N$^0$ d'ordre :27/2014 – M/MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINIST□RE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE-ALGER
Faculté de Mathématiques

**MÉMOIRE**

Présenté pour l'obtention du diplôme de MAGISTER

**En: MATHÉMATIQUES**

Spécialité :Arithmétique, Codage et Combinatoire : Théorie des Nombres

Par : **RAFA Souad**

**Thème**

# Ramifications dans une extension de degré 8 de $\mathbb{Q}$

Soutenu publiquement le 15/07/2014. devant le jury composé de

| | | |
|---|---|---|
| Mme. BENFERHATLeila | Maître de Conférences /A à L'USTHB | Présidente |
| M. BENSEBAA Boualem | Maître de Conférences /A à L'USTHB | Directeur de mémoire |
| MmeSELMANESchehrazad | Maître de Conférences /A à L'USTHB | Examinatrice |
| M. BENCHERIF Farid | Professeur à l'USTHB | Examinateur |

***Remerciements***

En tout premiers lieu, je me dois de remercier tous ceux et celles qui m'ont aidé et soutenu.

Précisément, je tiens à remercier mon directeur de mémoire, Monsieur Boualem BENSEBA qui n'a pas cessé de m'aider et m'encourager dans cette oeuvre.

Mes remerciment vont aussi à l'endroit du Madame BENFERHAT Leila qui a accepté de présider le jury de ma soutenance.

Que Madame SELMANE Schehrazad et Monsieur BENCHRIF Farid, trouvent ici l'expression de ma reconnaissance pour avoir participé au jury de mémoire et pour leurs remarques pertient et leurs conceils qui m'ont permis d'enrichir mon travail et d'entrevoir de nouvelles perspectives.

Mes remerciment vont aussi à ma famille et surtout mes parents pour leur soutien tout au long de mes études, ainsi que mes frères Khadidja, Omar, Mohamed et Wiam.
Je remercie également la famille de mon mari pour leur compréhension et leur soutiens, surtout mon mari Rachid Abdoun .

Finalement j'exprime tout mon amité et ma sympathie à tous me camarades de l'étude surtout Aziza Hanani et aussi à mon ami Khadidja Naher.

# Table des matières

# Notations

| | | |
|---|---|---|
| $L, K, M, N$ | : | Corps de nombres. |
| $L/K$ | : | Extension de corps de nombres. |
| $[L : K]$ | : | Degré de l'extension $L/K$. |
| $Min\,(\alpha, K, X)$ ou $Irr\,(\alpha, K, X)$ | : | Le polynôme minimal de $\alpha$ sur $K$. |
| $Gal\,(L/K)$ | : | Groupe de Galois de $L$ sur $K$. |
| $Gal\,(P/K)$ | : | Groupe de Galois du polynôme $p$ sur $K$. |
| $\mathcal{O}_K$ | : | Anneau des entiers du corps $K$. |
| $S_n$ | : | Groupe de permutation de degré $n$. |
| $A_n$ | : | Le groupe alterné. |
| $N_{S_n}\,(G)$ | : | Le normalisateur de $G$ dans $S_n$. |
| $N_{L/K}\,(x)$ | : | Norme de $x$ de $L$ sur $K$. |
| $T_{L/K}\,(x)$ | : | Trace de $x$ de $L$ sur $K$. |
| $det\,(u)$ | : | Déterminant de l'endomorphisme $u$. |
| $P_u\,(X)$ | : | Polynôme caractéristique de l'endomorphisme $u$. |
| $d_K$ | : | Le discriminant du corps de nombres $K$. |
| $D\,(f)$ | : | Le discriminant du polynôme $f$. |
| $\wp, \mathfrak{p}, \mathfrak{P}...$ | : | Idéaux premiers. |
| $N_{L/K}\,(\mathfrak{p})$ | : | Norme sur $L/K$ de l'idéal $\mathfrak{p}$. |
| $\phi(n)$ | : | Fonction d'Euler. |
| $k_K = \frac{\mathcal{O}_K}{\mathfrak{p}}$ | : | Corps résiduel de l'idéal premier $\mathfrak{p}$. |
| $\lvert x\rvert_p$ | : | Valeur absolue $p$-adique de $x$. |

| | | |
|---|---|---|
| $v_p(x)$ | : | Valuation $p$-adique de $x$. |
| $v_{\mathfrak{p}(a)}$ | : | Valuation $\mathfrak{p}$-adique de $a$. |
| $e(\mathfrak{p})$ et $f(\mathfrak{p})$ | : | Indice de ramification et degré résiduel de l'idéal $\mathfrak{p}$. |
| $\mathbb{Q}_p$ | : | Corps des nombres $p$-adiques. |
| $\mathbb{Z}_p$ | : | Anneau des entiers de $\mathbb{Q}_p$. |
| $V$ | : | Anneau de valuation . |
| $\mathfrak{M}$ ou $m$ | : | idéaux maximaux. |
| $N_{n,p}$ | : | La valeur maximal possible de $v_p(d_K)$. |
| $\xi_K(s)$ | : | La fonction Zêta de Dedekind. |
| $GRH$ | : | Hypothèse de Riemann généralisée. |
| $r_1$ | : | Le nombre de places réels. |
| $r_2$ | : | Le nombre de places complexes. |
| $(r_1, r_2)$ | : | La signature du corps de nombres. |
| $T_1 ... T_{50}$ | : | Sous- groupes transitifs du groupe symétrique $S_8$ |
| | | Suivant les notations de Butler et Mc Kay. |

# Introduction

Le but de notre travail est de déterminer les différentes ramifications possibles des corps de nombres de degré 8 en un unique premier $p < 11$.

Le calcul du discriminant, la détermination de l'anneau des entiers $\mathcal{O}_K$ et la décomposition d'un nombre premier $p$ dans cet anneau sont des notions intimement liées en théorie algébrique des nombres .

Par la théorie de la ramification, le corps $K$ est ramifié en un premier $p$ si et seulement si $p$ divise $d_K$.

Dedekind montre que la valuation $p-$adique du discriminant $d_K$ du corps de nombres $K$, notée $v_p(d_K)$ depend de la relation

$$p\mathcal{O}_K = \sum_{\wp|p} \wp^{e_\mathfrak{p}}$$

et, de plus si le corps de nombres est modérement ramifié en $p$, alors on a

$$v_p(d_K) = \sum_{\wp|p} f_\wp (e_\wp - 1).$$

Ore [18] traite le cas général, c'est-à-dire le cas modérement ramifié et le cas sauvagement ramifié et donne la relation suivant :

Si $K$ est ramifié en $p$ on a

$$v_p(d_K) \leq \sum_{\wp|p} f_\wp (e_\wp + e_\wp v_p(e_\wp) - 1).$$

où la somme s'étend aux idéaux premiers $\wp$ de $\mathcal{O}_K$ au- dessus de $p$.

Ce mémoire se décline en 3 chapitres, les deux premiers donnent un aperçu des notions de théorie algébrique utiles pour l'étude de la ramification dans un corps de nombres, et

le troisième traite de la décomposition possibles d'un idéal $p\mathcal{O}_K$ au dessus d'un nombre premier $p < 11$ dans une extension de degré 8 de $\mathbb{Q}$.

Dans le premier chapitre, nous revisitons les notions de base de la théorie des extensions. et énoncer les résultats qui seront utilisés dans tout au long de ce mémoire. Ainsi, les deux premiers paragraphes sont consacrée aux rappels et autres résultats sur les extensions.

Dans les autres paragraphes, nous définirons les notions de discriminant $d_K$ d'un corps de nombres $K$ ainsi que la norme d'un idéal, ce qui nous permettra d'aborder la notion de ramification d'un nombre premier $p$ dans l'anneau $\mathcal{O}_K$ des entiers du corps de nombres $K$. Nous donnons quelques propriétés liées à la ramification.

Dans le deuxième chapitre, nous étudions les extensions $K_{\mathfrak{p}}/\mathbb{Q}_p$ de corps de nombres $p-$adique, où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ au- dessus de $p$, et nous verrons, dont l'étude de la ramification se trouve bien plus simplifié que celle dans le cadre global des corps de nombres. Enfin nous terminirons ce chapitre par la relation entre polygone de Newton et la ramification qui généralise les travaux de Dedekind dans le cas d'indice inessentiel et dont on étudiera un exemple qui illustrera l'importance de cet outil dans le cas de la ramification.

Dans le chapitre 3, on étudier les différents cas de ramifications possibles en utilisant la méthode de Ore.

Ainsi, dans le premier paragraphe notre étude va consister d'abord en la minoration de la valeur absolue du discriminant des corps de nombres de degré 8 en fonction de la signature, ce résultat représente l'un des outils principaux de l'étude de la ramification puis nous donnons la détermination des différentes ramifications possibles des corps octiques en un premier $p < 11$.

Ensuite nous verrons pour les cas possibles, les différentes décomposition de l'idéal $p\mathcal{O}_K$ ce qui nous permet de déterminer les valeurs possibles de discriminant $d_K$ du corps de nombres $K$ ramifié seulement en un premier $p < 11$.

Par abus de langage lorsque nous perlerons de la ramification dans la clôture galoisienne

$L$ en un premier $p$, il va s'agir de la ramification en un idéal $\mathfrak{P} \mid p$, on dira aussi que $L$ est ramifié en un unique premier $p$ si les idéaux premiers $\mathfrak{P}$ ramifiés dans $L$ sont ceux au-dessus de $p$.

# Chapitre 1

# Extensions de corps

## 1.1 Définitions et notations

**Définition 1.1** *Soit $L$ et $K$ deux corps commutatif on dit que $L$ est une extension de $K$ si et seulement si $K$est un sous corps de $L$, et on note : $L/K$ ou $K \subset L$.*

**Exemple :** voici quelques exemples d'extensions de corps.

1. Le corps des nombres complexes $\mathbb{C}$ est une extension du corps des nombres réels $\mathbb{R}$.
2. $E = \left\{a + b\sqrt{2}, avec\ a, b \in \mathbb{Q}\right\}$ muni des opérations + et $\times$, addition et multiplication, est une extension de $\mathbb{Q}$.
3. $\mathbb{C}$ et $\mathbb{R}$ sont des extensions de $\mathbb{Q}$.
4. Pour tout corps $K$, le corps $K(X)$ des fractions rationnelles à coefficients dans $K$ est une extension de $K$.

**Définition 1.2** *Si $L/K$ est une extension, on appelle degré de cette extension la dimension du $K-$espace vectoriel $L$, cette dimension est notée $[L : K] = dim_K L$.*
*Si $dim_K L$ est finie, on dit que $L/K$ est une extension finie, sinon l'extension $L/K$ est infinie.*

**définitions :**

1)Si $[L\ :\ K]=2$ on dit que l'extension $L/K$ est quadratique.

2) Si $[L\ :\ K]=3$ on dit que l'extension $L/K$ est cubique.

**Exemple :** nous donnons ici quelques exemples d'extensions de degrés divers.

1. $\mathbb{C}/\mathbb{R}$ est une extension quadratique.
2. L'ensemble $\{a+bj\ , a\ et\ b\in\mathbb{Q}\}$, où $j\neq 1$ et $j^3=1$, est une extension quadratique de $\mathbb{Q}$.
3. L'ensemble $\left\{a+b\alpha+c\alpha^2\ avec\ a,b,c\in\mathbb{Q}\ et\ \alpha=\sqrt[3]{3}\right\}$ est une extension cubique de $\mathbb{Q}$.
4. $\mathbb{R}$ et $\mathbb{C}$ sont des extensions infinie de $\mathbb{Q}$.
5. $\mathbb{R}(X)$ est une extension infinie de $\mathbb{R}$.

**Proposition 1.1** *soit $K\subset L\subset M$ une suite d'extensions. Alors $M/K$ est de degré fini si et seulement si les extensions $M/L$ et $L/K$ sont de degrés finis et dans ce cas on a :*

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

**Preuve :**

Supposons que $[M\ :\ K]<+\infty$ et comme $L$ est $K$-un sous-espace vectoriel de $M$, alors $[L\ :\ K]<\infty$. D'autre part, si $\{y_1,y_2,...,y_m\}$ est une base de $M$ sur $K$, alors les $y_i$ engendrent $M$ comme $L$-espace vectoriel et donc $[M\ :\ L]<[M\ :\ K]$. Réciproqueent, supposons que $dim_K L=n$ et $dim_L M=m$ et soient $B_1=\{x_1,x_2,...,x_n\}$ une base de $L$ sur $K$, et $B_2=\{y_1,y_2,...,y_m\}$ une base de $M$ sur $L$.

Soit $z\in M$ en peut ecrire $z$ et de manière unique sous la forme

$$z=\sum_{i=1}^{m}\alpha_i y_i,\ \alpha_i\in L,\ 1\leq i\leq m$$

d'autre part on a

$$\alpha_i=\sum_{j=1}^{n}\beta_{ij}x_j,\ \beta_{ij}\in K;\ 1\leq i\leq m\ et\ 1\leq j\leq n$$

Alors on obtient :

$$z = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} x_j y_i$$

avec : $B_1 B_2 = \{x_j, y_i\}$ $i = 1, ...m$ *et* $j = 1...n$ une base de $M$ sur $K$.

Le nombre d'éléments de la base de $M/K$ est $m \times n$ alors, $[M \ : \ K] = m \times n$, et donc $[M \ : \ K] = [M \ : \ L] \times [L \ : \ K]$

**Exemple :**

Soit $L = \left\{a + b\sqrt{5} \ avec \, a, b \in \mathbb{Q}\right\}$ et $M = \{u + vj \, avec \, u, v \in L \, et \, j \neq 1, j^3 = 1\}$

Alors $[L \ : \ \mathbb{Q}] = 2$ et $[M \ : \ L] = 2$ et donc $[M \ : \ \mathbb{Q}] = [M \ : \ L] \times [\mathbf{L} \ : \ \mathbb{Q}] = \mathbf{4}$

$M$ est un $\mathbb{Q}$-espace vectoriel de dimension 4 dont une base est $\left\{1, \sqrt{5}, j, j\sqrt{5}\right\}$.

la proposition précédente peut être généralisée à une tour de $n$ extensions

$K = K_1 \subset K_2 \subset ... \subset K_n$ et on a :

**Proposition 1.2** *Soit* $(K_i)$ *une famille d'extension telles que* $K_i \subset K_{i+1}$, $\forall i$, $1 \leq i \leq n-1$, *alors* $K_n/K_1$ *est finie si et seulement si ,* $\forall i$, $1 \leq i \leq n-1$ *l'extension* $K_{i+1}/K_i$ *est finie et dans ce cas on a*

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

## 1.2 Extension algébrique

**Définition 1.3** *Soit* $L/K$ *une extension de corps. Un élément* $\alpha$ *de* $L$ *est algébrique sur* $K$ *s'il existe un polynôme non nul* $P \in K[X]$ *tel que* $P(\alpha) = 0$.

**Définition 1.4** *Une extension* $L/K$ *est algébrique si tout élément de* $L$ *est algébrique sur* $K$ .

**Proposition 1.3** *Soit* $L/K$ *une extension de corps tel que* $L = K(\alpha)$ *ou* $\alpha \in L$ *est algébrique sur* $K$, *alors l'extension* $L$ *est algébrique sur* $K$. *Plus généralement,* $L = K(A)$ *ou* $A = \{\alpha, \ \alpha \ \ algébrique \ surK\}$

**Preuve :**

On va montrer que $\forall x \in L$, $x$ est algébrique sur $K$. 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 $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Soit $x \in L$, alors la famille $\{1, x, x^2, \ldots, x^n\}$ est liée et $\exists \lambda_i \in K, 0 \leq i \leq n$ , non tous nuls tels que :

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n = 0$$

ce qui montre que $x$ est un zéro du polynôme $P(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \neq 0$ et entraine que $x$ est algébrique sur $K$ . Par conséquent tout élément de $L$ est algébrique sur $K$ et donc $L$ est algébrique sur $K$ .

**Proposition 1.4** *Toute extension finie est algébrique.*

**Preuve :** Soient $L/K$ une extension finie et $\alpha \in L$ ; puisque $dim_K(K(\alpha)) \leq dim_K(L)$, il existe un entier $n$ tel que $1, \alpha, \ldots, \alpha^n$ soient linèarement dépendants . Il existe donc des éléments $a_0, a_1, \ldots, a_n$ de $K$ tels que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Autrement dit il existe un polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$.

**Théorème 1.1** *Soit $L/K$ une extension et $\alpha \in L$ un élément algébrique sur $K$.*

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

**Preuve :**

1. considérons le morphisme d'anneau

$$\begin{array}{rcl} \varphi : K[X] & \longrightarrow & K(\alpha) \\ X & \longmapsto & \varphi(X) = \alpha \end{array}$$

on a : $Im(\varphi) \simeq {}^{K[X]}/_{ker(\varphi)}$

puisque l'anneau $K[X]$ est principal, l'idéal $ker(\varphi)$ est engendré par un polynôme $P(X)$. Puisque $Im(\varphi)$ est contenu dans $L$, qui est un anneau intègre, par conséquent l'idéal $(P(X))$ est premier, Il est donc engendré par un polynôme irréductible, qui est unique si on le suppose unitaire. Soit $M_\alpha(X)$ ce polynôme. puisque $M_\alpha(X)$ est irréductible et $K[X]$ est principal, l'idéal $ker(\varphi)$ est maximal, donc $Im(\varphi)$ est un corps contenant $K$ et $\alpha$, $Im(\varphi) = K(\alpha)$ . On a

$$\dim({}^{K[X]}/_{(M_\alpha(X))}) = deg(M_\alpha(X))$$

et l'isomorphisme

$${}^{K[X]}/_{(M_\alpha(X))} \to K(\alpha)$$

envoie la base $1, \overline{X}, \ldots, \overline{X}^{n-1}$ de ${}^{K[X]}/_{(M_\alpha(X))}$ sur $1, \alpha, \ldots, \alpha^{\mathbf{n-1}}$.

2. Si $F(X) \in K[X]$ avec $f(\alpha) = 0$, alors $f(X) \in (M_\alpha(X))$ ceci implique que $f(X)$ est divisible par $M_\alpha(X)$.

**Définition 1.5** *Avec les notations ci-dessus, le polynôme $M_\alpha(X)$ est appelé le polynôme minimale de $\alpha$ sur $K$, on le note $Min(\alpha, K, X)$.*
*L'entier* $\deg(M_\alpha(X)) = [K(\alpha) : K]$ *est appelé le degré de $\alpha$ sur $K$.*

**Exemples :** on a les exemples suivants :

1. $X^2 - 5 \in \mathbb{Q}[X]$, $\sqrt{5}$ est une racine de $X^2 - 5$ donc $\sqrt{5}$ est algébrique sur $\mathbb{Q}$, d'autre part $X^2 - 5$ est irréductible sur $\mathbb{Q}$ car $\sqrt{5} \notin \mathbb{Q}$ et $-\sqrt{5} \notin \mathbb{Q}$, alors $Min(\sqrt{5}, \mathbb{Q}, X) = X^2 - 5$ et $\sqrt{5}$ est de degré 2 sur $\mathbb{Q}$.
2. Soit $P(X) = X^2 + X + 1 \in \mathbb{R}[X]$, de racines $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ et $\beta = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ .
comme $\alpha$ et $\beta \notin \mathbb{R}$, alors $X^2 + X + 1$ est irréductible sur $\mathbb{R}$ et donc
$Min(\alpha, \mathbb{R}, X) = X^2 + X + 1$ et $\alpha$ de degré 2 sur $\mathbb{R}$.

