N° d'ORDRE :03/2012-M/MT

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

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

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER
EN: MATHÉMATIQUES
Spécialité : Algèbre et Théorie des Nombres

par AIT MOHAMED Hocine

Arithmétique des corps cubiques

Soutenu publiquement le 26 Septembre 2012, devant le jury composé de :

Mr BERRACHEDI Abdelhafid	Professeur à l' USTHB	Président:
Mr BENSEBAA Boualem	Maître de Conférences/A, à USTHB	Directeur de Mémoire
Mr BENCHERIF Farid	Maître de Conférences/A, à l' USTHB	Examinateur
Mme CHERCHEM Leïla	Maître de Conférences/A, à l' USTHB	Examinateur
Mr BOUCHENNA Rachid	Maître Assistant/A, à l' USTHB	Invité

Remerciements

Tout d'abord je veux exprimer tout mes remerciements à celles et ceux qui, de près ou de loin, ont contribué à la réalisation de cet humble travail, qui j'espère constituera une contribution du travail de recherche dans le domaine de la théorie algébrique des nombres.

Précisément, je voudrais exprimer ma plus vive reconnaissance à mon directeur de mémoire, Monsieur Boualem BENSEBA, qui n'a pas cessé de m'aider et m'encourager dans cette oeuvre.

Mes remerciement vont aussi à l'endroit du Professeur Abdelhafid BERRACHEDI qui a accepté de présider le jury de ma soutenance.

Que Madame Leïla BENFERHAT, Monsieur Farid BENCHERIF et Monsieur Rachid BOUCHENNA trouvent ici l'expression de ma reconnaissance pour avoir participé au jury de ce mémoire et pour leurs remarques pertinents et leurs conseils qui m'ont permis d'enrichir mon travail et d'entrevoir de nouvelles perspectives.

Notations

L, K, M, $N, \ldots$:	Corps de nombres
L/K :	Extension de corps de nombres
$[L : K]$:	Degré de l'extension L/K
$\mathrm{Min}\,(\alpha,\, K, X)$ ou $\mathrm{Irr}\,(\alpha,\, K, X)$:	Le polynôme minimal de α sur K
$\mathrm{Gal}\,(L/K)$:	Groupe de Galois de$L$ sur K
$\mathrm{Gal}\,(P/K)$:	Groupe de Galois dupolynôme$P$ sur K
S_n :	Groupe de permutation de degré n
$\mathcal{O}_K$:	Anneau des entiers du corps K
$\mathrm{disc}\,(f)$:	Le discriminant du polynôme f
$\mathrm{Tr}_{L/K}\,(x)$:	Trace de l'endomorphisme multiplication par x du $K-$automorphisme L
$\det(u)$:	Déterminant de l'endomorphisme u
$P_u\,(X)$:	Polynôme caractéristique de l'endomorphisme$u$
$\mathrm{N}_{B/A}\,(x)$ et $\mathrm{Tr}_{B/A}\,(x)$:	La norme et la trace de$x \in B$ relativement à A
$D\,(x_1, \ldots, x_n)$:	Discriminant du système $\{x_1, \ldots, x_n\}$
d_K :	Discriminant du corps$K$
$\mathcal{D}_{B/A}$:	Idéal discriminant de B sur A
$\wp$, $\mathfrak{b}$, $\mathfrak{p}$, $\mathfrak{q}$:	Idéaux premiers
$\mathrm{N}_{L/K}\,(\wp)$:	Norme sur L/K de l'idéal $\wp$
$k_K = \dfrac{\mathcal{O}_K}{\mathfrak{p}}$:	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 $\mathfrak{p}$
$i\,(\theta) = (\mathcal{O}_K : \mathbb{Z}\,[\theta])$:	Indice du sous-groupe $\mathbb{Z}\,[\theta]$ dans le groupe additif $\mathcal{O}_K$
$\mathbb{Q}_p$:	Corps des nombres p-adiques
$\mathbb{Z}_p$:	Anneau des entiers de $\mathbb{Q}_p$
$\mathfrak{D}\,(E/F)$:	Différente de l'extension E/F
$i\,(K)$:	Indice du corps K,

Table des matières

Introduction

Ce mémoire porte sur la détermination de la décomposition d'un entier rationnel premier p dans un corps cubique de nombres algébriques K (K extension de $\mathbb{Q}$ de degré 3) engendré par une racine θ d'un polynôme de la forme X^3-aX+b avec a et b deux entiers rationnels (voir le théorème 3.1 du chapitre 3).

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. Le discriminant d_K du corps de nombres K est lié au discriminant Δ du polynôme $X^3 - aX + b$ par la relation

$$\Delta = i(\theta)^2 d_K$$

où $i(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]$ est l'indice du groupe $\mathbb{Z}[\theta]$ dans le groupe additif de l'anneau $\mathcal{O}_K$ et $\Delta = 4a^3 - 27b^2$.

Par la théorie de la ramification, les nombres premiers ramifiés sont les diviseurs du discriminant d_K du corps K, donc des diviseurs du discriminant Δ du polynôme $X^3 - aX + b$.

Dedekind montre que cette ramification est déterminée par la factorisation de X^3-aX+b dans $\mathbb{F}_p$ si ce nombre premier p n'est pas un diviseur de l'indice $i(\theta)$. Dans le cas des diviseurs inessentiels du discriminant d_k, c'est à dire que $p \mid i(\theta)$, alors la factorisation de $X^3 - aX + b$ dans $\mathbb{F}_p$ ne reflète pas celle de p dans $\mathcal{O}_K$. Dans tous les cas, l'utilisation de la théorie de Ore sur les $(p-\varphi)$-polygones permet de donner une version locale de la ramification d'un nombre

premier dans une extension $K_{\mathfrak{p}}$ du corps des nombres p-adique $\mathbb{Q}_p$, où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ au dessus de p, en d'autres termes $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

les nombres premiers inessentiels sont en nombre au plus égal à $[K : \mathbb{Q}] - 1$ où $[K : \mathbb{Q}]$ est le degré de l'extension K/Q. Le calcul de la valuation p– adique du discriminant d_K de K par l'application du théorème 3.2 (voir chapitre 3) puis le calcul de d_K par déduction du discriminant d du corps $\mathbb{Q}\left(\sqrt{d}\right)$ à partir de l'écriture de d_K sous la forme

$$d_K = d \times 3^{2m} f^2$$

avec $f = \prod_{i=1}^{s} p_i$, où les p_i sont des nombres premiers distincts vérifiant

$$\mathrm{p\,gcd}(f, 3d) = 1 \text{ et } \left(\frac{d}{p_i}\right) \equiv p_i(\ \mathrm{mod}\ )\, 3$$

pour tout i, $1 \leq i \leq s$,$m \leq 2$ un entier naturel tel que

$$\begin{aligned} &m \neq 1, \quad \text{si } 3 \nmid d \\ &m \neq 2, \quad \text{si } d \equiv 3 \bmod 9 \end{aligned}$$

Ce mémoire se décline suivant 3 chapitres qui donneront, pour les deux premiers un aperçu des notions de théorie algébrique citées ci-dessus, et pour le troisième la décomposition complète d'un nombre premier p dans une extension du corps des nombres rationnels engendrée par une racine du polynôme irréductible $X^3 - aX + b$.

Dans le chapitre 1, nous revisitons les notions de bases de la théorie des extensions. En outre, soit $K/\mathbb{Q}$ un corps de nombres engendrée par une racine θ d'un polynôme unitaire et irréductible $f(X)$ sur $\mathbb{Q}$. Nous définirons les notions de discriminant d_K d'un corps de nombres K ainsi que celui du discriminant $D(f)$ du polynôme f. Cette déterminantion est utile pour cerner les nombres

premiers ramifiés, ce sont exactement les diviseurs de d_K. Par la relation

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

ces derniers sont des diviseurs du discriminant $D(f)$ du polynôme f.
Nous exposerons ensuite 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 chapitre 2, nous étudions les extensions $K_{\mathfrak{p}}/\mathbb{Q}_p$ de corps de nombres p-adiques, où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$ au dessus du nombre premier p. Le principe de localisation-globalisation permet de traduire au niveau global les propriétés obtenues au niveau local. En outre, la ramification au niveau local permet de mettre en évidence une suite de sous-groupes du groupe de Galois de la clôture normale de K sur $\mathbb{Q}$. le critère de Dedekind permet de mettre une passerelle entre des catégories de structures de groupes et la catégorie des entiers que sont les indices de ramification et les degrés résiduels des idéaux premiers ramifiés dans $\mathcal{O}_K$.
Le Théorème de Ore permet de rendre effectif la ramification d'un nombre premier. En outre, nous donnons quelques exemples de ramification d'un nombre premier dans une extension de corps de nombres.

Le chapitre 3 étudie la ramification d'un nombre premier dans l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres cubique K . Ce dernier est engendré par une racine du trinôme $X^3 - aX + b$.
En outre, cette ramification est intimement liée à la nature des entiers a et b. Comme les nombres premiers ramifiés sont des diviseurs du discriminant de ce polynôme, ceux-ci peuvent être en même temps des diviseurs de l'indice $i(\theta)$, un tel nombre premier est appelé diviseur inessentiel. Nous donnons une condition nécessaire et suffisante pour qu'un nombre premier soit un diviseur inessentiel.

Chapitre 1

Extensions de corps

1.1 Notion d'extensions

1.1.1 Définitions et notations

Soit Kun corps commutatif.

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

Exemple 1 *voici quelques exemples d'extensions de corps.*

1. $\mathbb{R}$ *et* $\mathbb{C}$ *sont des extensions de* $\mathbb{Q}$.
2. *L'ensemble* $\left\{a + b\sqrt{3}, \text{ avec } a, b \in \mathbb{Q}\right\}$ *muni des opérations* $+$ *et* $\times$, *addition et multiplication, est une extension de* $\mathbb{Q}$.
3. *Le corps des fractions* $\mathbb{R}(X)$ *de l'anneau des polynômes* $\mathbb{R}[X]$ *à une indéterminée* X *est une extension de* $\mathbb{R}$.

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

Proposition 1.2 *Une extension L d'un corps K est munie d'une structure de K-espace vectoriel.*

Définition 1.3 *La dimension de L comme K espace vectoriel est appeléé degré de l'extension L/K, qu'on note $[L : K]$.*
On dit que l'extension L/K est finie si $[L : K] < +\infty$.

Notations Si $[L : K] = 2$, on dit que l'extension L/K est quadratique
Si $[L : K] = 3$, on dit que l'extension L/K est cubique

Exemple 2 *Nous donnons ici quelques exemples d'extensions de degrés diverss.*

1. $\mathbb{C}/\mathbb{R}$ *est une extension quadratique.*
2. *L'ensemble* $\{a + bj, \text{ avec } a, b \in \mathbb{Q}\}$, *où* $1 \neq j$ *et* $j^3 = 1$, *est une extension quadratique de* $\mathbb{Q}$.
3. *L'ensemble* $\left\{a + b\alpha + c\alpha^2, \text{ avec } a, b, c \in \mathbb{Q} \text{ et } \alpha = \sqrt[3]{2}\right\}$ *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 1.4 *Soit $K \subset L \subset M$ une suite d'extensions.*
Alors M/K est de degré fini si et seulement si M est de degré fini sur L et L est de degré fini sur K et dans ce cas on a

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

Exemple 3 *Soit* $L = \left\{a + b\sqrt{2},\ \text{ avec } a, b \in \mathbb{Q}\right\}$ *et* $M = \{u + vj,\ \text{ avec } u, v \in L \text{ et } j^3 = 1,\ j \neq 1\}$.
Alors $[L : \mathbb{Q}] = 2$ *et* $[M : L] = 2$ *et donc* $[M : \mathbb{Q}] = 4$.
M *est un* $\mathbb{Q}$*-espace vectoriel de dimension 4 dont une base est* $\left\{1,\ \sqrt{2},\ j,\ j\sqrt{2}\right\}$.

La proposition précédente peut être généralisée à une tour de n extensions $K = K_1 \subset K_2 \subset \cdots \subset K_n = M$ et on a

Proposition 1.5 *l'extension* K_n/K *est finie si et seulemnt si ,*
$\forall i,\ 1 \leq i \leq n-1$,*l'extension* K_{i+1}/K_i *est finie et dans ce cas on a*

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

1.1.2 Elément algébrique et polynôme minimal

Définition 1.6 *Soit* L/K *une extension de corps.*
Un élément $\alpha \in L$ *est dit algébrique sur* K *s'il existe un polynôme non nul de* $K[X]$ *ayant* α *comme racine.*

Définition 1.7 *On dit qu'une extension* L/K *est algébrique si tout élément de* L *est algébrique sur* K.

Proposition 1.8 *Soit* L *une extension d'un corps* K *telle que* $L = K(\alpha)$, *où* $\alpha \in L$ *est algébrique sur* K. *Alors l'extension* L *est algébrique sur*K, *et plus généralement* $L = K(A)$ *où* $A = \{\alpha,\ \alpha$*algébrique sur* $\}\ K$

Preuve : 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, alors $\exists \lambda_i \in K$, $0 \leq i \leq n$, 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 $P = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \neq 0$ et entraine que x est algébrique sur K .
Par conséquent tout élément de L est algébrique sur K et donc que L est algébrique sur K.

□

Proposition 1.9 *Toute extension L de degré fini sur K est algébrique sur K.*

Preuve : Soit $x \in L$, alors $K(x)/K$ est une extension de degré fini. Par suite x est algébrique sur K et donc que L est algébrique sur K

□

Définition 1.10 *Soit K un corps, L une extension de K et α un élément de L algébrique sur K.*
L'unique polynôme unitaire P de $K[X]$ de degré minimal s'annulant en α est appelé polynôme minimal de α sur K, on le note $P = Min(\alpha, X, K)$.
Si $\deg P = n$ *on dit que α est de degré n sur K.*

Proposition 1.11 *Soit K un corps, L une extension de K et α un élément de L algébrique sur K de polynôme minimal P sur K. Alors ona les propriétés suivantes :*

1. *tout polynôme de $K[X]$ s'annulant en α est divisible par P ;*
2. *P est irréductible sur K ;*
3. *si $\beta \in L$ tel que $P(\beta) = 0$ alors $Min(\beta, K, X) = P$.*

Preuve : .

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

2. Supposons que P est réductible sur K , alors $P = u.v$ avec $u, v \in K[X]$ tels que $\deg u \geq 1$ et $\deg v \geq 1$ avec $u(\alpha).v(\alpha) \neq 0$, sinon $p \neq \text{Min}(\alpha, K, X)$, ce qui entraine $P(\alpha) \neq 0$ ce qui est absurde.

3. Si $\beta \in L$ et $P(\beta) = 0$, alors $P = \lambda \text{Min}(\beta, K, X)$ avec $\lambda \in K^*$. Puisque P et $\text{Min}(\beta, K, X)$ sont unitaires, alors $\lambda = 1$ et par suite $\text{Min}(\beta, K, X) = P$.

□

Exemple 4 *$(i) X^2-2 \in \mathbb{Q}[X]$, $\sqrt{2}$ est racine de X^2-2 donc $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. D'autre part, $X^2 - 2$ est irréductible sur $\mathbb{Q}$ car $\sqrt{2} \notin \mathbb{Q}$ et $-\sqrt{2} \notin \mathbb{Q}$, alors Min $\left(\sqrt{2}, \mathbb{Q}, X\right) = X^2 - 2$ et $\sqrt{2}$ est de degré 2 sur $\mathbb{Q}$.*

- *Soit $P = X^2+X+1 \in \mathbb{R}[X]$ de racines $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ et $\beta = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Comme α, $\beta \notin \mathbb{R}$, alors X^2+X+1 est irréductible sur $\mathbb{R}$ et donc Min $(\alpha, \mathbb{R}, X) = X^2 + X + 1$ et α de degré 2 sur $\mathbb{R}$.*

- *Soit α une racine de $X^3+X+1 \in \mathbb{Q}[X]$, alors α est algébrique sur $\mathbb{Q}$. On suppose qu'il existe deux entiers $u \in \mathbb{Z}$ et $v \in \mathbb{N}^*$ tels que*

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

, alors $\frac{u}{v} \in \{-1, +1\}$. Or, les nombres -1 et 1 ne sont pas racine 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 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

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

Critère Soit un polynôme $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier.
Si $p \mid a_i$, $0 \leq i \leq n-1$, $p \nmid a_n$ et $p^2 \nmid a_0$ alors $P(X)$ est irréductible sur $\mathbb{Q}$.
On dit alors que le polynôme $P(X)$ est d'Eisenstein en p

Exemple 5 *Considérons les exemples suivants :*

1. *Soit $P(X) = X^3+4X^2-6X+10$ 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 appliquer le critère d'Eisenstein pour ce polynôme. Comme 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 1.12 *Soit K un corps, On appelle clôture algébrique de K 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.*

Définition 1.13 *Soit K un corps, on dit qu'un polynôme $f \in K[X]$ de degré n est séparable sur K s'il admet exactement n racines distinctes dans une clôture algébrique de K.*

Exemple 6 .

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

Les polynômes séparables sont caractérisés par

Proposition 1.14 *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.

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

Corollaire 1.15 *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.*

Exemple 7 *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 $\mathbb{Q}$.

Corollaire 1.16 *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 $f(X) = g(X^p)$.

Définition 1.17 *Soit L/K une extension et $\alpha \in L$ un élément algébrique sur K.*
On dit que α est séparable sur K si son polynôme minimal $Irr(\alpha, K, X)$ est séparable sur K.

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

Définition 1.18 *On dit qu'une extension L/K est séparable sur K si tout élément de L est séparable sur K.*

Théorème 1.19 ***(Téorème 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 $\omega \in L$ tel que $L = K(\omega)$. Dans ce cas ω est appelé élément primitif de L.

Proposition 1.20 *Soit $K \subset L \subset M$ une tour d'extensions de corps de degrés finis. Alors M est séparable sur K si et seulement si M est séparable sur L et L est séparable sur K.*

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

Définition 1.21 *On dit que L est séparable sur K si le polynôme minimal de tout élément $\alpha \in L$, $Irr(\alpha, K, X)$, est séparable sur K*

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.

Exemple 8 .

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. L'extension $\mathbb{Q}\left(\exp\left(\frac{2i\pi}{7}\right)\right)/\mathbb{Q}$ est une extension normale sur $\mathbb{Q}$, puisque l'élément $\alpha = \left(\frac{2i\pi}{7}\right)$ a pour polynôme minimal $\phi(X) = X^6+X^5+X^4+X^3+X^2+X+1$, qui est le 7ème polynôme cyclotomique et qui a pour racines les $\alpha_k = \exp\left(\frac{2ik\pi}{7}\right)$, $0 \leq 1 \leq 6$, qui sont toutes dans $\mathbb{Q}\left(\exp\left(\frac{2i\pi}{7}\right)\right)$.
3. L'extension $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ n'est pas une extension normale car le polynôme minimal de $\alpha = \sqrt[3]{2}$ est X^3-2 admet pour autre racine les nombres complexes non réels αj et αj^2, où $j = \exp\left(\frac{2i\pi}{3}\right)$.

