorème précédent :

Si $p \nmid e$, alors L/F est modérément ramifiée et G_1 est d'ordre 1 et il en sera de mêmes de tous les i-èmes groupes de ramification G_i, $i \geq 2$ Par conséquent, on aura

$$\mathfrak{D}(L/F) = \mathfrak{p}^{e-1}$$

Si $p \mid e$, alors l'extension L/F est sauvagement ramifiée, Ainsi $\mathfrak{D}(L/F)$ est divisible par $\mathfrak{p}^e$ et donc on a $\mathfrak{D}(L/F) = \mathfrak{p}^d$ avec $d \geq e$.

Dans notre situation de $\mathbb{Q}_p-$extensions, on a $[K_\mathfrak{p} : \mathbb{Q}_p] = ef$.

En posant $m = v_p(d_K)$ et $d = v_p(\mathfrak{D}(K_\mathfrak{p}/\mathbb{Q}_p))$, on a la relation suivante : $m = fd$

où

$$\begin{cases} d = e - 1 & \text{si } p \nmid e \\ d \geq e & \text{si } p \mid e \end{cases}$$

Chapitre 3

Groupe de Galois d'un polynôme

3.1 Introduction

Soit $f(X) = X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n$ un polynôme séparable à coefficients dans un corps parfait K et de degré n, et soit $\Omega = (\alpha_1, \alpha_2, ..., \alpha_n)$ un n-uplet formé des n racines (distinctes) de f (avec $n > 0$). Le corps $K(\Omega)$ est son corps de décomposition.

Soit $K[X_1, X_2, ..., X_n]$ désignent l'anneau des polynôme en n indéterminées à coefficients dans K .

Définition 3.1. Un polynôme $P \in K[X_1, X_2, ..., X_n]$ est appelé une Ω-relation si $P(\Omega) = 0$.

Définition 3.2. L'idéal I_Ω de $K[X_1, X_2, ..., X_n]$ défini par

$$I_\Omega = \{\Phi \in K[X_1, X_2, ..., X_n] \mid \Phi(\Omega) = 0\}$$

est connu sous le nom d'idéal des Ω-relations.

Définition 3.3. Le groupe de Galois de Ω est sous-groupe G_Ω de S_n défini par

$$G_\Omega = \{\sigma \in S_n \mid (\forall \Phi \in I_\Omega)\ \sigma.\Phi \in I_\Omega\}.$$

On appelle G_Ω le Groupe de Galois de f sur K et on le note $Gal_X(f, K)$ ou $Gal(f, K)$. C'est la définition concrète originale de Galois.

Selon la définition abstraite moderne, le groupe de Galois d'une extension normale L d'un corps K est défini comme étant le groupe de tous les $K-$automorphismes de L et est noté $Gal(L, K)$. Notez qu' une extension normale L d'un corps K est un corps obtenu en adjoignant à K toutes les racines d'un famille de polynômes univariés à coefficients

dans K. Pour relier les deux définitions, soit $L = K(\Omega)$ et notons que on obtient un isomorphisme de $Gal(L, K)$ sur $Gal(f, K)$ en envoyant tout $\tau \in Gal(L, K)$ à cela $\sigma \in Gal(f, K)$ pour lequel $\tau(\alpha_i) = \alpha_{\sigma(i)}$ pour $1 \leq i \leq n$.

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

3.2 Groupe de permutation

La définition concrète ci-dessus fait ressortir le lien étroit entre la théorie des groupes et la théorie des équations.

A savoir, le groupe de Galois $Gal(f, K)$ est maintenant un sous-groupe de S_n où, comme d'habitude, S_n désigne le groupe symétrique de degré n, c'est-à-dire le groupe de toutes les permutations de n symboles ; notez que l'ordre de S_n est $n!$. Assez généralement, un sous-groupe de S_n est appelé groupe (de permutation) de degré n.

Définition 3.4. On dit qu'un sous-groupe G de permutation du groupe symétrique S_n est transitif si, pour tout $i \neq j$, $1 \leq i, j \leq n$, il existe $\sigma \in G$ tel que $\sigma(i) = j$.

Pour faire ressortir davantage le parallélisme entre la théorie des groupes et la théorie des équations, on remarque que.

Théorème 3.5. *Soit K un corps, $P \in K[X]$ un polynôme de degré n et de groupe de Galois G, alors*

si P est irréductible, alors n divise $|G|$ 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 dans un corps de décomposition L de celui-ci, $\deg P \geq n \geq 1$.

Si P est irréductible, alors pour toute racine α de P, dans une clôture algébrique de K, $[K(\alpha) : K] = n = \deg P$. Sachant que $K(\alpha) \subset L$, où L est le corps de décomposition de P, on en déduit que n divise $|G| = [L : K]$. D'autre part, pour pour $1 \leq i, j \leq n$, avec $i \neq j$, il existe un K-isomorphisme $\sigma : K(\alpha_i) \longrightarrow K(\alpha_j)$ donné par $\sigma(\alpha_i) = \alpha_j$ qui se prolonge en un K-automorphisme de L, ce qui montre que G est transitif isomorphe à un sous-groupe transitif de S_n.

□

De même,
on dit que G est 2-transitif (ou doublement transitif) si pour tout $i \neq i'$ et$j \neq j'$ dans Ω, il existe $\sigma \in G$ tel que $\sigma(i) = j$ et $\sigma(i\prime) = j\prime$. Assez généralement, G est l-transitif pour un entier positif $l \leq n$, si pour tout élément deux à deux distinct $i_1, i_2, ..., i_l$ en Ω et des éléments deux à deux distincts $j_1, j_2, ..., j_l$ dans Ω, il existe $\sigma \in G$ tel que $\sigma(i_k) = j_k$ pour $1 \leq k \leq l$.

Par analogie avec le concept de transitivité , on dit que G est k-antitransitif pour un entier positif $k \leq n$, si pour tout éléments deux à deux distinct$i_1, i_2, ..., i_k$ dans Ω on a que l'identité est le seul élément de G qui les maintient fixes. De plus, pour des entiers positifs $l \leq k \leq n$, on dit que G est (l, k)-transitif si G est l-transitif et k-antitransitif ; nous pouvons exprimer cela en disant simplement que G est (l, k).

En particulier G est $(1, 1)$ est équivalent à G est régulier. Or si G est l-transitif, avec $l > 1$, alors le stabilisateur en un point de G est évidemment $(l - 1)$-transitif en tant que groupe de permutation de degré $n - 1$, agissant sur les $n - 1$ éléments restants ; inversement, si G est transitif et que son stabilisateur en un point est $(l - 1)$-transitif alors G est l-transitif. De même, si G est k-antitransitif, avec $k > 1$, alors le stabilisateur en un point de G est $(k - 1)$-antitransitif en tant que groupe de permutation de degré $n - 1$, agissant sur les $n - 1$ éléments restants ; inversement, si G est transitif et que son stabilisateur en un point est $(k - 1)$-antitransitif alors G est k-antitransitif.

3.3 Les groupes finis doublement transitifs

La classification des groupes simples finis est un outil permettant de décider sur le choix de la réalisation d'un groupe de permutations comme groupe de Galois d'un trinôme.

Plusieurs auteurs ont décrit la liste de réalisations possibles des groupes de permutations en tant que groupes de permutations des racines d'un trinôme irréductible. Cette liste est établie selon la nature de la transitivité des groupes de permutations[1]. La liste complète des groupes simples finis est :

1. Le groupe cyclique d'ordre p, p premier
2. Le groupe alterné A_n,$n \geq 5$
3. Les 16 groupes simples de type de lie
4. Les 26 groupes sporadiques comprenant les 5 groupes de Mathieu.

Le théorème suivant de Burnside a été la clé pour la classification des groupes de permutations doublement transitifs :

Théorème 3.6. *(Burnside)*

Un groupe de permutation doublement transitif admet un unique sousgroupe normal minimal. Un tel sous-groupe est, soit un groupe abélien élémentaire, soit un groupe simple non-abélien.

Démonstration. (cf. [1, p ; 22]).

□

Lemme 3.7. *Le degré d'un groupe de permutations, doublement transitif , ayant un sous-groupe normal minimal abélien est nécessairement de la forme p^m, $m > 1$. Son sous-groupe normal minimal est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^m$ et le stabilisateur d'un point par le groupe G est lui même isomorphe à un sous groupe de $GL(m, p)$.*

Démonstration. (cf. [12, Theorem 4.7A. , p132]).

□

En particulier, il s'ensuit que (à isomorphisme près) le groupe affine $AGL(m, p)$ est l'unique groupe doublement transitif maximal de degré p^m à sous-groupe normal minimal abélien.

Comme conséquence de la classification des groupes finis simples, Abhyankar [1, page 20] dresse la liste complète des groupes de permutations triplement transitifs que nous reprenons ici rapidement sans trop de détail :.

1. Tout groupe G tel que $PGL(2,q) \subseteq G \subseteq P\Gamma L(2,q)$, de degré $q+1$, pour tout entier q puissance d'un nombre premier.
2. tout groupe G tel que $PML(2,q) \subseteq G \subseteq P\Gamma L(2,q)$, de degré $q+1$, pour tout entier q puissance d'un nombre premier impair.
3. Le groupe $AGL(m,2)$, pour tout entier $m > 1$, de degré 2^m.
4. Le sous-groupe de $AGL(4,2)$ de degré 2^4 et d'ordre $2^4.7!$.
5. Les groupes de mathieu M_{11}, M_{12}, M_{22} , M_{23}et M_{24}, de degrés respectifs $11, 12, 22$, 23 et 24.
6. Le groupe $\alpha(M_{11})$, image de M_{11} par un automorphisme d'ordre 2 de M_{12}, de degré 12, ainsi que $Aut(M_{22})$ de degré 22.
7. Le groupe alterné A_n, $n \geq 5$ et le groupe symétrique S_n, $n \geq 3$.

On y donne aussi une liste de 9 groupes de permutation doublement transitif et non triplement transitif ayant un sous-groupe normal minimal non abélien.