3. Soit $\alpha$ une racine de $X^3 + X + 1 \in \mathbb{Q}[\mathbf{X}]$, alors $\alpha$ est algébrique sur $\mathbb{Q}$.

   On suppose qu'il existe deux entiers $u \in \mathbb{Z}$ et $v \in \mathbb{N}^\star$ tels que

   $$(\frac{u}{v})^3 + \frac{u}{v} + 1 = 0$$

   Alors $\frac{u}{v} \in \{-1, 1\}$. Or, les nombres $-1$ et $1$ ne sont pas racines du polynôme $X^3 + X + 1$, ce qui montre que ce polynôme est irréductible sur $\mathbb{Q}$, et par suite $Min(\alpha, \mathbb{Q}, X) = X^3 + X + 1$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

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

**Lemme 1.1** *Soit un polynôme $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ , et $p$ un nombre premier vérifiant les conditions suivantes*

*i)* $p/a_i, 0 \leq i \leq n-1$.

*ii) $p$ ne divise pas $a_n$.*

*iii)* $p^2$ *ne divise pas* $a_0$.

*alors $P(X)$ est irréductible sur $\mathbb{Q}$.*

*On dit alors que le polynôme $P(X)$ est d'Eisenstein en $p$.*

**Exemples :** considérons les deux exemples suivants :

1. Soit $P(X) = X^3 + 6X^2 - 8X + 10$ un polynôme. On remarque que $P(X)$ est d'Eisenstein en $p = 2$, il est donc irréductible.

2. Soit $P(X) = X^5 + 10X + 9$, on ne peut pas appliquer le critère d'Eisenstein pour ce polynôme, mais le polynôme

   $$Q(X) = P(X + 1) = X^5 + 5X^4 + 10X^3 + 10X^2 + 15X + 10$$

   est d'Eisenstein en $p = 5$, alors $P$ est irréductible.

**Définition 1.6** *Soit $K$ un corps, toute extension algébrique $L/K$ telle que tout polynôme $P \in L[X]$ de degré deg $P \geq 1$, admet au moins une racine dans $L$ est appelé clôture algébrique de $K$.*

## 1.3 Extensions séparables-Extensions normales

### 1.3.1 Extensions séparables

**Définition 1.7** *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 $K$.*

**Exemples :** On a les deux exemples suivants :

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

Les polynômes séparables sont caractérisés par

**Proposition 1.5** *Soit $K$ un corps et $f \in K[X]$ un polynôme .*
*$f$ est séparable sur $K$ si, et seulement si $f(X)$ et sa dérivée formelle $f'(X)$ sont premiers entre eux.*

**Preuve :** Soit $f \in K[X]$ un polynôme séparable de degré $n$, alors $f$ possède $n$ racines distinctes dans une certaine extension $L$ de $K$, ce qui entraine qu'aucune de ces racines n'annulle $f'$.
Réciproquement, supposons que $f$ n'est pas séparable, ce qui implique qu'il existe $\alpha \in L$ et un entier $k \geq 2$ tels que $f(X) = (X-\alpha)^k g(X)$, $g \in K[X]$. Ce qui montre que $\alpha$ est racine de $f'$.

**Corollaire 1.1** *Soit $K$ un corps et $f(X) \in K[X]$ un polynôme irréductible de degré $\deg f \geq 1$. $f$ est séparable sur $K$ si, et seulement si $f'$ est non nul*

**Preuve :** Si $f$ est séparable sur $K$, par la proposition 1.5 on tire que $f'$ est non nul.
Inversement, Si $f$ est un polynôme irréductible non séparable, alors $f$ et $f'$ ont un zéro

commun , d'après la proposition 1.5. Soit $\alpha$ ce zéro, alors $f$ est son polynôme minimal, puisqu'il est irréductible, et ceci entraîne que $f \mid f'$ ce qui montre que $f = 0$, puisque $\deg f > \deg f'$.

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

**Corollaire 1.2** *Soit $K$ un corps, de caractéristique $0$ et $f(X) \in K[X]$ un polynôme irréductible de degré $\deg f \geq 1$, alors $f$ est séparable sur $K$.*

**Preuve :** La condition $f' = 0$ implique que $f$ est constant.

**Exemple :**

1. Soit le polynôme $X^4 + 4X + 2 \in \mathbb{Q}[X]$

   par le critère d'Eisenstein en $p = 2$ , le polynôme ci-dessus est irréductible, alors il est séparable sur $\mathbb{Q}$.

2. Soit $K = \mathbb{F}_p[T^p]$ et considérons $f = X^p - T^p \in K$. ALors $f$ se décompose dans $L = \mathbb{F}_p[T]$, $K \subset L$, sous la forme : $f = (X - T)^p$. Comme $T^i \notin K$, alors $f$ est irréductible sur $K$ mais il est inséparable sur $K$.

**Corollaire 1.3** *Soit $K$ un corps de caractéristique $p$, $p$ premier, et soit $f(X) \in K[X]$ un polynôme irréductible de degré $\deg f \geq 1$.*

*Alors $f$ est inséparable sur $K$ si et seulement si $\exists g \in K[X]$ tel que $f(X) = g(X^p)$.*

**Preuve :** Soit $f = \sum_{i=0}^{n} a_i X^{n-i}$ un polynôme irréductible de degré $n$ sur $K$, alors $f' = \sum_{i=0}^{n-1} (n-i) a_i X^{n-1-i}$. La condition $f' = 0$ implique $(n-i)a_i = 0$, ce qui montre que $p \mid (n-i)$ dès que $a_i \neq 0$ et donc $f$ est un polynôme en $X^p$.

Réciproquement, si $f = g(X^p)$, alors $f$ est inséparable étant donné que $f'$ est nul

**Définition 1.8** *Soit $L/K$ une extension et $\alpha \in L$ un élément algébrique sur $K$.*

*On dit que $\alpha$ est séparable sur $K$ si son polynôme minimal $Irr(\alpha, K, X)$ est séparable sur $K$.*

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

**Définition 1.9** *une extension algébrique $L/K$ est dite séparable si tous les éléments de $L$ sont séparables sur $K$.*

**Théorème 1.2** *(théorème de l'élément primitif) Soit $K$ un corps infini et $L$ une extension de $K$ de degré fini. Si $L$ est séparable sur $K$ , alors il existe $\alpha \in L$ tel que $L = K(\alpha)$. dans ce cas $\alpha$ est appelé élément primitif de $L$.*

**Proposition 1.6** *Soit $K \subset L \subset M$ une tour d'extensions de corps de degrés finis. Alors $M$ est séparable si et seulement si $M$ est séparable sur $L$ et $L$ est séparable sur $K$.*

Soit $K \subset L$ une extension de corps .

### 1.3.2 Extension normale

**Définition 1.10** *On dit qu'une extension $L/K$ de degré fini est normale sur $K$ si et seulement si le polynôme minimal $irr(\alpha, K, X)$ a toutes ses racines dans $L$.*

**Exemples :**

1. $\mathbb{Q}(i)/\mathbb{Q}$ est une extension de degré 2, normale sur $\mathbb{Q}$ puisque $\alpha = i$ a pour polynôme minimal $X^2 + 1$ dont les racines sont dans $\mathbb{Q}(i)$.
2. Soit $\alpha = \sqrt[3]{2}$ un zéro du polynôme $X^3 - 2$, qui est irréductible sur $\mathbb{Q}$, alors $F = \mathbb{Q}(\alpha, j)$ est le corps des racines, c'est donc une extension normale de $\mathbb{Q}$. Par contre, $\mathbb{Q}(\alpha)$ qui ne contient que le racine $\alpha$ n'est pas une extension normale de $\mathbb{Q}$.

**Définition 1.11** *Une extension $L/K$ est dite galoisienne si elle est algébrique, normale et séparable.*

**Remarque :** Une extension algébrique $L/K$ est galoisienne si et seulement si pour tout $\alpha \in L$, le polynôme minimal $Irr(\alpha, K, X)$ de $\alpha$ sur $K$ a toutes ses racines simples et contenues dans $L$.

**Exemples :**

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

**Définition 1.12** *Soit $L/K$ une extension galoisienne. L'ensemble de $K-$automorphisme de $L$ est un groupe, appelé groupe de Galois de l'extension galoisienne $L/K$, qu'on note $Gal(L/K)$.*

**Proposition 1.7** *Si $L/K$ est une extension galoisienne de degré $n$, alors le groupe de Galois $Gal(L/K)$ est d 'ordre $n$.*

## 1.4 Corps de nombres

### 1.4.1 Définitions

**Définition 1.13** *On appelle corps de nombres algébriques ( ou corps de nombres ) toute extension de degré fini (et donc algébrique ) de $\mathbb{Q}$.*

- *Un corps de nombres de degré 2 s'appelle corps quadratique.*
- *Un corps de nombres de degré 3 s'appelle corps cubique.*

**Exemple :** Les coprs $\mathbb{Q}\left(\sqrt{2}\right)$ et $\mathbb{Q}\left(exp\left(2i\pi/13\right)\right)$ sont des coprs de nombres de degré respectifs 2 et 12.

**Proposition 1.8** *Tout extension finie d'un corps de nombres est un corps de nombres .*

### 1.4.2 Norme, trace et discriminant

#### Norme et trace d'un élément

Soit $L/K$ une extension finie de corps de nombres.

Soit $\alpha \in L$, on considère l'application :

$$\begin{array}{rccc} \mu_\alpha : & L & \longrightarrow & L \\ & x & \longmapsto & \alpha x \end{array}$$

$\mu_\alpha$ est une application linéaire.

**Définition 1.14** *On appelle norme de $\alpha$ le déterminant de la matrice associée à $\mu_\alpha$*

$$N_{L/K}(\alpha) = det(\mu_\alpha)$$

**Exemple :** Soit $K = \mathbb{Q}$ , $L = \mathbb{Q}\left(\sqrt{5}\right)$, alors $\{1, \sqrt{5}\}$ est une base de $L$ sur $K$

Pour $\alpha = 1$ on a :

$$\begin{array}{rccc} \mu_1 : L & \longrightarrow & L \\ x & \longmapsto & x \end{array}$$

$\mu_1(1) = 1.1 + 0.\sqrt{5}$ et $\mu_1(\sqrt{5}) = 0.1 + 1.\sqrt{5}$

La matrice associée est $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $det(A) = 1$

Alors $N(1) = 1$.

**Définition 1.15** *On appelle trace de $\alpha$, la trace de la matrice associée à $\mu_\alpha$ et on note :*

$$tr_{L/K}(\alpha) = tr_{L/K}(\mu_\alpha)$$

**Définition 1.16** *On appelle polynôme caractéristique de $\alpha$ le polynôme*

$det(X.id - \mu_\alpha) \in K[\alpha]$

**Définition 1.17** *Soient $L_1$et $L_2$ deux corps de nombres, on appelle plongement de $L_1$ dans $L_2$ tout homomorphisme $\sigma : L_1 \longrightarrow L_2$.verifiant :*

1. $\sigma(a.b) = \sigma(a).\sigma(b)$.
2. $\sigma(a + b) = \sigma(a) + \sigma(b)$.
3. $\sigma(1) = 1$.

*4.* $\sigma(0) = 1$.

**Proposition 1.9** *Soit $L/K$ une extension de corps de nombres et soit $\sigma_1, \sigma_2, \ldots, \sigma_n$ les plongements distincts de $L$ dans $\bar{\mathbb{Q}}$ .*

*$\forall \sigma \in L$ on a :*

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \text{ et } tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

.

*Les $\sigma_i(\alpha)$ s'appellent les conjugué de $\alpha$ dans $\bar{\mathbb{Q}}$ . De plus on a :*

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta) \text{ et } tr_{L/K}(\alpha+\beta) = tr_{L/K}(\alpha) + tr_{L/K}(\beta).$$

**Exemples :** Soit $K = \mathbb{Q}(\sqrt{13})$ et $\alpha = 1 + \sqrt{13}$ et $\beta = \frac{3+\sqrt{13}}{2}$

On a deux plongement : $\sigma_1 : \sqrt{13} \longrightarrow \sqrt{13}$ et $\sigma_2 : \sqrt{13} \longrightarrow -\sqrt{13}$

on alors : $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (1+\sqrt{13})(1-\sqrt{13}) = -12$.

$N(\beta) = \sigma_1(\beta)\sigma_2(\beta) = \left(\frac{3+\sqrt{13}}{2}\right)\left(\frac{3-\sqrt{13}}{2}\right) = -1$.

$tr(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (1+\sqrt{13}) + (1-\sqrt{13}) = 2$.

$tr(\beta) = \sigma_1(\beta) + \sigma_2(\beta) = \left(\frac{3+\sqrt{13}}{2}\right) + \left(\frac{3-\sqrt{13}}{2}\right) = 3$.

$N(\alpha\beta) = N\left(\left(1+\sqrt{13}\right)\left(\frac{3+\sqrt{13}}{2}\right)\right) = N\left(8+2\sqrt{13}\right) = 8^2 - 4 \times 13 = 12$ , d'autre part $N(\alpha)N(\beta) = (-12)(-1) = 12$.

Alors $N(\alpha\beta) = N(\alpha)N(\beta)$.

et $tr(\alpha+\beta) = tr\left(\left(1+\sqrt{13}\right) + \left(\frac{3+\sqrt{13}}{2}\right)\right) = tr\left(\frac{5+3\sqrt{13}}{2}\right) = 5$, d'autre part : $tr(\alpha)+tr\beta) = 2+3 = 5$.

Alors $tr(\alpha+\beta) = tr(\alpha) + tr(\beta)$.

**Corollaire 1.4** *Si $\alpha$ est entier algébrique, alors $tr_{L/K}(\alpha)$ et $N_{L/K}(\alpha)$ sont des entiers.*

**Définition 1.18** *Soit $L$ une extension finie d'un corps $K$, et $x \in L$. Alors on définit la norme de $x$ de $L$ sur $K$, $N_{L/K}(x)$ comme le déterminant de l'endomorphisme du $K-$ espace vectoriel $L$ donné par $y \longmapsto xy$ .*

*Si $P(X) = X^d + \cdots + a_0$ est le polynôme minimal unitaire de $x$ sur $K$, alors*

$$N_{L/K}(x) = \left[(-1)^d a_0\right]^{\frac{[L:K]}{d}}$$

### 1.4.3 Discriminant d'un corps de nombres

**Définition 1.19** *Soient $B$ un anneau et $A$ un sous- anneau de $B$ tel que $B$ soit un $A-$module libre de rang fini $n$. Pour $(x_1, ..., x_n) \in B^n$, on appelle discriminant du système $(x_1, ..., x_n)$ l'élément de $A$ défini par*

$$D(x_1, ..., x_n) = det(Tr_{B/A}(x_i x_j))$$

**Proposition 1.10** *Si $(y_1, ..., y_n) \in B^n$ est un autre système d'élément de $B$ tel que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ avec $a_{ij} \in A$, on a*

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

**Proposition 1.11** *Soit $K = \mathbb{Q}(\alpha)$ un corps de nombres avec $[K : \mathbb{Q}] = n$.*
*Si $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ une $\mathbb{Q}-$base de $K$, et $\sigma_j \, (1 \leq j \leq n)$ plongements distincts.*
*Le discriminant de $B$ est donné par :*

$$D(B) = det\left(\sigma_j(\alpha_i)\right)^2$$

$$D(\alpha_1, \alpha_2, \ldots, \alpha_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & . & . & .\sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & . & .. & \sigma_2(\alpha_n) \\ . & . & . & . & . \\ . & . & . & . & . \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & .. & . & \sigma_n(\alpha_n) \end{vmatrix}^2$$

**Lemme 1.2** *Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ un corps de nombres de degré $n$, et soit $P_\theta$ le polynôme minimal de $\theta$. Alors*

$$D\left(1, \theta, \theta^2, \ldots, \theta^{n-1}\right) = (-1)^{\frac{n(n-1)}{2}} N\left(P'_\theta(\theta)\right)$$

*( où $P'_\theta(\theta)$ désigne le polynôme dérivé de $P_\theta(\theta)$)*

**Définition 1.20** *(discriminant d'un polynôme)*

*Soient* $f(X) = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{C}[X]$

*tel que* $n \in \mathbb{N}$, *et* $a_n \neq 0$, *et* $x_1, ..., x_n \in \mathbb{C}$ *les racine de* $f(X)$.

*On défini le discriminant de* $f(X)$ *par*

$$D(f(X)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{C}$$

**Théorème 1.3** *Soient* $K$ *un corps de nombre algébrique de degré fini* $n$, *et* $\alpha \in K$, *donc*

$$D(\alpha) = D(Min(\alpha, K, X))$$

*où* $Min(\alpha, K, X)$ *désigne le polynôme minimal de* $\alpha$ *sur* $K$.

**Preuve :**(cf.[1]).

**Exemple :** Soient $K = \mathbb{Q}(\sqrt[3]{2})$, et $\alpha = \sqrt[3]{2}$, les conjugués de $\alpha$ sont $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = j\sqrt[3]{2}$ et $\alpha_3 = j^2\sqrt[3]{2}$, où $j = \frac{-1+i\sqrt{3}}{2}$.

alors

$$\begin{aligned} \alpha_1 - \alpha_2 &= (1-j)\sqrt[3]{2} \\ \alpha_2 - \alpha_3 &= j(1-j)\sqrt[3]{2} \\ \alpha_3 - \alpha_1 &= j^2(1-j)\sqrt[3]{2} \end{aligned}$$

Donc

$$(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) = (1-j)^3 2.$$

d'autre part ; on a

$$(1-j)^3 = 1 - 3j + 3j^2 - j^3 = -3(j - j^2)$$

Donc :

$$(1-j)^6 = 3^2(j-j^2)^2 = 3^2(j^2 + j - 2) = -3^3.$$

Alors on obtient

$$D(\alpha) = ((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1))^2 = (1-j)^6 2^2 = -2^2.3^3.$$

**Théorème 1.4** *( Stickelberger)*

*Soient $K$ un corps de nombres de degré $n$, $d_K$ son discriminant. Alors on a :*

$$d_K \equiv 0 \, ou \, 1 \ (mod \, 4)$$

**Preuve :**(cf.[14]).

**Théorème 1.5** *Soit $K$un corps de nombres avec $[K : \mathbb{Q}] = n$.*

- *Si $\omega_1, \omega_2, \ldots, \omega_n \in K$ , alors $dis(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{Q}$.*
- *Si $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$, alors $dis(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{Z}$.*
- *Si $dis(\omega_1, \omega_2, \ldots, \omega_n) \neq 0 \Longleftrightarrow \{\omega_1, \omega_2, \ldots, \omega_n\}$ est une $\mathbb{Q}-$base de $K$.*

**Preuve :** (cf.[1])

## 1.5 Anneau d'entiers de corps de nombres

### 1.5.1 Anneaux noethériens

**Théorème 1.6** *Soient $A$ un anneau, et $M$ un $A-$module, les conditions suivantes sont équivalentes.*

*a) Toute famille non vide de sous-modules de $M$ possède un élément maximal.*

*b) Toute suite croissante de sous-modules de $M$ est stationnaire.*

*c) Tout sous-module de $M$ est de type fini.*

**Définition 1.21** *Un $A$ module $M$ est dit noethérien s'il satisfait aux conditions équivalentes du théorème précédente.*

*Un anneau $A$ est dit noethérien si, considère comme $A-$module c'est un module noethérien.*

### 1.5.2 Anneaux de Dedekind

**Définition 1.22** *Un anneau $A$ est appelé un anneau de Dedekind s'il est :*

1. *Noethérien.*
2. *Intégralement clos (donc intègre).*
3. *Tout idéal premier non nul de $A$ est maximal.*

**Exemple :**

1. L'anneau $\mathbb{Z}$ est un anneau de Dedekind .
2. Si $K$ est un corps, l'anneau $K[X]$ est un anneau de Dedekind.
3. Tout anneau principal est un anneau de Dedekind.
4. L'anneau des entiers d'un corps de nombres est un anneau de Dedekind d'après le théorème suivant :

**Théorème 1.7** *Soient $A$ un anneau de Dedekind, $K$ son corps des fractions, $L$ une extension de degré fini de $K$ et $A'$ la fermeture intégrale de $A$ dans $L$.*
*On suppose $K$ de caractéridtique $0$. Alors $A'$ est un anneau de Dedekind et un $A-$module de type fini.*

**Preuve :**(cf.[15])

### 1.5.3 Anneau d'entiers de corps de nombres

**Théorème 1.8** *(éléments entiers sur un anneau)*

*Soit $R$ un anneau, $A$ un sous-anneau de $R$, et $x$ un élément de $R$.*

*Les propriétés suivantes sont équivalentes :*

*a) Il existe $a_0, a_1, \ldots, a_{n-1} \in A$ tels que*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1.1}$$

*(autrement dit $x$ est un racine d'un polynôme unitaire sur $A$).*

*b) L'anneau $A[x]$ est un $A-$module de type fini .*

*c) Il existe un sous-anneau $B$ de $R$ contenant $A$ et $x$, et qui est un $A-$module de type fini.*

**Pruve :**(cf. [15]).

**Définition 1.23** *Soient $R$ un anneau et $A$ un sous-anneau de $R$, un élément $x$ de $R$ est dit entier sur $A$ s'il satisfait aux conditions équivalentes $a), b), c)$ du théorème* 1.8.
*Soit $P \in A[x]$ un polynôme unitaire tel que $P(x) = 0$ , la relation $P(x) = 0$ est appellée une équation de dépendance intégrale de $x$ sur $A$.*

**Exemple :** L'élément $x = \sqrt{2}$ de $\mathbb{R}$ est entier sur $\mathbb{Z}$, une équation de dépendance intégrale est donnée par $x^2 - 2 = 0$.