1.2 Extensions galoisiennes

Une des propriétés des extensions normales est donnée par

Théorème 1.22 *Soit L/K une extension de degré fini avec $L \subset \overline{K}$, où $\overline{K}$ est la clôture algébrique de K. Alors les propriétés suivantes sont équivalentes :*

1. *L est normale sur K,*
2. *L est le corps de décomposition d'un polynôme de $K[X]$,*
3. *L est invariant par tout K-homomorphisme injectif de L dans $\overline{K}$*

Définition 1.23 *On dit qu'une extension L/K est galoisienne si elle est à la fois normale et séparable sur K*

Exemple 9 .

1. *Les extensions quadratiques* $\mathbb{Q}\left(\sqrt{d}\right)$ *sur* $\mathbb{Q}$, *d entier sans facteur carré, sont galoisiennes.*

2. *Les extensions cyclotomiques* $\mathbb{Q}\left(\exp\left(\frac{2i\pi}{n}\right)\right)$ *sont galoisiennes sur* $\mathbb{Q}$.

Définition 1.24 *Soit* L/K *une extension galoisienne. L'ensemble des* K*-automorphismes de* L *est un groupe, appelé groupe de Galois de l'extension galoisienne* L/K, *on le note* $Gal(L/K)$.

Proposition 1.25 *Si* L/K *est une extension galoisienne de degré* n, *alors le groupe de Galois* $Gal(L/K)$ *est d'ordre* n.

Définition 1.26 *Soit* K *un corps et* $P \in K[X]$ *un polynôme de degré* n, *dont les racines sont distinctes. Soit* $\sum$ *le corps des racines de* P, *alors* $\sum$ *est une extension galoisiennne de* K, *dont le groupe de Galois est appelé groupe de Galois sur* K *du polynôme* P, *qu'on note* $Gal(P/K)$.

Remarque 1 *Le groupe de Galois d'un polynôme* P *de degré* n *est un groupe de permutations des racines de* P, *c'est donc un sous-groupe du groupe des permutations* S_n.

Exemple 10 *Le corps* $\mathbb{Q}(\alpha, j)$, *où* $\alpha = \sqrt[3]{2}$ *et* $j = \exp\left(\frac{2i\pi}{3}\right)$, *est une extension galoisienne de degré 6 sur* $\mathbb{Q}$. $\mathbb{Q}(\alpha, j)$ *est le corps de décomposition du polynôme* $P = X^3 - 2$ *dont le groupe de Galois est le groupe de permutations des racines de* P. *Alors* $Gal(P/\mathbb{Q}) = Gal(\mathbb{Q}(\alpha, j)/\mathbb{Q})$ *est un sous-groupe de* S_3 *d'ordre 6 c'est donc* S_3 .

1.3 Arithmétique dans les corps de nombres

1.3.1 Notations et définitions

Définition 1.27 *On appelle corps de nombres toute extension de degré fini de* $\mathbb{Q}$.
Un corps de nombres de degré 2 est appelé corps de nombres quadratique.
Un corps de nombres de degré 3 est appelé corps cubique.

Définition 1.28 *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* $\mathcal{O}_K$.

Exemple 11 *(a) Soit* $d \in \mathbb{Z} - \{0, 1\}$ *un entier sans facteur carré. Soit* $\mathcal{O}_K$ *l'anneau des entiers de* $K = \mathbb{Q}\left(\sqrt{d}\right)$.

- *Si* $d \equiv 2$ *ou* $3 \, mod 4$, *alors* $\mathcal{O}_K$ *est un* $\mathbb{Z}-$*module libre de rang 2, dont une base est* $\left\{1, \sqrt{d}\right\}$.
- *Si* $d \equiv 1 \ mod \ 4$, *alors* $\mathcal{O}_K$ *est un* $\mathbb{Z}-$*module libre de rang 2 dont une base est* $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$

(b) Pour tout nombre premier p, *le* p*-ème corps cyclotomique* $K = \mathbb{Q}(\zeta_p)$, *où* ζ_p *est une racine primitive* p*-ème de 1, est de degré* $p-1$.
L'anneau des entiers de K *est un* $\mathbb{Z}-$*module libre de rang* $p-1$ *dont une base est* $\left\{1, \zeta_p, \ldots, \zeta_p^{p-2}\right\}$

1.3.2 Discriminant d'un polynôme à une indéterminée

Définition 1.29 *Soit* K *un corps et* $f \in K[X]$ *un polynôme non nul de degré* m *et de coefficient dominant* a.

Le discriminant de f est le nombre noté $dis(f) = \dfrac{(-1)^{\frac{m(m-1)}{2}} Res(f, f')}{a}$, *où $Res(f, f')$ est le résultant de f et f', f' étant la dérivée formelle de f .*

Exemple 12 *Voici quelques formules de discriminant de polynômes.*

1. $f(X) = aX^2 + bX + c$, $dis(f) = b^2 - 4ac$,
2. $f(X) = aX^3+bX^2+cX+d$, $dis(f) = 18abcd+b^2c^2-4ac^3-4b^3d-27a^2d^2$
3. *Si* $f(X) = a \prod_{1\leq i\leq n} (X - \alpha_i)$, *alors*

$$dis(f) = a^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a^{n-2} \prod_{1\leq i\leq n} f'(\alpha_i).$$

1.3.3 Déterminant, trace et polynôme caractéristique d'un endomorphisme de module libre

Définition 1.30 *Soient A un anneau et M un $A-$module libre de rang n. Soient u un endomorphisme de M, $\{e_1, \ldots, e_n\}$ une base de M et $(a_{ij})_{1\leq i\leq j\leq n}$ la matrice de u dans cette base. La trace, le déterminant et le polynôme caractéristique de l'endomorphisme u sont :*

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

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

$$\begin{array}{rccc} m_x & B & \longrightarrow & B \\ & y & \longrightarrow & yx \end{array}$$

Définition 1.31 *On appelle trace (respectivement norme, polynôme caractéristique) de $x \in B$, relativement à B et A, la trace (respectivement déterminant, polynôme caractéristique) de l'endomorphisme m_x.*
la trace et la norme de x relativement à B et A sont notées

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

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

Proposition 1.32 *Pour tout $x, x' \in B$ et pour tout élément $\lambda \in A$ on a*

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

et

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

Définition 1.33 *Soit B un anneau et A un sous anneau de B tel que B soit un $A-$module libre de rang n.*
On appelle discriminant d'un système $(x_1, \ldots, x_n)$ d'éléments de B l'élément de A noté $D(x_1, \ldots, x_n)$ défini par

$$D(x_1, \ldots, x_n) = det\left(Tr_{B/A}(x_i x_j)\right)_{1 \leq i \leq j \leq n}$$

Suivant les conditions de la définition précédente on a

Proposition 1.34 *Si $(y_1, \ldots, y_n) \in B^n$ tels que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ pour $i \in \{1, \ldots, n\}$ et $a_{ij} \in A$, alors*

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

où (a_{ij}) est la matrice de passage du système $(x_1, \ldots, x_n)$ au système $(y_1, \ldots, y_n)$.

On a un résultat analogue dans la cas où A est un corps et B une extension de A

Proposition 1.35 *Soient K un corps fini ou de caractéristique 0, L une extension de K de degré n et $\sigma_1, \ldots, \sigma_n$ les n $K-$homomorphismes injectifs de L dans une clôture algébrique de K*
Si $(x_1, \ldots, x_n)$ est un système d'éléments de L alors :

- $D(x_1, \ldots, x_n) = \left[det(\sigma_i(x_j))_{1 \leq i \leq j \leq n}\right]^2$,
- *$(x_1, \ldots, x_n)$ est une base de L sur K si, et seulement si, $D(x_1, \ldots, x_n) \neq 0$*

Définition 1.36 *Soient B un anneau et A un sous-anneau de B tel que B soit un A-module libre de rang n.*
L'idéal principal engendré par une base de B sur A est appelé idéal discriminant qu'on note $\mathcal{D}_{B/A} = (D(e_1, \ldots, e_n))$ (celui-ci ne dépend pas de la base choisie).

Dans le cas des extensions de corps on a

Théorème 1.37 *Soit K un corps de nombres de degré n sur $\mathbb{Q}$ et $\mathcal{O}_K$ l'anneau des entiers de K. Alors le $\mathbb{Z}-$module $\mathcal{O}_K$ est libre de rang n.*

Remarque 2 *Il est utile d'interprêter quelques propriétés des bases à la lumière des résultats précédents :*

1. *Toute base du $\mathbb{Z}-$module $\mathcal{O}_K$ est une base de K sur $\mathbb{Q}$, une telle base est appelée base intégrale*
2. *Toutes les bases intégrales ont même discriminant, on appelera ce discriminant le discriminant de K qu'on notera $Dis(K)$ ou bien d_K.*

Le discriminant d'un corps de nombres algébrique et le discriminant du polynôme minimal d'un élément primitif de ce corps sont liés par la relation donnée par :

Proposition 1.38 *Soit $K = \mathbb{Q}(\alpha)$ un corps de nombre de degré n sur $\mathbb{Q}$, avec $\alpha \in \mathcal{O}_K$, et $f(X) = Irr(\alpha, \mathbb{Q}, X)$. Alors*

- $Disc(1, \alpha, \ldots, \alpha^{n-1}) = Disc(f) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}\left(f'(\alpha)\right)$
- $Disc(f) = m^2 Disc(K)$, $m \in \mathbb{N}$ *est l'indice du groupe* $\mathbb{Z}[\alpha]$ *dans* $\mathcal{O}_K$.

Exemple 13 *Nous donnons dans ce qui suit des exemples de calcul du discriminant d'un corps de nombres.*

1. *Discriminant d'un corps quadratique.*
   Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$, avec $0, 1 \neq d \in \mathbb{Z}$ sans facteur carré.
   L'anneau $\mathcal{O}_K$ des entiers de K est un $\mathbb{Z}-$module libre de rang 2

   (a) *Si $d \equiv 2 \, mod 4$ ou $d \equiv 3 \ mod\ 4$ alors $DiscK = Disc\left(1, \sqrt{d}\right) = 4d$,*

   (b) *Si $d \equiv 1 \ mod\ 4$, alors $DiscK = Disc\left(1, \frac{1+\sqrt{d}}{2}\right) = d$.*

2. *Discriminant d'un corps cyclotomique*
   Soit $K = \mathbb{Q}(\zeta)$, avec ζ racine primitive p-ème de 1, p étant un nombre premier. Alors $[K : \mathbb{Q}] = p - 1$.
   L'anneau $\mathcal{O}_K$ des entiers de K est un $\mathbb{Z}-$module libre de rang $p-1$ de base $\{1, \zeta, \ldots, \zeta^{p-2}\}$. Alors,

$$DiscK = (-1)^{\frac{3(p-1)(p-2)}{2}} p^{p-2}$$

1.4 Idéaux dans un corps de nombres

Définition 1.39 *Soient A un anneau intègre,K son corps des fractions. Un sous-A–module $\mathfrak{a}$ non nul de K est un idéal fractionnaire de K par rapport à A s'il vérifie les propriétés équivalentes suivantes*

1. *Il existe $\alpha \in A$, $\alpha \neq 0$, tel que $\alpha\mathfrak{a} \subset A$.*

2. *Il existe $\delta \in K$,$\delta \neq 0$, tel que $\mathfrak{a} \subset A$*

On dira aussi que $\mathfrak{a}$ est un idéal fractionnaire de A.

Dans le cas d'un corps de nombre K, un idéal entier de K est un idéal de l'anneau des entiers $\mathcal{O}_K$ de K, c'est-à dire un idéal fractionnaire de $\mathcal{O}_K$ contenu dans $\mathcal{O}_K$.

Soient K un corps de nombres, $\mathcal{O}_K$ son anneau d'entiers, $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, on sait que K est engendré par une racine α d'un polynôme irréductible sur $\mathbb{Q}$
Comme $\alpha \in \mathfrak{p}$ a pour polynôme minimal $X^n + a_{n-1}X^{n-1} + \cdots + a_0$, avec $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ alors a_0 appartient $\mathfrak{p} \cap \mathbb{Z}$, donc cette intersection n'est pas réduite à 0.
L'injection de $\mathbb{Z}$ dans $\mathcal{O}_K$ induit une injection de $\dfrac{\mathbb{Z}}{\mathfrak{p} \cap \mathbb{Z}}$ dans l'anneau $\dfrac{\mathcal{O}_K}{\mathfrak{p}}$ qui est intègre, donc $\dfrac{\mathbb{Z}}{\mathfrak{p} \cap \mathbb{Z}}$ est intègre et l'idéal $\mathfrak{p} \cap \mathbb{Z}$ de $\mathbb{Z}$ est premier non nul. Par conséquent, $\dfrac{\mathbb{Z}}{\mathfrak{p} \cap \mathbb{Z}}$ est un corps, puisque $\mathfrak{p} \cap \mathbb{Z}$ est maximal
Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$, le corps fini $k_K = \dfrac{\mathcal{O}_K}{\mathfrak{p}}$ est appelé corps résiduel de $\mathfrak{p}$. Dans ce cas $\dfrac{\mathbb{Z}}{\mathfrak{p} \cap \mathbb{Z}}$ est un sous-corps de k_K, et le générateur positif du sous-groupe $\mathfrak{p} \cap \mathbb{Z}$ de $\mathbb{Z}$, qui est un nombre premier p, est appelé la caractéristique du corps résiduel k_K. La norme de $\mathfrak{p}$ dans $K/\mathbb{Q}$, qui est le nombre d'éléments du corps fini $k_K = \dfrac{\mathcal{O}_K}{\mathfrak{p}}$ est donc p^f où $f = [k_K : \mathbb{F}_p]$ est

appelé degré résiduel du corps k_K Nous interprétons ces résultats par le schéma suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \dfrac{\mathcal{O}_K}{\mathfrak{p}} = k_K \\ \bigcup & & | \\ \mathbb{Z} & \longrightarrow & \dfrac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p \end{array}$$

On a résultat suivant

Lemme 1.40 *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$ et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$.*
On désigne par k_K le corps résiduel $\dfrac{\mathcal{O}_K}{\mathfrak{p}}$, alors $\dfrac{\mathfrak{a}}{\mathfrak{p}\mathfrak{a}}$ est un k_K-espace vectoriel de dimension ≥ 1.

En fait, nous établirons que la dimension de cet espace vectoriel est 1.
En effet, soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$ alors $\mathfrak{p}^m \neq \mathfrak{p}^{m+1}$ pour tout $m \geq 0$ ce qui entraine que la suite

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^m \supset \ldots$$

est donc strictement décroissante. Par le lemme précédent le quotient $\dfrac{\mathfrak{p}^m}{\mathfrak{p}^{m+1}}$ est isomorphe comme $\mathcal{O}_K$-module à $\dfrac{\mathcal{O}_K}{\mathfrak{p}}$; il en résulte que la norme de $\mathfrak{p}^m$ est égal à $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^m$.
Notons que l'intersection de tous les $\mathfrak{p}^m$ est $\{0\}$

Théorème 1.41 *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. L'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ qui contiennent $\mathfrak{a}$ est fini et on a*

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \in \mathcal{O}_K \\ 0 \neq \mathfrak{p},\ premier}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

De plus une telle décomposition est unique.

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$,

Définition 1.42 *L'indice de ramification $e(\mathfrak{p})$ de l'idéal $\mathfrak{p}$ est l'entier naturel donné par*

$$e(\mathfrak{p}) = v_p\left(p\mathcal{O}_K\right), \text{ avec } g \in \mathbb{N}^*$$

où p désigne la caractéristique du corps résiduel de $\mathfrak{p}$.

Soit p un nombre premier et soit $p\mathcal{O}_K$ l'idéal principal de $\mathcal{O}_K$ qu'il engendre. Le théeorème ci dessus montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

où $g \geq 1$ est un entier , $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont des idéaux premiers de $\mathcal{O}_K$, distincts deux à deux, et $e_i \geq 1$ est l'indice de ramification de $\mathfrak{p}_i$, $1 \leq i \leq g$. Les idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont précisément les idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, on dit qu'il sont au dessus de p. De la décomposition précédente on déduit que

$$\frac{\mathcal{O}_K}{p\mathcal{O}_K} \simeq \frac{\mathcal{O}_K}{\mathfrak{p}^{e_1}} \times \dots \times \frac{\mathcal{O}_K}{\mathfrak{p}^{e_g}}$$

En posant $[K : \mathbb{Q}] = n$ et en désignant par f_i le degré résiduel de $\mathfrak{p}_i$, par la multiplicativité de la norme on obtient

$$p^n = \mathrm{N}_{K/\mathbb{Q}}(p) = \prod_{i=1}^{g} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{g} p^{e_i f_i}$$

ce qui entraine que $n = \sum_{i=1}^{g} e_i f_i$.

Définition 1.43 *Suivant les notations ci-dessus :*

1. *On dit que $\mathfrak{p}_i$ est ramifié au dessus de p si l'exposant e_i est ≥ 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 $e_1 = n$ (respactivement $e_1 = 1$), alors $g = 1$ et $f_1 = 1$ (respectivement $f_1 = n$)*

4. *On dit que p totalement décomposé dans K si $g = n$ et donc on a $e_i = f_i = 1$, $1 \leq i \leq n$.*

Dans le cas d'un corps quadratique nous avons :

Théorème 1.44 *Soit p un nombre premier et d un entier sans facteur carré. la décomposition de p dans $K = \mathbb{Q}\left(\sqrt{d}\right)$ est donnée par :*

- *Si p divise d, alors p est ramifié dans K et on a $p\mathcal{O}_K = \mathfrak{p}^2$, avec $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$.*
- *Si $\left(\frac{d}{p}\right) = 1$, alors p est décomposé dans K : $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, avec $N_{K/\mathbb{Q}}(\mathfrak{p}_1) = N_{K/\mathbb{Q}}(\mathfrak{p}_2) = p$.*
- *Si $\left(\frac{d}{p}\right) = -1$, alors p est inerte dans K : $p\mathcal{O}_K = \mathfrak{p}$, 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 :

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

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

Théorème 1.45 *Soit K un corps de nombres, alors les nombres premiers qui se ramifient dans K sont en nombre fini : ce sont précisément les diviseurs premiers du discriminant d_K*

Pour illustrer ce théorème, nous examinons la ramification d'un nombre premier p dans les cas d'un corps quadratique et d'un corps cyclotomique

Exemple 14 *Examinons la ramification dans les cas suivant :*

- *Cas d'un corps quadratique*
  Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$, $d \in \mathbb{Z}$, $d \neq 0, 1$, d *sans facteur carré. Soit* p *un nombre premier.*

  - *Si* $d \equiv 2$ *ou* $3 \bmod 4$, *alors* $\mathcal{O}_K$ *est un* $\mathbb{Z}$*-module libre de base* $\left\{1, \sqrt{d}\right\}$, *alors* $d_K = 4d$.
    Par conséquent, les nombres premiers qui se ramifient sont 2 *et les premiers* p *impairs divisant* d.
  - *Si* $d \equiv 1 \bmod 4$, *alors* $\mathcal{O}_K$ *est un* $\mathbb{Z}$*-module libre de base* $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$, *alors* $d_K = d$.
    Par conséquent, les nombres premiers qui se ramifient sont les premiers p *impairs divisant* d.