1. Tout groupe G tel que $PSL(m,q) \subseteq G \subseteq P\Gamma L(m,q)$ de degré $(q^m-1)/(q-1)$, $m > 1$ et q un entier puissance d'un nombre premier.
2. Le groupe $S_p(2M,2)$, $m > 2$, de degré $2^{2m-1} + 2^{m-1}$ et d'ordre $2^{2m-1} - 2^{m-1}$.
3. Pour $q = p^\nu > 2$ où p est premier, tout groupe compris entre les groupes $PSU(3,q)$ et $AutPSU(3,q)$ de degré $q^3 + 1$.
4. Pour toute puissance propre impaire $q = 2^\nu$ de 2, tout groupe compris entre le groupe de Suzuki $Sz(q)$ et son groupe d'automorphisme $AutSz(q)$ de degré $q^2 + 1$.
5. Pour toute puissance impaire $q = 3^\nu$ de 3, tout groupe compris entre le groupe de Ree $R_1(q)$ et son groupe d'automorphisme $AutR_1(q)$ de degré $q^3 + 1$.
6. Les deux représentations de degré 11 du groupe $PSL(2,11)$.
7. Les deux représentations de degré 15 du groupe alternéA_7.
8. Les deux représentations de degré 176 du groupe sporadique "Higman- Sims"

9. Le troisième groupe sporadique de Conway de degré 276.

Comme le groupe de Galois d'un tel trinôme contient une involution fixant au plus trois points. La classification des groupes de permutations permet d'énoncer le résultat suivant :

Lemme 3.8. *[10, Sec. 2, Lemma 2.5] Le groupe de Matieu M_{23} ne se réalise pas comme groupe de Galois d'un $\mathbb{Q}-$trinôme, car il ne contient pas une involution fixant au plus trois points.*

De plus on montre :

Proposition 3.9. *[10, Sec. 2, Proposition 2.4] Soit q une puissance d'un nombre premier p et $d \geq 3$. Pour que le groupe $P\Gamma L(d,q)$ contienne une involution fixant au plus trois points, il est nécessaire et suffisant que (d,q) soit l'un des cas suivants*

1. $q = 2$ et $d = 3$ ou 4.

2. q est impair et d est pair ..

3.4 $\mathbb{Q}-$trinômes et ramification

Soit $f(X) = X^n + aX^s + b$ un trinôme de degré n,$n \geq 3$, irréductible sur $\mathbb{Q}$ et à coefficients dans $\mathbb{Z}$

où $1 \leq s < n$.

Soit α une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$. On note par $K = \mathbb{Q}(\alpha)$ le corps obtenu en adjoignant la racine α au corps $\mathbb{Q}$ des nombres rationnels.

On pose $r = \text{pgcd}(n,s)$, $n = rn\prime$ et $s = rs\prime$. Par [41, Théorème 2], le discriminant.

$D(f)$ du trinôme $f(X)$ est :

$$D(f) = (-1)^{\frac{n(n-1)}{2}} r^n b^{s-1} \left[(n\prime)^{n\prime} b^{n\prime-s} + (-1)^{n\prime-1}(n\prime - s)^{n\prime-s}(s\prime)^{s\prime} a^{n\prime}\right]^r$$

Le discriminant d_K de K est lié au discriminant $D(f)$ du trinôme $f(X)$ par la relation :

$$D(f) = i(\alpha)^2 d_K$$

où $i(\alpha)$ désigne l'indice de $\mathbb{Z}[\alpha]$ dans l'anneau des entiers du corps de nombres K.

Alors, les nombres premiers q qui se ramifient dans K sont ceux qui divisent d_K, donc sont parmi les diviseurs premiers du discriminant $D(f)$ du trinôme $f(X)$. Dans [23], P. Llorente, E. Nart et N. Villa ont étudié la ramification d'un nombre premier dans K. De plus ils montrent :

Théorème 3.10. *[23, Theorem 2]*

Avec les notations précédentes, soit q un nombre premier tel que $q \nmid abr$, alors,

$$v_q(d_K) = \begin{cases} 0 & si\ v_q(D(f))/r\ est\ pair \\ r & si\ v_q(D(f))/r\ est\ impair \end{cases}$$

Dans le cas où $a = b$ et $n = p^n$, p premier divise a un seule fois , nous déterminons la ramification du nombre premier p. Nous considérons pour cela le trinôme irréductible sur $\mathbb{Q}$, $f(X) = X^{p^n} + aX + a$, de discriminant donné par :

$$D(f) = (-1)^{\frac{p^n-1}{2}} p^{p^n} b^{p^n-1} D_0$$

où

$$D_0 = p^{np^n-1} + \frac{a}{p}(p^n - 1)^{p^n-1}$$

Pour déterminer la ramification d'un nombre premier q dans K, nous étudierons séparément les cas $q = p$ et $q \neq p$.

Dans les deux cas nous utilisons La méthode d'Ore .

La méthode d'Ore a été évoquée à cet effet dans [11] pour déterminer la valuation $q-$adique du discriminant du corps de nombre K ainsi que la détermination de la ramification d'un nombre premier q dans K, à travers le polygone de Newton associé à un polynôme et relatif à un nombre premier q.

3.5 Polygones de Newton et Ramification

On se donne un polynôme f$(X) \in \mathbb{Q}_p[X]$; de degré n, et $\phi(X)$ un polynôme unitaire de degré m à coefficients entiers $p-$adiques. Le développement de $f$suivant les puissances de $\phi(X)$, donné par la division euclidienne, est

$$f(X) = \sum_{j=0}^{t} p^{\alpha_j} Q_j(X)\phi(X)^{t-j} \tag{3.5.1}$$

où les polynômes $Q_j(X) \in \mathbb{Z}[X]$ sont de degrés $degQ_j(X) < m$ pour tout j, et t le plus grand entier vérifiant $t \leq \frac{n}{m}$.

Dans l'égalité (3.5.1), les coefficients de $Q_j(X)$ ne divisent pas tous le nombre premier p , sauf si $Q_j = 0$ et dans ce cas le terme correspondant est omis de la somme.

Si $f(X)$ est unitaire, on a $\alpha_0 = 0$.

Le développement donné dans (3.5.1) est appelé décomposition canonique de $f(X)$. Le $(p, \phi)-$ polygone de $f(X)$ est défini par :

Définition 3.11. Le $(p, \phi)-$ polygone de $f(X)$ est la frontière de l'enveloppe convexe supérieur de l'ensemble des points (j, α_j), sans la partie verticale. La partie du $(p, \phi)-$ polygone diminuée de la partie horizontale (s'il y a lieu) est appelée partie principale du $(p, \phi)-$ polygone.

Soient $S_1, ..., S_k$ les côtés de la partie principale du $(p, \phi)-$ polygone de $f(X)$ de pentes croissantes.

On définit :

$l_0 :=$ longueur du côté horizontal

$l_i :=$ longueur de la projection de S_i sur l'axe des x.

$h_i :=$ longueur de la projection de S_i sur l'axe des y.

On pose

$$\epsilon_i = \text{ pgcd}(l_i, h_i)$$

et

$$\lambda_i = \frac{l_i}{\epsilon_i},\ k_i = \frac{h_i}{\epsilon_i}$$

Par rapport au côté S_i, considérons la somme des termes $p^{\alpha_j} Q_j(X)\phi(X)^{t-j}$ dans la décomposition canonique de $f(X)$ correspondant aux points $(j, \alpha_j) \in S_i$. Cette somme fait apparaître un facteur commun

$$\phi(X)^{t-l_0-...-l_i} p^{h_1+...+h_{i-1}}$$

de l'expression

$$R_{i,0}(X)\phi(X)^{l_i} + R_{i,1}(X)p^{k_i}\phi(X)^{l_i-\lambda_i} + R_{i,2}(X)p^{2k_i}\phi(X)^{l_i-2\lambda_i} + ... + R_{i,\epsilon_i}(X)p^{h_i}$$

où les polynômes $R_{i,j}(X)$ sont de degré $< m$. En particulier, $R_{i,0}(X)$ est premier avec $\phi(X)$, dans $\mathbb{F}_p[X]$, il existe alors un polynôme $A_i(X) \in \mathbb{Z}[X]$ tel que

$$R_{i,0}(X)A_i(X) \equiv 1 \mod (p, \phi(X))$$

On définit alors le polynôme $S_{i,j}(X)$ donné par :

$$S_{i,j}(X) = A_i(X).R_{i,j}(X)$$

Définition 3.12. On appelle polynôme associé à $f(X)$ et relatif au côté S_i, le polynôme $F_i(X;Y)$ donné par

$$F_i(X,Y) = Y^{\epsilon_i} + S_{i,1}(X)Y^{\epsilon_i - 1} + ... + S_{i,\epsilon_i}(X)$$

Par construction, le polynôme $F_i(X;Y)$ dépend du choix de$A_i(X)$, ce qui n'est pas le cas de sa classe modulo l'idéal $(p;\phi(X))$. La relation entre $(p,\phi)-$polygone et ramification est donnée par :

Théorème 3.13. *[11, Theoreme 1.5]*
Soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire irréductible tel que $f(X) \mod p$ n'est pas irréductible, et soit θ une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$ fixée. On considère la factorisation modulo p de $f(X)$

$$f(X) \equiv \phi_1(X)^{a_1}...\phi_s(X)^{a_s} \mod p$$

où $\phi_\nu(X) \in \mathbb{Z}$ de degré $deg\phi_\nu(X) = m_\nu$.

Alors,

$$p = \mathfrak{a}_1...\mathfrak{a}_s$$

où les $\mathfrak{a}_\nu$ sont des idéaux de $K = \mathbb{Q}(\theta)$ tels que $N_{K/\mathbb{Q}}(\mathfrak{a}_i) = p^{a_\nu m_\nu}$ ($N_{K/\mathbb{Q}}$ désigne la norme absolue du corps K).

A chaque idéal $\mathfrak{a} = \mathfrak{a}_\nu$ correspond un facteur irréductible $\phi(X) = \phi_\nu(X)$. On détermine ainsi le $(\mathbb{Q}_p, \phi)-$ polygone de $f(X)$. Pour chaque au côté S_i de la partie principale de ce polygone, on considère la factorisation modulo (p,ϕ) du polynôme associé $F_i(X,Y)$

$$F_i(X,Y) \equiv F_1^{(i)}(X,Y)^{a_i^{(i)}}...F_{t_i}^{(i)}(X,Y)^{a_{t_i}^{(i)}} \mod (p, \phi(X))$$

Alors

$$\mathfrak{a} = \prod_{i=1}^{k} \prod^{t_i} \left[\mathfrak{c}_j^{(i)}\right]^{\lambda_i}$$

où $\lambda_i = l_i/\epsilon_i$ est le paramètre défini au dessus et les $\mathfrak{c}_j^{(i)}$ sont des idéaux de K premiers entre eux. De plus

$$N_{K/\mathbb{Q}}(\mathfrak{c}_j^{(i)}) = p^{m.m_j^{(i)}a_j^{(i)}}, m_j^{(i)} = deg_Y F_j^{(i)}(X,Y)$$

En outre, si $a_j^{(i)} = 1$, alors l'idéal $\mathfrak{c}_j^{(i)}$ est premier.