**Définition 1.24** *Soit $K$ un corps de nombres, les éléments de $K$ qui sont entiers sur $\mathbb{Z}$ sont les entiers de $K$, ils forment l'anneau des entiers de $K$ qu'on note $\mathcal{O}_K$ .*

**Théorème 1.9** *soit $K$ un corps de nombres de degé $n$ 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 $n$.*

**Proposition 1.12** *On a les résultats suivants :*

1. *Le corps des fractions de $\mathcal{O}_K$ est $K$.*
2. *L'anneau $\mathcal{O}_K$est noethérien et intégralemant clos.*
3. *Le $\mathbb{Z}-$module $\mathcal{O}_K$ est libre de rang $[K : \mathbb{Q}]$.*

**Définition 1.25** *Soient $L/K$ une extension fini de corps de nombres, et $\mathcal{O}_K$ l'anneau des entiers de $K$. Toute base de $\mathbb{Z}-$ module $\mathcal{O}_K$ est une base de $K$ sur $\mathbb{Q}$, une telle base est appelée base intégrale.*

**Définition 1.26** *Toutes les bases intégrales ont même discriminant, on appelera ce discriminant le discriminant de $K$ qu'on notera $D(K)$ ou $d_K$.*

**Proposition 1.13** *Soit $K = \mathbb{Q}(\sqrt{d})$ un corps de nombres quadratique d'anneau d'entier $\mathcal{O}_K$ donné par :*

$$\begin{cases} \mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right] \text{ si } d \equiv 2 ou\ 3\,(mod\ 4) \\ \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \text{ si } d \equiv 1\,(mod\ 4) \end{cases}$$

*Alors $d_K = 4d$ si $d \equiv 2 ou 3\,(mod 4)$ et $d_K = d$ si $d \equiv 1\,(mod 4)$*

**Preuve :** • Si $d \equiv 2\text{ou } 3\,(\text{mod } 4)$ on a :

$$d_K = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$

• Si $d \equiv 1\,(\text{mod } 4)$ on a :

$$d_K = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d$$

**Exemples :**

1. Soit $K = \mathbb{Q}\left(\sqrt{2}\right)$ alors $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{2}\right]$ et $B = \left\{1, \sqrt{2}\right\}$ une base de $\mathcal{O}_K$
   et $\sigma_1 : \sqrt{2} \longrightarrow \sqrt{2}$ ,$\sigma_2 : \sqrt{2} \longrightarrow -\sqrt{2}$ .
   Alors : $D(B) = det\left(\sigma_j(\alpha_i)\right)^2 = det \begin{pmatrix} \sigma_1(1) & \sigma_1\left(\sqrt{2}\right) \\ \sigma_2(1) & \sigma_2\left(\sqrt{2}\right) \end{pmatrix}^2 = det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2$
   $= \left(-2\sqrt{2}\right)^2 = 8.$

2. Soit $K = \mathbb{Q}(\xi)$, $\xi = \exp\left(\frac{2i\pi}{p}\right)$ , $p$ premier, un corps cyclotomique.
   On sait que $\mathcal{O}_K = \mathbb{Z}[\xi]$ , donc $\{1, \xi, \xi^2, \ldots, \xi^{p-2}\}$ est une base de $K$ sur $\mathbb{Z}$, et que le polyôme minimal $P_\xi(x)$ de $\xi$ sur $\mathbb{Q}$ satisfait à $(X-1)P_\xi(x) = X^p - 1$. On va calculer le discriminant en utilisant la formule $D(1, \xi, ..., \xi^{p-2}) = N(P_\xi(x))$.
   Par dérivation de $(X-1)P_\xi(x) = X^p - 1$, on obtient $(X-1)P'_\xi(x) = p\xi^{p-1}$ ( car $P_\xi(\xi) = 0$). Or $N(p) = p^{p-1}$, $N(\xi) = \pm 1$, $N(\xi - 1) = p$. On a donc

   $$D(1, \xi, ..., \xi^{p-2}) = \pm p^{p-2}$$

3. Si $K = \mathbb{Q}\left(\sqrt{2}\right)$, alors $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{2}\right]$ , donc $B = \left\{1, \sqrt{2}\right\}$ est une base intégrale de $K$.

4. Les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ , avec $j = \exp(2i\pi/3)$ sont respectivement les anneaux d'entiers de $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$.

5. Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, avec $d \in \mathbb{Z}$ sans facteurs carrés.On a alors :
   •Si $d \equiv 2$ ou $d \equiv 3\, mod 4$. L'anneau $O_K$ des entiers de $K$ est l'ensemble des $a + b\sqrt{d}$, avec $a, b \in \mathbb{Z}$, dont une base est $\{1, \sqrt{d}\}$.
   •Si $d \equiv 1\, mod 4$. L'anneau $O_K$ des entiers de $K$ est l'ensemble des $\frac{1}{2}(a + b\sqrt{d})$, avec $a, b \in \mathbb{Z}$, dont une base est $\{1, \frac{1+\sqrt{d}}{2}\}$

6. Pour tout nombre premier $p$, le $p-$ème corps cyclotomique $K = \mathbb{Q}(\zeta_p)$, où $\zeta_p$ est une racine primitive $p-$ème de l'unité, est de degré $p - 1$.
   L'anneau des entiers de $K$ est $O_K = \mathbb{Z}[\zeta_p]$, dont une base est $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$.

## 1.6 Idéaux dans un corps de nombres

### 1.6.1 Idéaux dans un anneau de Dedekind

Dans ce paragraphe, on désigne par $A$ un anneau de Dedekind de caractéristique 0, par $K$ son corps des fractions, par $L$ une extension de degré fini $n$ de $K$ , et par $B$ la fermeture intégrale de $A$ dans $L$, on rappelle que $B$ est un anneau de Dedekind .
Si $A = \mathbb{Z}$ et $K = \mathbb{Q}$. $L$ est un corps de nombres et $B$ l'anneau des entiers de $L$.

$$\begin{array}{cc} B & L \\ | & |n \\ A & K \end{array}$$

**Définitions et notations**

**Définition 1.27** *un idéal $P$ d'un anneau $A$ est dit premier s'il satisfait les conditions suivantes :*

1. $P \neq A$ .
2. *Si* $xy \in P \Longrightarrow x \in P$ *ou* $y \in P$ *pour* $x, y \in A$.

Il revient au même de dire que l'anneau quotient $^{A}/_{P}$ est intègre.

**Définition 1.28** *Soient $A$ un anneau intègre. $K$ son corps des fractions. On appelle idéal fractionnaire de $A$ ( ou de $K$ par rapport à $A$)tout sous $A-$module $I$ non nul de $K$ tel qu'il existe $d \in A$, $d \neq 0$ satisfaisant à $I \subset d^{-1}A$, ceci revient à dire que les éléments de $I$ ont un ( dénominateur commun) $d \in A$.*
*Dans le cas d'un corps de nombres $K$, un idéal entier de $K$ est un idéal de l'anneau des entiers $\mathcal{O}_K$ de $K$, c'est dire un idéal fractionnaire de $\mathcal{O}_K$ contenu dans $\mathcal{O}_K$.*

**Norme d'un idéal**

**Définition 1.29** *Soit $I$ un idéal premier de $B$.*

$$\begin{array}{ccc} I \subset B & \longrightarrow & K \\ | & & \\ p \subset \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

On défini le norme de $I$ par $N(I) = |^{B}/_{I}|$, le nombre de classe modulo $I$.

**Théorème 1.10** *si $I$ et $J$ deux idéaux premiers de $B$, alors $N(I.J) = N(I).N(J)$.*

**Preuve :**
Supposons d'abord que $I$ et $J$ sont premiers entre eux . Par le théorème chinois des restes nous aurons :

$$\mathcal{O}_K/_{I.J} \cong \mathcal{O}_K/_{I} \oplus \mathcal{O}_K/_{J}$$

Donc $|\mathcal{O}_K/_{I.J}| = |\mathcal{O}_K/_{I}| \,.\, |\mathcal{O}_K/_{J}|$.
Il reste à montrer que $N\left(\mathfrak{p}^k\right) = \left(N\left(\mathfrak{p}\right)\right)^k$pour tout entier $k \geq 1$ et $\mathfrak{p}$ un idéal premier .
Notons que le thérème d'isomorphisme nous permet d'écrire

$$N\left(\mathfrak{p}^{k-1}\right) = |\mathcal{O}_K/_{\mathfrak{p}^{k-1}}| = \left|\frac{\mathcal{O}_K/_{\mathfrak{p}^k}}{\mathfrak{p}^{k-1}/_{\mathfrak{p}^k}}\right| = \frac{|\mathcal{O}_K/_{\mathfrak{p}^k}|}{\left|\mathfrak{p}^{k-1}/_{\mathfrak{p}^k}\right|} = \frac{N\left(\mathfrak{p}^k\right)}{N\left(\mathfrak{p}\right)}$$

Par récurrence sur $k$, on déduit que $N\left(\mathfrak{p}^k\right) = N\left(\mathfrak{p}^{k-1}\right).N\left(\mathfrak{p}\right)$.

**Corollaire 1.5** *Soit $I$ un idéal, si $N(I)$ est premier alors $I$ est un idéal premier.*

**Preuve :**

Supposons que :$I = I_1 I_2$

On a $N(I) = N(I_1)N(I_2)$, comme $N(I)$ est premier i-e $N(I) = \pm p$. Alors on obtient $N(I_1)$ ou $N(I_2) = \pm 1$ , donc $I_1$ ou $I_2$ unité.

contradiction .

**Proposition 1.14** *$N(I) \in I$, céd $I$ divise $N(I)$ ( en particulier : $I$ divise l'idéal principal engendrée par $N(I)$).*

**Preuve :**

Soit $N(I) = |{}^{B}/_{I}| = r$ .

Si $x \in B$, on a : $r\,(x + I) = 0$ dans $|{}^{B}/_{I}|$( car l'ordre d'un élément de groupe divise l'ordre de groupe).

Donc : $rx \in I$, $\forall r \in B$

pour $x = 1$ on obtient $r \in I$. Alors $N(I) \in I$.

**Corollaire 1.6** *Si $I$ est un idéal premier de $B$. Alors $I$ divise exactement un unique nombre premier $p$.*

**Preuve :**

On a $I$ divise $N(I)$. Alors $N(I) = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}$

donc $I$ divise $p_i$ , mais si $p$ divise deux nombres premiers distincts $p_1$ et $p_2$ alors $\exists u, v$ tel que $up_1 + vp_2 = 1$. Donc $I$ divise 1. Alors $I = B$ contradiction. Donc $I$ divise un unique nombre premier $p$.

**Définition 1.30** *(Norme d'un idéal premier )*

*Soit* $\mathfrak{p}$ *un idéal premier, et* $p$ *l'unique nombre premier dans* $\mathfrak{p}$ *.*

*On sait que* $f(\mathfrak{p}) = [{}^{B}\!/_{\mathfrak{p}} : {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}]$ *, alors :* $N(\mathfrak{p}) = |{}^{B}\!/_{\mathfrak{p}}| = p^{f(\mathfrak{p})}$

### Factorisation d'un idéal premier dans un anneau de Dedekind

**Théorème 1.11** *(propiété des anneaux de Dedekind)*

*Soit* $P$*un idéal premier non nul de* $A$*. Alors* $P$ *se décompose de manière unique en un produit des idéaux premiers*

$$P = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_g^{e_g}$$

*où les* $\mathfrak{p}_i$ $(i = 1, ..., g)$ *sont d' idéaux premiers de* $B$*, avec* $e_i \in \mathbb{N}$ *pour* $i = 1, ..., g$*.*

**Définition 1.31** *Soit* $P$ *un idéal premier non nul de* $A$*. Alors* $PB$ *est un idéal de* $B$ *.*

$$\begin{array}{ccc} PB & B & L \\ | & | & |n \\ P & A & K \end{array}$$

*$PB$ n'est pas forcement premier dans $B$, mais l'anneau $B$ est de Dedekind, donc on a la factorisation unique eu premiers de $B$ .*

*Alors*

$$PB = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \tag{1.2}$$

*où les* $\mathfrak{p}_i$ *sont des idéaux premiers de* $B$ *et* $e_i$ *des entiers positifs.*

*On dit alors que* $\forall i$*, l'idéal* $\mathfrak{p}_i$ *est au dessus de* $P$*.*

**remarque :** Soit $\mathcal{Q}$ un idéal premier de $B$ au dessus de $P$, On a alors : $P = \mathcal{Q} \cap A$ est un idéal premier de $A$, on dit que $\mathcal{Q}$ est au-dessus de $P$.

**Proposition 1.15** *Soit* $\mathcal{Q}$ *un idéal premier de* $B$*.Alors*

$\mathcal{Q}$*est dans la factorisation de* $PB$ *si et seulement si* $\mathcal{Q} \cap A = P$*.*

**Preuve :**

Supposons que $\mathcal{Q} \cap A = P$ , alors $P \subseteq \mathcal{Q}$ donc $PB \subseteq \mathcal{Q}$ car $\mathcal{Q}$ est un idéal de $B$. d'où $\mathcal{Q}$ divise $PB$ .Alors $\mathcal{Q}$ est dans la factorisation de $PB$.

Réciproquement, on suppose que $\mathcal{Q}$ divise $PB$, alors $PB \subseteq \mathcal{Q}$

D'autres part on a : $P = P \cap A \subseteq PB \cap A \subseteq \mathcal{Q} \cap A$ , donc $P \subseteq \mathcal{Q} \cap A$.

Comme $A$ est de Dedekind (tout idéal premier est maximal ), alors $\mathcal{Q} \cap A = P$.

**Proposition 1.16** *On peut avoir* $^{A}/_{\mathbf{P}}$ *comme sous corps de* $^{B}/_{\mathfrak{p}_i}$*. Comme* $B$ *est un* $A$*- module de type fini,* $^{B}/_{\mathfrak{p}_i}$ *est un espace vectoriel de dimension finie sur* $^{A}/_{\mathbf{P}}$*.*

**Preuve :** On a l'application

$$\begin{array}{ccc} {}^{A}/_{P} & \longrightarrow & {}^{B}/_{\mathfrak{p}_i} \\ a & +P \longmapsto & a + \mathfrak{p}_i \end{array}$$

est bien défini et injective car $P = A \cap \mathfrak{p}_i$ et est un homomorphisme .

$B = A-$module de type finie ($B$ noethérien).

Si $B =< b_1, ..., b_n >$ comme $A-$module alors $\{b_1 + \mathfrak{p}_i, b_2 + \mathfrak{p}_i \ldots, b_n + \mathfrak{p}_i\}$ engendre $^{B}/_{\mathfrak{p}_i}$ comme $^{A}/_{P}$ espace vectoriel.

De même $^{B}/_{PB}$ est un $^{A}/_{P}$ espace vectoriel de dimension finie.

**remarque :** Nous noterons $f_i$ cette dimension, et l'appellerons l'indice d'inertie où le degré résiduel de $\mathfrak{p}_i$ sur $A$. L'exposant $e_i$ dans (1.2) s'appelle l'indice de ramification de $\mathfrak{p}_i$ sur $A$ .

### 1.6.2 Idéaux dans un corps de nombres

**Proposition 1.17** *Avec les notations précédentes on a*

$$n = [L \ : \ K] = \sum_{i=1}^{g} e_i f_i.$$

**Preuve :** (cf.[15])

**Remarque :** Si l'extension $L/K$ est galoisienne, tous les indices de ramification $e_i$ sont

égaux et tous les indices d'inertie $f_i$ sont égaux .

On obtient alors : $efg = n$.

**Définition 1.32** *Soient $K$ un corps de nombres et $p$ un nombre premier. On a $pO_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$.*

1. *on dit que $\mathfrak{p}_i$ est ramifié au - dessus de $p$ si l'un des indices de ramification $e_i$, est $\geq 2$ .*
2. *On dit que $p$ est ramifié dans $K$ si l'un des $\mathfrak{p}_i$ est ramifié .*
3. *On dit que $p$ est totalement ramifié ( respectivement inerte ) dans $K$ si $e_1 = n$ ( respectivement $e_1 = 1$).*
4. *On dit que $p$ est totalement décomposé dans $K$ si $g = n$ .*

Dans le cas d'un corps quadratique nous avons :

**Théorème 1.12** *Soient $d \in \mathbb{Z}$ un entier sans facteurs carré, $K$ le corps quadratique $K = \mathbb{Q}\left(\sqrt{d}\right)$, $\mathcal{O}_K$ l'anneau des entiers de $K$, et $p$ un nombre premier.*

*La formule $\sum_{i=1}^{g} e_i f_i = 2$ entraîne $g \leq 2$ et on a*

1. *Si $p > 2$ et $p$ divise $d$, ou $p = 2$ et $d \equiv 2$ ou $3\ (mod\ 4)$, alors $p\mathcal{O}_K = \mathfrak{p}^2$, avec $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$.*
2. *Si $p > 2$ et $\left(\frac{d}{p}\right) = 1$, ou $p = 2$ et $d \equiv 1 (mod\ 8)$, alors $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, tel que $\mathfrak{p}_1$ et $\mathfrak{p}_2$ deux idéaux premiers distincts, avec $N_{K/\mathbb{Q}}(\mathfrak{p}_1) = N_{K/\mathbb{Q}}(\mathfrak{p}_2) = p$.*
3. *Si $p > 2$ et $\left(\frac{d}{p}\right) = -1$, ou $p = 2$ et $d \equiv 5 (mod\ 8)$ alors $p\mathcal{O}_K = \mathfrak{p}$ , tel que $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$, avec $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^2$.*

*où $\left(\frac{d}{p}\right)$ désigne le symbole de Legendre du résidu quadratique de $d$ modulo $p$ c'est-à-dire :*

$$\left(\frac{d}{p}\right) = \left\{ \begin{array}{cc} 0 & si\ p \mid d \\ 1 & si\ p est\ un\ carré\ modulo\ p \\ -1 & sinon \end{array} \right\}$$

**Preuve :**(cf.[1])

**Théorème 1.13** *Soient $m \in \mathbb{Z}$ un entier sans facteur carrés, $K$ le corps quadratique $K = \mathbb{Q}(\sqrt{m})$, $d = d_K$, et $p$ un nombre premier.*

1. *$p\mathcal{O}_K$ est décomposé dans $K \Leftrightarrow (\frac{d}{p}) = 1$.*
2. *$p\mathcal{O}_K$ est ramifié dans $K \Leftrightarrow (\frac{d}{p}) = 0$.*
3. *$p\mathcal{O}_K$ est inerte dans $K \Leftrightarrow (\frac{d}{p}) = -1$.*

**Exemples :**

1. $< 11 >$ est inerte dans $\mathbb{Q}\left(\sqrt{-163}\right)$ car

$$\left(\frac{-163}{11}\right) = \left(\frac{2}{11}\right) = -1$$

2. $< 23 >$ est inerte dans $\mathbb{Q}\left(\sqrt{37}\right)$car

$$\left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = (+1)(-1) = -1$$

3. $< 2 >$ est ramifié dans $\mathbb{Q}\left(\sqrt{7}\right)$ car

$$\left(\frac{28}{2}\right) = 0$$

Alors : $< 2 >=< 2, 1 + \sqrt{7} >^2$.