- *Cas d'un corps cyclotomique.*
  Soit $K = \mathbb{Q}(\zeta)$, *où* ζ *est une racine primitive* p*-ème de l'unité,* p *premier .*
  L'anneau $\mathcal{O}_K$ *des entiers est un* $\mathbb{Z}$*-module libre de base* $\{1, \zeta, \ldots, \zeta^{p-2}\}$.
  Le discriminant absolu de K *sur* $\mathbb{Q}$ *est*

$$d_K = (-1)^{\dfrac{3(p-1)(p-2)}{2}} p^{p-2}$$

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

Exemple 15 *Nous allons examiner dans ce qui suit l'exemple de la décomposition d'un nombre premier dans une extension engendrée par une racine d'un*

polynôme irréductible sur $\mathbb{Q}$.
Soit $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Z}[X]$ *et* L *son corps de décomposition sur* $\mathbb{Q}$, *c'est donc une extension galoisienne de* $\mathbb{Q}$.
Le polynôme f *est irréductible sur* $\mathbb{Q}$. *En effet, si* f *était réductible il admettrait un facteur de degré 1, donc une racine* $\alpha \in \mathbb{Q}$ *qui serait alors dans* $\mathbb{Z}$ *et vérifierait*

$$\alpha^3 + \alpha^2 - 2\alpha = 1$$

ce qui impose que $\alpha \mid 1$ *dans* $\mathbb{Z}$ *et donc* $\alpha = -1$ *ou* 1. *Puisque aucune de ces valeurs n'est racine de* f, *alors* f *est irréductible.*
Ainsi, si θ*est une racine de* f *dans* L, *alors* $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$. *et par suite* $3 \mid [L : \mathbb{Q}]$. *De plus,* $Gal(L/\mathbb{Q})$ *est un groupe de permutations des racines de* f, *qui sont au nombre de 3, alors il est d'ordre un diviseur de* 6,

$$\#Gal(L/\mathbb{Q}) = [L : \mathbb{Q}] \in \{3, 6\}.$$

D'autre part, le discriminant $f(X)$ *est égal à* 7^2, *c'est donc un carré, ce qui implique que le groupe de Galois* $Gal(L/\mathbb{Q})$ *est un sous-groupe du groupe alterné,* $Gal(L/\mathbb{Q}) \subseteq A_3$, *ce qui montre que* $[L : \mathbb{Q}] = 3$ *et* $Gal(L : \mathbb{Q}) = A_3$.
L'anneau $\mathcal{O}_L$ *des entiers de* L *est un* $\mathbb{Z}$*-module libre de rang 3 et une bse de l'espace vectoriel* L *sur* $\mathbb{Q}$ *est* $\{1, \theta, \theta^2\}$ *de discriminant* $D(1, \theta, \theta^2)$ *vérifiant :*

$$D\left(1, \theta, \theta^2\right) = 7^2 = m^2 d_L$$

où d_L *est le discriminat absolu de* L *sur* $\mathbb{Q}$ *et* m *et l'indice de* $\mathbb{Z}[\theta]$ *dans* $\mathcal{O}_L$, $m = [\mathcal{O}_L : \mathbb{Z}[\theta]]$.
Commme $d_L \neq 1$ *et* $m^2 \neq 7$, *alors* $d_L = 7^2$ *et* $m = 1$, *alors* $\{1, \theta, \theta^2\}$ *est une base du* $\mathbb{Z}$*-module* $\mathcal{O}_L$.
Examinons la décomposition d'un nombre premier p *dans* L. *Comme* $L/\mathbb{Q}$ *est*

une extension galoisienne alors

$$p\mathcal{O}_L = \left(\prod_{i=1}^{g} \wp_i\right)^e$$

où les $\wp_i$ sont des idéaux premiers tous distincts dnas L et e étant leur indice de ramification commun. Alors le degré résiduel de chacun des idéaux $\wp_i$ est commun et est égal à f et il vérifie $efg = 3$. Par conséquent, soit $g = 1$ et donc $e = 3$ et $f = 1$ ou bien $e = 1$ et $f = 3$, soit $g = 3$ et donc $e = f = 1$. Ce qui donne les différents factorisations de p dans L suivantes :

$$\text{soit } p\mathcal{O}_L = \wp_1^3 \text{ ou } p\mathcal{O}_L = \wp_2, \quad \text{soit } p\mathcal{O}_L = \wp_3\wp_4\wp_5$$

où $N_{L/\mathbb{Q}}(\wp_i) = p^f$.
Comme 7 est le seul diviseur premier du discriminant de $L/\mathbb{Q}$, alors le nombre premier 7 se ramifie dans L et on a

$$7\mathcal{O}_L = \wp^3$$

et il est complètement ramifié dans L.
Pour $p \neq 7$, p est soit inerte, soit décomposé, et on a

$$\frac{\mathcal{O}_L}{\wp\mathcal{O}_L} \simeq \frac{\mathbb{F}[X]}{(X^3 + X^2 - 2X - 1) \mod p}$$

ce qui conduit à deux possibilités : soit $X^3 + X^2 - 2X - 1 \mod p$ n'admet pas de racine dans $\mathbb{F}_p$ ce qui entraine

$$p\mathcal{O}_L = \wp, \text{ avec } N_{L/\mathbb{Q}}(\wp) = p^3,$$

Le nombre premier p est inerte dans L, soit $X^3 + X^2 - 2X - 1 \mod p$ admet

trois racines distinctes dans $\mathbb{F}_p$ *et on a*

$$p\mathcal{O}_L = \wp_1\wp_2\wp_3, \quad avec \ \ N_{L/\mathbb{Q}}(\wp_i) = p$$

et le nombre premier p *est totalement décomposé dans* L.
Comme exemples de nombres premiers inertes on a

$$2\mathcal{O}_L = \wp_1, \quad 3\mathcal{O}_L = \wp_2, \quad 23\mathcal{O}_L = \wp_3$$

Comme exemples de nombres premiers complètement décomposés on a

$$13\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3, \quad 39\mathcal{O}_L = \mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6, \quad 43\mathcal{O}_L = \mathfrak{q}'_1\mathfrak{q}'_2\mathfrak{q}'_3.$$

Chapitre 2

Corps de nombres $p-$adiques

2.1 Valuation p-adique

Soit $p \in N$ un nombre premier, et $\mathbb{Q}$ le corps des nombres rationnels.

Définition 2.1 *On appelle valeur absolue $p-$adique sur $\mathbb{Q}$ l'application notée $|\ |_p$ de $\mathbb{Q}$ dans $\mathbb{Q}^+$ définie par*

$$|\,0\,|_p = 0$$
$$\left|\frac{a}{b}\right|_p = \frac{1}{p^\lambda},\ si\ \frac{a}{b} = p^\lambda \frac{a'}{b'}$$

où a, $a' \in \mathbb{Z}$ et b, $b'\mathbb{Z}^*$ et $p \nmid a'b'$.

Exemple 16 *Par la définition ci-dessus on a*

$$|\,16\,|_2 = \frac{1}{2^4}, \quad |\,15\,|_3 = \frac{1}{3}, \quad |\,50\,|_5 = \frac{1}{5^2}$$

$$|\,50\,|_7 = 1, \quad \left|\frac{8}{15}\right|_3 = 3.$$

Proposition 1 *La valeur absolue $p-$adique sur $\mathbb{Q}$ vérifie*

- $\forall x, y \in \mathbb{Q}$, *on a* $|xy|_p = |x|_p |y|_p$
- $\forall x, y \in \mathbb{Q},$, $y \neq 0$, *on a* $\left|\frac{x}{y}\right|_p = \frac{|x|_p}{|y|_p}$
- $\forall x, y \in \mathbb{Q},$, *on a* $|x+y|_p \leq \sup\left(|x|_p, |y|_p\right)$ *(inégalité ultramétrique)*
- $\forall x, y \in \mathbb{Q}$ *tels que* $|x|_p \neq |y|_p$ *on a* $|x+y|_p = \sup\left(|x|_p, |y|_p\right)$

Définition 2.2 *On appelle valuation p-adique sur* $\mathbb{Q}$, $p \in \mathbb{N}$ *premier, l'application* v_p *de* $\mathbb{Q}$ *dans* $\mathbb{Z} \cup \{+\infty\}$ *définie comme suit*

1. $v_p(0) = +\infty$,
2. $v_p\left(\frac{a}{b}\right) = \lambda$ *si* $\frac{a}{b} = p^{\lambda}\frac{a'}{b'}$, *avec* a, b, a', $b' \in \mathbb{Z}^*$, $\lambda \in \mathbb{Z}$ *et* $p \nmid a'b'$

Remarque 3 *Notons quelques remarques :*

- *Si* $x, y \in \mathbb{Q}^*$, *alors* $v_p(x+y) \geq \inf(v_p(x), v_p(y))$,
- *si* $x, y \in \mathbb{Q}^* v_p(x) \neq v_p(y)$, *alors* $v_p(x+y) = \inf(v_p(x), v_p(y))$.

Exemple 17 $v_3(2) = 0$, $v_3(6) = 1$ *et* $v_5(25) = 2$

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

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

Proposition 2.4 *L'ensemble* $\mathcal{E}$ *muni de l'addition et de la multiplication usuelles des suites est un anneau commutatif. De plus, l'ensemble* $I = \left\{(u_n) \in \mathcal{E}, \text{ tels que } \lim_{n\to+\infty} u_n = 0\right\}$ *est un idéal maximal de* $\mathcal{E}$ *et l'anneau quotient* $\frac{\mathcal{E}}{I}$ *vérifie :*

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

  Le corps $\dfrac{\mathcal{E}}{I}$ *est noté* $\mathbb{Q}_p$.

Preuve : (voir[1])

□

2.2 Extensions et completion

Proposition 2.5 *Soit K un corps muni d'une valeur absolue $|\,|$. Il existe un surcorps $\hat{K}$ de K muni d'une valeur absolue prolongeant celle de K et complet pour cette valeur absolue et tel que K soit dense dans $\hat{K}$.De plus ce sur-corps est unique à isomorphisme près. $\hat{K}$ est appelé le complété de K pour la valeur absolue $|\,|$.*

Preuve : On construit le complété de K pour $|\,|$. Les suites de Cauchy définies sur K forment un anneau A dans lequel K s'injecte.
L'déal I formé des suites de Cauchy tendant vers 0 est maximal dans A. Le complété de K pour $|\,|$ est le corps $\dfrac{A}{I}$noté $\hat{K}$. La valeur absolue $|\,|$ définie sur K est prolongeable par continuité au corps $\hat{K}$.
Si la valeur absolue $|\,|$ sur K est ultramétrique, alors l'ensemble des valeurs prises par $|\,|$ sur K est le même que celui sur le complété .
Si la valeur absolue $|\,|$ sur K provient d'une valuation discrète, il en est de même de son prolongement au complété

□

Proposition 2.6 *Soit K corps local (un corps complet pour une valeur absolue provenant d'une valuation discrète) dont on note A l'anneau de valuation. On considère une extension L de K de degré fini, alors le corps L est local d'anneau de valuation la fermeture intégrale B de A dans L. L'anneau B est un anneau de valuation discrète, c'est à dire qu'il est local, principal et distinct de son corps des fractions.*
De plus, si on note $\mathfrak{m}$ et $\mathfrak{M}$ les idéaux maximaux respectivement de A et B, alors $\mathfrak{m}B = \mathfrak{M}^e$ et $\left[\dfrac{B}{\mathfrak{M}} : \dfrac{A}{\mathfrak{m}}\right] = f$ où $ef = [L : K]$.

Proposition 2.7 *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 le complété $\hat{L}$ de L pour cette valeur absolue contient le complété $\hat{K}$ de K pour la valeur absolue $|\ |_{|K}$ induite de $|\ |$ par restriction à K. De plus, $\hat{L}/\hat{K}$ est une extension de degré fini et on a $\left[\hat{L} : \hat{K}\right] \leq [L : K]$.*

Soit p un nombre premier, K un corps de nombres algébrique d'anneau d'entier $\mathcal{O}_K$.
Soit $\mathfrak{p}$un idéal premier de $\mathcal{O}_K$ au dessus de p.
Le complété $K_\mathfrak{p}$ de K pour la valeur absolue $|\ |_\mathfrak{p}$ associée à $\mathfrak{p}$ est une extension de $\mathbb{Q}_p$ de degré fini et on a

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

2.3 Les corps des nombres p-adiques

2.3.1 Notations et définitions

Soit $p \in \mathbb{N}$ un nombre premier.

Définition 2.8 *On appelle corps de nombres p-adiques toute extension finie de $\mathbb{Q}_p$.*

Le corps $\mathbb{Q}_p$ est le complété du corps $\mathbb{Q}$ des nombres rationnels pour la valuation p-adique.

Proposition 2.9 *L'ensemble noté*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p \ \text{ tel que } \ |x|_p \leq 1 \right\}$$

est l'anneau des entiers de $\mathbb{Q}_p$. Cest un anneau local et principal.

Preuve : (voir [1])

□

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

Proposition 2.10 ***(Développement de Hensel)***
Soit $\alpha \in \mathbb{Z}_p$, il existe une unique suite $(a_n)_{n\geq 0}$, avec $0 \leq b_n < p$, tel que la série

$$\sum_{n\geq 0} b_n p^n$$

converge vers α Cette série est appelée développement de Hensel infini de α

Proposition 2.11 *Soit $\alpha \in \mathbb{Z}_p$, alors il existe $a \in \mathbb{Z}$ tel que $|\alpha - a|_p < 1$*

Remarque 4 *La proposition ci-dessus permet de donner plus de précision sur l'écriture d'un nombre p-adique. En effet ;*

- *Soit $\alpha \in \mathbb{Z}_p$, il existe $a_0 \in \{0, 1, \ldots, p-1\}$ tel que $|\alpha - a_0|_p < 1$, cela veut dire que $\alpha - a_0 \in p\mathbb{Z}_p$.*
  Ainsi, $\alpha - a_0 = p\alpha_1$, avec $\alpha_1 \in \mathbb{Z}_p$ ce qui entraine l'existence de $a_1 \in \{0, 1, \ldots, p-1\}$ avec $|\alpha - a_1|_p < 1$ et $\alpha - a_1 \in p\mathbb{Z}_p$
  On en déduit alors qu'il existe α_2 tel que $\alpha_1 - a_1 = p\alpha_2$

$$\alpha = a_0 + p\left(a_1 + p\alpha_2\right) = a_0 + pa_1 + p^2\alpha_2.$$

En continuant ce processus, on met en évidence des entier $a_i \in \{0, 1, \ldots, p-1\}$, $i \geq 0$ *tel que*

$$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots$$

- *Soit* $\alpha \in \mathbb{Q}_p - \mathbb{Z}_p$, $\alpha \neq 0$, *alors* $|\alpha|_p = \dfrac{1}{p^\lambda}$, $\lambda < 0$, *alors*

$$\left|\frac{\alpha}{p^\lambda}\right|_p = \frac{|\alpha|_p}{|p^\lambda|_p} = 1$$

On pose $\alpha' = \dfrac{\alpha}{p^\lambda}$ *avec* $\alpha' \in \mathbb{Q}_p$ *et* $\lambda = -m$ *avec* $m \in \mathbb{N}^*$, *alors*

$$\alpha = p^\lambda \alpha' = \frac{\alpha'}{p^{-\lambda}} = \frac{a_0}{p^m} + \frac{a_1}{p^{m-1}} + \cdots + \frac{a_{m-1}}{p} + a_m + a_{m+1} p + \ldots$$

Ainsi le développement de Hensel est unique.

Théorème 2.12 *On a l'isomorphisme suivant*

$$\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$$

2.3.2 Anneau des entiers d'un corps de nombres p-adiques

2.4 Anneau des entiers d'un corps de nombres p-adiques

Soit K une extension de $\mathbb{Q}_p$ de degré n.
la valeur absolue p-adique définie sur K prolongeant celle de $\mathbb{Q}_p$est l'application

$$|\,|_p : K \longrightarrow \mathbb{R}_+$$

vérifiant

$$\forall x \in K, \quad |x|_p = \left|\mathrm{N}_{K/\mathbb{Q}_p}(x)\right|_p^{\frac{1}{n}}.$$

Soit $A_K = \left\{ x \in K \text{ tel que } |x|_p \leq 1 \right\}$. On vérifie que A_K est un sous-anneau de K, et c'est un anneau de valuation discrète pour la valuation v_p définie par

$$\begin{array}{rl} v_p & K \longrightarrow \frac{1}{n}\mathbb{Z} \cup \{+\infty\} \\ & x \longrightarrow v_p(x) \end{array}$$

et vérifiant

$$\begin{cases} v_p(0) = & +\infty \\ v_p(x) = & \frac{1}{n} v_p\left(\mathrm{N}_{K/\mathbb{Q}_p}(x)\right), \text{ si } x \neq 0 \end{cases}$$

Proposition 2.13 *L'anneau de valuation A_K est l'anneau des entiers de K et il est principal.*

Preuve : Montrons tout d'abord que l'annau A_K est l'anneau des entiers de K.
Soit $\alpha \in A_K$ de polynôme minimal $P_\alpha(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$.
Soit $L = \mathbb{Q}_p(\alpha_1, \ldots, \alpha_d)$ le corps des racines de $P_\alpha(X)$, où $\alpha_1, \ldots, \alpha_d$ sont ses racines distinctes.
Pour tout $i \in \{1, \ldots, d\}$ on a

$$\left|\mathrm{N}_{L/\mathbb{Q}_p}(\alpha_i)\right|^{\frac{1}{[L:\mathbb{Q}_p]}} = \left|\mathrm{N}_{\mathbb{Q}_p(\alpha_i)/\mathbb{Q}_p}(\alpha_i)\right|^{\frac{1}{d}} = \left|\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|^{\frac{1}{d}} = \left|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)\right|^{\frac{1}{n}}$$

Par suite, comme $|\alpha|_p \leq 1$ alors $|\alpha_i|_p \leq 1$, $\forall i \in \{0, \ldots, d-1\}$.
Comme les coefficients a_j sont des sommes des produits de α_i, alors $|a_j|_p \leq 1$ pour tout $j \in \{0, 1, \ldots, d-1\}$. Par conséquent, $P_\alpha(X) \in \mathbb{Z}_p[X]$ et donc $\alpha \in A_K$ est un entier sur $\mathbb{Z}_p$.
Réciproquement, on suppose que α est un entier sur $\mathbb{Z}_p$, soit $f(X) \in \mathbb{Z}_p[X]$ son polynôme minimal. Alors on aura

$$\mathrm{N}_{K/\mathbb{Q}_p}(\alpha) = (-1)^n f(0)^d, \quad d = [K : \mathbb{Q}_p(\alpha)]$$

Comme $f(0) \in \mathbb{Z}_p$,alors $\left|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)\right| \leq 1$ ce qui entraine $|\alpha|_p \leq 1$ et donc $\alpha \in A_K$.
par conséquent, A_K est l'anneau des entiers de K.
Pour montrer la principalité de A_K, on considère l'idéal $\mathfrak{M}_K$ de A_K donné par

$$\mathfrak{M}_K = \left\{ x \in A_K,\ tel\text{que}\ |x|_p < 1 \right\}$$

Comme A_K est de Dedekind, alors

$$\mathfrak{M}_K^2 \subset \mathfrak{M}_K, \quad avec \mathfrak{M}_K^2 \neq \mathfrak{M}_K$$

alors il existe $\Pi \in \mathfrak{M}_K$ et $\Pi \notin \mathfrak{M}_K^2$ tel que

$$\Pi A_K = (\Pi) \text{ et } \Pi A_K \subset \mathfrak{M}_K$$

Par suite, on a

$$\mathfrak{M}_K^r = \Pi A_K, \text{ avec } r \in \mathbb{N}^*$$

ce qui entraine que $r = 1$, car sinon $\Pi^2 \in \mathfrak{M}_K$, et donc $\mathfrak{M}_K = (\Pi)$ dans A_K.
De plus, si $I \neq 0$ est un idéal quelconque de A_K, alors

$$I = \mathfrak{M}_K^e = \Pi^e A_K = (\Pi^e)$$

et donc I est principal, ce qui entraine que A_K est principal.
Notons que l'idéal $\mathfrak{M}_K$ est maximal et il est unique défini par

$$\mathfrak{M}_K = \Pi A_K, \text{ avec } v_p(\Pi) = \frac{1}{e}, \text{ si } pA_K = \mathfrak{M}_K^e$$

Π est appelé uniformisante de K.