Notons que dans [24], par l'utilisation des polygones de Newton et selon la terminologie d'Ore, les auteurs donnent une description détaillée de la décomposition d'un nombre premier dans le corps de rupture du trinôme $X^n + AX + B$.

Dans [5] les auteurs ont utilisé les polygones de Newton pour la détermination de la ramification des nombre premier dans le corps K engendré par une racine du trinôme $f(X) = X^p + aX^s + a \in \mathbb{Z}[X]$, irréductible sur $\mathbb{Q}$. Dans le cas où $a = bp^{\upsilon_p(a)}$, ils montrent au résultats suivants :

Proposition 3.14. *Soient a un entier, p un nombre premier divisant a et $f(X) = X^p + aX^s + a$ un trinôme irréductible sur $\mathbb{Q}$. Alors, le nombre premier p est totalement ramifié dans K dans chacun des cas suivants*

1. *p divise $\upsilon_p(a)$ et $\upsilon_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) = 1$, où $k = \upsilon_p(a)/p$*
2. *p ne divise pas $\upsilon_p(a)$ et dans ces cas on a $p = \mathfrak{p}^p$.*

Proposition 3.15. *Soient a un entier, p un diviseur premier de a, et $f(X) = X^p + aX^s + a$ un trinôme irréductible sur $\mathbb{Q}$. On suppose que $\upsilon_p(a) = kp$ et que $\upsilon_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) > 1$, $k \geq 1$, alors*

$$p = \begin{cases} \mathfrak{p}_1^{p-1}\mathfrak{p}_2 & si\ ks > 1\ ou\ ks = 1 et\ p \nmid b+1 \\ \mathfrak{p}_1^{p-2}\mathfrak{a} & sinon \end{cases}$$

où $\mathfrak{a}$ est un idéal de K tel que

$$\mathfrak{a} = \begin{cases} \mathfrak{p}_2^2 & si\ \upsilon_p(b^{p-1} + pb - 1) \leq 2\upsilon_p(b+1) + 1\ et\ \upsilon_p(b^{p-1} + pb - 1)\ paire \\ \mathfrak{p}_2\mathfrak{p}_3 & si\ \upsilon_p(b^{p-1} + pb - 1) > 2\upsilon_p(b+1) + 1 \end{cases}$$

où $\mathfrak{p}_1$, $\mathfrak{p}_2$ *et* $\mathfrak{p}_3$ *sont des idéaux premiers de* K, *distincts.*

La preuve repose sur la détermination du $(\mathbb{Q}_p, X)-$polygone du trinôme

$$g(X) = \frac{1}{p^{kp}} f(p^k(X-b)) = X^p + \sum_{i=1}^{p-1} a_i X^{p-i} + a_p$$

où

$$a_i = \begin{cases} \binom{p}{i}(-b)^i & \text{si } 1 \leq i \leq p-s-1 \\ \binom{p}{i}(-b)^i - \binom{s}{i+s-p} p^{ks}(-b)^{i+s-p-1} & \text{si } p-s \leq i \leq p-1 \\ -b^p + (-1)^s p^{ks} b^{s+1} + b & \text{si } i = p \end{cases}$$

Exemple 3.16. Soit à déterminer la ramification de p dans l'extension $K/\mathbb{Q}$ engendrée par une racine α du trinôme irréductibe $\varphi(X) = X^p + p^p X + p^p$. Pour cela, considérons le polynôme $g(X)$ suivant :

$$g(X) = \frac{1}{p^p} \varphi(p(X-1) = X^p + \sum_{i=1}^{p-1} a_i X^{p-i} + a_p$$

où

$$a_i = \begin{cases} (-1)^i \binom{p}{i} & \text{si } 1 \leq i \leq p-2 \\ 2p & \text{si } i = p-1 \\ -p & \text{si } i = p \end{cases}$$

Le polygone de Newton associé au polynôme $g(X)$ est formé d'un seul côté reliant les points $(0,0)$ et $(p,1)$.

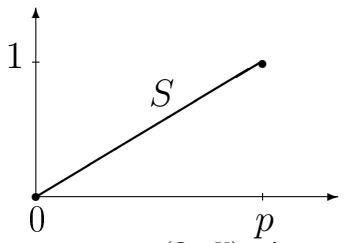

Figure 1. Le $(\mathbb{Q}_p, X)$-polygon of $g(X)$

Le polynôme associé G à g est

$$G(Y) = Y + 1$$

Alors, par [31, Sect. 2, Theorem 5], $p = \mathfrak{p}^p$, où $\mathfrak{p}$ est un idéal premier de K. Le nombre premier p est donc totalement ramifié dans $K/\mathbb{Q}(\alpha)$.

3.6 Groupe de Galois de $\varphi(X) = X^p + aX + a$

En [18], [19] , K. Komatsu a étudié le groupe de Galois G d'un trinôme de la forme $\varphi(X) = X^p + aX + a$, où a est un entier rationnel et p un nombre premier.Il montre les résultats suivants :

Théorème 3.17. *Soit a un entier rationnel, et soit p un nombre premier avec les propriétés suivantes :*

1. $p \equiv 3$ *ou* 5 *ou* 7 $(mod 8)$ $p \neq 3$;
2. $pgcd(p, a) = 1$;
3. $\varphi(X) = x^p + ax + a$ *est irréductible sur* $\mathbb{Q}$.

Alors le groupe de Galois de $\varphi(X) = 0$ sur $\mathbb{Q}$ est le groupe symétrique S_p.

on a besoin du lemme suivant de van der Waerden :

Lemme 3.18. *Soit K un corps de nombres algébriques de degré n, et soit $\overline{K}$ la fermeture galoisienne de K sur $\mathbb{Q}$. Si le discriminant d_K de K est exactement divisible par un nombre premier q (i.e. $q|d_K$, $q^2, \nmid d_K$), alors le groupe de Galois de $\overline{K}/\mathbb{Q}$ contient une transposition (en tant que groupe de permutation sur $\{1, 2, \cdots, n\}$)..*

Démonstration. (preuve de théorème 3.17)

Soit α une racine de $\varphi(X)$, et soit $K = \mathbb{Q}(\alpha)$, alors le discriminant de $f$donné par

$$D = a^{p-1} D_0$$

où

$$D_0 = (p-1)^{p-1} a + p^p$$

Alors $|D_0|$ ne peut pas être un carré. En fait, si $|D_0| = m^2$ avec un entier m, alors

$$D_0 \equiv p^p \equiv p \equiv \pm m^2 (mod 8).$$

Cela implique que $p \equiv 7(mod 8)$, et $D_0 = -m^2$.
puisque

$$\frac{p-1}{2} \equiv 3(mod 4),$$

il existe au moins un facteur premier p_0 de $(p-1)/2$ tel que $p_0 \equiv 3(mod 4)$. Maintenant

$$-m^2 = D_0 \equiv p^p \equiv 1(mod p_0)$$

depuis $p \equiv 1(mod p_0)$. On voit que -1 est un résidu quadratique $mod p_0$. Cependant, cela est impossible, puisque $p_0 \equiv 3(mod 4)$. Une contradiction montre que $|D_0|$ n'est pas un carré. Il existe donc un nombre premier q tel que $v_q(D_0)$ soit un entier impair. Puisque $\text{pgcd}(p, a) = 1$, on a

$$q \neq p, \text{pgcd}(q, a) = 1, (q, p-1) = 1$$

.

Soit d_K le discriminant de K. Alors d_K est divisible par q une seule fois , puisque $v_q(D)$ est impair. Il découle du (lemme 3.18) que le groupe de Galois G de $\varphi(X) = 0$ sur $\mathbb{Q}$ contient une transposition. Puisque p est premier, G est primitif. D'où $G = S_p$.

□

Remarque 3.19. Si $p = 3$, le groupe de Galois de $\varphi(X) = 0$ n'est pas toujours symétrique.

Par exemple, le groupe de Galois de $x^3 - 7x - 7 = 0$ est cyclique, puisque son discriminant est

$$-4(-7)^3 - 27(-7)^2 = 7^2.$$

Théorème 3.20. *Soit $p \equiv 1(mod 8)$ un nombre premier et soit a un entier rationnel avec $pgcd(p, a) = 1$ tel que $\varphi(X) = x^p + ax + a$ est irréductible sur $\mathbb{Q}$. Alors le groupe de Galois G de $\varphi(X) = 0$ sur $\mathbb{Q}$ est le groupe symétrique S_p si et seulement si $(p-1)^{p-1}a + p^p$ n'est pas un carré. Si $(p-1)^{p-1}a + p^p$ est un carré, alors G est un groupe simple non cyclique, et le corps de décomposition de $\varphi(X) = 0$ n'est pas ramifié (par rapport aux places premiers finis) sur $\mathbb{Q}(\alpha)$, où α désigne un racine arbitraire de $\varphi(X)$.*

Démonstration. Puisque $p^p \equiv p \equiv 1(mod 8)$, $(p-1)^{p-1}a + p^p = -m^2$ est impossible.

Dès lors, si $(p-1)^{p-1}a + p^p$ n'est pas un carré, il existe un nombre premier q tel que le discriminant d_K de $K = \mathbb{Q}(\alpha)$ est exactement divisible par q, et donc $G = S_p$ (Voir la démonstration du théorème 3.17).

La seconde moitié du Théorème 2 est démontrée dans [17]

□

Remarque 3.21. il est prouvé dans [17] (Théorème 5 et sa démonstration) que, pour tout nombre premier $p \equiv 1(mod 8)$, il existe une infinité d'entiers a avec les propriétés suivantes :

1. $\varphi(X) = x^p + ax + a$ est irréductible sur $\mathbb{Q}$;
2. $\text{pgcd}(p, a) = 1$;
3. $(p-1)^{p-1}a + p^p$ est un carré.

en [19] il est prouvé aussi.