4. $< 7 >$ est ramifié dans $\mathbb{Q}\left(\sqrt{7}\right)$ car

$$\left(\frac{28}{7}\right) = 0$$

Alors $< 7 >=< \sqrt{7} >^2$.

5. $< 3 >$ est décomposé dans $\mathbb{Q}\left(\sqrt{7}\right)$ car

$$\left(\frac{28}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Comme $x^2 \equiv 7(mod\, 3)$ admet une solution $x = 1$ on obtient :

$$< 3 >=< 3, 1 + \sqrt{7} >< 3, 1 - \sqrt{7} > .$$

Dans le cas d'un corps cyclotomique nous avons :

Soient $m$ un entier positive, et $\xi_m$ un racine primitive $m-$ème de l'unité. On note par $K_m$ le corps cyclotomique $\mathbb{Q}(\xi_m)$, soient $\mathcal{O}_{Km}$ l'anneau des entiers de $K_m$, et $p$ un nombre premier.

**Théorème 1.14** *Soit $m = p^r m_1$, tel que $r \in \mathbb{N}$, $m_1 \in \mathbb{N}^*$ et $m_1$ n'est pas divisible par $p$. Soit $h$ l'entier positive qui vérifier $p^h \equiv 1 (mod\, m_1)$, tel que $h \mid \phi(m_1)$ . Alors*

$$< p >= \left(\mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_{\phi(m_1)/h}\right)^{\phi(p^r)}$$

*avec $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{\phi(m_1)/h}$ sont des idéaux premiers distincts, et $N(\mathfrak{p}_i) = p^h, i = 1, ..., \phi(m_1)/h$.*

**preuve :**(cf.[1])

**Exemples :**

1. On va déteminer la décomposition de l'idéal $< 2 >$ dans $\mathcal{O}_{K_5}$.

   Dans ce cas on a : $p = 2, m = 5, r = 0, m_1 = 5, \phi(m_1) = 4, \phi(p^r) = 1$, et $h = 4$.

   donc : $< 2 >= \mathfrak{p}$.

   tel que $\mathfrak{p}$ est un idéal premier avec $N(\mathfrak{p}) = 2^4$.

2. On va déteminer la décomposition de l'idéal $< 2 >$ dans $\mathcal{O}_{K_7}$.

   Dans ce cas on a : $p = 2, m = 7, r = 0, m_1 = 7, \phi(m_1) = 6, \phi(p^r) = 1$, et $h = 3$.

   donc : $< 2 >= \mathfrak{p}_1\mathfrak{p}_2$.

   tel que $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont des idéaux premiers distincts avec $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 2^3$.

La nature de la ramification d'un nombre premier $p$ dans un corps de nombres $K$ est liée à la divisibilité par $p$ du discriminant $d_k$ de $K$.

**Théorème 1.15** *Soit $K$ un corps de nombres, alors les nombres premiers qui se ramifient dans $K$ sont en nombres fini : se sont précisément les diviseurs premiers du discriminant $d_K$.*

**Exemples :** Examinons la ramification dans les cas suivants

– **cas des corps quadratiques**

Prenons $K = \mathbb{Q}\left(\sqrt{d}\right)$, $d \in \mathbb{Z}$, $d \neq 0, 1$ ; $d$ sans facteur carré.

1. Si $d \equiv 2$ ou $3 \bmod 4$ , alors $d_K = 4d$. Par conséquent, les nombres premiers qui se ramifient sont 2 et les diviseurs premiers de $d$.
2. Si $d \equiv 1 \bmod 4$, alors $d_K = d$. Par conséquent, les nombres premiers qui se ramifient sont les diviseurs de $d$.

– **cas des corps cyclotomiques**

Soient $p$ un nombre premier, $L = \mathbb{Q}(\zeta)$, où $\zeta$ est un racine primitive $p-$ième de l'unité.

on a

$$d_K = \pm p^{p-2}$$

Alors $p$ est le seul nombre premier qui se ramifie dans $K$.

# Chapitre 2

# Corps de nombres $p$ -adiques

## 2.1 Valuation $p$ -adique

Soit $p$ un nombre premier et soit $x$ un rationnel non nul , on peut l'écrire sous la forme $x = p^k \frac{a}{b}$ , avec $k \in \mathbb{Z}$ , $a$ et $b$ premiers entre eux et $p \nmid ab$.

**Définition 2.1** *On appelle valeur absolue p-adique de $x$ l'application noté $|\ |_p$ de $\mathbb{Q}$ dans $\mathbb{Q}^+$ définie comme suit :*

1. $|0|_p = 0$.
2. $|x|_p = p^{-k}$

voici quelques propriétés de la valeur absolue $p$-adique :

1. $\forall x, y \in \mathbb{Q}$ on a $|x.y|_p = |x|_p |y|_p$.
2. $\forall x, y \in \mathbb{Q}$ on a$|x + y|_p \leq max\left(|x|_p, |y|_p\right)$.
3. $\forall x, y \in \mathbb{Q}$, $y \neq 0$ on a $\left|\frac{x}{y}\right|_p = \frac{|x|_p}{|y|_p}$
4. $|x|_p = 0 \Longleftrightarrow x = 0$

**Exemple :**

1. Si $p = 5$ et $x = 125$, on a $125 = 5^3$ donc $|x|_5 = 5^{-3}$
2. Si $p = 3$ et $x = \frac{16}{30}$ on peut écrire $x$ comme suite $x = 3^{-1}\left(\frac{16}{10}\right)$ alors $|x|_3 = 3$.

**Définition 2.2** *on appelle valuation p-adique sur* $\mathbb{Q}$ *l'application* $v_p$ *de* $\mathbb{Q}$ *dans* $\mathbb{Z} \cup \{+\infty\}$*définie par :*

1. $v_p(0) = +\infty$.
2. $v_p(x) = k$.

**Proposition 2.1** *la valuation p-adique sur* $\mathbb{Q}$ *vérifie :*

1. $\forall x, y \in \mathbb{Q}^\star$ *on a* $v_p(x.y) = v_p(x) + v_p(y)$.
2. $\forall x, y \in \mathbb{Q}^\star$ *on a* $v_p(x+y) \geq min(v_p(x), v_p(y))$.
3. $v_p(x) = \infty \Longleftrightarrow x = 0$.

**Remarque :** Si $x, y \in \mathbb{Q}^\star$ et $v_p(x) \neq v_p(y)$ alors $v_p(x+y) = inf(v_p(x), v_p(y))$.
**Exemple :** Si $p = 3$ et $x = 471$ on a $471 = 3^1 \times 157$, donc 1 est la valuation $3-$*adique* du nombre 471.

**Définition 2.3** *Soit p un nombre premier et* $(x_n)$ *une suite dans* $\mathbb{Q}$.
*On dit que la suite* $(x_n)$ *est de Cauchy, si* $\forall \epsilon \in \mathbb{Q}_+^\star, \exists N \in \mathbb{N}$ *tel que* $\forall n, m \in \mathbb{N}$, $n > N$ *et* $m > N$ *entraine* $|x_n - x_m|_p < \epsilon$.

**Définition 2.4** *Soit p un nombre premier et K un corps muni d'une valeur absolue* $|\ |_p$.
*Une suite* $(x_n)$ *dans K est dite convergente si :* $l \in K$ *tel que :*

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \exists l \in K \text{tel que } n \geq N \Rightarrow |x_n - l|_p \leq \epsilon$$

**Définition 2.5** *Soit K un corps muni d'une valeur absolue* $|\ |_p$ *avec p un nombre premier. On dit que K est complet pour cette valeur absolue si toute suite de Cauchy dans K est convergente dans K.*

## 2.2 Extensions et complétion

Soit $E$ l'ensemble des suites de Cauchy à valeurs dans $\mathbb{Q}$ pour la valeur absolue $p$-adique $|\,|_p$.

**Proposition 2.2** *L'ensemble $E$ muni de l'addition et de la multiplication usuelles des suites est un anneau commutatif, de plus l'ensemble $I = \{(x_n) \in E$ tels que $\lim_{n\to\infty}(x_n) = 0\}$ est un idéal maximal de $E$, et l'anneau quotient $\frac{E}{I}$ vérifie :*

- $\mathbb{Q} \subset \frac{E}{I}$.
- *$\frac{E}{I}$ est un corps commutatif.*
- *la valeur absolue $|\,|_p$ sur $\mathbb{Q}$ se prolonge à $\frac{E}{I}$.*
- *$\mathbb{Q}$ est dense dans $\frac{E}{I}$ qui est complet pour cette valeur absolue.*

*Le corps $\frac{E}{I}$ est noté $\mathbb{Q}_p$ ( le complété de $\mathbb{Q}$ pour la valeur absolue p-adique).*

**Théorème 2.1** *Soit $K$ un corps muni d'une valeur absolue $|\,|$ , alors il existe une esxtension $\hat{K}$ de $K$ et une valeur absolue sur $\hat{K}$ prolongeant celle de $K$ telle que :*

1. *$\hat{K}$ est complet pour cette valeur absolue .*
2. *$K$ est dense dans $\hat{K}$.*

*On dit que $\hat{K}$est le completé de $K$ pour la valeur absolue $|\,|$.*

**Preuve :**

On construit le complété de $K$ pour $|\,|$ comme on construit $\mathbb{R}$ à partir des suit de Cauchy de $\mathbb{Q}$ pour la valeur absolue usuelle. Les suite de Cauchy forment un anneau $A$ dans lequel $K$ s'injecte. L'idéal $I$ défini par $I = \{(x_n) \in A,\ \lim_{n\mapsto\infty}(x_n) = 0\}$ est un idéal maximal de $A$. Le complété de $K$ pour $|\,|$ est le quotient $\frac{A}{I}$ noté $\widehat{K}$.

Par continuité, si la valeur absolue$|\,|$ sur $K$ est ultramétrique alors l'ensemble des valeur prises par $|\,|$ sur $K$ est le même que celui sur le complété .

**Exemple :** Le corps $\mathbb{Q}_p$ est le complété de $\mathbb{Q}$ pour la valeur absolue $p$-adique.

**Définition 2.6** *( Anneau de valuation )*

*Soit $K$ un corps muni d'une valuation $v$, on vérifie aisément que L'ensemble $V = \{x \in K,\ v(x) \geq 0\}$ est un sous-anneau de $K$. On dit que $V$ est l'anneau de valuation de $K$ associé à $v$. Et l'ensemble $\mathfrak{M} = \{x \in K,\ v(x) > 0\}$ est un idéal maximal de $V$ .*
*On note $k = \frac{V}{\mathfrak{M}}$ le corps résiduel de $K$.*

**Exemple :** L'anneau de valuation de $\mathbb{Q}$ associé à $v = v_p$ est noté $\mathbb{Z}_p$ et $\mathfrak{M} = p\mathbb{Z}_p$, et $k = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ .

**Définition 2.7** *Soit $K$ un corps muni d'une valuation discrète.*
*Dans ce cas, $v(K^\times) = a\mathbb{Z}, a \in \mathbb{R}_+^\star$. On appelle uniformisante de $K$ tout élément $\pi$ de $K$ tel que $v(\pi) = a$.*

**Remarque :** Il n'y a pas unicité de l'uniformisante. En effet ;
Si $\pi$ est un uniformisante quelconque de $K$ en multipliant $\pi$ par une unité $u$ $(v(u) = 0)$, on obtient $\pi' = \pi u$ et $\pi'$ est aussi une uniformisante puisque :

$$v(\pi') = v(\pi) + v(u) = v(\pi) = a$$

**Proposition 2.3** *Soit $K$ un corps muni d'une valuation discrète dont $\pi$ est une uniformisante, alors son idéal maximal est $\mathfrak{M} = \pi V$ , où $V$ désigne l'anneau de valuation de $K$.*
*Tout idéal de $V$ est une puissance de $\mathfrak{M}$ donc un idéal de la forme $\pi^n V$.*

**Théorème 2.2** *( ecriture d'un élément dans un corps complet pour une valuation discrète)*
*Soit $K$ un corps muni d'une valuation discrète $v$, de corps résiduel $k$ et d'uniformisante $\pi$.*
*Soit $S$ un système de représentants de $k$ dans l'anneau de valuation $V$, alors :*

1. *Tout élément de $V$ s'écrit et de manière unique sous la forme :*

$$x = \sum_{n \geq 0} s_n \pi^n, \text{ avec } s_n \in S, \forall n$$

2. *Tout élément de $K$ s'écrit et de manière unique sous la forme :*

$$x = \sum_{n \gg -\infty} s_n \pi^n, \text{ avec } s_n \in S, \forall n$$

**Proposition 2.4** *Soit $K$ un corps muni d'une valeur absolue $||$, $V$ l'anneau de valuation associé à cette valeur absolue et $m$ son idéal maximal.*
*Soit $\widehat{K}$ le complété de $K$ pour $||$. On note encore$||$ le prolongement de $||$ à $\widehat{K}$. Considérons $\widehat{V}$ l'anneau de valuation de $\widehat{K}$ associé à $||$ et $\widehat{m}$ l'idéal maximal de $\widehat{V}$ . Alors , $V = \widehat{V} \cap K$ et est dense dans $\widehat{V}$ de même $m = \widehat{m} \cap V$ est dense dans $\widehat{m}$, de plus ; on a*

$$m\widehat{V} = \widehat{m} \text{ et } {}^{V}/_{m} \simeq {}^{\widehat{V}}/_{\widehat{m}}$$

**Preuve :** (cf.[13]).

**Théorème 2.3** *Soit $K$ un corps de nombres , alors ; il y a une correspondance bi-univoque entre les idéaux premiers de $K$ et les anneaux de valuations pour $K$.*
*Plus précisément, si $\mathcal{O}_K$ désigne l'anneau des entiers de $K$ et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, et $Val(K)$ l'ensemble des anneaux de valuation pour $K$. alors la correspondance précédente est donnée par :*

$$\begin{array}{ccc} Spec_p(\mathcal{O}_K) & \longleftrightarrow & Val(K) \\ \mathfrak{p} & \longmapsto & \mathcal{O}_{\mathfrak{p}} \\ \mathfrak{M} \cap \mathcal{O}_K & \longleftarrow & V \end{array}$$

*tel que pour tout $V \in Val(K)$ , $\mathfrak{M}$ est l'unique idéal maximal de $V$, et pour tout $\mathfrak{p}$ de $\mathcal{O}_K$, $\mathcal{O}_{\mathfrak{p}}$ est un anneau de valuation ( discrète ) pour $K$.*

**Preuve :** (cf.[13]).

**Définition 2.8** *Soit $K$ un corps muni d'une valaution discrète . On dit que $K$ est un corps local si $K$ est complet pour cette valuation et de corps résiduel est parfait.*

**Exemples :**

1. $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la valuation $p$-adique est un corps local dont $p$ est une uniformisante.
2. $\mathbb{F}_q((x))$ est un corps local (où $\mathbb{F}_q$ est un corps fini ( où $q = p^m$)) .
3. Si $K$ est un corps , alors $K((T))$ muni de la valuation $v_T$ est un corps local, dont $T$ est une uniformisante .

**Proposition 2.5** *Soit $K$ un corps local dont on note $A$ l'anneau de valuation . On considère une extension finie $L$ de $K$. Alors $L$ est un corps local dont l'anneau de valuation est la fermeture intégral $B$ de $A$ dans $L$.*
*L'anneau $B$ est donc anneau de valuation discrète (i.e local principal et distinct de son corps des fractions). De plus, si on note $m$ et $\mathfrak{M}$ les idéaux maximaux respectifs des anneaux $A$ et $B$ , alors :*

$mB = \mathfrak{M}^e$ *, et* $[L : K] = ef$ *avec* $f = [{}^{B}/_{\mathfrak{M}} : {}^{A}/_{m}]$.

**Preuve :**(cf.[13]).

**Proposition 2.6** *Soit $L$ un corps muni d'une valeur absolue $||$ et $K$ un sous-corps de $L$ tel que l'extension $L/K$ soit de degré fini. Alors $\widehat{L}$ contient $\widehat{K}$ le complélté de $K$ pour la valeur absolue $||_{|K}$ ; de plus $\widehat{L}$ est une extension de $\widehat{K}$ de degré fini et on a l'inégalité*

$$\left[\widehat{L} : \widehat{K}\right] \leq [L : K]$$

**Remarque :** Revenons au corps $\mathbb{Q}_p$, $p$ étant un nombre premier. Soit $K$ un corps de nombre algébrique d'anneau des entier $\mathcal{O}_K$, et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au dessus d 'un nombre premier $p$. Le complété $K_\mathfrak{p}$ de $K$ pour la valeur absolue $||_\mathfrak{p}$ associé à $\mathfrak{p}$ contient celui de $\mathbb{Q}$ ( i.e $\mathbb{Q}_p$) . De plus l'extension $\mathbb{Q}_p \subset K_\mathfrak{p}$ est finie telle que

$$[K_\mathfrak{p} : \mathbb{Q}_p] \leq [K : \mathbb{Q}]$$

## 2.3 Le corps de nombres p-adiques

### 2.3.1 Notations et définitions

Soit $p$ un nombre premier .

**Définition 2.9** *On appelle corps de nombres p-adiques toute extension finie de $\mathbb{Q}_p$.*

Les élément de l'anneau de valuation $\mathbb{Z}_p$ de $\mathbb{Q}_p$ vérifient :

**Proposition 2.7** *( Développement de Hensel )*
*Soit p un nombre premier, tout élément de l'anneau de valuation $\mathbb{Z}_p$ de $\mathbb{Q}_p$ peut s'écrire et de manière unique sous la forme*

$$\sum_{n\geq 0} S_n p^n \, avec \, S_n \in \{0, 1, ..., p-1\} \, \forall n$$

*Tout élément de $\mathbb{Q}_p$ peut s'écrire et de manière unique sous la forme*

$$\sum_{n\gg -\infty} S_n p^n \, avec \, S_n \in \{0, 1, ..., p-1\} \, \forall n$$

**Exemple :** Si $p = 2$ on a :

1. $5 = 1 + 2^2 = S_0 + S_1 2^1 + S_2 2^2$ avec $S_0 = 1, S_1 = 0, S_2 = 1$.
2. $-1 = \frac{1}{1-2} = 1 + 2 + 2^2 + 2^3 + .... = \sum_{n\geq 0} 2^n$.
3. $-2 = 2 \times (-1) = 2\sum_{n\geq 0} 2^n = \sum_{n\geq 1} 2^n$.