□

2.5 Extension de corps de nombres p adiques

2.5.1 Définition

Proposition 2.14 *Il y a une correspondance biunivoque entre les idéaux premiers de $\mathcal{O}_K$ au dessus d'un nombre premier p et les corps de nombres p-adiques dans lesquel K est dense.*
Notons $Spec_p(\mathcal{O}_K)$ et $Ext_{\mathbb{Q}_p}(K)$,respectivement l'ensembles des idéaux premier de $\mathcal{O}_K$ au dessus de p est l'ensemble des extension de $\mathbb{Q}_p$ de degré fini dans lesquel K est dense.
Pour tout $E \in Ext_{\mathbb{Q}_p}(K)$, soit $\mathfrak{p}_E$ l'unique idéal maximal de E, on a

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

De plus, si $\mathcal{O}'$ est l'anneau des entiers de $K_{\mathfrak{p}}$ et $\mathfrak{m}$ son unique idéal maximal, alors

1. *l'idéal $\mathfrak{p}\mathcal{O}'$ est premier dans $\mathcal{O}'$: $\mathfrak{p}\mathcal{O}' = \mathfrak{m}$,*
2. $\dfrac{\mathcal{O}_K}{\mathfrak{p}} \simeq \dfrac{\mathcal{O}'}{\mathfrak{m}}$ *de dimension commune sur $\mathbb{F}_p$ égale à $f_{\mathfrak{p}}$,*
3. *les indices de ramification de $\mathfrak{p}$ sur $\mathbb{Z}$ et de $\mathfrak{m}$ sur $\mathbb{Z}_p$ sont les mêmes : $p\mathcal{O}' = \mathfrak{m}^{e_{\mathfrak{p}}}$.*
   L'extension $K_{\mathfrak{p}}$sur $\mathbb{Q}_p$ est de degré $e_{\mathfrak{p}}f_{\mathfrak{p}}$.

Examinons de façon précise le cas d'un corps de nombres algébriques K engendré par une racine d'un polynôme unitaire irréductible sur $\mathbb{Q}$.
Soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible, alors $f(X)$ est séparable et il sera donc sans facteur carré sur $\mathbb{Z}_p[X]$, p étant un nombre premier.
Soit $f(X) = \prod_{i=1}^{r} f_j(X)$ la décomposition de $f(X)$ en facteurs irréductibles et unitaire sur $\mathbb{Z}_p[X]$.

Théorème 2.15 *Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$, K un corps de nombre engendré par une racine de f dans $\overline{\mathbb{Q}}$.*
Il y a une correspondance biunivoque entre les facteurs irréductible de f dans $\mathbb{Z}_p[X]$ et les idéaux premiers de $\mathcal{O}_K$ au dessus de 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 morhisme injectif d'anneaux, alors $\ker\varphi \simeq \mathbb{Q}[X] \cap g\mathbb{Q}_p[X] = f\mathbb{Q}[X]$ car les idéaux (f) et (g) sont maximaux, ce qui entraine que $\dfrac{\mathbb{Q}[X]}{(f)}$ et $\dfrac{\mathbb{Q}_p[X]}{(g)}$ sont des corps. 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 premier de $\mathcal{O}_K$ au dessus de p, à savoir $\mathfrak{M} \cap \mathcal{O}_K$.
Inversement, 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 et de $\mathbb{Q}_p$ avec $[K_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p}$. Ainsi $K_\mathfrak{p} = \mathbb{Q}_p(\theta)$, où $\theta \in \mathcal{O}_K$ 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 correspondance 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 2.16 *(Lemme de HENSEL)*

Soit le polynôme $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}_p[X]$. *On suppose qu'il existe deux polynômes* $g(X)$ *et* $h(X)$ *dans* $\mathbb{F}_p[X]$ *tels que*

- $g(X)$ *et unitaire ,*
- $g(X)$ *et* $h(X)$ *premiers entre eux dans* $\mathbb{F}_p[X]$.
- $\overline{f}(X) = g(X).h(X)$

Alors il existe deux polynômes $G(X)$ *et* $H(X)$ *dans* $\mathbb{Z}_p[X]$ *tels que*

$$\begin{cases} \overline{G}(X) = & g(X) \\ \overline{H}(X) = & h(X) \end{cases}$$

vérifiant $f(X) = G(X).H(X)$

Corollaire 2.17 *Soit* $f(X) \in \mathbb{Z}_p[X]$ *un polynôme unitaire.*
On suppose que $\overline{f}(X)$ *possède une racine simple dans* $\mathbb{F}_p[X]$, *alors* $f(X)$ *possède une racine simple dans* $\mathbb{Z}_p[X]$.

Corollaire 2.18 *Soit* $f(X) \in \mathbb{Q}_p[X]$ *un polynôme unitaire, irréductible sur* $\mathbb{Q}_p$.

On suppose que $f(0) \in \mathbb{Z}_p[X]$, *alors* $f(X) \in \mathbb{Z}_p[X]$.

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

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

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

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

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

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

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

Définition 2.19 *Soit L/K une extension de corps p-adiques.*

- *On dit que l'extension L/K est non ramifiée si $e = 1$,*
- *On dit que l'extension L/K est totalement ramifiée si $e = n$,*
- *On dit que l'extension L/K est sauvagement ramifiée si p divise e, sinon on dit que l'extension est modérément ramifiée.*

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

Théorème 2.20 *(Caractérisation des extensions totalement ramifiées)*

(i) Si L est une extension totalement ramifiée de $\mathbb{Q}_p$ de degré n, alors $L = \mathbb{Q}_p(\pi)$, où π est une uniformisante et $Min(\pi, \mathbb{Q}_p, X)$ est un polynôme d'Eisenstein.

(ii) Si $L = \mathbb{Q}_p(\theta)$ est une extension de degré n de $\mathbb{Q}_p$ où $Min(\theta, \mathbb{Q}_p, X)$ est un polynôme d'Eisenstein, alors θ est une uniformisante de L et l'extension $L/\mathbb{Q}_p$ est totalement ramifiée.

Preuve : *(i)* Soit v_p la valuation définie sur L dont sa restriction à $\mathbb{Q}_p$ est une valuation sur ce corps définie par

$$\begin{cases} v_p(0) = +\infty \\ v_p(x) = \frac{1}{n} v_p\left(\mathrm{N}_{L/\mathbb{Q}_p}(x)\right) & \text{si } x \in L^* \end{cases}$$

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

$$v_p(\pi) = \frac{1}{n} = \frac{1}{n} v_p\left(\mathrm{N}_{L/\mathbb{Q}_p}(\pi)\right)$$

ce qui donne $v_p\left(\mathrm{N}_{L/\mathbb{Q}_p}(\pi)\right) = 1$.
Soit $f(X) = \mathrm{Min}(\pi, \mathbb{Q}_p, X) = X^s + a_{s-1}X^{s-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}_p[X]$, alors

$$\mathrm{N}_{L/\mathbb{Q}_p}(\pi) = (-1)^n a_0^d, \quad \text{où } d = \frac{n}{s}$$

ce qui entraine

$$1 = v_p\left(\mathrm{N}_{L/\mathbb{Q}_p}(\pi)\right) = d v_p(a_0)$$

ce qui implique que $d = 1$ puisque $v_p(a_0) \in \mathbb{Z}$. Par conséquent, $n = s$ et $L = \mathbb{Q}_p(\pi)$.
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 $v_p(a_0) = 1$.
Soient $\pi_1, \ldots, \pi_n$ les n racines de $f(X)$ dans une clôture algébrique C contenant $\mathbb{Q}_p$, soit F le corps de décomposition de $f(X)$ et v la valuation définie sur F qui prolonge v_p telle que

$$v(0) = \infty \text{ et } v(x) = \frac{1}{m} v_p\left(\mathrm{N}_{F/\mathbb{Q}_p}(x)\right), \text{ si } x \neq 0$$

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

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

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 $f(X)$ est d'Eisenstein.

(ii) Soit $[L : \mathbb{Q}_p] = n$ avec $L = \mathbb{Q}_p(\theta)$, et $g(X) = \text{Min}(\theta, \mathbb{Q}_p, X)$ un polynôme d'Eisenstein. Alors

$$v_p(\theta) = \frac{1}{n} v_p\left(\text{N}_{L/\mathbb{Q}_p}(\theta)\right) \text{ et } \text{N}_{L/\mathbb{Q}_p}(\theta) = (-1)^n g(0)$$

ce qui donne

$$v_p\left(\text{N}_{L/\mathbb{Q}_p}(\theta)\right) = v_p(g(0)) = 1$$

et $v_p(\theta) = \frac{1}{n}$ car $g(X)$ est un polynôme d'Eisenstein.
Soit π une uniformisante de L et soit $e = e(L/\mathbb{Q}_p)$, alors $v_p(\pi) = \dfrac{1}{e}$ et il existe $\beta \in \mathcal{O}_L$ tel que $\theta = \pi\beta$.
Ainsi, $v_p(\theta) \geq v_p(\pi)$, c'est à dire que $n \leq e$ et comme $e \leq n$ alors $e = n$.
Ce qui montre que $L/\mathbb{Q}_p$ est une extension totalement ramifiée.
β étant un élément inversible dans $\mathcal{O}_L$, car $v_p(\beta) = 0$, par suite $(\pi) = (\theta)$ ce qui veut dire que θ est une uniformisante de L.

□

Exemple 18 *Soit $f(X) = X^n - p \in \mathbb{Q}_p[X]$.*
On a $v_p(a_0) = v_p(p) = 1$ et $v_p(a_i) = +\infty$, $\forall i \in \{1, \ldots, n-1\}$, alors $f(X)$ est d'Eisenstein en p ; il est donc irréductible. Par conséquent, si θ est une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}_p$, alors l'extension $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$ est totalement ramifiée.

Le théorème précédent se généralise pour une extension de corps de nombres quelconques :

Théorème 2.21 *Si K est un corps de nombres p-adique 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, toute extension de K engendrée par une racine d'un polynôme d'Eisenstein est totalement ramifiée.

Corollaire 2.22 *Il existe une unique extension totalement ramifiée de degré donné.*

Corollaire 2.23 *Si M est la composée de toutes les extensions totalement ramifiées de L sur K, alors M est une extension totalement ramifiée sur L.*

Les extension non ramifiées sont caractérisées par

Théorème 2.24 *Soit L/K une extension de corps de nombres p-adiques de degré fini. Soient $\mathcal{O}_L$ et $\mathcal{O}_K$ les anneaux d'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 le polynôme minimal de α sur K, alors $\overline{g}(X)$, obtenu par réduction de $g(X)$ modulo p de ses coefficient, est 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 α 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 2.25 *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 2.26 *SI L/K et F/K sont des extensions non ramifiées, il en est de même de LF/K.*

Corollaire 2.27 *Il existe une unique extension non ramifiée de degré donné.*

Les extensions modérément ramifiées sont caractérisées par :

Proposition 2.28 *Une extension L/K de corps de nombres p-adiques de degré n est modérément ramifiée si, et seulement si, le discriminant $d_{L/K}$ de L/K n'est pas divisible par p^n.*

Lemme 2.29 *Si L/K est modérément ramifiée et M/K de degré fini, alors LM/M est modérément ramifiée.*

Lemme 2.30 *Soient L et M deux extensions d'un corps p-adique K telles que M/K soit modérément ramifiée.*
Si $e(M/K)$ divise $e(L/K)$, alors LM/L est non ramifiée.

Proposition 2.31 *Une extension L/K de degré n, $n \in \mathbb{N}^*$, est totalement et modérément ramifiée si, et seulement si $L = K(\theta)$ où θ est une racine d'un binôme $X^n - b$, où $b \in K$ tel que $v_p(b) = 1$.*

Les extension sauvagement ramifiées sont caractérisées par :

Proposition 2.32 *Une extension L/K de degré fini n de corps de nombres p-adiques est sauvagement ramifiée si, et seulement si, $d_{L/K}$ est divisible par p^n.*

2.6 Groupe de Galois

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

Définition 2.33 *On appelle groupe d'inertie de $\wp$ dans L, le sous groupe G_0 du groupe de Galois G donné par*

$$G_0 = \{\sigma \in G,\, \sigma(x) \equiv x \, mod \, \wp \; x \in \mathcal{O}_L right\}.$$

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

$$G_i = \left\{\sigma \in G_0,\, \sigma(x) \equiv x \, mod\, \wp^{i+1},\, x \in \mathcal{O}_L\right\}$$

est appelé i-ème groupe de ramification.

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

Théorème 2.34 *Sous les hypothèses ci dessous on a*

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

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

Corollaire 2.35 *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 rmification 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 2.36 *(Critère de van der Waerden-Dedekind)*
Soit K un corps de nombres algébrique et L la clôture normale de K sur $\mathbb{Q}$ de groupe de Galois G.
Soit $\wp$ un idéal premier de L au dessus d'un nombre premier p.

On considère $\mathcal{D}_\wp$ et $\mathcal{I}_\wp$ les deux sous groupes de G que sont respectivement le groupe de décomposition et le groupe d'inertie de $\wp$ dans L.
On suppose que la décomposition de $p\mathcal{O}_K$ est de la forme

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

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

Proposition 2.37 *Soient K K' deux corps et $\sigma \in Hom_{\mathbb{Q}}(K, K')$. On considère $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers de K et K' respectivement, $|\ |_{\mathfrak{p}}$ et $|\ |_{\mathfrak{p}'}$ les valeurs absolues définies sur K et K' respectivement. Alors σ préserve les valeurs absoulues si, et seulement si, $\sigma_{-1}(\mathfrak{p}') = \mathfrak{p}$*

En particulier, si $K = K' = L$ est une extension galoisienne on a

Corollaire 2.38 *Soit L un corps de nombres galoisien, pour tout idéal premier $\wp$ de L le sous-groupe de $Gal(L/\mathbb{Q})$ qui préserve la valeur absolue $|\ |_\wp$ n'est autre que $\mathcal{D}_\wp$, le groupe de décoposition $\mathcal{D}_\wp$.*

Proposition 2.39 *Soit L/K une extension galoisienne, $|\ |_L$ une valeur absolue définie sur L. Alors $\hat{L}/\hat{K}$ est une extension galoisienne et $Gal\left(\hat{L}/\hat{K}\right)$ s'identifie canoniquement au sous-groupe de $Gal(L/K)$ qui préserve la valeur absolue $|\ |_L$.*

Exemple 19 *Soit $F(X) = X^5 + 20X + 16$, il est irréductible sur $\mathbb{Q}$ puisque $g(X) = F(X-1) = X^5 - 5X^4 + 10X^3 - 10X^2 + 25X - 5$ est d'Eisentein 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.
D'autre part, le disciminant de F est égal à $2^{16} \times 5^6$,c'est un carré, alors

$G \subset A_5$.
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 θ une racine de F dans L, la décomposition de 2 dans $K = \mathbb{Q}(\theta)$ est $2 = \mathfrak{p}^4\mathfrak{q}$. Alors, par le critère de Van der Waerden-Dedekind, legroupe 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 La différente

Soit F un corps de nombres p-adique et E une extension galoisiennne de F de degré $n = \mathrm{Gal}(E/F)$.
Soit $\wp$ l'idéal maximal de l'anneau $\mathcal{O}_E$ des entiers de E sur F, et on note $\mathfrak{D}(E/F)$ la différente de l'extension E/F.

Théorème 2.40 *La différente $\mathfrak{D}(E/F)$ est donnée par*

$$\mathfrak{D}(E/F) = \wp^{e-1+\sum_{i=1}^{t}(card\ G_i - 1)}$$

où G_t est le dernier groupe de ramification, $e = e(E/F)$ est l'indice de ramification de l'extension E/F .

Remarque 5 *notons quelques conséquences du théorème précédent :*

- *Si $p \nmid e$, alors E/F est modérément ramifiée et G_1 est d'ordre 1 et il en sera de mêmes de tous les i-èmes groupes de ramification G_i, $i \geq 2$. Par conséquent, on aura*
$$\mathfrak{D}(E/F) = \wp^{e-1}.$$

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

Comme application du dernier résultat, examinons la situation d'une extension normale $L/\mathbb{Q}_p$ de degré fini.
Soit $e = e(L/\mathbb{Q}_p)$ et $f = f(L/\mathbb{Q}_p)$ l'indice de ramification et le degré résiduel de l'extension normale $L/\mathbb{Q}_p$, alors $n = [L : \mathbb{Q}_p] = ef$.
Soit $\wp$ l'idéal maximal de $\mathcal{O}_L$, alors

$$\mathfrak{D}(L/\mathbb{Q}_p) = \wp^d, \text{ où } \begin{cases} d = e-1, & \text{si } p \nmid e \\ d \geq e, & \text{si } p \mid e \end{cases} \text{ et } \mathrm{N}_{L/\mathbb{Q}_p}(\wp) = p^f.$$

Le discriminant $\mathrm{d}_{L/\mathbb{Q}_p}$ de l'extension $L/\mathbb{Q}_p$ est donné par la relation

$$\mathrm{d}_{L/\mathbb{Q}_p} = \mathrm{N}_{L/\mathbb{Q}_p}(\mathfrak{D}(L/\mathbb{Q}_p)) = p^{fd}$$

Proposition 2.41 *Si L/K est une extension de degré fini de corps de nombres p-adiques sauvagement ramifiée, alors la différente $\mathfrak{D}_{L/K}$ de l'extension L/K est divisible par $\mathfrak{q}^e$, où $e = e(L/K)$ et $\mathfrak{q}$ étant l'idéal maximal de $\mathcal{O}_L$.*

2.8 Passage du global au local

Dans cette section nous allons décliner un dictionnaire qui interprète des situations locales pour les interpréter au niveau global.
On considère un corps de nombre L galoisien sur $\mathbb{Q}$ de groupe de Galois G, et $K/\mathbb{Q}$ une extension de degré n contenue dans L.
Soit $p \in \mathbb{Z}$, p un nombre premier, et $\wp$ un idéal premier de L au dessus de p.
On considère la factorisation de p dans K

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}, \text{ avec } \mathrm{N}_{K/L}(\mathfrak{p}_i) = p^{f_i}$$

On pose $K_i = K_{\mathfrak{p}_i}$, $1 \leq i \leq g$, et on note $\underline{K_i}$ l'ensemble formé par les n_i $\mathbb{Q}_p$-morphismes $K_i \longrightarrow L_\wp$ où $n_i = e_i f_i$.
Chaque $\underline{K_i}$ est isomorphe canoniquement à l'orbite de $\underline{K}$ sous l'action de $\mathcal{D}_\wp$ associé à $\mathfrak{p}_i$. On note par K_i^{gal} le composé des $\sigma(K_i)$, $\sigma \in \underline{K_i}$, c'est une extension galoisienne de $\mathbb{Q}_p$.
Connaissant les groupes d'inertie des extensions locales $K_i^{gal}/\mathbb{Q}_p$, $1 \leq i \leq g$, on en déduit des précisions sur $\mathcal{I}_\wp$

Nous sommes en mesure de déduire quelques résultats de l'aritmétique des corps au niveau local et global.