Théorème 3.22. *Soit p un nombre premier impair, et soit t et b des entiers rationnels tels que $0 < t < p$, $pgcd(p, b) = 1$. Supposer que $|(p-1)^{p-1}b + p^{p-t}|$ n'est pas un carré. Alors le groupe de Galois de*

$$x^p + p^t b(x+1) = 0$$

sur $\mathbb{Q}$ est le groupe symétrique S_p.

Démonstration. (cf. [19, théorème 2]), .

□

Théorème 3.23. *Soit p un nombre premier, et k un entier rationnel tel que $pgcd(p, k) = 1$. Alors le groupe de Galois de*

$$x^p + pk^2(x+1) = 0$$

sur $\mathbb{Q}$ est le groupe symétrique S_p.

Démonstration. (cf.[19, théorème 3]).

□

Comme cas particulier ($k = 1$) du théorème précédent , on obtient.

Théorème 3.24. *Pour tout nombre premier p, le groupe de Galois de*

$$x^p + px + p = 0$$

sur $\mathbb{Q}$ est le groupe symétrique S_p.

Théorème 3.25. *Soit p, $(p > 3)$ un nombre premier et soit b et m des entiers rationnels tels que*

$$0 < 2m < p, pgcd(p, b) = 1$$

Soit G le groupe de Galois de l'équation

$$x^p + p^{2m}b(x + 1) = 0$$

sur $\mathbb{Q}$.

1. Si $p \equiv 3$ ou 5 ou 7 $(mod 8)$, alors G est le groupe symétrique S_p.

2. Supposons que $p \equiv 1(mod 8)$. Alors $G = S_p$ si et seulement si $(p-1)^{p-1}b + p^{p-2m}$ n'est pas un carré.

Si $(p-1)^{p-1}b + p^{p-2m}$ est un carré, alors G est contenu dans le groupe alterné A_p .

Démonstration. Nous avons

$$p^{p-2m} \equiv p(mod 8). \tag{3.6.1}$$

Aussi, pour tout facteur premier q de $p - 1$,

$$p^{p-2m} \equiv 1(mod q) \tag{3.6.2}$$

.

Si $p \equiv 3$ ou 5 ou $7(mod 8)$, alors

$$|(p-1)^{p-1}b + p^{p-2m}|$$

n'est pas un carré ([18], la preuve du théorème 1), donc $G = S_p$ (Théorème 3.22). Supposons maintenant que $p \equiv 1\ (mod 8)$. Il découle de (3.6.1) que $-\{(p-1)^{p-1}b+p^{p-2m}\}$ n'est pas un carré. Donc, si $(p-1)^{p-1}b + p^{p-2m}$ n'est pas un carré, alors $G = S_p$ (Théorème 3.22). Supposons en outre que $(p-1)^{p-1}b + p^{p-2m}$ soit un carré. Soit α_1, α_2, $\cdots$, α_p les racines de $f(x) = x^p + p^{2m}b(x + 1) = 0$, et soit $\delta = f'(\alpha_1)$, $D = N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}(\delta)$. Ensuite, par [19, (2.1)] on voit que D est aussi un carré.

Soit maintenant A la matrice suivante :

$$A = (a_{ij}), a_{ij} = \alpha_i^{j-1}(1 \leq i \leq p; 1 \leq j \leq p).$$

Alors nous avons

$$(\det A)^2 = (-1)^{p\langle p-1)/2}D = D.$$

Donc $\det A$ est un entier rationnel. Si $g \in G$ est une permutation impaire, alors $(\det A)^g = -(\det A)$, ce qui est impossible. Donc G est contenu dans A_p.

□

A. Movahhedi dans [28] est d'étudier le groupe de Galois absolu G de un tel trinôme $\varphi(X)$. lorsqu'il est de type Eisenstein par rapport à p .Il a commencé par ce lemme.

Lemme 3.26. *Soit $E/\mathbb{Q}_p$ une extension non galoisienne de degré p, et soit F la clôture galoisienne de $E/\mathbb{Q}_p$. Supposons que le discriminant absolu de E soit égal à p^p. Alors F est une extension totalement ramifiée de $\mathbb{Q}_p$ avec groupe de Galois isomorphe au groupe affine Aff$(\mathbb{F}_p)$.*

Démonstration. En choisissant un élément primitif α de $E/\mathbb{Q}_p$, et en prenant son polynôme minimal $f(X)$, le groupe de Galois $Gal(F/\mathbb{Q}_p)$ peut être identifié à un groupe de permutation de degré p, agissant sur les racines de $f(X)$.

Puisque $Gal(F/\mathbb{Q}_p)$ est aussi résoluble en tant que groupe de Galois local, il est isomorphe à un sous-groupe de Aff$(\mathbb{F}_p)$. Il suffit donc de montrer que l'extension F/E est totalement ramifiée de degré égal à $p-1$.

Soit $\mathfrak{D}(F/\mathbb{Q}_p)$ la différent de l'extension locale $F/\mathbb{Q}_p$. Par la transitivité du différent, on a

$$\mathfrak{D}(F/\mathbb{Q}_p) = \mathfrak{D}(F/E).\mathfrak{D}(E/\mathbb{Q}_p).$$

Soit $(G_i)_{i\geq 0}$ les groupes de ramification de l'extension galoisienne $F/\mathbb{Q}_p$. Nous avons alors

$$\begin{aligned}\mathfrak{D}(F/\mathbb{Q}_p) &= \mathfrak{p}^{\sum_{i\geq 0}(\#G_i - 1)} \\ &= \mathfrak{p}^{e-1+\lambda(p-1)}\end{aligned}$$

où $\mathfrak{p}$ est l'idéal maximal de F, l'entier e est l'indice de ramification de l'extension $F/\mathbb{Q}_p$, et G_λ est le dernier groupe de ramification non trivial.

D'autre part, comme F/E est modérément ramifiée

$$\mathfrak{D}(F/E) = \mathfrak{p}^{\frac{e}{p-1}}$$

et, par hypothèse, on a

$$\mathfrak{D}(E/\mathbb{Q}_p) = (\mathfrak{p}^{\frac{e}{p}})^p = \mathfrak{p}^e$$

En tenant compte de toutes ces dernières égalités, on obtient $e = \lambda p(p-1)$. On a donc nécessairement $\lambda = 1$ et $e = p(p-1)$.

□

par l'utilisation du lemme précédent et les polygones de Newton, l'auteur a déterminé les groupes d'inertie de tous les nombres premiers qui divisent a.

Si on note par K et N les corps de rupture et de décomposition de $\varphi(X)$ sur $\mathbb{Q}$.on a :

Lemme 3.27. *Le groupe d'inertie (défini à conjugaison près) de p dans $N/\mathbb{Q}$ est isomorphe au groupe affine Aff($\mathbb{F}_p$).*

Lemme 3.28. *[28, lemme 1.3] Sous l'hypothèse $\left|p^{p-1} + \frac{a}{p}(p-1)^{p-1}\right|$ est un carré, un nombre premier rationnel est soit non ramifié, soit totalement ramifié dans le corps de nombres K.*

Ce dernier lemme combiné au lemme d'Abhyankar [30, p ; 229], donnent immédiatement :

Proposition 3.29. *le groupe d'inertie de chaque idéal premier ramifié de N, qui n'est pas au-dessus de p, est cyclique d'ordre p.*

Après la détermination des groups d'inertie A. Movahhedi donne une condition nécessaire et suffisante, sur le corps de décomposition N, pour que le groupe de Galois G soit résoluble.

Théorème 3.30. *[28, théorème 2.2] Soit $\varphi(X) = X^p + aX + a$ un trinôme d'Eisenstein par rapport à $p > 3$. Le groupe de Galois absolu G de $\varphi(X)$ est résoluble si et seulement si le corps de décomposition N de $\varphi(X)$ est obtenu en adjoignant à $\mathbb{Q}$ une racine π de $\varphi(X)$ et une racine primitive $p-$ième d'unité ζ_p. En particulier, si G est résoluble alors G est isomorphe au groupe affine Aff($\mathbb{F}_p$).*

fin il a prouvé le résultat que nous généraliser dans notre article pour une puissance quelconque d'un premier impaire

Théorème 3.31. *[28, théorème 3.3]Soit $\varphi(X) = X^p + aX + a$ un trinôme d'Eisenstein par rapport à p. Le groupe de Galois absolu G de $\varphi(X)$ est soit le groupe symétrique S_p , soit le groupe affine Aff$(\mathbb{F}_p)$.*

Chapitre 4

Groupe de Galois de $X^{p^n} + aX + a$

4.1 Groupe de Galois de $X^{p^2} + aX + a$

4.1.1 groupe d' inertie

Soit p un nombre premier impair et a un entier rational tel que $\upsilon_p(a) = 1$. On note par $\alpha = \alpha_1, \alpha_2, ..., \alpha_{p^2}$ les racines distinctes du trinôme $f(X) = X^{p^2} + aX + a$, qui est de type d'Eisenstein dans une clôture algébrique de $\mathbb{Q}$. Soient $K = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_{p^2})$ les corps de rupture et de décomposition de $f(X)$ sur $\mathbb{Q}$.

Le groupe de Galois G de$f(X)$, qui est le groupe de Galois de l'extension $N/\mathbb{Q}$, est un groupe de permutation transitif agissant sur les p^2 racines distinctes de $f(X)$. Le discriminant D du trinôme $f(X)$ est :

$$D = p^{p^2} b^{p^2-1} D_0$$

où $b = \frac{a}{p}$ et $D_0 = p^{2p^2-1} + b(p^2-1)^{p^2-1}$

Nous allons maintenant déterminer, les groupes d'inertie en les déférentes places de N.

Proposition 4.1. *Le groupe d'inertie (défini à conjugaison près) de p dans $N/\mathbb{Q}$ est isomorphe au groupe affine $AGL(1, p^2)$ de dimension 1 sur le corps fini $\mathbb{F}_{p^2}$.*

Démonstration. Fixons un premier $p-$adique $\mathfrak{P}$ de N au dessus de p et soit $\mathfrak{p} = \mathfrak{P} \cap K$ un idéal premier de K au dessus de p. Notons par $N_{\mathfrak{P}}$ et $K_{\mathfrak{p}}$ les complété de N et K pour les valuations $\mathfrak{P}$-adique et $\mathfrak{p}$-adique respectivement. Comme le trinôme f est d'Eisenstein en p sur $\mathbb{Q}$, alors l'extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ est totalement ramifiée.