### 2.3.2 Anneau des entiers des corps de nombres $p$-adiques

**Proposition 2.8** *Soit K une extension de degré n de $\mathbb{Q}_p$, la relation :*

$$\forall x \in K, \, |x|_p = \left|N_{K/\mathbb{Q}p}(x)\right|_p^{\frac{1}{n}}$$

*définit l'unique valeur absolue de K prolongeant la valeur absolue p-adique.*
*Soit $V = \left\{x \in K, \, |x|_p \leq 1\right\}$, on vérifie que V est un sous-anneau de K, et c'est un anneau de valuation discrète pour la valuation $v'_p$ definie par :*

$$\forall x \in K;\ v'_p(x) = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p(x)}\right)$$

*Si* $x = 0$ *on a* $v'_p(x) = \infty$.

**Proposition 2.9** *Soit* $K$ *une extension de degré fini* $n$ *de* $\mathbb{Q}_p$*, la relation :*

$$\forall x \in K;\ v'_p(x) = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p(x)}\right)$$

*définit l'unique valuation de* $K$ *prolongeant la valuation* $v_p$ *de* $\mathbb{Q}_p$*. (* $N_{K/\mathbb{Q}_p}(x)$ *désigne la norm de* $x \in K$ *sur* $\mathbb{Q}_p$*) .*

**Preuve :**

On peut voir $K$ comme un espace vectoriel de dimension fini $[K : \mathbb{Q}_p]$.

Si $v'_1$ et $v'_2$ sont deux valuation sur $K$ prolongeant $v_p$ , alors $v'_1, v'_2$ définissent la même topologie sur $K$ dont toutes normes ( au sons valeur absolues ) de $K$ sur $\mathbb{Q}_p$ sont équivalentes , on en déduit le prolongement .

Pour conclure , il reste à montrer que la formule ci-dessus définit bien une valuation sur $K$

En effet , $v'_p(x) = +\infty$ équivaut à $N(x) = 0$, ce qui signifie que la multiplication par $x$ est un endomorphisme non inversible du $\mathbb{Q}_p$-espace vectoriel $K$, donc que $x = 0$.

Il est clair , par définition , que $N(xy) = N(x) N(y)$, donc $v'_p(xy) = v'_p(x) + v'_p(y)$.

Reste à prouver l'inégalité triangulaire : elle est triviale si $x$ ou $y$ est nul. Supposons $xy \neq 0$, et par exemple, $v_p(y) \geq v_p(x)$ .Soit $z = \frac{y}{x}$, alors :

$$v'_p(x + y) = v'_p(x) + v'_p\left(1 + \frac{y}{x}\right)$$

il suffit donc de montrer que $v'_p\left(1 + \frac{y}{x}\right) \geq 0$. Or $N(z) = N(y)/N(x) \in \mathcal{O}_{\mathbb{Q}_p}$ , car $v_p(N(y)) \geq v_p(N(x))$. Soit :

$$P(X) = X^d + \cdots + a_d$$

le polynôme minimal de $z$, alors $N(z) = \pm a_d^{n/d}$ ( car le polynôme normal de $z$ est $P^{n/d}$). Donc si $N(z) \in \mathcal{O}_{\mathbb{Q}_p}$, $a_d \in \mathcal{O}_{\mathbb{Q}_p}$.

Alors, d'après le corollaire précédent , $P \in \mathcal{O}_{\mathbb{Q}_p}[X]$, donc $z \in \mathcal{O}_K$, alors $1+z \in \mathcal{O}_K$, $N(1+z) \in \mathcal{O}_{\mathbb{Q}_p}$, et $v_p'(1+z) \geq 0$, ce qui achève démonstration.

**Proposition 2.10** *L'anneau de valuation $V$ est l'anneau des entiers de $K$ .*

**Preuve :**

On va montrer tout d'abord que $V$ est l'anneau des entiers de $K$.

Soit $\alpha \in V$ de polynôme minimal $P_\alpha(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0$.

Soit $L = \mathbb{Q}_p(\alpha_1, \alpha_2, ..., \alpha_r)$ le corps des racines de $P_\alpha(X)$, où $\alpha_1, \alpha_2, ..., \alpha_r$ sont ses racines distinctes.

Pour tout $i \in \{1, 2, ...r\}$ on a :

$$\left|N_{L/\mathbb{Q}_p}(\alpha_i)\right|^{\frac{1}{[L:\mathbb{Q}_p]}} = \left|N_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\alpha_i)\right|^{\frac{1}{r}} = \left|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|^{\frac{1}{r}} = \left|N_{K/\mathbb{Q}_p}(\alpha)\right|^{\frac{1}{r}}.$$

Par suite, comme $|\alpha|_p \leq 1$ alors $|\alpha_i|_p \leq 1$ $\forall i \in \{0, 1, ..., r-1\}$.

Comme les coefficients $a_j$ sont des sommes des produits de $\alpha_i$, alors $|a_j|_p \leq 1$ pour tout $j \in \{1, 0, ..., r-1\}$. Par conséquent, $P_\alpha(X) \in \mathbb{Z}_p[X]$ et donc $\alpha \in V$ un entier sur $\mathbb{Z}_p$.

Réciproquement, on suppose que $\alpha$ est un entier sur $\mathbb{Z}_p$, soit $g(x) \in \mathbb{Z}_p[X]$ son polynôme minimal, alors

$$N_{K/\mathbb{Q}_p}(\alpha) = (-1)^n g(0)^r,\ r = [K : \mathbb{Q}_p(\alpha)].$$

Comme $g(0) \in \mathbb{Z}_p$, alors $\left|N_{K/\mathbb{Q}_p}(\alpha)\right| \leq 1$ ce qui entraine $|\alpha| \leq 1$ et donc $\alpha \in V$.

D'où, $V$ est l'anneau des entier de $K$.

## 2.4 Extension de corps de nombres $p$-adiques

### 2.4.1 Correspondance idéaux premiers de $K$ et corps $p$-adiques dans lesquels $K$ est dense

**Théorème 2.4** *Il y a une correspondance bi-univoque entre les idéaux premiers de $K$ au dessus de $p$ et les corps de nombres $p$-adiques dans lesquels $K$ est dense . Notons $Spec_p(K)$ l'ensembles d' idéaux premiers de $K$ au dessus de $p$, $Ext_{\mathbb{Q}_p}(K)$ l'ensemble des extensions de $\mathbb{Q}_p$ dans lesquelles $K$ est dense, puis pour $E \in Ext_{\mathbb{Q}_p}(K)$, $\mathfrak{M}_E$ l'unique idéal maximal de $E$ . Alors la correspondance précédente est donnée par :*

$$\begin{array}{ccc} Spec_p(K) & \longleftrightarrow & Ext_{\mathbb{Q}_p}(K) \\ \mathfrak{p} & \longrightarrow & K_{\mathfrak{p}} \\ \mathfrak{M}_E \cap K & \longleftarrow & E \end{array}$$

*De plus si désigne $\mathcal{O}$ l'anneau des entiers de $K$, $\mathcal{O}'$ celui de $K_{\mathfrak{p}}$( i.e la clôture intégrale de $\mathbb{Z}_p$ dans $K_{\mathfrak{p}}$) et $\mathfrak{M}$ l'unique idéal maximal de $\mathcal{O}'$, alors :*

1. *Le premier $\mathfrak{p}$ de $K$ rest premier dans $K_{\mathfrak{p}}$, i.e . $\mathfrak{p}\mathcal{O}' = \mathfrak{M}$.*
2. *Les corps résiduels sont isomorphes, i.e. $\mathcal{O}/\mathfrak{p} \simeq \mathcal{O}'/\mathfrak{m}$ , de dimension commune sur $\mathbb{F}_p$ égale à $f_{\mathfrak{p}}$, le degré résiduel du premier $\mathfrak{p}$.*
3. *les indices de ramifications de $p$ par rapport à $\mathfrak{p}$ ( dans $K$) et par rapport à $\mathfrak{M}$ ( dans $K_{\mathfrak{p}}$) sont les mêmes ; autrement dit $\mathfrak{p}\mathcal{O}' = \mathfrak{M}^{e_{\mathfrak{p}}}$.*
4. *l'extension $\mathbb{Q}_p \subset K_{\mathfrak{p}}$ est de degré $e_{\mathfrak{p}} f_{\mathfrak{p}}$.*

**Preuve :** (cf.[13])

### 2.4.2 Complétion et polynômes

Il s'agira du complété d'un corps de nombres algébrique engendré par une racine d'un polynôme unitaire irréductible sur $\mathbb{Q}$

Soit $K$ un corps de nombres algébrique engendré par une racine d'un polynôme $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, puisque $f$ est irréductible son discriminant est non nul, par

conséquent $f$ reste sans facteur carré dans $\mathbb{Z}_p[X]$, $p$ étant un nombre premier .

Soit

$$f(X) = \prod_{i=1}^{r} f_i(X)$$

la factorisation de $f$ en facteurs irréductible dans $\mathbb{Z}_p[X]$.

**Théorème 2.5** *Soit $f \in \mathbb{Z}[X]$ unitaire irréductible, $K$ un corps de nombres engendré par une racine de $f$ dans $\overline{\mathbb{Q}}$. A tout facteur irréductible $g \in \mathbb{Z}_p[X]$ de $f$ dans $\mathbb{Z}_p[X]$ est associé un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus de $p$ tel que :*

$$deg(g) = e_{\mathfrak{p}} f_{\mathfrak{p}}$$

*Réciproquement à tout idéal premier de $\mathcal{O}_K$ au-dessus de $p$ est associé un diviseur irréductible $g$ de $f$ dans $\mathbb{Z}_p[X]$ et ${}^{\mathbb{Q}_p[X]}/_{\langle g \rangle}$ est le complété de ${}^{\mathbb{Q}[X]}/_{\langle f \rangle}$ pour la valeur absolue associé à $v_{\mathfrak{p}}/e_{\mathfrak{p}}$.*

**Preuve :**

Considérons $g \in \mathbb{Z}_p[X]$ un diviseur unitaire et irréductible de $f$ dans $\mathbb{Z}_p[X]$.

Soit $E$ une extension de $\mathbb{Q}_p$ de degré celui de $g$.

Soit

$$\varphi : \mathbb{Q}[X] \longrightarrow {}^{\mathbb{Q}_p[X]}/_{(g)}$$

un morphisme injectif d'anneaux, alors $Ker\varphi \simeq \mathbb{Q}[X] \cap g\mathbb{Q}_p[X]$ est un idéal premier de $\mathbb{Q}[X]$ contenant $f\mathbb{Q}[X]$ donc $f\mathbb{Q}[X] = \mathbb{Q}[X] \cap g\mathbb{Q}_p[X]$ , et ${}^{\mathbb{Q}[X]}/_{(f)}$, ${}^{\mathbb{Q}_p[X]}/_{(g)}$ sont des corps car les idéaux $(f)$ et $(g)$ sont maximaux . Par suite $E$ est donc une extension de $K$ et $\mathcal{O}_K \subset \mathcal{O}_E$.

Or $\mathcal{O}_E$ est un anneau de valuation discrète, c'est donc un anneau local d'idéal maximal que l'on note $\mathfrak{M}$. Ainsi $\mathfrak{M} \cap \mathcal{O}_K$ est premier dans $\mathcal{O}_K$ et il est au-dessus de $p$ puisque

$$\mathfrak{M} \cap \mathcal{O}_K \cap \mathbb{Z} = \mathfrak{M} \cap \mathbb{Z} = (\mathfrak{M} \cap \mathbb{Z}_p) \cap \mathbb{Z}_p = p\mathbb{Z}_p \cap \mathbb{Z} = p\mathbb{Z}$$

Par conséquent, à tout facteur irréductible $g$ de $f$ dans $\mathbb{Z}_p[X]$ , $g$ irréductible et unitaire est associé un idéal premir de $\mathcal{O}_K$ au-dessus de $p$ à savoir $\mathfrak{M} \cap \mathcal{O}_K$.

Réciproquement. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au- dessus de $p$, $K_{\mathfrak{p}}$ le complété de $K$ pour la valeur absolue $|\,|_{\mathfrak{p}}$. Alors $K_{\mathfrak{p}}/K$ est une extension de $\mathbb{Q}_p$ avec $[K_{\mathfrak{p}} : \mathbb{Q}_p] = e_{\mathfrak{p}} f_{\mathfrak{p}}$. Ainsi $K_{\mathfrak{p}} = \mathbb{Q}_p(\theta)$, ou $\theta \in \mathcal{O}_K$ est une racine d'un polynôme irréductible $g(X)$ sur $\mathbb{Q}_p$. Par conséquent $g(X)$ est un facteur irréductible unitaire de $f$ dans $\mathbb{Z}_p[X]$, ce qui donne la crrespondance entre l'idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus de $p$ et un diviseur irréductible $g(X)$ de $f(X)$ dans $\mathbb{Z}_p[X]$.

**Théorème 2.6** *( lemme de Hensel )*
*Soit* $f(X) = X^d + a_1 X^{d-1} + \cdots + a_{d-1}X + a_d \in \mathbb{Z}_p[X]$ *un polynôme non nul de degré* $d$.
*Supposons qu'il existe deux polynômes unitaires* $g$ *et* $h$ *dans* $\mathbb{Z}_p[X]$ *tels que :*
$\overline{f}(X) = g(X)\,h(X)$, $deg(g) + deg(h) \leq d$ *et* $(g, h) = 1$.
*Alors il existe* $G$ *et* $H$ *dans* $\mathbb{Z}_p[X]$ *tels que :* $\overline{G}(X) = g(X)$, $\overline{H}(X) = h(X)$, *et*
$f(X) = G(X)\,H(X)$.
*Rapplons que* $\overline{f}$ *désigne l'image de* $f$ *dans* $\mathbb{F}_p[X]$ .

**Corollaire 2.1** *Soit* $P \in K[X]$ *un polynôme irréductible et unitaire tel que* $P(0) \in \mathcal{O}_K$, *alors* $P \in \mathcal{O}_K[X]$.

**Preuve :** (cf.[2]).

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

Nous allaons maintenant voir que la théorème de la ramification pour les corps locaux se trouve bien plus simple que celle des corps des nombres.
Soit $p$ un nombre premier et $E$ un corps de nombre $p$-adique (i.e. une extension finie de $\mathbb{Q}_p$) .
On note $\mathcal{O}_E$ l'anneau des entiers de $E$ est un anneau de valuation discrète ; de plus, si on note $\mathfrak{M}$ son ( unique) idéal maximal , on a :

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

où $e$ est l'indice de ramification de l'extension $E/\mathbb{Q}_p$ , le degré résiduel $f$ est donné par :

$$f = dim_{\mathbb{F}_p}\mathcal{O}_E/\mathfrak{M}$$

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

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

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

**Définition 2.10** *Soit $L/K$ une extension de corps de nombres $p-$adique .*
*On dit que l'extension $L/K$ est non ramifiée si $e = 1$. Elle est totalement ramifiée si $e = n$ avec $n = [L:K]$ . Elle est modérement ramifiée si $e$ est premier avec $p$, et sauvagement ramifiée dans le cas contraire .*

### 2.5.1 Extensions totalements ramifiées :

Les extensions totalement ramifiées sont décrites par la

**Théorème 2.7** *Si $K$ est un corps de nombres $p$-adiques, et $L/K$ une extension de degré fini totalement ramifiée, alors il existe un polynôme d'Eisenstein $f(X)$ sur $K$ dont une racine engendre $L$ sur $K$ . Réciproquement, tout extension de $K$ engendrée par une racine d'un polynôme d'Eisenstein est totalement ramifée .*

**Preuve :**(cf.[13]).

**Théorème 2.8** .

1. *Si $K/\mathbb{Q}_p$ est une extension ( finie ) totalement ramifie , alors $K = \mathbb{Q}_p(\pi)$ où $\pi$ est une uniformisante et $Min(\pi, \mathbb{Q}_p, X)$ est un polynôme d'Eisenstein .*

2. *Si* $K = \mathbb{Q}_p(\alpha)$ *est une extension de degré* $n$ *de* $\mathbb{Q}_p$*, où* $Min(\alpha, \mathbb{Q}_p, X)$*est un polynôme d'Eisenstein, alors* $\alpha$ *est un uniformisante de* $K$ *et l'extension* $K/\mathbb{Q}_p$ *est totalement ramifie .*

**Preuve :**

1. Soit $v_p$ la valuation définie sur $K$ dont sa restriction à $\mathbb{Q}_p$ est une valuation sur ce corps définie par

$$\begin{cases} v_p(0) = \infty \\ v_p(x) = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p}(x)\right) \text{ si } x \in K \end{cases}$$

Soit $\mathfrak{M}$ l'unique idéal maximal de $K$, soit $\mathfrak{M} = (\pi)^n$ où $\pi$ est une uniformisante de $K$. Alors

$$v_p(\pi) = \frac{1}{n} = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p}(\pi)\right)$$

ce qui donne $v_p\left(N_{K/\mathbb{Q}_p}(x)\right) = 1$.

Soit $g(X) = Min(\pi, \mathbb{Q}_p, X) = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}_p[X]$ .

Alors $N_{K/\mathbb{Q}_p}(\pi) = (-1)^n a_0^d$ où $d = \frac{n}{r}$.

ce qui entraine

$$1 = v_p\left(N_{K/\mathbb{Q}_p}(\pi)\right) = d v_p(a_0)$$

. Ce qui implique que $d = 1$ puisque $v_p(a_0) \in \mathbb{Z}$.

Par conséquent $n = r$ et $K = \mathbb{Q}_p(\pi)$.

Montrons que $v_p(a_i) \geq 1$ pour $1 \leq i \leq n-1$, sachant que $d v_p(a_0) = 1$ et $d = 1$, alors $v_p(a_0) = 1$.

Soit $\pi_1, \pi_2, ..., \pi_n$ les racines de $g(X)$ dans une clôture algébrique $C$ contenant $\mathbb{Q}_p$, soit $G$ le corps de décomposition de $g(X)$ et $v$ la valuation définie sur $G$ qui prolonge $v_p$ telle que :

$$\begin{cases} v(0) = \infty \\ v(x) = \frac{1}{n} v_p\left(N_{G/\mathbb{Q}_p}(x)\right), \text{Si } x \neq 0 \end{cases}$$

Pour tout $i \in \{1, 2, ..., n-1\}$ on a $v(\pi_i) = \frac{1}{n}$, ce qui donne :

$$v_p(a_{n-1}) = v_p(a_{n-1}) = v\left(\sum_{i=1}^{n} \pi_i\right) \geq inf(v(\pi_i)) > 0$$

Comme $a_{n-1} \in \mathbb{Q}_p$ et $v_p(a_{n-1}) > 0$, alors $v_p(a_{n-1}) \geq 1$.

De la même manière, en utilisant les fonctions symétriques des racines on montre que $v_p(a_i) \geq 1$, ce qui montre que $g(X)$est d'Eisenstein .

2. Soit $[K : \mathbb{Q}_p] = n$ avec $K = \mathbb{Q}_p(\alpha)$ ,et $f(X) = Min(\alpha, \mathbb{Q}_p, X)$ un polynôme d'Eisenstein .Alors

$$v_p(\alpha) = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p}(\alpha)\right) \text{ et } N_{K/\mathbb{Q}_p}(\alpha) = (-1)^n f(0)$$

ce qui donne

$$v_p\left(N_{K/\mathbb{Q}_p}(\alpha)\right) = v_p(f(0)) = 1$$

et $v_p(\alpha) = \frac{1}{n}$ car $f(X)$ est un polynôme d'Eisenstein .

Soit $\pi$ une uniformisante de $K$ et soit $e = e(K/\mathbb{Q}_p)$, alors $v_p(\pi) = \frac{1}{e}$et il existe $\beta \in \mathcal{O}_K$ tel que $\alpha = \pi\beta$.

Ainsi, $v_p(\alpha) \geq v_p(\pi)$, c'est à dire que $n \leq e$ et comme $e \leq n$ alors $n = e$.