Commençons par l'isomorphisme suivant

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

Du point de vue des dimension, on aura

$$n = \dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}_p} (K \otimes_{\mathbb{Q}} \mathbb{Q}_p)$$

$$= \dim_{\mathbb{Q}_p} \prod_{i=1}^{g} K_i = \sum_{i=1}^{g} \dim_{\mathbb{Q}_p} K_i$$

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

Du point de vue des anneaux des entiers on a

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

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

$$\mathrm{disc} K = \prod_{i=1}^{g} \mathrm{disc} K_i$$

par suite

$$v_p\left(\text{disc}K\right)=\sum_{i=1}^{g}v_p\left(\text{disc}K_i\right)$$

ce qui assure le passage du local au global.

Exemple 20 *Etude d'une situation locale.*
Examinons un exemple d'une extension locale dont le discriminat de valuation p-adique petite.
Soit E un corps de nombres p-adique, p premier, dont les notations sont regroupées dans la ligne suivante

$$\Gamma=Gal\left(E^{gal}/\mathbb{Q}_p\right)\quad \mathcal{I}=\mathcal{I}\left(E^{gal}/\mathbb{Q}_p\right)\quad \underline{E}=Hom_{\mathbb{Q}_p}\left(E,E^{gal}\right)$$

Soit $\mathfrak{D}_{E/\mathbb{Q}_p}$la différente de l'extension $E/\mathbb{Q}_p$, $\mathfrak{q}$ l'idéal maximal de $\mathcal{O}_E$, on pose

$$\mathfrak{D}_{E/\mathbb{Q}_p}=\mathfrak{q}^d,\ m=v_p\left(discE\right)$$

alors on a

$$m=fd,\ avec\ \begin{cases} d=e-1, & si\ p\nmid e \\ d\geq e & si\ p\mid e \end{cases}.$$

Nous allons décliner les extensions $E/\mathbb{Q}_p$ telles que $1\leq m\leq 3$, et déterminer dans chaque cas l'image du groupe d'inertie de $\mathfrak{q}$ dans S_n.
le tableau suivant donne les valeurs de f, n et e dans chacun des cas examinés ci-dessus.

<table>
<tr><th></th><th>$d=1$</th><th colspan="2">$d=2$</th><th colspan="3">$d=3$</th></tr>
<tr><td>$m=1$</td><td>$f=1$
$e=2$
$n=2$
$p\neq 2$
$\mathcal{I}=S_2$</td><td colspan="2">*impossible*</td><td colspan="3">*impossible*</td></tr>
<tr><td>$m=2$</td><td>$f=3$
$e=2$
$n=4$
$p\neq 2$
$\mathcal{I}=<$ *double transitivité* $>$</td><td colspan="2">$f=1$
$e=3$ | $e=2$
$n=2$ | $n=2$
$p\neq 3$ | $p=2$
$\mathcal{I}=A_3$ | $\mathcal{I}=S_2$</td><td colspan="3">*impossible*</td></tr>
<tr><td>$m=3$</td><td>$f=3$
$e=2$
$n=6$
$p\neq 2$
$\mathcal{I}=<$ *triple transposition* $>$</td><td colspan="2">*impossible*</td><td colspan="3">$f=1$
$e=4$ | $e=2$ | $e=3$
$n=4$ | $n=2$ | $n=3$
$p\neq 2$ | $p=2$ | $p=3$
$\mathcal{I}=C_4$ | $\mathcal{I}=S_2$ | $\mathcal{I}=S_3$</td></tr>
</table>

Conclusions :

Le valeurs de e, f, n et p du tableau sont obtenues en utilisant directement les relations suivantes

$$m=fd,\ n=ef \ \ et \ \begin{cases} e=d+1, & si\ p\nmid e \\ e\leq d, & si\ p\mid e \end{cases}$$

Pour cerner le groupe d'inertie $\mathcal{I}$, nous utilisons le critère de Van der Waerden-Dedekind ainsi que les résultats suivants :

- Le groupe Γ est constitué de permutations paires de Perm $(\underline{E})$ si, et seulement si, disc$E\in(\mathbb{Q}_p)^2$.
- Soit $\mathcal{O}$ l'anneau des entiers de E^{gal} et $\mathfrak{q}$ l'idéal maximal de $\mathcal{O}$. Alors

$$I=\{\sigma\in\Gamma,\ \sigma(x)\equiv x \mod \mathfrak{q},\ \forall x\in\mathcal{O}\}$$

est le groupe d'inertie de $\mathfrak{q}$ dans E^{gal} , et on a

$$I_1 = \left\{\sigma \in I,\, \sigma(x) \equiv x \mod \mathfrak{q}^2,\, x \in \mathcal{O}\right\}$$

est le 1er groupe de ramification, et on a $I \simeq I_1 \times I/I_1$, où I_1 est un groupe cyclique d'ordre premier avec p.
Ainsi, l'extension $E^{\text{gal}}/\mathbb{Q}_p$ est modérément ramifiée si et seulement si $\#\, I_1 = 1$, et par suite I est cyclique.

Toutefois, il est utile d'expliquer les résultats du tableau ci-dessus.

- La première ligne s'obtient très aisément.
- Dans les cases (2.1) et (2.2) colonne1, le critère de Van der Waerden-Dedekind permet d'obtenir respectivement les injection $I \hookrightarrow S_2 \times S_2$ et $I \hookrightarrow S_3$. Mais dans les deux cas, l'extension $E^{\text{gal}}/\mathbb{Q}_p$ est modérément ramifiée, ce qui implique que I est cyclique.
- Dans la case (3.1) on a l'injection $I \hookrightarrow S_2 \times S_2 \times S_3$, d'après le critère de Van der Waerden-Dedekind. Comme l'extension $E^{\text{gal}}/\mathbb{Q}_p$ est modérément ramifiée, alors I est cyclique.
- Dans la case (3.3) colonne 1, le critère de Van der Waerden-Dedekind implique l'injection $I \hookrightarrow S_4$(I est un sous-groupe transitif de S_4, de plus $E^{\text{gal}}/\mathbb{Q}_p$ est modérément ramifiée. Comme les sous-groupes transitifs de S_4 sont : S_4, A_4, D_4, C_4 et $(\mathbb{Z}/2\mathbb{Z})^2$, alors $I = C_4$.
- Dans la case (3.3), le groupe I est un sous groupe transitif de S_3, donc $I = S_3$ ou bien $I = A_3$. Comme disc$E \notin (\mathbb{Q}_p)^2$, car m est impair, alors $I = S_3$.

2.9 Polygone de Newton et ramification

On se donne un polynôme $f(X) \in \mathbb{Q}_p[X]$; de degré n, et $\phi(X)$ un polynôme unitaire de degré m

m à coefficients entiers p-adiques. Le développement de f suivant les puissaces de $\phi(X)$, donné par la division euclidienne, est

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

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

Définition 2.42 *Le $(p, \phi)-$polygone de $f(X)$ est la frontière de l'enveloppe convexe supérieur de l'ensemble des points (j, α_j), sans la partie verticale. La partie du $(p, \phi)-$polygone diminuée de la partie horizontale (s'il y a lieu) est appelée partie principale du $(p, \phi)-$polygone.*

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

l_0 := longueur du côté horizontal

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

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

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

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

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

de l'expression

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

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

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

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

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

Définition 2.43 *On appelle polynôme associé à $f(X)$ et relatif au côté S_i, le polynôme $F_i(X, Y)$ donné par*

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

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

La relation entre (p, ϕ)-polygone et ramification est donnée par

Théorème 2.44 (4, Theoreme 1.5) *Soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire irréductible tel que $f(X) \mod p$ n'est pas irréductible, et soit θ une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$ fixée. On considère la factorisation modulo p de f(X)*

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

où $\phi_\nu(X) \in \mathbb{Z}[X]$ de degré $deg\phi(X) = m_\nu$. Alors,

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

où les $\mathfrak{a}_\nu$ sont des idéaux de $K = \mathbb{Q}(\theta)$ tels que $N_K(\mathfrak{a}_i) = p^{a_\nu m_\nu}$
(N_K désigne la norme absolue du corps K).
A chaque idéal $\mathfrak{a} = \mathfrak{a}_\nu$ correspond un facteur irréductible $\phi(X) = \phi_\nu(X)$. On détermine ainsi le $(\mathbb{Q}_p, \phi)$ polygone de $f(X)$. Pour chaque côté S_i de la partie principale de ce polygone, on considère la factorisation modulo (p, ϕ) du polynôme associé $F_i(X, Y)$

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

Alors

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

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

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

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

Exemple 21 *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 θ une racine de $f(X)$ dans $\overline{\mathbb{Q}}$, la clôture algébrique 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 la factorisation de $f(X)$ modulo 5 :

$$\overline{f}(X) = (X+2)\left(X^2+3X+4\right) \in \frac{\mathbb{Z}}{71\mathbb{Z}}[X]$$

On pose

$$\varphi_1(X) = X+2, \text{ et } \varphi_2(X) = X^2+3X+4\,.$$

Ainsi, la factorisation de $f(X)$ modulo 5 donne :

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

où les $\mathfrak{a}_i$ et $\mathfrak{a}_2$ sont des idéaux de $\mathcal{O}_K$ premiers entre eux tels 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 non nul de $\mathcal{O}_K$ de norme absolue égale à $N_{K/\mathbb{Q}}(\mathfrak{p}_1) == 5$.
La partie principale du $(5,\varphi_2)$-polygone de $f(X)$ est formée d'un seul côté reliant les points $(0,0)$ et $(1,1)$, il lui 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 non nul de $\mathcal{O}_K$ de norme absolue égale à $N_{K/\mathbb{Q}}(\mathfrak{p}_2) = 25$.

Par conséquent, $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ *avec* $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_1} : \mathbb{F}_5\right] = 1$ *et* $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_2} : \mathbb{F}_5\right] = 2$*, où* $\mathfrak{p}_1$ *et* $\mathfrak{p}_2$ *sont des idéaux distincts puisqu'il sont de normes différentes.*

Chapitre 3

Décomposition d'un nombre premier dans une extension cubique

Soit $f(X) = X^3 - aX + b \in \mathbb{Z}[X]$ un polynôme irréductible, θ une racine de $f(X)$ dans $\overline{\mathbb{Q}}$.
On considère $K = \mathbb{Q}(\theta)$, le corps de nombre engendré par une racine θ de $f(X)$. Nous allons examiner dans ce qui suit la factorisation d'un nombre premier p dans l'anneau des entiers $\mathcal{O}_K$ du corps K.
On suppose que les entiers a et b vérifient simultanément

$$v_p(a) \geq 2 \text{ et } v_p(b) \geq 3$$

alors le polynôme $g_1(X)$ donné par

$$g_1(X) = \frac{1}{p^3} f(pX) = X^3 - a_1 X + b_1$$

où $a_1 = \dfrac{a}{p^3}$ et $b_1 = \dfrac{b}{p^3}$ est irréductible dont une racine engendre K sur $\mathbb{Q}$.
Si $v_p(a_1) \geq 2$ et $v_p(b_2) \geq 3$, on réitère la même construction et on obtient un polynôme irréductible $g_2(X)$

$$g_2(X) = \frac{1}{p^3} g(pX) = X^3 - a_2 X + b_2$$

Par la technique de la descente on aboutit à un trinôme de la forme

$$g_k(X) = \frac{1}{p^3} g_{k-1}(pX) = X^3 - a_k X + b_k$$

tels que $v_p(a_k) < 2$ ou bien $v_p(b_k) < 3$ Désormais, pour la suite on considère le polynôme

$$f(X) = X^3 - aX + b \in \mathbb{Z}[X]$$

vérifiant l'une aiu moins des conditions suivantes

$$v_p(a) < 2 \text{ ou } v_p(b) < 3$$

Le discriminant Δ de ce trinôme est égal à $\Delta = 4a^3 - 27b^2$.

Pour tout nombr premier p, On note par s_p la valuation p-adique de ce discriminant et $\Delta_p = \dfrac{\Delta}{p^{s_p}}$

3.1 Problématique

On considère un polynôme irréductible dans $\mathbb{Z}[X]$, $f(X) = X^3 - aX + b$ dont les coefficients a et b vérifient l'une au moins des condition

$$v_p(a) < 2 \text{ ou bien } v_p(b) < 3.$$

Soit $K = \mathbb{Q}(\theta)$, où θ est une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$.
Le discriminant Δ de $f(X)$ est donné par

$$\Delta = 4a^3 - 27b^2$$

il est lié au discriminant absolu d_K du corps K par la relation

$$\Delta = i(\theta)^2 d_K$$

Nous allons dans ce qui suivra déterminer la décomposition de l'idéal $p\mathcal{O}_K$ dans l'anneau $\mathcal{O}_K$ des entiers du corps de nombres K.
Nous aurons besoin pour la suites de certains lemmes utiles pour la preuve des résultats donnant cette décomposition.

Lemme 1 *(Dedekind)*
Soit $g(X)$ un polynôme irréductible, ω une racine de $g(X)$ et soit $L = \mathbb{Q}(\omega)$. Soit p un nombre premier et on considère la factorisation de $g(X)$ modulo p suivante

$$g(X) \equiv \varphi_1(X)^{e_1} \dots \varphi_r(X)^{e_r} \ mod\ p$$

où les φ_i sont irréductibles.
Si $p \nmid i(\omega)$, alors on a

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

où les $\mathfrak{p}_i = (p, \varphi_i(\omega))$, $1 \leq i \leq r$, sont des idéaux premiers de $\mathcal{O}_K$ au dessus de p, de degrés résiduel respectifs $f(\mathfrak{p}_i/p) = \deg(\varphi_i)$.

Lemme 2 *(Dedekind)*
Soit $g(X) \in \mathbb{Z}[X]$ un polynôme irréductible, ω une racine de $g(X)$ et $L = \mathbb{Q}(\omega)$.

Pour tout nombre premier p, on suppose que

$$g(X) = \varphi_1(X)^{e_1} \dots \varphi_r(X)^{e_r} + pM(X)$$

où $M(X) \in \mathbb{Z}[X]$. Alors , Pour tout i tel que $e_i > 1$, $p \nmid i(\omega)$si, et seulement si, $\varphi_i(X) \nmid M(X)$ mod p.

Lemme 3 *3(Bauer)*
On considère les hypothèses du Lemme 1. A chaque idéal $\mathfrak{p}$ de L au dessus de p, le quotient $\frac{v_p(\omega)}{e(\mathfrak{p}/p)}$ est la pente de l'un des côtés du polygone de Newton de $g(X)$ relatif à p. Inverssement, si λ est la pente d'un côté du polygone de Newton de $g(X)$ relatif à p, alors il existe un idéal premier $\mathfrak{p}$ de L au dessus de p tel que $\lambda = \frac{v_p(\omega)}{e(\mathfrak{p}/p)}$.

Lemme 4 *4 Soit $f(X) = X^3 - aX + b \in \mathbb{Z}[X]$ un polynôme irréductible, θ une racine de $f(X)$ dans $\mathbb{Q}^{alg}$.*
On considère $K = \mathbb{Q}(\theta)$, le corps de nombre engendré par une racine θ de $f(X)$ et Δ le discriminant de $f(X)$.

- *Si $p\mathcal{O}_K = \mathfrak{pq}^2$ dans K et $p \neq 2$, alors $v_p(d_K) = 1$.*
- *Si $p\mathcal{O}_K = \mathfrak{p}^3$ dans K et $p \neq 3$, alors $v_p(d_K) = 2$.*
- *Si $2\mathcal{O}_K = \mathfrak{pq}^2$ dans K, alors $v_2(d_K) = 2$ ou 3.*
- *Si $3\mathcal{O}_K = \mathfrak{p}^3$ dans K, alors $v_3(d_K) = 3$, 4 ou 5.*

Lemme 5 *5 On considère les mêmes hypothèses du Lemme 4.*

- *Si $p\mathcal{O}_K = \mathfrak{p}$ ou $p\mathcal{O}_K = \mathfrak{pqa}$ dans K, alors $\Delta \in \mathbb{Q}_p^2$.*

- *Si* $p\mathcal{O}_K = \mathfrak{pq}$ *ou* $p\mathcal{O}_K = \mathfrak{pq}^2$ *dans* K*, alors* $\Delta \notin \mathbb{Q}_p^2$.