On considère le polynôme

$$\varphi(X)=\frac{f(\alpha X+\alpha)}{\alpha^{p^2}X}=X^{p^2-1}+\sum_{i=1}^{p^2-1}a_iX^{p^2-i-1}\in\mathbb{Q}(\alpha)[X].$$

où les coefficients a_i sont donnés par

$$a_i=\begin{cases}\begin{pmatrix}p^2\\ i\end{pmatrix} & \text{if}1\leq i\leq p^2-2\\ \left(p^2+a\alpha^{1-p^2}\right) & \text{if } i=p^2-1\end{cases}$$

Soient π une uniformisante de $K_{\mathfrak{p}}$, et υ_π la valuations $\pi-$adiques normalisé, de $K_{\mathfrak{p}}$, alors $\upsilon_\pi(\alpha)=\upsilon_p(a)=1$ et $\upsilon_\pi(\lambda)=p^2\upsilon_p(\lambda)$ pour tout $\lambda\in\mathbb{Q}_p$, puisque l' extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ est totalement ramifié. Alors $\upsilon_\pi(a_i)\geq p^2$ pour tout $i=1,...,p^2-2$, et $\upsilon_\pi(a_{p^2-1})=1$. Ainsi, le $(K_{\mathfrak{p}},\,X)$ - polygone de $\varphi(X)$ est formé d'un seul côté S joignant les points $(0,0)$ et $(p^2-1,1)$. Par conséquent, et d'après [11, Theorem 1.5] l'indice de ramification de l'extension locale $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ est égal à p^2-1.

Notons par $I_{\mathfrak{P}}$ le groupe d'inertie de l 'extension $N_{\mathfrak{P}}/\mathbb{Q}_p$, et par $I'_{\mathfrak{P}}=I_{\mathfrak{P}}\cap Gal(N_{\mathfrak{P}}/K_{\mathfrak{p}})$ le groupe d'inertie de l 'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}$, $I'_{\mathfrak{P}}$ est un stabilisateur d'un point de $I_{\mathfrak{P}}$. Par le Lemme d'Abhyankar [30, p. 229], l'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}(\alpha_2)$ est non ramifiée, alors l'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}$ est modérément ramifiée, ce qui entraine, dans ce cas, que le groupe d'inertie $I'_{\mathfrak{P}}$ est cyclique engendré par un cycle d'ordre p^2-1. Introduisons le corps d'inertie L_0 dans $N_{\mathfrak{P}}/\mathbb{Q}_p$, alors L'extension totalement ramifiée $K_{\mathfrak{p}}/\mathbb{Q}_p$ est linéairement disjointe de l'extension non ramifiée $L_0/\mathbb{Q}_p$, ce qui entraine que le polynôme $f(X)$ reste irréductible sur L_0. Par conséquent, $I_{\mathfrak{P}}=Gal(N_{\mathfrak{P}}/L_0)$ agit transitivement sur les racines de $f(X)$. D' autre part, l'extension totalement ramifiée $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ est linéairement disjointe de l'extension non ramifiée $L_0(\alpha)/K_{\mathfrak{p}}$, ce qui entraine que le polynôme $\varphi(X)$ reste irréductible sur $L_0(\alpha)$. Par suite, $I'_{\mathfrak{P}}=Gal(N_{\mathfrak{P}}/L_0(\alpha))$ agit transitivement sur les racines de $\varphi(X)$ et donc $I'_{\mathfrak{P}}$ est un sous-groupe transitif et régulier de $I_{\mathfrak{P}}$. Par conséquent, $I_{\mathfrak{P}}$ est 2-transitif et 2-antitransitif [1, § 15] de degré p^2 et d'ordre $p^2(p^2-1)$, dont les stabilisateurs d'un point sont abéliens, ce qui montre que le groupe $I_{\mathfrak{P}}$ est isomorphe à $AGL(1,p^2)$ [12, Corollair 7.6A (ii), p 239].

□

Lemme 4.2. *Soit $q\neq p$ un diviseur premier de a.*

(i) Si p^2 divise $\upsilon_q(a)$, alors le nombre premier q est non ramifié dans $K=\mathbb{Q}(\alpha)$.

(ii) Si $pgcd(p^2;\upsilon_q(a)) \leq p$, *alors le nombre premier* q *est modérément ramifié dans* $K=\mathbb{Q}(\alpha)$. *De plus si* $pgcd(p^2;\upsilon_q(a))=1$, *alors le nombre premier* q *est totalement ramifié dans* $K=\mathbb{Q}(\alpha)$.

Démonstration. .

Le $(\mathbb{Q}_q, X)$- polygone de $f(X)$ est formé d'un seul côté S reliant les point$(0,0)$ et $(p^2, \upsilon_q(a))$.
Le polynôme associé à $f(X)$ et relatif au côté S est le binôme

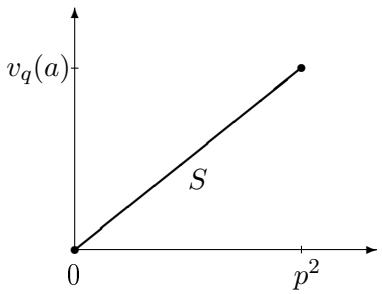

Figure 2. Le $(\mathbb{Q}_q, X)$-polygon of $f(X)$

$$G(Y)=Y^m+a_q$$

où $m=\text{pgcd}(p^2;\upsilon_q(a))$ et $a_q={}^{a}/_{q^{\upsilon_q(a)}}$.

Ainsi d'après [31, Sect. 2, Théorèm 5], $q=\mathfrak{A}^{p^2/m}$, avec $\mathfrak{A}$ un idéal de K.

En outre, $G(Y)$ est séparable modulo q, alors $\mathfrak{A}$ est un produit des idéaux premiers de K, distincts. [31, Sect. 2, Théorèm 6].

□

Ce dernier Lemme combiné au Lemme d'Abhyankar [30, p.229], donnent immédiatement :

Proposition 4.3. *Soit* $q \neq p$ *un diviseur premier de* a, *ramifié dans* N. *Le groupe d'inertie (défini à conjugaison près) de* q *dans* $N/\mathbb{Q}$ *est cyclique d'ordre* p^2 *ou* p *suivant que* $pgcd(p^2;\upsilon_q(a))=1 ou\ p$.

4.1.2 Groupe de Galois

Noter que si $|D_0|$ n' est pas un carré, alors le groupe de Galois G de $f(X)$ est le groupe symétrique S_{p^2}. En effet, si un nombre premier ℓ divise $|D_0|$ en une puissance impaire, alors l divise le discriminant absolu du corps $K=\mathbb{Q}(\alpha)$ une seule fois [23, Théorem 2]. Ce qui implique que le groupe de Galois G de $f(X)$ contiendrait une transposition [18, Lemme 1], et comme il est doublement transitive (Proposition 4.1), c'est donc, d' aprés [12, Théorem 3.3A , p 77], tout le groupe symétrique S_{p^2}.

Maintenant, il est naturel de seposer la question suivante : « pour quelles valeurs de p, la valeur absolue de D_0 n'est pas un carré ? »

Lemme 4.4. *Soit p un nombre premier impair, et le trinôme $f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$qui est de type d'Eisenstein relatif à p. Alors l' entier rationnel $|D_0|$ n'est pas un carré dans chacun des cas suivants :*

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, *et il existe un diviseur premier q de $p+1$ tel que* $q \equiv -1 \mod 4$.

Démonstration. Supposons que $|D_0| = k^2$ pour un entier rationnel k, alors on a

$$D_0 \equiv p^{2p^2-1} \equiv p \equiv \pm k^2 \mod 8.$$

Si $p \not\equiv 1 \mod 8$, alors $p \equiv -1 \mod 8$ et $D_0 = -k^2$.

Ainsi, $\frac{p-1}{2} \equiv -1 \mod 4$ et il existe alors diviseur premier q de $\frac{p-1}{2}$ tel que $q \equiv -1 \mod 4$. Comme $p \equiv 1 \mod q$, alors $-k^2 \equiv p^{2p^2-1} \equiv p \equiv 1 \mod q$, ce qui entraine que -1 est un résidu quadratique modulo q, et ceci est contradictoire avec la congruence $q \equiv -1 \mod 4$.

Si (ii) est vérifiée, alors $D_0 \equiv p^{2p^2-1} \equiv p \equiv 1 \mod 8$, et l'égalité $D_0 = -k^2$ est impossible. Par conséquent, $D_0 = k^2$ et dans ce cas $k^2 \equiv p^{2p^2-1} \equiv p \equiv -1 \mod q$, ce qui entraine que -1est un résidu quadratique modulo q, qui est une contradiction puisque $q \equiv -1 \mod 4$. Par conséquent, l'entier $|D_0|$ n'est pas un carré.

□

La discussion ci-dessus et le dernier lemme entraîne immédiatement le résultat suivant :

Théorème 4.5. *Soit p un nombre premier impair, et le trinôme $f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$qui est de type d'Eisenstein relatif à p. Alors le groupe de Galois G du trinôme $f(X) = X^{p^2} + aX + a$ c'est le groupe symétrique S_{p^2} dans chacun des cas suivants :*

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, *et il existe un diviseur premier q de $p+1$ tel que*

$q \equiv -1 \mod 4$.

D'après le (Proposition 4.1), le groupe de de Galois G du trinôme $f(X) = X^{p^2} + aX + a$ est doublement transitive. Les groupes doublement transitifs ont listés dans [1, CTT , et

weak CDT] et [12, Theorem 4.7 A], ce qui nous permet de donner la liste suivante de réalisations possibles du groupe de Galois G du trinôme f

1. $G \simeq S_{p^2}$; ou
2. $G \simeq A_{p^2}$; ou
3. $(Z)_p^2 \leq G \leq AGL\,(2,p)$, où (Z_p) est le groupe cyclique d'ordre p ; ou
4. $PSL(m,q) \leq G \leq P\Gamma L(m,q)$. pour un entier $m>1$ et une puissance d'un nombre premier impair q telle que ${}^{(q^m-1)}/_{(q-1)} = p^2$.