Ce qui montre que $K/\mathbb{Q}_p$ est une extension tatalement ramifie .

$\beta$ étant un élément inversible dans $\mathcal{O}_K$, car $v_p(\beta) = 0$, par suit $(\alpha) = (\pi)$ ce qui veut dire que $\alpha$ est un uniformisante de $K$.

**Exemple :** Soit $K$ l'extension de $\mathbb{Q}_p$ engendrÃ© par les racines $p$-ièmes de l'unité : $K$ est définie par le polynôme irréductible $f(X) = (X^p - 1)/(X - 1)$. Or $f(1 + Y)$ est un polynôme d'Eisenstein, donc $K$ est totalement ramifiée de degré $p-1$. Si $x$ est une racine primitive $p$-ième de 1, $x - 1$ est un uniformisante de $k$ et $v(x - 1) = \frac{1}{p-1}$.

**Corollaire 2.2** *Il existe une unique extension totalement ramifiée de degré donné .*

**Lemme 2.1** *(Critère d'Eisenstein ) :*

*Soit $K$ un corps valué, ultramétrique, d'anneau de valuation $V$, d'idéal maximal $\mathfrak{M}$ est soit $P$ un polynôme unitaire de $V[X]$ :*

*$P(X) = X^n + a_1X^{n-1} + \cdots + a_n$. Si $a_i \in \mathfrak{M}$ pour $i = 1, ..., n$ et $a_n \notin \mathfrak{M}^2$, le polynôme $P$ est irréductible dans $K[X]$. Si $K$ est en plus complet , $P$ définit une extension totalement ramifiée de $K$.*

### 2.5.2 Extensions non ramifiées :

Maintenant , quelques résultats sur les extensions non ramifiées. On pourra caractériser les extensions non ramifiées par

**Théorème 2.9** *Soit $L/K$ une extension de corps de nombres p-adiques de degré fini. Soient $\mathcal{O}_L$ et $\mathcal{O}_K$ les anneaux des entiers respectivement de $L$ et $K$, de corps résiduel respectifs $k_L$et $k_K$.*

1. *Si $L/K$ est non ramifiée, alors il existe un élément $\alpha \in \mathcal{O}_L$ tel que $L = K(\alpha)$ et $k_L = k_K(\overline{\alpha})$.*
   *De plus si $g(X)$est un polynôme minimal de $\alpha$ sur $K$, alors $\overline{g}(\alpha)$ obtenu par réduction de $g(X)$ modulo p, de ses coefficients, et irréductible et séparable sur $k_K$.*
2. *Si $g(X)$ est un polynôme unitaire dans $\mathcal{O}_K[X]$ avec $\overline{g}(X)$ irréductible et séparable sur $k_K$ et si $\alpha$ est une racine de $g(X)$, alors $L = K(\alpha)$ est une extension non ramifiée de $K$, et $k_L = k_K(\overline{\alpha})$.*

**Corollaire 2.3** *il existe une unique extension non ramifiée de degré donné .*

**Corollaire 2.4** *Si $L/F$ est une extension non ramifiée et $K/\mathbb{Q}_p$ est de degré fini, alors l'extension $LK/FK$ est non ramifiée.*

**Corollaire 2.5** *Si $L/K$ et $F/K$ sont des extensions non ramifiées, il en est de même de $LF/K$.*

### 2.5.3 Extensions modérements ramifiées :

Les extension modérement ramifiée sont caractérisées par

**Proposition 2.11** *Une extension $L/K$ de corps de nombres p-adiques de degré $n$ est modérement ramifiée si et seulement si le discriminant $d_{L/K}$ de $L/K$ n'est pas divisible par $p^n$.*

**Lemme 2.2** *Si $L/K$ est modérement ramifiée et $M/K$ de degré fini, alors $LM/M$ est modérement ramifiée.*

**Lemme 2.3** *Soient $L$ et $M$ deux extensions d'un coprs de nombres p-adiques $K$, telles que $M/K$ soit modérement ramifiée .*
*Si $e(M/K)$ divise $e(L/K)$ alors $ML/L$ est modérement ramifiée .*

**Proposition 2.12** *Une extension $L/K$ de degré $n, n \in \mathbb{N}^\star$ est totalement et modérement ramifiée si et seulement si $L = K(\theta)$ où $\theta$ est une racine d'un binôme $X^n - a$, où $a \in K$ tel que $v_p(a) = 1$.*

**Proposition 2.13** *Une extension $L/K$ de degré fini $n$ de corps de nombres p-adiques est sauvagement ramifiée si et seulement si le discriminant $d_{L/K}$ est divisible par $p^n$.*

### 2.5.4 Conclusion sur la structure des extensions finies

**Théorème 2.10** *Si $L$ est une extension finie de $K$ telle que $k_L/k_K$ soit séparable , alors $L$ contient deux sous - extension $L_0 \subset L_1$ de $K$ qui sont uniquement déterminées par les propriétes suivantes :*

1. *$L_0/K$ est non ramifiée .*
2. *$L/L_1$ est totalement ramifiée de degré une puissance de $p$.*

*3.* $L_1/L_0$ *est totalement ramifiée de degré une puissance de* $p$*.*

Ceci peut se résumer avec les diagrammes suivants :

$$\text{pou } L/K \text{ avec } \begin{matrix} k_L \\ |sép \\ k_K \end{matrix} \text{ , on a } \begin{matrix} L \\ |t.r \\ L_1 \\ |t.r \\ L_0 \\ |n.r \\ K \end{matrix} .$$

# 2.6 Groupe de Galois et ramification

## 2.6.1 groupe de décomposition et groupe de ramification

soient $K$ un corps de nombres , $L$ une extension galoisienne de $K$ de degré $n$, $G$ le groupe de Galois de $L/K$ et $\mathcal{O}_K$(respectivement $\mathcal{O}_L$) l'anneau des entiers e $K$ ( respectivement de $L$) .

$$\begin{matrix} \mathfrak{p} & \mathcal{O}_L & L \\ | & | & | \\ \wp & \mathcal{O}_K & K \end{matrix}$$

On note $\mathfrak{p}$ un idéal premier de $\mathcal{O}_L$ au-dessus d'un idéal premier $\wp$ de $\mathcal{O}_K$ et

$$D_{\mathfrak{p}} = \{\sigma \in G \setminus \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

le groupe de décomposition de $\mathfrak{p}|\wp$ .

Le groupe

$$G_0 = \{\sigma \in D_{\mathfrak{p}} \setminus \forall x \in \mathcal{O}_L, \sigma(x) - x \in \mathfrak{p}\}$$

est le groupe d'inertie de $\mathfrak{p}|\wp$ est son cardinal est égal à l'indice de ramification $e(\mathfrak{p}|\wp)$de $\mathfrak{p}$ dans $L/K$. Tous les indices de ramification des idéaux premiers $\mathfrak{p}$ de $L$ au-dessus de $\wp$

sont égaux car l'extension $L/K$ est galoisienne.

Le groupe

$$G_k = \left\{\sigma \in G \setminus \forall x \in \mathcal{O}_L, \sigma(x) - x \in \mathfrak{p}^{k+1}\right\},\ k \geq 1$$

est le $k-$ième groupe de ramification.

**Théorème 2.11** *Avec les notations précédentex, on a :*

1. *$G_0/G_1$ est un sous- groupe cyclique du groupe multiplicatif du corps résiduel $O_L/\mathfrak{p}$. De plus il est d'ordre premier à la caractéristique $p$ du corps résiduel $O_K/\wp$.*
2. *$G_1$ est un sous- groupe qui mesure la ramification sauvage en $\wp$ ; $G_1$ est trivial si et seulement si l'extension $L/K$ est modérement ramifiée en $\wp$.*

### 2.6.2 Correspondance de galois et ramification

Soit $p$ un nombre premier, et $L/K$ une extension normal de corps de nombres $p$-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 $K$.

Par la théorié de Galois, à chaque sous groupe $G_i$ , $i \geq 0$ correspond un sous corps $L_i$ laissé fixe par $G_i$ qu'est le groupe de Galois de l'extension $L/L_i$ .

**Théorème 2.12** *Sous les hypothèses ci dessous on a :*

1. *L'extension maximal 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 est cyclique d'ordre $f(L/K) = [k_L : k_K]$.*
2. *L'extension maximal modérement 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 $p$.*

**Corollaire 2.6** *Si $L/K$ est non ramifiée, alors son groupe de Galois est cyclique d'ordre $f(L/K)$.*

Le critère de Van der Waerden - Dedekind exprime le lien entre la ramification d'un nombre premier $p$ dans un corps de nombres $K$ et les cycles composant des sous-groupes du groupe de Galois de la clôture normale de $K$ sur $\mathbb{Q}$.

**Théorème 2.13** *( critère de Van der Waerden - Dedekind )*
*Soit $K$ un corps de nombres et $L/\mathbb{Q}$ un corps de nombres galoisien de groupe de Galois $G$ , contenant $K$. Soit $\mathfrak{P}$ un premier de $L$ au-dessus d'un premier $p$ de $\mathbb{Z}$, on considère $D(\mathfrak{P})$et $G_0(\mathfrak{P})$ les deux sous -groupes de $G$ que sont respectivement le croupe de décomposition et le groupe d'inertie de $\mathfrak{P}$.*
*On suppose que la décomposition de $p$ dans $K$ est de la forme :*

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \text{ avec } N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$$

*On considère l'action de $G_i$ sur $\underline{K} = Hom_{\mathbb{Q}}(K, L)$ par composition à gouche , alors $\underline{K}$ se décompose en $g$ $D(\mathfrak{P})$- orbites de longueur respective $e_i f_i$, et chacune d'entre elles se décompose en $f_i$ $G_0(\mathfrak{P})-$orbites de longueur $e_i$.*

**Preuve :**(cf.[13]).

**Proposition 2.14** *Soit $K$ et $K'$ deux corps de nombres et $\sigma$ un élément de $Hom_{\mathbb{Q}}(K, K')$ ,on considère $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers de $K$ et $K'$ respectivement ; on note $|\,|$ la valeur absolue sur $K$ associée à $\mathfrak{p}$ et $|\,|'$ celle sur $K'$ associée à $\mathfrak{p}'$. Alors $\sigma$ préserve les valeurs absolues ie :*

$$|\sigma(x)|' = |x| \text{ si et seulement si } \sigma^{-1}(\mathfrak{p}') = \mathfrak{p}$$

**Preuve :**(cf.[9]).

**Corollaire 2.7** *Soit $L$ un corps de nombres galoisienne. Pour tout premier $\mathfrak{P}$ de $L$, le sous - groupe de Galois 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 $D(\mathfrak{P})$.*

**Exemple :** Soit $f(X) = X^5 + 20X + 16$ .

$f$ est irréductible sur $\mathbb{Z}$ car ( $g(X) = f(X-1) = X^5 - 5X^4 + 10X^3 - 10X^2 + 25X - 5$ est d'Eisenstein en $p = 5$ ). Soit $L$ le corps de décomposition de $f$ sur $\mathbb{Q}$, alors le groupe de Galois $G$ de $L/K$ est un sous groupe de $S_5$. Et $dis(f) = 2^{16} \times 5^6$, est un carré , par suite $G$ est un sous - groupe transitif de $A_5$.

Comme $G$ opère transitivement sur les racines de $f$, et les sous - groupes transitifs de $A_5$ sont : $C_5$ qui est cyclique d'ordre 5, le sous groupe Dihédral $D_5$ d'ordre 10 est $A_5$.

Soit $\alpha$ une racine de $f$ dans $K$, la décomposition de 2 dans $K = \mathbb{Q}(\alpha)$est $\langle 2 \rangle = \mathfrak{p}^4\mathfrak{q}$ avec $f_{\mathfrak{p}} = f_{\mathfrak{q}} = 1$.

Alors , par le critère de Van der Waerden - Dedekind, le groupe d'inertie contient un cycle d'ordre 4, ce qui montre que l'ordre de $G$ est divisible par 4 . Par conséquent $G \simeq A_5$.

## 2.7 Polygone de Newton et ramification

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

$$f(X) = \sum_{j=0}^{t} p^{\alpha_j} Q_j(X) \varphi(X)^{t-j} \tag{2.1}$$

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

Dans l'égalité (2.1), les coefficients de $Q_j(X)$ ne divisent pas tous les nombres premiers $p$, 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 (2.1) est appelé décomposition canonique de $f(X)$.

Le $(p, \varphi)-$polygone de $f(X)$ est défini par

**Définition 2.11** *Le $(p, \varphi)-$polygone de $f(X)$ est la frontière de l'enveloppe convexe supérieur de l'ensemble des points $(j, \alpha_j)$ dans la partie vertical. La partie du $(p, \varphi)-$polygone*

*diminuée de la partie horizontale ( s'il ya lieu ) est appelée partie principale du* $(p,\varphi)-$*polygone*

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

*On définit :*

$l_0 :=$ *longueur du côté horizontale.*

$l_i :=$ *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* $\epsilon_i = pgcd(l_i, h_i)$, $\lambda_i = \frac{l_i}{\epsilon_i}$ *et* $k_i = \frac{h_i}{\epsilon_i}$.

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

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

*de l'expression*

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

*Où les polynôme* $R_{i,j}(X)$ *sont de degré* $< m$*.*

*En particulier,* $R_{i,0}(X)$ *est premier avec* $\varphi(X)$ *dans* $\mathbb{F}_p[X]$*, il existe alors on polynôme* $A_i(X) \in \mathbb{Z}[X]$ *tel que*

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

*On définit alors le polynôme* $S_{i,j}(X) = A_i(X)R_{i,j}(X)$.

**Définition 2.12** *On appelle polynôme associé à* $f(X)$*et relatif au côté* $S_i$*, le polynôme* $F_i(X,Y)$ *donnée par*

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

*Par construction, le polynôme* $F_i(X,Y)$ *dépend du choix de* $A_i(X)$*, ce qui n'est pas le cas de sa calsse modulo l'idéal* $(p,\varphi(X))$.

La relation entre $(p,\varphi)$ −polygone et ramification est donnée par

**Théorème 2.14** *( [7] Thérème 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 $\theta$ une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$ fixée. On cosidère la factorisation modulop de $f(X)$*

$$f(X) = \varphi_1(X)^{a_1} ... \varphi_s(X)^{a_s}\ (mod\, p)$$

*Où $\varphi_\nu(X) \in \mathbb{Z}[X]$ de degré $deg\varphi(X) = m_\nu$. Alors,*

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

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

*A chaque idéal $\mathfrak{a} = \mathfrak{a}_\nu$ correspond un facteur irréductible $\varphi(X) = \varphi_\nu(X)$.*

*On détermine ainsi le $(p,\varphi)$- polygone de $f(X)$ .Pour chaque $S_i$ de la partie principale de ce polygone, on considère la factorisation modulo $(p,\varphi)$ du polynôme associé $F_i(X,Y)$*

$$F_i(X,Y) \equiv F_1^{(i)}(X,Y)^{a_1^{(i)}} \dots F_{t_i}^{(i)}(X,Y)^{a_{t_i}^{(i)}}\ mod\,(p,\varphi(X))$$

*Alors*

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

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

*De plus*

$$N_K\left(\mathfrak{c}_j^{(i)}\right) = p^{m.m_j^{(i)} a_j^{(i)}};\ m_j^{(i)} = deg\, F_j^{(i)}(X,Y)$$

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

**Exemple :** Soit $f(X) = X^3 - 2 \in \mathbb{Z}[X]$, alors est d'Eisenstein en $p = 2$ ce qui montre qu'il est irréductible sur $\mathbb{Q}$.

Soit $\theta$ une racine de $f(X)$ dans $\overline{\mathbb{Q}}$, la clôture algèbrique de $\mathbb{Q}$ et $K = \mathbb{Q}(\theta)$, alors $K$ est

une extension de degré 3 sur $\mathbb{Q}$, on note $\mathcal{O}_K$ son anneau d'entiers .
Déterminons la factorisation de l'idéal $5\mathcal{O}_K$ dans $\mathcal{O}_K$, pour cela nous aurons besoin en premier lieu de factorisation de $f(X)\, modulo 5$ on obtient

$$\overline{f}(X) = (X+2)\left(X^2+3X+4\right)$$

On pose $\varphi_1(X) = X+2$ et $\varphi_2(X) = X^2+3X+4$. Ainsi, la factorisation de $f(X)\, modulo 5$ donnee

$$5\mathcal{O}_K = \mathfrak{a}_1\mathfrak{a}_2$$

où les $\mathfrak{a}_1$et $\mathfrak{a}_2$ sont des idéaux de $\mathcal{O}_K$ premiers entre eux, tel que $N_{K/\mathbb{Q}}(\mathfrak{a}_1) = 5$ et $N_{K/\mathbb{Q}}(\mathfrak{a}_2) = 25$.
La division de $f(X)$ suivant les puissaces croissantes de $\varphi_1(X)$ puis par $\varphi_2(X)$ donne

$$f(X) = -10 + 12\varphi_1(X) - 6\varphi_1(X)^2 + \varphi_1(X)^3$$

et

$$f(X) = 5(X+2) + (X-3)\varphi_2(X)$$

Par la théorie de Ore, la partie principale du $(5,\varphi_1)-$polygone de $f(X)$ est formée d'un seul côté reliant les points $(2,0)$ et $(3,1)$, il lui est associé le polynôme $G_1(Y) = 12Y-2$ qui est séparable $modulo 5$. Alors $\mathfrak{a}_1 = \mathfrak{p}_1$ est un idéal premier no nul de $\mathcal{O}_K$, de norme absolue égal à $N_{K/\mathbb{Q}}(\mathfrak{p}_1) = 5$.
La partie principale du $(5,\varphi_2)-$polygone de $f(X)$ est formé d'un seul côté reliant les points $(0,0)$ et $(1,1)$ il lui seul est associé le polynôme $G_2(Y) = Y+1$ qui est séparable $modulo 5$. Alors $\mathfrak{a}_2 = \mathfrak{p}_2$ est un idéal premier no nul de $\mathcal{O}_K$ , de norme absolue égal à $N_{K/\mathbb{Q}}(\mathfrak{p}_2) = 25$.
Par conséquent, $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ avec :

$$\left[\mathcal{O}_K/\mathfrak{p}_1 : \mathbb{F}_5\right] = 1 \text{ et } \left[\mathcal{O}_K/\mathfrak{p}_2 : \mathbb{F}_5\right] = 2$$

où $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont des idéaux premiers distincts .

# Chapitre 3

# Etude de la ramification des corps de degré 8

## 3.1 Rappels et Notations

### 3.1.1 Hypothèse de Reimann généralisée ( GRH)

Considérons la fonction zêta de Dedekind attachée à un corps de nombres $K$ de degré $n$ définie pour $s \in \mathbb{C}$ et $Re\,(s) > 1$ par :

$$\zeta_K\,(s) = \sum_{\mathfrak{a}} \frac{1}{N_{K/\mathbb{Q}}\,(\mathfrak{a})^s}$$

où la sommation est étendue à tout les idéaux entiers non nuls $\mathfrak{a}$ de $K$. La famille du deuxième membre est sommable et on a le produit eulérien :

$$\zeta_K\,(s) = \prod_{\wp} \frac{1}{1 - \frac{1}{N_{K/\mathbb{Q}}(\wp)^s}}$$

où produit s'étend à tous les idéaux premiers non nuls $\wp$ du corps de nombres $K$.
L'hypothèse de Riemann généralisée notée en abrégé GRH affirme que :
tous les zéros non triviaux $s = \sigma + i\beta$ ( s'ils existent ) de la fonction $\zeta_K\,(s)$ tels que $0 < \sigma < 1$, sont situés sur la droite critique $\sigma = \frac{1}{2}$.