La factorisation de p dans $\mathcal{O}_K$ est donnée par

Théorème 3.1 *On suppose les hypothèses du lemme 4 précédent sont données. Alors la décomposition d'un nombre premier* 2 *dans* K *est donnée comme suit :*

- *Si* $\begin{cases} a \text{ pair} \\ b \text{ pair} \end{cases}$ *alors* $\begin{array}{c} 1 \leq v_2(b) \leq v_2(a) \text{ si, et seulement si, } 2\mathcal{O}_K = \mathfrak{p}^3 \\ 1 = v_2(a) < v_2(b) \text{ si, et seulement si,} 2\mathcal{O}_K = \mathfrak{pq}^2 \end{array}$
- *Si* $\begin{cases} a \text{ pair} \\ b \text{ impair} \end{cases}$ *alors* $2\mathcal{O}_K = \mathfrak{pq}$
- *Si* $\begin{cases} a \text{ impair} \\ b \text{ pair} \\ s_2 \text{ pair} \end{cases}$ *alors* $\begin{array}{c} \Delta_2 \equiv 3 \bmod 4 \text{ si, et seulement si,} 2\mathcal{O}_K = \mathfrak{pq}^2 \\ \Delta_2 \equiv 5 \bmod 8 \text{ si, et seulement si,} 2\mathcal{O}_K = \mathfrak{pq} \\ \Delta_2 \equiv 1 \bmod 8 \text{ si, et seulement si,} 2\mathcal{O}_K = \mathfrak{bpq} \end{array}$
- *Si* $\begin{cases} a \text{ impair} \\ b \text{ pair} \\ s_2 \text{ impair} \end{cases}$ *alors* $2\mathcal{O}_K = \mathfrak{pq}^2$
- *Si* $\begin{cases} a \text{ impair} \\ b \text{ impair} \end{cases}$ *alors* $2\mathcal{O}_K = \mathfrak{p}$

Théorème 3.2 *On suppose les hypothèses du lemme 4 précédent sont vérifiées. La décomposition du nombre premier* 3 *dans* K *est donnée comme suit*

- *Si* $\begin{cases} 3 \mid a \\ 3 \mid b \end{cases}$ *alors* $\begin{array}{c} 1 \leq v_3(b) \leq v_3(a) \text{ si, et seulement si, } 3\mathcal{O}_K = \mathfrak{p}^3 \\ 1 = v_3(a) < v_3(b) \text{ si, et seulement si,} 3\mathcal{O}_K = \mathfrak{pq}^2 \end{array}$
- *Si* $\begin{cases} 3 \nmid a \\ 3 \nmid b \end{cases}$ *alors* $\begin{array}{c} a \equiv 1 \bmod 3 \text{ implique } 3\mathcal{O}_K = \mathfrak{p} \\ a \equiv -1 \bmod 3 \text{ et } b \equiv 1 \bmod 3 \text{ impliquent } 3\mathcal{O}_K = \mathfrak{p}^2 \\ a \equiv -1 \bmod 3 \text{ et } b \equiv -1 \bmod 3 \text{ impliquent } 3\mathcal{O}_K = \mathfrak{pq} \end{array}$

- $Si \begin{cases} 3 \nmid a \\ 3 \mid b \end{cases} \quad alors \quad \begin{array}{c} a \equiv 1 \mod 3 \text{ implique } 3\mathcal{O}_K = \mathfrak{b}\mathfrak{p}\mathfrak{q} \\ a \equiv -1 \mod 3 \text{ implique } 3\mathcal{O}_K = \mathfrak{p}\mathfrak{q} \end{array}$

- $Si \begin{cases} 3 \mid a \\ 3 \nmid b \end{cases}$
$$\begin{cases} a \equiv 3 \mod 9 \\ b^2 \equiv a+1 \mod 27 \\ s_3 \text{ impair} \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$$
$$\begin{cases} a \equiv 3 \mod 9 \\ b^2 \not\equiv a+1 \mod 27 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}^3$$
$$\begin{cases} a \equiv 3 \mod 9 \\ b^2 \equiv a+1 \mod 27 \\ s_3 \text{ pair} \\ \Delta_3 \equiv -1 \mod 3 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$$
$$\begin{cases} a \equiv 3 \mod 9 \\ b^2 \equiv a+1 \mod 27 \\ s_3 = 6 \\ \Delta_3 \equiv 1 \mod 3 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}$$
$$\begin{cases} a \equiv 3 \mod 9 \\ b^2 \equiv a+1 \mod 27 \\ 6 < s_3 \text{ pair} \\ \Delta_3 \equiv 1 \mod 3 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{b}\mathfrak{p}\mathfrak{q}$$
$$\begin{cases} a \not\equiv 3 \mod 9 \\ b^2 \equiv a+1 \mod 9 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$$
$$\begin{cases} a \not\equiv 3 \mod 9 \\ b^2 \not\equiv a+1 \mod 9 \end{cases} \text{impliquent } 3\mathcal{O}_K = \mathfrak{p}^3$$

Théorème 3.3 *On suppose que les hypothèses du Lemme 4 précédent sont vérifiées. La décomposition d'un nombre premier $p > 3$ est donnée comme suit :*

- $Si \begin{cases} p \mid a \\ p \mid b \end{cases} \quad alors \quad \begin{array}{c} 1 \leq v_p(b) \leq v_p(a) \text{ si, et seulement si, } p\mathcal{O}_K = \mathfrak{p}^3 \\ 1 = v_p(a) < v_p(b) \text{ si, et seulement si,} p\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2 \end{array}$

$$p \equiv -1 \mod 3 \text{ implique } p\mathcal{O}_K = \mathfrak{pq}$$

- $\begin{cases} p \mid a \\ p \nmid b \end{cases}$ alors $\begin{cases} p \equiv 1 \mod 3 \\ \left(\frac{b}{p}\right)_3 = 1 \end{cases}$ imlpiquent $p\mathcal{O} = \mathfrak{pq}\mathfrak{R}$

  $\begin{cases} p \equiv 1 \mod 3 \\ \left(\frac{b}{p}\right)_3 \neq 1 \end{cases}$ imlpiquent $p\mathcal{O} = \mathfrak{p}$

- Si $\begin{cases} p \nmid a \\ p \mid b \end{cases}$ alors $\left(\frac{a}{p}\right) = 1$ implique $p\mathcal{O}_K = \mathfrak{bpq}$

  $\left(\frac{a}{p}\right) = -1$ implique $p\mathcal{O}_K = \mathfrak{pq}$

$$s_p \text{ impair implique } p\mathcal{O}_K = \mathfrak{pq}^2$$

- Si $p \nmid ab$, alors $\begin{cases} s_p \text{ pair} \\ \left(\frac{\Delta_p}{p}\right) = 1 \\ f(X) \text{ admet des racines dans } \mathbb{F}_p \end{cases}$ impliquent $p\mathcal{O}_K = \mathfrak{bpq}$

  $\begin{cases} s_p \text{ pair} \\ \left(\frac{\Delta_p}{p}\right) = 1 \\ f(X) \text{ est irréductible dans } \mathbb{F}_p[X] \end{cases}$ impliquent $p\mathcal{O}_K = \mathfrak{p}$

  $\begin{cases} s_p \text{ pair} \\ \left(\frac{\Delta_p}{p}\right) = -1 \end{cases}$ impliquent $p\mathcal{O}_K = \mathfrak{pq}$

Preuve : Nous démontrons les théorèmes ci-dessus en examinant chacun des cas cités dans ces théorèmes

$p \mid a$ et $p \mid b$, d'après le théorème on a $3v_p(a) \neq 2v_p(b)$ ce qui montre que les seules possibilités sont

$$2 \leq 2v_p(b) < 3v_p(a) \text{ et } 3 \leq 3v_p(a) < 2v_p(b).$$

Pour la première possibilité on a $1 \leq v_p(b) \leq v_p(a)$, le polygone de Newton

de $f(X)$relatif à p est formé d'un seul côté de pente $\frac{1}{3}$ ou $\frac{2}{3}$. Alors, d'après le Lemme 3, p se factorise dans $\mathcal{O}_K$ comme suit :

$$p\mathcal{O}_K = \mathfrak{p}^3$$

où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$.
Pour la seconde possibilité, on a $v_p(a) = 1$ et $v_p(a) < v_p(b)$, et le polygone de Newton de $f(X)$ est formé de 2 côtés de pentes respectivement $\frac{1}{2}$ et $\frac{v_p(b)-1}{1}$. Alors, et d'après le Lemme 3, p se factorise dans $\mathcal{O}_K$ comme suit :

$$p\mathcal{O}_K = \mathfrak{pq}^2.$$

où $\mathfrak{p}$ et $\mathfrak{q}$ sont des idéaux premiers distincts de $\mathcal{O}_K$.

$p \nmid a$ et $p \mid b$. Dans ce cas $f(X) \equiv X(X^2 - a) \bmod p$ et par suite dans $\mathcal{O}_K$ on a la faactorisation

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

où $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux de $\mathcal{O}_K$, non nuls et premiers entre eux, ainsi il y a au moins deux idéaux premiers de K au dessus de p.

- Si $p \neq 2$ alors $s_p = 0$ et par suite $p \nmid i(\theta)$ et le lemme 1 entraine

$$p\mathcal{O}_K = \begin{cases} \mathfrak{bpq} & \text{si } \left(\frac{a}{p}\right) = 1 \\ \mathfrak{pq} & \text{si si } \left(\frac{a}{p}\right) = -1 \end{cases}$$

- Si $p = 2$ alors $s_2 \geq 1$.
  Si s_2 est impair et $2 \mid D$ alors 2 se ramifie dans K : $2\mathcal{O}_K = \mathfrak{pq}^2$.
  Si s_2 est pair, d'après le Lemme 5 on a $2\mathcal{O}_K = \mathfrak{bpq}$ si , et seulemnt si, $\Delta \in \mathbb{Q}_2^2$ ce qui équivaut à $\Delta_2 \equiv 1 \bmod 8$.

- Si $\Delta_2 \not\equiv 1 \bmod 8$, alors $f(X) = g(X)h(X)$ dans $\mathbb{Z}_2[X]$, avec $\deg g(X) = 1$ et $\deg h(X) = 2$, $h(X)$ et $g(X)$ sont irréductibles dans $\mathbb{Z}_2[X]$. Par

suite on a $2\mathcal{O}_K = \mathfrak{pq}$ si, et seulement si, l'extension quadratique de $\mathbb{Q}_2$ engendrée par les racines de $h(X)$ est non ramifiée.
Comme $\mathbb{Q}_2\left(\sqrt{5}\right)$ est l'unique extension non ramifiée de $\mathbb{Q}_2$ alors $2\mathcal{O}_K = \mathfrak{pq}$ si, et seulement si, l'extension quadratique de $\mathbb{Q}_2$ définie par les racines de $h(X)$ et $\mathbb{Q}_2\left(\sqrt{5}\right)$, et ceci est valable si et seulement si $\Delta_2 \equiv 5 \mod 8$

Si $p \mid a$ et $p \nmid b$, alors $f(X) \equiv X^3 + b \mod p$.

- Supposons que $p \neq 3$, alors $s_p = 0$.
  Soit $\overline{g}$ un générateur du groupe cyclique $\left(\mathbb{F}_p^*, \cdot\right)$, alors b est un résidu cubique modulo p, ce qui entraine

$$f(X) \equiv (X - \overline{\alpha})\left(X^2 - \overline{\alpha}X + \alpha^2\right) \mod p$$

  avec $\overline{\alpha}^3 = \overline{b}$; comme

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

  alors le polynôme $X^2 - \overline{\alpha}X + \alpha^2$ est irréductible dans $\mathbb{F}_p$. Ainsi, par le Lemme 1, on a

$$p\mathcal{O}_K = \mathfrak{pq}, \text{ avec } f(\mathfrak{p}/p) = 1 \text{ et } f(\mathfrak{q}/p) = 2.$$

  Si $p \equiv 1 \mod 3$ et $\left(\frac{b}{p}\right)_3 = 1$, alors $\overline{f}(X)$ admet 3 racines distinctes dans $\mathbb{F}_p^*$, puisque $\overline{f}(X)$ est séparable ce qui entraine, d'après le Lemme 1, entraine

$$p\mathcal{O}_K = \mathfrak{bpq}.$$

  Si $p \equiv 1 \mod 3$ et $\left(\frac{b}{p}\right)_3 \neq 1$, alors $\overline{f}(X)$ est irréductible sur $\mathbb{F}_p[X]$, et d'après le Lemme 1 on aura

$$p\mathcal{O}_K = \mathfrak{p} \text{ avec } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p^3.$$

- Supposons que $p = 3$, dans ce cas $f(X) \equiv (X+b)^3 \mod 3$. On pose $\theta_1 = \theta + b$ racine du polynôme $f_1(X) = f(X-b)$, alors

$$f_1(X) = X^3 - 3bX^2 + \left(3b^2 - a\right)X - \left(b^3 - ab - b\right)$$

Comme $b^2 \equiv 1 \mod 3$, alors $3b^2 \equiv 3 \mod 9$.

  - Si $a \not\equiv 3 \mod 9$, alors $3b^2 - a \not\equiv 0 \mod 9$ ce qui entraine que $v_3(3b^2 - a) = 1$ et donc $v_3(b^3 - ab - b) = v_3(3b^2 - a - 1)$, puisque $p \nmid b$.
  - Si $b^2 \equiv a + 1 \mod 9$, alors $v_3(b^2 - a - 1) \geq 2$. Ainsi, le $(3, X)$-polygone de $f_1(X)$ est formé de 2 côtés dont l'un est de pente égale à $\frac{1}{2}$ et l'autre de pente égale à $\dfrac{v_3(b^2 - a - 1)}{1}$, ce qui d'après le Lemme 3 entraine $3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$.
  - Si $a \not\equiv 3 \mod 9$ et $b^2 \not\equiv a+1 \mod 9$, alors $v_3(3b^2 - a) = v_3(-b^3 + ab + b) = 1$. Ainsi le $(3, X)$-polygone de $f_1(X)$ est formé d'un côté de pente $\dfrac{1}{3}$, d'après le Lemme on aura $3\mathcal{O}_K = \mathfrak{p}^3$.

- Supposons que $a \equiv 3 \mod 9$.

  - Si $b^2 \not\equiv a + 1 \mod 27$, alors le $(3, X)$-polygone de $f_1(X)$ est formé d'un côté de pente $\dfrac{1}{3}$ ou $\dfrac{2}{3}$ selon que 9 divise ou non $b^2 - (a+1)$. Ainsi, d'après le Lemme 3, $3\mathcal{O}_K = \mathfrak{p}^3$.
  - Si $b^2 \equiv a+1 \mod 27$ on pose $\theta_2 = \dfrac{\theta_1}{3}$ de polynôme minimal $f_2(X) = \dfrac{f_1(3X)}{3^3}$

$$f_2(X) = X^3 - bX^2 + \frac{3b^2 - a}{9}X - \frac{b^3 - ab - b}{3^3}.$$

Puisque $3 \nmid b$, alors $f_2(X) \not\equiv (X+c)^3 \mod 3$, $c \in \mathbb{Z}$, ce qui implique

que $3\mathcal{O}_K \neq \mathfrak{p}^3$ et d'après le théorème de Ore

$$3\mathcal{O}_K = \mathfrak{p} \text{ si, et seulement si } f(X) \bmod 3 \text{ est irréductible.}$$

- Si $3\mathcal{O}_K = \mathfrak{pq}^2$, alors s_3 est impair d'après le Lemmme 4 .
  Inversement, si s_3 est impair, alors la valuation 3-adique $v_3(d_K)$ du discriminat d_K est impaire, ce qui implique que 3 se ramifie dans K et donc $3\mathcal{O}_K = \mathfrak{pq}^2$.
- Si $3\mathcal{O}_K = \mathfrak{pq}$, alors s_3 est pair et $\Delta_3 \notin \mathbb{Q}_3^2$, ce qui veut dire que $\left(\frac{\Delta_3}{3}\right) = -1$.
  Inversement, si s_3 est pair et $\left(\frac{\Delta_3}{3}\right) = -1$, alors $3\mathcal{O}_K = \mathfrak{pq}$ d'après le Lemme 5. Notons que $\left(\frac{\Delta_3}{3}\right) = -1$ signifie que $\Delta \equiv -1 \bmod 3$.
- Si s_3 est pair et $\left(\frac{\Delta_3}{3}\right) = 1$, donc $\Delta \equiv 1 \bmod 3$, alors $\Delta \in \mathbb{Q}_3^2$. Comme le fait que $3\mathcal{O}_K = \mathfrak{pq}$ signifie, d'après le théorème de Ore, que $f_2(X)$ admet une seule racine modulo 3, par suite $\Delta \notin \mathbb{Q}_3^2$, ce qui contredit l'hypothèse. Ainsi $f_2(X)$ ne peut avoir une seule racine modulo 3.
  De plus, $f_2(X)$ ne peut admettre trois racines simple modulo 3 et ne peut admettre une racine triple puisque $3 \nmid b$.
  Ceci implique alors soit que $f_2(X)$ admet une racine simple et une racine double modulo 3, soit que $f_2(X)$ est irréductible dans $\mathbb{F}_3[X]$.
  Par suite on aura

$$3\mathcal{O}_K = \mathfrak{p} \text{ si, et seulement si, } f_2(X) \text{ est irréductible}$$

ou bien

$$3\mathcal{O}_K = \mathfrak{bpq} \text{ si, et seulement si, } f_2(X) \text{ n'est pas irréductible .}$$

On désigne par D_2 le discriminant de $f_2(X)$, alors $D_2 = \dfrac{\Delta}{27^2}$, par suite $v_3(D_2) = s_3 - v_3(27^2) = s_3 - 6$.
Supposons que $s_3 = 6$, alors $3 \nmid i(\theta)$. Dans ce cas, si $f_2(X)$ n'était pas irréductible dans $\mathbb{F}_3[X]$ alors d'après le Lemme 1 on aura $3\mathcal{O}_K = \mathfrak{pq}^2$ et par suite $\Delta \notin \mathbb{Q}_3^2$, ce qui absurde. Ainsi si $s_3 = 6$, alors $f_2(X)$ est irréductible .
Inversement, si $f_2(X)$ est irréductible dans $\mathbb{F}_3[X]$, alors $3\mathcal{O}_K = \mathfrak{p}$, alors 3 est non ramifié dans K et donc $3 \nmid D$, d'après le Lemme 1 on a $v_3(D_2) = 0$ et $s_3 = 6$.
Par conséquent, les proposition suivantes sont équivalentes

1. $s_3 = 6$, $3 \nmid D_2$ si, et seulement si, $f_2(X)$ est irréductible et $3\mathcal{O}_K = \mathfrak{p}$
2. $3\mathcal{O}_K = \mathfrak{bpq}$ si, et seulement si, $s_3 > 6$.

□

$p \nmid ab$.

- Si $p = 2$ ou $p = 3$, alors $s_p = 0$. Ainsi, par le Lemme 1, la décomposition de p dans K est le reflet de la décomposition de $\overline{f}(X)$ dans $\mathbb{F}_p[X]$.

- Si $p > 3$, alors $f(X) \equiv (X + c)^3 \bmod p$, par suite, le Théorème de Ore entraine $p\mathcal{O}_K \neq \mathfrak{p}^3$.
  D'autre part, et d'après le Lemme 4, nous avons :

$$p\mathcal{O}_K = \mathfrak{pq}^2 \text{ si et seulement si, } s_p \text{ est impair}$$

  et d'après le Lemme 5 on a

$$p\mathcal{O}_K = \mathfrak{pq} \text{ si et seulement si, } s_p \text{ est pair et } \left(\frac{\Delta_p}{p}\right) = -1.$$

Ainsi, on a

$$p\mathcal{O}_K = \mathfrak{p} \text{ ou } p\mathcal{O}_K = \mathfrak{bpq} \text{ si et seulement si, } s_p \text{est pair et } \left(\frac{\Delta_p}{p}\right) = 1.$$

Plus précisément,
Si s_p pair et $\left(\frac{\Delta_p}{p}\right) = 1$ et $f(X)$ mod p est irréductible dans $\mathbb{F}_p[X]$, alors $p\mathcal{O}_K = \mathfrak{p}$
Si s_p pair et $\left(\frac{\Delta_p}{p}\right) = 1$ et $f(X)$ mod p n'est pas irréductible dans $\mathbb{F}_p[X]$, alors $p\mathcal{O}_K = \mathfrak{bpq}$.