Théorème 4.6. *Soit p un nombre premier impair, et le trinôme $f(X) = X^{p^2}+aX+a \in \mathbb{Z}[X]$qui est de type d'Eisenstein relatif à p. Alors le groupe de Galois absolu G de $f(X)$ est soit le groupe symétrique S_{p^2}, ou $AGL\left(1,p^2\right) \leq G \leq AGL\,(2,p)$.*

Démonstration. On remarque d'abord que D n'est pas un carré, donc G n'est pas contenu dans le groupe alterné A_{p^2}.

Supposons maintenant que $PSL(m,q) \leq G \leq P\Gamma L(m,q)$. pour un entier $m>1$ et une puissance d'un nombre premier impair q, alors

$$p^2 = \tfrac{q^m-1}{q-1} = q^{m-1}+q^{m-2}+...+q+1.$$

Si q est impair, alors m doit être un nombre impair, ce qui implique que G ne contient pas d'involution fixant au plus trois points [10, Proposition 2.4] ; cela contredit l'hypothèse que G est un groupe de Galois de trinôme.

Si q est pair, en utilisant [1, lemme numérique, p. 23] et [10, Proposition 2.4], le seul cas restant est $(m,q)=(2,8)$ et $(n,p)=(2,3)$ ce qui est impossible par (Théorem 4.5).

Sachant par la (Proposition 4.1) que le groupe linéaire affine $AGL(1,p^2) \leq G$, ce qui complète la preuve.

□

Maintenant, nous supposerons que le nombre premier $p \equiv 1 \mod 8$ tel que chaque diviseur premier q de $p+1$ vérifie $q \not\equiv -1 \mod 4$. Il convient de noter que D_0 est un carré pour une infinité d'entiers rationnels b. En effet, nous avons $p^{2p^2-1} \equiv 1 \mod 8$, et pour tout diviseurs premiers impairs l de $p-1$ et q de $p+1$ on a $p^{2p^2-1} \equiv 1 \mod l$ et

$p^{2p^2-1} \equiv -1 \mod q$. Sachant que $q \equiv 1 \mod 4$, alors p^{2p^2-1} est un résidu quadratique modulo q. Donc la congruence

$$X^2 \equiv p^{2p^2-1} \mod (p^2-1)^{p^2-1}$$

est résoluble. Soit maintenant α une solution de la congruence ci-dessus et on peut supposer que α n'est pas divisible par p, puisque $\alpha + (p^2-1)^{p^2-1}$ est aussi une solution de cette congruence. Alors il existe un entier β qui n'est pas divisible par p tel que

$$\alpha^2 - p^{2p^2-1} = \beta(p^2-1)^{p^2-1}$$

Pour tout $r \in \mathbb{Z}$, soit

$$b = \beta + 2rp\alpha + r^2p^2(p^2-1)^{p^2-1},$$

alors D_0 est un carré.

En résumé, nous avons établi

Théorème 4.7. *Soit p un nombre premier impair, et $f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$ un trinôme qui est de type d'Eisenstein relatif à p. S'il existe un diviseur premier $q \neq p$ de a tel que $pgcd(\upsilon_q(a), p) = 1$, alors le groupe de Galois absolu G de f est le groupe symétrique S_{p^2}.*

Démonstration. On peut supposer que $|D_0|$ est un carré, car sinon G serait le groupe symétrique S_{p^2}. On fixe un idéal premier $\mathfrak{Q}$ de N au-dessus de q. Soit $\mathfrak{q} = \mathfrak{Q} \cap K$. Notons par $N_{\mathfrak{Q}}$ le complété de N en $\mathfrak{Q}$ et $K_{\mathfrak{q}}$ le complété de K en$\mathfrak{q}$. Le corps local $K_{\mathfrak{q}}$ est obtenu par adjonction à $\mathbb{Q}_q$ d'une racine de f c'est une extension totalement ramifiée de $\mathbb{Q}_q$ (Lemme 4.2). Notons par $I_{\mathfrak{Q}}$ le groupe d'inertie de $\mathfrak{Q}$ au dessus de $\mathfrak{q}$ dans $N/\mathbb{Q}$. Introduisons le corps d'inertie L_0 dans $N_{\mathfrak{Q}}/\mathbb{Q}_q$. L'extension totalement ramifiée $K_{\mathfrak{q}}/\mathbb{Q}_q$ est linéairement disjointe de l'extension non ramifiée $L_0/\mathbb{Q}_q$, ce qui entraine que le polynôme $f(X)$ reste irréductible sur L_0. Par conséquent, $I_{\mathfrak{Q}} = Gal(N_{\mathfrak{Q}}/L_0)$ agit transitivement sur les racines de $f(X)$. Comme le groupe d'inertie $I_{\mathfrak{Q}}$ est cyclique, il contient un cycle d'ordre p^2 (Proposition 4.3). Par[22, Proposition 1.1] , et (Théorem 4.6) nous concluons que le groupe G est S_{p^2}.

□

4.2 Groupe de Galois de $X^{p^n}+aX+a$, avec $n \geq 3$

Soit p un nombre premier impair, $n \geq 3$ un entier rationnel, et soit $f(X) = X^{p^n} + aX + a$ un trinôme qui est de type d'Eisenstein relatif à p. Nous prouvons que le groupe de Galois G de $f(X)$ sur le corps $\mathbb{Q}$ des nombres rationnels, est soit le groupe symétrique S_{p^n}, soit $AGL(1,p^n) \leq G \leq AGL(n,p)$. On montre aussi que $G = S_{p^n}$, sauf peut-être quand $|p^{np^n-1} + \frac{a}{p}(p^n-1)^{p^n-1}|$ est un carré, et pour chaque diviseur premier l de a/p, p divise la valuation l-adique $\upsilon_l(a)$ de l'entier a.

4.2.1 groupe d' inertie

Soient p un nombre premier impair, n un entier positif et a un entier rationnel tel que $\upsilon_p(a) = 1$. On note par $\alpha = \alpha_1,\alpha_2,...,\alpha_{p^n}$ les racines distinctes du trinôme $f(X) = X^{p^n} + aX + a$, qui est de type d'Eisenstein dans une clôture algébrique de $\mathbb{Q}$. Soient $K = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_{p^n})$ les corps de rupture et de décomposition de $f(X)$ sur $\mathbb{Q}$. Le groupe de Galois G de$f(X)$, qui est le groupe de Galois de l'extension $N/\mathbb{Q}$ est un groupe de permutation transitif agissant sur les p^n racines distinctes de $f(X)$. Nous allons maintenant déterminer, les groupes d'inertie en les déffirents places de N.

Lemme 4.8. *Le groupe d'inertie (défini à conjugaison près) de p dans $N/\mathbb{Q}$ est isomorphe au groupe $AGL(1,p^n)$, le groupe affine de dimension 1 sur le corps fini $\mathbb{F}_{p^n}$.*

Démonstration. Fixons un idéal premier $\mathfrak{P}$ de N au-dessus de p. Soit $\mathfrak{p} = \mathfrak{P} \cap K$. Notons par $N_{\mathfrak{P}}$ le complété de N en $\mathfrak{P}$ et $K_{\mathfrak{p}}$ le complété de de K en $\mathfrak{p}$. Comme le trinôme f est d'Eisenstein sur $\mathbb{Q}_p$, donc l'extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ est totalement ramifiée.

On considère le polynôme

$$\varphi(X) = \frac{f(\alpha X + \alpha)}{\alpha^{p^n} X} = X^{p^n-1} + \sum_{i=1}^{p^n-1} a_i X^{p^n-i-1} \in \mathbb{Q}(\alpha)[X].$$

où les coefficients a_i sont donnés par

$$a_i = \begin{cases} \binom{p^n}{i} & \text{if} 1 \leq i \leq p^n - 2 \\ \left(p^n + a\alpha^{1-p^n}\right) & \text{if } i = p^n - 1 \end{cases}$$

Soient π une uniformisante de $K_{\mathfrak{p}}$, et υ_π la valuations $\pi-$adiques normalisé, de $K_{\mathfrak{p}}$, alors $\upsilon_\pi(\alpha) = \upsilon_p(a) = 1$ et $\upsilon_\pi(\lambda) = p^n\upsilon_p(\lambda)$ pour tout $\lambda \in \mathbb{Q}_p$, puisque l' extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ est totalement ramifié. Alors $\upsilon_\pi(a_i) \geq p^n$ pour tout $i = 1, ..., p^n - 2$, et $\upsilon_\pi(a_{p^n-1}) = 1$.

Ainsi le polynôme $\varphi(X)$ est de type d'Eisenstein sur le corps local $K_{\mathfrak{p}}$. Remarquons que $\zeta = \alpha_2/\alpha - 1$ est une racine de $\varphi(X)$. Ainsi $K_{\mathfrak{p}}(\alpha_2) = K_{\mathfrak{p}}(\zeta)$. Ainsi d'après [30, Théorème 5.27], l'extension locale $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ est totalement ramifiée et son indice de ramification est égal à p^n-1. Notons par $I_{\mathfrak{P}}$ le groupe d'inertie de l 'extension $N_{\mathfrak{P}}/\mathbb{Q}_p$, et par $I'_{\mathfrak{P}} = I_{\mathfrak{P}} \cap Gal(N_{\mathfrak{P}}/K_{\mathfrak{p}})$ le groupe d'inertie de l 'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}$, $I'_{\mathfrak{P}}$est un stabilisateur d' un point de $I_{\mathfrak{P}}$. Par le Lemme d'Abhyankar [30, p. 229], l'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}(\alpha_2)$ est non ramifiée, alors l'extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}$ est modérément ramifiée, ce qui entraine, dans ce cas, que le groupe d'inertie $I'_{\mathfrak{P}}$ est cyclique ; il est engendré par un cycle d'ordre p^n-1. Introduisons le corps d'inertie L_0 dans $N_{\mathfrak{P}}/\mathbb{Q}_p$, alors L'extension totalement ramifiée $K_{\mathfrak{p}}/\mathbb{Q}_p$ est linéairement disjointe de l'extension non ramifiée $L_0/\mathbb{Q}_p$, ce qui entraine que le polynôme $f(X)$ reste irréductible sur L_0. Par conséquent, $I_{\mathfrak{P}} = Gal(N_{\mathfrak{P}}/L_0)$ agit transitivement sur les racines de $f(X)$. D' autre part L'extension totalement ramifiée $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ est linéairement disjointe de l'extension non ramifiée $L_0(\alpha)/K_{\mathfrak{p}}$, ce qui entraine que le polynôme $\varphi(X)$ reste irréductible sur $L_0(\alpha)$. Par conséquent, $I'_{\mathfrak{P}} = Gal(N_{\mathfrak{P}}/L_0(\alpha))$ agit transitivement sur les racines de $\varphi(X)$, alors $I'_{\mathfrak{P}}$ est un sous-groupe transitif de $I_{\mathfrak{P}}$, donc régulier . Par conséquent, $I_{\mathfrak{P}}$ est 2-transitif et 2-antitransitif [1, § 15] de degré p^n et d'ordre $p^n(p^n - 1)$, et ces stabilisateurs d'un point sont abileans. Par [12, Corollair 7.6A (ii), p 239] le groupe $I_{\mathfrak{P}}$ est isomorphe à $AGL(1, p^n)$.