**Théorème 3.1** *Soit $K$ un corps de nombres de degré $n$ et de discriminant $d_K$. Sous GRH, on a :*

$$\frac{1}{n}log\left|d_K\right| \geq \left(\gamma + log8\pi + \frac{r_1}{n}\frac{\pi}{2} - \frac{2\pi^2\left(\lambda\left(3\right) + \frac{r_1}{n}\beta\left(3\right)\right)}{\left(log\, n\right)^2} - \frac{16\pi^2\left(1+\frac{1}{n}\right)}{\left(log\, n\right)^3\left(1+\frac{\pi^2}{(log\, n)^2}\right)^2}\right)$$

*où $\gamma = 0,5772156649...$ est la constante d'euler, $\lambda\left(3\right) = 1,0517997902...$,$\beta\left(3\right) = 0,9689461462...$, et $r_1$ est le nombre de places réelles du corps de nombres $K$.*

Sachant qu'une meilleure minoration ( en valeur absolue ) du discriminant d'un corps de nombres de degré $n$ pair est obtenue pour un corps totalement imaginaire, l'inégalité précédente donne alors :

$$\frac{1}{n}log\left|d_K\right| \geq \left(\gamma + log8\pi - \frac{2\pi^2\lambda\left(3\right)}{\left(log\, n\right)^2} - \frac{16\pi^2\left(1+\frac{1}{n}\right)}{\left(log\, n\right)^3\left(1+\frac{\pi^2}{(log\, n)^2}\right)^2}\right)$$

Dans le cas d'un corps de nombres de degré $n$ impair, on a la minoration suivant pour $r_1 = 1$

$$\frac{1}{n}log\left|d_K\right| \geq \left(\gamma + log8\pi + \frac{\pi}{2n} - \frac{2\pi^2\left(\lambda\left(3\right) + \frac{r_1}{n}\beta\left(3\right)\right)}{\left(log\, n\right)^2} - \frac{16\pi^2\left(1+\frac{1}{n}\right)}{\left(log\, n\right)^3\left(1+\frac{\pi^2}{(log\, n)^2}\right)^2}\right)$$

### 3.1.2 Minoration des valeurs absolues des discriminants d'un corps de nombres de degré 8

Le tableau suivant établis par Diaz y Diaz dans [9] donnent des minorations des valeurs absolues des discriminant des corps de nombres de degré 8 en fonction de leurs signatures $(r_1, r_2)$ où $r_1 + 2r_2 = 8$. Ces résultats de façon inconditionnelle ( sans GRH), ne tiennent pas compte non plus de la contribution des idéaux premiers non nule de petite norme des corps.

| Signateures | $(8,0)$ | $(6,1)$ | $(4,2)$ | $(2,3)$ | $(0,4)$ |
|---|---|---|---|---|---|
| Minorations | 158960873 | 42071532 | 11660853 | 3403708 | 1052302 |

Des travaux plus avancés du même auteur dans [8] ont montré que la valeur minimale du discriminant d'un corps de nombres totalement imaginaire en degré 8 est 1257728. Sachant que la plus petite valeur en valeur absolue du discriminant d'un corps de nombres de degré $n$ pair est obtenue dans le cas totalement imaginaire, on en déduit alors que la valeur précédente est le minima du discriminant d'un corps de nombres octique, Le corps donnant ce minima est imprimitif ( i.e contenant un sous- corps ) , c'est une extension quartique du corps quadratique $\mathbb{Q}(i)$.

### 3.1.3 Les travaux de Dedekind et de Ore

Soit $K$ un corps de nombres de degré $n$, de discriminant $d_K$, $\mathcal{O}_K$ l'anneau des entiers de $K$ et $p$ un nombre premier. L'idéal $p\mathcal{O}_K$ engendré par le nombre premier $p$ dans $\mathcal{O}_K$ se décompose de la façon suivant :

$$p\mathcal{O}_K = \prod_{\wp|p} \wp^{e_\wp} \tag{3.1}$$

Où le produit s'étend aux idéaux premiers $\wp$ de $\mathcal{O}_K$ au-dessus de $p$, $e_\wp$ est l'indice de ramification de $\wp$ dans $K/\mathbb{Q}$, $f_\wp$ le degré résiduel, et on a $\sum_{\wp|p} e_\wp f_\wp = n$ , et $N(\wp) = p^{f_\wp}$. Le corps $K$ est ramifié en $p$ si et seulement si $p$ divise $d_K$. Dedekind montre que la valuation en $p$ du discriminant $d_K$ du corps de nombres $K$, notée $v_p(d_K)$ dépend de la relation (3.1), et, de plus si le corps de nombres est modérement ramifié en $p$ ( i.e pour tout $\wp|p$ on a $p \nmid e_\wp$) alors on a :

$$v_p(d_K) = \sum_{\wp|p} f_\wp (e_\wp - 1).$$

Ore traite le cas général, c'est-à-dire le cas modérement ramifié et le cas sauvagement ramifié à travers le théorème suivant :

**Théorème 3.2** *(Ore)*

*Avec les notations précédentes, si $K$ est ramifié en $p$ on a :*

$$v_p(d_K) \leq \sum_{\wp|p} f_\wp (e_\wp + e_\wp v_p(e_\wp) - 1). \tag{3.2}$$

*où la somme s'étend au idéaux premiers $\wp$ de $\mathcal{O}_K$ au-dessus de $p$.*
*Plus précisement en posant $n = \sum_{i=0}^{q} b_i p^i$ avec $0 \leq b_i < p$ et $b_q \neq 0$, le développement $p-$adique de $n$, on a :*

1. *La valeur maximale possible de $v_p(d_K)$, notée $N_{n,p}$ est donnée par :*

$$N_{n,p} = \sum_{i=0}^{q} b_i (i+1) p^i - h$$

*où $h$ désigne le nombre de coefficients $b_i$ non nuls.*

2. *Si $p$ est impair, alors $v_p(d_K)$ peut prendre toutes les valeurs comprises entre $0$ et $N_{n,p}$ à l'exception de $\alpha p^\alpha - 1$ pour $n = p^\alpha, \alpha \geq 1$ ou pour $n = p^\alpha + 1$ avec $\alpha \geq 2$.*
3. *Si $p = 2$ le résultat est le même qu'en $2)$avec en plus $v_p(d_K) \neq 1$. Les résultats ci-dessus sont essentiel dans le cas où le nombre premier $p$ considéré est infèrieur au degré $n$ du corps de nombres. Dans la cas $p > n$ , on a le corollaire plus simple .*

**Corollaire 3.1** *Si $p > n$ alors les valeurs possible de $v_p(d_K)$sont comprises entre $0$ et $n-1$. De plus si $f_\wp = 1$ pour tout $\wp|p$, alors $v_p(d_K) = n - j$, où $j$ est le nombre d' idéaux $\wp$ au dessus de $p$.*

**Preuve :**
En effet si $p > n$ alors le dévelopement $p-$adique de $n$ donne $n = b_0 p^0$ avec $b_0 = n$, et donc $N_{n,p} = n - 1$. Dans ce cas $v_p(d_K)$ prend ses valeurs dans l'intervalle $[0, n-1]$.
La condition $p > n$ implique que le corps de nombres est modérement ramifié en $p$ et si $f_\wp = 1$ pour tout $\wp|p$, dans ce cas , d'aprés les travaux de Dedekind , on a $v_p(d_K) = n - j$ où $j$ est le nombre d'idéaux premiers $\wp|p$ tel que $1 \leq j \leq n$.

Dans toute la suite, on désigne par $K$ un corps de nombres de degré 8, $L$ sa clôture galoisienne, $\mathcal{O}_K$ ( resp. $\mathcal{O}_L$) l'anneau des entiers de $K$ ( resp. de $L$) et $d_K$ (resp. $d_L$) le discriminant de $K$ (resp. de $L$).

**Proposition 3.1** *Les corps $K$ et $L$ sont ramifiés en les mêmes premiers $p$ .*

**Preuve :**

Si $K$ est ramifié en un premier $p$ alors il en est de même dans sa clôture galoisienne $L$.

Réciproquement si $L$ est ramifié en un premier $p$, nous allons montrer par l'absurde que $K$ ne peut être non ramifié en ce premier. Supposons donc $L$ ramifié en $p$ et $K$ non ramifié.

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \wp \\ | & | \\ \mathbb{Q} & p \end{array}$$

Le corps $L$ étant galoisien et ramifié en $p$, on a alors la décomposition $p\mathcal{O}_L = \prod_{\mathfrak{P}|p} \mathfrak{P}^e$ où le produit s'etend aux idéaux premiers $\mathfrak{P}$ de $\mathcal{O}_L$ au-dessus du nombre premier $p$. Le corps $K$ étant non ramifié en $p$ alors il est non ramifié en tout idéal premier $\wp$ de $\mathcal{O}_K$ au-dessus de $p$ ; on a donc la décomposition suivante $p\mathcal{O}_K = \prod_{\wp|p} \wp$ . Pour chaque $\mathfrak{P}$ au-dessus de $p$, il existe $\wp$ au-dessus de $p$ tel que $\mathfrak{P}$ soit au-dessus de $\wp$ ; de plus pour tout $\wp|p$, on a $\wp\mathcal{O}_L = \prod_{\mathfrak{P}|\wp} \mathfrak{P}^e$. Pour chaque $\mathfrak{P}|p$ fixé, notons $K_{\mathfrak{P}}$ la sous-extension maximale de $L$ non ramifiée en $\mathfrak{P}$. On a $K \subset K_{\mathfrak{P}}$ et par suite $K \subset \cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$. Le corps $\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$ est une extension galoisienne de $\mathbb{Q}$ contenant $K$.

En effet pour tout $\sigma \in Gal\,(L/K)$, on a $\sigma\left(\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}\right) = \cap_{\sigma(\mathfrak{P}|p)} K_{\sigma(\mathfrak{P})} = \cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$ .

Comme $L$ est la plus petite extension galoisienne de $\mathbb{Q}$ contenant $K$ alors $L \subseteq \cap_{\beta|p} K_{\mathfrak{P}}$.

Mais le corps $\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$ n'étant ramifié en aucun $\mathfrak{P}|p$, et donc non ramifié en $p$, ce qui implique que son sous-corps $L$ et non ramifié en $p$. Ceci est impossible.

**Proposition 3.2** *Les corps $K$ et $L$ sont sauvagement ramifiés en les mêmes nombres premiers $p$.*

**Preuve :**

Si $K$ est sauvagement ramifié en $p$ alors il est de même pour sa clôture galoisienne $L$.

Supposons maintenant $L$ sauvagement ramifié en un premier $p$ et $K$ modérement ramifié.

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \wp \\ | & | \\ \mathbb{Q} & p \end{array}$$

On a les décomposition suivantes :

$p\mathcal{O}_L = \prod_{\mathfrak{P}|p} \mathfrak{P}^e$ où $p$ divise l'indice de ramification $e$ et $p\mathcal{O}_K = \prod_{\wp|p} \wp^{e_\wp}$ où $p$ ne divise aucun indice de ramification $e_\wp$ des idéaux $\wp$ au-dessus de $p$.

Pour chaque $\mathfrak{P}|p$ fixé, on note $L_\mathfrak{P}$ la sous-extension maximale de $L$ modérement ramifiée en $\mathfrak{P}$. On montre que le corps $\cap_{\mathfrak{P}|p} L_\mathfrak{P}$ est une extension galoisienne de $\mathbb{Q}$ contenant $K$. Comme cette extension est modérement ramifié en $p$. Cette situation contredit donc notre hypothèse de départ.

## 3.2 Etude de la ramification des corps de degré 8

### 3.2.1 Ramification en $p = 2$

**Proposition 3.3** *Si le corps $K$ est ramifié seulement en 2, alors il est sauvagement ramifié.*

**Preuve :**

Supposons $K$ modérement ramifié en 2 ; la relation (3.2) du théorème 3.2 de Ore donne :

$$v_2(d_K) \leq 8 - \sum_{\wp|2} f_\wp$$

Le corps $K$ étant modérement ramifié en 2, il y a au moins deux idéaux $\wp|2$. On a alors $v_2(d_K) \leq 6$. Le calcul donne $|d_K| < 1257728$, ce qui est en contradition avec la valeur minimale ( en valeur absolue ) du discriminant d'un corps de nombre de degré 8.

**Corollaire 3.2** *Si la clôture galoisienne $L$ est ramifiée seulement en 2 alors le corps $K$ l'est sauvagement.*

**Preuve :**

Le corps $K$ étant un sous-corps de la clôture galoisienne $L$, si $L$ est ramifiée seulement en 2 alors il en est de même du corps $K$. On conclut d'après la proposition précèdente.

Notons que le calcul par la méthode de Ore donne comme valeur maximale de la valuation $v_2(d_K)$ la valeur :

$N_{8,2} = \sum_{i=0}^{3} b_i(i+1) - 1$( car $8 = 2^3$donc $q = 3$ et $h = 1$) donc :

$N_{8,2} = 4(2)^3 - 1 = 31$ .

On en déduit donc que $|d_K| \leq 2^{31}$.

Cette valeur est atteinte pour la décomposition suivante :

$$2\mathcal{O}_K = \wp^8$$

c'est à dire pour $K$ totalement ramifié en 2.

Voyons ce qu'il en est du type de ramification du corps $L$ grâce au corollaire suivant qui découle des propositions 3.2 et 3.3.

**Corollaire 3.3** *Si le corps $L$ est ramifié seulement en 2 alors il est sauvagement ramifié.*

Le type de ramification étant connu aussi bien pour le corps $K$ que pour le corps $L$, nous allons maintenant déterminer les différentes décopositions de l'idéal $2\mathcal{O}_K$ engendré par 2 dans l'anneau $\mathcal{O}_K$.

**Théorème 3.3** *Si le corps $K$ est ramifié seulement en 2, alors les seules décompositions possibles de l'idéal engendré par 2 dans l'anneau $\mathcal{O}_K$sont : $2\mathcal{O}_K = \wp^8$ ,$2\mathcal{O}_K = \wp_1^4\wp_2^4$ et $2\mathcal{O}_K = \wp^4$,ou le degré résiduel est égal à 1 dans les deux premieres décompositions et à 2 dans la dernière.*

**Preuve :**

Le corps $K$ étant ramifié seulement en 2 on sait d'après ce qui précède qu'il est sauvagement ramifié. Voyons parmi les différentes décompositions de

$$2\mathcal{O}_K = \prod_{\wp|2} \wp^{e_\wp} \text{avec } \sum_{\wp|2} e_\wp f_\wp = 8$$

celles qui donnent la plus grande valeur de $v_2(d_K)$.

1) **Si** $v_2(e_\wp) = 0$ **ou** 1**pour tuot** $\wp \mid 2$ **:**

1.1 **Si** $f_\wp = 1$ **pour tout** $\wp \mid 2$ **:**

la décomposition donnant la plus grande valeur de $v_2(d_K)$ dans ce cas est :

$$2\mathcal{O}_K = \wp_1^6 \wp_2^2$$

La calcul à partir de la relation (3.2) du théorème de Ore donne :

$v_2(d_K) \leq 8+6\times1+2\times1-2$ donc $v_2(d_K) \leq 14$ . Ce cas est impossible car $2^{14} < 1257728$.

1.2 **S'il existe un** $\wp|2$ **tel que** $f_\wp \geq 2$ **:**

La décomposition donnant la plus grande valeur de $v_2(d_K)$ est :

$$2\mathcal{O}_K = \wp_1 \wp_2^6$$

avec $f_1 = 2$ et $f_2 = 1$.

La calcul donne $v_2(d_K) \leq 13$ . Ce cas est impossible pour la même raison

que précédemment.

2) **S'il existe** $\wp|2$ **tel que** $v_2(e_\wp) = 2$ **:**

2.1 **Si** $f_\wp = 1$**pour tout** $\wp|2$ **:**

La plus grande valeur de $v_2(d_K)$ est atteinte par la décomposition :

$$2\mathcal{O}_K = \wp_1^4 \wp_2^4$$

et on a $v_2(d_K) \leq 22$ . Ce cas est possible car $2^{22} > 1257728$.

2.2 **S'il existe** $\wp|2$ **tel que** $f_\wp = 2$ **:**

La décomposition donnant la plus grande valeur de $v_2(d_K)$ est :

$$2\mathcal{O}_K = \wp^4$$

avec $f_\wp = 2$. Le calcul donne $v_2(d_K) \leq 22$. Ce cas est possible car $2^{22} > 1257728$.

3) **S'il existe** $\wp|2$ **tel que** $v_2(e_\wp) = 3$ **:**

La seule décomposition possible est alors :

$$2\mathcal{O}_K = \wp^8$$

et on a $v_2(d_K) \leq 31$. Ce cas est possible car $2^{31} > 1257728$.

**Remarque :** Nous voyons bien à travers ce théorème que si le corps de nombres $K$est ramifié seulement en 2 alors il contient des idéaux premiers de norme 2 ou des idéaux premiers de norme 4.

Déterminons maintenant les valeurs possibles du discriminant $d_K$ dans le cas où $K$ est ramifié seulement en 2.

**Théorème 3.4** *Si le corps $K$ est ramifié seulement en 2 alors les valeurs possibles prises par le discriminant $d_K$ appartiennent à l'ensemble :*

$$\left\{\pm 2^{21}, \pm 2^{22}, \pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}, \pm 2^{31}\right\}.$$

**Preuve :**

En calculant la plus grande puissance de 2 divisant $d_K$ par la méthode de Ore, on obtient $N_{8,2} = 31$. Le résultat s'ensuit en utilisant le 3) du théorème de Ore donnant les valeurs possible de $v_2(d_K)$, et en remarquant que $2^{20} < 1257728 < 2^{21}$. Le théorème de Stickelberger ($d_K \equiv 0, 1\,(mod 4)$) ne permet pas ici d'avoir des renseignements supplémentaires sur le signe de $d_K$.

### 3.2.2 Ramification en $p = 3$

Nous allons montrer dans ce paragraphe que le corps $K$ et sa clôture galoisienne $L$ ne peuvent être ramifiés seulement en 3.

**Proposition 3.4** *Le corps de nombres $K$ ne peut être ramifié seulement en* 3.

**Preuve :**

Si $K$ est ramifié seulement en 3, on a $N_{8,3} = 12$ d'aprés le théorème de Ore. On en déduit que

$$|d_K| \leq 3^{12} < 1257728.$$

Ceci est impossible.

Nous avons le corollaire suivant qui découle de la proposition précédente et de celle vue en 3.1.

**Corollaire 3.4** *le corps $L$ ne peut être ramifié seulement en* 3.

### 3.2.3 Ramification en $p = 5$

En utilisant la méthode de Ore décrite dans le paragraphe 3.1 et le fait que : $8 = 3 \times 5^0 + 1 \times 5$, on a $N_{8,5} = 3 \times 1 + 1 \times 2 + 2 \times 5 - 2 = 11$. On en déduit donc que $|d_K| \leq 5^{11}$.

Ce résultat ne permet pas a priori de savoir si la ramification seulement en 5 du corps $K$ est possible . Nous montrerons, en supposant vérifiée l'hypothèse de Riemann générallisée (GRH ), que ni le corps $L$, ni le corps $K$ ne peuvent être ramifiés seulement en 5.

Tout d'abord commençons par démontrer que la la ramification modérée seulement en 5 n'est possible ni pour le corps $K$ ni pour le corps $L$.

**Proposition 3.5** *Si le corps $K$ ramifié seulement en* 5 *alors il ne peut l'être modérement.*

**Preuve :**

supposons $K$ modérément ramifié en 5 alors la relation (3.2) du théorème de Ore donne :

$$v_5(d_K) \leq 8 - \sum_{\wp|5} f_\wp \leq 7$$

D'où

$$|d_K| \leq 5^7 < 1257728$$

Ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres $K$ de degré 8 ne peut vérifier de cette inégalité.