Exemple 22 (1)*Soit $f(X) = X^3 - 2X + 2 \in \mathbb{Z}[X]$, il est d'Eisenstein en 2, alors il est irréductible sur $\mathbb{Q}$.*
Soit θ une racine de $f(X)$ dans $\overline{\mathbb{Q}}$,on note $K = \mathbb{Q}(\theta)$ d'anneau d'entier $\mathcal{O}_K$.
D'après le Théorème 1, on a

$$2\mathcal{O}_K = \mathfrak{p}^3, \quad 5\mathcal{O}_K = \mathfrak{p}, \quad 7\mathcal{O}_K = \mathfrak{p}, \quad 11\mathcal{O}_K = \mathfrak{pq}$$

Soit $g(X) = X^3 + 9X + 27 \in \mathbb{Z}[X]$, il engendre sur $\mathbb{Q}$ la même extension que le, polynôme $f(X) = \frac{1}{3^3}g(3X) = X^3 + X + 1$ qui est irréductible sur $\mathbb{Q}$. Soit $K = \mathbb{Q}(\theta)$ le corps obtenu par adjonction à $\mathbb{Q}$ d'une racine θ de g dans $\overline{\mathbb{Q}}$ et $\mathcal{O}_K$ l'anneau des entiers de K.
Par le Théorème 1 on aura

$$2\mathcal{O}_K = \mathfrak{p}, \quad 3\mathcal{O}_K = \mathfrak{p}^2 \text{ et } 5\mathcal{O}_K = \mathfrak{p}$$

A la lumière des résultats du théorème ci-dessus, examinons quelques exemples de décompositions de nombres premiers $p > 3$. dans les cas où $p \nmid ab$, s_p pair et $\left(\frac{\Delta_p}{p}\right) = 1$.

Cas $p = 5$

Soient $a, b \in \mathbb{Z}$ tels que $5 \nmid ab$, s_5 pair et $\left(\dfrac{\Delta_5}{5}\right) = 1$, ce qui veut dire que $\overline{\Delta_5} \in \left\{\overline{1}, \overline{4}\right\}$.

- Supposons que $\Delta \equiv 0 \bmod 5$, cela veut dire que $a^3 \equiv 3b^2 \bmod 5$, alors

$$\left(\overline{a}, \overline{b}\right) \in E = \left\{\left(\overline{2}, \overline{1}\right), \left(\overline{2}, \overline{4}\right), \left(\overline{3}, \overline{2}\right), \left(\overline{3}, \overline{3}\right)\right\}.$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, où $\left(\overline{a}, \overline{b}\right) \in E$, admet une racine simple et une racine double dans $\mathbb{F}_5$; alors d'après le Théorème 1 on a

$$5\mathcal{O}_K = \mathfrak{b}\mathfrak{p}\mathfrak{q}.$$

  Ainsi, l'identité $a^3 \equiv 3b^2 \bmod 5$ entraine $5\mathcal{O}_K = \mathfrak{b}\mathfrak{p}\mathfrak{q}$..

- Supposoons que $\Delta \not\equiv 0 \bmod 5$, alors $\overline{\Delta} \in \left\{\overline{1}, \overline{4}\right\}$ ce qui signifie que

$$\left(\overline{a}, \overline{b}\right) \in F = \left\{\left(\overline{1}, \overline{2}\right), \left(\overline{1}, \overline{3}\right), \left(\overline{2}, \overline{2}\right), \left(\overline{2}, \overline{3}\right) \left(\overline{3}, \overline{1}\right), \left(\overline{3}, \overline{4}\right), \left(\overline{4}, \overline{1}\right), \left(\overline{4}, \overline{4}\right)\right\}.$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, où $\left(\overline{a}, \overline{b}\right) \in F$, est irréductible sur $\mathbb{F}_5$; alors d'après le Théorème 1 on a

$$5\mathcal{O}_K = \mathfrak{p}.$$

  Ainsi, $4\overline{a}^3 - 2\overline{b}^2 \in \left\{\overline{1}, \overline{4}\right\}$implique $5\mathcal{O}_K = \mathfrak{p}$.

En conclusion, ona les équivalences suivantes

- $5\mathcal{O}_K = \mathfrak{b}\mathfrak{p}\mathfrak{q}$ si, et seulement si, $a^3 \equiv 3b^2 \bmod 5$
- $5\mathcal{O}_K = \mathfrak{p}$ si, et seulement si, $4\overline{a}^3 - 2\overline{b}^2 \in \left\{\overline{1}, \overline{4}\right\}$

Cas $p = 7$

Soient $a, b \in \mathbb{Z}$ tels que $7 \nmid ab$, s_5 pair et $\left(\dfrac{\Delta_7}{7}\right) = 1$, ce qui veut dire que $\overline{\Delta_7} \in \left\{\overline{1}, \overline{2}, \overline{4}\right\}$.

- Supposons que $\Delta \equiv 0 \bmod 7$, cela veut dire que $a^3 \equiv 5b^2 \bmod 7$, alors

$$\left(\overline{a}, \overline{b}\right) \in E = \left\{\left(\overline{3}, \overline{2}\right), \left(,\overline{3}, \overline{5}\right), \left(\overline{5}, \overline{2}\right), \left(\overline{5}, \overline{5}\right), \left(\overline{6}, \overline{2}\right), \left(\overline{6}, \overline{5}\right)\right\}.$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, où $\left(\overline{a}, \overline{b}\right) \in E$, admet une racine simple et une racine double dans $\mathbb{F}_7$; alors d'après le Théorème 1 on a

$$7\mathcal{O}_K = \mathfrak{bpq}.$$

  Ainsi, l'identité $a^3 \equiv 5b^2 \bmod 5$ entraine $7\mathcal{O}_K = \mathfrak{bpq}$.

- Supposoons que $\Delta \not\equiv 0 \bmod 7$, alors $\overline{\Delta} \in \left\{\overline{1}, \overline{2}, \overline{4}\right\}$ ce qui signifie que $\left(\overline{a}, \overline{b}\right) \in F_1 \cup F_2$, où

$$F_1 = \left\{\left(\overline{1}, \overline{2}\right), \left(\overline{1}, \overline{5}\right), \left(\overline{2}, \overline{2}\right), \left(\overline{2}, \overline{5}\right) \left(\overline{3}, \overline{1}\right), \left(\overline{3}, \overline{4}\right), \left(\overline{3}, \overline{6}\right)\right\}$$

  et

$$F_2 = \left\{\left(\overline{4}, \overline{2}\right), \left(\overline{4}, \overline{5}\right), \left(\overline{5}, \overline{1}\right), \left(\overline{5}, \overline{6}\right), \left(\overline{6}, \overline{1}\right), \left(\overline{6}, \overline{6}\right)\right\}.$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, où $\left(\overline{a}, \overline{b}\right) \in F$, est irréductible sur $\mathbb{F}_7$; alors d'après le Théorème 1 on a

$$7\mathcal{O}_K = \mathfrak{p}.$$

  Ainsi, $\overline{4}\overline{a}^3 - \overline{6}\overline{b}^2 \in \left\{\overline{1}, \overline{2}, \overline{4}\right\}$implique $7\mathcal{O}_K = \mathfrak{p}$.

En conclusion, ona les équivalences suivantes

- $7\mathcal{O}_K = \mathfrak{bpq}$ si, et seulement si, $a^3 \equiv 5b^2 \bmod 7$

- $7\mathcal{O}_K = \mathfrak{p}$ si, et seulement si, $\overline{4}\overline{a}^3 - \overline{6}\overline{b}^2 \in \left\{\overline{1}, \overline{2}, \overline{4}\right\}$

Cas $p = 11$.

Soient $a, b \in \mathbb{Z}$ tels que $11 \nmid ab$, s_5 pair et $\left(\dfrac{\Delta_{11}}{11}\right) = 1$, ce qui veut dire que $\overline{\Delta_{11}} \in \left\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\right\}$.

- Supposons que $\Delta \equiv 0 \bmod 11$, cela veut dire que $a^3 \equiv 4b^2 \bmod 11$, alors

  $$\left(\overline{a}, \overline{b}\right) \in E = \left\{\left(\overline{1}, \overline{5}\right), \left(\overline{1}, \overline{6}\right), \left(\overline{3}, \overline{2}\right), \left(\overline{3}, \overline{9}\right) \left(\overline{4}, \overline{4}\right), \left(\overline{4}, \overline{7}\right), \left(\overline{5}, \overline{1}\right), \left(\overline{5}, \overline{10}\right), \left(\overline{9}, \overline{3}\right), \left(\overline{9}, \overline{8}\right)\right\}.$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, où $\left(\overline{a}, \overline{b}\right) \in E$, admet une racine simple et une racine double dans $\mathbb{F}_{11}$; alors d'après le Théorème 1 on a

  $$11\mathcal{O}_K = \mathfrak{bpq}.$$

  Ainsi, l'identité $a^3 \equiv 4b^2 \bmod 11$ entraine $7\mathcal{O}_K = \mathfrak{bpq}$.

- Supposoons que $\Delta \not\equiv 0 \bmod 11$, alors $\overline{\Delta} \in \left\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\right\}$ ce qui signifie que $\left(\overline{a}, \overline{b}\right) \in F \cup G$ avec

  $$F = \left\{\left(\overline{2}, \overline{1}\right), \left(\overline{2}, \overline{10}\right), \left(\overline{6}, \overline{4}\right), \left(\overline{6}, \overline{7}\right) \left(\overline{7}, \overline{5}\right), \left(\overline{7}, \overline{6}\right), \left(\overline{8}, \overline{3}\right), \left(\overline{8}, \overline{8}\right), \left(\overline{10}, \overline{2}\right), \left(\overline{10}, \overline{9}\right)\right\}.$$
  $$= \left\{(\overline{x}, \overline{y}) \in \left(\mathbb{F}_{11}^*\right)^2 \text{ tels que } x^3 \equiv 8y^2 \bmod 11\right\}$$

  et

  $$G = \left\{(\overline{x}, \overline{y}) \in \left(\mathbb{F}_{11}^*\right)^2 \text{ tels que } x^3 \not\equiv 8y^2 \bmod 11 \text{ et } \left(\overline{4}\overline{x}^3 - \overline{5}\overline{y}^2\right) \in \left\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\right\}\right\}$$

  Le polynôme $X^3 - \overline{a}X + \overline{b}$, admet trois racine simples dans $\mathbb{F}_{11}$ si $\left(\overline{a}, \overline{b}\right) \in F$, et il est irréductible sur $\mathbb{F}_{11}$ si $\left(\overline{a}, \overline{b}\right) \in G$; alors d'après le Théorème 1 on a

  $$\begin{cases} 11\mathcal{O}_K = \mathfrak{bpq}. & \text{si } \left(\overline{a}, \overline{b}\right) \in F \\ 11\mathcal{O}_K = \mathfrak{p}. & \text{si } \left(\overline{a}, \overline{b}\right) \in G \end{cases}$$

  Ainsi,

  $$a^3 \equiv 8b^2 \bmod 11 \text{ implique } 11\mathcal{O}_K = \mathfrak{bpq}$$

  et

  $$x^3 \not\equiv 8y^2 \bmod 11 \text{ et } \left(\overline{4}\overline{x}^3 - \overline{5}\overline{y}^2\right) \in \left\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\right\} \text{ impliquent } 11\mathcal{O}_K = \mathfrak{p}$$

En conclusion, ona les équivalences suivantes

- $11\mathcal{O}_K = \mathfrak{bpq}$ si, et seulement si, $a^3 \equiv 4b^2$ ou $8b^2 \bmod 11$

- $11\mathcal{O}_K = \mathfrak{p}$ si, et seulement si, $x^3 \not\equiv 8y^2 \bmod 11$ et $\left(\overline{4}\overline{x}^3 - \overline{5}\overline{y}^2\right) \in \left\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\right\}$.

3.2 Calcul de la valuation p-adique de d_K

Nous utiliserons le Théorème 1 pour la détermination de la valuation $v_p(d_K)$ du discriminant du corps de nombre K.

Rappelons le résultat suivant donnant une relation entre la valuation du discriminant d_K) du corps de nombres K et les indices de ramification et les degrés résiduels des idéaux premiers de K au dessus d'un nombre premier p

Lemme 3.4 *Soit L un corps de nombres de degré n, de discriminant D_L. Soit p un nombre premier dont la décomposition dans L est*

$$p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g},$$

alors

$$v_p(D_L) \geq \sum_{i=1}^{g} (e_i - 1) f_i.$$

L'égalité a lieu si, et seulement si, la ramification est modérée, en d'autres termes lorsue $p \nmid e_i$, $1 \leq i \leq g$.

Preuve : [12, Proposition 4, Chapitre IV, §1]

□

Nous supposerons vérifiées les hypothèses du Théorème 1.

Théorème 3.5 *Sous les hypothèses du Théorème 1 nous aurons*

- *Si $p > 3$, alors*

  - *$v_p(d_K)) = 2$ si, et seulement si, $1 \leq v_p(b) \leq v_p(a)$,*

- $v_p(d_K)) = 1$ *si, et seulement si,* s_p *est impair,*
- $v_p(d_K)) = 0$ *si, et seulement si,* s_p *est pair et* $p \nmid a$ *ou* $p \nmid b$.

- *Si* $p = 2$, *alors*

  - $v_p(d_K)) = 3$ *si, et seulement si,* s_2 *est impair,*
  - $v_p(d_K)) = 2$ *si, et seulement si,* $\begin{cases} 1 \leq v_2(b) \leq v_2(a) \\ ou \\ s_2 \text{ pair et } \Delta_2 \equiv 3 \, mod \, 4 \end{cases}$
  - $v_p(d_K)) = 0$ *si, et seulement si,* $\begin{cases} b \text{ impair} \\ ou \\ a \text{ impair } s_2 \text{ pair et } \Delta_2 \not\equiv 3 \, mod \, 4 \end{cases}$

- *Si* $p = 3$, *alors*

  - $v_3(d_K)) = 5$ *si, et seulement si,* $1 \leq v_3(b) \leq v_3(a)$
  - $v_3(d_K)) = 4$ *si, et seulement si,* $\begin{cases} v_3(a) = v_3(b) = 2 \\ ou \\ a \equiv 3 \mod 9, \, 3 \nmid betb^2 \not\equiv 4 \, mod \, 9 \end{cases}$
  - $v_3(d_K)) = 3$ *si, et seulement si,* $\begin{cases} v_3(a) = v_3(b) = 1 \\ ou \\ 3 \mid a, \, 3 \nmid b, \, a \not\equiv 3 \, mod \, 9 \text{ et } b^2 \not\equiv 4 \, mod \, 9 \\ ou \\ a \equiv 3 \mod 9, b^2 \equiv 4 \, mod \, 9 \text{ et } b^2 \not\equiv a + 1 \, mod \, 27 \end{cases}$
  - $v_3(d_K)) = 1$ *si, et seulement si,* $\begin{cases} 1 = v_3(a) \text{ et } v_3(a) < v_3(b) \\ ou \\ 3 \mid a, \, a \not\equiv 3 \, mod \, 9 \text{ et } b^2 \equiv a + 1 \mod 9 \\ ou \\ a \equiv 3 \mod 9, b^2 \equiv a + 1 \, mod \, 27 \text{ et } s_3 impair \end{cases}$

– $v_3(d_K)) = 0$ *si, et seulement si,* $\begin{cases} 3 \nmid a \\ \text{ou} \\ a \equiv 3 \mod 9,\ 3 \nmid b \text{et} b^2 \equiv a+1 \mod 27 \ \text{ et } s_3 \text{pair} \end{cases}$

Preuve : Nous allons démontrer les résultats de chacune des situations présentées dans le théorème.

1. Cas $p > 3$.

   - Montrons que $v_p(d_K)) = 2$ si, et seulement si, $1 \leq v_p(b) \leq v_p(a)$.
     - Supposons que $v_p(d_K) = 2$, alors s_p est pair avec $s_p \geq 2$.
       Si $p \nmid ab$, le Théorème 1 implique que p ne se ramifie pas dans K et par suite $v_p(d_K) = 0$, ce qui est absurde. Ainsi $p \mid ab$.
       Comme $s_p \neq 0$ et $p \mid ab$, alors $p \mid a$ et $p \mid b$.
       Si $v_p(a) = 1$ et $v_p(a) < v_p(b)$, alors $p\mathcal{O}_K = \mathfrak{pq}^2$ et donc, d'après le Lemme 4, $v_p(d_K) = 1$, ce qui est absurde. Ainsi, $1 \leq v_p(a) \leq v_p(b)$
     - Inversement, supposons que $1 \leq v_p(a) \leq v_p(b)$, alors $p \mid a$ et $p \mid b$, et d'après le théorème 1 on a $p\mathcal{O}_K = \mathfrak{p}^3$ ce qui, d'après le Lemme 4, donne $v_p(d_K) = 2$.
   - Montrons que $v_p(d_K) = 1$si, et seulement si, s_p est impair.
     - Comme s_p est pair si, et seulement si, $v_p(d_K)$ est pair, alors $v_p(d_K) = 1$ implique s_p impair.
     - Inversement, supposons que s_p est impair.
       Si $p \nmid ab$, alors, par le Théorème 1, on a $p\mathcal{O}_K = \mathfrak{pq}^2$ ce qui, d'après le Lemme 4, entraine $v_p(d_K) = 1$.
   - Montrons que : $v_p(d_K) = 0$ si, et seulement si, s_p pair et ($p \nmid a$ ou $p \nmid b$).
     - Supposons que $v_p(d_K) = 0$, alors s_p est pair.
       Si $p \mid a$ et $p \mid b$ alors, d'après le Théorème 1, p se ramifie dans K et par suite $v_p(d_K) \geq 1$, ce qui est absurde.

Par conséquent, si $v_p(d_K) = 0$, alors s_p est pair et on a $p \nmid a$ ou $\nmid b$.

– Inversement, si $p \nmid a$ ou $p \nmid b$ et si s_p est pair, alors, et d'après le Théorème 1, p ne se ramifie pas dans K, ce qui implique que $v_p(d_K) = 0$.