□

Lemme 4.9. *Soit $q \neq p$ un diviseur premier de a.*

(i) Si p^n divise $\upsilon_q(a)$, alors le nombre premier q est non ramifié dans $K = \mathbb{Q}(\alpha)$.

(ii) Si p^n ne divise pas $\upsilon_q(a)$, alors tout idéal premier de K au-dessus de q est modérément ramifié dans $K = \mathbb{Q}(\alpha)$. De plus si $pgcd(p^n; \upsilon_q(a)) = 1$, alors le nombre premier q est totalement ramifié dans $K = \mathbb{Q}(\alpha)$.

Démonstration. .

Le $(\mathbb{Q}_q, X)$- polygon de $f(X)$ est formé d'un seul côté S reliant les points $(0,0)$ et $(p^n, v_q(a))$. Le polynôme associé à $f(X)$ et relatif au côté S est un binôme de la forme

$$G(Y) = Y^m + a_q$$

où $m = \text{pgcd}(p^n; v_q(a))$ et $a_q = {}^{a}/_{q^{v_q(a)}}$.

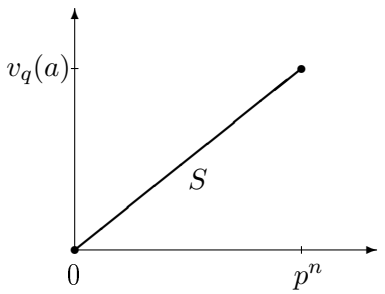

Figure 3. Le $(\mathbb{Q}_q, X)$-polygon of $f(X)$

De plus, $G(Y)$ est séparable modulo q , donc d'après [11, Théoreme 1.5] l'indice de ramification de $\mathbb{Q}_q(\alpha)/\mathbb{Q}_q$ est égal à $\frac{p^n}{m}$.

□

Ce dernier Lemme combiné au Lemme d'Abhyankar [30, p.229], donnent immédiatement :

Proposition 4.10. *Soit $q \neq p$ un diviseur premier de a, ramifié dans N. Le groupe d'inertie (défini à conjugaison près) de q dans $N/\mathbb{Q}$ est cyclique d'ordre $\frac{p^n}{pgcd(p^n; v_q(a))}$.*

4.2.2 Groupe de Galois

Dans le reste de la section, nous supposerons que $n \geq 3$. Le discriminant D du trinôme $f(X) = X^{p^n} + aX + a$ est donné par

$$D = (-1)^{\frac{p^n-1}{2}} p^{p^n} b^{p^n-1} D_0$$

où $b = \frac{a}{p}$ et $D_0 = p^{np^n-1} + b(p^n-1)^{p^n-1}$

Lemme 4.11. *Soit p un nombre premier impair, et $n > 3$ un entier rational pair. Soit le trinôme $f(X) = X^{p^n} + aX + a \in \mathbb{Z}[X]$ qui est de type d'Eisenstein relatif à p. Alors l'entier rationnel $|D_0|$ n'est pas un carré dans chacun des cas suivants :*

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, *et il existe un diviseur premier q de $p^{n-1} + p^{n-2} + ... + p + 1$ tel que* $\left(\frac{q}{p}\right) = -1$.

Démonstration. Supposons que $|D_0| = k^2$ pour un entier rationnel k, alors on a

$$D_0 \equiv p^{np^n-1} \equiv p \equiv \pm k^2 \mod 8.$$

Si $p \not\equiv 1 \mod 8$, alors $p \equiv -1 \mod 8$ et $D_0 = -k^2$.

Ainsi, $\frac{p-1}{2} \equiv -1 \mod 4$ et il existe alors diviseur premier q de $\frac{p-1}{2}$ tel que $q \equiv -1 \mod 4$. Comme $p \equiv 1 \mod q$, alors

$$-k^2 \equiv p^{np^n-1} \equiv p \equiv 1 \mod q,$$

ce qui entraine que -1 est un résidu quadratique modulo q, et ceci est contradictoire avec la congruence $q \equiv -1 \mod 4$.

Si (ii) est vérifiée, alors

$$D_0 \equiv p^{np^n-1} \equiv p \equiv 1 \mod 8,$$

et l'égalité $D_0 = -k^2$ est impossible. Par conséquent, $D_0 = k^2$ et dans ce cas $k^2 \equiv p^{np^n-1} \mod q$, ce qui entraine que p doit être un résidu quadratique modulo q ; cependant, c'est une contradiction, puisque $p \equiv 1 \mod 4$ et $\left(\frac{q}{p}\right) = -1$ Par conséquent, l'entier $|D_0|$ n'est pas un carré.

□

Théorème 4.12. *Soit p un nombre premier impair, et $n > 3$ un entier rational pair. Soit le trinôme $f(X) = X^{p^n} + aX + a \in \mathbb{Z}[X]$ qui est de type d'Eisenstein relatif à p. Alors le groupe de Galois G du trinôme $f(X) = X^{p^n} + aX + a$ c'est tout le groupe symétrique S_{p^n} dans chacun des cas suivants :*

(i) $p \not\equiv 1 \mod 8$

(ii) $p \equiv 1 \mod 8$, *et il existe un diviseur premier q de $p^{n-1} + p^{n-2} + ... + p + 1$ tel que $\left(\frac{q}{p}\right) = -1$.*

Démonstration. Soit l un nombre premier qui divise$|D_0|$ en une puissance impaire Théorem 4.11, alors l divise le discriminant absolu du corps $K = \mathbb{Q}(\alpha)$ une seule fois [23, Théoreme 2]. Ceci implique que le groupe de Galois G contient une transposition [18, Lemme 1]. Or G est un groupe de permutation doublement transitif (voir la preuve de la (Proposition 4.8)) et contient une transposition, alors d'après [12, Théoreme 3.3A, p. 77] G est tout le groupe symétrique S_{p^n}.

□

Maintenant, nous supposerons que $|D_0|$ est un carré pour voir à quel groupe le groupe de Galois G peut être isomorphe, autre que S_{p^n}. Il est important de noter que si n

est pair et $p \equiv 1 \mod 8$ tel que $\left(\frac{q}{p}\right) = 1$ pour chaque diviseur premier impair q de $p^{n-1}+p^{n-2}+...+p+1$, alors l'expression

$$D_0 = p^{np^n-1} + b(p^n-1)^{p^n-1}$$

est un carré pour une infinité d'entiers rationnels b avec $p \nmid b$. En effet, nous avons $p^{np^n-1} \equiv 1 \mod 8$, et pour tout diviseur premier impair l de $p-1$ on a $p^{np^n-1} \equiv 1 \mod l$, aussi pour chaque q de $p^{n-1}+p^{n-2}+...+p+1$ on a $\left(\frac{q}{p}\right) = 1$. Ce qui implique que p^{np^n-1} est un résidu quadratique modulo q. Donc la congruence

$$X^2 \equiv p^{np^n-1} \mod (p^n-1)^{p^n-1}$$

est résoluble. Soit maintenant α une solution de la congruence ci-dessus et on peut supposer que α n'est pas divisible par p, puisque $\alpha + (p^n-1)^{p^n-1}$ est aussi une solution de cette congruence. Alors il existe un entier β qui n'est pas divisible par p tel que

$$\alpha^2 - p^{np^n-1} = \beta(p^n-1)^{p^n-1}$$

Pour tout $r \in \mathbb{Z}$, soit

$$b = \beta + 2rp\alpha + r^2p^2(p^n-1)^{p^n-1}$$

alors $D_0 = (\alpha + rp(p^n-1)^{p^n-1})^2$.

L'exemple suivant montre qu'il est possible que $p \equiv 1 \mod 8$ et pour tout facteur premier impair q de p^n-1 on ait $\left(\frac{q}{p}\right) = 1$, et aussi que b puisse être choisi tel que D_0 soit un carré.

Exemple 4.13. soit $n = 6$, on a $p = 193$ est le premier nombre premier tel que $193 \equiv 1 \mod 8$, et pour tout facteur premier impair q de p^n-1, on a $\left(\frac{q}{p}\right) = 1$.

En effet, la factorisation première est $(193^6-1) = 2^7 \times 3^2 \times 7 \times 97 \times 1783 \times 37057$. Maintenant nous pouvons voir que pour tout facteur premier impair q de $(193^6-1)^{193^6-1}$, nous avons $\left(\frac{193^{6\times 193^6-1}}{q}\right) = \left(\frac{193}{q}\right) = \left(\frac{q}{193}\right) = 1$, ce qui implique que l'équation $x_1^2 = 193^{6\times 193^6-1} + x_2(193^6-1)^{193^6-1}$ est résoluble [28, 27, p. 3]. Enfin, il suffit de prendre $D_0 = x_1^2$ and $b = x_2$.

Le second nombre premier qui satisfait $p \equiv 1 \pmod 8$ et pour tout facteur premier impair q de p^6-1 on a $\left(\frac{q}{p}\right) = 1$ est 337, puisque la factorisation première de $(337^6-1) = 2^5 \times 3^2 \times 7 \times 13^2 \times 43 \times 883 \times 113233$, et $\left(\frac{3}{337}\right) = \left(\frac{7}{337}\right) = \left(\frac{13}{337}\right) = \left(\frac{43}{337}\right) = \left(\frac{883}{337}\right) = \left(\frac{113233}{337}\right) = 1$.