**Corollaire 3.5** *Si $L$ est ramifié seulement en 5 alors il ne peut l'être modérement.*

**Preuve :** ce résultat découle des praposition 3.2 et 3.5 .

**Ramification sous GRH :**

**Proposition 3.6** *Sous GRH, le corps $L$ ne peut être ramifié seulement en 5.*

Avant de démontrer cette proposition, voyons d'abord le lemme suivant

**Lemme 3.1** *Soient $G_1$ un sous-groupe de $S_8$ engendré par un $5-$cycle et $N_{S_8}(G_1)$ (resp.$N_{A_8}(G_1)$) le normalisateur de $G_1$ dans $S_8$( resp.le groupe alterné $A_8$) . Alors*

*i)* $N_{S_8}(G_1)/G_1 \simeq S_3 \times C_4$

*ii)* $N_{A_8}(G_1)/G_1 \simeq S_3 \times C_2$

**Preuve :**

Notons $\sigma$ le $5-$cycle qui engendre $G_1$, par exemple $\sigma = (1\,2\,3\,4\,5)$( on peut toujours se ramener à ce cas ), $B$ ( resp, $B^C$) le support de $\sigma$ ( resp. le complémentaire de $B$) et $I$ l'ensemble $\{0,1,2,3,4\}$.

Le normalisateur $N_{S_8}(G1)$ de $G_1$ dans $S_8$ est l'ensemble

$$\left\{g \in S_8 |\, \forall i \in I, \exists k \in I |\, g\sigma^i g^{-1} = \sigma^k\right\}$$

On montre que $S_{(B^C)} \simeq S_3$ est contenu dans $N_{S_8}(G_1)$ car pour tout $g \in S_{(B^C)}$, on a $g\sigma g^{-1} = \sigma$.

*i) a)* Montrons d'abord que $N_{S_8}(G_1) \simeq S_3 \times N_{S_5}(G_1)$.

Pour tout $h \in N_{S_8}(G_1)$ on a

$$h(\{1,2,3,4,5\}) = \{1,2,3,4,5\}\, et\, h(\{6,7,8\}) = \{6,7,8\}.$$

En effet soit $h \in N_{S_8}(G_1)$ tel qu'il existe $(i,j) \in \{1,2,3,4,5\} \times \{6,7,8\}$avec $h(i) = j$.

En utilisant le fait que $h\sigma h^{-1} = (h(1)\, h(2)\, h(3)\, h(4)\, h(5))$ ,cela montre que $j$ appartient au $Supp\,(h\sigma h^{-1}) = B$.

Ceci est impossible car pour tout entier $k, j \notin Sopp\left(\sigma^k\right)$.

La restriction de $h$ au cinq premiers symbôles appartient donc au normalisateur de $G_1$ dans $S_5$, noté $N_{S_5}(G_1)$. On peut aussi choisir $h$ librement sur l'nsemble $B^C = \{6, 7, 8\}$.

Considérons le morphisme

$$\begin{array}{ccc} \varphi : N_{S_8}(G_1) & \longrightarrow & S_3 \times N_{S_5}(G_1) \\ h & \longmapsto & (h_1, h_2) \end{array}$$

où $h_1$ est la restriction de $h$ à $B$ et $h_2$ sa restriction à $B^C$.

Le noyau de $\varphi$ est l'ensemble

$$ker\varphi = \{h \in N_{S_8}(G_1) \,|\varphi(h) = (h_1, h_2) = (Id, Id)\} = \{Id\}.$$

Le morphisme $\varphi$ est surjectif car tout $(h_1, h_2) \in S_3 \times N_{S_5}(G_1)$ est l'image par $\varphi$ de $h_1 h_2$.

*b*) Précisons à présent la structure du groupe $N_{S_5}(G_1)$ .

Nous allons montrer que $N_{S_5}(G_1)$ est le groupe $H$ produit semi -direct du sous-groupe distingué $G_1$ par un sous-groupe d'ordre 4. Considérons $s \in S_5$ tel que $s\sigma s^{-1} = \sigma^2$. on en déduit que le $4-$cycle $s = (2\,3\,5\,4)$ convient, et que $s \in N_{S_5}(G_1)$ car pour tout $i \in I$, il existe $j \in I$ etl que $s\sigma^i\sigma^{-1} = \sigma^j$. Le sous-groupe engendré par $s$ est le groupe cyclique $C_4$ d'ordre 4, et on vérifie aussi que $C_4 \cap G_1 = \{Id\}$. Le sous-groupe du $N_{S_5}(G_1)$

engendré par $\sigma$ et $s$ est d'ordre 20 et est égal à $H$. On vérifie que $H$ n'est pas contenu dans $A_5$ ( car il contient la permutation $s$ qui est impaire ). Le groupe $H \cap A_5$ est un sous-groupe pair engendré par $\sigma$ et $s^2$ ( la seule puissance de $s$ qui est pair est $s^2$) .

C'est un sous-groupe diédral d'ordre 10 produit semi-direct de $G_1$ par le sous-groupe engendré par $s^2$ qui est lui-même isomorphe à $C_2$. Comme $H$ est contenu dans $N_{S_5}(G_1)$, on en déduit que $N_{S_5}(G_1) \cap A_5$ contient un sous-groupe d'ordre 10 et que l'ordre de $N_{S_5}(G_1) \cap A_5$ est $10, 20, 30$ ou $60$ ( car contenu dans $A_5$) . Or il n'y a pas de sous-groupe

de $A_5$ d'ordre 20 ou 30 , et si on avait $N_{S_5}(G_1) \cap A_5 = A_5$ alors $G_1$ serait distingué ans $A_5$; cela est impossible car $A_5$ est simple. d'où $N_{S_5}(G_1) \cap A_5 = H \cap A_5$.
Comme $N_{S_5}(G_1)$ contient le groupe $H$ d'ordre 20 et que l'ordre d'un sous-groupe de $S_5$ est 5, $10, 20, 60$ ou 120 ; on vérifie alors que la seule possibilité est que l'ordre de $N_{S_5}(G_1)$est 20. On a donc $N_{S_5}(G_1) = H = G_1 \times C_4$. Le résultat s'ensuit en utilisant le fait que

$$N_{S_8}(G_1) \simeq S_3 \times (G_1 \rtimes C_4)$$

et en quotientant par le sous-groupe $G_1$.

*ii*) Le groupe $N_{A_8}(G_1)$ est égal à $N_{S_8}(G_1) \cap A_8$. On montre comme précédemment que $N_{A_8}(G_1) \simeq S_3 \times N_{A_5}(G_1)$ . Le groupe $N_{A_5}(G_1)$ est un sous-groupe de $A_5$ engendré par $\sigma$ et $s^2$. On vérifié que c'est un sous-groupe diédral d'ordre 10 produit semi-direct du sous-groupe distingué $G_1$ par le sous-groupe engendré par $s^2$qui est lui -même isomorphe à $C_2$. Le résultat s'ensuit en utillisant le fait que

$$N_{A_8}(G_1) \simeq S_3 \times (G_1 \rtimes C_2)$$

et en quotientant par le sous-groupe $G_1$.

**Preuve de la proposition** 3.6 **:** Si le corps $L$ est ramifié seulement en 5 alors d'aprés la proposition précédente il ne peut l'être que sauvagement .

Supposons $L$ sauvagement ramifié en 5 ; le groupe $G = Gal(L/\mathbb{Q})$ est un sous-groupe transitif de $T_{50}$ suivant la numérotation de Butler et Mckay . L'extension $L/\mathbb{Q}$ étant galoisienne on a :

$$5\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^e$$

où les $\mathfrak{P}_i$ sont les idéaux premiers de $\mathcal{O}_L$ au-dessus de 5 avec $|G| = efg$ et 5 divise $|G|$ ( car 5 divise $e$ et $e$ divise $|G|$). Comme 5 est sauvagement ramifié dans $L$ et que 25 ne divise pas $|T_{50}|$ alors $v_5(e) = 1$. La relation

$$|G| = [L : \mathbb{Q}] = [L : K]\,[K : \mathbb{Q}] = 8\,[L : K]$$

montre que 8 divise $|G|$. On en déduit que 40 divise $|G|$( car $(8, 5) = 1$), et donc $G = T_{50}$ ou $T_{49}^{+}$.

Désignons par $G_0$ le groupe d'nertie et par $G_1$ le premier groupe de ramification d'un idéal premier $\mathfrak{P}$ de l'anneau $\mathcal{O}_L$ au-dessus du nombre premier 5. D'après le théorème 2.11, $G_1$ est un $5-$sous-groupe distingué non trivial de $G_0$ tel que $G_0/G_1$ est cyclique d'ordre premier à 5. Comme $|G_1| = 5^r$ ( où l'entier $r \geq 1$) divise $|G_0| = e$ et que $e$ divise $|G|$ alors $|G_1|$ divise $|G|$, et par suite $r = 1$ car la plus grande puissance de 5 qui divise $|T_{50}|$ ou $\left|T_{49}^{+}\right|$est 5. D'où $|G_1| = 5$.

Nous allons étudier séparément le cas où $G = T_{50}$ et celui où $G = T_{49}^{+}$.

1. Si $G = T_{50}$ : on note $N_{T_{50}}(G_1)$ le normalisateur de $G_1$ dans $T_{50}$. Comme $G_1 \lhd G_0$ et que $N_{T_{50}}(G_1)$ est le plus grand sous-groupe de $T_{50}$ dans lequel $G_1$ distingué , alors $G_0$ est une sous-groupe de $N_{T50}(G_1)$ car $G_0 = N_{G_0}(G_1) \subseteq N_{T_{50}}(G_1)$. On en déduit donc que $|G_0| = e$ divise $|N_{T_{50}}(G_1)|$. Or d'après le lemme précédent le cardinal du normalisateur d'un $5-$cycle dans $T_{50}$ est 120. Mais si $e = 120$ alors $G_0 = N_{T_{50}}(G_1)$ ,et dans ce cas $G_0/G_1 = N_{T_{50}}(G_1)/G_1$ n'est pas cyclique . Ce cas est impossible .On a donc $G_0 \subset N_{T_{50}}$ et $e|60$.
2. Si $G = T_{49}^{+}$ : on note $N_{T_{49}^{+}}(G_1)$ le normalisateur de $G_1$ dans $T_{49}^{+}$. D'après le lemme précedent , le cardinal du normalisateur d'un $5-$cycle dans $T_{49}^{+}$ est 60. On montre comme précédemment que $G_0$ est un sous-groupe de $N_{T_{49}^{+}}(G_1)$ ; on en déduit donc que $|G_0|$divise $\left|N_{T_{49}^{+}}(G_1)\right| = 60$.

Dans les deux cas l'indice de ramification $e$ divise 60 et $v_5(e) = 1$. En utilisant la relation (3.2) du théorème de Ore pour une extension galoisienne , on a :

$$v_5(d_L) \leq f(e + e - 1)\,g = f(2e - 1)\,g = |G|(2 - 1/e) \;et\; \frac{1}{60} \leq \frac{1}{e} \leq \frac{1}{5}.$$

Comme

$$\frac{9}{5} \leq 2 - \frac{1}{e} \leq \frac{119}{60}.$$

On en déduit

$$|d_L|^{1/|G|} \leq 5^{\frac{119}{60}} \approx 24,338.$$

Supposons que l'hypothèse de Reimann généralisée soit vraie pour la fonction zêta de Dedekind du corps $L$. On peut, dans ces condition, améliorer sensiblement les minorations de discriminants avec correction locales . La relation (2)du paragraphe 3.1 donne alors :

$$\frac{1}{|G|} log\,|d_L| \geq \left( 3,801 - \frac{20,766}{(log\,|G|)^2} - \frac{157,914\,(1+1/\,|G|)}{(log\,|G|)^3\left(1+\frac{\pi^2}{(log|G|)^2}\right)^2} \right).$$

On obtient :

Si $G = T_{50}$ alors $|d_L|^{(1/|T_{50}|)} \geq 33,248$.

Si $G = T_{49}^{+}$ alors $|d_L|^{\left(1/|T_{49}^{+}|\right)} \geq 31,678$.

Ces deux résultats sont en contradition avec la majoration précédente.

**Corollaire 3.6** *Sous GRH le corps $K$ ne peut être ramifié seulement en* 5.

**Ramification sans GRH :** De façon inconditionnelle ( sans GRH ) , on obtient les résultats suivants

**Proposition 3.7** *Si $K$ est ramifié seulement en* 5 *alors il l'est sauvagement . De plus les différentes décompositions possibles de l'idéal engendré par* 5 *dans $\mathcal{O}_K$ sont de la forme :*

1. $5\mathcal{O}_K = \wp_1^5\wp_2^3$ *avec* $f_1 = f_2 = 1$.
2. $5\mathcal{O}_K = \wp_1^5\wp_2^2\wp_3$ *avec* $f_1 = f_2 = f_3 = 1$.
3. $5\mathcal{O}_K = \wp_1^5\wp_2\wp_3$ *avec* $f_1 = f_2 = 1$ *et* $f_3 = 2$.
4. $5\mathcal{O}_K = \wp_1^5\wp_2\wp_3\wp_4$ *avec* $f_1 = f_2 = f_3 = f_4 = 1$.
5. $5\mathcal{O}_K = \wp_1^5\wp_2$ *avec* $f_1 = 1$ *et* $f_2 = 3$.

*Déterminons maintenant grâce à la proposition qui suit les différentes valeurs possibles du disriminant.*

**Proposition 3.8** *Si $K$ est ramifié seulement en* 5 *alors le discriminant $d_K$ appartient à l'ensemble*

$$\left\{5^9, 5^{10}, 5^{11}\right\}.$$

**Preuve :**

Le calcul de la plus grande puissance de 5 divisant $d_K$par la méthode de Ore donne $N_{8,5} = 11$. Le résultat s'ensuit en utilisant le théorème de Stickelberger $(d_K \equiv 0, 1\,(mod 4))$et le fait que $|d_K| \geq 1257728$.

### 3.2.4 Ramification en $p = 7$

Nous allons étudier maintenant le dernier cas de ramification , soit en $p = 7$. Nous terminerons ce paragraphe en donnant les différentes valeurs possible du discriminant $d_K$.

**Proposition 3.9** *Si le corps $K$ est ramifié seulement en* 7 *alors il est sauvagement ramifié.*

**Preuve :**

Supposons $K$ modérement ramifié en 7 alors la relation (3.2)du théorème 3.2de Ore permet d'écrire :

$$v_7(d_K) \leq 8 - \sum_{\wp|7} f_\wp \leq 7$$

et donc

$$|d_K| \leq 7^7 < 1257728$$

ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres de degré 8 ne peut vérifier de telle inégalité.

**Corollaire 3.7** *Si $L$ est ramifié seulement en* 7 *alors il est sauvagement ramifié.*

**Corollaire 3.8** *Si $L$ est ramifié seulement en* 7 *alors la sous-corps $K$ est sauvagement ramifié en* 7.

**Preuve :**

Si $L$ est ramifié seulement en 7 alors le sous-corps$K$ est aussi ramifié seulement en 7. Le résultat découle de ce qui précède .

Voyons comment se décompose l'idéal $7\mathcal{O}_K$ engendré par le nombre premier 7 dans cas où la ramification en 7 est possible.

**Théorème 3.5** *Si le corps $K$ est ramifié seulement en 7 alors la seule décomposition possible de l'idéal engendré par 7 dans l'anneau $\mathcal{O}_K$ est de la forme :*

$$7\mathcal{O}_K = \wp_1^7 \wp_2.$$

*où $f_1 = f_2 = 1$.*

**Preuve :**

D'après les résultats qui précédent, on sait que si le corps $K$ est ramifié seulement en 7 alors il l'est sauvagement . La décomposition :

$$7\mathcal{O}_K = \wp_1^7 \wp_2$$

est alors évidente.

**Théorème 3.6** *Si le corps $K$ est ramifié seulement en 7 alors le discriminant $d_K$ prend ses valeurs dans l'ensemble suivant :*

$$\left\{7^8, -7^9, 7^{10}, -7^{11}, 7^{12}, -7^{13}\right\}.$$

**Preuve :**

Le corps $K$ étant ramifié seulement en 7, on sait qu'il l'est sauvagement. En appliquant la méthode de calcul de Ore , on a $N_{8,7} = 13$. On en déduit $|d_K| \leq 7^{13}$.
Le corps $K$ étant ramifié seulement en 7, on a $d_K = \pm 7^s$ avec $s \in \mathbb{N} - \{0\}$ .Comme $7^7 < 1257728 < 7^8$ alors les valeurs possibles de $|d_K| = 7^s$ sont les suivantes :

$$7^8, 7^9, 7^{10}, 7^{11}, 7^{12}, 7^{13}.$$

En utilisant le théorème de Stickelberger ($d_K \equiv 0, 1\,(mod 4)$) et le fait que $7 \equiv -1\,(mod 4)$ alors on a $d_K \equiv 1\,(mod 4)$ .Deux cas présentent en fonction de la parité de $s$ :

1. Pour $s$ pair : $d_K = 7^s$.

   En effet , si $d_K = -7^s$ alors $d_K \equiv -1\,(mod 4)$ , ce qui est impossible.

2. Pour $s$ impair : $d_K = -7^s$.

   En effet , si $d_K = 7^s$ alors $d_K \equiv -1\,(mod 4)$ , ce qui est impossible.

# Bibliographie


[1] S. Alaca and K. Williams, Introductory algebraic number theory, Cambridge university Press, New York.

[2] Y.AMICE, Les nombres $p$-adiques. PUF, 1ère Edition, 1975.

[3] B. BENSEBAA, Groupe de Galois de trinomes. Thèse de Doctorat d'Etat, USTHB, décembre 2008.

[4] Z. BOREVITCH, Théorie des nombres. Gauthier villard, ed . 1967.

[5] J.W.S.CASSELS, Local Fields, Cambridge university Press. Press 1986.

[6] H.Cohen, F. Diaz et M. Olivier, Imprimitive octic fields with small discriminants. Université Bordeaux1, laboratoire $A2X, 351$ cours de la libération, 33405 Talence, France.

[7] S.D.COHEN, A. MOVAHHEDI and A. SALINIER, Factorization over Local Fields and the irreductibility of generalized difference polynomials. J. N. T, 2000.

[8] F.D. Y Diaz, petits discriminants des corps de nombres totalement imaginaires de degré 8. Journal of Number Theory $25, 34 - 52(1987)$.

[9] F.D. Y Diaz, Tables minorant la racine n-ième du discriminant d'un corps de nombres de degré $n$. Publication Mathématiques d'Orsay $80.06, 1980$.

[10] F. Diaz. Y. Diaz , J. Martinet et M. Pahst, The minimum discriminant of totally real octic fields.ournal of Number Theory $36, 145 - 159(1990)$ .

[11] P.ESCOFIER, Théorie de Galois. DUNOD, 2000.

[12] D. Guin et T. Hausberger, Algèbre 1, Groupes, corps et théorie de Galois, COLLECTION ENSEIGNEMENT SUP// Mathématiques.

[13] E. HALLOUIN, Parcours initiatique à travers la théorie des valuations, " Université de Poitiers. Département de matématiques (1997).

[14] R. A. Mollin, Algebraic Number Theory, SECOND EDITION, CRC Press.

[15] P. SAMUEL, Théorie algèbrique des nombres. HERMANN, Paris 1967.

[16] J.P.SERRE, Cours d'arithmétiques. PUF-2nd Edition, Paris, 1977.

[17] J.P.SERRE, corps Locaux. 3ème Edition, HERMANN, 1980.

[18] L. Sylla, Autour d'une conjecture de B. Gross relative à l'existence de corps de nombres de groupe de Galois no résoluble et ramifiés en unique premier $p$ petit, Thèse de Doctorat de Mathématiques pures à l'Université Bordeaux1.2005 .