2. Cas $p = 2$.

- Montrons que $v_2(d_K) = 3$ si, et seulement si, s_2 est impair.
  – Supposons que $v_2(d_K) = 3$, alors $v_2(d_K)$ est impair, ce qui implique que s_2 est impair.
  – Inversement, supposons que s_2 est impair, alors $v_2(d_K)$ est impair ce qui, d'après le Lemme 4, entraine $v_2(d_K) = 3$, puisque s_2 est impair. Cette dernière condition implique, d'après le Lemme 4, $2\mathcal{O}_K \neq \mathfrak{p}^3$.
  Si $2 \mid a$, alors $2\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$, d'après le Théorème 1, et par suite $v_2(d_K) = 3$, d'après le Lemme 4, car s_1 est impair.
- Montrons que $v_2(d_K) = 2$ si, et seulement si, $\begin{cases} 1 \leq v_2(a) \leq v_2(b) \\ \text{ou} \\ s_2 \text{ pair et } \Delta_2 \equiv 3 \bmod 4 \end{cases}$.
  – Supposons que $v_2(d_K) = 2$, alors s_2 est pair.
  Si b est impair, et d'après le Théorème 1, alors 2 ne se ramifie pas dans K, par suite on a $v_2(d_K) = 0$ ce qui est absurde.
  Ainsi, b est pair.
  Si a est impair, alors $\Delta_2 \equiv 3 \bmod 4$ puisque s_2 est pair et donc 2 se ramifie dans K.
  Soit a pair avec $v_2(a) = 1$ et $v_2(b) > 1$. Si $v_2(b) \geq 3$, alors $s_2 = 5$ et par suite $v_2(d_K)$ est impair, ce qui est absurde. Par conséquent, $v_2(b) = 2$.
  Ainsi, on pose $b = 4b'$ et $a = 2a'$ avec $2 \nmid a'b'$. Alors $\Delta = 4a^3 -$

$27b^2 = 16\left(2a'^3 - 27b'^3\right)$ et par suite $s_2 = 4$ et $\Delta_2 = 2a'^3 - 27b'^2$.
Par suite, $\Delta_2 \equiv 3 \bmod 4$ puisque $a'b' \equiv 1$ ou $3 \bmod 4$ et on a

$$v_2(d_K) = 2 \Rightarrow \begin{cases} 1 \leq v_2(b) \leq v_2(a) \\ \text{ou} \\ s_2 \text{ pair et } \Delta_2 \equiv 3 \bmod 4 \end{cases}.$$

– Inversement, supposons que $\begin{cases} 1 \leq v_2(b) \leq v_2(a) \\ \text{ou} \\ s_2 \text{ pair et } \Delta_2 \equiv 3 \bmod 4 \end{cases}$.
Si $1 \leq v_2(b) \leq v_2(a)$, alors $2 \mid a$ et $2 \mid b$ et par suite, d'après le Théorème 1, on aura $2\mathcal{O}_K = \mathfrak{p}^3$ce qui, d'après le Lemme 4, entraine $v_2(d_K) = 2$.
Si $v_2(a) < v_2(b)$, alors $2 \mid b$. On suppose de plus que s_2 pair et $\Delta_2 \equiv 3 \bmod 4$.

* Si $2 \mid a$, et par le Théorème 1, alors $2\mathcal{O}_K = \mathfrak{pq}^2$, ce qui, d'après le Lemme 4, donne $v_2(d_K) = 2$, puisque
* Si $2 \nmid a$, alors, d'après le Théoeème 1, $2\mathcal{O}_K = \mathfrak{pq}^2$, ce qui, d'après le Lemme 4, donne $v_2(d_K) = 2$ puisque s_2 est pair s_2 est pair.

Par conséquent, on a

$$\begin{cases} 1 \leq v_2(b) \leq v_2(a) \\ \text{ou} \\ s_2 \text{ pair et } \Delta_2 \equiv 3 \bmod 4 \end{cases} \Rightarrow v_2(d_K) = 2.$$

- Montrons que

$$v_2(d_K) = 0 \Leftrightarrow \begin{cases} b \text{ impair} \\ \text{ou} \\ a \text{ impair}, s_2 \text{ pair et } \Delta_2 \not\equiv 3 \bmod 4 \end{cases}.$$

– Supposons que b est impair, alors $2 \nmid \Delta$ et $2 \nmid d_K$ ce qui entraine que $v_2(d_K) = 0$.
Supposons que b est pair, a est impair, $s_2$est pair et $\Delta_2 \not\equiv 3 \bmod 4$.
Alors, d'après le Théorème 1, 2 est non ramifié dans K ce qui implique que $v_2(d_K) = 0$.

– Inversement, on suppose que $v_2(2\mathrm{O}_K = \mathfrak{pq} = 0$ par suite s_2 est pair. Comme $v_2(2\mathrm{O}_K = \mathfrak{pq} \notin \{2, 3\}$, alors $2\mathcal{O}_K \neq \mathfrak{p}^3$ et $2\mathcal{O}_K \neq \mathfrak{pq}^2$.
Si b est pair, alors a est impair et $\Delta_2 \not\equiv 3 \bmod 4$.

3. Cas $p = 3$
Les deux derniers cas sont des cas étudiés du Théorème 3 précédent. Il reste à étudier les cas liés à la valuation 3-adique $v_3(d_K) \geq 3$ du discriminant d_K).
par le lemme 4, cela correspond au cas $3\mathcal{O}_K = \mathfrak{p}^3$. Connaissant la valeur de $v_3(\Delta)$ on tire celle de $v_3(d_K)$. Si $v_3(\Delta) = 3$ alors $v_3(d_K) = 3$, et si $v_3(\Delta)$ pair entraine $v_3(d_K) = 4$. Par conséquent, il ne reste à étudier que les cas suivants : $v_3(b) < v_3(a)$, avec $v_3(b) = 1$ ou 2, et lorsqu'on a à la fois $a \equiv 3 \bmod 9$, $b^2 \equiv 4 \bmod 9$ et $b^2 \not\equiv a + 1 \bmod 27$.

• Montrons que $1 \leq v_3(b) < v_3(a)$ implique $v_3(d_K) = 5$.

– Supposons que $1 \leq v_3(a) < v_3(b)$, alors $v_3(b) \in \{1, 2\}$.

∗ Si $v_3(b) = 1$ et $v_3(a) > 1$, alors $s_3 = 5$.
Dans ce cas, $f(X) \equiv X^3 \bmod 3$ et $f(X) = X^3 + M(X)$ où $M(X) = -a'X + b'$, avec a' et b' dans $\mathbb{Z}$ et tels que $3 \mid a'$ et $3 \nmid b'$.
Puisque $X \nmid M(X) \bmod 3$, alors, d'après le Lemme 2, $3 \nmid i(\theta)$, et par suite $v_3(d_K) = s_3 = 5$.

$*$ Si $v_3(b) = 2$ et $v_3(a) > 2$, alors $s_3 = 7$. Dans ce cas on pose $\theta_1 = \dfrac{\theta_2}{3}$, alors θ_1 est racine du polynôme $g(X)$ donné par

$$g(X) = X^3 - \frac{2a}{3}X^2 + \frac{a^2}{9}X - \frac{b^2}{27} \in \mathbb{Z}[X],$$

il est d'Eisenstein en $p = 3$, donc irréductible sur $\mathbb{Q}$.
De plus, $g(X) \equiv X^3 \bmod 3$ ce qui entraine que

$$g(X) = X^3 + 3M_1(X)$$

, où $M_1(X) = a_1X^2 + b_1X + C_1 \in \mathbb{Z}[X]$ avec $3 \mid a_1$, $3 \mid b_1$ et $3 \nmid c_1$.
Comme $X \nmid M_1(X) \bmod 3$, alors d'après le Lemme 2 on a $3 \nmid i(\theta_1)$, par suite $v_3(d_K) = v_3(\Delta_1)$, où $\Delta_1 = \dfrac{\Delta b^2}{27}$ est le discriminant de $g(X)$. Ainsi, $v_3(d_K) = 5$, d'où

$$1 \leq v_3(b) < v_3(a) \text{ implique } v_3(d_K) = 5$$

– Soit $a \equiv 3 \bmod 9$, $b^2 \equiv 4 \bmod 9$ et $b^2 \not\equiv a + 1 \bmod 27$. Dans ce cas $v_5(\Delta) = 5$. Par le Théorème 3.1 on a $3 \mid i(\theta)$, ce qui entraine que $v_3(d_K) \leq 3$, d'après le Lemme 2. Ainsi, par le Théorème 1, on a $2\mathcal{O}_K = \mathfrak{p}^3$ ce qui, par le Lemme 4, entraine $v_3(d_K) = 3$

□

Exemple 23 *Examinons quelques exemples de calcul de l'indice de θ, racine d'un trinôme irréductible de degré 3, dans l'anneau des entiers d'un corps de nombre engendré sur $\mathbb{Q}$ par cette racine.*

1. *Soit $f(X) = X^3 - 3X + 3 \in \mathbb{Z}[X]$, il est d'Eisenstein en 3, alors il est irréductible sur $\mathbb{Q}$.*

Soit θ une racine de f dans $\overline{\mathbb{Q}}$, et soit $K = \mathbb{Q}(\theta)$ le corps obtenu par adjonction de θ au corps des nombres rationnels.
Le discriminant Δ de f est : $\Delta = -5 \times 3^3$. Comme $v_3(-3) = v_3(3) = 1$, d'après le Théorème 2 on a $v_3(d_K)) = 3$.
De plus, $v_5(\Delta) = 1$, alors $v_5(d_K) = 1$.
Par conséquent, $i(\theta) = \sqrt{\dfrac{\Delta}{D}} = 1$.

2. *Soit $g(X) = X^3 - 60X + 90 \in \mathbb{Z}[X]$, il est irréductible sur $\mathbb{Q}$. Soit θ une racine de g dans $\overline{\mathbb{Q}}$ et soit $K = \mathbb{Q}(\theta)$.*
le discriminant Δ de g est donné par

$$\Delta = 645300 = 2^2 \times 3^3 \times 5^2 \times 239$$

On pose $a = 60$ et $b = 90$, alors on a

$$v_2(a) = 2,\ v_2(b) = 1,\ v_3(a) = 1,\ v_3(b) = 2,\ v_5(a) = v_b(b) = 1$$

et $v_{239}(a) = v_{239}(b) = 0$.
par le Théorème 2 on a

$$v_2(d_K) = 2,\ v_3(d_K) = 1,\ v_5(d_K) = 2 \ \text{ et } v_{239}(d_K) = 1,$$

par suite

$$D = 2^2 \times 3 \times 5^2 \times 239 = 71700.$$

Ainsi l'indice $i(\theta)$ est égal à

$$i(\theta) = \sqrt{\frac{\Delta}{D}} = \sqrt{9} = 3$$

Le théorème ci-dessus permet de donner une preuve relativement aisée du Théorème de HASSE : [HASSE]

Soit d le discriminant de $\mathbb{Q}\left(\sqrt{d_K}\right)$, où $d_K)$ désigne le discriminant du corps K. Alors on a

$$D = d \times 3^{2m} \times f^2$$

où

- $f = \prod_{i=1}^{g} p_i$, les p_i sont des nombres premiers distincts, $\mathrm{p\,gcd}\,(f, 3d) = 1$ et $p_i \equiv \left(\frac{d}{p_i}\right) \bmod 3$, $\forall i \in \{1, \ldots g\}$.
- $0 \leq m \leq 2$, avec $m \neq 1$ si $3 \nmid d$ et $m \neq 2$ si $d \equiv 3 \bmod 9$.

Pour la preuve du Théorème précédent, nous aurons besoin du critère suivant de Stickelberger [7] :

Critère Si K est un corps de nombres algébriques, soit $\{x_1, \ldots, x_n\}$ une base de $\mathbb{Q}$-espace vectoriel K formée d'éléments entiers sur $\mathbb{Z}$. Alors

$$D_{K/\mathbb{Q}}\,(x_1, \ldots, x_n) \equiv 0 \text{ ou } 1 \bmod 4.$$

Preuve : Soit $D = d_0 \times 3^{2m} \times f_0^2$, d_0 est un entier sans facteur carré et $\mathrm{p\,gcd}\,(f_0, 3d) = 1$, et on a $\mathbb{Q}\left(\sqrt{d_K}\right) = \mathbb{Q}\left(\sqrt{d_0}\right)$.
Si $d_0 \equiv 1 \bmod 4$, alors $d = d_0$.
Supposons que $d_0 \not\equiv 1 \bmod 4$, cela veut dire que $d_0 \equiv 2$ ou $3 \bmod 4$. Par le Critère de Stickelberger on tire $D \not\equiv 1 \bmod 4$, ce qui veut dire que $D \equiv 0 \bmod 4$.

Si f_0 est impair, alors $D \equiv 2$ ou $3 \bmod 4$, ce qui est absurde d'après le critère de Stickelberger. Par suite, f_0 est pair, $f_0 = 2f_1$ce qui donne

$$D = 4d_0 \times 3^{2m} f_1^2 = d \times 3^{2m} \times f_1^2.$$

Par conséquent $d_K)$ s'écrit toujours sous la forme (ii).

- Montrons que $p_i = \left(\frac{d}{p_i}\right) \bmod 3$

– Soit $p_i \mid f$, p_i premier impair.
Comme $\mathrm{p\,gcd}\,(f_0, 3d) = 1$, alors $p_i > 3$. On a alors les équivalences suivantes

$$p \mid f \Leftrightarrow v_p\,(d_K) = 2$$

ce qui, par le Théorème 2 est équivalent à $1 \leq v_p\,(b) \leq v_p\,(a)$. Mais alors, le Théorème 1 montre qu'il y a équivalence entre $1 \leq v_p\,(b) \leq v_p\,(a)$ et la forme $p\mathcal{O}_K = \mathfrak{p}^3$ de la décomposition d p dans K.
Par conséquent, pour un nombre premier p tel que $3 < p \mid f$ on a

$$\left(\frac{d}{p}\right) = \left(\frac{\Delta_p}{p}\right) = \left(\frac{-27}{p}\right) = \left(\frac{-3}{p}\right) \equiv p \bmod 3.$$

– Soit $p = 2$, alors la condition $2 \mid f$ entraine $2 \nmid d$. Ainsi, $v_2\,(d_K) = 2$, ce ci entraine d'après le Théorème 4 $1 \leq v_2(b) \leq v_2(a)$. Par suite, $d = \Delta_2 \equiv 5 \bmod 8$. par conséquent on a

$$\left(\frac{d}{p}\right) = \left(\frac{d}{2}\right) \equiv 2 \bmod 3.$$

- Montrons que $0 \leq m \leq 2$; avec $m \neq 1$ si $3 \nmid d$ et $m \neq 2$ si $d \equiv 3 \bmod 9$.
Par le Théorème 2 on tire $0 \leq m \leq 2$.

– Par le Théorème 2 on a $v_3\,(d_K) \neq 2$, ce qui montre que si $3 \nmid d$ alors $m \neq 1$

– Par le Théorème 2, si $3 \mid d$, alors $v_3\,(d_K) = 1$. De plus, si $d \equiv 3 \bmod 9$ et $m = 2$, le Théorème 2 implique que $1 \leq v_3\,(b) \leq v_3\,(a)$. Ceci correspond à $\Delta_3 \equiv -1 \bmod 3$ ou encore $d \equiv 6 \bmod 9$. Par conséquent, si $d \equiv 3 \bmod 9$, alors $m \neq 2$.

□

3.3 Caractérisation des corps de nombres dont 2 est un diviseur inessentiel

Une autre application du Théorème 3 est la caractérisation des corps dont 2 est un diviseur de l'indice $i(\theta)$ de l'élément entier primitif θ. Soit K un corps de nombres. On appelle diviseur commun inessentiel du discriminant d_K) de K, le nombre $i(K)$

$$i(K) = \mathrm{p\,gcd}\{i(\theta) \text{ où } \theta \text{ est un entier de } K = \mathbb{Q}(\theta)\}$$

Dans la décomposition d'un nombre premier p, celui-ci peut-être un diviseur de $i(\theta)$, c'est le cas notamment de l'exemple classique où θ est une racine dans $\overline{\mathbb{Q}}$ du polynôme irréductible $X^3 + X^2 - 2X + 8$ dû à Dedekind. D'autre part, ces nombres premier inessentiels sont en nombre au plus égal à $[K : \mathbb{Q}] - 1$.
Dans le cas d'un corps cubique K, $i(K) = 1$ ou 2.
Engstrom ([ENG]) donne une caractérisation des corps cubiques où le diviseur commun inessentiel du discriminant est 2

Proposition 3.6 *Soit K un corps cubique de nombres algébriques, alors on a l'équivalence suivante*

$$i(K) = 2 \Leftrightarrow 2\mathcal{O}_K = \mathfrak{bpq}$$

Soit 2^χ la plus grande puissance de 2 dans la factorisation de $i(\theta)$, θ*étant*un élément primitif de K.
D'après Engstrom [5, p. 234], on a $\chi = 1$, cela veut dire que 2 est la plus grande puissance de 2 dans la factorisation de $i(\theta)$, par suite

$$2\mathcal{O}_K = \mathfrak{bpq} \Leftrightarrow 2 \mid i(\theta),\ \forall \theta \text{ entier primitif de } K$$

Par conséquent, compte tenu du fait que $i(K) \in \{1, 2\}$, on a l'équivalence

$$2\mathcal{O}_K = \mathfrak{bpq} \Leftrightarrow i(K) = 2.$$

Théorème 3.7 *Avec les mêmes hypothèses du Théorème 3.1 on a*

$$i(K) = 2 \Leftrightarrow a \textit{ impair}, b \textit{ bair}, s_2 \textit{ pair et } \Delta_2 \equiv 1 \textit{ mod } 8.$$

Preuve : D'après la Proposition 3.3 on a

$$i(K) = 2 \Leftrightarrow 2\mathcal{O}_K = \mathfrak{bpq}$$

et d'après le Théorème 3.1 on a

$$2\mathcal{O}_K = \mathfrak{bpq} \Leftrightarrow a \text{ impair}, b \text{ bair}, s_2 \text{ pair et } \Delta_2 \equiv 1 \bmod 8$$

En combinant les deux équivalences précédentes on aura

$$i(K) = 2 \Leftrightarrow a \text{ impair}, b \text{ bair}, s_2 \text{ pair et } \Delta_2 \equiv 1 \bmod 8$$

□

Bibliographie

[1] Y. AMICE, "<Les nombre p-adiques">, PUF, 1ère Edition, 1975
[2] B. BENSEBAA, "<Groupe de Galois de trinômes">, Thèse de Doctorat d'Etat, USTHB, Décembre 2008,
[3] Z. BOREVITCH, "<Théorie des Nombres">, Gauthier villard, ed. 1967
[4] S.D. COHEN, A. MOVAHHEDI and A. SALINIER, "<Factorization over local fields and the irreductibility of generalized difference polynomials">, J.N.T, 2000
[5] H. ENGSTROM, "<On the common index divisors of an algebraic field,
[6] P. ESCOFIER, "<Théorie de Galois">, DUNOD, 2000
[7] E. HALLOUIN, "<Parcourt initiatique à travers la théorie des valuations,
[8] J. MONTES, E. NART, "<Théorie de ORE">
[9] N. NARKIEWICZ, "<Elementary and analytic Theory of algebraic number">, Monogr. Math. 57 (1974)
[10] J. J. PAYAN, "<Sur les extensions cubiques non galoisiennes des rationnel et leur clôture galoisienne">, J. Reine Angew. Math 228(1967), 15-37_ [11] P. SAMUEL, "<Théorie algébrique des nombres">, HERMAN, 1967
[12] J.P. SERRE "<Cours d'arithmétiques,">, PUF-2nd Edition, Paris, 1977
[13] J.P. SERRE, "<Corps locaux">,3ème Edition, HERMAN, 1980
[14] L. TORNHEIM, "<Minimal basis and inessential discriminant divisors for a cubic field">, Pacific J. Math. 5(1955), 623-631