Il convient également de noter que si n est impair alors pour chaque nombre premier impair p, D_0 est un carré pour une infinité d'entiers rationnels b. En effet, si

$$b = r^2(p^n - 1)^{p^n-1} + 2rp^{\frac{np^n-1}{2}},$$

tel que p ne divise pas l'entier r, alors D_0 est un carré.

D'après la preuve de la (Proposition 4.8), nous voyons que le groupe de Galois G est doublement transitif. Ainsi par [7, Théoreme 1] nous concluons que le groupe de Galois G du trinôme $f(X)$ doit être l'un des suivants :

1. $(Z)_p^n \leq G \leq AGL\,(n,p)$, où (Z_p) est le groupe cyclique d'ordre p ; ou
2. $G \simeq S_{p^n}$; ou
3. $G \simeq A_{p^n}$; ou
4. $PSL(m,q) \leq G \leq P\Gamma L(m,q)$. pour un entier $m > 1$ et une puissance d'un nombre premier impair q telle que ${}^{(q^m-1)}/_{(q-1)} = p^n$.

Théorème 4.14. *Soit p un nombre premier impair, $n \geq 3$ un entier rationnel, et soit $f(X) = X^{p^n} + aX + a$ un trinôme qui est de type d'Eisenstein relatif à p. Alors le groupe de Galois absolu G de $f(X)$ est soit le groupe symétrique S_{p^n}, ou $AGL\,(1,p^n) \leq G \leq AGL\,(n,p)$.*

Démonstration. On remarque d'abord que D n'est pas un carré, donc G n'est pas contenu dans le groupe alterné A_{p^n}. Supposons maintenant que $PSL(m,q) \leq G \leq P\Gamma L(m,q)$. pour un entier $m > 1$ et une puissance d'un nombre premier impair q, alors

$$p^n = \tfrac{q^m-1}{q-1} = q^{m-1} + q^{m-2} + ... + q + 1.$$

Si q est impair, alors m doit être un nombre impair, ce qui implique que G ne contient pas d'involution fixant au plus trois points [10, Proposition 2.4] ; cela contredit l'hypothèse que G est un groupe de Galois de trinôme.

Si q est pair, le cas $m \geq 3$ est exclu par [10, Proposition 2.4]. Alors il existe un entier positif u tel que $p^n = 2^u + 1$. D'après [1, lemme numérique, p. 89], on voit que $u = 3$ et $p^n = 9$; cela contredit l'hypothèse que $n \geq 3$. Comme le groupe linéaire affine $AGL(1,p^n) \leq G$ est un sous-groupe de G (voir (Proposition 4.8)), la preuve est complète. □

Théorème 4.15. *Soit p un nombre premier impair, $n \geq 3$ un entier rationnel, et soit $f(X) = X^{p^n} + aX + a \in \mathbb{Z}[X]$ un trinôme qui est de type d'Eisenstein relatif à p. S'il existe un diviseur premier $q \neq p$ de a tel que $pgcd(\upsilon_q(a), p) = 1$, alors le groupe de Galois absolu G de f est le groupe symétrique S_{p^n}.*

Démonstration. On peut supposer que $|D_0|$ est un carré, car sinon G serait le groupe symétrique S_{p^n}. On fixe un idéal premier $\mathfrak{Q}$ de N au-dessus de q. Soit $\mathfrak{q} = \mathfrak{Q} \cap K$. Notons par $N_{\mathfrak{Q}}$ le complété de N en $\mathfrak{Q}$ et $K_{\mathfrak{q}}$ le complété de K dans $\mathfrak{q}$. Le corps local $K_{\mathfrak{q}}$ est obtenu par adjonction à $\mathbb{Q}_q$ d'une racine de f c'est une extension totalement ramifiée de $\mathbb{Q}_q$ (Lemme 4.9). Notons par $I_{\mathfrak{Q}}$ le groupe d'inertie de $\mathfrak{Q}$ dans $N/\mathbb{Q}$. Introduisons le corps d'inertie L_0 dans $N_{\mathfrak{Q}}/\mathbb{Q}_q$. L'extension totalement ramifiée $K_{\mathfrak{q}}/\mathbb{Q}_q$ est linéairement disjointe de l'extension non ramifiée $L_0/\mathbb{Q}_q$, ce qui entraîne que le polynôme $f(X)$ reste irréductible sur L_0. Par conséquent, $I_{\mathfrak{Q}} = Gal(N_{\mathfrak{Q}}/L_0)$ agit transitivement sur les racines de $f(X)$. Comme le groupe d'inertie $I_{\mathfrak{Q}}$ est cyclique d'ordre p^n (Proposition 4.10), d'après [21, corollaire 1.2], et (Théorem 4.14) nous concluons que le groupe G est S_{p^n}.

□

Bibliographie

[1] S. S. Abhyankar, Galois theory on the line in nonzero characteristic, Bull. Amer. Math. Soc. **27**(**1**) (1992), 68--133.

[2] Y. AMICE,Les nombre p-adiques, PUF, 1ère Edition, 1975.

[3] J.Angelli, Trinômes irréductibles résolubles sur un corps de nombres, Acta Arith. **127** (2007), n ° 2, 169--178.

[4] M. D. Atkinson, Doubly transitive but not doubly primitive permutation group II, J. London Math. Soc. (**2**)**10** (1975), 53--60..

[5] B.Bensebaa, A. Movahhedi, and A. Salinier, The Galois group of $X^p + aX^s + a$, Acta Arith. **134**(**1**) (2008), 55--65.

[6] B. Bensebaa, A. Movahhedi, and A. Salinier, Wild ramification in trinomial extensions and Galois groups, Galsg. Math. J. **63** (2021), 106--120.

[7] Q. Cai and H. Zhang, A note on primitive permutation groups of prime power degree, J. of Discrete Math., (2015), 1--4.

[8] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, London and New York, 1967..

[9] S. D. Cohen, A. Movahhedi, and A. Salinier, Double transitivity of Galois groups of trinomials, Acta Arith. **82**(**1**) (1997), 1--15.

[10] S. D. Cohen, A. Movahhedi, and A. Salinier, Galois groups of trinomials, J. Algebra . **222**(**2**) (1999), 561--573.

[11] S. D. Cohen, A. Movahhedi, and A. Salinier, Factorization over local fields and the irreducibility of generalized difference polynomials, Mathematika. **47** (2000), 173--196.

[12] J. D. Dixon and B. Mortimer, Permutation Groups, Grad. Texts in Math. **163** Springer, 1996.

[13] W. Feit, Some consequences of the classification of finite simple groups, Proc. sympos. Pure Math. **37** (1980), 175-181.

[14] L. Gauckler, The Galois group of the Eisenstein polynomial X^5+aX+a, Arch. Math. **90** (2008), 136-139.

[15] F. Q. Gouvêa, p-adic Numbers An Introduction, 3rd Edition, Springer Nature Switzerland AG 2020.

[16] B. Huppert and N. Blackburn, "Finite Groups III", Springer-Verlag, New york, 1982.

[17] K. Komatsu, Discriminant of certain algebraic number felds, J. Reine Angew. Math. **285** (1976), 114--125.

[18] K. Komatsu, On the Galois group of $X^p+aX+a=0$, Tokyo J. Math. **14**(**1**) (1991), 227--229.

[19] K. Komatsu, On the Galois group of $X^p+p^tb(X+1)=0$, Tokyo J. Math. **15**(**2**) (1992), 351--356.

[20] T. Lalesco, Sur le groupe des èquations trinômes, Bull. Soc. Math. France., **tome35** (1907), 75--76.

[21] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, Proc. London Math. Soc. **87** (2003), 725--748.

[22] C. H. Li, Permutation groups with a cyclic regular subgroup and arc transitive circulants, J. Algebraic Combin., 21 (2005), 131–136.

[23] P. Llorente, E. Nart, and N. Vila, Discriminants of number fields defined by trinomials, Acta Arith. **43** (1984), 367--373.

[24] P. Llorente, E. Nart and N. Villa, Décomposition in number fields defined by trinomials, Acta Arith. XLIII (1991), 27--41.

[25] D. A. Marcus, Number Fields, 2nd edition, Springer International Publishing AG, 2018.

[26] P. Morandi, Field and Galois Theory, Springer-Verlag New York,1st edition 1996.

[27] L. J. Mordell, Diophantine equations, Academic Press, 1969.

[28] A. Movahhedi, Galois Group of X^p+ax+a, J. Algebra. **180**(**3**) (1996), 966--975.

[29] A. Movahhedi and A. Salinier, The primitivity of the Galois Group of a trinomial, J. Lond. Math. Soc. (2). **53**(**2**) (1996), 433--440.

[30] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, 3rd edition Springer-Verlag Berlin Heidelberg, 2004.

[31] O. Ore, Newtonsche Polygone in der Theorie der algebraischen K"orper, Math. Ann. **99** (1928), 84--117.

[32] H. Osada, The Galois group of the polynomials $x^n + ax^s + b$. II , Tôhoku Math. J. (2) . **39**(**3**) (1987), 437-445.

[33] .J. Rotman, Galois Theory, 2nd Edition, Springer-Verlag New York 1998.

[34] D. J. S. Robinson, A course in the theory of groups, GTM 80, SpringerVerlag, New York/Heidelberg Berlin, 1982.

[35] P. Samuel, Théorie algébrique des nombres, deuxième ed. Hermann, 1971.

[36] P. Samuel and O. Zariski, Commutative Algebra, **Volume I**, D. Van Nostrand / Springer, 1960.

[37] P. Samuel and O. Zariski, Commutative Algebra, **Volume II**,Springer-Verlag Berlin Heidelberg, 1960.

[38] E. S. Selmer, On the irreductibility of certain trinomials, Math. Scand. **4** (1956), 287-302.

[39] J. P. Serre, Corps locaux, troisième ed. Hermann, 1968.

[40] J. P. Serre, Topics in Galois theory, Jones and barlett Publishers, Boston, 1992.

[41] R. G. Swan, Factorization of polynomials over finite fields, pacific J. Math **12** (1962), 1099-1106.

[42] K. Uchida, Unramified extensions of quadratic number fields II, Tôhoku Math. J. (2) **22** (1970), 220-224.

[43] H. Wielandt, Finite Permutation Groups, Academic Press, 1964.